

看图学大模型

看图学

2024 年 4 月 27 日

当前版本为 v0.20240427, 还在更新中, 目前维持每周更新。

本电子书目前进度完成不到 10%, 可以关注下方公众号回复”看图学大模型”来获取最新版。



看图学

微信扫描二维码, 关注我的公众号

目前 PDF 排版等还略有问题，Latex 还需要略微调整。

目录

Chapter 1: 大模型发展史	3
AI 的起源	3
符号派、链接派，相爱又相杀	18
从 one-hot 到 ChatGPT	18
Chapter 2: 主流大模型的模型架构和细节分析	19
Transformers 起源	19
Transformers 架构	33
Position Embedding	43
Chapter 3: 大语言模型 pipeline	49
Stage 1: Pretrain	49
Stage 2: SFT	49
Stage 3: Alignment	49
Stage 0: 数据处理	49
Chapter 4: 大语言模型训练	49
显卡和模型训练基础知识	49
多卡并行训练	49
当前流行训练框架	49
Chapter 5: 大语言模型推理	50
KV Cache	50
Chapter 6: MOE, 多模态等	54
Chapter 7: 大语言模型评估	54
Chapter 8: 大语言模型应用	54
Prompt Engineering	54
Agent	54

Chapter 1: 大模型发展史

AI 的起源

翻一翻历史其实是蛮有意思的一件事情，我们可以看到很多现在与历史上一些相似的瞬间，仿佛 Yesterday Once More。

AI 的发展到今天差不多也有 70 多年的历史了，让我们来回顾一下这段跌宕起伏的历史。

机器能不能思考？

1900 年的科幻小说《绿野仙踪》里，有个铁皮人，这可能是早期人们对人工智能机器人的一种幻想。



50 年后，图灵认为人类通过信息和推理来解决问题和做出决策，那机器能不能做同样的事情？1950 年，图灵发表了论文《计算机械和智能》，在里面讨论了如何构建智能机器以及如何测试机器的智能，也就是大家都熟知的“图灵实验”，开始把幻想映射到现实。

但是图灵提出设想后并没有做出一台智能机器。原因有很多，但是主要的原因可能有两个。

一个是图灵在研究人工智能的时候，冯诺依曼正在研究计算机体系结构，所以那个时候计算机还没有使用冯诺依曼结构，自然也就缺乏一个智能体的关键结构：记忆。那个时候的计算机只存储数据，并不存储命令。也就是说你可以告诉计算机要干啥，但是它并没有记住自己干了什么。是不是感觉跟现在的大模型有点像？

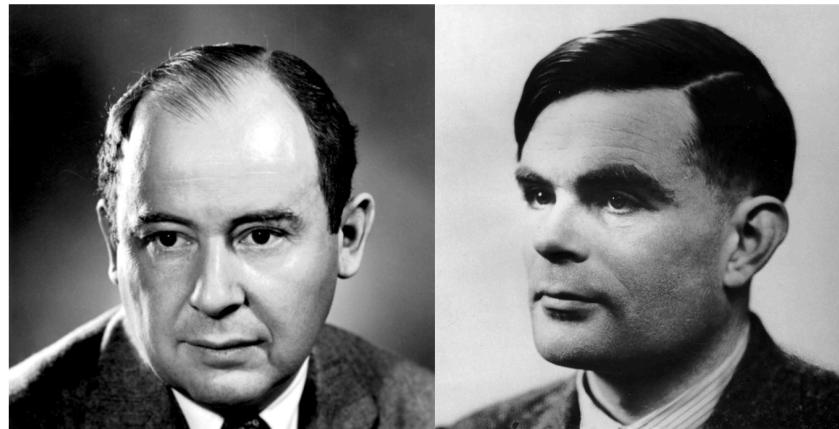
再一个，那个时候计算机是真的贵，当时租用一台计算机要花 20 万美元，只有高科技公司和大学才有机会使用。现在大模型训练成本也高的离谱。

相似瞬间

历史	现在	启发
当时的计算机只存储了数据，没有存储指令，没有记忆	大模型也可以认为是存储了数据，目前也没有记忆	Agent目前是外挂记忆，后续大型会不会内置一个指令存储单元
成本高，计算机租金每月20万美元	大模型训练成本高，GPT3最开始训练一次几千万美元	成本在当时是瓶颈，摩尔定律会解决这个瓶颈

这段历史中出现了两个大佬。

冯诺依曼被人们称作“计算机之父”，“博弈论之父”。图灵被人们称作“计算机科学之父”，“人工智能之父”。



冯诺依曼
计算机之父
博弈论之父

艾伦图灵
“计算机科学之父”
“人工智能之父”

冯诺依曼比图灵大 10 岁，这两个都是天才级别的人物。

达特矛斯会议：AI 一大

目前大家普遍认为是 AI 的起源是 1956 年的达特矛斯会议。因为这次会议上，人工智能研究的先行者聚集在了一起，搞了个为期 2 个月的头脑风暴。第一次提出了“人工智能”这个词，虽然后来考证可能是麦卡锡把维纳的 Cybernetics 换了个名字。

当时参加会议的人，大都是某学科的开山鼻祖，混的差一点的也都是几年后的图灵奖获得者。

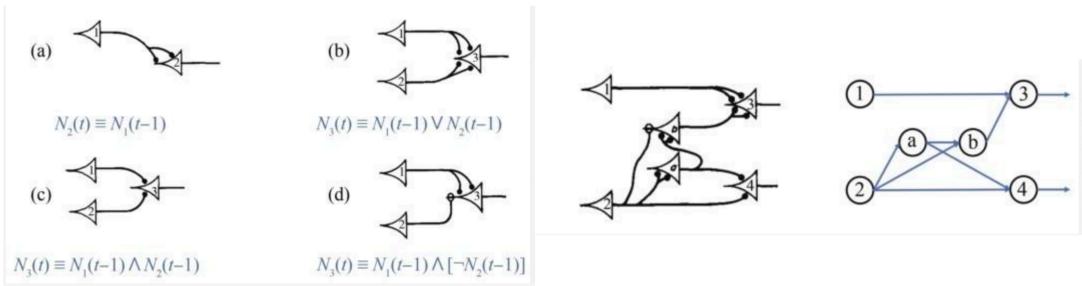
这帮人之间也有千丝万缕的关系，这也告诉我们一个道理，你要想成为大佬，先要接近大佬。

我们按时间线来讲一下参加这次会议的人是怎么凑到一起的。

1936 年，图灵在论文《论可计算数及其在判定问题上的应用》中，提出了图灵机理论。

1943 年，神经生理学家沃伦·麦卡洛克 (Warren McCulloch) 和数学家沃尔特·皮茨 (Walter Pitts) 参考了图灵机里面的一些思想，开发了神经元基本模型，将神经网络的概念引入计算机领域，被认为人工智能第一项工作。¹

¹ <https://www.cs.cmu.edu/~epxing/Class/10715/reading/McCulloch.and.Pitts.pdf>

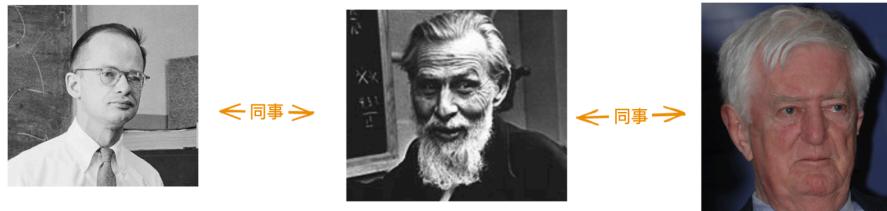


上图为论文中的神经元结构，右侧的图甚至有点像后来的 GRU 和 LSTM。

皮茨是个天才，12岁，3天读完了罗素的《数学原理》，还给罗素写了封信，指出了其中的几处错误。这个罗素就是提出“罗素悖论”的那个，看到信后邀请他去剑桥读他的研究生，根本没想到是个12岁的小屁孩，结果这个小屁孩没钱，十动然拒，罗素痛失天才弟子。皮茨由于都是自学成才，高中都没毕业，没学位也让他四处碰壁。但是他实在过于优秀，很多大佬给他站台。曾跟随芝加哥大学的逻辑学家卡尔纳普（Rudolf Carnap）学习，卡尔纳普无论是在学习还是生活都给了皮茨很大的帮助。后来皮茨被沃伦·麦卡洛克（Warren McCulloch）推荐给控制论之父诺伯特·维纳（Norbert Wiener），维纳发现了皮茨的潜力，直接收了他作为博士生，要注意皮茨连高中和本科学位都没有啊。沃伦·麦卡洛克（Warren McCulloch）本来在芝加哥大学好好的当教授，可能是比较崇拜维纳，辞去教授去MIT当了个研究员，就是为了和维纳一起工作。

1945年以后，奥利弗·塞尔弗里奇（Oliver Selfridge）在MIT读研究生，他的导师就是上面提到的诺伯特·维纳（Norbert Wiener）。这个时候他与沃尔特·皮茨（Walter Pitts）和沃伦·麦卡洛克（Warren McCulloch）在一起工作，研究人类智能。²

q



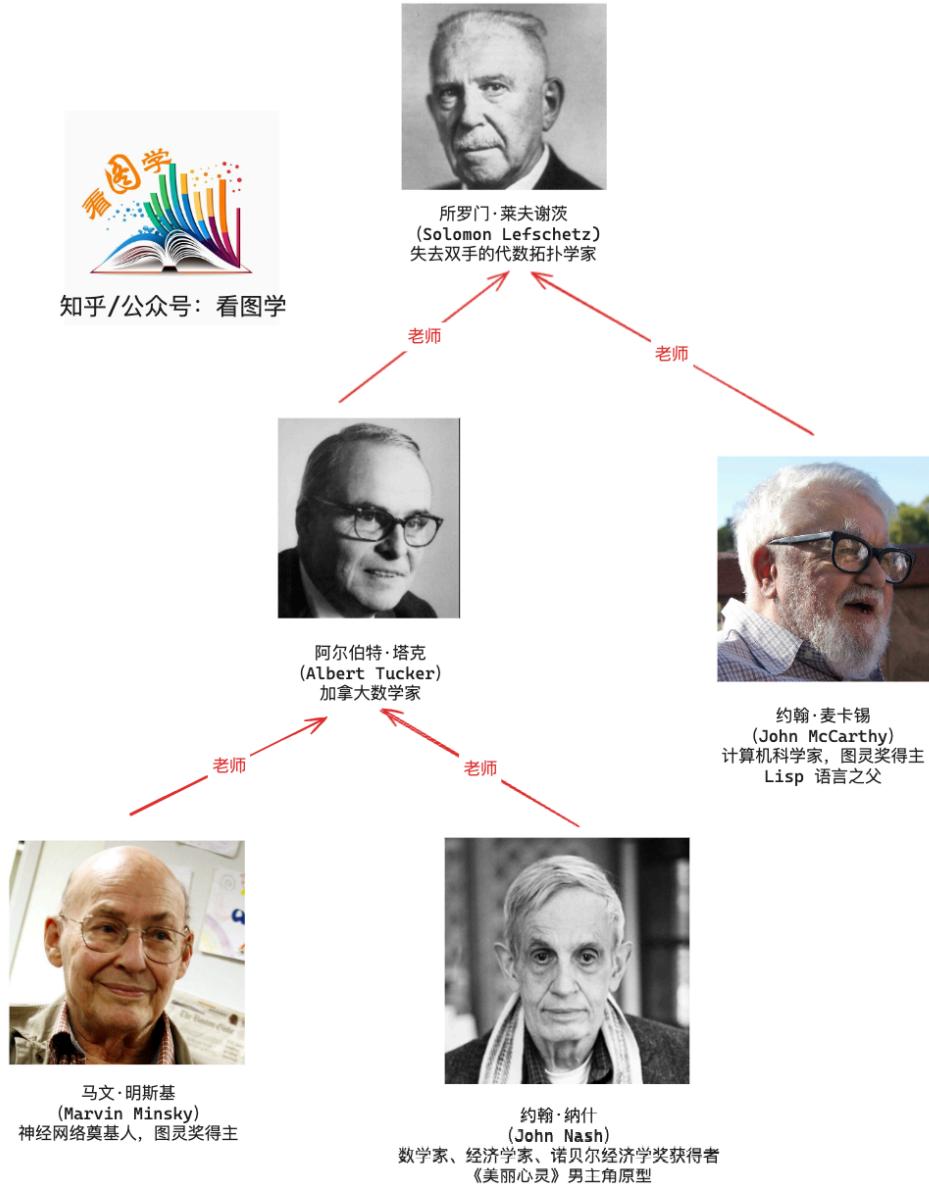
1951年，塞尔弗里奇加入了麻省理工学院的林肯实验室，很快成为一个研究通信技术、模式识别、指挥和控制以及交互式计算的团队的组长。折腾一些机器识别摩尔斯电码的早期工作。塞尔弗里奇可以认为模式识别的奠基人，他写了第一个可工作的AI程序，后来被人们称为“机器知觉之父”。那一年的夏天，他招了伙计，这个人叫马文·明斯基（Marvin Minsky）。

²<https://vineyardgazette.com/obituaries/2009/01/29/oliver-selfridge-computer-pioneer-loved-chappy>



马文·明斯基 (Marvin Minsky) 呢，在这一年搞出了第一部能自我学习的人工神经网络机器，SNARC。他奠定了人工神经网络的研究基础，然而造化弄人，在不久的将来他却亲自给人工神经网络判了死刑，导致很长一段时间神经网络变成了冷板凳。

马文·明斯基的导师是塔克 (Tucker)，塔克还有个学生就是电影《美丽心灵》的主角约翰纳什 (John Nash)。所以纳什是明斯基的师兄。塔克的导师是失去双手的代数拓扑学家所罗门·莱夫谢茨 (Lefschetz)。莱夫谢茨还有个学生，叫约翰·麦卡锡 (John McCarthy)。从师承上讲约翰·麦卡锡是马文·明斯基和纳什的师叔，算是老相识。



马文·明斯基的博士论文是神经网络，但是他当时是数学系的学生，博士委员会看了就有点迷糊，神经网络算是数学么？当时冯诺依曼也是博士委员会的，说虽然现在可能不算，但是不久之后就是数学了。所以马文·明斯基的博士答辩通过，冯诺依曼是大恩人。

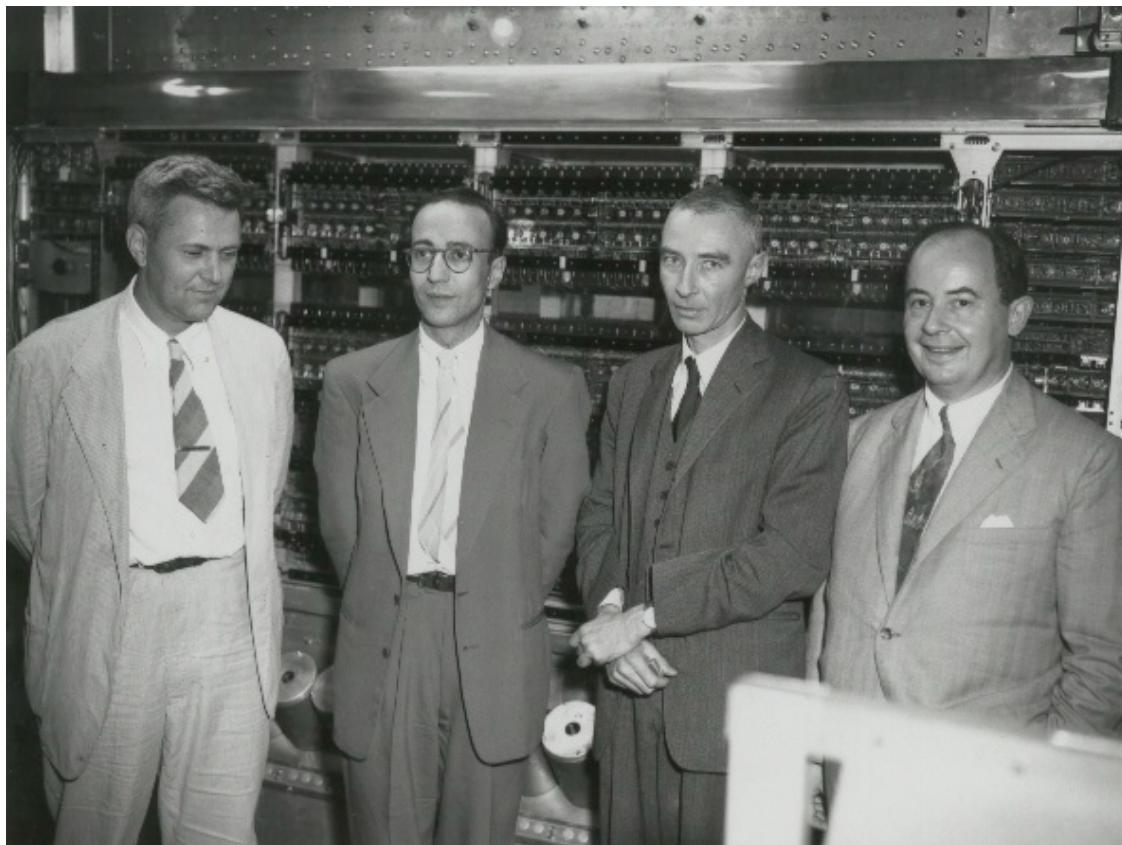
约翰·麦卡锡是个共产主义战士。他是达特茅斯会议的发起人。他是怎么到达特茅斯学院的呢？当时达特茅斯数学系的系主任是克门尼 (Kemeny)。克门尼是图灵的师弟，都师从普林斯顿逻辑学家丘奇 (Church)，他战时和物理学家费曼一起工作，还一度当过爱因斯坦的数学助理，就问牛不牛逼。当时达特茅斯数学系一下子退休了 4 个教授，克门尼压力山大，人都走光了，工作还怎么展开。就去普林斯顿找了 4 个博士，其中一个就是麦卡锡。克门尼和麦卡锡合作还是很愉快的，一起琢磨出了计算机的分时系统，克门尼创造了 Basic 编程语言，而麦卡锡则创造了 Lisp。Lisp 现在可能很多人没听说，但是 Lisp 的设计理念可以说是影响了后续所有的编程语言，我现在因为使用 Emacs 还偶尔用一下。

1953年夏天，麦卡锡和明斯基都在贝尔实验室为克劳德·香农（Claude Shannon）打工。香农是信息论的创始人，和图灵、冯诺依曼是同一个级别的，就不多介绍了。这里有个段子就是香农作为学生的时候，天天问诺伯特·维纳（Norbert Wiener）问题，借鉴他的思想。导致后来维纳拒绝跟香农见面，说：“香农就是来挖我脑浆子的”。后来被认为是创立了信息论的香农的硕士论文《通信的数学原理》中，香农自己都说：“Credit should also be given to Professor N. Wiener”，也就是荣誉也当属于维纳教授。³

Acknowledgments

The writer is indebted to his colleagues at the Laboratories, particularly to Dr. H. W. Bode, Dr. J. R. Pierce, Dr. B. McMillan, and Dr. B. M. Oliver for many helpful suggestions and criticisms during the course of this work. Credit should also be given to Professor N. Wiener, whose elegant solution of the problems of filtering and prediction of stationary ensembles has considerably influenced the writer's thinking in this field.

