Transformers, Large Language Models (LLMs), and Foundation Models

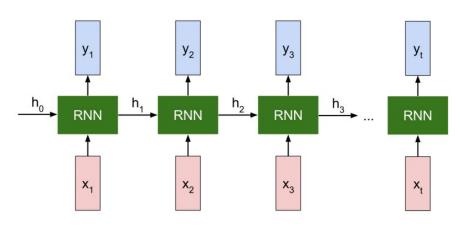
Ju Sun Computer Science & Engineering

Nov 15, 2023



Quick recap

RNN: model sequences

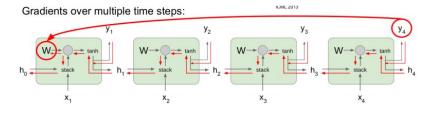


(Credit: Stanford CS231N)

$$egin{aligned} oldsymbol{h}_t &= anh \left(oldsymbol{W}_{oldsymbol{h}} oldsymbol{h}_{t-1} + oldsymbol{W}_{oldsymbol{x}} oldsymbol{x}_t
ight) \ oldsymbol{y}_t &= oldsymbol{V}_y oldsymbol{h}_t \end{aligned}$$

 ${f W}_h, {f W}_x$ and ${f V}_y$ are shared across the sequence

Vanishing/exploding gradient issue



(Credit: Stanford CS231N)

$$\frac{\partial L_t}{\partial W} = \frac{\partial L_t}{\partial \boldsymbol{h}_t} \frac{\partial \boldsymbol{h}_t}{\partial h_{t-1}} \cdots \frac{\partial \boldsymbol{h}_1}{\boldsymbol{W}} = \frac{\partial L_t}{\partial \boldsymbol{h}_t} \left(\prod_{k=2}^t \frac{\partial \boldsymbol{h}_k}{\partial \boldsymbol{h}_{k-1}} \right) \frac{\partial \boldsymbol{h}_1}{\partial \boldsymbol{W}}$$

$$= \frac{\partial L_t}{\partial \boldsymbol{h}_t} \left(\prod_{k=2}^t \operatorname{diag} \left(\tanh' \left(\boldsymbol{W}_h \boldsymbol{h}_{k-1} + \boldsymbol{W}_{\boldsymbol{x}} \boldsymbol{x}_k \right) \right) \boldsymbol{W}_h \right) \frac{\partial \boldsymbol{h}_1}{\partial \boldsymbol{W}}$$

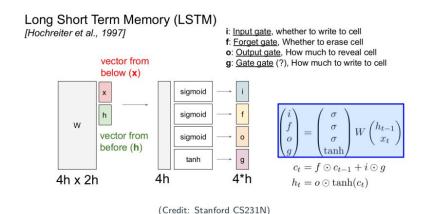
- * when $\|\boldsymbol{W}_h\| > 1$, gradient explodes if t large
- * when $\|\boldsymbol{W}_h\| < 1$, gradient vanishes if t large

$$\left\| \prod_{k=2}^{t} \operatorname{diag} \left(\tanh' \left(\boldsymbol{W}_{\boldsymbol{h}} \boldsymbol{h}_{k-1} + \boldsymbol{W}_{\boldsymbol{x}} \boldsymbol{x}_{k} \right) \right) \boldsymbol{W}_{h} \right\|$$

$$\leq \prod_{k=2}^{t} \left\| \operatorname{diag} \left(\tanh' \left(\boldsymbol{W}_{\boldsymbol{h}} \boldsymbol{h}_{k-1} + \boldsymbol{W}_{\boldsymbol{x}} \boldsymbol{x}_{k} \right) \right) \right\| \left\| \boldsymbol{W}_{h} \right\|$$

$$\leq \prod_{t} \left\| \operatorname{diag} \left(\tanh' \left(\boldsymbol{W}_{\boldsymbol{h}} \boldsymbol{h}_{k-1} + \boldsymbol{W}_{\boldsymbol{x}} \boldsymbol{x}_{k} \right) \right) \right\| \left\| \boldsymbol{W}_{h} \right\|^{t-1}$$

Gated RNNs



u: update gate, control state update

r: reset gate, control how previous state affects new content

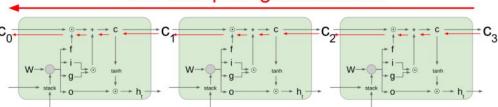
g: new content

Gated recurrent unit (GRU)

$$egin{aligned} egin{aligned} egin{aligned\\ egin{aligned} egi$$

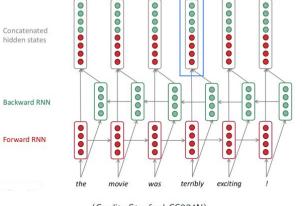
f, i, o are merged

Uninterrupted gradient flow!



(Credit: Stanford CS231N)

Modern RNNs



(Credit: Stanford CS224N) (Credit: Stanford CS231N)

RNN layer 3

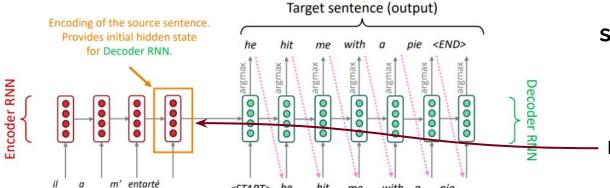
RNN layer 2

RNN layer 1

Bidirectional RNN

with

pie



hit

Seq2Seq model

Bottleneck problem

(Credit: Stanford CS231N)

<START> he

0000

0000

0000

terribly

000

0000

0000

exciting

0000

0000

0000

movie

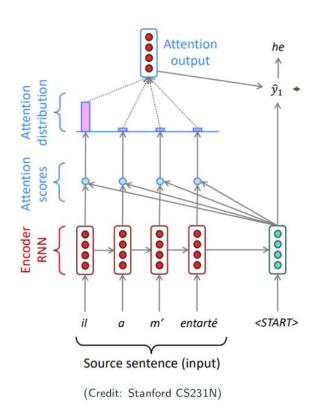
Deep RNN

0000

0000

0000

Attention mechanism



Input: source vectors $oldsymbol{s}_1,\dots,oldsymbol{s}_N\in\mathbb{R}^h$, and target vector $oldsymbol{t}$

