

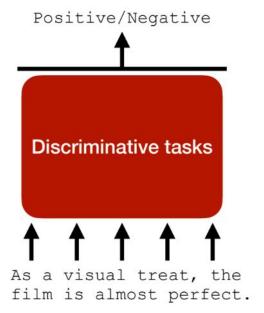
# Механизм внимания, архитектура трансформер

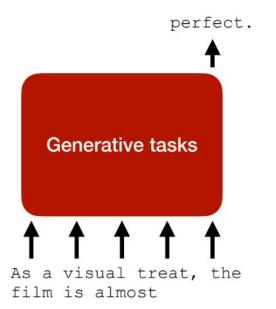
к.ф.-м.н. Тихомиров Михаил Михайлович

научный сотрудник НИВЦ МГУ имени М. В. Ломоносова

#### NLР задачи

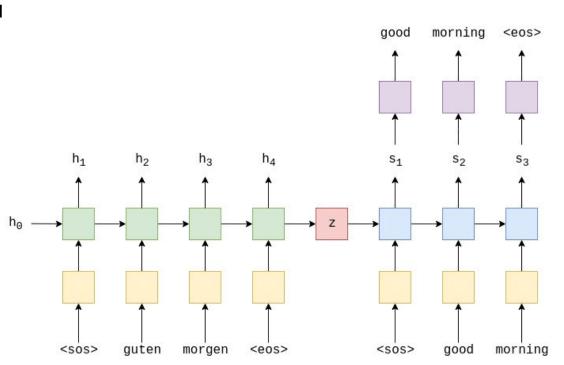
- Дискриминативные задачи: классификация, NER, и др.
- Генеративные задачи: перевод, аннотирование (summarization), языковое моделирование





#### Seq2Seq до трансформеров

- Вектор финального состояния должен хранить всю информацию из предложения
- По сути является векторным представлением (эмбеддингом) предложения
- Теряет информацию на длинных последовательностях



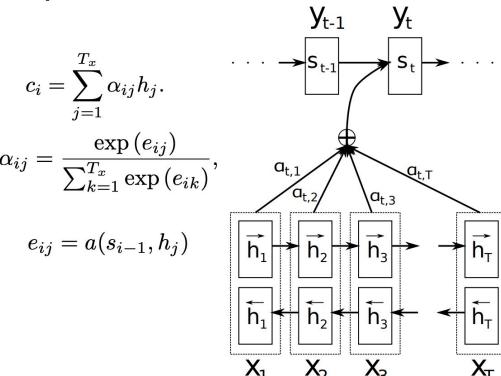
# Механизм внимания (2014)

# <u>Автокодирующая модель</u> состоит из:

- Encoder(text) -> vector:
   переводит текст в необходимое
   векторное представление
- **Decoder**(vector) -> text: расшифровывает представление в ответ модели

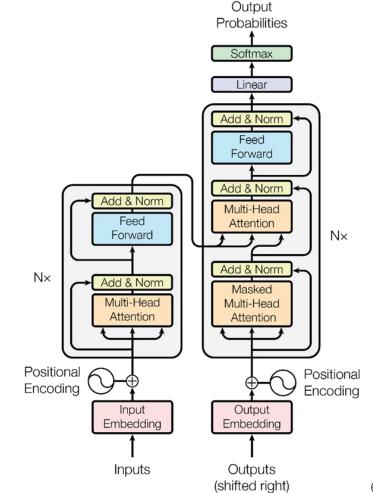
**Проблема:** в vector помещается только общий контекст

**Решение:** сохранять векторы для каждого слова и подбирать нужные под каждый шаг decoder

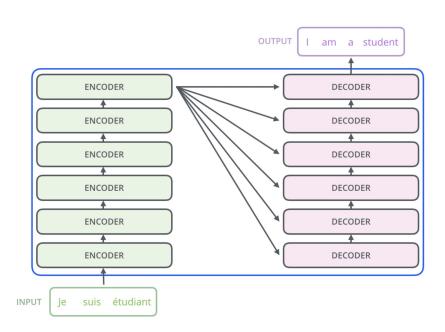


# Архитектура трансформер

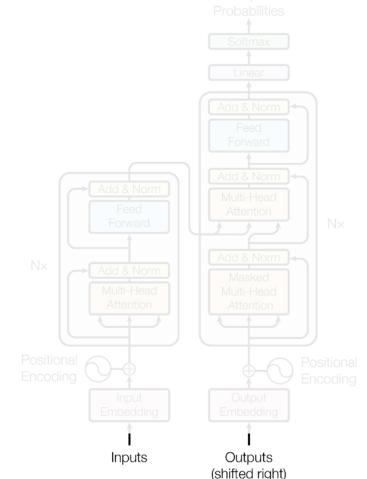
- Токенизация слов
- Позиционное кодирование
- Преобразование векторов через трансформер-блоки
  - Multi-head attention (MHA)
  - Feed-forward (FFN)
  - LayerNorm
- Итоговое предсказание слова линейным слоем (Im head)



- Исходно encoder-decoder архитектура
- Блоки архитектурно эквивалентны и последовательно преобразует входной вектор в выходной вектор той же размерности
- Сами веса слоев в блоках при этом отличаются



- Токенизация слов
- Позиционное кодирование
- Преобразование векторов через трансформер-блоки
  - Multi-head attention (MHA)
  - Feed-forward (FFN)
  - LayerNorm
- Итоговое предсказание слова линейным слоем (Im head)



#### Токенизация текста

Цель - отобразить текст в последовательность id

- Символы?
  - Небольшой словарь, не более 256 токенов!
  - Но длина последовательности будет огромной.
- Каждое слово токен?
  - Количество различных слов огромное.
  - Если отсекать по частоте, будут UNK токены
- Решение: subword tokenization
  - Словарь включает в себя как символы, так и би-три-н граммы (символьные), на основе частоты в корпусе.

