

21 | 注意力机制、兴趣演化：推荐系统如何抓住用户的心？

你好，我是王喆。

近几年来，注意力机制、兴趣演化序列模型和强化学习，都在推荐系统领域得到了广泛的应用。它们是深度学习推荐模型的发展趋势，也是我们必须要储备的前沿知识。

作为一名算法工程师，足够的知识储备是非常重要的，因为在掌握了当下主流的深度学习模型架构（Embedding MLP 架构、Wide&Deep 和 DeepFM 等等）之后，要想再进一步提高推荐系统的效果，就需要清楚地知道业界有哪些新的思路可以借鉴，学术界有哪些新的思想可以尝试，这些都是我们取得持续成功的关键。

所以，我会用两节课的时间，带你一起学习这几种新的模型改进思路。今天我们先重点关注注意力机制和兴趣演化序列模型，下节课我们再学习强化学习。

什么是“注意力机制”？

“注意力机制”来源于人类天生的“选择性注意”的习惯。最典型的例子是用户在浏览网页时，会有选择性地注意页面的特定区域，而忽视其他区域。

比如，图 1 是 Google 对大量用户进行眼球追踪实验后，得出的页面注意力热度图。我们可以看到，用户对页面不同区域的注意力区别非常大，他们的大部分注意力就集中在左上角的几条搜索结果上。

