第七部分

物品冷启动

王树森 著

第 1 章 物品冷启动的评价体系

物品冷启动解决的问题是如何将新发布的物品推荐给合适的用户。在小红书的场景下，物品冷启动指的是用户新发布的笔记。为什么要特殊对待新物品？新物品推荐有何特殊之处？能否用已有的推荐链路、评价指标、实验方案？

第一，与充分曝光的物品相比，新物品推荐的难度大、效果差。推荐系统主要用到三种物品特征——内容特征、统计特征、ID embedding——新物品缺乏后两种特征。新物品尚未得到充分曝光，系统收集到的点击率、点赞率等指标不准，不能反映出物品受欢迎的程度。由于缺乏充分的用户—物品交互，召回模型、排序模型尚未学好新物品 ID embedding 向量。缺乏三种物品特征中的两种，导致新物品的召回和排序不够精准。

第二，在 UGC 平台，物品冷启动策略要作者侧发布指标负责，而普通的推荐链路只需要负责用户侧消费指标。小红书的实验表明，在新笔记发布之后，曝光越多、越早，对作者发布意愿的激励越强。背后的逻辑也是很显然的。试想你作为小红书的作者，如果你发布的新笔记几个小时没人看、没人交互，你以后还会发布吗？因此，推荐系统要专门针对新物品推荐做优化，让新物品的曝光变早、变多，在不损害用户体验的前提下，提升作者侧发布指标。

第三，物品冷启动的评价指标、AB 测试方案都区别于普通物品推荐。冷启的评价指标不仅包括用户侧指标，还包括作者侧指标、内容侧指标。普通物品的推荐只需要用户侧 AB 测试，实验容易，结论比较可信。而作者侧实验要复杂得多，各种 AB 测试方案都存在缺点。甚至可以这么说，工业界没有一个完美的作者侧 AB 测试方案。

本章内容分为两节。第 1.1 节介绍物品冷启动的三种评价指标，包括作者侧指标、用户侧指标、内容侧指标。第 1.2 节讨论作者侧和用户侧的 AB 测试方案，并分析其中存在的缺点。

1.1 评价指标

小红书是一个 UGC 平台，用户既是消费者也是创作者。UGC 平台的新物品数量巨大，内容质量良莠不齐，分发难度大于 PGC 平台。但这也意味着 UGC 物品冷启动的提升空间大于 PGC 平台。对于小红书这样的 UGC 平台，算法工程师优化物品冷启动的目标主要有三个：

- 激励发布：流量向低曝光新笔记倾斜，激励作者发布，从而丰富我们的内容池。
- 精准推荐：克服新物品推荐中的困难，让新笔记给合适的用户曝光，不引起用户反感。
- 挖掘高潜：通过初期“雨露均沾”的小流量的试探，找到高质量的笔记，给与流量倾斜。

物品冷启动主要有三类评价指标，分别对应上述三个目标。

1.1.1 作者侧指标

小红书的用户既是消费者（阅读），也是创作者（发布）。作者侧指标反映出用户的发布意愿，通常用发布渗透率（penetration rate）、人均发布量作为评价指标。对低曝光的新物品扶持得越好，作者侧发布指标就越高。发布渗透率定义为：

$$\text{发布渗透率} = \text{当日发布人数} / \text{日活人数}。$$

人均发布量的定义为：

$$\text{人均发布量} = \text{当日发布物品数} / \text{日活人数}。$$

今天一位用户只要发布一篇笔记，他就给小红书贡献了一个发布人数。但不论他今天发布一篇或是十篇，他只算一个发布人数，不会影响发布渗透率，但是会影响人均发布量。

例 1.1

假设今天有 100 万用户在小红书上发布新笔记，一共发布 200 万篇。假设今天小红书的日活用户数为 5000 万。那么

$$\text{发布渗透率} = 100/5000 = 2\%,$$

$$\text{人均发布量} = 200/5000 = 0.04.$$

人均发布量大于发布渗透率，原因是部分用户一天发多篇笔记。 ♣

想要提升作者侧发布指标，要让新物品的曝光和交互出现得尽量早、次数尽量多。通过召回的工程架构优化，让新物品从发布到第一次曝光的间隔缩短，比方说从 5 分钟缩短到 1 分钟，可以提升用户的发布意愿。通过流量调控机制，给予低曝光新物品流量倾斜，让前 24 小时内达成 100 次曝光的物品的占比提升，比方说从 50% 提升到 80%，也可以提升用户发布意愿。

1.1.2 用户侧指标

物品冷启动存在“跷跷板效应”，即给与低曝光物品流量倾斜，有利于作者侧发布指标，但不利于用户侧消费指标。一个原因是低曝光物品缺少推荐所需的很多特征，推荐难度大，推荐不够准。另一个原因是低曝光物品本身的质量可能不高，增大它们的曝光量确实会损害用户体验。我们主要考察两类用户侧指标：新物品自身的消费指标、大盘整体的消费指标。

新物品自身的消费指标： 新物品自身的点击率、点赞率等消费指标可以反映新物品的推荐是否精准。如果把新物品推荐给更合适的用户，那么新物品的消费指标会提升。但这里存在一个问题，全体新物品的点击率、点赞率等指标不能反映真实的推荐效果。

例 1.2

只看小红书发布 24 小时之内的新笔记，曝光次数大于 1000 的新笔记的点击率记作 y%，曝光次数小于 1000 的新笔记的点击率记作 z%。y 显著大于 z，道理很显然，点击率高的笔记受到推荐算法的流量倾斜，曝光次数当然会更高。

假想实验：不改变召回和排序模型，把低曝光新物品的部分流量分给高曝光新物品。那么新物品整体的点击率会升高。我们明明没有改善推荐模型，没有让推荐更精准，但是流量调控让消费指标变好了，我们获得了虚假的繁荣。 ♣

例 1.3

限定在发布 24 小时内的新物品，计算曝光次数的基尼系数，数值越大说明头部效应越严重，即少量的物品占据了绝大部分的曝光。包括小红书在内，工业界的推荐系统都存在严重的头部效应，基尼系数往往超过 0.9。

假想实验：一个新模型微弱地改善高曝光物品的推荐准确性，但是严重伤害低曝光物品的推荐准确性。尽管新的模型更差，但是 AB 测试显示新物品整体的点击率提升。 ♣

以上两个例子说明全体新物品的消费指标具有误导性。更合理的指标应该是分组考察新物品的消费指标，比如按曝光次数分为 $[0, 99]$、$[100, 999]$、$[1000, +\infty)$ 三组。我们只需要关注前两组的消费指标。一方面是因为低曝光的新物品占比很高，绝大部分的新物品都是低曝光，而高曝光的新物品占比很低。另一方面是低曝光新物品的推荐不容易做好、推荐不够准，需要设计专门的技术处理低曝光新物品。而高曝光物品的推荐很容易做好，无需特殊对待高曝光新物品。