Output: weighted summation

$$\sum_{j=1}^N w_j oldsymbol{s}_j$$
 where $w_j = ext{similarity}(oldsymbol{s}_j, oldsymbol{t})$

Many possibilities:

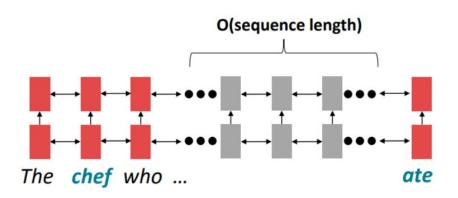
Attention scores

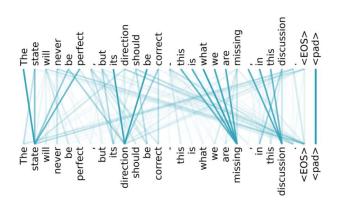
- dot-product attention: $\widehat{w_j}=\langle s_j,t\rangle$ (Is is better to normalize this or rescale it by the dimension factor?)
- multiplicative attention: $\widehat{w_j} = \langle s_j, Wt
 angle$
- "additive attention": $\widehat{w_j} = oldsymbol{v}^\intercal \sigma \left(oldsymbol{W}_1 oldsymbol{s}_j + oldsymbol{W}_2 oldsymbol{t}
 ight)$

The actual weights are attention scores passed through **softmax**

$$w_j = \frac{\exp\left(\widehat{w_j}\right)}{\sum_k \exp\left(\widehat{w_k}\right)}$$

Self-attention





RNN

- Long interaction distance
- Resistant to parallelization

Self-attention

- O(1) interaction distance
- Highly parallelizable

Each token gets a selective summary of information from all others

Self-attention

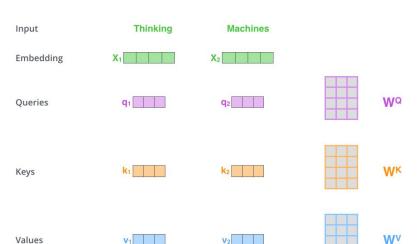


Image credit: https://jalammar.github.io/illustrated-transformer/

- Each word now encoded as (query, key, value) triple
- For an input x_i , we have:

$$oldsymbol{q}_i = (oldsymbol{W}^Q)^\intercal oldsymbol{x}_i, \quad oldsymbol{k}_i = (oldsymbol{W}^K)^\intercal oldsymbol{x}_i, \quad oldsymbol{v}_i = (oldsymbol{W}^V)^\intercal oldsymbol{x}_i$$

- Calculate attention scores between query and all keys: $e_{ij} = \langle m{q}_i, m{k}_j
 angle$
- softmax normalization $w_{ij} = \exp\left(e_{ij}\right) / \sum_k \exp\left(e_{ik}\right)$
- output the weighted sum of values $\sum_j w_{ij} oldsymbol{v}_j$

In matrix notation

- Compute queries, keys, and values

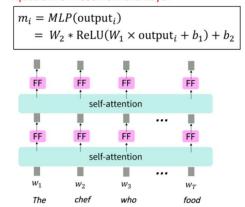
$$Q = XW^Q$$
, $K = XW^K$, $V = XW^V$

- Calculate attention scores between query and all keys: $E=QK^{\intercal}$
- softmax normalization $A = \operatorname{softmax}(E)$
- output the weighted sum of values AV

$$\mathrm{output} = \mathrm{softmax}(\boldsymbol{Q}\boldsymbol{K}^{\mathsf{T}})\boldsymbol{V}$$

Question: why we need both query and key?

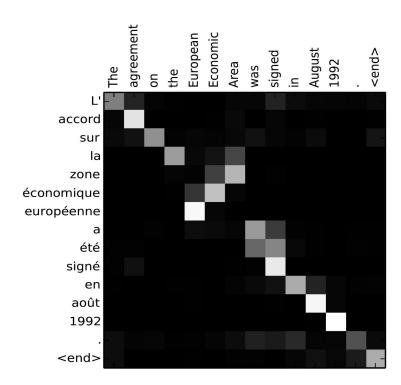
Equation for Feed Forward Layer



Adding in nonlinearity!

First step toward Transformers!

Attention matrices—visualizing correlations



K emains dived but remains involved in programs with amr corp. american airlines unit and delta air lines

General attention

Self-attention

Transformers

Transformers

Attention Is All You Need

Ashish Vaswani* Google Brain avaswani@google.com Noam Shazeer*
Google Brain
noam@google.com

Niki Parmar* Google Research nikip@google.com

Jakob Uszkoreit* Google Research usz@google.com

Llion Jones* Google Research llion@google.com Aidan N. Gomez* †
University of Toronto
aidan@cs.toronto.edu