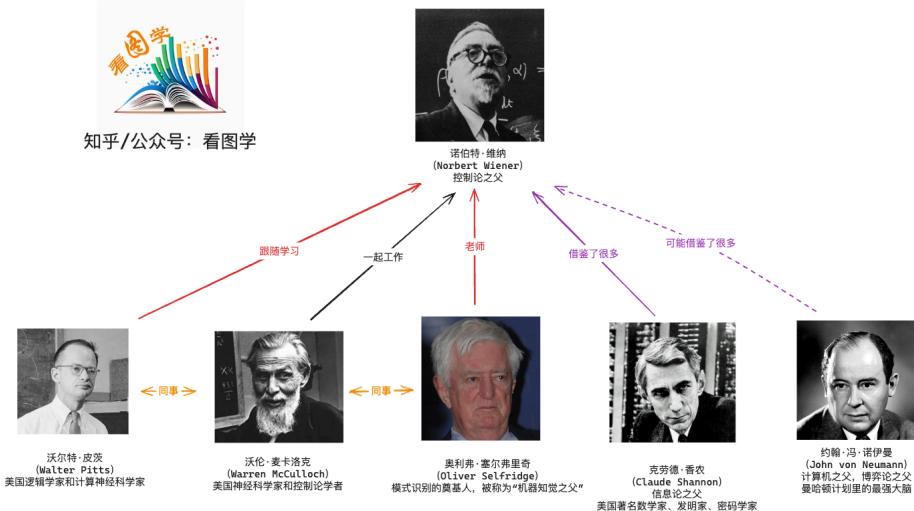
在一本书《维纳传：信息时代的隐秘英雄》曾经提到，冯诺依曼也经常参加维纳的控制论相关的会议，而且是“毫无保留地或者几乎毫无保留地把自己对计算机和自动机器的想法告诉了冯·诺依曼”，而且还派了朱利安·毕格罗（Julian Bigelow）给冯诺依曼当助手。所以有人认为冯诺依曼架构应该叫做维纳-冯诺依曼架构。维纳对后世的贡献很有可能被低估了。



³https://pure.mpg.de/rest/items/item_2383164/component/file_2383163/content

从左到右依次是朱利安·毕格罗、赫尔曼·戈德斯汀、罗伯特·奥本海默(原子弹之父)和约翰·冯·诺依曼

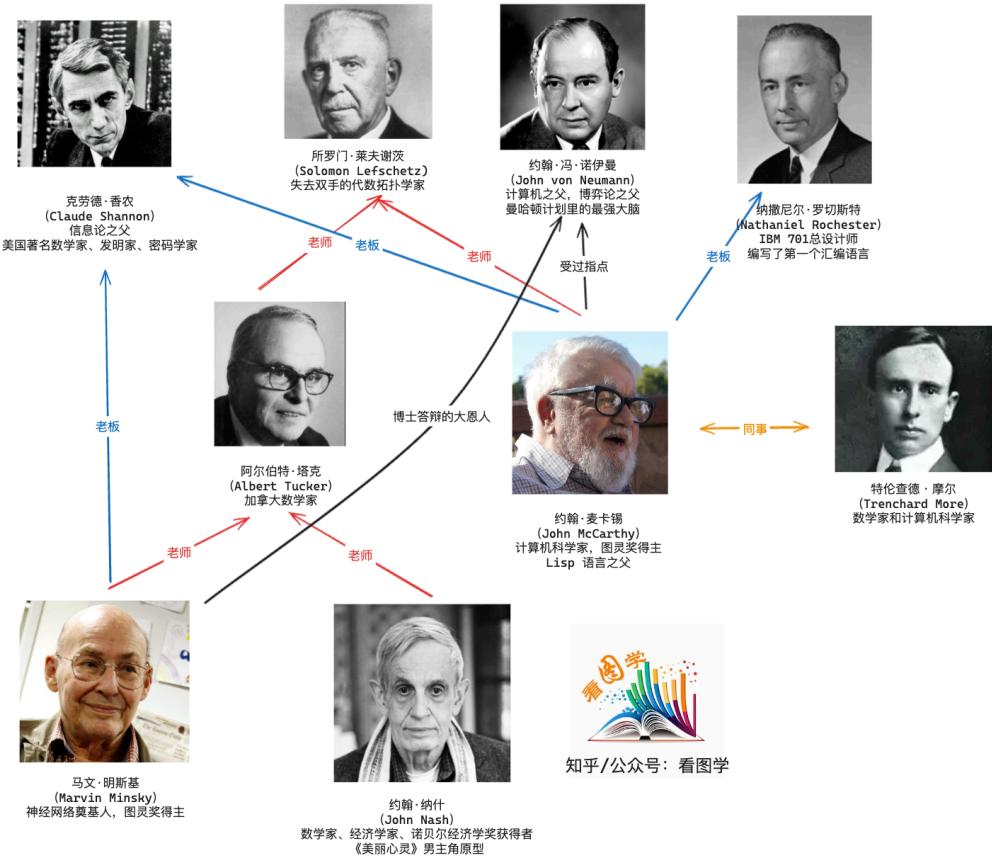
维纳的影响力在当时是巨大的。



1954年，一个叫艾伦·纽厄尔(Allen Newell)的年轻人在一次研讨会上听到奥利弗·塞尔弗里奇(Oliver Selfridge)描述“运行一个计算机程序，学会了识别字母和其他模式”，也开始做人工智能相关的工作，但是他与他的博导司马贺(Herbert Simon)后来开辟了一条全新的道路。

1955年夏天，麦卡锡又跑去IBM打工了。为啥麦卡锡老在夏天跑出去打工？因为那个时候美国的教授只发9个月工资，你要是没有科研经费，就得趁着暑假出去打工，年轻教授真是不容易。打工的老板是纳撒尼尔·罗切斯特(Nathaniel Rochester)，这个老板对神经网络很感兴趣。麦卡锡一看，机会来了，有现老板和前老板站台，再加上前同事明斯基，4个人决定搞一次人工智能的会议。

麦卡锡之所以拉上另外3个人，是因为要申请会议经费，另外三个名气当时都很大。很明显，麦卡锡是达特茅斯会议的KOL。



1955 年还发生了一件事，那就是在美国西部计算机联合大会上，前面提到的奥利弗·塞尔弗里奇 (Oliver Selfridge) 发表了一篇模式识别的文章，他之前都跟神经网络的大牛们混在一起，所以自然是研究神经网络。但是当时研究智能还有另外一派，那就是模拟人的心智。艾伦·纽厄尔 (Allen Newell) 作为这一方向的研究者在会上探讨了计算机下棋。

讨论会的主持人是前面讲对最早提出人工神经元对沃尔特·皮茨 (Walter Pitts)，他最后总结时说：“(一派人) 企图模拟神经系统，而纽厄尔则企图模拟心智 (mind) ……但殊途同归。”

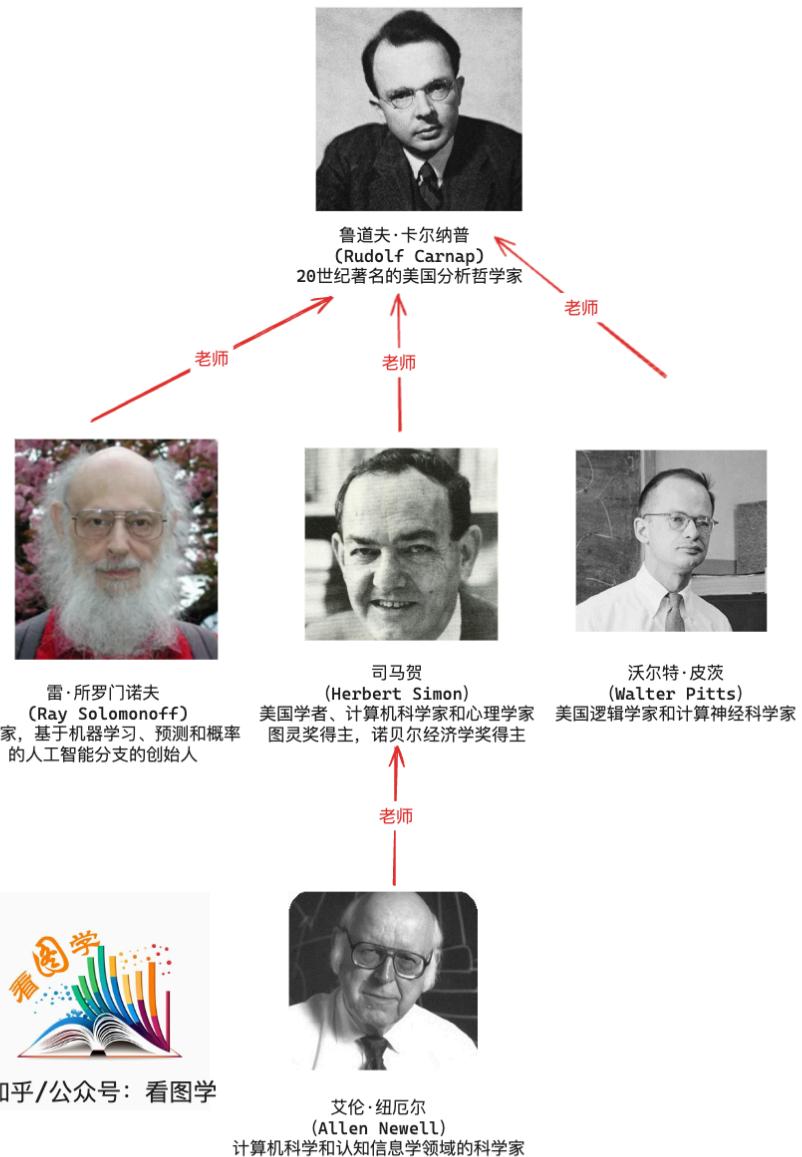
但是从后面的 AI 的发展来看，这两派丝毫没有同归的意思，反而想要同归于尽。

艾伦·纽厄尔 (Allen Newell) 的博导是司马贺 (Herbert Simon)，这两个人是后来人工智能符号派的代表。这两个人后来和第一届图灵奖获得者阿兰·珀里思 (Alan Perlis) 一起创办了卡内基梅隆大学的计算机系，硬是把一个三本提升到了世界一流学校。



司马贺（Herbert Simon）对中国大陆学术界有较深影响。“乒乓外交”打破了中美坚冰后的 1972 年 7 月，赫伯特·西蒙作为美国计算机科学代表团成员首次访问中国，后多次访华交流讲学及合作研究。其中文名字司马贺，即是他 1980 年作为美国心理学代表团成员第二次访华时所起，其本人 70 多岁的年龄开始学习汉语。1994 年当选为中国科学院外籍院士。

司马贺在芝加哥大学求学时，也曾经跟皮茨的老师卡尔纳普（Rudolf Carnap）学习，受他的影响开启了研究人工智能之路。所以虽然后面的人工智能分成了连接派和符号派，但是他们的启蒙老师都是卡尔纳普（Rudolf Carnap）。



终于，在 1956 年，麦卡锡筹备的会议开始了，这次会议名就叫：达特茅斯夏季人工智能研究计划（Dartmouth Summer Research Project on Artificial Intelligence）。

下面这张照片，展示了本次参会的主要 7 个人。



Nathaniel Rochester Marvin L. Minsky John McCarthy
Oliver G. Selfridge Ray Solomonoff Trenchard More Claude E. Shannon

August 1956

当时还有很多人也参加了。比如同样受到卡尔纳普（Rudolf Carnap）影响的所罗门诺夫（Solomonoff），还有两个是来自 IBM 的撒缪尔（Arthur Samuel），达特茅斯的教授摩尔（Trenchard More）。

所以后来有些文献说主要有 10 个人参加。这 10 个人有时候被称为 AI 之父。

2016.4
3
40.

a medal". All of them are heroes. But did this workshop leave out some

1956 Dartmouth Conference: The Founding Fathers of AI



John McCarthy



Marvin Minsky



Claude Shannon



Ray Solomonoff



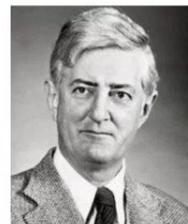
Alan Newell



Herbert Simon



Arthur Samuel



Oliver Selfridge



Nathaniel Rochester



Trenchard More

after him?

麦卡锡后来把参会名单弄丢了，好在所罗门诺夫（Solomonoff）全程参与了两个月的会议，他有个好习惯是记笔记。他的笔记中，记录了 20 个人参加了这次会议，比如纳什。

T.M.

from 196

People at Summer research project.

Solomonoff

Maurice Wilsky MIT Lincoln

John McCarthy IBM, Dartmouth

Claude Shannon MIT, Bell

French More IBM, MIT

Mat Rochester IBM Poughkeepsie

Oliver Selfridge MIT Lincoln

Julian Bigelow IAS

W. Ross Ashby Barnwood house (?)

W.S. McCulloch, MIT, RLE

Abraham Robinson Montreal logic

Tom Etter

John Nash MIT

David Sayre IBM New York

Samuels (IBM) non checkers

Shoulders MIT RLE or Lincoln components man

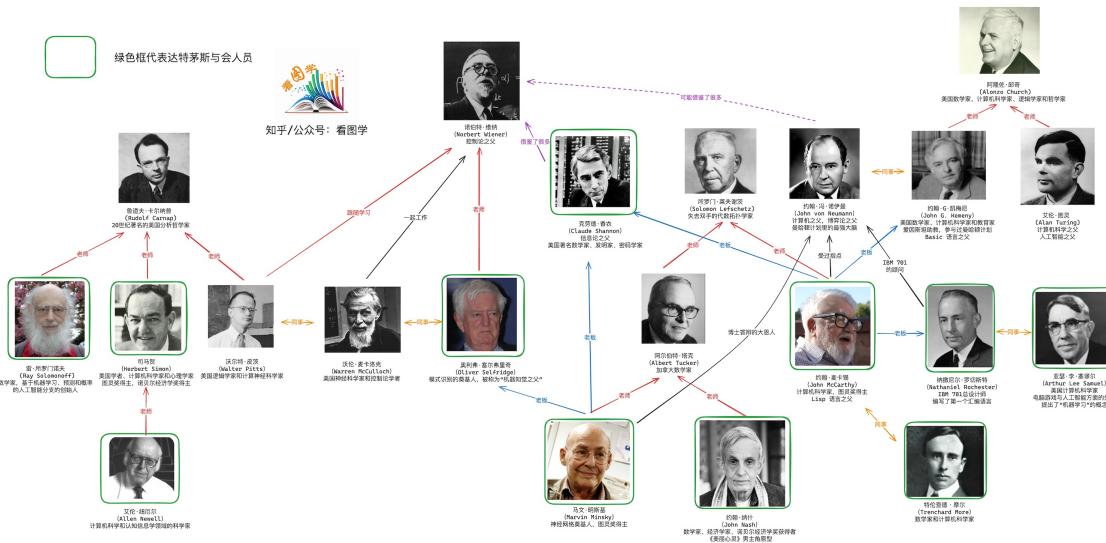
... (with Shoulders)

Alex Bernstein IBM (New York) chess

Herbert Simon: U of Pa (?)

Allen Newell: Rand

上面提到的人建立个关系图谱，大概是下面这个样子。



AI 一大都研究了什么？

会议的主要议题如下：

1. 自动计算机

如果一台机器可以做一项工作，则一台可编程自动计算机能用来模拟这台机器。现有计算机的速度和内存容量可能不足以模拟人脑的许多高级功能，但主要障碍不是缺乏机器容量，而是我们无法编写充分利用我们所拥有优势的程序。

作者注：这个目标似乎已经实现，目前图像识别，语音识别等都已经做的不错了。

2. 如何使用语言对计算机进行编程

可以推测，人类思想的很大一部分包括根据推理规则和猜想规则来操控单词。从这个角度来看，形成包括承认一个新词和一些规则的概括，其中含有它的句子暗示并被其他人暗示。这个想法从未如此精确地制定，也没有制定出实例。

作者注：站在现在的角度看，这就是 NLP 发展的一个基本思想，如何表示一个单词？大佬们 70 年前就已经尝试从 NLP 这个领域来突破 AI 了。

3. 神经网络

如何安排一组（假设的）神经元以形成概念。乌特利·拉什夫斯基 (Uttley, Rashevsky) 和他的团队，法利 (Farley) 和克拉克 (Clark)，皮茨 (Pitts) 和麦卡洛克 (McCulloch)，明斯基 (Minsky)，罗切斯特 (Rochester) 和霍兰德 (Holland) 等人在这个问题上做了大量的理论和实验工作。已经获得了部分结果，但问题是需要更多的理论工作。

作者注：最最早期的神经网络的探索。

4. 计算大小的理论

如果给出一个定义明确的问题（可以用机械方式测试提出的答案是否是有效答案），解决问题的方法是按顺序尝试所有可能的答案。这种方法效率低，要排除它，必须有一些计算效率的标准。一些考虑将表明，为了测量计算的效率，有必要手头有一种测量计算装置复杂性的方法，如果有一个具有功能复杂性的理论，则可以这样做。香农 (Shannon) 和麦卡锡 (McCarthy) 也获得了关于这个问题的部分结果。

作者注：这个属于计算机科学中的算法理论的范畴了。

5. 自我改进

可能真正智能的机器将开展可以最好地描述为自我改进的活动。已经提出了一些这样做的方案，值得进一步研究。这个问题似乎也可以抽象地进行研究。

作者注：已经是机器学习的基本套路了。

6. 抽象

许多类型的“抽象”可以明确定义，而其他几个则不那么明显。直接尝试对这些进行分类并描述从感官数据和其他数据形成抽象的机器方法似乎是值得的。

作者注：如何数据中归纳出知识，也可以归到机器学习。

7. 随机性和创造力

一个相当有吸引力但又不完全不完整的猜想是，创造性思维和缺乏想象力的能力思维之间的区别在于注入一些随机性。随机性必须由直觉引导才能有效。换句话说，受过教育的猜测或预感包括在其他有序思维中的受控随机性。

作者注：这个就有点 AGI 的味道了。当时是通过加入随机性来提高创造性，现在可以通过 Temperature 来调整。那个时候的大牛们是真的没想到后来 GPT “涌现”出来的智能。

AI 一大的影响

从上面可以看出，大佬们在会上还是讨论了很多东西，而且很多东西站在现在来看也并没有过时。这次会议上关于 AI 的研究方向已经隐隐划分为两派：

1. 符号派。他们开创性的认为：知识可以由一组规则来表示，而计算机程序可以使用逻辑来操控这些知识。这一派参会的主要代表人物是：艾伦·纽厄尔 (Allen Newell)、司马贺 (Herbert Simon)，约翰·麦卡锡 (John McCarthy)，马文·明斯基 (Marvin Minsky)。明斯基早期应该是连接派的，因为他的博士论文就是研究神经网络，后来给神经网络死刑，然后叛变成符号派了。在这个会上，符号派的代表纽厄尔和司马贺公布了一款程序“逻辑理论家”(Logic Theorist)，这个程序可以证明怀特海和罗素《数学原理》中命题逻辑部分的一个很大子集。是整个会议最令人印象深刻的。此时此刻符号派稳压连接派一头。
2. 连接派。连接派就是通过一种刻画人类大脑中神经元之间相互连接的机制，来模拟人类行为。当时在会上只是讨论，当时还没有特别亮眼的表现，提到了皮茨 (Pitts) 和麦卡洛克 (McCulloch)。但是会后没多久，神经网络也有了突破。

有意思的是，鲁道夫·卡尔纳普 (Rudolf Carnap) 的两个学生，司马贺与皮兹，分别成了符号派和连接派最早期的代表，还有个学生雷·所罗门诺夫 (Ray Solomonoff) 则在机器学习领域有开创性的贡献，从这个角度来看，AI 的起源，鲁道夫·卡尔纳普是有巨大贡献的。