大盘的消费指标： 大盘的核心消费指标包括用户每日使用 APP 的时长、日活用户数、月活用户数。这些指标不区分新物品与老物品，也不区分低曝光物品与高曝光物品。物品冷启动通常不承担大盘消费指标的增长目标，但是冷启动策略不能显著损害大盘消费指标。

1.1.3 内容侧指标

冷启动策略对推荐系统的影响并不止局限于冷启动阶段（比如发布前 24 小时的物品）。好的冷启动策略可以从海量新物品中挖掘出优质物品，帮助优质物品爬坡，成长为热门。好的冷启动策略还可以避免流量浪费在低质量物品上，减少“高曝光低转化”的物品。总而言之，冷启动策略会对 UGC 平台整体生态产生影响。

该如何衡量冷启动策略对整体生态的影响呢？作者侧和用户侧指标都不行，它们只能反映出策略在冷启动阶段产生的影响，反映不出对后续分发的影响。内容侧指标可以考察推荐系统对整体生态的影响。有两种常见的内容侧指标：高热物品占比、高曝低转物品占比。

高热物品占比衡量有多少物品能在生命周期中成长为热门物品。举个例子，小红书首页推荐只分发年龄小于 30 天的笔记，那么笔记的生命周期是 30 天。我们设定高热阈值为 1 千次点击。比方说小红书上今天新发布了 200 万篇新笔记，在 30 天后，其中有 20 万篇笔记获得超过 1 千次点击，那么

$$\text{高热物品占比} \ = \ 20/200 \ = \ 10\%.$$

高热物品占比高，就说明冷启阶段挖掘优质优质的能力强、成功助力优质物品成长为热门，因此高热物品占比越高越好。以高热物品占比为优化目标，是否会让流量集中在头部高热物品上，加重头部效应?

- 这种观点是有道理的。如果把“雨露均沾”的流量富集到优质物品上，这些优质物品就可以达到高热的阈值，提升高热物品占比。优化高热物品占比，确实有可能加重头部效应。
- 但从另一个角度看，提升高热物品占比也有可能会降低头部效应。举个例子，某物品曝光 100 万次，如果把它的流量平均分给 100 个物品，这 100 个物品都获得 1 万次曝光，大概率会获得 1 千次点击，达到高热阈值。如此打压头部，反倒能增加高热物品的数量。

综上所述，以高热物品占比为优化目标，会让流量向头部物品富集，但也会避免少数物品吸走过多流量。

高曝低转物品占比衡量冷启动策略的效率，如果推荐系统对流量分配不合理，则这个指标会偏高。举个例子，“高曝”定义为曝光次数大于 1000，“低转”定义为点击率小于 5%。举个例子，小红书今天新发布了 200 万篇新笔记，记录这些新笔记在发布第 24 小时后是否满足“高曝”和“低转”。假如有 10 万篇笔记满足“高曝”，其中 2 万篇笔记同时满足“高曝”和“低转”，那么

$$\text{高曝低转占比} \ = \ 2/10 \ = \ 20\%.$$

高曝低转物品占比越低越好。高曝低转化意味着推荐不精准和浪费流量。可能是对新物品的扶持过猛，把物品推荐给了不感兴趣的用户，造成点击率偏低。也可能是流量分配的不合理，把流量浪费在了低质量的物品上。

1.2 实验设计

想要上线新的推荐策略，需要做 AB 测试，用线上的小流量考察新策略是否产生收益，从而决定是否上线新策略。冷启动实验不但需要考察用户侧指标，还需要考察作者侧指标，后者远比前者复杂。可以这么说，工业界并没有很合理的作者侧 AB 测试方案，所有的方案都有明显的缺点。

1.2.1 用户侧实验

图 1.1 是推荐系统标准的 AB 测试方案，考察用户侧消费指标。同样的方法也可以用于物品冷启动。这种方案对用户做分组，不对物品做分组。当实验组用户发起推荐请求时，系统调用新策略，从全体物品中选出最合适的若干物品，曝光给用户；当对照组用户发起推荐请求时，系统调用旧策略。在实验运行一段时间后，对比两组用户的消费指标之差（diff），比如用户日均使用 APP 的时长、曝光小于 100 的物品的点击率、等等。如果 diff 具有显著性，则可以判断新策略是否对用户体验更有利。

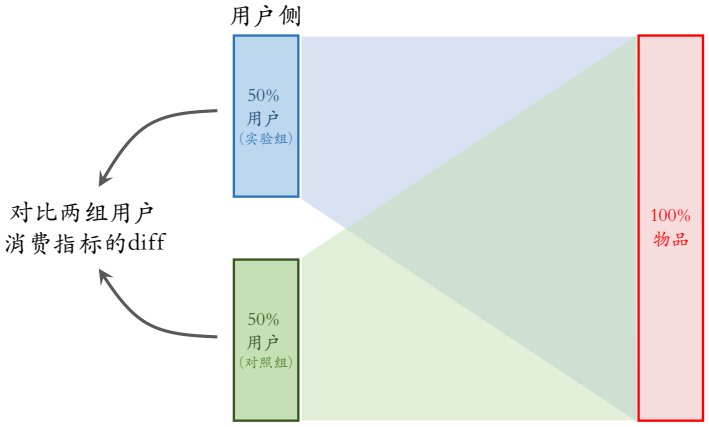


图 1.1: 用户侧实验方案。

这种 AB 测试的方案有个缺点，会导致 AB 测试得到的 diff 与真实情况有偏差。我们举个例子分析实验方案的缺点，这个例子做如下设定。

- 设定：冷启流量调控有保量 100 的机制，即系统要尽量保证新物品在发布 24 小时之内获得 100 次曝光。
- 设定：在排序阶段，给新物品的分数乘以提权系数 α (≥ 1)，然后让新老物品一起参与排序，自由竞争。
- 假设：新物品获得曝光越多，用户日均使用 APP 时长就越低。这个假设是合理的。通常来说，新物品推荐不够准，新物品太多会影响体验。
- 策略：旧策略的提权系数为 α，新策略的提权系数为 2α。新策略会让新物品获得更多曝光，导致用户体验变差，损害用户侧消费指标，AB 测试观察到的 diff 应当为负数。

这种实验方案的缺点是实验观测到的 diff 与推全后的 diff 不一致。比方说实验观测到用户日均使用 APP 时长的 diff 等于 -2%，但推全之后，实际上时长只跌了 1%，没有跌 2% 那么多。为什么会出现不一致呢?