Łukasz Kaiser* Google Brain lukaszkaiser@google.com

Illia Polosukhin* † illia.polosukhin@gmail.com

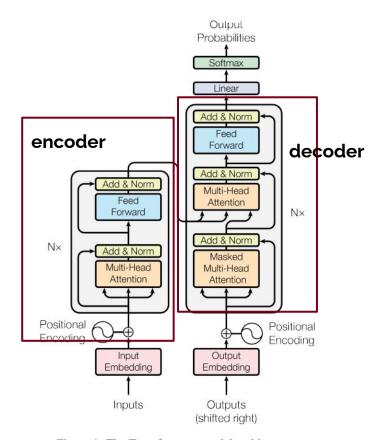
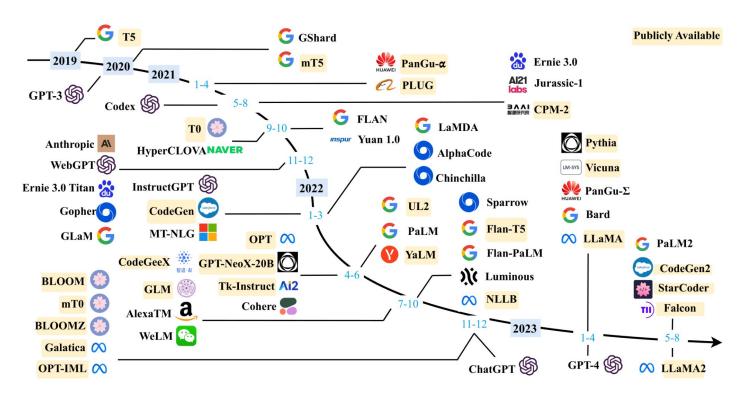
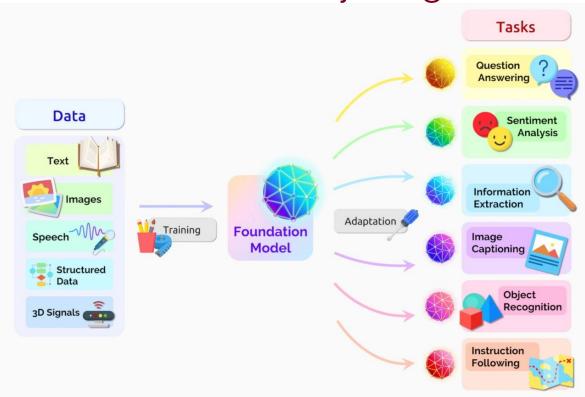


Figure 1: The Transformer - model architecture.

Transformers reign in NLP!



Transformers for everything!



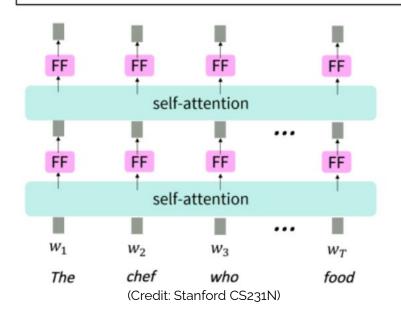
- Transformers have been modified to deal with **almost all** kinds of structured and **unstructured** data
- Enable multimodal data integration and interaction

Starting from self-attention

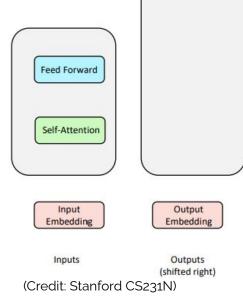
Equation for Feed Forward Layer

$$m_i = MLP(\text{output}_i)$$

= $W_2 * \text{ReLU}(W_1 \times \text{output}_i + b_1) + b_2$



Encoder

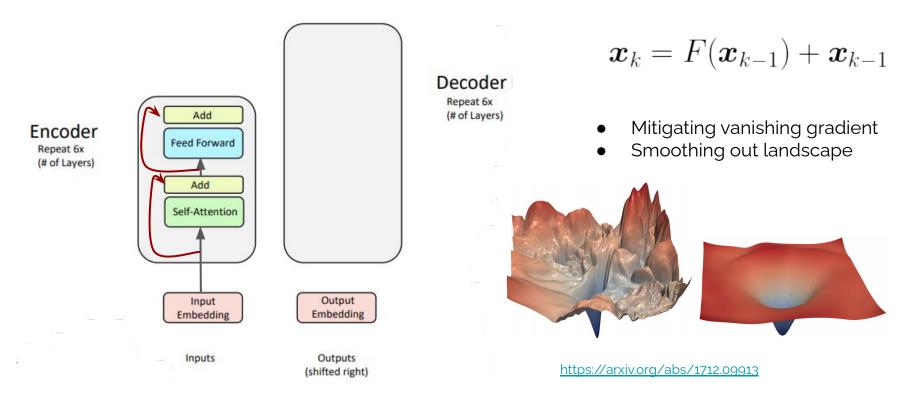


Three tricks to build in depth:

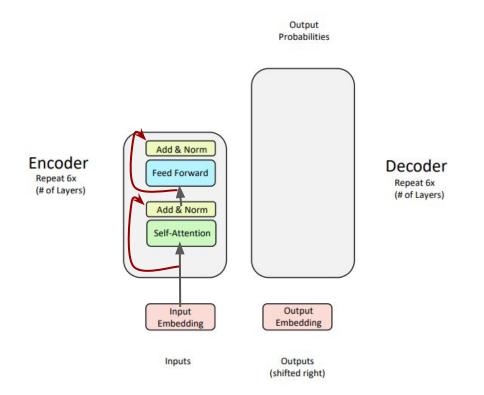
- Residual connection
- Layer normalization
- Scaled inner product attention

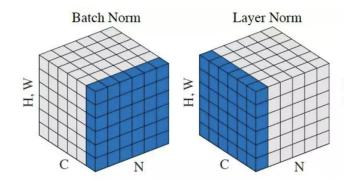
Decoder

Trick 1: Residual connection



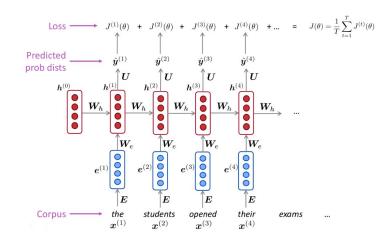
Trick 2: Layer normalization



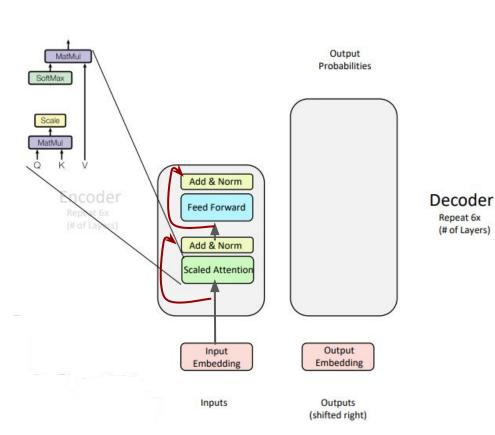


$$x^{\ell'} = \frac{x^{\ell} - \mu^{\ell}}{\sigma^{\ell} + \epsilon}$$

Why not batchnorm?