那说了这么多，“注意力机制”对我们构建推荐模型到底有什么价值呢？

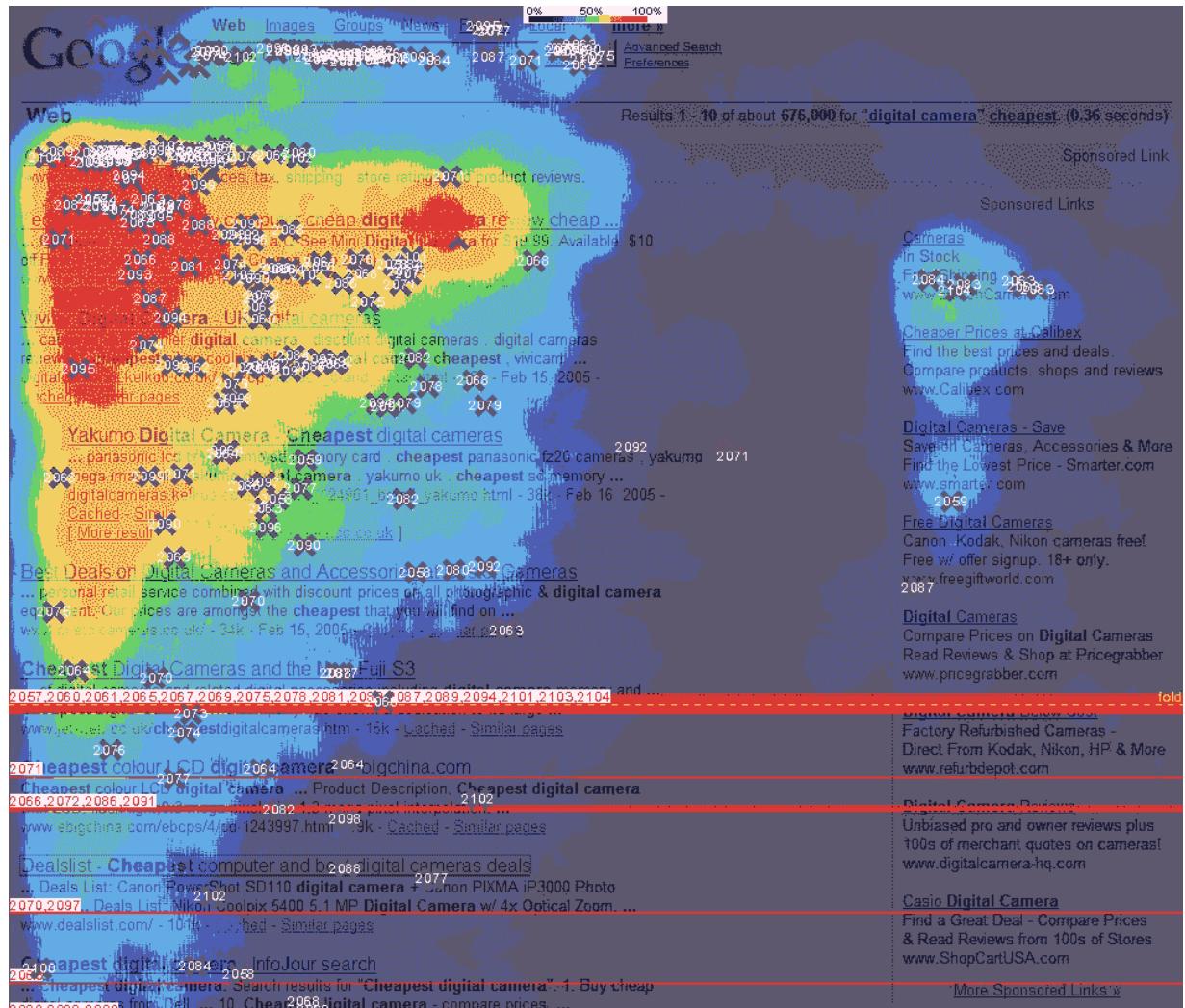


图1 Google搜索结果的注意力热度图

价值是非常大的。比如说，我们要做一个新闻推荐的模型，让这个模型根据用户已经看过的新闻做推荐。那我们在分析用户已浏览新闻的时候，是把标题、首段、全文的重要性设置成完全一样比较好，还是应该根据用户的注意力不同给予不同的权重呢？当然，肯定是后者比较合理，因为用户很可能都没有注意到正文最后的几段，如果你分析

内容的时候把最后几段跟标题、首段一视同仁，那肯定就把最重要的信息给淹没了。

事实上，近年来，注意力机制已经成功应用在各种场景下的推荐系统中了。其中最知名的，要数阿里巴巴的深度推荐模型，DIN (Deep Interest Network，深度兴趣网络)。接下来，我们就一起来学习一下 DIN 的原理和模型结构。

深度兴趣网络 DIN 的原理和结构

DIN 模型的应用场景是阿里最典型的电商广告推荐。对于付了广告费的商品，阿里会根据模型预测的点击率高低，把合适的广告商品推荐给合适的用户，所以 DIN 模型本质上是一个点击率预估模型。

注意力机制是怎么应用在 DIN 模型里的呢？回答这个问题之前，我们得先看一看 DIN 在应用注意力机制之前的的基础模型是什么样的，才能搞清楚注意力机制能应用在哪，能起到什么作用。

下面的图 2 就是 DIN 的基础模型 Base Model。我们可以看到，Base Model 是一个典型的 Embedding MLP 的结构。它的输入特征有用户属性特征 (User Profile Features)、用户行为特征 (User Behaviors)、候选广告特征 (Candidate Ad) 和场景特征 (Context Features)。