如图 1.2 所示，由于对实验组用户用了新策略，实验组用户看到了更多的新物品，消费指标变差。而“保量 100 次曝光”这个量是确定的，既然一个物品从实验组得到更多曝光，那么从对照组获得的曝光次数会减少，导致对照组的消费指标变好。实验组消费指标变差，对照组消费指标变好，导致 AB 测试观察到的 diff 很大。但是实验推全之后，消费指标实际上跌不了那么多。

1.2.2 作者侧实验

方案一： 图 1.3 是最简单的作者侧实验方案，它存在严重的缺点。这种实验方案把作者分成两组，但是不对老物品分组，也不对用户分组。实验组作者新发布的物品用新策略，比如给新物品的提权系数为 2α；对照组作者发布的新物品用旧策略，比如给新物

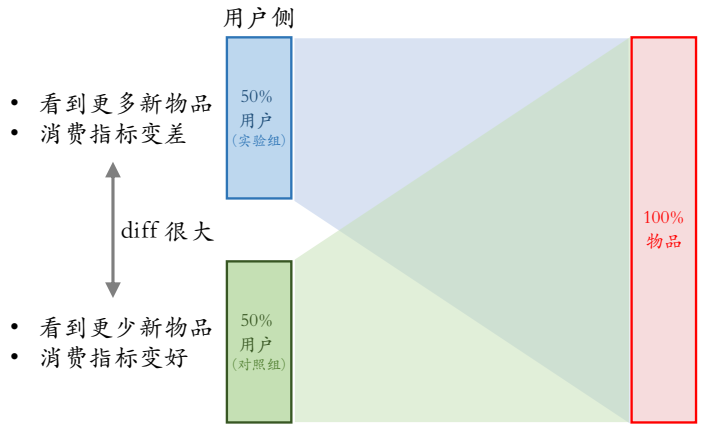


图 1.2: 在保量的设定下，这种用户侧实验方案存在缺陷。

品的提权系数为 α。通过对比两组作者发布指标的 diff，就可以判断新策略是否能激励发布。

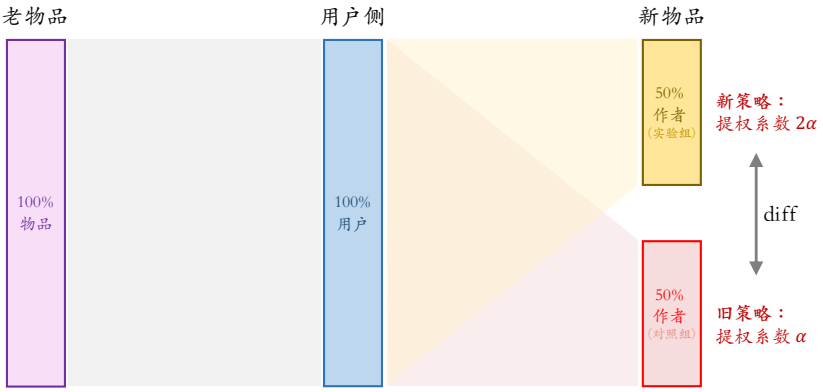


图 1.3: 作者侧实验方案一：只对新物品做分桶。

作者侧实验方案一存在严重的缺点——两组新物品相互抢流量。有可能 AB 测试观察到发布指标 diff，但是实验推全之后 diff 完全消失。我们举个例子分析实验方案的缺点，这个例子做如下设定。

- 设定：新老物品走两个独立的队列，各自做排序和截断，互不竞争。系统给与新老物品固定的曝光占比，比如新物品占 $1/3$，老物品占 $2/3$。
- 策略：旧策略给新物品的提权系数为 α，新策略给新物品的提权系数为 2α。

基于独立队列的设定，新老物品互不竞争，也就是说给新物品提权不会让新物品抢走老物品的曝光。提权系数同等影响所有新笔记，哪怕提权系数增加一万倍，也不会对推荐系统产生任何影响，新物品之间仍旧公平竞争。因此，把新策略推全，作者侧发布指标不会发生任何变化。但是在 AB 测试中，实验组新物品提权系数更大，抢走了对照组的新物品的流量，使得实验组新物品获得更多曝光，发布指标变好。AB 测试观测到了正向

的 diff，但推全前后发布指标不会有任何变化。

作者侧实验方案一还存在一种不太严重的缺点——新物品抢老物品的流量。我们举个例子分析这种缺点，这个例子做如下设定，与上文的设定有所不同。

- 设定：在排序阶段，给新物品的分数乘以提权系数 α (≥ 1)，然后让新老物品一起参与排序，自由竞争。
- 策略：旧策略给新物品的提权系数为 α，新策略给新物品的提权系数为 2α。

在 AB 测试中，50% 的实验组新物品与 100% 的老物品抢流量，平均一份新物品抢走两份老物品的曝光。推全之后，100% 的实验组新物品与 100% 的老物品抢流量，平均一份新物品只能抢走一份老物品的曝光。这会造成 AB 测试高估新策略的收益。举个例子，AB 测试观测到发布渗透率的 diff 为 +2%，但是实验推全只让总的发布渗透率增长 +1.5%。

方案二： 图 1.4 是某些公司用的实验方案，它同时对作者和用户做分组。方案二避免了两组新物品抢流量，因此结论更可信。方案二与方案一共同的缺点是新物品与老物品抢流量，这会导致 AB 测试估不准新策略的收益。

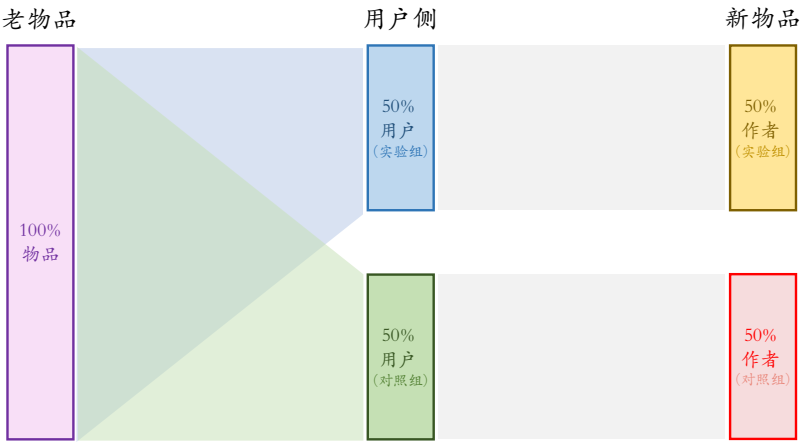


图 1.4: 作者侧实验方案二：同时对新物品和用户做分桶。

方案二最大的缺点在于伤害大盘的消费指标。方案二同时隔离作者和用户。给实验组用户做推荐时，只能从实验组的新物品池中做选择，导致有效的新物品池缩小了一半。假如不做隔离，召回和排序从新物品池中选出 n 个用户最感兴趣的物品。做隔离之后，这 n 个物品只剩 $n/2$ 个。为了凑够 n 个，系统要选出差一些的 $n/2$ 个。显然这会影响用户的体验，让大盘消费指标变差。