Trick 3: Scaled inner product attention



 $\operatorname{output} = \operatorname{softmax}(QK^{\mathsf{T}})V$

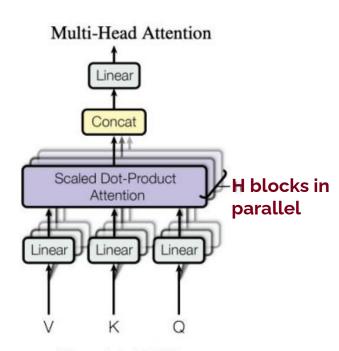
- Suppose that entries of Q and K behaves like IID zero-mean, unit variance
- $\mathbb{E}\langle \boldsymbol{q}^i, \boldsymbol{k}^j \rangle = 0$ but $\operatorname{Var}\langle \boldsymbol{q}^i, \boldsymbol{k}^j \rangle = d_k$

This can blow up exp computation in the softmax normalization for large d_k !

Solution: normalize by standard deviation

$$\text{output} = \text{softmax}(\boldsymbol{Q}\boldsymbol{K}^\intercal/\sqrt{d_k})\boldsymbol{V}$$

Multi-head attention



[Vaswani et al. 2017]

Multiple, independent self-attention blocks in parallel

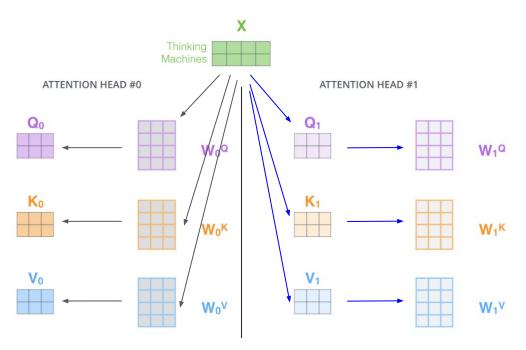
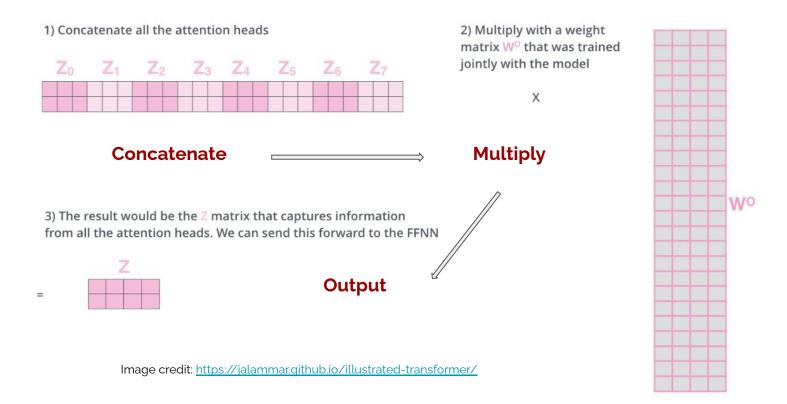


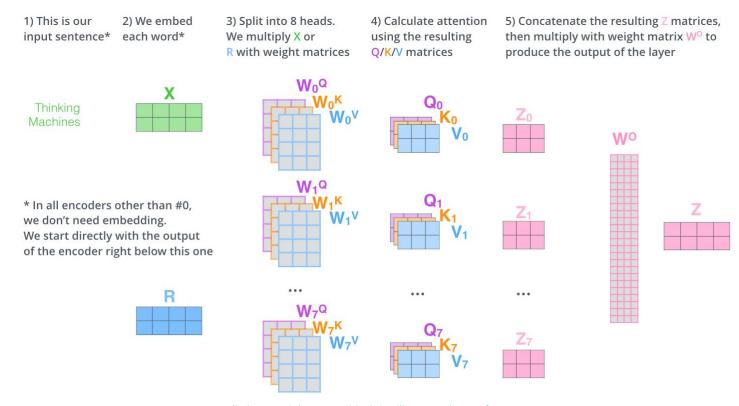
Image credit: https://jalammar.github.io/illustrated-transformer/

Intuition: allow the flexibility of capturing different kinds of "relevance"/correlations

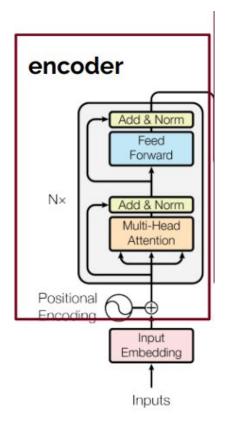
Multi-head attention



Multi-head attention



Positional encoding



Does the input order matter or not?

$$Q = XW^Q$$
, $K = XW^K$, $V = XW^V$
output = softmax $(QK^T/\sqrt{d_k})V$

Positional encoding to break the order invariance

Idea: a positional vector to (hopefully) encode the position information

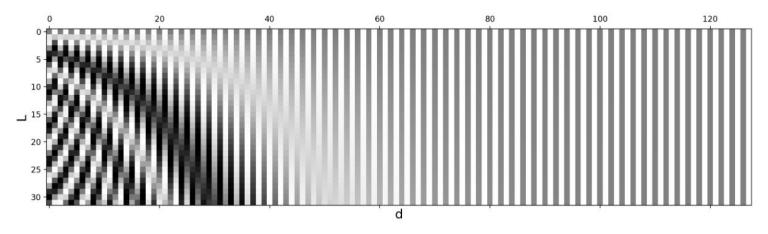
E.g.,
$$oldsymbol{X}_p = oldsymbol{X} + oldsymbol{P}, ext{ or } oldsymbol{X}_p = [oldsymbol{X}, oldsymbol{P}]$$