还有一个流派也隐藏在上面的图中，那就是起源于维纳的控制论，也就是后来的行为主义。采用“感知-动作”来研究，通过环境反馈和智能行为之间的因果去探寻智能，后来就发展除了强化学习和现在正火的 Agent 。

维纳对 AI 的贡献甚至比想象中的还要大，以至于 Michael Jordan (2018) 曾讽刺的说到：“维纳提出的方法却披着麦卡锡发明的术语的外衣”。维纳提出的 Cybernetics，被翻译成了控制论，但实际上“机械大脑论”可能更符合这个词的本意。只不过当时维纳突然与自己的学生决裂，导致年轻学生们都想“离维纳的控制论越远越好”。麦卡锡当时就是这么想的，他曾在“控制论”和“自动机”之间徘徊不定，最后选择了“人工智能”。而且当时计算机的三大“之父”，除了图灵以外，香农、冯诺依曼都深深的受到维纳的影响。图灵是真的天才，自己独立搞了一套。所以维纳可能是活成了 AI 的里子。

AI 的故事到现在才刚刚开始，后续几年，符号派和连接派的内战就要开始了，我们下次再讲。

符号派、链接派，相爱又相杀

从 one-hot 到 ChatGPT

Chapter 2: 主流大模型的模型架构和细节分析

Transformers 起源

要真正搞懂 Transformers 光看《Attention is All you Need》估计还远远不够，因为这篇已经是站在很多巨人的肩膀上了，其中的很多设计都有历史渊源。所以不要想着直接吃第 7 个馒头就饱了。

今天就来聊聊 Transformers 的进化史，相信你看完之后对现在 Transformers 的架构会有更深刻的理解。

Transformers 的进化史同样是神经网络机器翻译 (NMT) 的发展史。在攻克机器翻译这个难题的过程中，模型的框架经过了多次迭代变成了今天的 Transformers。所以先讲一下机器翻译的背景。

神经网络机器翻译

机器翻译干的事情，就是利用机器学习将 A 语言的一句话 $\mathbf{x} = \{x_1, x_2, \dots, x_S\}$ 翻译为 B 语言的一句话 $\mathbf{y} = \{y_1, y_2, \dots, y_T\}$

神经网络机器翻译 (NMT) 建模为：

$$P(\mathbf{y}|\mathbf{x}) = \prod_{t=1}^T P(y_t|y_0, y_1, \dots, y_{t-1}, \mathbf{x})$$

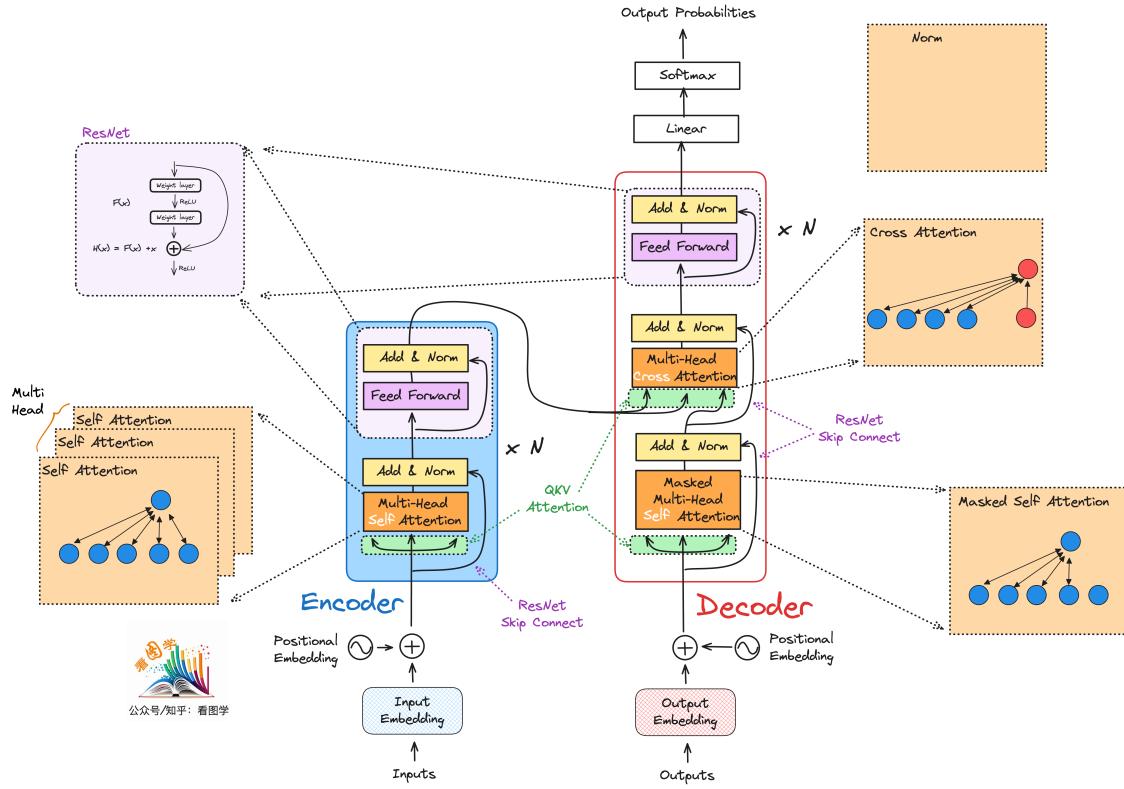
这个建模方式被提出来之后，基本上没什么变化，统计机器翻译 (SMT) 也是一样的，但是模型的架构演进了很多版本。

Transformers 的进化 (或者 NMT 的进化) 大概经历了如下几个重要的节点。

RCTM -> RNN Encoder-Decoder -> Bahdanau Attention -> Luong Attention -> Self Attention/Multihead Attention -> QKV Attention -> Transformers

当然还加入了已经成为神经网络基建的 ResNet。

当前架构每个地方设计的来源，见下图：



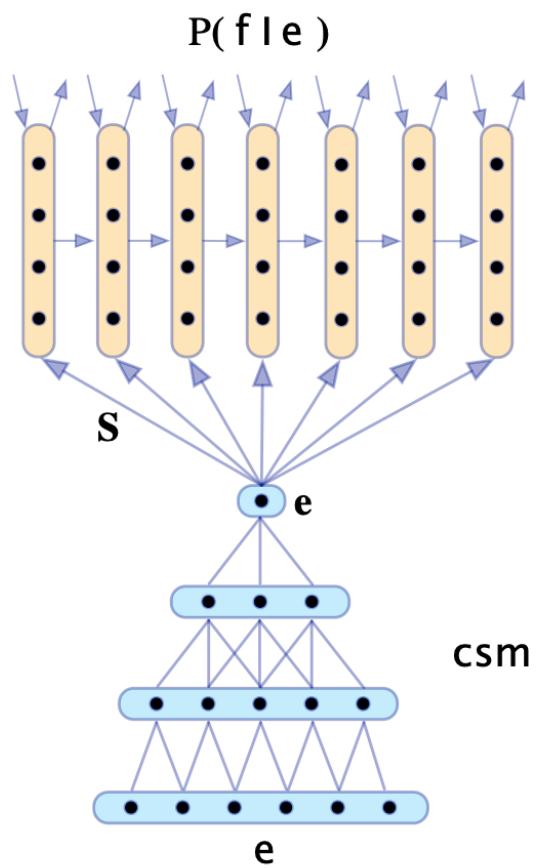
我们按时间顺序来看。

RCTM (Kalchbrenner and Blunsom, 2013)

这是牛津大学在 2013 年提出的一篇论文，这篇文章被认为是神经网络机器翻译 (NMT) 的开篇之作。

这篇论文已经有 Encoder-Decoder 的框架，但是并没有给这个框架命名。文中使用了 CNN 来将源文本“表示”为连续向量，现在通常被称作 Context，就是所谓的 Encoder。然后将连续向量输入给 RNN，RNN 作为 Decoder 去拟合目标句子。

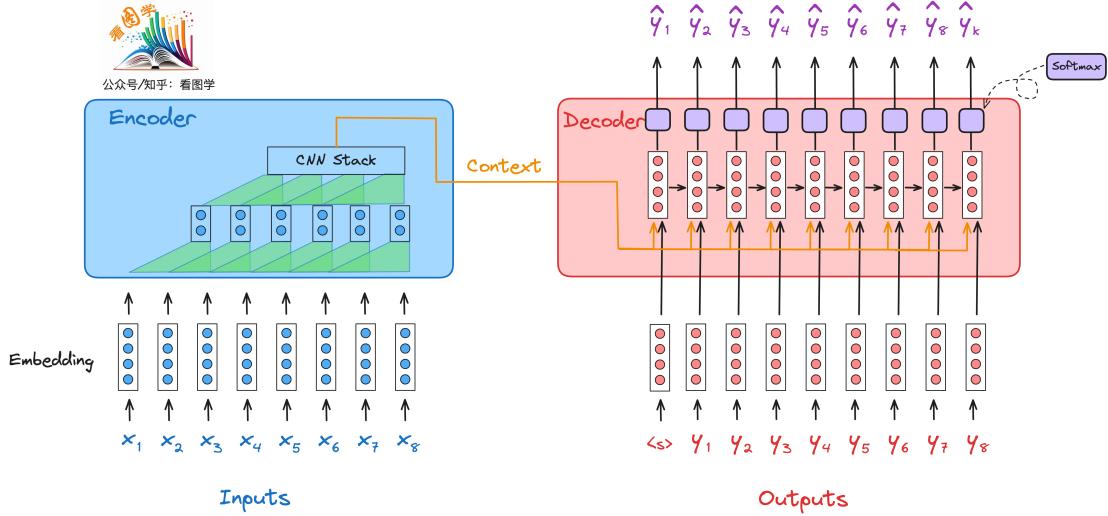
论文中的架构长这样：



RCTM I

转换成现在常见的样子是这样:

RCTM 架构

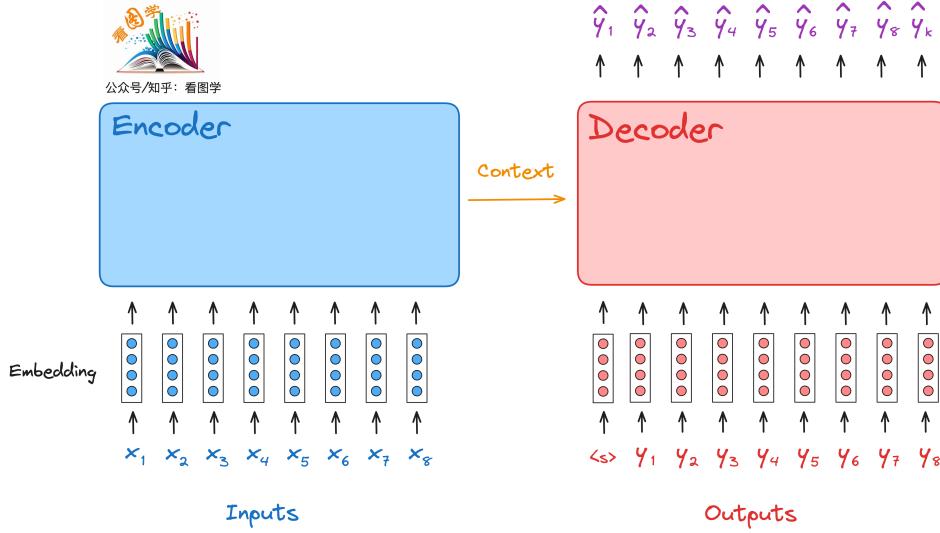


可以看出，这篇论文已经有 Encoder-Decoder 的样子了，只不过左边用了 CNN。之所以使用 CNN 是因为大家那个时候都是搞统计机器学习，n-gram 是无论如何都绕不开的，CNN 的 kernel 大小刚好跟 n-gram 有点像。估计作者这个时候也不敢步子迈的太大，所以采用了 CNN 作为 Encoder，RNN 作为 Decoder。

还有一点要注意的是 Context 参与了 Decoder 的每一步计算。早起大家都是这么干的，后面变成了 Context 只作为 Decoder 的初始状态向量。

该论文的顶层架构设计一直沿用至今，包括 Transformers。虽然内部可能略有差异，但是 框架一直是下面这个样子。为了表述的方便，后面 Encoder 的图示用蓝色表示，其内部的隐向量为蓝色的 h_j ，下标用 j 表示。Decoder 则用红色表示，其内部隐向量为红色的 s_i ，下标用 i 表示。

Encoder-Decoder 的通用架构



这篇神经网络机器翻译的开山之作当时取得了很好的效果，但依然存在一些问题。比如原生的 RNN 因

为梯度爆炸和消失对长句子无能为力。

1. 进化路径

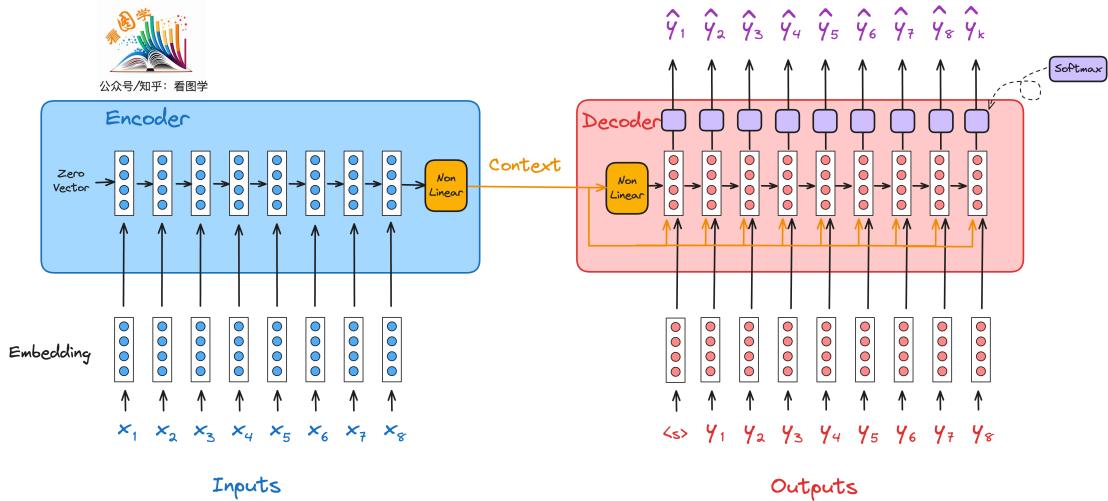
- 神经网络机器翻译的初号机。
- 实现了 Encoder-Decoder 架构。
- Encoder 提取的 Context 参与了所有目标字符串的预测。
- Decoder 用来预测下一个字符。
- 这是个 end-to-end 的神经网络模型。

RNN Encoder-Decoder (Cho et al., 2014a)

这篇论文和下面的 Bahdanau Attention 都是 Bengio 团队的成果，Bahdanau 是这篇论文的二作。

这篇论文首次明确提出了 Encoder 和 Decoder 的概念。但是整体的架构和 RCTM 基本一样，只不过是 Encoder 也变成了 RNN。可能是觉得这么做学术创新点不太够，所以本文另外还提出了和 LSTM 齐名的 GRU 架构。

RNN Encoder-Decoder 架构



从上图可以看出，和 RCTM 一样，Encoder 编码后的隐向量被用到了 Decoder 的每一个 step。
用公式来描述为：

- Encoder

$$h_0 = \mathbf{0}$$

$$h_j = \text{RNN}_{GRU}(h_{j-1}, x_j)$$

$$C = \tanh(V \cdot h_T)$$

- Decoder

$$s_0 = \tanh(V' \cdot C)$$

$$s_i = \text{RNN}_{GRU}(s_{i-1}, [y_i; C])$$

$$= \text{softmax}(\text{MLP}(s_i))$$

可惜的是这个 Encoder-Decoder 的架构并没有做成一个端到端的模型，只是把 Decoder 的输出概率作为特征喂给了统计机器翻译 (SMT) 模型。

有时候看论文确实是有这么一种感觉，总感觉离更好的答案就差一口气了，但是很可惜，这一口气就是没喘上来。这也正是科研的艰难之处，筚路褴褛。就像在山洞里挖出口，可能再挖一铲子就打通了，但是在挖下去之前，谁也不知道挖的方向对不对，但是研究经费可能不够了。要知道香农作为信息论的创始人，自己都没有找出最佳编码算法，反而是几年后被霍夫曼给想出来了。

1. 进化路径

- Encoder 采用了 RNN
- 为了解决长文本的梯度消失/爆炸，采用了 GRU 架构
- 开倒车了，从 end-to-end 变成了特征提取器。

Bahdanau Attention (Bahdanau et al., 2014)

这篇论文也是 Bengio 团队的成果，是对前一篇 RNN Encoder-Decoder 论文工作的延续。

这篇文章中，提出了 Attention 的概念。作者认为在翻译过程中，两种语言中相同含义的词或者段落应该能对齐。比如“How(多) old(大) are you(你)?”，就是一个中英文的对齐。神经网络理应学习到这个知识，但是目前好像并没有学到。所以作者就设计了一个网络来计算输入输出两种语言之间不同词之间的关联分数，也就是 Attention Score。

等一下，我设计一个全连接网络是不是也能计算输入输出的关联？和 Attention 有什么区别？

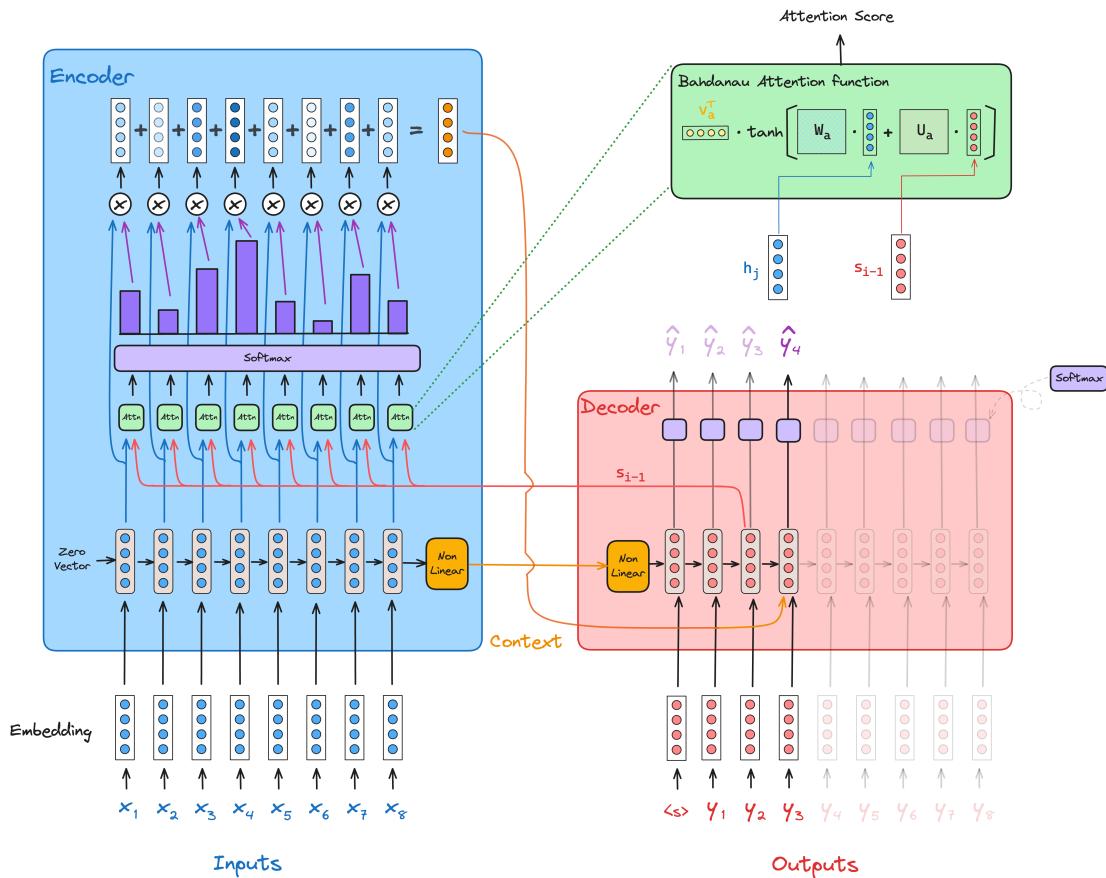
这两个其实是一静一动。全连接网络训练完成之后，权重就固定了，不能变了。但是 Attention 则可以动态的，根据输入来计算出输出应该更关注哪些输入。