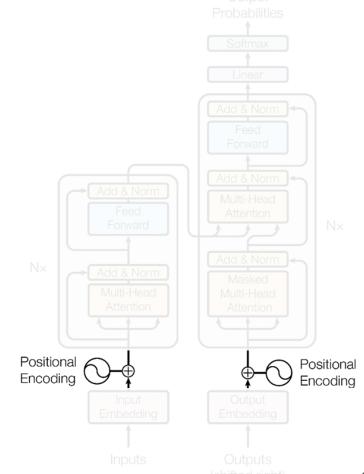
Token count

Price per prompt \$0.00041

Б<mark>ольшие языковые модели в в</mark>опросно-ответных системах: от тр ансформера до собственного чат б<mark>от</mark>а

[61432, 17461, 30480, 1532, 46410, 9136, 4655, 90877, 5173 6, 71239, 61642, 5927, 5927, 29256, 42057, 13999, 12, 1333 7, 48074, 44786, 93099, 1506, 10693, 25, 20879, 11047, 3568 2, 2297, 57719, 91883, 57297, 5524, 14082, 20812, 5372, 399 00, 17756, 8131, 14391, 13337, 1506]

- Токенизация слов
- Позиционное кодирование
- Преобразование векторов через трансформер-блоки
  - Multi-head attention (MHA)
  - Feed-forward (FFN)
  - LayerNorm
- Итоговое предсказание слова линейным слоем (Im head)



#### Позиционные эмбеддинги

- В отличии от RNN трансформер смотрит на входную последовательность как на мешок слов, нет информации о позиции.
- Решение позиционные "эмбеддинги" как добавка к эсбедингам токенов.

$$PE_{(pos,2i)} = sin(pos/10000^{2i/d_{\text{model}}})$$
  
 $PE_{(pos,2i+1)} = cos(pos/10000^{2i/d_{\text{model}}})$ 

pos - позиция в последовательности, і - координата вектора.

"We also experimented with using learned positional embeddings instead, and found that the two versions produced nearly identical results"

#### Позиционные эмбеддинги

$$egin{aligned} \mathsf{X}_\mathsf{t} + & \overrightarrow{p_t} = egin{bmatrix} \sin(\omega_1.\,t) \ \cos(\omega_1.\,t) \ \sin(\omega_2.\,t) \ \cos(\omega_2.\,t) \ & \vdots \ \sin(\omega_{d/2}.\,t) \ \cos(\omega_{d/2}.\,t) \end{bmatrix}_{d imes 1} \ \omega_k = rac{1}{10000^{2k/d}} \end{aligned}$$

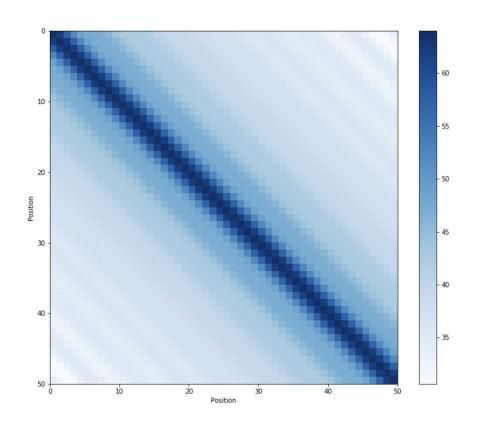
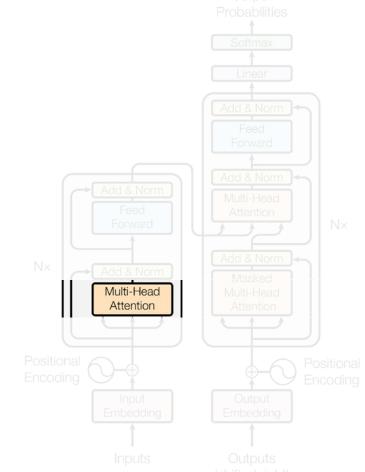


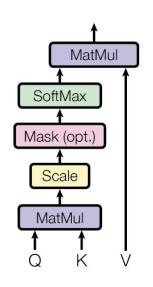
Figure 3 - Dot product of position embeddings for all time-steps

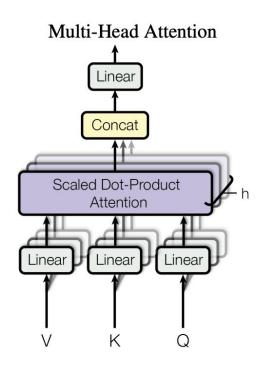
- Токенизация слов
- Позиционное кодирование
- Преобразование векторов через трансформер-блоки
  - Multi-head attention (MHA)
  - Feed-forward (FFN)
  - LayerNorm
- Итоговое предсказание слова линейным слоем (Im head)



#### **Multi-Head Attention**

Scaled Dot-Product Attention





$$Attention(Q, K, V) = softmax(\frac{QK^T}{\sqrt{d_k}})V$$

#### Multi-Head Attention: нормировка весов внимания

Зачем делить на корень из размерности?

->

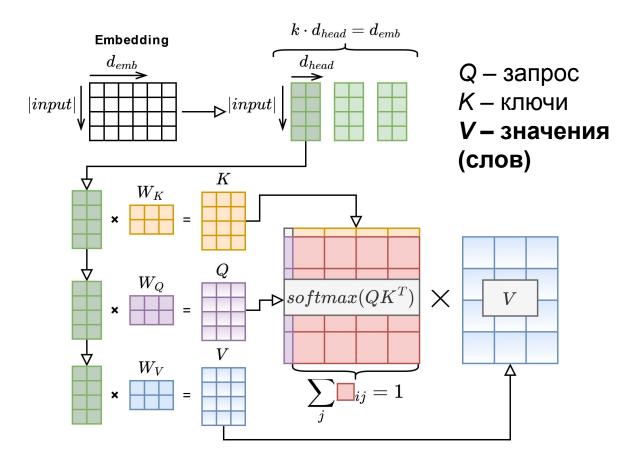
Чтобы веса внимания имели единичное стандартное отклонение.