ullet can be pre-defined, or made learnable

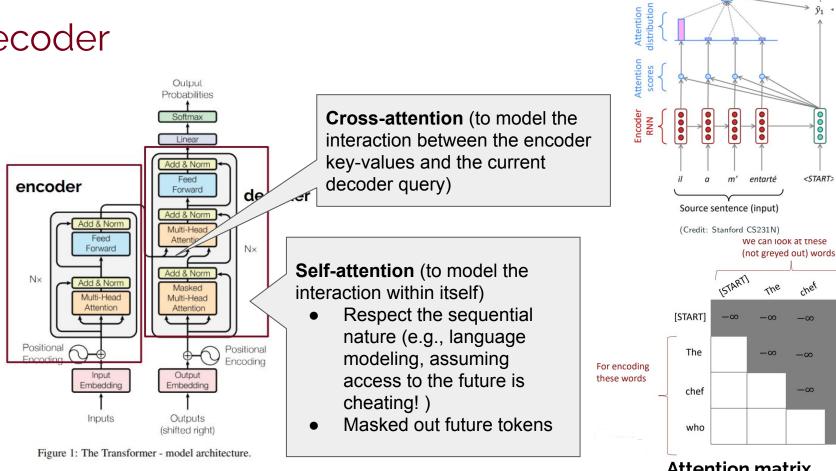
Sinusoidal positional encoding

L: sequence length d: embedding dimension

$$ext{PE}(i,\delta) = egin{cases} \sin(rac{i}{10000^{2\delta'/d}}) & ext{if } \delta = 2\delta' \ \cos(rac{i}{10000^{2\delta'/d}}) & ext{if } \delta = 2\delta' + 1 \end{cases}$$



Decoder



Attention output

 $-\infty$

 $-\infty$

Strong performance in machine translation

Table 2: The Transformer achieves better BLEU scores than previous state-of-the-art models on the English-to-German and English-to-French newstest2014 tests at a fraction of the training cost.

Model	BL	EU	Training C	Training Cost (FLOPs)		
Model	EN-DE	EN-FR	EN-DE	EN-FR		
ByteNet [18]	23.75					
Deep-Att + PosUnk [39]		39.2		$1.0 \cdot 10^{20}$		
GNMT + RL [38]	24.6	39.92	$2.3 \cdot 10^{19}$	$1.4 \cdot 10^{20}$		
ConvS2S [9]	25.16	40.46	$9.6 \cdot 10^{18}$	$1.5\cdot 10^{20}$		
MoE [32]	26.03	40.56	$2.0\cdot10^{19}$	$1.2\cdot 10^{20}$		
Deep-Att + PosUnk Ensemble [39]		40.4		$8.0 \cdot 10^{20}$		
GNMT + RL Ensemble [38]	26.30	41.16	$1.8 \cdot 10^{20}$	$1.1 \cdot 10^{21}$		
ConvS2S Ensemble [9]	26.36	41.29	$7.7\cdot 10^{19}$	$1.2 \cdot 10^{21}$		
Transformer (base model)	27.3	38.1		10^{18}		
Transformer (big)	28.4	41.8	$2.3 \cdot$	10^{19}		

Computation

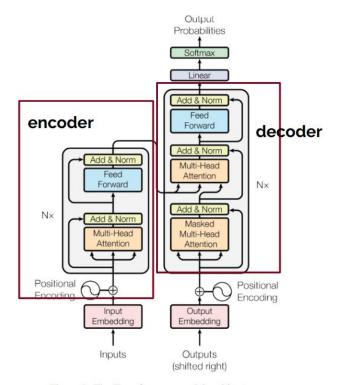


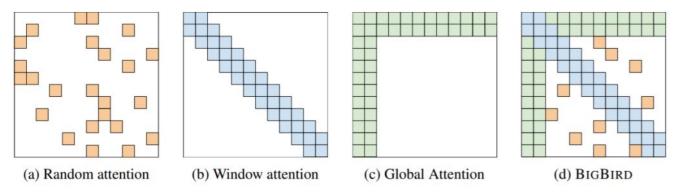
Figure 1: The Transformer - model architecture.

What's the total computation?

$$m{Q} = m{X}m{W}^Q, \quad m{K} = m{X}m{W}^K, \quad m{V} = m{X}m{W}^V$$
 output = softmax $(m{Q}m{K}^\intercal/\sqrt{d_k})m{V}$
$$O(T^2d)$$

Quadratic computation vs. linear computation in RNNs (\mathbf{T} is the length of each input sequence, \mathbf{d} is the embedding dimension)

Computation



Idea; building in sparsity https://arxiv.org/abs/2007.14062

Do Transformer Modifications Transfer Across Implementations and Applications?

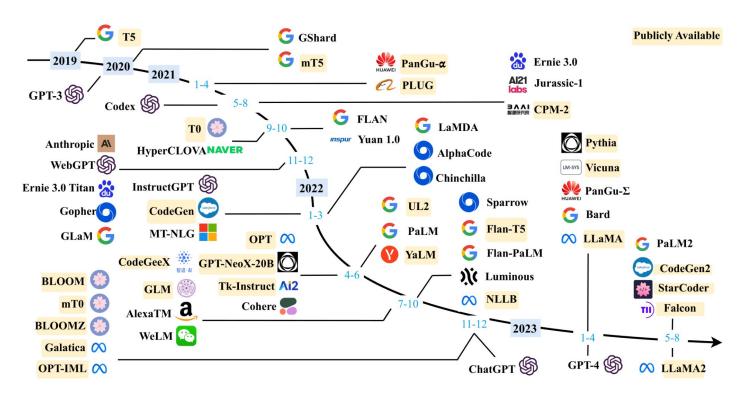
Sharan Narang*	Hyung Won Chung	Yi Tay	William Fedus
Thibault Fevry [†]	${\bf Michael~Matena}^{\dagger}$	Karishma Malkan †	Noah Fiedel
Noam Shazeer	Zhenzhong $\operatorname{Lan}^{\dagger}$	Yanqi Zhou	Wei Li
Nan Ding	Jake Marcus	Adam Roberts	Colin Raffel †