用户属性特征和场景特征我们之前也已经讲过很多次了，这里我们重点关注用户的行为特征和候选广告特征，也就是图 2 中彩色的部分。

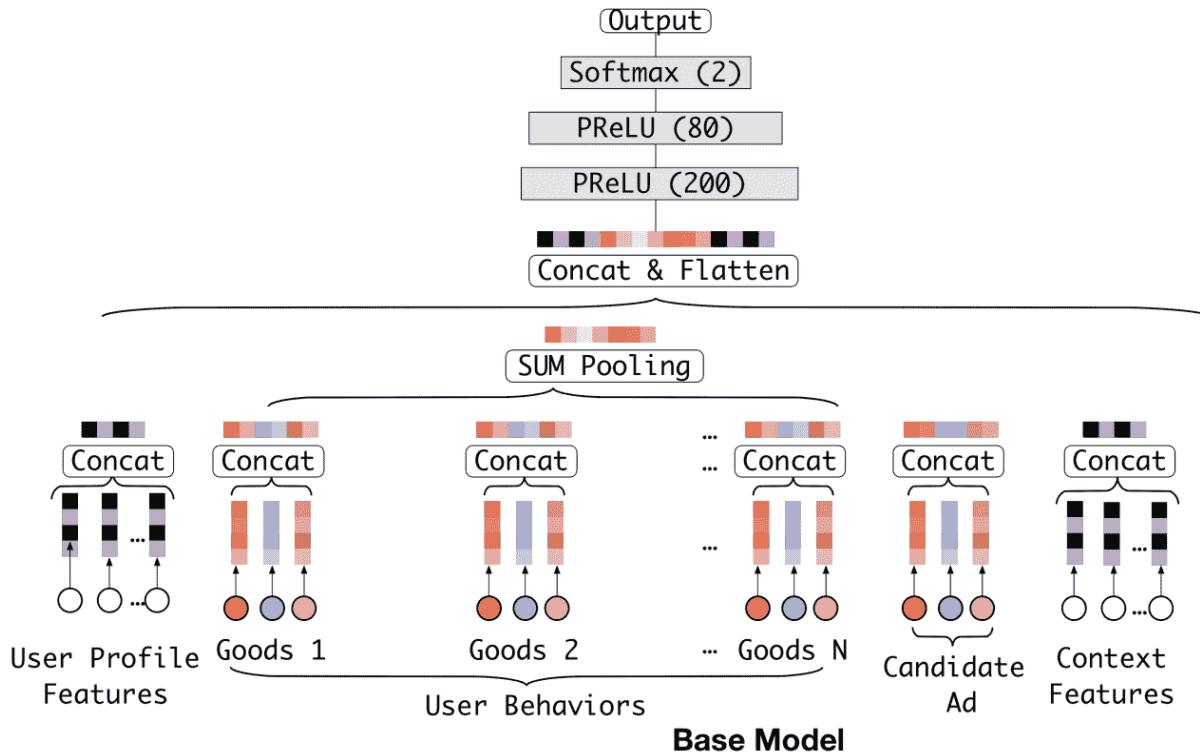


图2 阿里Base模型的架构图

(出自论文 Deep Interest Network for Click-Through Rate Prediction)

我们可以清楚地看到，用户行为特征是由一系列用户购买过的商品组成的，也就是图上的 Goods 1 到 Goods N，而每个商品又包含了三个子特征，也就是图中的三个彩色点，其中红色代表商品 ID，蓝色是商铺 ID，粉色是商品类别 ID。同时，候选广告特征也包含了这三个 ID 型的子特征，因为这里的候选广告也是一个阿里平台上的商品。

我们之前讲过，在深度学习中，只要遇到 ID 型特征，我们就构建它的 Embedding，然后把 Embedding 跟其他特征连接起来，输入后续的 MLP。阿里的 Base Model 也是这么做的，它把三个 ID 转换成了对应的 Embedding，然后把这些 Embedding 连接起来组成了当前商品的 Embedding。

完成了这一步，下一步就比较关键了，因为用户的行为序列其实是一组商品的序列，这个序列可长可短，但是神经网络的输入向量的维度必须是固定的，那我们应该怎么把这一组商品的 Embedding 处理成一个长度固定的 Embedding 呢？图 2 中的 SUM Pooling 层的结构就给出了答案，就是直接把这些商品的 Embedding 叠加起来，然后再把叠加后的 Embedding 跟其他所有特征的连接结果输入 MLP。

但这个时候问题又来了，SUM Pooling 的 Embedding 叠加操作其实是把所有历史行为一视同仁，没有任何重点地加起来，这其实并不符合我们购物的习惯。

举个例子来说，候选广告对应的商品是“键盘”，与此同时，用户的历史行为序列中有这样几个商品 ID，分别是“鼠标”“T 恤”和“洗面奶”。从我们的购物常识出发，“鼠标”这个历史商品 ID 对预测“键盘”广告点击率的重要程度应该远大于后两者。从注意力机制的角度出发，我们在购买键盘的时候，会把注意力更多地投向购买“鼠标”这类相关商品的历史上，因为这些购买经验更有利于我们做出更好的决策。