Attention
$$(Q, K, V) = \operatorname{softmax}(\frac{QK^T}{\sqrt{d_k}})V$$

$$lpha = q_i k_j^T = \sum_{n=1}^{d_k} q_{in} k_{jn}$$

- 1) Предположим, что Q и K имеют 0 среднее и 1 стандартное отклонение
- Дисперсия суммы = сумма дисперсий -> дисперсия a = d, a значит стандартное отклонение это корень из d.

# **Multi-Head Attention (tensors)**



# Multi-Head Attention (Pytorch code, LLaMa) [1]

```
Self.q_proj = nn.Linear(self.hidden_size, self.num_heads * self.head_dim, bias=config.attention_bias)

Self.k_proj = nn.Linear(self.hidden_size, self.num_key_value_heads * self.head_dim, bias=config.attention_bias)

self.v_proj = nn.Linear(self.hidden_size, self.num_key_value_heads * self.head_dim, bias=config.attention_bias)

self.o_proj = nn.Linear(self.hidden_size, self.hidden_size, bias=config.attention_bias)
```

```
Pacчет матриц Q, K, V: — query_states = self.q_proj(hidden_states) key_states = self.k_proj(hidden_states) value_states = self.v_proj(hidden_states)
```

```
query_states = query_states.view(bsz, q_len, self.num_heads, self.head_dim).transpose(1, 2)

"Нарезка" на головы: — key_states = key_states.view(bsz, q_len, self.num_key_value_heads, self.head_dim).transpose(1, 2)

value_states = value_states.view(bsz, q_len, self.num_key_value_heads, self.head_dim).transpose(1, 2)
```

# Multi-Head Attention (Pytorch code, LLaMa) [2]

Pacчет весов

внимания и

умножение на V:

attn\_weights = nn.functional.softmax(attn\_weights, dim=-1, dtype=torch.float32).to(query\_states.dtype)

attn\_weights = nn.functional.dropout(attn\_weights, p=self.attention\_dropout, training=self.training)

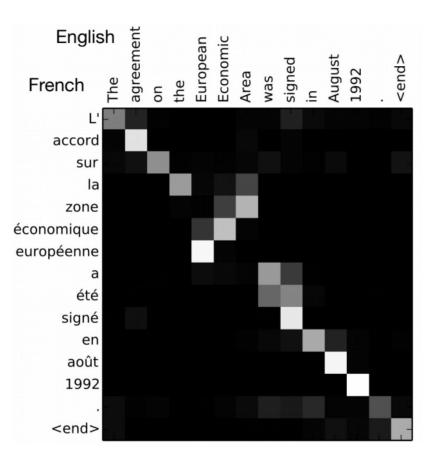
attn\_output = torch.matmul(attn\_weights, value\_states)

"Конкатенация" attn\_output = attn\_output.transpose(1, 2).contiguous()

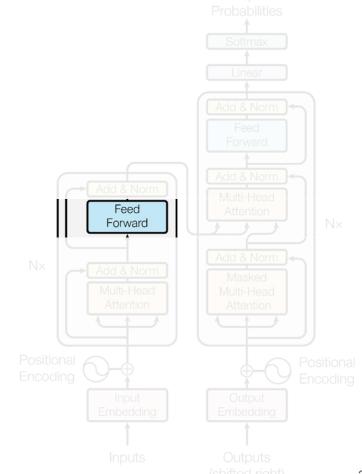
голов: attn\_output = attn\_output.reshape(bsz, q\_len, self.hidden\_size)

И еще один
линейный слой на → attn\_output = self.o\_proj(attn\_output)
выходе:

# Визуализация Self Attention



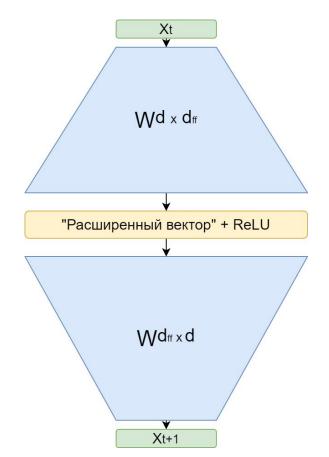
- Токенизация слов
- Позиционное кодирование
- Преобразование векторов через трансформер-блоки
  - Multi-head attention (MHA)
  - Feed-forward (FFN)
  - LayerNorm
- Итоговое предсказание слова линейным слоем (Im head)



#### Блок Feed Forward (MLP, FCNN)

- Внутренняя размерность обычно сильно больше hidden\_size, например, x4.
- Интуиция: FF являются хранилищем "знаний" моделей (так ли это, не известно).

$$FFN(x) = \max(0, xW_1 + b_1)W_2 + b_2$$



# Блок Feed Forward (Pytorch code, LLaMa)

```
self.gate_proj = nn.Linear(self.hidden_size, self.intermediate_size, bias=False)

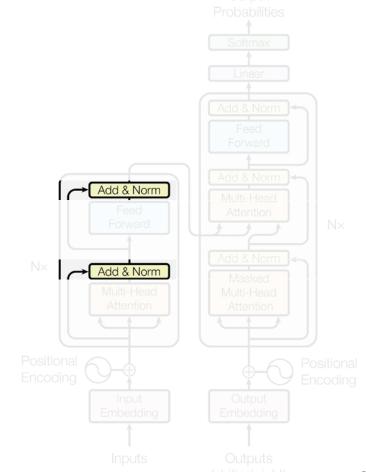
Инициализация:

— self.up_proj = nn.Linear(self.hidden_size, self.intermediate_size, bias=False)

self.down_proj = nn.Linear(self.intermediate_size, self.hidden_size, bias=False)
```

```
Forward: \longrightarrow down_proj = self.down_proj(self.act_fn(self.gate_proj(x)) * self.up_proj(x))
```