方案三： 图 1.5 是更极端的方案，新物品、老物品、用户都被隔离。给一个用户做推荐时，系统只能从 50% 的新物品、老物品中做选择，小红书就像是被拆分成了两个 APP。如果希望实验结果精准，那么实验方案三是最优的。然而方案三比方案二更严重伤害用户体验，造成大盘的消费指标大幅下跌。

方案四： 图 1.6 是我们团队同学设计的，它优于方案二。老物品不分桶，用户分为

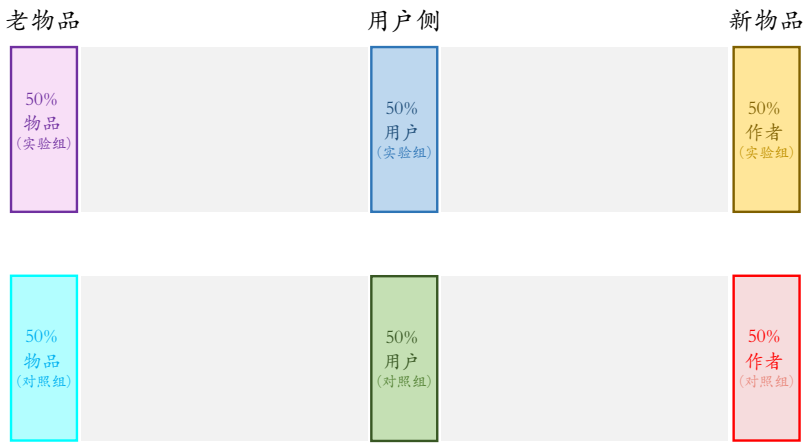


图 1.5: 作者侧实验方案三：同时对新物品、老物品、用户做分桶，数据被彻底隔离。

两个桶，作者分为三个桶。第二个作者桶既可以作为实验组，也可以作为对照组。当实验组用户发起推荐请求时，系统从前两个新物品桶中做选择，并应用新策略。当对照组用户发起推荐请求时，系统从后两个新物品桶中做选择，并应用旧策略。在分析数据时，我们只看两个 25% 的作者桶的发布指标，计算指标的 diff。

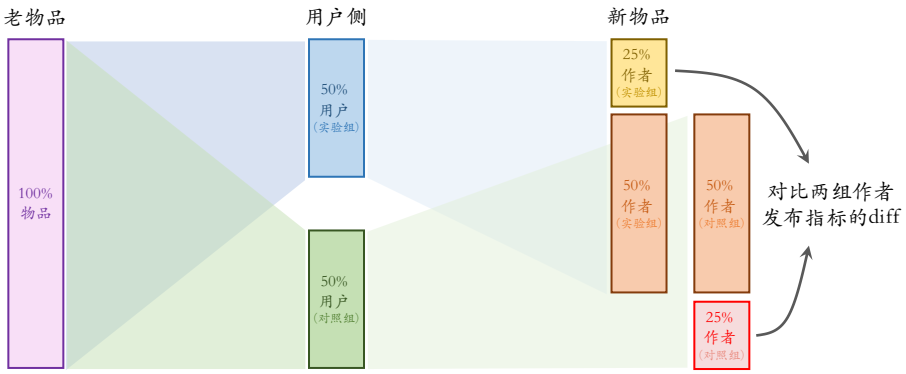


图 1.6: 作者侧实验方案四。

方案四会伤害用户体验，但是伤害小于方案二。用方案二，从用户的角度看，新物品池减小了 50%。用方案四，从用户的角度看，新物品池减小了 25%。如果图 1.6 中第二个作者桶（50% 的作者）的大小减小到 0，则方案四变成方案二。

方案四的另一个好处是保护高粉作者。如图 1.7 所示，把高粉作者放到第二个桶，那么高粉作者发布的新物品可以触及全体用户，这样有利于高粉作者的发布体验。假如把作者放在第一个或第三个桶，那么作者发布的新物品只能触及 50% 的用户。

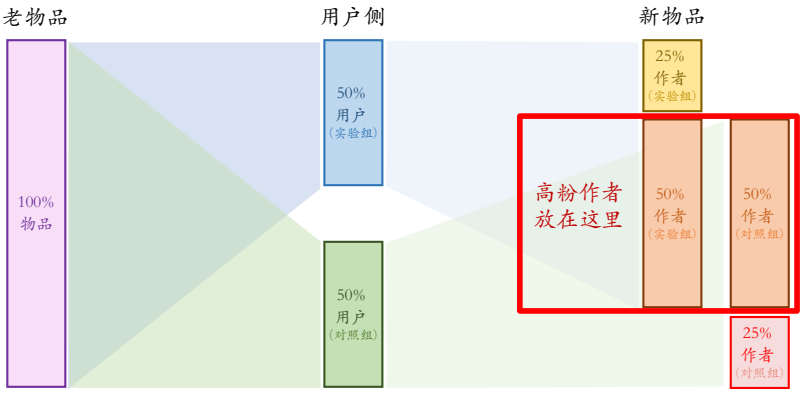


图 1.7: 如果使用作者侧实验方案四，可以把高粉作者放在第二个桶。

1.3 总结

- 物品冷启动有三个目标——激励发布、精准推荐、挖掘高潜。相应地用用三种指标考察冷启动——作者侧指标、用户侧指标、内容侧指标。
- 在 UGC 平台，物品冷启动需要负责作者侧发布指标的增长。让新发布的物品曝光和交互数量更多、发生更早，可以激励作者发布。
- 用户侧指标考察冷启阶段（比如前 24 小时）的新物品和大盘的消费指标。物品冷启动不应当负责用户侧指标的增长，但冷启动策略也不能显著伤害用户体验。
- 内容侧指标反映出冷启策略对冷启阶段结束之后（比如第 2 到 30 天）的影响。如果冷启策略可以很好地挖掘出优质物品，帮助优质物品成长为热门，则会改善整个推荐系统生态。
- 用户侧 AB 测试比较容易。虽然存在不足之处，但相对比较可信。
- 目前已知的作者侧 AB 测试方案都存在缺陷，缺陷可能会导致 AB 测试的结论不可信。算法工程师在设计实验方案时，应当问自己以下几个问题：
  - 实验组和对照组的新物品会不会抢流量？
  - 新物品、老物品怎么抢流量？AB 测试阶段与推全后抢流量的方式是否一致？
  - 同时隔离物品、用户，会不会让内容池变小？
  - 如果对新物品做保量，会发生什么？会不会导致新物品从实验组用户获得更多曝光，从对照组用户获得更少曝光？