Bahdanau Attention 的思路如下。

Bahdanau Attention 架构



means RNN Cell means vector



- Encoder

$$h_0 = \mathbf{0}$$

$$h_j = \begin{bmatrix} \vec{h_j} \\ \overleftarrow{h_j} \end{bmatrix}$$

$$h_j = \text{RNN}_{GRU}(h_{j-1}, x_j)$$

$$C = \tanh(V \cdot h_T)$$

- Decoder

$$s_0 = \tanh(V' \cdot \overleftarrow{h_1})$$

$$e_{ij} = v_a^\top \tanh(W_a s_{i-1} + U_a h_j)$$

$$\alpha_{ij} = \frac{e_{ij}}{\sum_{k=1}^T e_{ik}}, \alpha_{ij} \text{ is a scalar}$$

$$c_i = \sum_{j=1}^T \alpha_{ij} h_j$$

$$s_i = \text{Bi-RNN}_{GRU}(s_{i-1}, [y_i; c_i])$$

$$= \text{softmax}(\text{MLP}(s_i))$$

- 需要注意的是原论文计算词概率的时候并不是简单的 $\hat{y}_i = \text{softmax}(\text{MLP}(s_i))$, 而是在 GRU 后再加了两层网络实现了一个 maxout。这里为了方便和其他模型对比简化了公式。

1. 进化路径

- 在 Encoder-Decoder 的基础上增加了 Attention 机制。
- 终于变成了 End-to-End 模型。
- Encoder 的 context 不再作为 Decoder 的每一个 step 的输入。

Seq2Seq (Sutskever et al., 2014)

这篇是 Ilya 的论文, 当时还是很轰动的, 因为是 Google 的论文, 再一个效果确实很好。但是实际上就是将 RNN Encoder-Decoder 做成了端到端, 模型结构非常简单。然后堆叠 LSTM 的参数量取得了不错的效果。当然也有些 Trick, 比如逆序输入能够提升效果, 个人猜测可能是一句话重要的部分往往放在前面的原因。逆序后 Encoder 和 Decoder 开头的部分离的近, 信息衰减变小了。

有意思的是 seq2seq 和 Bahdanau Attention 的论文几乎是同时写的, 所以这两篇论文相互引用了。所以只将 Encoder Context 作为 Decoder 的初始化参数可能影响了 Bahdanau Attention 的结构设计, 但是也没多大影响, 因为 Bahdanau Attention 相当于 Encoder 的所有 context 都是用了。

然后 seq2seq 的效果比 Bahdanau Attention 要好, 主要原因也是参数量更大, 这么比较有点不太公平。

1. 进化路径

- 可能影响了 Bahdanau Attention 的结构设计。
- 对 Transformers 进化影响不大。

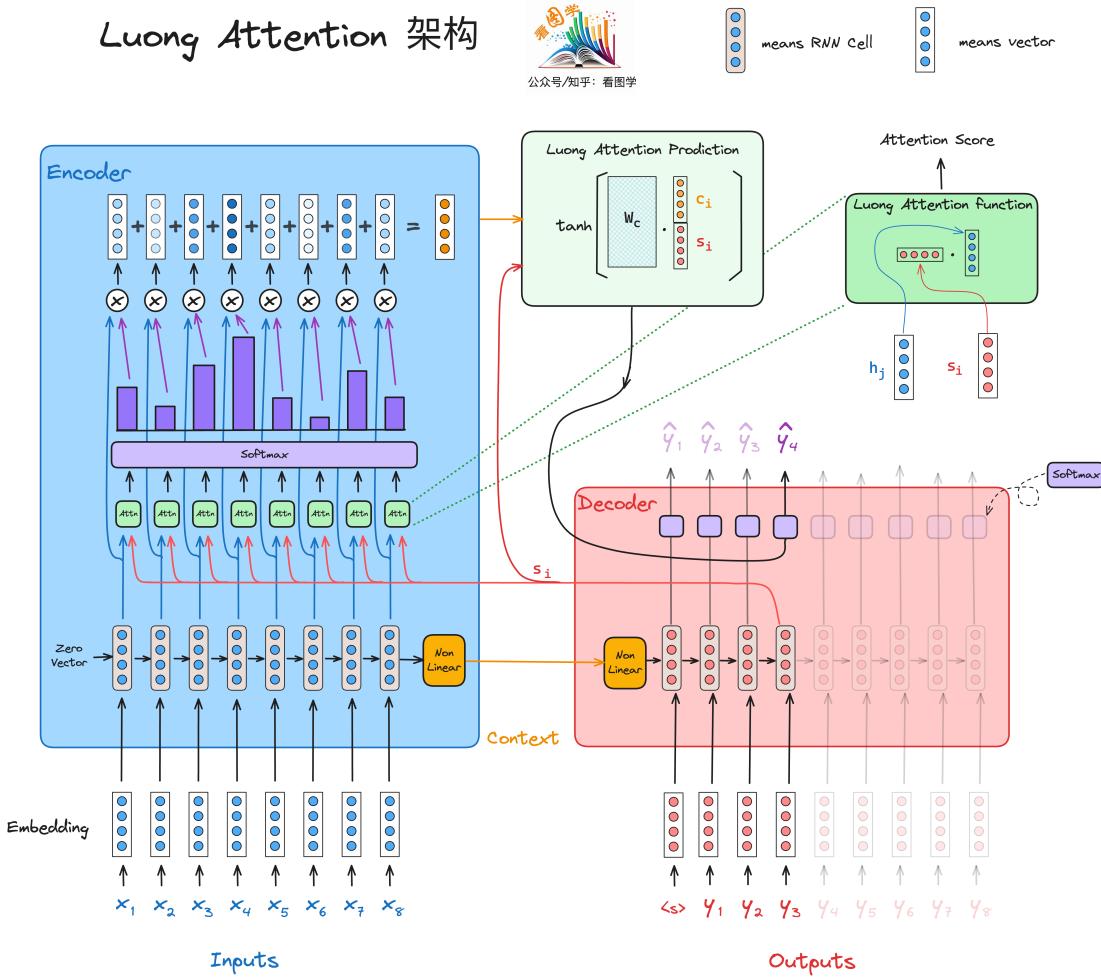
2. Seq2Seq vs. Encoder-Decoder:

- Seq2Seq but not Encoder-Decoder: RNN, HMM, GPT
- not Seq2Seq but Encoder-Decoder: VAE
- Seq2Seq and Encoder-Decoder: Transfomers

Luong Attention (Luong et al., 2015).

Bahdanau Attention 计算 Attention Score 的方法是相加。Luong Attention 则尝试了更多方法，比如点积。

结构上略有修改。



1. 进化路径

- Attention 的计算方法多样性探索。

Self Attention

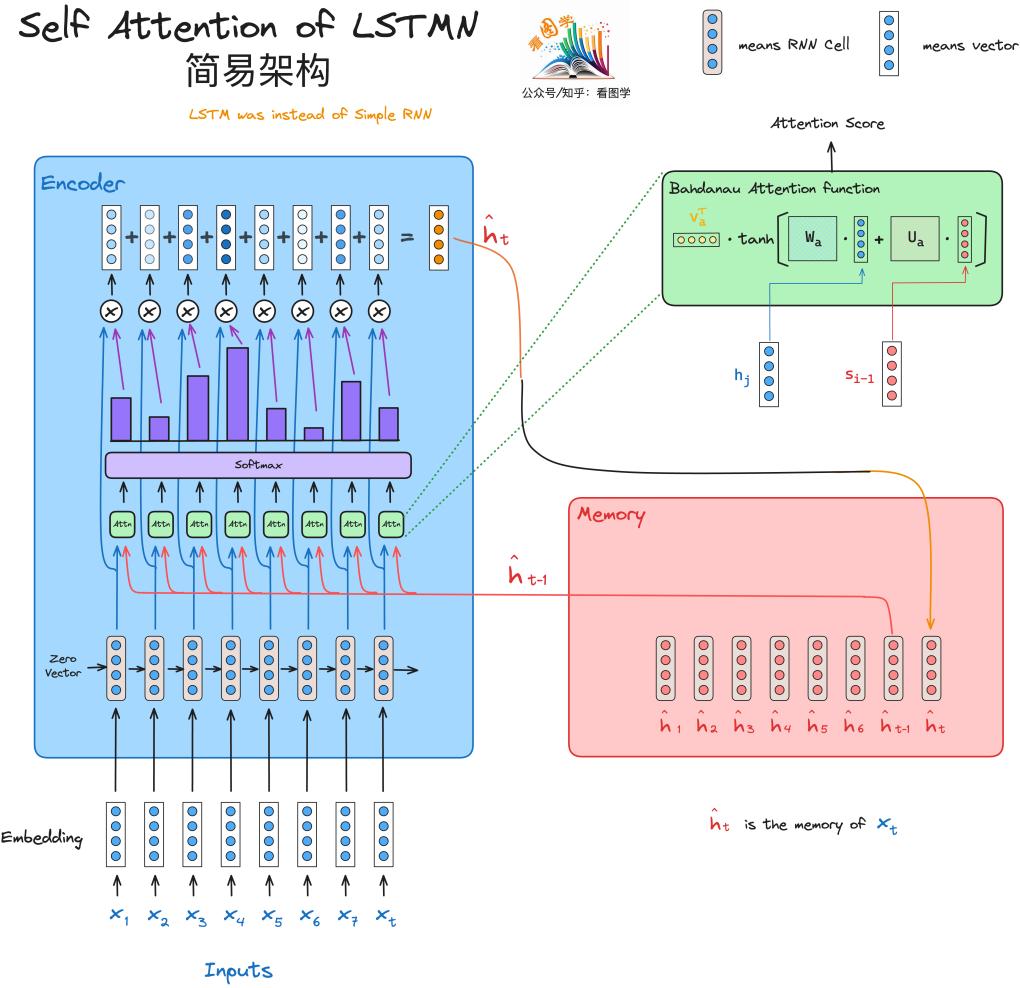
之前的 Attention 关注的都是不同序列之间的 Attention，比如机器翻译的原始文本和目标文本，文生图中的文本序列和图像序列。这种 Attention 称作 Cross Attention，Cross Attention 可以说是 Encoder-Decoder 或者 seq2seq 中使用 Attention 的标准结构。

这篇论文将 Attention 的思想借鉴到了机器阅读理解中。作者认为我们在顺序的阅读每个单词的时候，每个单词和前面单词的关联度是不一样的，如下图所示。其实之前也有很多类似的工作，比如依存分析。这个工作是否可以让 Attention 来做呢？

作者提出的框架，整体上沿用了 Bahdanau Attention 的架构，但是 Bahdanau Attention 计算分数是 Encoder 和 Decoder 之间的。这里只有 Encoder，作者就给每个输入构建了一个 Memory State。下图为了和 Attention 对比，将 Memory State 放到了 Decoder 的位置，但是要记住 Encoder 和 Memory 两个模块是同步更新的。

下图做了两点简化：

1. LSTM 简化为 Simple RNN，不然画起来有点复杂。
2. Attention 的计算少了词向量部分。论文中在计算 Attention 的时候，词向量也参与了计算。



将上图的 Simple RNN Cell 替换为 LSTM，同时计算 Attention 的时候加入词向量，就是论文的最终架构。需要注意，LSTM 中的 Carry Memory 的计算也采用了 Attention 的计算方式。

具体的计算公式为：

- Encoder

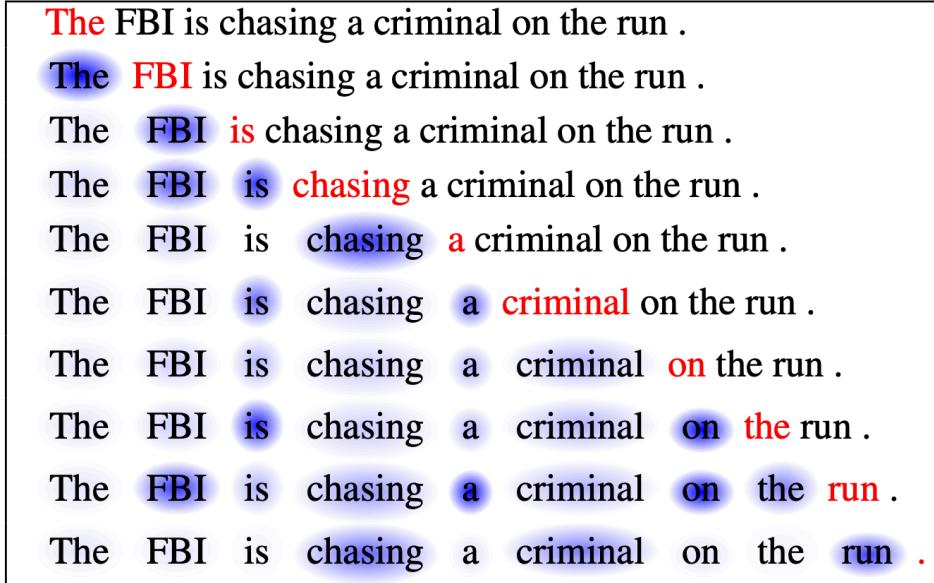
$$e_{ij} = v_a^\top \tanh(W_a \tilde{h}_{i-1} + U_a h_j + W_x x_i)$$

$$\alpha_{ij} = \frac{e_{ij}}{\sum_{k=1}^T e_{ik}}, \alpha_{ij} \text{ is a scalar}$$

$$\begin{bmatrix} \tilde{c}_i \\ \tilde{h}_i \end{bmatrix} = \sum_{j=1}^{i-1} \alpha_{ij} \begin{bmatrix} c_j \\ h_j \end{bmatrix}$$

$$\begin{bmatrix} c_i \\ h_i \end{bmatrix} = \text{LSTM}\left(\begin{bmatrix} \tilde{c}_i \\ \tilde{h}_i \end{bmatrix}, x_i\right)$$

关于 LSTM 的知识, 这里不再赘述。LSTM 的知识见:https://mp.weixin.qq.com/s/Yyf_8VlSS6VE0wKwsrkAww
 最后, 由于本论文只关注前面词的 Attention, 所以其实是 Masked Self Attention。
 最终效果的可视化结果如下:



1. 进化路径

- 在 cross attention 的基础上, 提出了 self-attention, 或者叫 intra-attention.

MultiHead Self Attention (Lin et al., 2017)

这篇论文将 Attention 的思想借鉴到了文本表示学习中。其出发点也很简单, 我们读一段文本自己有时候会划重点, 或者圈关键词, 这个工作能不能交给 Attention 呢?

作者同样参考了 Bahdanau Attention, 只不过在计算 attention score 的时候, 输入从 h_j 、 s_i 改成里双向 LSTM 的两个方向的 hidden states。

- Encoder

$$\begin{aligned}
\overrightarrow{h_t} &= R_{LSTM}(\mathbf{w}_t, \overrightarrow{h_{t-1}}) \in \mathbb{R}^u \\
\overleftarrow{h_t} &= R_{LSTM}(\mathbf{w}_t, \overleftarrow{h_{t-1}}) \in \mathbb{R}^u \\
h_t &= \begin{bmatrix} \overrightarrow{h_t} \\ \overleftarrow{h_t} \end{bmatrix} \in \mathbb{R}^{2u} \\
&\quad =
\end{aligned}$$

$$\begin{aligned}
e_{ij} &= w_{s2}^\top \tanh(W_{s1} h_j) \\
w_{s2}^\top \tanh(\begin{bmatrix} W_{s1}[:, u] & W_{s1}[u, :] \end{bmatrix} \begin{bmatrix} \overrightarrow{h_j} \\ \overleftarrow{h_j} \end{bmatrix}) \\
&= w_{s2}^\top \tanh(W_{s1}[:, u] \cdot \overleftarrow{h_j} + W_{s1}[u, :] \cdot \overrightarrow{h_j})
\end{aligned}$$

$$\begin{aligned}
\alpha_{ij} &= \frac{e_{ij}}{\sum_{k=1}^T e_{ik}}, \alpha_{ij} \text{ is a scalar} \\
m_i &= \textcolor{brown}{c_i} = \sum_{j=1}^T \alpha_{ij} \textcolor{blue}{h_j}
\end{aligned}$$

可以看出，Self Attention 计算 Score 的设计明显是参考了 Bahdanau Attention 的计算方法。

上面的计算是单个 Attention 的计算方法。然后借鉴一下卷积网络的多个 kernel 的思想，作者设计了多个 Attention，期望不同的 Attention 学习到不同的注意力，从而更好的提取特征。这种一个不行就上多个到方法在深度学习中经常使用，比如 CNN 多 kernel，MultiHead Attention，Mixture of Experts 等。

然后作者提出了 Attention 的矩阵运算形式。

$$H = (h_1, h_2, \dots, h_n) \in \mathbb{R}^{n \times 2u}$$

$$W_{s1} \in \mathbb{R}^{d \times 2u}$$

$$W_{s2} \in \mathbb{R}^{r \times d}$$

$$E = W_{s2} \tanh(W_{s1} \cdot H^\top) \in \mathbb{R}^{r \times n}$$

$$A = \text{softmax}(E) \in \mathbb{R}^{r \times n}$$

$$M = AH \in \mathbb{R}^{r \times 2u}$$

可以看出，MultiHead 是通过 r 来体现的。然后这个矩阵相乘 AH 已经和 Transformers 最终形态的 Attention $AV = \text{softmax}(\frac{QK^\top}{\sqrt{d}})V$ 有点类似了。

效果也很显著，如下图。从此之后，Self Attention 成为表示学习中的扛把子。

- I really enjoy Ashley and Ami salon she do a great job be friendly and professional I usually get my hair do when I go to MI because of the quality of the highlight and the price the price be very affordable the highlight fantastic thank Ashley i highly recommend you and ill be back
- love this place it really be my favorite restaurant in Charlotte they use charcoal for their grill and you can taste it steak with chimichurri be always perfect Fried yucca cilantro rice pork sandwich and the good tres lech I have had.The desert be all incredible if you do not like it you be a mutant if you will like diabeetus try the Inca Cola
- this place be so much fun I have never go at night because it seem a little too busy for my taste but that just prove how great this restaurant be they have amazing food and the staff definitely remember us every time we be in town I love when a waitress or waiter come over and ask if you want the cab or the Pinot even when there be a rush and the staff be run around like crazy whenever I grab someone they instantly smile acknowledge us the food be also killer I love when everyone know the special and can tell you they have try them all and what they pair well with this be a first last stop whenever we be in Charlotte and I highly recommend them
- great food and good service what else can you ask for everything that I have ever try here have be great
- first off I hardly remember waiter name because its rare you have an unforgettable experience the day I go I be celebrate my birthday and let me say I leave feel extra special our waiter be the best ever Carlos and the staff as well I be with a party of 4 and we order the potato salad shrimp cocktail lobster amongst other thing and boy be the food great the lobster be the good lobster I have ever eat if you eat a dessert I will recommend the cheese cake that be also the good I have ever have it be expensive but so worth every penny I will definitely be back there go again for the second time in a week and it be even good this place be amazing