- Токенизация слов
- Позиционное кодирование
- Преобразование векторов через трансформер-блоки
  - Multi-head attention (MHA)
  - Feed-forward (FFN)
  - LayerNorm
- Итоговое предсказание слова линейным слоем (Im head)



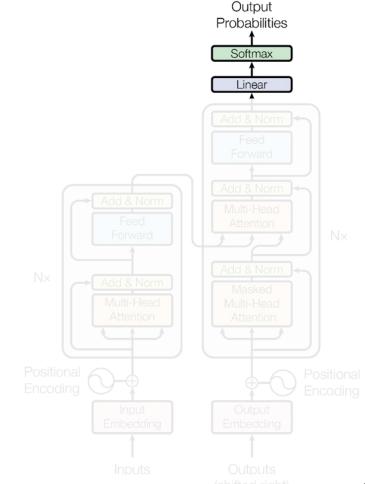
#### **Layer Norm**

- Layer Norm это метод нормализации активации слоя нейронной сети.
- В оригинальной архитектуре "add and norm" шли после блока внимания и после блока FF: **Post-LN**.
- В дальнейшем слой нормализации был перенесен перед и после слоя внимания: **Pre-LN**.

# Layer Norm (Pytorch code, LLaMa)

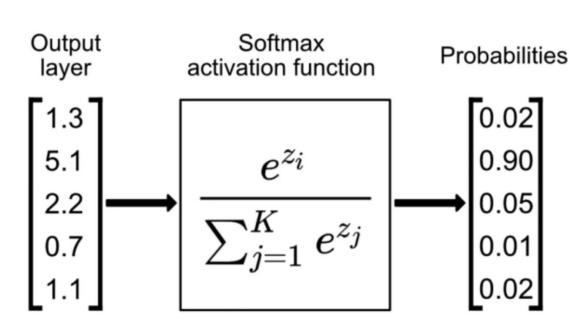
residual = hidden states LN на входе блока hidden states = self.input layernorm(hidden states) # Self Attention hidden states, self attn weights, present key value = self.self attn( Блок внимания hidden states=hidden states, attention mask=attention mask, position ids=position ids, past key value=past key value, output attentions=output attentions, use cache=use cache, cache position=cache position, \*\*kwargs, hidden states = residual + hidden states # Fully Connected residual = hidden states hidden states = self.post attention layernorm(hidden states) LN на выходе блока hidden states = self.mlp(hidden states) MLP (Feed Forward) hidden states = residual + hidden states

- Токенизация слов
- Позиционное кодирование
- Преобразование векторов через трансформер-блоки
  - Multi-head attention (MHA)
  - Feed-forward (FFN)
  - LayerNorm
- Итоговое предсказание слова линейным слоем (Im head)



#### Im head

- Линейный слой отображающий вектор, получаемый из трансформера в вектор "логитов", размерностью в |V|.
- Вектор логитов затем преобразуется через softmax для получения "вероятностей" токенов.



#### Генерация с помощью LLM

 В идеале хотелось бы уметь с помощью LLM генерировать текст, который максимизирует вероятность

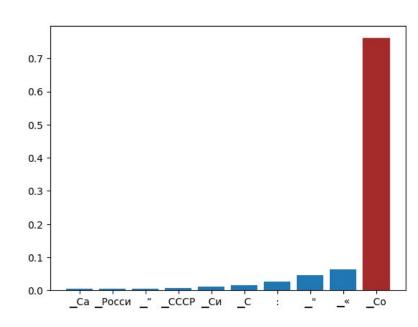
$$y' = \arg\max_{y} p(y|x) = \arg\max_{y} \prod_{t=1}^{n} p(y_t|y_{< t}, x)$$

- Перебрать все существующие цепочки невозможно.
- Выход: Генерация токен за токеном на основе текущих вероятностей - Sampling:
  - o greedy,
  - top-k,
  - o top-p,
  - beam\_search