But not much consistent improvement so far

https://arxiv.org/abs/2102.11972

Large language models (LLMs)

Large language models



LLMs: large models trained on large datasets

				_				-
	Model	Release	Size			GPT-3 55	May-2020	
	MIDUEI	Time	(B)			GShard 91	Jun-2020	
	T5 [73]	Oct-2019	11	-		Codex 92	Jul-2021	
						ERNIE 3.0 93	Jul-2021	
	mT5 74	Oct-2020	13			Jurassic-1 94	Aug-2021	
	PanGu- α 75	Apr-2021	13*			HyperCLOVA 95	Sep-2021	
	CPM-2 76	Jun-2021	198			FLAN 62	Sep-2021	
	T0 28	Oct-2021	11			Yuan 1.0 [96]	Oct-2021	
	CodeGen 77	Mar-2022	16			Anthropic 97	Dec-2021	
	GPT-NeoX-20B 78	Apr-2022	20			WebGPT 72	Dec-2021	
	Tk-Instruct 79	Apr-2022	11			Gopher 59	Dec-2021	
	UL2 <u>80</u>	May-2022	20			ERNIE 3.0 Titan 98	Dec-2021	
		May-2022	175			GLaM 99	Dec-2021	
	NLLB 82	Jul-2022	54.5			LaMDA 63	Jan-2022	
	CodeGeeX 83	Sep-2022	13	(Closed	MT-NLG 100	Jan-2022	
	GLM [84]	Oct-2022	130		Source	AlphaCode 101	Feb-2022	
	Flan-T5 [64]	Oct-2022	11			InstructGPT 61	Mar-2022	
Publicly	BLOOM 69	Nov-2022	176			Chinchilla 34	Mar-2022	
Available		Nov-2022	13			PaLM 56	Apr-2022	
	Galactica 35	Nov-2022	120			AlexaTM 102	Aug-2022	
	BLOOMZ 85	Nov-2022	176			Sparrow 103	Sep-2022	
	OPT-IML 86	Dec-2022	175			WeLM 104	Sep-2022	
	LLaMA 57	Feb-2023	65			U-PaLM 105	Oct-2022	
	Pythia 87	Apr-2023	12			Flan-PaLM 64	Oct-2022	
	CodeGen2 88	May-2023	16			Flan-U-PaLM 64	Oct-2022	
	StarCoder 89	May-2023	15.5			GPT-4 46	Mar-2023	
	LLaMA2 90	Jul-2023	70			PanGu- Σ 106	Mar-2023	
						PaLM2 [107]	Mav-2023	

LLMs: large models trained on large datasets

TABLE 2: Statistics of commonly-used data sources.

Corpora	Size	Source	Latest Update Time
BookCorpus 138	5GB	Books	Dec-2015
Gutenberg [139]	_	Books	Dec-2021
C4 73	800GB	CommonCrawl	Apr-2019
CC-Stories-R 140	31GB	CommonCrawl	Sep-2019
CC-NEWS 27	78GB	CommonCrawl	Feb-2019
REALNEWs 141	120GB	CommonCrawl	Apr-2019
OpenWebText 142	38GB	Reddit links	Mar-2023
Pushift.io 143	2TB	Reddit links	Mar-2023
Wikipedia 144	21GB	Wikipedia	Mar-2023
BigQuery 145	_	Codes	Mar-2023
the Pile 146	800GB	Other	Dec-2020
ROOTS 147	1.6TB	Other	Jun-2022

Two crucial technical steps toward LLMs

- Pretraining
- Finetuning (Adaptation)

Recall transfer learning?

14

32

Pretraining: data collection

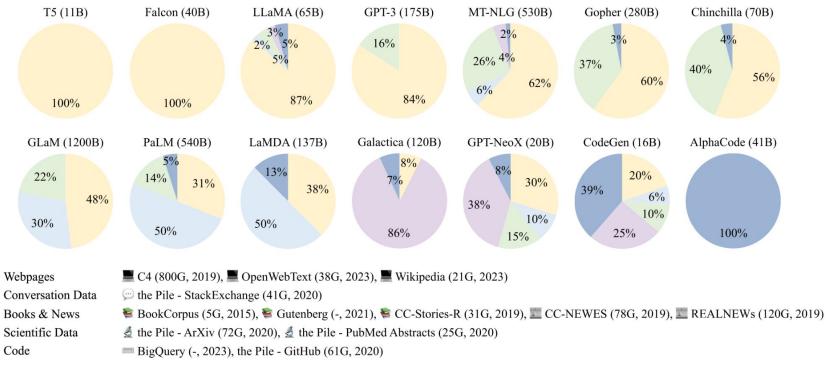


Image credit: A Survey of Large Language Models https://arxiv.org/abs/2303.18223

Pretraining: data collection

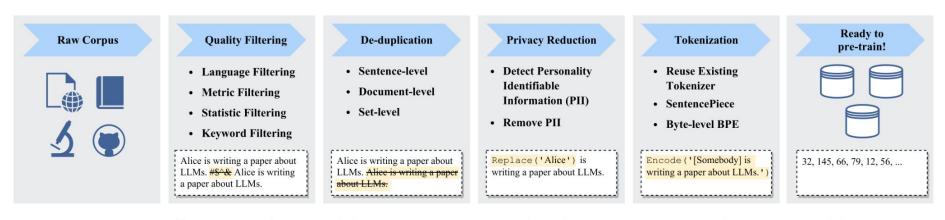
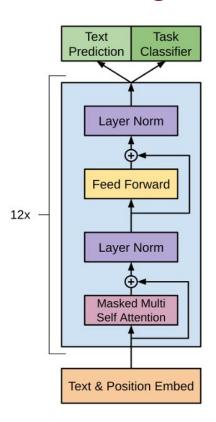
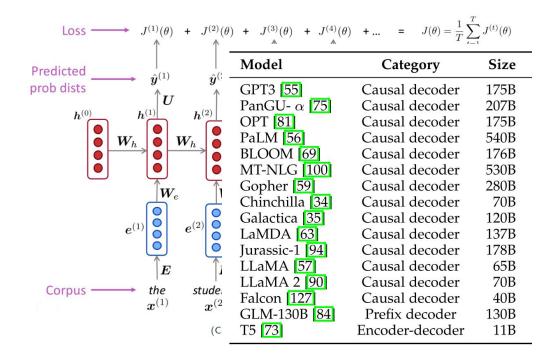


Fig. 6: An illustration of a typical data preprocessing pipeline for pre-training large language models.