第 2 章 冷启召回

上一章讨论过，新发布的物品缺少与用户的交互历史。这会导致一些召回通道完全不适用。以 ItemCF 为例，做召回的依据是两个物品的相似度。把与两个物品发生交互的用户记作集合 $\mathcal{U}_1$ 和 $\mathcal{U}_2$。交集 $\mathcal{U}_1 \cap \mathcal{U}_2$ 越大，则判定两个物品越相似。如图 2.1 所示，如果第二个物品是新发布的，那么 $\mathcal{U}_2$ 为空集、或者接近空集。这使得 ItemCF 难以判断两个物品的相似度。由于新物品的特殊性，ItemCF 等协同过滤召回通道对新物品不适用，双塔模型等深度神经网络效果不佳。

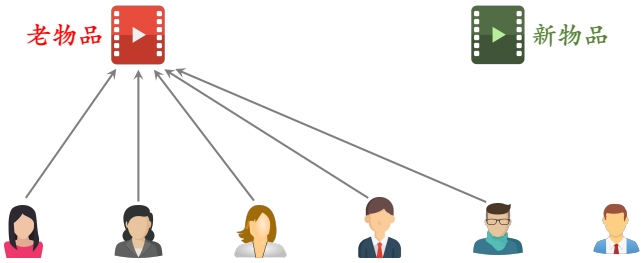


图 2.1: ItemCF 召回不适用于物品冷启动。

我们希望在新物品刚发布的时候，就有机会获得曝光。在新物品缺少统计信息和用户交互的情况下，主要通过类目召回、聚类召回等基于内容的通道获得曝光机会。在出现少量用户交互之后，look-alike 可以更准确地召回新物品。随着曝光和交互次数增长，双塔模型和协同过滤逐渐起到更重要的作用。本章第 2.1 到 2.4 节分别介绍类目召回、聚类召回、look-alike 召回、双塔召回这四种通道。

2.1 类目召回

凡是做信息流、社交、电商的互联网公司，都会维护用户画像，上面记录了用户的人口属性和兴趣标签。算法通过分析用户的点击、交互行为，推断出用户感兴趣的二级类目和关键词。以我为例，我感兴趣的二级类目包括美食探店、职场行业、大学教育，关键词包括历史、日漫、美食。

在物品刚发布的时候，NLP 算法会自动给物品打上类目和关键词标签，这些标签可以用作召回。如图 2.2 所示，我们建立从类目到物品的索引，索引上的物品按照发布时间倒排，新物品在最前面。类目召回的逻辑是这样的：

$$\text{用户} \longrightarrow \text{类目} \longrightarrow \text{物品}。$$

当用户发起推荐请求时，首先查看用户画像，取回用户感兴趣的类目。然后利用“类目 $\longrightarrow$ 物品”的索引，取回每个类目下最前面（即最新）的 k 个物品。比方说我感兴趣的类目是美食探店、职场行业、大学教育，那么类目召回通道会取回 $3k$ 个物品。

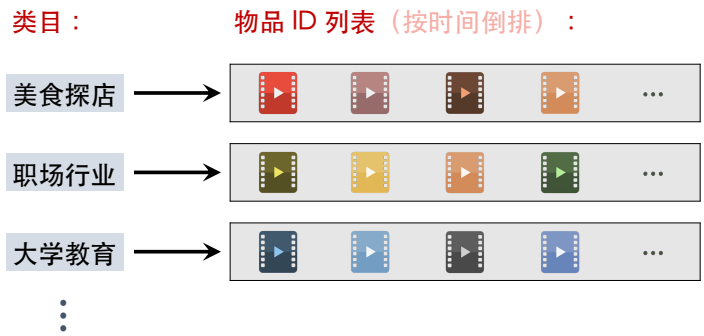


图 2.2: 类目召回的索引

类目召回是新物品获得曝光最快的途径。理论上，只要一个新物品进入“类目 ⟶ 物品”的索引，它立刻有机会被曝光。设“类目 ⟶ 物品”索引刷新的间隔为 t，那么一个物品从发布到第一次曝光的间隔至少为 t。大量实验表明，间隔 t 越短，越有利于提升创作积极性。因此很有必要用工程的方法缩短 t。在小红书，原本索引是 5 分钟做一次批量更新，后来改为实时流建索引，做到秒级更新，显著提升作者侧发布指标。

类目召回存在两个缺点。第一，类目召回的本质是匹配用户画像类目和物品类目，个性化很弱，召回不够精准。来自类目召回通道的物品的点击率、点赞率等指标显著低于大盘指标。第二，类目召回只对刚刚发布的新物品有效，留给新物品的窗口期很短。这是因为“类目 ⟶ 物品”索引按照物品发布时间倒排，在几十分钟之后，物品就排不到前 k，也就没有机会由这条通道透出。

关键词召回与类目召回非常类似，唯一的区别在于用关键词代替二级类目。关键词的数量远大于二级类目，因此关键词的粒度更细。关键词召回有同样的缺点，个性化很弱，留给新物品的时间窗口很短。

2.2 聚类召回

聚类召回是基于物品内容的召回通道。聚类召回假设如果用户喜欢一个物品，那么他会喜欢内容相似的物品。比方说小红书用户点赞了一篇萌宠的笔记，那么系统可以给用户推荐更多萌宠的笔记。

内容相似度： 为了基于物品内容做召回，需要事先训练一个多模态神经网络，把物品的图文或视频映射到特征向量，并使用两个特征向量夹角的余弦判断两个物品的相似度。如图 2.3 所示，假设一个物品只有一张图和一段文字，那么可以用卷积神经网络（CNN）提取图片特征，用 BERT 提取文字特征，将两个特征向量拼接，输入全连接层，得到物品最终的向量表征。

理想的情况下，如果两个物品的图文内容相似，则两个特征向量的余弦相似度较大。可以用图 2.4 的方式做训练。每次取一个三元组，其中包括种子物品、正样本、负样本，它们的向量表征分别记作 $\boldsymbol{a}$、$\boldsymbol{b}^+$、$\boldsymbol{b}^-$。正样本是指图文内容与种子物品相似的物品，负