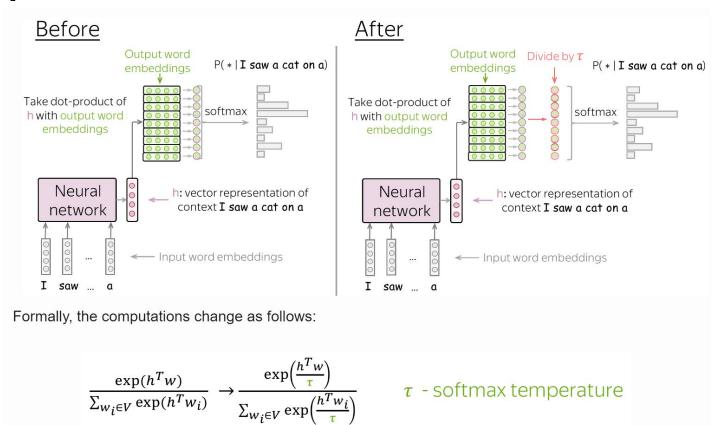
#### **Greedy sampling**

#### СССР расшифровывается как?

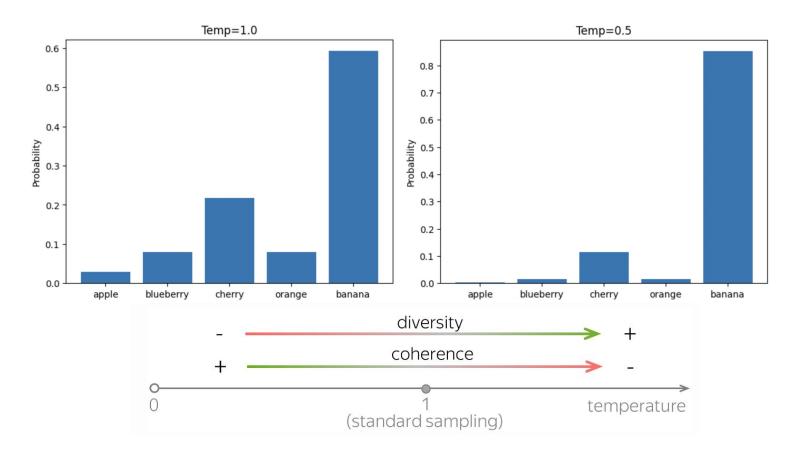
- Каждый раз берем токен с максимальной вероятностью.
- Минусы: полное отсутствие разнообразия.
- Альтернатива: sampling в зависимости от вероятности самого токена.



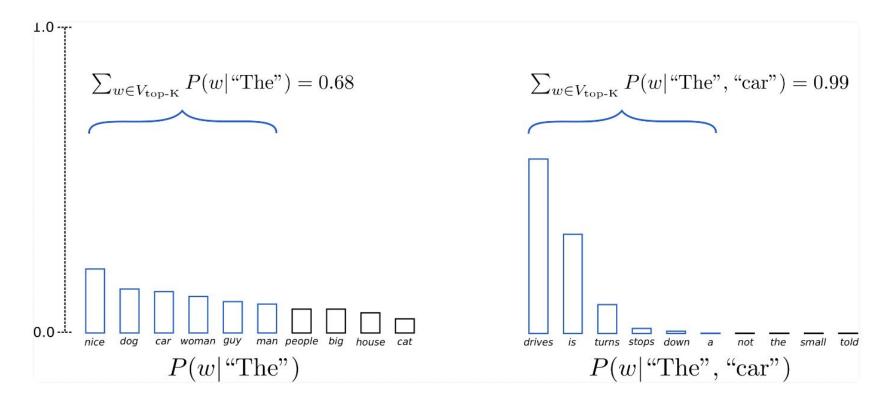
#### **Temperature**



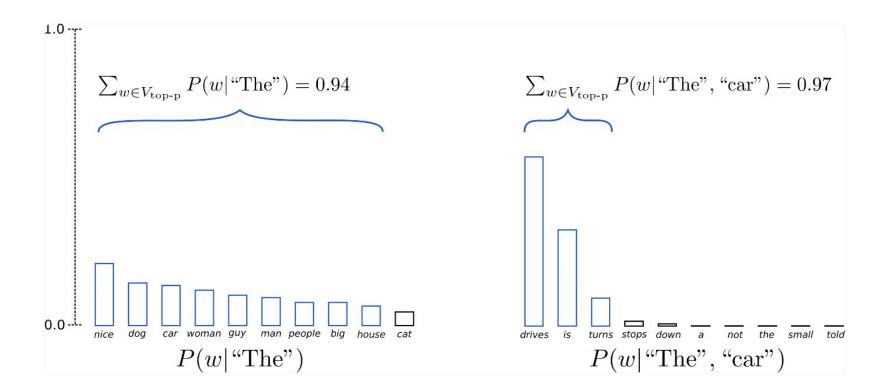
## **Temperature**



#### Top-K

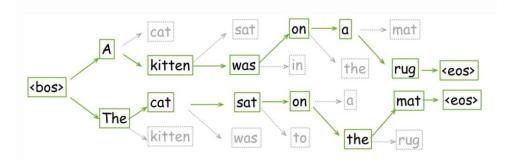


# Top-P (nucleus sampling)



#### Beam search

- Отслеживание нескольких наиболее вероятных гипотез, вместо одной.
- Вес цепочки сумма logprobs нормированная на длину.



 Раньше активно применялся, сейчас редко из-за накладных расходов (необходимо вести beam\_size генераций) и низкого разнообразия ответов.

# Архитектура Transformer: начало современного NLP

# Transformer: первое впечатление

| Model                           | BLEU  |       | Training Cost (FLOPs) |                     |
|---------------------------------|-------|-------|-----------------------|---------------------|
|                                 | 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 | $2.0\cdot 10^{19}$    | $1.2 \cdot 10^{20}$ |
| Deep-Att + PosUnk Ensemble [39] |       | 40.4  | 0.10.00               | $8.0 \cdot 10^{20}$ |
| 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  | $3.3\cdot 10^{18}$    |                     |
| Transformer (big)               | 28.4  | 41.8  | $2.3\cdot 10^{19}$    |                     |

- Тестирование на задаче перевода,
- Нет существенного "скачка" в качестве.

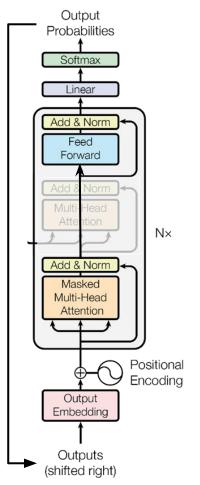
## **OpenAl GPT-1 (2018)**

- 12 слоев Transformer decoder (~117 млн.),
- Обучение в 2 этапа:
  - о Предобучение (pre-training) на задаче моделирования языка

$$\max_{\Theta} \sum_{0 \le i \le n} \log P(w_i | w_{i-1} ... w_0; \Theta)$$

w - слова последовательности, Θ - параметры модели

- Дообучение (fine-tuning) на целевые задачи
- Предобучался только на художественной литературе