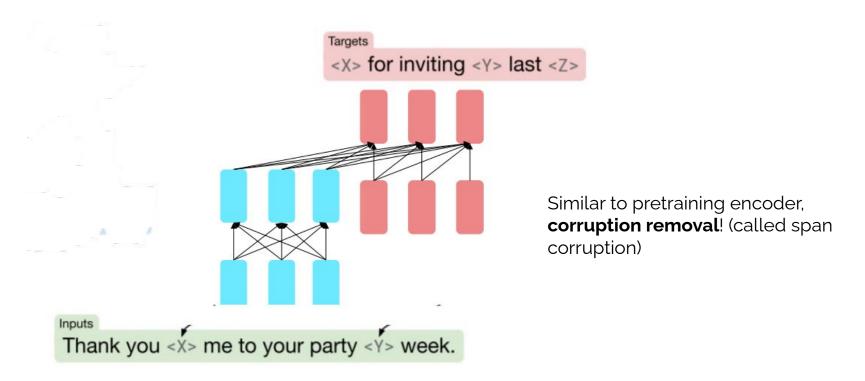
Pretraining: architecture & task



Most popular: (transformer-based) **decoder-only** architectures pretrained on **langua** $\mathbb{P}\left[x^{(t+1)} \mid x^{(t)}, \dots, x^{(1)}\right]$ nodel



Pretraining: architecture & task — alternative



Pretraining: architecture details

Configuration	Method	Equation
Normalization position	Post Norm 22 Pre Norm 26 Sandwich Norm 201	
Normalization method	LayerNorm 202 RMSNorm 203 DeepNorm 204	$\begin{vmatrix} \frac{\mathbf{x} - \mu}{\sqrt{\sigma}} \cdot \gamma + \beta, & \mu = \frac{1}{d} \sum_{i=1}^{d} x_i, & \sigma = \sqrt{\frac{1}{d} \sum_{i=1}^{d} (x_i - \mu)} \\ \frac{\mathbf{x}}{\text{RMS}(\mathbf{x})} \cdot \gamma, & \text{RMS}(\mathbf{x}) = \sqrt{\frac{1}{d} \sum_{i=1}^{d} x_i^2} \\ \text{LayerNorm}(\alpha \cdot \mathbf{x} + \text{Sublayer}(\mathbf{x})) \end{vmatrix}$
Activation function	ReLU 205 GeLU 206 Swish 207 SwiGLU 208 GeGLU 208	ReLU(\mathbf{x}) = max(\mathbf{x} , 0) GeLU(\mathbf{x}) = 0.5 \mathbf{x} \otimes [1 + erf($\mathbf{x}/\sqrt{2}$)], erf(x) = $\frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$ Swish(\mathbf{x}) = \mathbf{x} \otimes sigmoid(\mathbf{x}) SwiGLU($\mathbf{x}_1, \mathbf{x}_2$) = Swish(\mathbf{x}_1) \otimes \mathbf{x}_2 GeGLU($\mathbf{x}_1, \mathbf{x}_2$) = GeLU(\mathbf{x}_1) \otimes \mathbf{x}_2
Position embedding	Absolute 22 Relative 73 RoPE 209 Alibi 210	$ \begin{vmatrix} \mathbf{x}_{i} = \mathbf{x}_{i} + \mathbf{p}_{i} \\ A_{ij} = \mathbf{W}_{q} \mathbf{x}_{i} \mathbf{x}_{j}^{T} \mathbf{W}_{k}^{T} + r_{i-j} \\ A_{ij} = \mathbf{W}_{q} \mathbf{x}_{i} \mathbf{R}_{\theta, i-j} \mathbf{x}_{j}^{T} \mathbf{W}_{k}^{T} \\ A_{ij} = \mathbf{W}_{q} \mathbf{x}_{i} \mathbf{R}_{\theta, i-j} \mathbf{x}_{j}^{T} \mathbf{W}_{k}^{T} A_{ij} = \mathbf{W}_{q} \mathbf{x}_{i} \mathbf{x}_{j}^{T} \mathbf{W}_{k}^{T} - m(i-j) \end{vmatrix} $

Pretraining: optimization details

TABLE 5: Detailed optimization settings of several existing LLMs.