(b) 5 star reviews

1. 进化路径

- 提出了另一种 self-attention 的方法
- 提出了 Multi Head Attention

FRUSTRATINGLY SHORT ATTENTION SPANS IN NEURAL LANGUAGE MODELING

这篇论文可能是最早提出 query, key, value attention 的论文，但是引用量并不高。

这篇论文认为现有的 Attention，隐向量至少承担了 3 个功能：

1. 计算 attention score
2. 计算 context vector
3. 作为 hidden state 来进行 RNN 的计算。

任务实在有些繁重，所以提出了使用 3 个隐向量来计算 Attention，功能如下：

1. key 用来计算 attention score.
2. value 用来和 Attention score 相乘。
3. predict 用于预测词的分布。

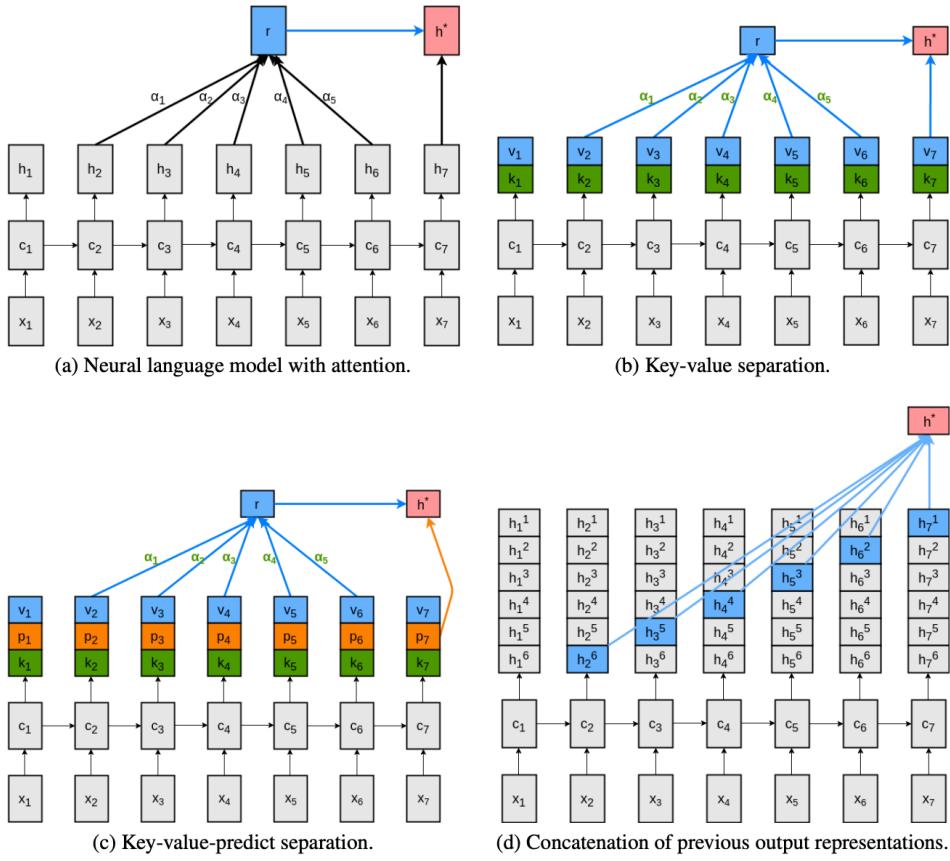


Figure 1: Memory-augmented neural language modelling architectures.

从后面 Transformers 的实现来看, 没有使用 predict, 新增了一个 query , query 和 key 用来计算 Attention Score, value 则用来鹤 Attention score 相乘。

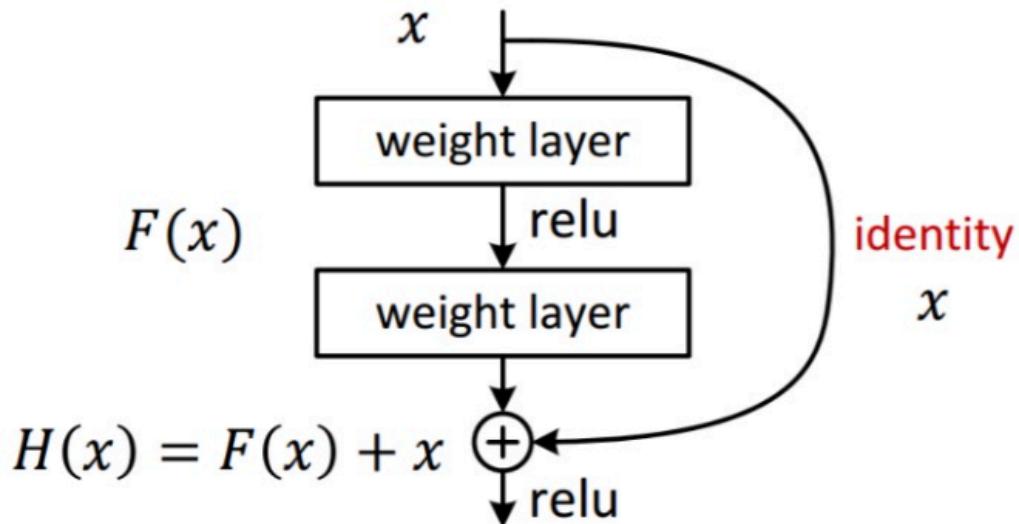
1. 进化路径

- 将隐向量投影为 3 个, 分别为 key, value, predict, 各自有不同的分工。

ResNet

随着神经网络层数增加, 梯度消失/爆炸问题越来越严重, 研究人员想了各种方法, 比如 ReLU, LSTM 等, 都取得了一定的效果, 但是基本到几十层就歇菜了。直到 ResNet 给神经网络修了一条高速公路, 神经网络层数的瓶颈才算突破。天不降生何凯明, DL 万古如长夜:)

• Residual net



关于 ResNet 的解读已经很多，何凯明自己就发了 3 篇相关的文献。分别为：

1. Deep Residual Learning for Image Recognition
2. Identity mappings in Deep Residual Networks
3. Aggregated Residual Transformation for Deep Neural Networks

这里就重点说一下个人觉得重要的几点：

1. 加入 skip connect 使得信息可以直达最后一层。
2. 再一个是在反向传播的时候， $\frac{\partial f(x)}{\partial x}$ 可能消散，但是 $\frac{\partial(f(x)+x)}{\partial x} = 1 + \frac{\partial f(x)}{\partial x}$ 保证了计算的稳定性。
1. 进化路径
 - 属于基建了。

Transformers

至此，Transformers 大部分零件已经凑齐，Let's Roll Out.

Transformers 架构

至此，Transformers 大部分零件已经凑齐，Let's Roll Out.

Transformers 也是为了机器翻译设计的，回顾一下 Transformers 之前的机器翻译模型，大多还是 RNN Encoder-Decoder 的范式，但是这样也就继承了 RNN 的所有问题。主要问题有两点：

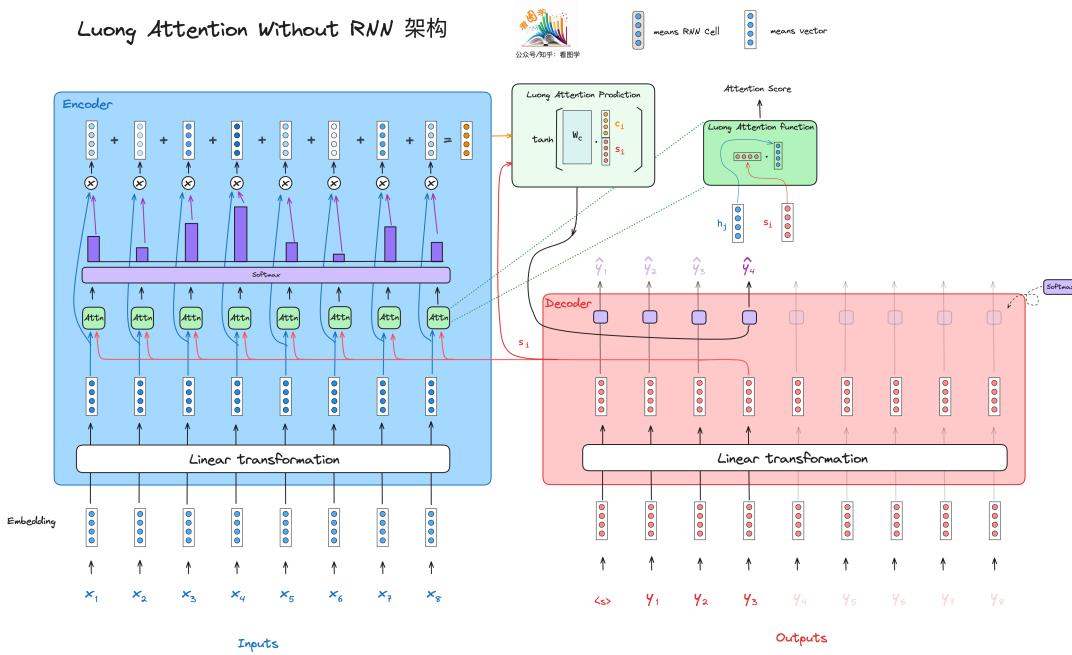
1. 长序列的梯度消失/爆炸问题。
2. 只能一步一步计算，无法并行。

通过堆叠 RNN，扩大参数量确实也取得了一定的效果，比如 Seq2Seq。但是 Bahdanau Attention 出现后，让研究人员看到了另外一种可能。

之前序列中某个节点要获取前面节点的信息，都是通过 RNN 这个中间商搬运过来的，特征提取或者信息压缩的效率么，总是有点差强人意。现在 Attention 来了，前面的节点信息可以厂家直销了，boss 直聘了，还需要 RNN 这个中间商赚差价么？

如果将 Bahdanau/Luong Attention 的 RNN 去掉，会得到了什么？我们来尝试一下。

Luong Attention without RNN



上图中，原来 RNN 的位置替换成了一个线性变换。现在的神经网络很少有将 Word Embedding 直接参与一些网络结构的计算，一般都会先做一个线性变换。这样做一方面是增加了模型可学习的参数，再一个是我们大家都希望 Word Embedding 就专注于学习词的表示。当然也有例外，比如 Word Embedding weight tying 技巧。

上图其实已经有点 Transformers 的影子了，你能找出与 Transformers 结构上的相同之处么？

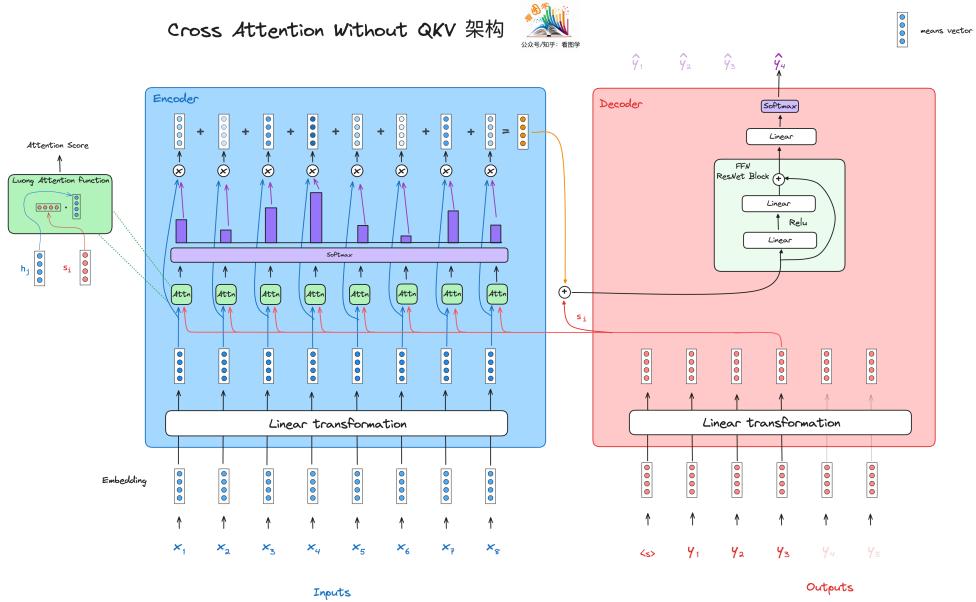
去掉 RNN 后，再也不需要一步一步的计算了，整个架构从原来的序列模型变成了一个全连接图模型，这就很方便的进行矩阵计算，从而享受并行计算或者 GPU 加速带来的运行效率的提升。关于如何实现矩阵计算，请参考后面 Attention 矩阵表示那一章。

去掉了 RNN 也有个明显的问题。那就是变成了全连接图之后，序列的位置信息丢失了。对于 Attention 来说，“八王大”、“八大王”、“王八大”还有“大王八”是一样的。这怎么行，必须让 Attention 知道位置信息，于是研究人员提出了 Position Embedding 的方法，可以认为是全连接图中每个节点带上了位置信息。设计非常巧妙，几句话说不明白，请看后面 Position Embedding 那一章。

修改 FFN 为 ResNet Block

早些年的时候 tanh, sigmoid 等激活函数还经常使用, 但是随着神经网络深度的增加, 计算量有点大。所以后来大多都是用 ReLU, GeLu 等。

Transformers 野心不小, 并不想搭几层就结束了, 所以将上图中 tanh + FFN 换成 ResNet Block 后, 上图变成了:



注意该图在 Attention 前后也加入了 skip connection。

然后论文中给这个 FNN 取名为 Position-wise feed-forward networks, 当时也没太注意这个 Position Wise。后来发现 Position Wise 其实就是常用的 [batch_size, hidden_size] 的矩阵, 在这里变成了 [batch_size, sequence_length, hidden_size] 的矩阵。上面的图就是对 sequence 中的 y_4 进行预测运算。

这里不得不提一点, 虽然论文的名字叫《Attention is All your Need》, 但是实际上, **FFN and ResNet are also your need.**

研究人员发现 FFN 和 ResNet 的 Skip Connection 无论去掉哪一个, 模型都会变得不可用。⁴ 所以说 **Attention, FFN, ResNet** 可以认为是 **Transformers** 架构的三驾马车, 缺一不可。

假设只用了 Attention, 仔细看一下 Attention 的计算公式, 虽然其中有一个 softmax 的非线性运算, 但是对于 value 来说, 并没有任何的非线性变换。所以每一次 Attention 的计算相当于是对 value 代表的向量进行了加权平均, 即使在上面堆叠多个 Self Attention, 依然只是对 value 向量的加权平均而已。一层和多层没有本质的区别。这就是 FFN 必须要存在的原因, 或者说更本质的原因是因为 FFN 提供了最简单的非线性变换。

假设 $\alpha_{(i)} = \text{softmax}(q_{(i)} k_{(i)}^T)$, 表示层 i 的 attention score.

⁴Attention is Not All You Need: Pure Attention Loses Rank Doubly Exponentially with Depth

$$\begin{aligned}
v_{(1)} &= xW_{(1)} \\
x_{(1)} &= \alpha_{(1)}v_{(1)} \\
v_{(2)} &= x_{(1)}W_{(2)} \\
x_{(2)} &= \alpha_{(2)}v_{(2)} \\
&= \alpha_{(2)}x_{(1)}W_{(2)} \\
&= \alpha_{(2)}\alpha_{(1)}xW_{(1)}W_{(2)} \\
x_{(3)} &= \alpha_{(3)}v_{(3)} \\
&= \alpha_{(3)}x_{(2)}W_{(3)} \\
&= \alpha_{(3)}\alpha_{(2)}\alpha_{(1)}xW_{(1)}W_{(2)}W_{(3)} \\
&\dots \\
x_{(i)} &= \alpha_{(i)}\alpha_{(i-1)}\dots\alpha_{(1)}xW_{(1)}W_{(2)}W_{(3)}\dots W_{(i)}
\end{aligned}$$

通过上面的公式可以看出，无论堆叠多少层，都是最开始输入 x 的一个线性变换。线性变换无法处理一些非线性的特征，恰如当年马文明斯基给神经网络判的死刑，只需要加个非线性变换的激活函数就能起死回生。

Attention, FFN, ResNet 缺一不可但却各司其职，我个人的观点（并不一定准确）是，Attention 的功能是做信息的提取和聚合，Resnet 提供信息带宽，而真正学到的知识或者信息都存储在 FFN 中。在图像领域中，也有一种说法，那就是 Attention 其实是 token mixer, FNN 其实是 channel mixer. 论文中对 FNN 的解释是可以看作用 1×1 的卷积核来进行特征的升维和降维，解释的比较浅显。

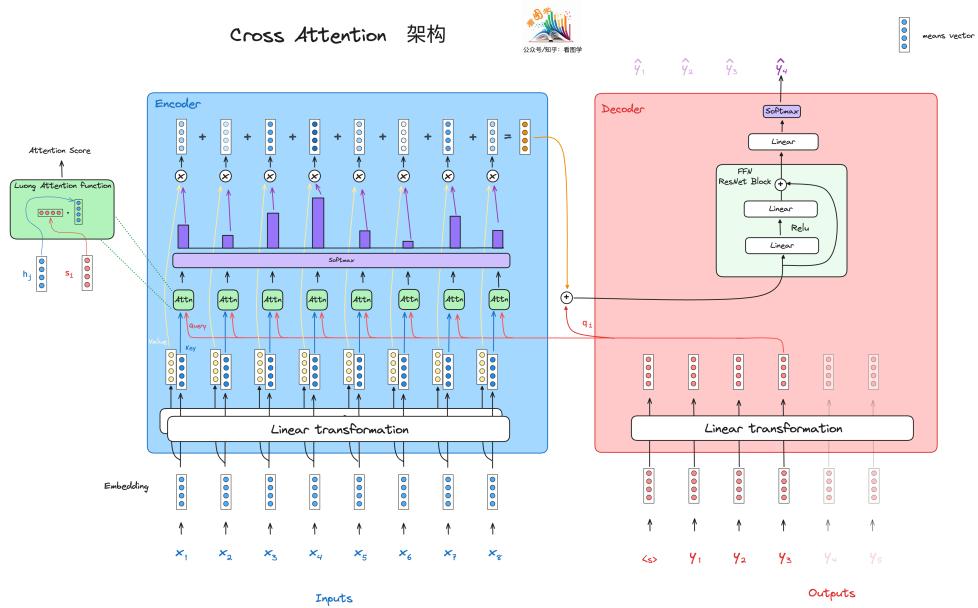
后续虽然有很多 Transformers 架构的魔改，但是真正取得不错的效果且落地的一个例子就是修改 FFN 的 MoE 架构。剩下的两辆马车，ResNet 几乎没法修改了，Attention 则在效率和效果之间寻求平衡。

关于 FFN 的作用后面专门有一章来说明，这里先稍为提一下。

Cross Attention 加上 QKV Attention

如之前论文所述，同一个 hidden state 承担了太多的职责，所以引申出了 query, key 和 value. 在 cross attention 中，decoder 的红线就是 query, key 和 value 则在 Encoder 一侧。我们给 Encoder 上增加 key 和 value。