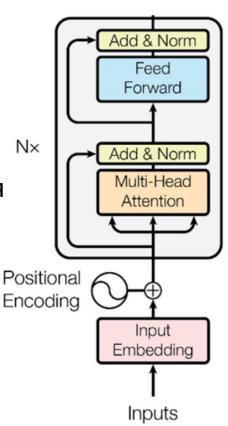
# OpenAl GPT-1: оценка качества

| Method                                  | MNLI-m | MNLI-mm   | SNLI         | SciTail | QNLI | RTE  |
|---|--------|-----------|--------------|---------|------|------|
| ESIM + ELMo [44] (5x)<br>CAFE [58] (5x) | 80.2   | -<br>79.0 | 89.3<br>89.3 | -       | -    | -    |
| Stochastic Answer Network [35] (3x)     | 80.6   | 80.1      | -            | -       | -    |      |
| CAFE [58]                               | 78.7   | 77.9      | 88.5         | 83.3    |      |      |
| GenSen [64]                             | 71.4   | 71.3      | -            | -       | 82.3 | 59.2 |
| Multi-task BiLSTM + Attn [64]           | 72.2   | 72.1      | -            | H       | 82.1 | 61.7 |
| Finetuned Transformer LM (ours)         | 82.1   | 81.4      | 89.9         | 88.3    | 88.1 | 56.0 |

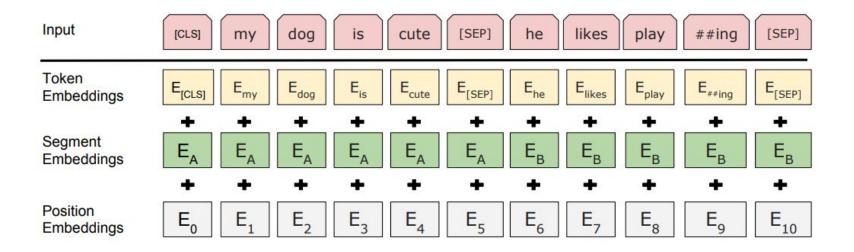
| Method                          | Story Cloze | RACE-m | RACE-h | RACE     |
|---------------------------------|-------------|--------|--------|----------|
| val-LS-skip [55]                | 76.5        | -      | -      | -        |
| Hidden Coherence Model [7]      | <u>77.6</u> | -      | =:     | <b>-</b> |
| Dynamic Fusion Net [67] (9x)    | -           | 55.6   | 49.4   | 51.2     |
| BiAttention MRU [59] (9x)       |             | 60.2   | 50.3   | 53.3     |
| Finetuned Transformer LM (ours) | 86.5        | 62.9   | 57.4   | 59.0     |

### **BERT (2018)**

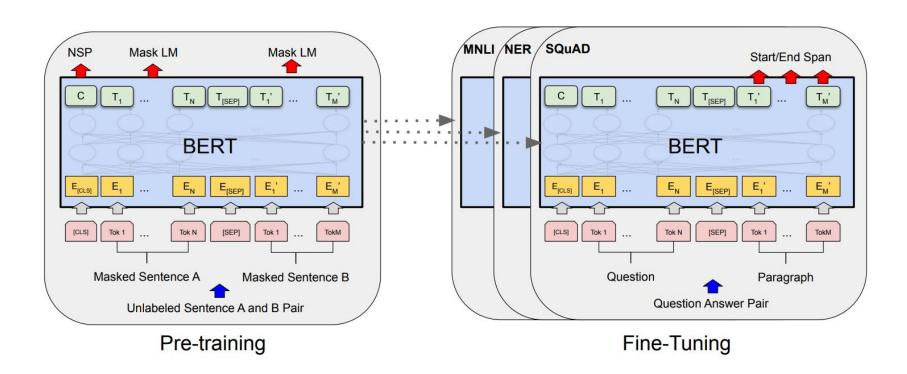
- Base: 12 слоев Transformer encoder (~110 млн. параметров),
- Обучение в 2 этапа!:
  - Предобучение (pre-training) на задачах:
    - маскированного языкового моделирования (MLM)
    - предсказания следующего предложения (NSP).
  - о Дообучение (fine-tuning) на целевые задачи
- 3.3 миллиарда слов English Wikipedia + BooksCorpus.



### BERT: формирование входа



## BERT: pre-training и fine-tuning



# BERT: результаты

| System               | MNLI-(m/mm) | QQP  | QNLI | SST-2 | CoLA | STS-B | MRPC | RTE  | Average |
|----------------------|-------------|------|------|-------|------|-------|------|------|---------|
|                      | 392k        | 363k | 108k | 67k   | 8.5k | 5.7k  | 3.5k | 2.5k | -       |
| Pre-OpenAI SOTA      | 80.6/80.1   | 66.1 | 82.3 | 93.2  | 35.0 | 81.0  | 86.0 | 61.7 | 74.0    |
| BiLSTM+ELMo+Attn     | 76.4/76.1   | 64.8 | 79.8 | 90.4  | 36.0 | 73.3  | 84.9 | 56.8 | 71.0    |
| OpenAI GPT           | 82.1/81.4   | 70.3 | 87.4 | 91.3  | 45.4 | 80.0  | 82.3 | 56.0 | 75.1    |
| BERT <sub>BASE</sub> | 84.6/83.4   | 71.2 | 90.5 | 93.5  | 52.1 | 85.8  | 88.9 | 66.4 | 79.6    |
| $BERT_{LARGE}$       | 86.7/85.9   | 72.1 | 92.7 | 94.9  | 60.5 | 86.5  | 89.3 | 70.1 | 82.1    |

# Некоторые практические аспекты работы с LLM

#### "Типы" LLM

- Foundational (базовая) LLM, которые обучались предсказывать следующее слово без специального дообучения инструкциям
  - На данном этапе приобретаются основные знания модели!
- Instruct (инструктивные) это базовые LLM, которые прошли дополнительный этап обучения инструкциям
  - Дообучение происходит в специальном формате, который фиксируется как chat\_template
  - Приобретаются навыки отвечать на вопросы пользователя так, чтобы ему понравилось (в частности, решать задачи в zero-shot)