好了，现在我们终于看到了应用注意力机制的地方，那就是用户的历史行为序列。阿里正是在 Base Model 的基础上，把注意力机制应用在了用户的历史行为序列的处理上，从而形成了 DIN 模型。那么，DIN 模型中应用注意力机制的方法到底是什么呢？

我们可以从下面的 DIN 模型架构图中看到，与 Base Model 相比，DIN 为每个用户的历史购买商品加上了一个激活单元（Activation Unit），这个激活单元生成了一个权重，这个权重就是用户对这个历史商品的注意力得分，权重的大小对应用户注意力的高低。

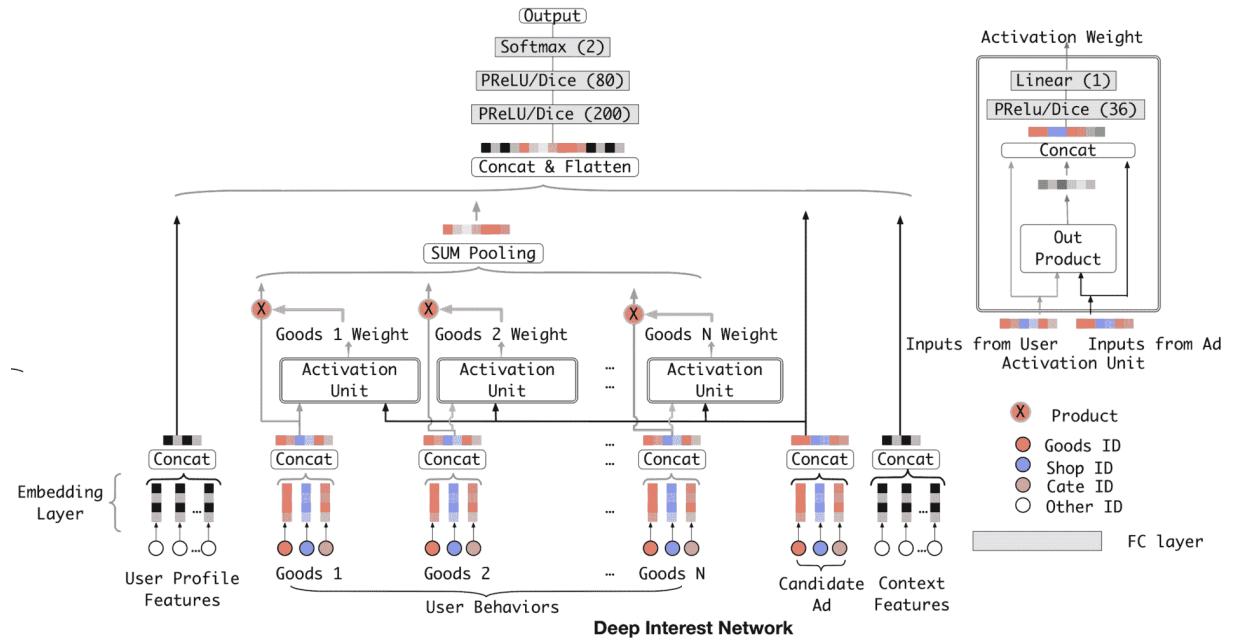


图3 阿里DIN模型的架构图

(出自论文 Deep Interest Network for Click-Through Rate Prediction)

那现在问题就只剩下一个了，这个所谓的激活单元，到底是怎么计算出最后的注意力权重的呢？为了搞清楚这个问题，我们需要深入到激活单元的内部结构里面去，一起来看看图 3 右上角激活单元的详细结构。

它的输入是当前这个历史行为商品的 Embedding，以及候选广告商品的 Embedding。我们把这两个输入 Embedding，与它们的外积结果连接起来形成一个向量，再输入给激活单元的 MLP 层，最终会生成一个注意力权重，这就是激活单元的结构。简单来说，**激活单元就相当于一个小的深度学习模型**，它利用两个商品的 Embedding，生成了代表它们关联程度的注意力权重。