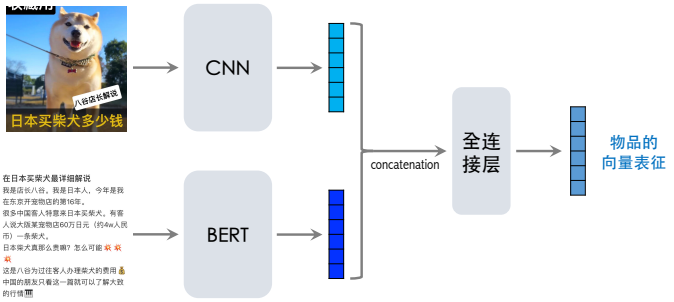


图 2.3: 多模态神经网络将一个物品表征为一个向量

样本是指内容与种子物品不相似的物品。

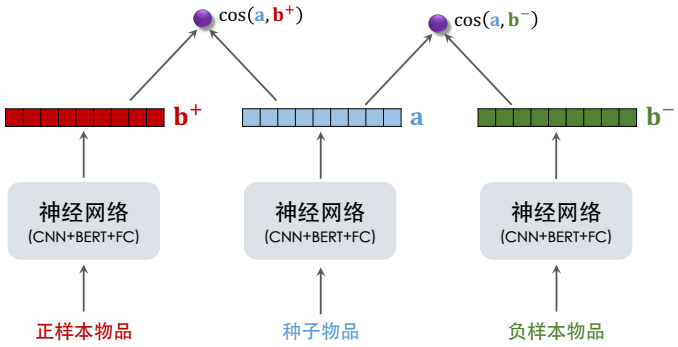


图 2.4: 用 triplet loss 训练多模态神经网络的方法

做训练的目的是更新神经网络参数，使得 $\cos(\boldsymbol{a}, \boldsymbol{b}^+)$ 变大，$\cos(\boldsymbol{a}, \boldsymbol{b}^-)$ 变小。可以使用 triplet hinge loss 作为损失函数：

$$L(\boldsymbol{a}, \boldsymbol{b}^+, \boldsymbol{b}^-) = \max\{0, \cos(\boldsymbol{a}, \boldsymbol{b}^-) + m - \cos(\boldsymbol{a}, \boldsymbol{b}^+)\},$$

公式中的 m 叫做 margin，是需要调的超参数，比如设置成 $m = 1$。也可以用 triplet logistic loss 作为损失函数：

$$L(\boldsymbol{a}, \boldsymbol{b}^+, \boldsymbol{b}^-) = \log\Big[1 + \alpha \cdot \exp\big(\cos(\boldsymbol{a}, \boldsymbol{b}^-) - \cos(\boldsymbol{a}, \boldsymbol{b}^+)\big)\Big],$$

公式中的 α 是需要调的超参数，控制 logistic 函数的形状。

上述方法是上一代的多模态向量表征技术，它的主要问题在于如何选取正负样本。如果靠人工标注，则成本太大，而且训练数据量有限。可以根据用户点击行为（协同过滤）判断两个物品是否相似，但是兴趣点相似不等于图文内容相似。当前最好的方法是 CLIP[1] 预训练方法，前面章节已经介绍过，此处不再赘述。

聚类索引： 在训练好多模态神经网络之后，可以把全量的物品映射到特征向量。然后以余弦作为相似度，对特征向量做聚类，得到 k 个 cluster，比方说 $k = 2048$。每个

cluster 包含内容相似的物品。建立正排索引

$$\text{cluster} \longrightarrow \text{物品列表（按照发布时间倒排）}$$

和倒排索引

$$\text{物品} \longrightarrow \text{cluster}。$$

当一个新物品发布时，用多模态神经网络计算向量表征，然后与 k 个 cluster 中心向量计算余弦相似度，寻找最相似的 cluster，然后添加到上述聚类索引上，排在物品列表的最前面。

线上召回： 线上召回的逻辑是“用户 $\longrightarrow$ 交互过的物品 $\longrightarrow$ cluster $\longrightarrow$ 前 m 个物品”。给定用户 ID，从用户画像取回用户最近交互过的物品，比方说点赞的 last n、收藏的 last n、转发的 last n、一共 $3n$ 个物品。把 $3n$ 个物品叫做种子，用倒排索引寻找每个种子所在的 cluster，然后取回每个 cluster 最新的 m 个物品。这样一共取回 $3mn$ 个物品。

读者可能有疑问：为什么不把种子物品的特征向量作为 query，用 ANN 召回它最相似的 m 个物品？这样不是不可以，但这样有个问题。我们希望召回内容比较相似的物品，但不是非常相似的物品。如果召回的物品与用户已经交互的物品过于相似，比方说首图几乎相同，应当被视作重复物品给过滤掉。

2.3 look—alike 召回

look-alike 起源于互联网广告。假设特斯拉是某互联网平台的广告主，特斯拉知道自己的典型用户是这样的：年龄介于 25 到 35，学历至少是本科，关注科技数码，喜欢苹果电子产品。把符合全部条件的用户圈出来，就是互联网平台上投放广告的对象。假设广告主想给 10 万用户投放广告，但是同时符合条件的用户只有 2 千人，那么该如何做到精准的广告投放呢？可以用 look-alike 人群扩散解决问题。如图 2.5 所示，把符合全部条件的用户称为种子用户，寻找有相似兴趣点的用户，把找到的用户叫做 look-alike 用户。

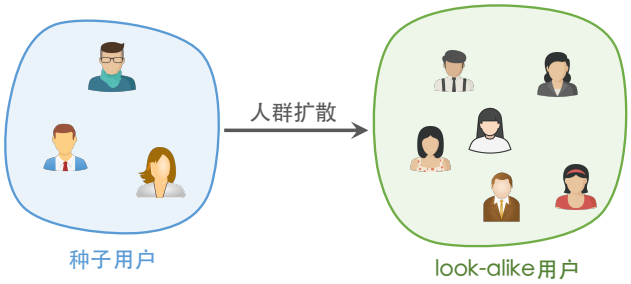


图 2.5: look-alike 的基本想法是人群扩散。

look-alike 只是个大致框架，不是具体算法。想要用 look-alike，需要算法工程师自己定义用户间的相似度。有不同的方法定义相似度。比如用 UserCF，以两个用户共同喜欢

的物品的数量，衡量两个用户的相似度。也可以用双塔模型学到的用户向量表征，如果两个用户向量的余弦相似度大，则判定两个用户相似。

look-alike 可以用于推荐系统的物品冷启动，在小红书推荐系统的落地取得了显著的收益。在推荐冷启动的场景下，look-alike 的主要思想是这样的。在新物品发布后，如果获得了用户的点击、点赞，说明用户对物品可能感兴趣，把这些用户作为这个新物品的种子用户。在选择种子用户的时候，需要设定一个阈值，比方说 $k = 3$。如果对新物品点赞、收藏、转发、评论的用户数超过 k，则不使用点击行为。这样做的原因是交互比点击更能说明用户对物品感兴趣。