图画到这里，应该已经可以发现，上图已经是部分 Transformers 了。对应 Transformers 架构中去除 Self Attention 的部分，如下图所示。



TODO: 上面的图中少了一个输出的线性变换。

剩余的部分就是 Encoder 和 Decoder 的 Self-Attention。

Transformers' Scaled Dot-Product Self Attention

在上面的结构中，输入的 Embedding 其实只做了一次线性变换，特征提取能力或者表示学习的能力及其有限。

前文也提到，Self Attention 在表示学习方面遥遥领先，所以 Transformers 自然也想把 Self Attention 加进去。论文从三个维度比较了当时特征提取的主流框架。这三个维度分别为：

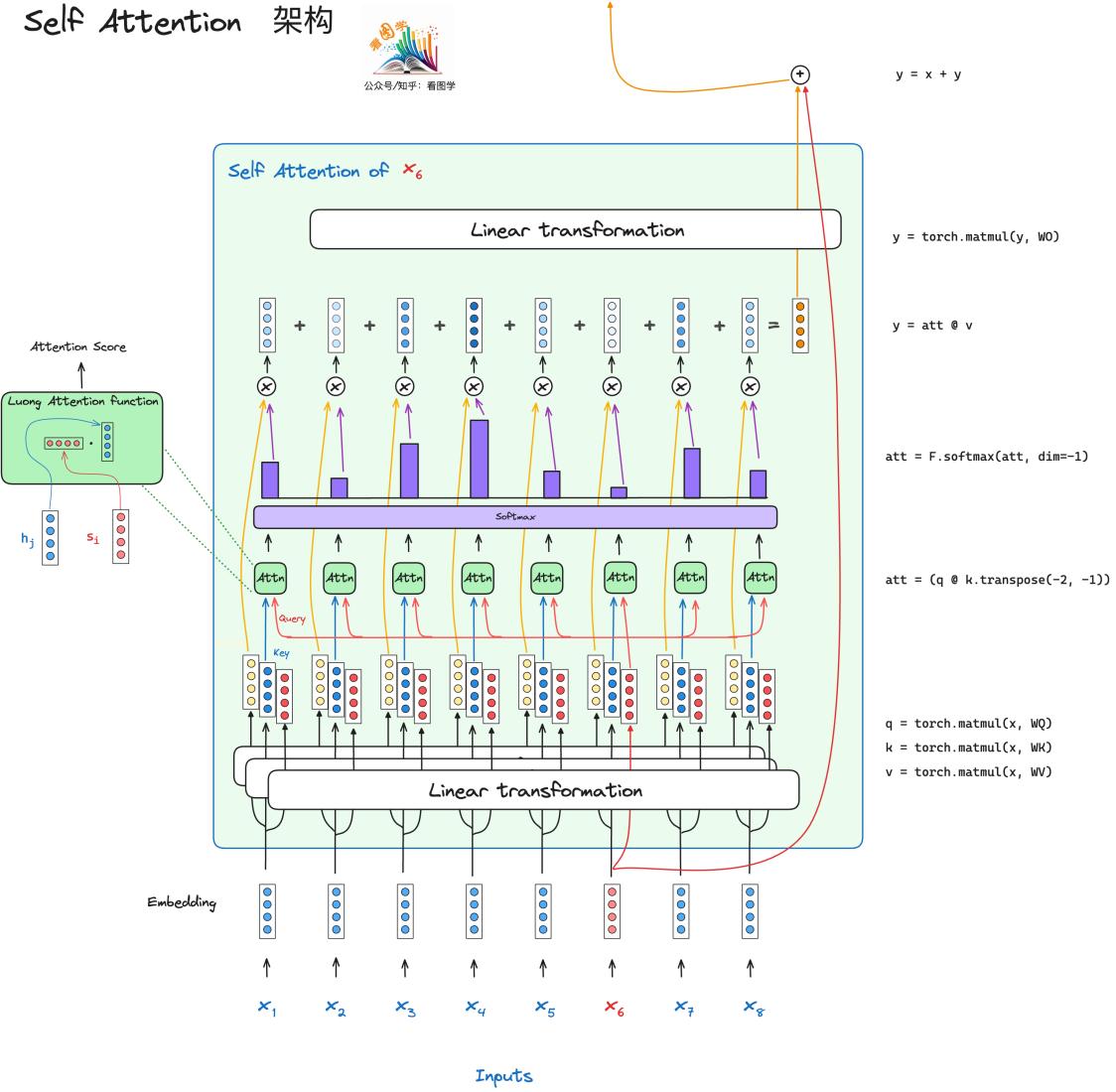
1. 计算的时间复杂度，越小越好。
2. 并行效率。这里用长度为 n 的寻猎计算完成所需要的步数来表示。如果为 1 则表示一步就可以完成，
并行度最高。RNN 则为 n，因为每一个计算都依赖前面的结果，所以需要 n 步才能完成，也就是无法
并行。
3. 序列中任意两个位置信息传递的最短路径。比如 CNN 是 $\log_k n$, self attention 因为每个位置都有链接，
值为 1，而 RNN 最坏情况下，开始位置和结束位置的距离为 n.

Table 1: Maximum path lengths, per-layer complexity and minimum number of sequential operations for different layer types. n is the sequence length, d is the representation dimension, k is the kernel size of convolutions and r the size of the neighborhood in restricted self-attention.

Layer Type	Complexity per Layer	Sequential Operations	Maximum Path Length
Self-Attention	$O(n^2 \cdot d)$	$O(1)$	$O(1)$
Recurrent	$O(n \cdot d^2)$	$O(n)$	$O(n)$
Convolutional	$O(k \cdot n \cdot d^2)$	$O(1)$	$O(\log_k(n))$
Self-Attention (restricted)	$O(r \cdot n \cdot d)$	$O(1)$	$O(n/r)$

从上图上可以看出，Self Attention 的唯一弱点就是计算复杂度是 $O(n^2d)$ ，当序列长度 n 比较大的时候，时间复杂度较高。而大模型时代对长文本的诉求，使这个弱点愈发凸显。目前也有很多方法来解决这个问题，比如滑动窗口，移动平均，甚至还有门机制来降低时间复杂度，这个我们以后再说。

如何构建 Self Attention 呢？Transformers 其实将上面的 Cross Attention 中的 query 改为自身 Embedding 的线性转换即可。大概如下图所示：



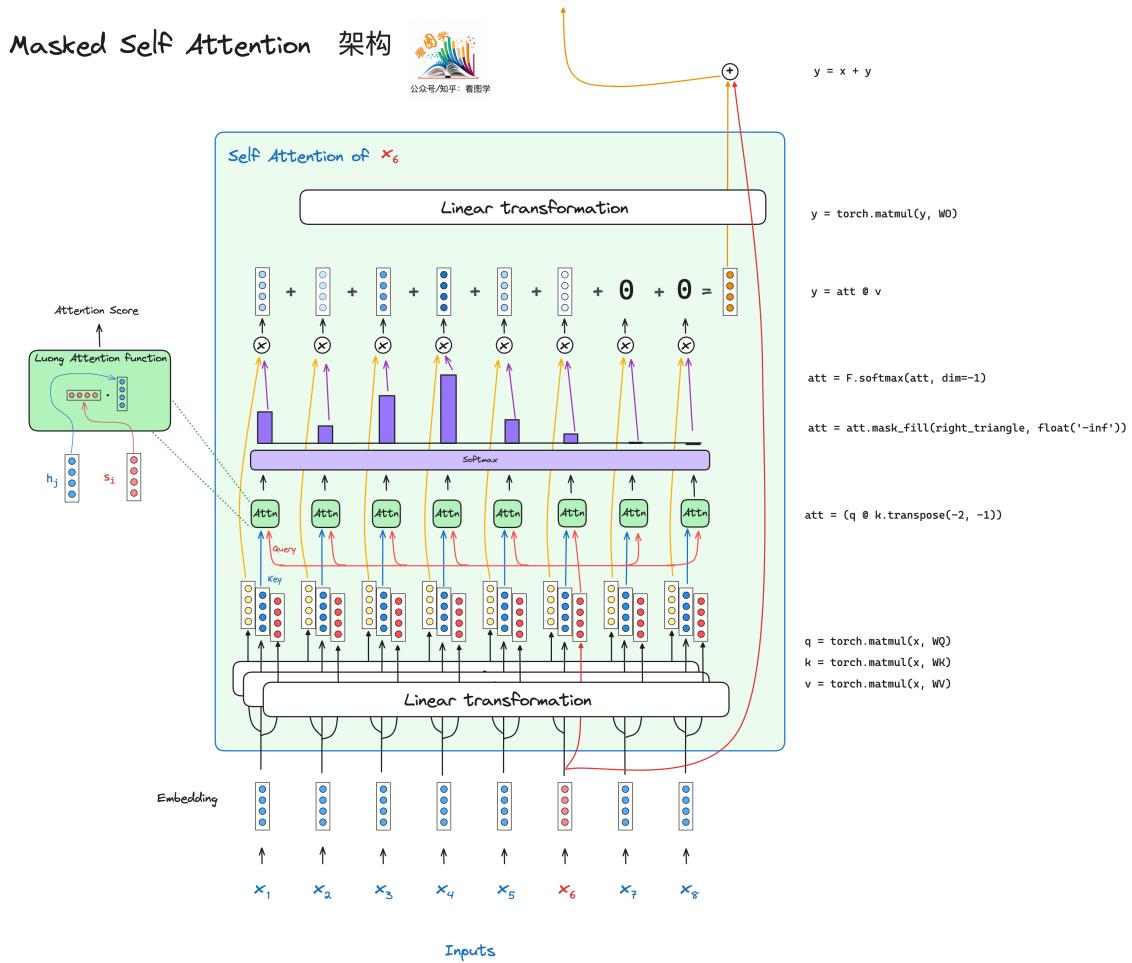
Transformers' Masked Scaled Dot-Product Self Attention

Encoder 部分既然已经加了 Self-Attention，那 Decoder 部分也必须加上。但是 Decoder 和 Encoder 有个很大的不同，那就是 Decoder 的输出，是一个一个往外蹦的。因为目前的建模就是通过前面的信息去预测下一个字。

所以最朴素的训练方法应该是一个长为 n 的预测序列，构造 n 条样本，第一个样本就根据 Encoder 预测第一个字符，最后一条样本则根据 Encoder 和前 $n - 1$ 个字符去预测第 n 个字符。但是这样做的话，训练效率未免有点太低，因为矩阵运算的加速完全用不上了。

怎么解决呢？其实也很简单，算还是照样算，但是算完之后丢弃一些数就完事了，也就是所谓的 mask

机制。在计算完所有的 Attention 后，把理论上无法看到的 Attention 直接变成 0 即可。如下图所示



Transofmers' Encoder

跟 Cross Attention 后添加 FFN 一样，Encoder 模块的 Self Attention 后面也加了 FFN 和 ResNet。所以说 Encoder 虽然只是整体模型的一部分，但是三驾马车都有，所以后来 Bert 几乎就是把 Transformers 的 Encoder 模块直接拿过来用了，在输入和输出的地方做了一点点修改。

Transformers' Decoder

Decoder 部分在之前的基础上也添加了 Self-Attention，但是这一次并没有添加 FFN。理论上增加会更好，(废话，参数变多了)，但是目前也有些研究证明，无论是 Encoder 和 Decoder 中的 FFN 模块已经有些冗余⁵。

当前的架构可以将 Cross Attention 和 Masked Cross Attention 是一个级联的 Attention，有点类似做了个二次索引。通过二次索引 Attend 到输入序列和输出序列的所有信息。

⁵One Wide Feedforward Is All You Need.

Attention 的矩阵表示

上面画的图展示的都是单个输入的计算流程。这些图也比较清晰的表明，在训练阶段，Encoder 和 Decoder 每个输入的计算流程都是一样的，所以很容易转化成矩阵的运算。

如下图所示。TODO

FFN 的作用

首先大家先猜一下整个 Transformers 中 FFN 的参数占比是多少？答案是 $2/3$ ，你猜对了么？

关于 FFN 的作用，后续研究人员做了很多实验和研究。但是直到目前也不能说就研究清楚了，因为神经网络的解释性本来就差。一个新技术的应用往往要比理论提前好久，比如 GBDT 等 ensemble 模型非常好用，但是很多年以后才用 Margin 的理论研究明白。

这里将一些 FFN 研究的成果做一个小汇总，只列举了目前大家都比较公认的结果。

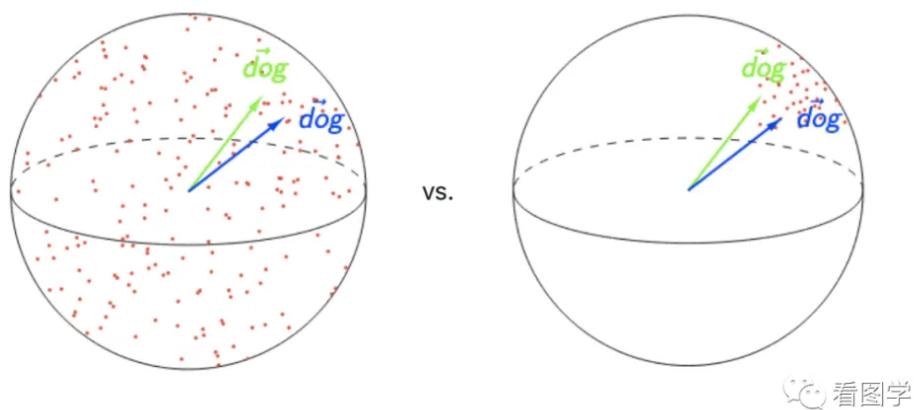
1. FFN/ResNet 是 Transformers 的必备模块

没有 FFN（或者 ResNet）的 Transformers 学不到什么东西。

《Attention is Not All You Need: Pure Attention Loses Rank Doubly Exponentially with Depth》这篇论文，提出了 Transformers 架构存在 token uniformity 的归纳偏置 (inductive bias，有时候也叫归纳偏好) 问题。如果去掉 FFN 或者 Resnet，则问题更加严重。

这里解释一下这两个名词，所谓归纳偏置，可以通俗的理解为模型的“个性”，就是满足训练集合的解法有无数种，但是不同的模型架构会让模型更偏向于某些解法。比如我们常用的一些正则化方法，其实就是在让模型的归纳偏置倾向于选择一些简单的解法。任何模型都有归纳偏置，尤其是碰到未见过的样本的时候，模型的归纳偏置就更容易体现出来。Transformers 的一个归纳偏执是什么呢？就是 token uniformity，有时候也叫 information diffusion，或者 anisotropic (各向异性)，也就是说训练完后的 token 会共享很多相似信息。

看下图大概就知道了，我们期望表示 token 的向量，相似的要相近，不相似的要远，而且最好是均匀的分布在空间中，比如下图所示。但是 Transformers 会存在各向异性的问题，也就是所有的 token 都挤到一个很窄的锥形区域了。



回到论文，论文将 FFN 和 ResNet 去掉之后做了一些消融实验，证明了 FFN 和 ResNet 是 Transformers 中的必备组件，这两个可以大大的缓解 token uniformity 或者各向异性的问题。

论文中从数学上证明了经过 Attention 变换后的输出与 rank-1 的矩阵之间的差值存在上界，但是有点复杂，我也没仔细推导过。简单一点的理解呢，就是 Attention 本质上是 value 的线性变换（虽然线性变换的权重是非线性的 softmax）。Every self-attention “layer” is a linear transformation of the previous layer (with non-linear weights)

当然并不是说 Transformers 就已经将 token uniformity 问题解决了，这个问题依然存在，所以后续又有 Bert-flow、whitening 等改进。详细可以参考：Bert 中的词向量各向异性具体什么意思啊？- 看图学的回答 - 知乎 <https://www.zhihu.com/question/460991118/answer/2353153090>

2. FFN 承担了记忆功能

这一节讲的两篇论文都非常有意思，建议大家看一看原始论文。

《Transformer Feed-Forward Layers Are Key-Value Memories》这篇文章做了很多实验和统计，得出了以下结论：

- (a) FFN 是一个 Key-Value 记忆网络，第一层线性变换是 Key Memory，第二层线性变换是 Value Memory。
- (b) FFN 学到的记忆有一定的可解释性，比如低层的 Key 记住了一些通用 pattern (比如以某某结尾)，而高层的 Key 则记住了一些语义上的 Pattern (比如句子的分类)。
- (c) Value Memory 根据 Key Memory 记住的 Pattern，来预测输出词的分布。
- (d) skip connection 将每层 FFN 的结果进行细化。

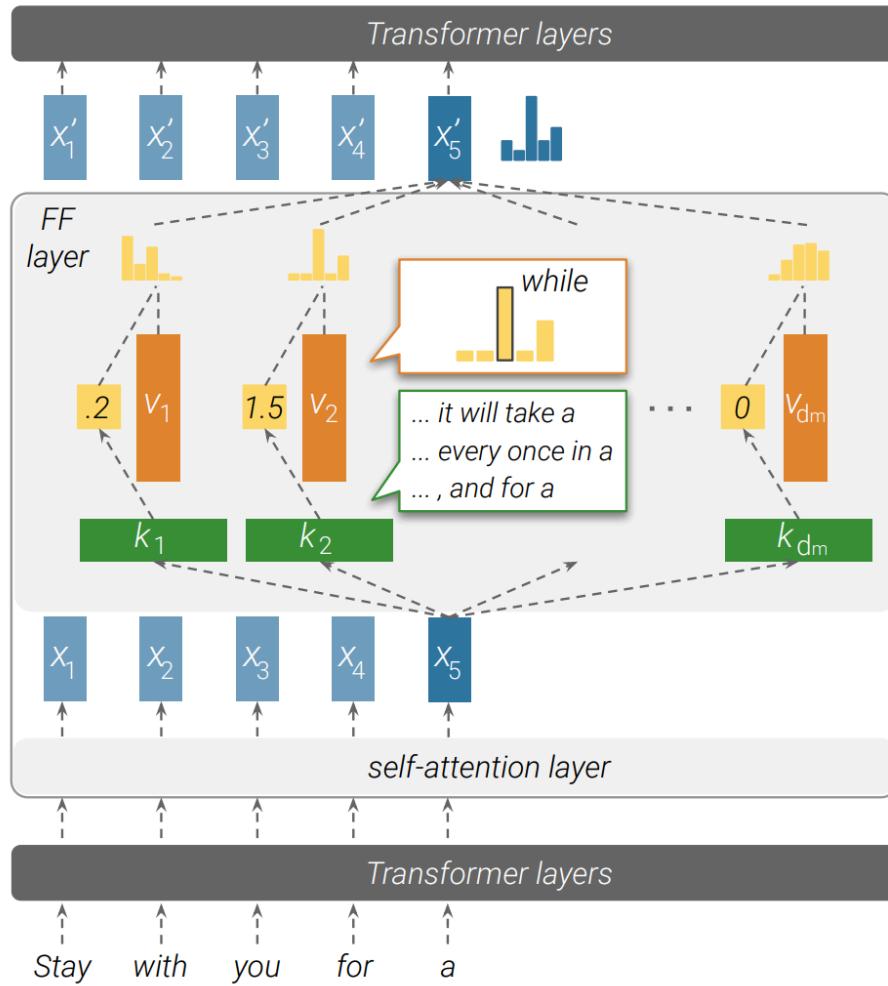
2015 年，《End-To-End Memory Networks》这篇论文提出了 Key-Value Memory 的结构，对于一个输入 x ，其网络结构为

$$\text{MemoryNet}(x) = \text{softmax}(x \cdot K^\top)V$$

FFN 的公式为，

$$\text{FFN}(x) = f(x \cdot W_1)W_2 = f(x \cdot K^\top)V$$

这里 f 是 ReLU 激活函数，可以看出两个结构的唯一区别就是一个是才用 softmax 进行归一化，另一个则采用 ReLU 进行筛选。本质上都差不多。



通过一些实验也确实证明了上面结论，也就是 FFN 确实将一些 pattern 或者知识记忆和存储起来了。这就很有意思，从这个角度来说，Attention 是对短期的信息进行提取，而 FFN 则对整个训练样本进行信息提取和记忆。这也就能解释为什么一个有限的窗口甚至对语料进行了暴力截断，模型也能记住语料库中的信息。