到这里，我们终于抽丝剥茧地讲完了整个 DIN 模型的结构细节。如果你第一遍没理解清楚，没关系，对照着 DIN 模型的结构图，反复再看

几遍我刚才讲的细节，相信你就能彻底消化吸收它。

注意力机制对推荐系统的启发

注意力机制的引入对于推荐系统的意义是非常重大的，它模拟了人类最自然，最发自内心的注意力行为特点，使得推荐系统更加接近用户真实的思考过程，从而达到提升推荐效果的目的。

从“注意力机制”开始，越来越多的对深度学习模型结构的改进是基于对用户行为的深刻观察而得出的。由此，我也想再次强调一下，**一名优秀的算法工程师应该具备的能力，就是基于对业务的精确理解，对用户行为的深刻观察，得出改进模型的动机，进而设计出最合适你的场景和用户的推荐模型。**

沿着这条思路，阿里的同学们在提出 DIN 模型之后，并没有停止其推荐模型演化的进程，而是又在 2019 年提出了 DIN 模型的演化版本，也就是深度兴趣进化网络 DIEN (Deep Interest Evolution Network)，那这个 DIEN 到底在 DIN 基础上做了哪些改进呢？

兴趣进化序列模型

无论是电商购买行为，还是视频网站的观看行为，或是新闻应用的阅读行为，特定用户的历史行为都是一个随时间排序的序列。既然是和时间相关的序列，就一定存在前后行为的依赖关系，这样的序列信息对于推荐过程是非常有价值的。为什么这么说呢？

我们还拿阿里的电商场景举个例子。对于一个综合电商来说，用户兴趣的迁移其实是非常快的。比如，上一周一位用户在挑选一双篮球鞋，这位用户上周的行为序列都会集中在篮球鞋这个品类的各个商品上，但在他完成这一购物目标后，这一周他的购物兴趣就可能变成买

一个机械键盘，那这周他所有的购买行为都会围绕机械键盘这个品类展开。

因此，如果我们能让模型预测出用户购买商品的趋势，那肯定会对提升推荐效果有益的。而 DIEN 模型，就正好弥补了 DIN 模型没有对行为序列进行建模的缺陷，它围绕兴趣进化这个点进一步对 DIN 模型做了改进。

图 4 就是 DIEN 模型的架构图，这个模型整体上仍然是一个 Embedding MLP 的模型结构。与 DIN 不同的是，DIEN 用“兴趣进化网络”也就是图中的彩色部分替换掉了原来带有激活单元的用户历史行为部分。这部分虽然复杂，但它的输出只是一个 $h'(T)$ 的 Embedding 向量，它代表了用户当前的兴趣向量。有了这个兴趣向量之后，再把它与其他特征连接在一起，DIEN 就能通过 MLP 作出最后的预测了。