### **Chat Template**

- У разных моделей чат темплейт может быть разным! Всегда смотрите в карточках модели + в токенайзере.
- Формирование промптов из последовательностей сообщений
- 3 основных роли: system, user, assistant (названия могут варьироваться)

```
<|im_start|>system
You are Qwen, created by Alibaba Cloud. You are a helpful assistant.<|im_end|>
<|im_start|>user

Что такое LLM?<|im_end|>
<|im_start|>assistant
```

### **HuggingFace**

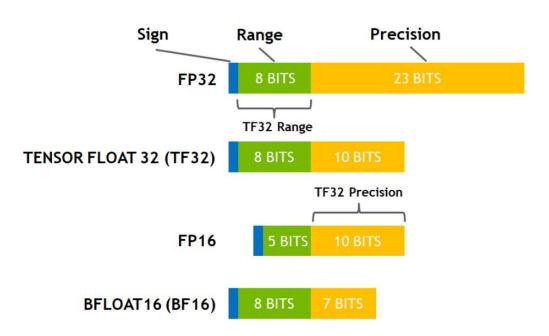
- Огромное сообщество профессионалов
- Платформа для хранения моделей, датасетов и тп
- Все опенсорс релизы LLM можно найти там

#### Также:

- transformers одна из основных библиотек для работы с LLM
- datasets библиотека для работы с датасетами из HF
- peft библиотека для эффективного дообучения LLM
- ...

#### Различные типы чисел

- В основном LLM обучают в fp16/bf16
- Некоторые операции
   / слои все еще могут
   быть в fp32
   (mixed-precision)



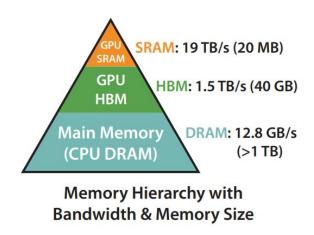
### Проблемы классического attention

- Квадратичная сложность от длины последовательности как по времени, так и по памяти.
- Как результат, проблемы с длинными последовательностями.

$$X \in \mathbb{R}^{n \times d}$$
 
$$Attention(Q, K, V) = softmax(\frac{QK^T}{\sqrt{d}})V$$
 
$$SelfAttention(X) = Attention(XW_Q, XW_K, XW_V)$$

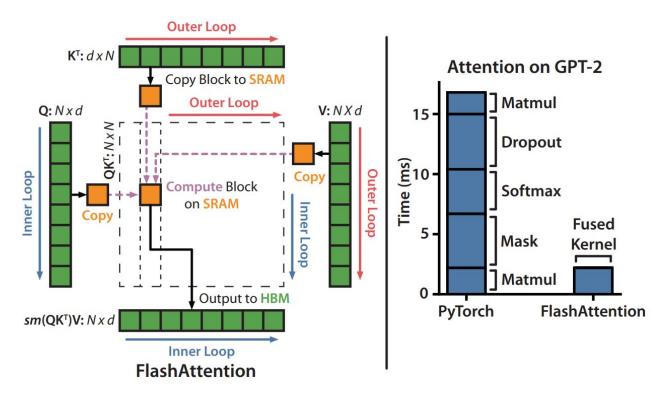
#### flash-attention: идея

- GPU имеет разную память.
- Чтения и записи между ними, а также использование более медленной памяти снижают скорость работы вычислений.



Dao T. et al. Flashattention: Fast and memory-efficient exact attention with io-awareness //Advances in Neural Information Processing Systems. – 2022. – T. 35. – C. 16344-16359.

#### flash-attention: метод



<sup>&</sup>quot;FlashAttention does not read and write the large  $N \times N$  attention matrix to HBM"

### flash-attention: результаты

| Models                      | ListOps | Text | Retrieval | Image | Pathfinder | Avg  | Speedup      |
|-----------------------------|---------|------|-----------|-------|------------|------|--------------|
| Transformer                 | 36.0    | 63.6 | 81.6      | 42.3  | 72.7       | 59.3 | -            |
| FLASHATTENTION              | 37.6    | 63.9 | 81.4      | 43.5  | 72.7       | 59.8 | $2.4 \times$ |
| Block-sparse FlashAttention | 37.0    | 63.0 | 81.3      | 43.6  | 73.3       | 59.6 | $2.8 \times$ |
| Linformer [84]              | 35.6    | 55.9 | 77.7      | 37.8  | 67.6       | 54.9 | 2.5×         |
| Linear Attention [50]       | 38.8    | 63.2 | 80.7      | 42.6  | 72.5       | 59.6 | 2.3×         |
| Performer [12]              | 36.8    | 63.6 | 82.2      | 42.1  | 69.9       | 58.9 | 1.8×         |
| Local Attention [80]        | 36.1    | 60.2 | 76.7      | 40.6  | 66.6       | 56.0 | 1.7×         |
| Reformer [51]               | 36.5    | 63.8 | 78.5      | 39.6  | 69.4       | 57.6 | 1.3×         |
| Smyrf [19]                  | 36.1    | 64.1 | 79.0      | 39.6  | 70.5       | 57.9 | 1.7×         |