Model	Batch Size (#tokens)	Learning Rate	Warmup	Decay Method	Optimizer	Precision Type	Weight Decay	Grad Clip	Dropout
GPT3 (175B)	32K→3.2M	6×10^{-5}	yes	cosine decay to 10%	Adam	FP16	0.1	1.0	_
PanGu- α (200B)	-	2×10^{-5}	-	- 1	Adam	-	0.1	-	-
OPT (175B)	2M	1.2×10^{-4}	yes	manual decay	AdamW	FP16	0.1	-	0.1
PaLM (540B)	$1M\rightarrow 4M$	1×10^{-2}	no	inverse square root	Adafactor	BF16	lr^2	1.0	0.1
BLOOM (176B)	4M	6×10^{-5}	yes	cosine decay to 10%	Adam	BF16	0.1	1.0	0.0
MT-NLG (530B)	$64 \text{ K} \rightarrow 3.75 \text{M}$	5×10^{-5}	yes	cosine decay to 10%	Adam	BF16	0.1	1.0	-
Gopher (280B)	$3M\rightarrow 6M$	4×10^{-5}	yes	cosine decay to 10%	Adam	BF16	_	1.0	-
Chinchilla (70B)	$1.5M \rightarrow 3M$	1×10^{-4}	yes	cosine decay to 10%	AdamW	BF16	-	-	-
Galactica (120B)	2M	7×10^{-6}	yes	linear decay to 10%	AdamW	-	0.1	1.0	0.1
LaMDA (137B)	256K	-	-		_	BF16	_	~	_
Jurassic-1 (178B)	$32 \text{ K} \rightarrow 3.2 \text{M}$	6×10^{-5}	yes	-	-	-	-	-	-
LLaMA (65B)	4M	1.5×10^{-4}	yes	cosine decay to 10%	AdamW	-	0.1	1.0	-
LLaMA 2 (70B)	4M	1.5×10^{-4}	yes	cosine decay to 10%	AdamW	-	0.1	1.0	-
Falcon (40B)	2M	1.85×10^{-4}	yes	cosine decay to 10%	AdamW	BF16	0.1	=	-
GLM (130B)	$0.4M \rightarrow 8.25M$	8×10^{-5}	yes	cosine decay to 10%	AdamW	FP16	0.1	1.0	0.1
T5 (11B)	64K	1×10^{-2}	no	inverse square root	AdaFactor	-	-	-	0.1
ERNIE 3.0 Titan (260B)	-	1×10^{-4}	=	-	Adam	FP16	0.1	1.0	-
PanGu- Σ (1.085T)	0.5M	2×10^{-5}	yes	-	Adam	FP16	-		-

Supervised adaptation—instruction tuning

TABLE 6: A detailed list of available collections for instruction tuning.

Categories	Collections	Time	#Examples
	Nat. Inst. 264	Apr-2021	193K
	FLAN 62	Sep-2021	4.4M
	P3 265	Oct-2021	12.1M
Task	Super Nat. Inst. 79	Apr-2022	5M
	MVPCorpus 266	Jun-2022	41M
	xP3 85	Nov-2022	81M
	OIC ²²	Mar-2023	43M
	HH-RLHF 267	Apr-2022	160K
	HC3 268	Jan-2023	87K
Chat	ShareGPT ²³	Mar-2023	90K
	Dolly ²⁴	Apr-2023	15K
	OpenAssistant 269	Apr-2023	161K
	Self-Instruct 129	Dec-2022	82K
	Alpaca 123	Mar-2023	52K
Synthetic	Guanaco ²⁵	Mar-2023	535K
	Baize 270	Apr-2023	158K
	BELLE 271	Apr-2023	1.5M

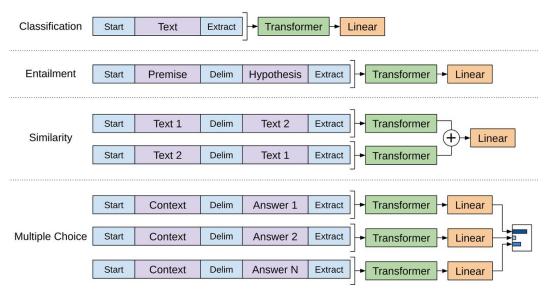


Image credit: Improving Language Understanding by Generative Pre-Training https://gwern.net/doc/www/s3-us-west-2.amazonaws.com/d73fdc5ffa86278ce4.pdf

Image credit: A Survey of Large Language Models https://arxiv.org/abs/2303.18223

Constructing the instruction sets

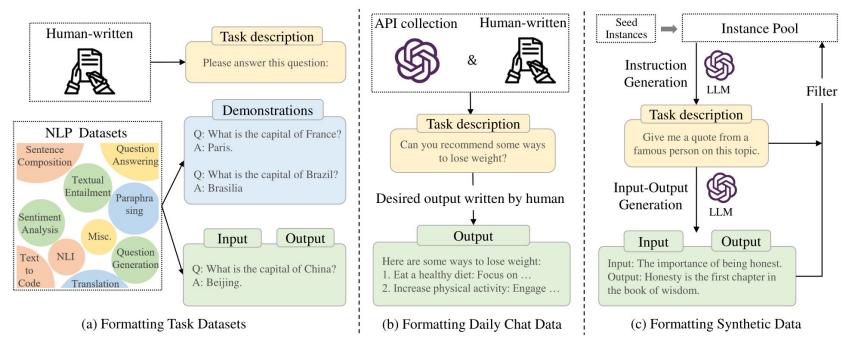
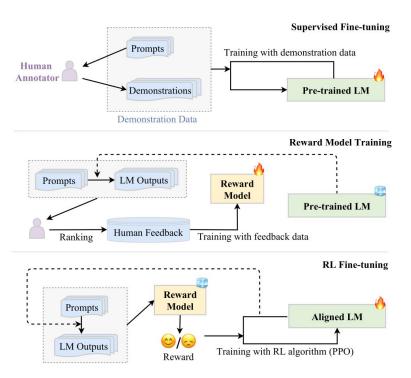


Fig. 9: An illustration of instance formatting and three different methods for constructing the instruction-formatted instances.

Supervised adaptation—alignment tuning



Make sure the output is aligned with human values and not harmful

Reinforcement learning with human feedback (RLHF)

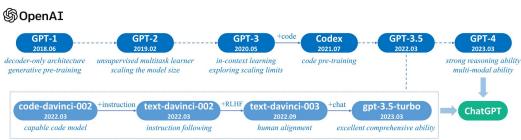


Fig. 3: A brief illustration for the technical evolution of GPT-series models. We plot this figure mainly based on the papers, blog articles and official APIs from OpenAI. Here, *solid lines* denote that there exists an explicit evidence (*e.g.*, the official statement that a new model is developed based on a base model) on the evolution path between two models, while *dashed lines* denote a relatively weaker evolution relation.