如图 2.6 所示，新物品有若干种子用户，用双塔模型学到的用户向量作为种子用户的表征。对这些用户向量取平均，把均值作为新物品的向量表征。把新物品以〈向量，物品 ID〉的形式存到向量数据库，供线上检索用。对于发布 1 小时以内的新物品，每 5 分钟刷新一次索引；对于 1 到 24 小时的物品，每 1 小时刷新一次索引。

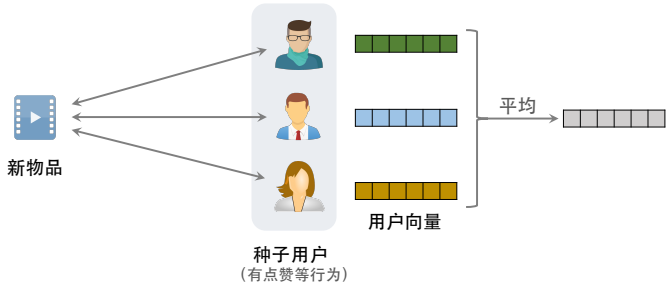


图 2.6: 以用户向量的平均作为新物品的向量表征

如图 2.7 所示，当用户发起推荐请求时，以用户向量作为 query，在向量数据库中做 ANN 查找，寻找最相似的物品。这种方法与 look-alike 有什么关系呢？如图 2.8 所示，右边的用户是发起推荐请求的用户，如果他跟中间三位种子用户相似，则系统判定右边用户对左边新物品感兴趣。这样做推荐，本质与广告的 look-alike 相同，都是根据用户相似度，做人群扩散。

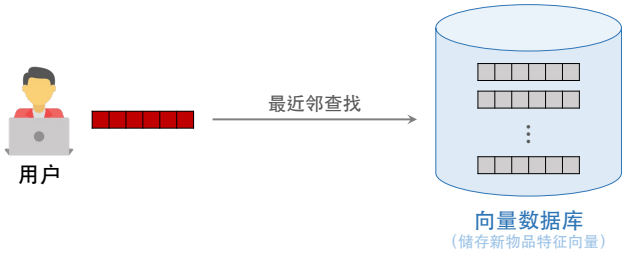


图 2.7: 以用户向量作为 query，在向量数据库中做 ANN 查找

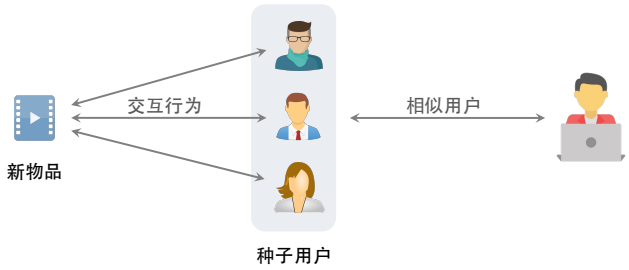


图 2.8: 本节的推荐召回通道的本质就是 look-alike 人群扩散。

look-alike 召回的想法不复杂，主要的难点是工程实现要保证实时性。追求速度的原因是新物品获得的用户交互很少，每一次交互都很宝贵，应该尽快利用到，让下一次召回变得更精准。每当物品获得新的用户交互，就要在尽量短的时间内对用户向量取平均，作为物品的向量表征（如图 2.6 所示）。从交互发生到更新物品向量的时间间隔记作 t_1。新算出的物品向量要进入向量数据库，向量数据库每隔时间 t_2 更新一次索引。那么从发生用户交互行为，到交互影响到物品向量的召回，间隔最多是 $t_1 + t_2$。用工程的方法降低 $t_1 + t_2$ 可以改善 look-alike 召回的表现。

2.4 双塔召回

双塔模型是推荐系统中最重要的召回通道，没有之一。但是将双塔模型直接应用于新物品效果不够好。这是因为物品的 ID embedding 需要通过用户与物品的点击记录学习，在物品的点击次数较少时，物品的 ID embedding 向量还没有学好。

针对新物品 ID embedding 没学好的问题，有几种改进策略。通常来说，神经网络中的 embedding 层将每个物品 ID 映射到不同的向量。default embedding 是一种简单有效的方法，它的意思是让所用新物品共享一个 default ID，而不是用各自真实的 ID。这样一来，所有的新物品共享一个 ID embedding 向量，这个向量是模型学到的。Default embedding 可以带来显著的收益。

另一种显而易见的改进是对双塔模型做实时增量更新，这样可以利用最新的点击信号更新物品的 ID embedding。做增量更新有两个工程上的难点。第一，要搭建实时的数据流，把最新发生的用户—物品交互打包成训练数据，并且实时更新模型。第二，定期发布模型，并用最新的模型计算物品的向量表征，存入向量数据库，并更新数据库索引。上述两部分都会造成延迟，两者延迟之和，就是从发生交互到物品向量更新所需的时间。

此外，还需要对双塔模型的内容池做划分，比如分成全量内容池、≤24h 内容池、≤1h 内容池、≤100 次曝光内容池。这些内容池用相同的双塔模型参数，因此训练的代价不变。划分多个内容池有两个好处。第一，新物品、低曝光物品有更多的机会被召回，从而获得曝光机会。第二，内容池越小，那么更新向量数据库索引就越快，可以减小建索引造成的延迟。举个例子，≤1h 内容池只有 ≤24h 内容池大小的 1/24，因此前者更新索引的

速度远比后者快。

2.5 总结

- 物品冷启动需要特殊的召回通道，让物品在发布初期就能获得曝光机会。在小红书，笔记从零曝光到高曝光，以下召回通道先后发生作用：

  类目召回、聚类召回 $\longrightarrow$ Look-Alike 召回 $\longrightarrow$ 双塔召回、协同过滤召回。

- 物品的曝光和交互发生越早，越有利于作者发布积极性。因此，应该用工程的手段缩短从发布到进入索引的时间间隔。

第 3 章 流量调控

流量调控的意思是如何将流量在新老物品之间分配。小红书的首页推荐分发年龄小于 30 天的笔记。假如让新老笔记自由竞争，那么 <24h 的新笔记约获得 1/30 的曝光机会。但实际上 <24h 的新笔记的曝光占比非常高，远远大于自由竞争应得的曝光。背后的原因是小红书推荐系统做了流量调控，让曝光机会向新笔记倾斜。

本章研究流量调控的技术，即如何给新笔记做扶持。3.1 节介绍流量调控的演化历程。3.2 节介绍流量调控中的保量技术。3.3 节介绍更高级的差异化保量技术。

3.1 流量调控的演化历程

小红书为什么要做流量调控扶持新笔记呢？一方面，流量调控起到激励作者发布的作用。第 1 章讨论过，新物品获得的曝光越多，则作者的发布意愿越强，发布渗透率越高，内容池会变大。另一方面，流量调控起到了挖掘优质物品的作用。假如一个优质物品没有几次曝光，系统也很难发现它是优质物品，不会给它流量倾斜，那么优质物品不会被更多用户看到，无法成长为热门。因此要在新物品的初期探索阶段给它足够多的曝光，比如前 24 小时给至少 100 次曝光。