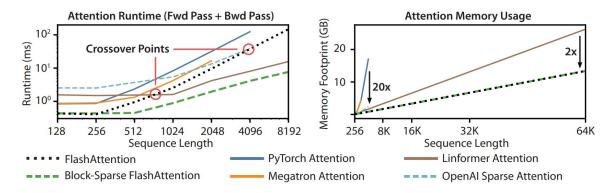
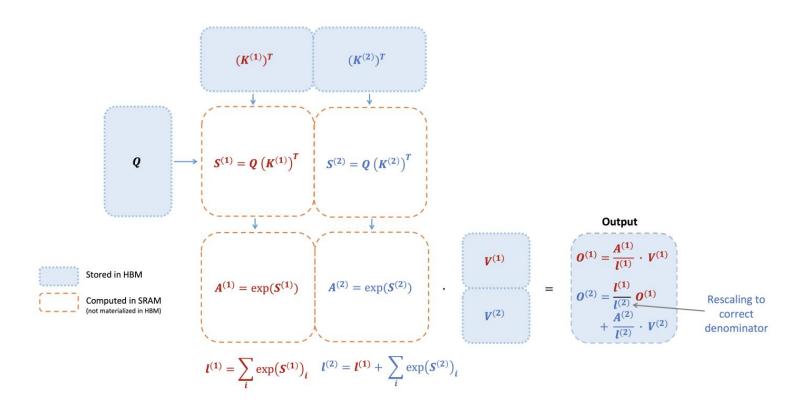


Figure 3: Left: runtime of forward pass + backward pass. Right: attention memory usage.

#### flash-attention-2

- Несмотря на то, что FlashAttention в 2-4 раза быстрее стандартной реализации, все равно forward pass достигает только 30-50% от теоретического максимума FLOPs/s на современных GPU.
  - Backward pass еще хуже, 25-35%
- Современные GPU имеют специализированные встроенные средства для перемножения матриц, благодаря которым пропускная способность matmul операции может быть в 16 раз выше, чем для non-matmul.

### flash-attention-2: метод



### flash-attention-2: результаты A100

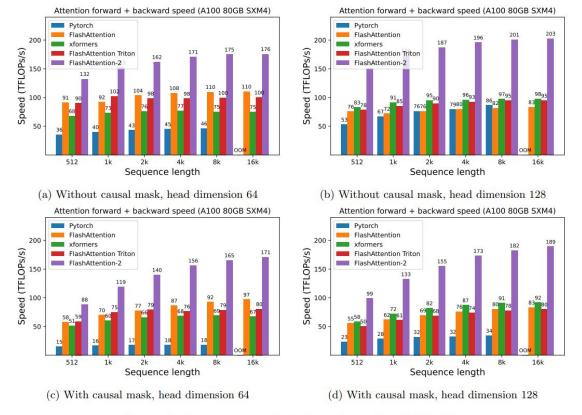


Figure 4: Attention forward + backward speed on A100 GPU

### flash-attention-2: результаты H100

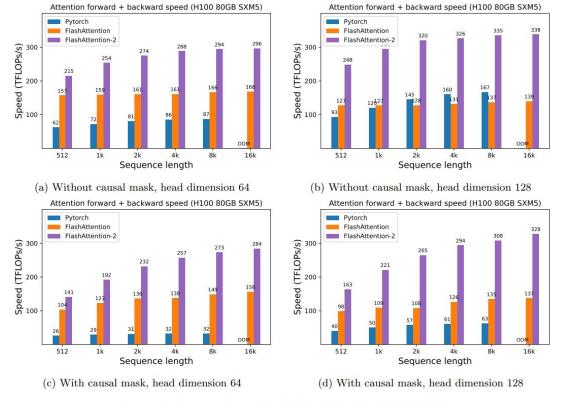


Figure 7: Attention forward + backward speed on H100 GPU

### flash-attention 1-2: выводы

- Существенное ускорение расчета attention, как во время обучения, так и во время инференса.
- Нет потери в качестве, так как по сути расчет attention не поменялся.
- Стала линейная зависимость по памяти.
- Применяется как есть на существующие уже обученные модели.
- Для FlashAttention-2 требуются современные ускорители.

#### FlashAttention-2 currently supports:

- 1. Ampere, Ada, or Hopper GPUs (e.g., A100, RTX 3090, RTX 4090, H100). Support for Turing GPUs (T4, RTX 2080) is coming soon, please use FlashAttention 1.x for Turing GPUs for now.
- 2. Datatype fp16 and bf16 (bf16 requires Ampere, Ada, or Hopper GPUs).
- 3. All head dimensions up to 256. Head dim > 192 backward requires A100/A800 or H100/H800.

#### Квантизация

- Квантизация еще один способ "уменьшить" модель, в частности для "инфера",
- Суть в **преобразовании весов модели** из типа float32, float16 в **int8**, а иногда и в **int4**,
- Преобразование делается не просто "напрямую", а более хитрыми способами. Существуют реализации, совместимые с huggingface transformers,
  - load\_in\_8bit, load\_in\_4bit флаги (не лучшая квантизация),
- Закономерный результат квантизации падение качества,
- Можно совмещать с обычным LoRa,
  - Замороженную модель в 8bit/4bit, но обучаемые веса в float16,
- QLoRa более эффективный способ обучения модели с квантизацией.

#### Домашнее задание 1

- Зайти на google colab / kaggle (или на своем железе, если есть)
- Создать нотбук с загрузкой и работой с LLM по аналогии с показанным в лекции
- Придумать 10 не самых простых вопросов к LLM и сравнить 2 модели на выбор:
  - Например, qwen-2.5-7B-Instruct и Phi-4-mini-instruct
- Сравнить вручную: лучше model1, лучше model2, одинаковы.
- Прислать нотбук + отчет (pdf)

### Задание: оценивание и сроки

- Срок 1 неделя: до 9 марта 23:59.
- Присылать на <u>tikhomirov.mm@gmail.com</u>
  - Название письма: Основы LLM: Задание 1, запуск LLM.
  - В письме Ваше полное ФИО, группа, решение и краткий отчет по нему в PDF.
- Оценка по шкале "-/-+/+-/-.".
  - ++ за те решения, которые особо мне понравятся чемлибо.