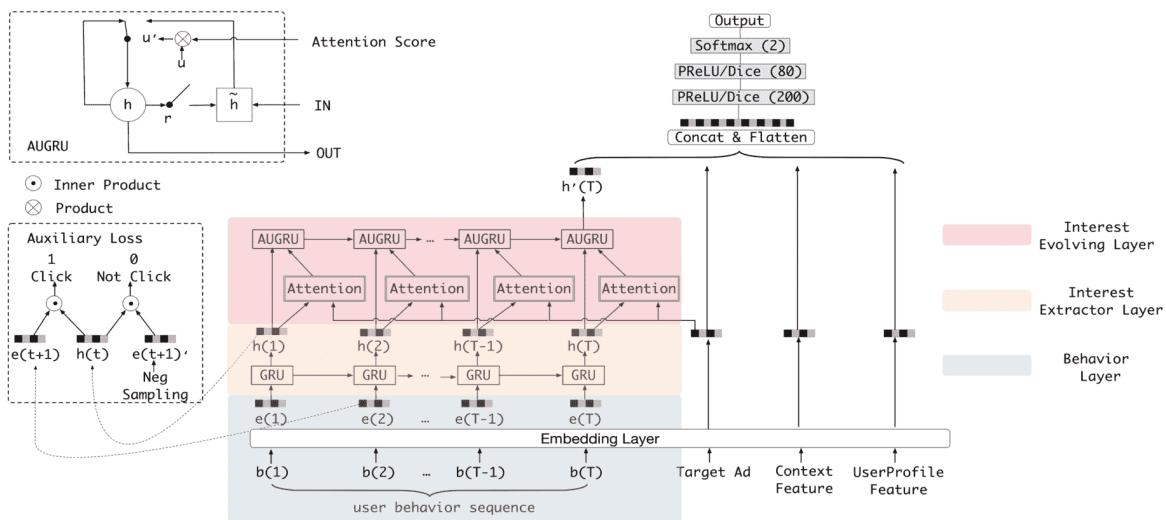


图4 DIEN模型的架构图（出自论文 Deep Interest Evolution Network for Click-Through Rate Prediction）

好了，现在问题的焦点就在，DIEN 模型是如何生成这个兴趣向量的。关键就在于 DIEN 模型中彩色部分的三层兴趣进化网络，下面，我就按照从下到上的顺序，给你讲讲它们的名称和作用。

最下面一层是行为序列层（Behavior Layer，浅绿色部分）。它的主要作用和一个普通的 Embedding 层是一样的，负责把原始的 ID 类行为序列转换成 Embedding 行为序列。

再上一层是兴趣抽取层（Interest Extractor Layer，浅黄色部分）。它的主要作用是利用 GRU 组成的序列模型，来模拟用户兴趣迁移过程，抽取每个商品节点对应的用户兴趣。

最上面一层是兴趣进化层（Interest Evolving Layer，浅红色部分）。它的主要作用是利用 AUGRU(GRU with Attention Update Gate) 组成的序列模型，在兴趣抽取层基础上加入注意力机制，模拟与当前目标广告（Target Ad）相关的兴趣进化过程，兴趣进化层的最后一个状态的输出就是用户当前的兴趣向量 $h'(T)$ 。

不知道你发现了吗，兴趣抽取层和兴趣进化层都用到了序列模型的结构，那什么是序列模型呢？直观地说，图 5 就是一个典型的序列模型的结构，它和我们之前看到的多层神经网络的结构不同，序列模型是“一串神经元”，其中每个神经元对应了一个输入和输出。

那在 DIEN 模型中，神经元的输入就是商品 ID 或者前一层序列模型的 Embedding 向量，而输出就是商品的 Embedding 或者兴趣 Embedding，除此之外，每个神经元还会与后续神经元进行连接，用于预测下一个状态，放到 DIEN 里，就是为了预测用户的下一个兴趣。这就是序列模型的结构和作用。

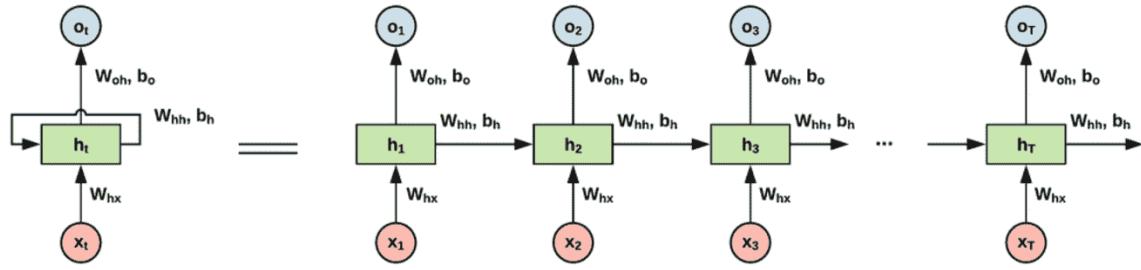


图5 RNN模型的经典结构

至于上面提到过的 GRU 序列模型，它其实是序列模型的一种，根据序列模型神经元结构的不同，最经典的有RNN、LSTM、GRU这3种。这里我们就不展开讲了，对理论感兴趣的同学，可以点击我给出的超链接，参考这几篇论文做更深入的研究。