《Knowledge Neurons in Pretrained Transformers》这一篇就更有意思，在上一篇的基础上，对 Transformers 进行了前额叶切除手术。擎天柱瑟瑟发抖。

研究人员先是定位到对某些事实或者知识影响较大的神经元，然后神经元内的数值进行增强或者抑制，发现 Transformers 对这些事实或者知识的回答效果也会变好或者变差。如果将这个神经元删掉，也就是值全部置 0，则 Transformers 完全忘记了这些知识，更神奇的是，对于其他的知识则影响不大。

更进一步的，研究人员还对神经元的内容进行了替换操作以达到“篡改记忆”的效果。当然作者只是在 BERT 上进行了实验，随着预料和模型的增大，像定位知识的记忆也愈发的困难，但是给了人们一个可控文本生成的研究方向，未来可期。

3. FFN 是一种混合专家模型

MoEification: Transformer Feed-forward Layers are Mixtures of Experts

这是刘知远团队的论文，其实一直以来，神经网络就存在稀疏激活的现象，也就是在推理的时候，其实只有极小一部分参数参与了计算。这篇论文则通过 MoE 的思想来将 FFN 层拆分成了多个专家，并且新增了一个路由模块来确定推理的时候来挂哪个专家的门诊：）

这么做完之后，在提升推理速度的同时，效果依然能保持原来的 95% 以上。挺有价值的工作，大模型上也可以这么做一把。

下一步写什么

到目前为止，可以说刚刚把 Transformers 的架构写完。里面还有很多小细节，比如 scaled, label smoothing, 输入的一些处理等，这一些小细节准备专门写一章 Transformers 的面试题。再一个就是 Transformers 后续的发展。

Position Embedding

从 Luong Attention 与 Bahdanau Attention 演变为 Transformers 的 Scaled Dot-Product Attention 后，出现了一个问题，那就是 token 的位置信息丢失了。

基于传统的 RNN 结构的 Attention 由于时刻 t 的隐层计算依赖时刻 $t - 1$ 的隐层，所以位置信息理论上是可以传递的。

Transformers 的 Attention 丢弃了 RNN 的结构之后，带来的好处就是可以并行计算了，但是信息通过时间/位置的传递的特性也就丢失了。

然而位置信息又很重要。

比如曾国藩写周报，如果写“臣屡战屡败”，结果可能是拖出去斩首。如果写“臣屡败屡战”，结果可能是忠勇无双有赏赐。

研究人员自然是想既要有要，所以就想办法从别的地方把位置信息加进去。我们来研究下 Position Embedding 的发展史。

朴素的想法

一个很直接的方法，就是直接把位置输入进去。这样做有两个缺点：

1. 泛化不好，没见过的位置模型处理不好
2. 这样模型的权重存在很大的数字，神经网络不喜欢大数字，影响训练的稳定性。

那如果是将位置做个归一化呢？也很难，因为无法找到一个归一化的标准。

绝对位置编码 (sinusoidal PE)

在《Attention is All you Need》的论文中，单独设置了一个绝对位置编码，叫 sinusoidal 位置编码，这个编码会和输入的词向量相加。文中的编码函数如下：

$$PE_{(t,2i)} = \sin\left(\frac{t}{10000^{2i/d}}\right)$$

$$PE_{(t,2i+1)} = \cos\left(\frac{t}{10000^{2i/d}}\right)$$

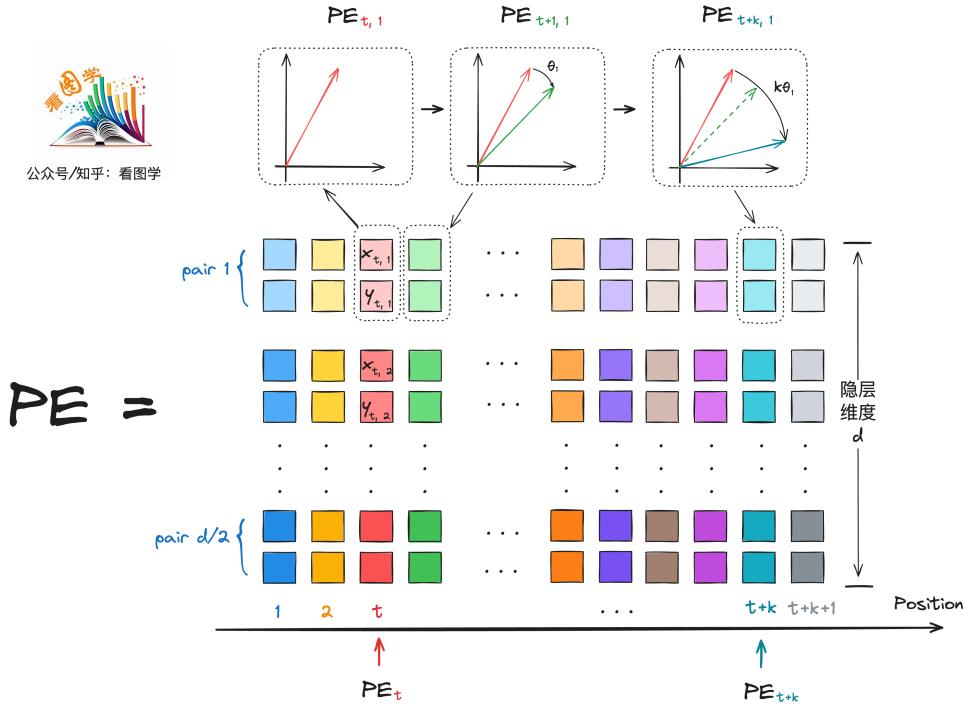
其中 t 代表了输入的位置。原文用了 pos 来表示，为了后续推导公式的方便，将 pos 统一改写为 t 。

i 则是 Position Embedding 的向量下标，向量长度为 d , i 的取值范围是 $[0, \frac{d}{2}]$

这个函数看起来奇怪又有些恐怖，到底是什么鬼？

我们先看下结论：用图示来解释一下这个函数到底有什么特性。

Sinusoidal 绝对位置编码中，分组后，相对位置之间的线性变换等价于【顺时针旋转】



通俗一点来说，这个函数就是根据向量的下标两两配对，分成多组，每一组的二维向量根据 **位置信息** 进行 **顺时针旋转**，旋转的角度跟相对位置是线性关系。

论文中对这个函数进行了解释：“We chose this function because we hypothesized it would allow the model to easily learn to attend by relative positions, since for any fixed offset k , $PE_{(pos+k)}$ can be represented as a linear function of PE_{pos} .

用学术一点的说法，就是该函数是相对位置 k 的一个线性变换，也就是符合这么一个特性：

$$PE_{t+k} = f(PE_t, k)$$

其中， f 在这里是进行了顺时针旋转，旋转的角度是相对位置 k 的线性函数。

1. 下面是详细的证明：

为了方便，我们把原函数进行一些简化。原函数为：

$$PE_{(t,2i)} = \sin\left(\frac{t}{10000^{2i/d}}\right)$$

$$PE_{(t,2i+1)} = \cos\left(\frac{t}{10000^{2i/d}}\right)$$

由于函数对向量进行了两两分组，我们用 j 来表示分组 $PE_{(t,2i)}, PE_{(2i+1)}$ ，则有

$$PE(t, j) = \begin{cases} \sin(\theta_j \cdot t), & \text{if } j = 2i/2 \\ \cos(\theta_j \cdot t), & \text{if } j = (2i+1)/2 \end{cases}$$

其中

$$\theta_j = \frac{1}{10000j/d}$$

, 则 Position Embedding 则可以表示为:

$$PE_t = \begin{bmatrix} \sin(\theta_1 \cdot t) \\ \cos(\theta_1 \cdot t) \\ \sin(\theta_2 \cdot t) \\ \cos(\theta_2 \cdot t) \\ \vdots \\ \sin(\theta_{d/2} \cdot t) \\ \cos(\theta_{d/2} \cdot t) \end{bmatrix}_{d \times 1}$$

对于第 j 个 pair $PE_{t,j}$ 来说, 如果 $PE_{t+k,j}$ 是 $PE_{t,j}$ 的线性变换, 则存在一个矩阵 $M \in \mathbb{R}^{2 \times 2}$ 使得:

$$M \cdot PE_{t,j} = PE_{t+k,j}$$

也就是

$$\begin{bmatrix} u_1 & v_1 \\ u_2 & v_2 \end{bmatrix} \cdot \begin{bmatrix} \sin(\theta_j \cdot t) \\ \cos(\theta_j \cdot t) \end{bmatrix} = \begin{bmatrix} \sin(\theta_j \cdot (t+k)) \\ \cos(\theta_j \cdot (t+k)) \end{bmatrix}$$

根据三角函数求和的公式:

$$\sin(\alpha + \beta) = \sin \alpha \cos \beta + \cos \alpha \sin \beta$$

$$\cos(\alpha + \beta) = \cos \alpha \cos \beta - \sin \alpha \sin \beta$$

将右侧展开, 左侧根据矩阵乘法展开, 则有

$$\begin{aligned} \begin{bmatrix} u_1 \times \sin(\theta_j \cdot t) + v_1 \times \cos(\theta_j \cdot t) \\ u_2 \times \sin(\theta_j \cdot t) + v_2 \times \cos(\theta_j \cdot t) \end{bmatrix} &= \begin{bmatrix} \sin(\theta_j \cdot t) \cos(\theta_j \cdot k) + \cos(\theta_j \cdot t) \sin(\theta_j \cdot k) \\ \cos(\theta_j \cdot t) \cos(\theta_j \cdot k) - \sin(\theta_j \cdot t) \sin(\theta_j \cdot k) \end{bmatrix} \\ &= \begin{bmatrix} \sin(\theta_j \cdot t) \cos(\theta_j \cdot k) + \cos(\theta_j \cdot t) \sin(\theta_j \cdot k) \\ -\sin(\theta_j \cdot t) \sin(\theta_j \cdot k) + \cos(\theta_j \cdot t) \cos(\theta_j \cdot k) \end{bmatrix} \end{aligned}$$

解这个方程会得到 (根据上面公式对号入座就可以):

$$M = \begin{bmatrix} u_1 & v_1 \\ u_2 & v_2 \end{bmatrix} = \begin{bmatrix} \cos(\theta_j \cdot k) & \sin(\theta_j \cdot k) \\ -\sin(\theta_j \cdot k) & \cos(\theta_j \cdot k) \end{bmatrix}$$

学过线代的看着这个矩阵是不是有点眼熟？没错，这个矩阵和逆时针旋转矩阵

$$\begin{bmatrix} \cos(\theta_j.k) & -\sin(\theta_j.k) \\ \sin(\theta_j.k) & \cos(\theta_j.k) \end{bmatrix}$$

非常像。

这两个矩阵什么联系呢？其实也很简单，上面的是顺时针旋转矩阵，下面的是逆时针旋转矩阵。

比如我顺时针旋转了 θ ，就相当于逆时针旋转了 $-\theta$ ，带入逆时针旋转矩阵有：

$$R(-\theta) = \begin{bmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{bmatrix} = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}$$

所以，我们就知道了这个论文中提到的线性变换 $PE_{t+k} = f(PE_t, k)$ 就是顺时针旋转，旋转的角度为 $\theta_j.k$ ，和相对位置 k 是线性关系。

对于所有 pair 来说， PE_{t+k} 相对于 PE_t 的顺时针旋转，写成矩阵形式为：

$$\begin{bmatrix} \cos(\theta_1.k) & \sin(\theta_1.k) & 0 & 0 & \cdots & 0 & 0 & \sin(\theta_1.t) \\ -\sin(\theta_1.k) & \cos(\theta_1.k) & 0 & 0 & \cdots & 0 & 0 & \cos(\theta_1.t) \\ 0 & 0 & \cos(\theta_2.k) & \sin(\theta_2.k) & \cdots & 0 & 0 & \sin(\theta_2.t) \\ 0 & 0 & -\sin(\theta_2.k) & \cos(\theta_2.k) & \cdots & 0 & 0 & \cos(\theta_2.t) \\ 0 & 0 & 0 & 0 & \ddots & 0 & 0 & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \cos(\theta_{d/2}.k) & \sin(\theta_{d/2}.k) & \sin(\theta_{d/2}.t) \\ 0 & 0 & 0 & 0 & \cdots & -\sin(\theta_{d/2}.k) & \cos(\theta_{d/2}.k) & \cos(\theta_{d/2}.t) \end{bmatrix}$$

不得不说这个设计还是很精彩的，虽然还是写死的绝对位置编码，但是却巧妙的捕捉到了相对位置关系。

下面是一些疑问和思考：

- 为什么要分组？不分组然后向量整体旋转行不行？理论上也可以，但是这样做的话上面的矩阵就变成了一个稠密矩阵，影响运算速度。
- 为什么随着下标的增加，旋转的角度越来越小？这个我也没有很严谨的证明过，感觉跟时钟系统有点像吧，时针分针秒针分别表示不同粒度的时间，在钟表上顺时针旋转。这里既然也是旋转，那用不同的颗粒度应该能捕获更细粒度的位置信息。

需要注意的是，《Attention is All your Need》中，词向量和绝对位置向量采用的是相加的操作，然后再进行线性变换和 Attention 操作。具体来说就是：

$$\begin{aligned}\mathbf{q}_i &= (\mathbf{x}_i + \mathbf{p}_i) \mathbf{W}_Q \\ \mathbf{k}_j &= (\mathbf{x}_j + \mathbf{p}_j) \mathbf{W}_K \\ \mathbf{v}_j &= (\mathbf{x}_j + \mathbf{p}_j) \mathbf{W}_V \\ a_{i,j} &= \text{softmax}(\mathbf{q}_i \mathbf{k}_j^\top) \\ \mathbf{o}_i &= \sum_j a_{i,j} \mathbf{v}_j\end{aligned}$$

比如将 $\mathbf{q}_i \mathbf{k}_j^\top$ 完全展开后

$$\mathbf{q}_i \mathbf{k}_j^\top = \mathbf{x}_i \mathbf{W}_Q \mathbf{W}_K^\top \mathbf{x}_j^\top + \mathbf{x}_i \mathbf{W}_Q \mathbf{W}_K^\top \mathbf{p}_j^\top + \mathbf{p}_i \mathbf{W}_Q \mathbf{W}_K^\top \mathbf{x}_j^\top + \mathbf{p}_i \mathbf{W}_Q \mathbf{W}_K^\top \mathbf{p}_j^\top$$

上面有颜色的部分代表了位置编码，有的将其变成可训练的参数，有的甚至把中间两项都去掉了。总之，后续的 Position Embedding 很多进展都是在 x_i, p_i 还有他们之间的组合关系上做文章。

苏剑林对 sinusoidal 绝对位置编码进行了改造，提出了一种更优雅和兼具外推性的编码方式，就是旋转位置编码 (RoPE).

旋转位置编码 (RoPE)

绝对位置编码采用的是词向量与 PE 相加，然后再做线性变换的方式。公式如下：

$$\mathbf{q}_t = (\mathbf{x}_t + \mathbf{p}_t) \mathbf{W}_Q$$

而 RoPE 则更简单直接，丢弃了绝对位置编码 PE，词向量做线性变换后，按照前面说的 PE 分组方式，直接进行旋转。

这个论文已经画的十分清楚了：

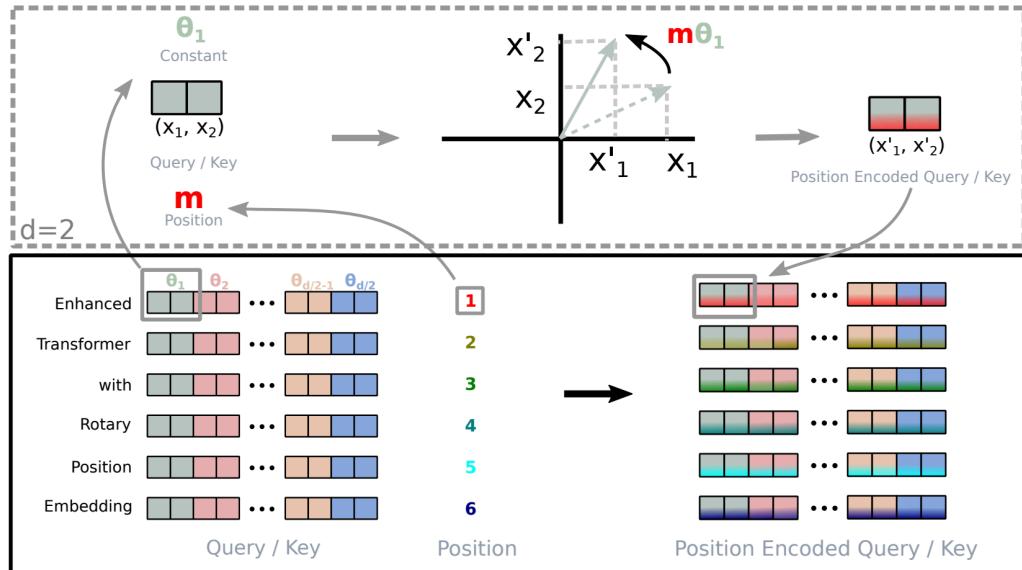


Figure 1: Implementation of Rotary Position Embedding(RoPE).

下面是详细的公式推导，去掉复数领域，只考虑旋转矩阵的一些证明。

假设 $\mathbf{q}_t = \mathbf{x}_t \mathbf{W}_Q$, 仿照绝对位置编码进行两两分组, 则

$$q_t = \begin{bmatrix} q_{t,1}^{(1)} \\ q_{t,1}^{(2)} \\ q_{t,2}^{(1)} \\ q_{t,2}^{(2)} \\ \vdots \\ q_{t,d/2}^{(1)} \\ q_{t,d/2}^{(2)} \end{bmatrix}_{d \times 1}$$

对于一个分组 $q_{t,j}$ 来说, 旋转后的 $RoPE(q_{t,j})$ 为:

$$RoPE(q_{t,j}) = R(\theta_j \cdot t)(q_{t,j}) = \begin{bmatrix} \cos(\theta_j \cdot t) & -\sin(\theta_j \cdot t) \\ \sin(\theta_j \cdot t) & \cos(\theta_j \cdot t) \end{bmatrix} \begin{bmatrix} q_{t,j}^{(1)} \\ q_{t,j}^{(2)} \end{bmatrix}$$

写成矩阵形式为:

$$RoPE(q_t) = R(\theta \cdot t)(q_t) = \begin{bmatrix} \cos(\theta_1 \cdot t) & -\sin(\theta_1 \cdot t) & 0 & 0 & \cdots & 0 & 0 \\ \sin(\theta_1 \cdot t) & \cos(\theta_1 \cdot t) & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cos(\theta_2 \cdot t) & -\sin(\theta_2 \cdot t) & \cdots & 0 & 0 \\ 0 & 0 & \sin(\theta_2 \cdot t) & \cos(\theta_2 \cdot t) & \cdots & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & \cos(\theta_{d/2} \cdot t) & -\sin(\theta_{d/2} \cdot t) \\ 0 & 0 & 0 & 0 & \cdots & \sin(\theta_{d/2} \cdot t) & \cos(\theta_{d/2} \cdot t) \end{bmatrix} \begin{bmatrix} q_{t,1}^{(1)} \\ q_{t,1}^{(2)} \\ q_{t,2}^{(1)} \\ q_{t,2}^{(2)} \\ \vdots \\ q_{t,d/2}^{(1)} \\ q_{t,d/2}^{(2)} \end{bmatrix}$$

RoPE 这么做的好处是, 当 q 和 k 进行 attention 操作后, 依然可以保留相对位置, 这样就很好的完成了位置编码的任务, 而且旋转位置编码就像时钟一样可以无限的旋转, 具备很好的外推性。

$$RoPE(q_{m,j}), RoPE(k_{n,j}) = RoPE(q_{m-n,j}), RoPE(k_{0,j})$$

证明如下:

假设位置 m 的 pair $q_{m,j}$ 和位置 n 的 pair $k_{n,j}$ 取点积操作计算 attention, 则有:

$$\begin{aligned}
RoPE(q_{m,j}), RoPE(k_{n,j}) &= \begin{bmatrix} \cos(\theta_j.m) & -\sin(\theta_j.m) \\ \sin(\theta_j.m) & \cos(\theta_j.m) \end{bmatrix} \begin{bmatrix} q_{m,j}^{(1)} \\ q_{m,j}^{(2)} \end{bmatrix}, \begin{bmatrix} \cos(\theta_j.n) & -\sin(\theta_j.n) \\ \sin(\theta_j.n) & \cos(\theta_j.n) \end{bmatrix} \begin{bmatrix} k_{n,j}^{(1)} \\ k_{n,j}^{(2)} \end{bmatrix} \\
&= \begin{bmatrix} q_{m,j}^{(1)} \cos(\theta_j.m) - q_{m,j}^{(2)} \sin(\theta_j.m) \\ q_{m,j}^{(1)} \sin(\theta_j.m) + q_{m,j}^{(2)} \cos(\theta_j.m) \end{bmatrix}, \begin{bmatrix} k_{n,j}^{(1)} \cos(\theta_j.n) - k_{n,j}^{(2)} \sin(\theta_j.n) \\ k_{n,j}^{(1)} \sin(\theta_j.n) + k_{n,j}^{(2)} \cos(\theta_j.n) \end{bmatrix} \\
&= (q_{m,j}^{(1)} \cos(\theta_j.m) - q_{m,j}^{(2)} \sin(\theta_j.m)) \times (k_{n,j}^{(1)} \cos(\theta_j.n) - k_{n,j}^{(2)} \sin(\theta_j.n)) \\
&\quad + (q_{m,j}^{(1)} \sin(\theta_j.m) + q_{m,j}^{(2)} \cos(\theta_j.m)) \times (k_{n,j}^{(1)} \sin(\theta_j.n) + k_{n,j}^{(2)} \cos(\theta_j.n)) \\
&= q_{m,j}^{(1)} k_{n,j}^{(1)} (\cos(\theta_j.m) \cos(\theta_j.n) + \sin(\theta_j.m) \sin(\theta_j.n)) \\
&\quad + q_{m,j}^{(1)} k_{n,j}^{(2)} (-\cos(\theta_j.m) \sin(\theta_j.n) + \sin(\theta_j.m) \cos(\theta_j.n)) \\
&\quad + q_{m,j}^{(2)} k_{n,j}^{(1)} (-\sin(\theta_j.m) \cos(\theta_j.n) + \cos(\theta_j.m) \sin(\theta_j.n)) \\
&\quad + q_{m,j}^{(2)} k_{n,j}^{(2)} (\sin(\theta_j.m) \sin(\theta_j.n) + \cos(\theta_j.m) \cos(\theta_j.n)) \\
&= q_{m,j}^{(1)} k_{n,j}^{(1)} \cos(\theta_j.(m-n)) + q_{m,j}^{(1)} k_{n,j}^{(2)} \sin(\theta_j.(m-n)) \\
&\quad + q_{m,j}^{(2)} k_{n,j}^{(1)} \sin(\theta_j.(m-n)) + q_{m,j}^{(2)} k_{n,j}^{(2)} \sin(\theta_j.(m-n)) \\
&= (q_{m,j}^{(1)} \cos(\theta_j.(m-n)) - q_{m,j}^{(2)} \sin(\theta_j.(m-n))) \times k_{n,j}^{(1)} \\
&\quad + (q_{m,j}^{(1)} \sin(\theta_j.(m-n)) + q_{m,j}^{(2)} \sin(\theta_j.(m-n))) \times k_{n,j}^{(2)} \\
&= RoPE(q_{m-n,j}), RoPE(k_{0,j})
\end{aligned}$$

其他编码方式

目前主流就是 RoPE，其他的方式后面慢慢更新。

Chapter 3: 大语言模型 pipeline

Stage 1: Pretrain

Continue Pretrain

Stage 2: SFT

- SFT 是否必须存在

Stage 3: Alginment

Stage 0: 数据处理

Chapter 4: 大语言模型训练

显卡和模型训练基础知识

多卡并行训练

当前流行训练框架

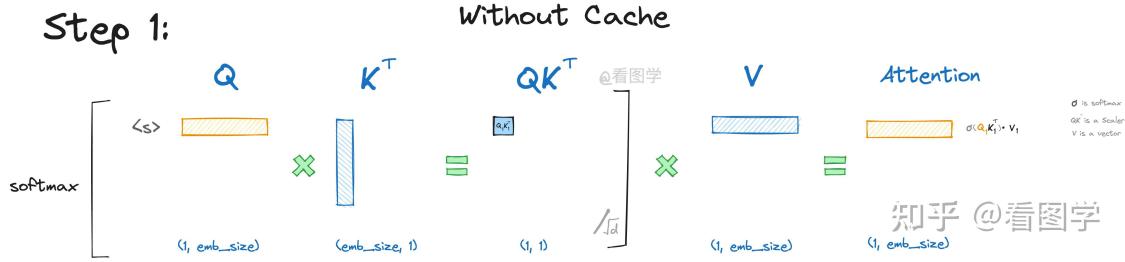
Chapter 5: 大语言模型推理

KV Cache

KV Cache 是 Transformer 标配的推理加速功能，transformer 官方 use_cache 这个参数默认是 True，但是它只能用于 Decoder 架构的模型，这是因为 Decoder 有 Causal Mask，在推理的时候前面已经生成的字符不需要与后面的字符产生 attention，从而使得前面已经计算的 K 和 V 可以缓存起来。

我们先看一下不使用 KV Cache 的推理过程。假设模型最终生成了“遥遥领先”4 个字。

当模型生成第一个“遥”字时，input=“<s>”，“<s>”是起始字符。Attention 的计算如下：

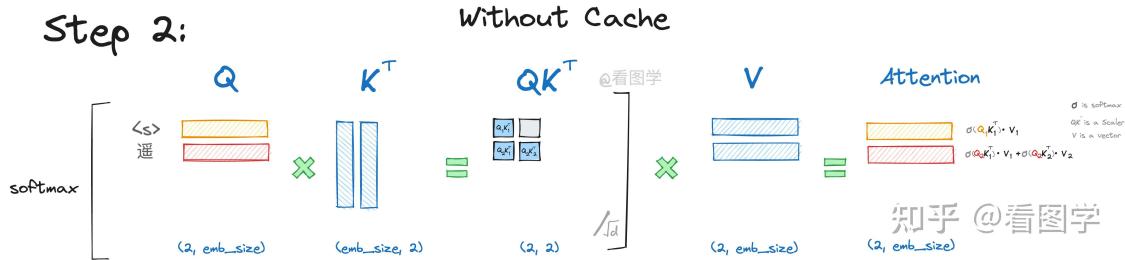


为了看上去方便，我们暂时忽略 scale 项 \sqrt{d} ，但是要注意这个 scale 面试时经常考。

如上图所示，最终 Attention 的计算公式如下，(softmaxed 表示已经按行进行了 softmax)：

$$Att_1(Q, K, V) = \text{softmax}(Q_1 K_1^T) \vec{V}_1 = \text{softmaxed}(Q_1 K_1^T) \vec{V}_1$$

当模型生成第二个“遥”字时，input=“<s> 遥”Attention 的计算如下：



当 QK^T 变为矩阵时，softmax 会针对 行进行计算。写详细一点如下，softmaxed 表示已经按行进行了 softmax。

$$\begin{aligned}
 Att_{step2}(Q, K, V) &= \text{softmax} \left(\begin{bmatrix} Q_1 K_1^T & -\infty \\ Q_2 K_1^T & Q_2 K_2^T \end{bmatrix} \right) \begin{bmatrix} \vec{V}_1 \\ \vec{V}_2 \end{bmatrix} \\
 &= \left(\begin{bmatrix} \text{softmax}(Q_1 K_1^T) & \text{softmax}(-\infty) \\ \text{softmax}(Q_2 K_1^T) & \text{softmax}(Q_2 K_2^T) \end{bmatrix} \right) \begin{bmatrix} \vec{V}_1 \\ \vec{V}_2 \end{bmatrix} \\
 &\stackrel{\$\$}{=} \left(\begin{bmatrix} \text{softmax}(Q_1 K_1^T) & 0 \\ \text{softmax}(Q_2 K_1^T) & \text{softmax}(Q_2 K_2^T) \end{bmatrix} \right) \begin{bmatrix} \vec{V}_1 \\ \vec{V}_2 \end{bmatrix} \\
 &= \left(\begin{bmatrix} \text{softmax}(Q_1 K_1^T) \times \vec{V}_1 + 0 \times \vec{V}_2 \\ \text{softmax}(Q_2 K_1^T) \times \vec{V}_1 + \text{softmax}(Q_2 K_2^T) \times \vec{V}_2 \end{bmatrix} \right) \\
 &= \left(\begin{bmatrix} \text{softmax}(Q_1 K_1^T) \times \vec{V}_1 \\ \text{softmax}(Q_2 K_1^T) \times \vec{V}_1 + \text{softmax}(Q_2 K_2^T) \times \vec{V}_2 \end{bmatrix} \right)
 \end{aligned}$$

假设 $\text{Att}_1(Q, K, V)$ 表示 Attention 的第一行， $\text{Att}_2(Q, K, V)$ 表示 Attention 的第二行，则根据上面推导，

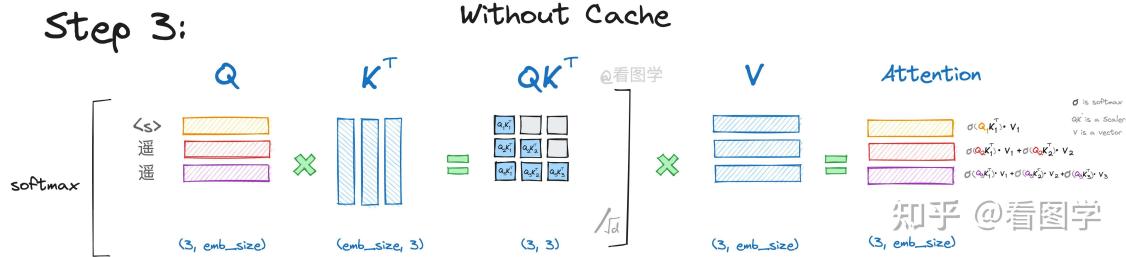
其计算公式为：

$$\begin{aligned} \text{Att}_1(Q, K, V) &= \text{softmax}(Q_1 K_1^T) \vec{V}_1 \\ \text{Att}_2(Q, K, V) &= \text{softmax}(Q_2 K_1^T) \vec{V}_1 + \text{softmax}(Q_2 K_2^T) \vec{V}_2 \end{aligned}$$

你会发现，由于 $Q_1 K_2^T$ 这个值会 mask 掉

- Q_1 在第二步参与的计算与第一步是一样的，而且第二步生成的 V_1 也仅仅依赖于 Q_1 ，与 Q_2 毫无关系。
- V_2 的计算也仅仅依赖于 Q_2 ，与 Q_1 毫无关系。

当模型生成第三个“领”字时，input="<s> 遥遥" Attention 的计算如下：

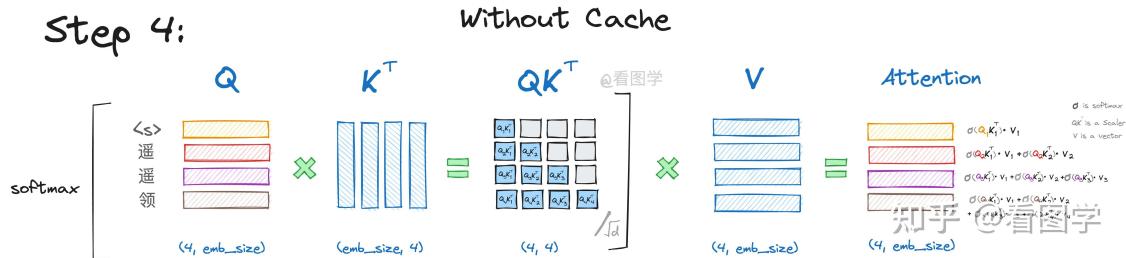


详细的推导参考第二步，其计算公式为：

$$\begin{aligned} \text{Att}_1(Q, K, V) &= \text{softmax}(Q_1 K_1^T) \vec{V}_1 \\ \text{Att}_2(Q, K, V) &= \text{softmax}(Q_2 K_1^T) \vec{V}_1 + \text{softmax}(Q_2 K_2^T) \vec{V}_2 \\ \text{Att}_3(Q, K, V) &= \text{softmax}(Q_3 K_1^T) \vec{V}_1 + \text{softmax}(Q_3 K_2^T) \vec{V}_2 + \text{softmax}(Q_3 K_3^T) \vec{V}_3 \end{aligned}$$

同样的， Att_k 只与 Q_k 有关。

当模型生成第四个“先”字时，input="<s> 遥遥领" Attention 的计算如下：



$$\begin{aligned} \text{Att}_1(Q, K, V) &= \text{softmax}(Q_1 K_1^T) \vec{V}_1 \\ \text{Att}_2(Q, K, V) &= \text{softmax}(Q_2 K_1^T) \vec{V}_1 + \text{softmax}(Q_2 K_2^T) \vec{V}_2 \\ \text{Att}_3(Q, K, V) &= \text{softmax}(Q_3 K_1^T) \vec{V}_1 + \text{softmax}(Q_3 K_2^T) \vec{V}_2 + \text{softmax}(Q_3 K_3^T) \vec{V}_3 \\ \text{Att}_4(Q, K, V) &= \text{softmax}(Q_4 K_1^T) \vec{V}_1 + \text{softmax}(Q_4 K_2^T) \vec{V}_2 + \text{softmax}(Q_4 K_3^T) \vec{V}_3 + \text{softmax}(Q_4 K_4^T) \vec{V}_4 \end{aligned}$$

和之前类似，不再赘述。

看上面图和公式，我们可以得出结论：

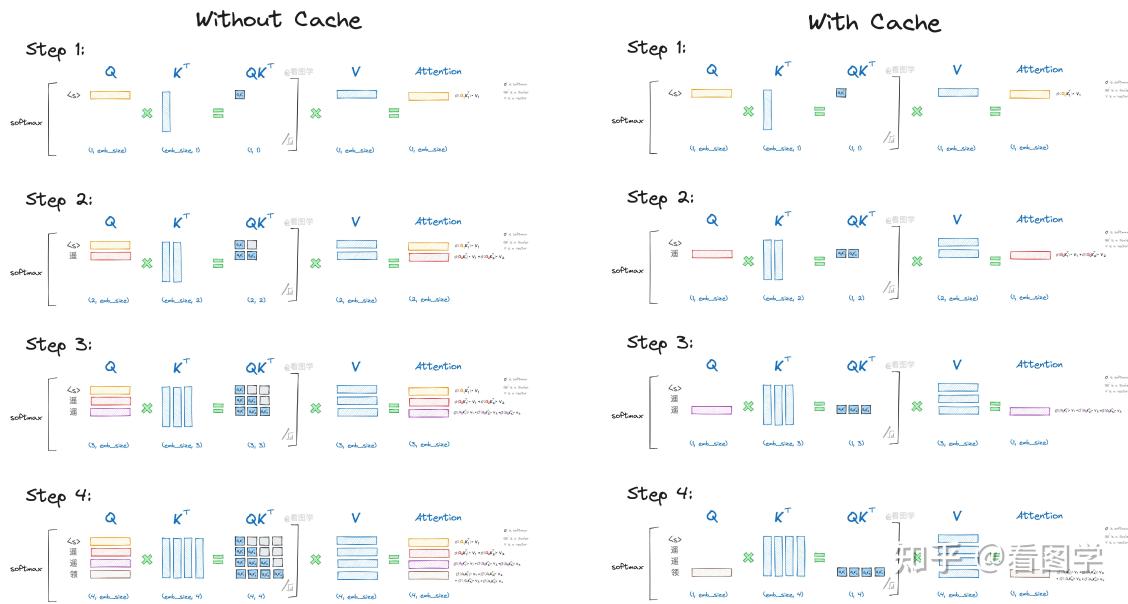
1. 当前计算方式存在大量冗余计算。
2. Att_k 只与 Q_k 有关。
3. 推理第 x_k 个字符的时候只需要输入字符 x_{k-1} 即可。

我们每一步其实之需要根据 Q_k 计算 Att_k 就可以，之前已经计算的 Attention 完全不需要重新计算。但是 K 和 V 是全程参与计算的，所以这里我们需要把每一步的 K, V 缓存起来。所以说叫 KV Cache 好像有点不太对，因为 KV 本来就需要全程计算，可能叫增量 KV 计算会更好理解。

下面 4 张图展示了使用 KV Cache 和不使用的对比。

推理加速KV Cache 示意图

看图学



下面是 gpt 里面 KV Cache 的实现。其实明白了原理后代码实现简单的不得了，就是 concat 操作而已。

https://github.com/huggingface/transformers/blob/main/src/transformers/models/gpt2/modeling_gpt2.py#L318C1-L331C97

```

if layer_past is not None:
    past_key, past_value = layer_past
    key = torch.cat((past_key, key), dim=-2)
    value = torch.cat((past_value, value), dim=-2)

if use_cache is True:
    present = (key, value)
else:
    present = None

if self.reorder_and_upcast_attn:
    attn_output, attn_weights = self._upcast_and_reordered_attn(

```

```
    query, key, value, attention_mask, head_mask)
else:
    attn_output, attn_weights = self._attn(query, key, value,
        attention_mask, head_mask)
```

最后需要注意当 sequence 特别长的时候，KV Cache 其实还是个 Memory 刺客。

比如 batch_size=32, head=32, layer=32, dim_size=4096, seq_length=2048, float32 类型，则需要占用的显存为 $2 * 32 * 4096 * 2048 * 32 * 4 / 1024/1024/1024 = 64G$ 。

针对内存的问题，学者们研发出了 Page Attention 之类的方法来优化。

Chapter 6: MOE, 多模态等

Chapter 7: 大语言模型评估

Chapter 8: 大语言模型应用

Prompt Engineering

Agent