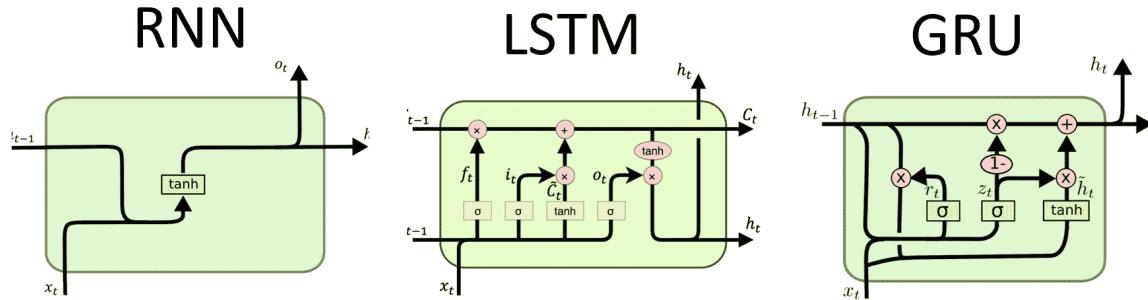


图6 序列模型中的不同单元结构

事实上，序列模型已经不仅在电商场景下，成功应用于推测用户的下次购买行为，在 YouTube、Netflix 等视频流媒体公司的视频推荐模型中，序列模型也用来推测用户的下次观看行为（Next Watch）。除此之外，音乐类应用也非常合适使用序列模型来预测用户的音乐兴趣变化。所以，掌握 DIEN 模型的架构对于拓宽我们的技术视野非常有帮助。

小结

注意力机制和兴趣演化序列模型的加入，让推荐系统能够更好地抓住用户的心。

对于注意力机制来说，它主要模拟了人类注意力的天性。具体到阿里的 DIN 模型上，它利用激活单元计算出用户对于不同历史商品的注意力权重，针对当前广告商品，作出更有针对性的预测。

而序列模型更注重对序列类行为的模拟和预测。典型的例子是 DIEN 模型对用户购买兴趣进化过程的模拟。DIEN 模型可以应用的场景非常广泛，包括电商平台的下次购买，视频网站的下次观看，音乐 APP 的下一首歌曲等等。

总的来说，注意力机制的引入是对经典深度学习模型的一次大的改进，因为它改变了深度学习模型对待用户历史行为“一视同仁”的弊端。而序列模型则把用户行为串联起来，让用户的兴趣随时间进行演化，这也是之前的深度学习模型完全没有考虑到的结构。

最后，我把今天的重要概念总结在了表格中，方便你及时查看和复习。

知识点	关键概述
注意力机制	人类天生的“选择性注意”的习惯
DIN模型的结构	经典的Embedding MLP的框架，加上应用了注意力机制的用户历史行为部分
DIN应用注意力机制的过程	根据历史行为商品和广告商品的Embedding，使用了激活单元来预测注意力权重
DIEN模型的结构	经典的Embedding MLP的框架，加上三层的序列模型结构
DIEN的三层序列模型结构	基于Embedding层的行为序列层 基于GRU序列模型的兴趣抽取层 基于AUGRU序列模型的兴趣进化层



课后思考

DIN 使用了一个结构比较复杂的激活单元来计算注意力权重，你觉得有没有更简单、更实用的方式来生成注意力权重呢？其实计算注意力权重就是为了计算历史行为物品和广告物品的相关性，在这个过程中，你觉得能不能利用到特征交叉的知识呢？为什么？

欢迎把你的思考和疑问写在留言区，如果你的朋友们也在关注注意力机制和兴趣演化序列模型的发展，那不妨也把这节课转发给他们，我们下节课见！