在包括小红书在内的 UGC 平台，物品冷启动的流量调控通常会有以下几个阶段的发展：强插 → 简单的提权 → 保量技术 → 差异化保量技术。

- 强插是指在重排阶段，往曝光队列中插入新物品，比如隔 3 插 1，这样可以让新物品获得曝光机会。之所以用强插扶持新笔记，是因为排序模型估不准新物品的点击率等指标，无法将新物品与老物品共同排序。强插的效果不佳，但技术落后的公司或业务线仍在使用这种技术。
- 如果粗排和精排模型可以给新物品打出基本可信的分数，那么可以使用简单提权（boost）这种稍微先进一点的技术。推荐系统的链路上有两大漏斗：粗排从召回的几千个物品中选出几百个送入精排，重排从几百个物品中选出几十个曝光给用户。如果想让新物品通过漏斗的几率大于自然分发的几率，可以对新物品的排序分数做提权，即给新物品的排序总分乘以一个大于 1 的权重。简单的提权容易实现，可以用较小的投入获得较大的产出。
- 保量是从互联网广告领域引入的技术，对于激励发布和挖掘高潜有非常显著的效果。在推荐系统物品冷启动的场景下，保量是指通过扶持新物品，使其在发布后前 T 小时内获得 N 次曝光。保量技术有很多种，大多是通过动态提权实现。
- 差异化保量是更高级的保量技术。在物品刚发布时，算法判定物品的价值，并以此决定保量的目标是多少次曝光。差异化保量可以让流量向优质新物品倾斜，提升内容侧指标。

强插与简单提权是非常简单的技术，无需赘述。后面的两节会详细讲解保量技术与差异化保量技术。

3.2 保量技术

保量这个概念来源于互联网广告，英文是 guaranteed delivery。某些大品牌希望让自己的广告在一段时间内获得匀速投放，并达到某个曝光目标，比如 30 天获得 100 万次曝光。推荐系统借用广告中的保量概念和技术，对新发布的物品做保量式的投放，达到激励发布和挖掘高潜的作用。在冷启动的场景下，保量的意思是不论物品质量高低，都要尽量达到一个预设的曝光目标，比如发布后的前 24 小时获得 100 次曝光。

例 3.1

保量目标是发布之后的前 24 小时（目标时间）获得 100 次曝光（目标曝光）。假设采用匀速投放的策略，那么前 6 小时应当获得 25 次曝光。某新物品发布 6 小时后（发布时间）实际获得 10 次曝光（已有曝光），低于预设的保量目标，则应当提高该物品的提权系数，加快它获得曝光的速度。 ♣

定义 $t = \frac{\text{发布时间}}{\text{目标时间}}$ 和 $x = \frac{\text{已有曝光}}{\text{目标曝光}}$ 为介于 0 和 1 之间的变量，用来衡量新物品投放的情况。假如我们希望新物品在目标时间（比如 24 小时）内匀速获得曝光，那么理想情况为 $x = t$。如果 $x < t$，则加大扶持力度，加速曝光。在例 3.1 中，$x = \frac{6}{24} = 0.25$，$t = \frac{10}{100} = 0.1$，那么应当加大扶持力度。然而工业界的实践中发现匀速投放并非最优的策略。以激励发布作为衡量标准，越早的曝光效用越高：同样是 100 次曝光，给在发布后第 1 小时，对激励发布的效用远大于给在发布后第 24 小时。因此，投放速度应该先快后慢、逐渐衰减，这样更有利于激励作者发布。

极简的提权公式。 业内的算法工程师通过摸索，找到一种简单的提权公式，它只依赖于上面定义的 t 和 x：

$$\text{提权系数} \quad = \quad \max\left\{\frac{\alpha}{\sqrt{1+\beta t+\gamma x}},\, 1\right\}.$$

上式中的 α、β、γ 是大于 0 的超参数，需要借助线上小流量实验调整。上式的含义是这样的：对刚刚发布的新物品扶持力度最大，力度随着时间衰减，即提权系数与 t 负相关；物品获得的曝光越多，则扶持力度越弱，即提权系数与 x 负相关。即使新物品曝光次数再多，也不会打压新物品，至少让它的提权系数等于 1，即自然分发。

提前投放（frontload）与投放曲线。 互联网广告通常会采用提前投放的策略，即前期多投，后期少投，这样可以避免无法完成投放目标。设 $y(t)$ 为投放曲线，意思是在时刻 t，我们希望投放量 x 接近 $y(t)$。投放曲线满足微分方程：

$$\frac{d\,y(t)}{d\,t} \quad = \quad \big[1+\theta(1-t)\big] \cdot \frac{1-y(t)}{1-t}.$$

方程中的超参数 θ 表示提前投放的速度，θ 越大，前期投放越快。曲线的初始斜率为 $1+\theta$，然后逐渐衰减。匀速投放曲线是 $\theta = 0$ 的特殊情况。求解该微分方程，得到：

$$y \quad = \quad 1 \; - \; (1-t) \cdot \exp(-\theta t).$$

如图 3.1 所示，θ 越大，则前期投放越快，后期投放越慢。

上文讨论过，物品冷启动也需要做提前投放，其原因是越早的曝光对激励发布的效

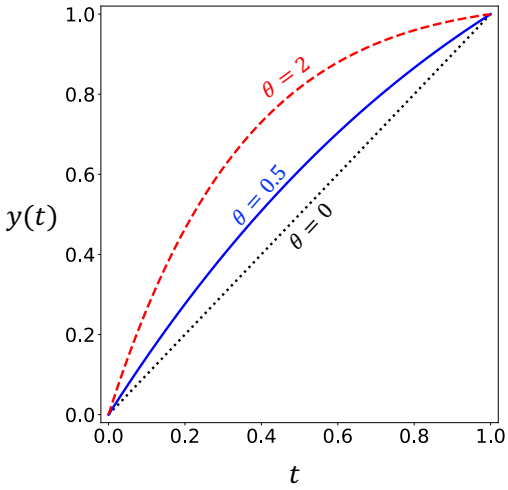


图 3.1: 三条投放曲线分别对应 $\theta = 0$、0.5、2

用越大。因此，物品冷启动可以借用互联网广告中的投放曲线，根据投放曲线决定提权系数，按照投放曲线 $y(t)$ 的节奏给新物品曝光，即让 x 接近 $y(t)$。需要设计一个单调递增的经验函数 $g(\cdot)$，比如 $g(\cdot) = \alpha \cdot \exp(\cdot)$，用它计算提权系数：

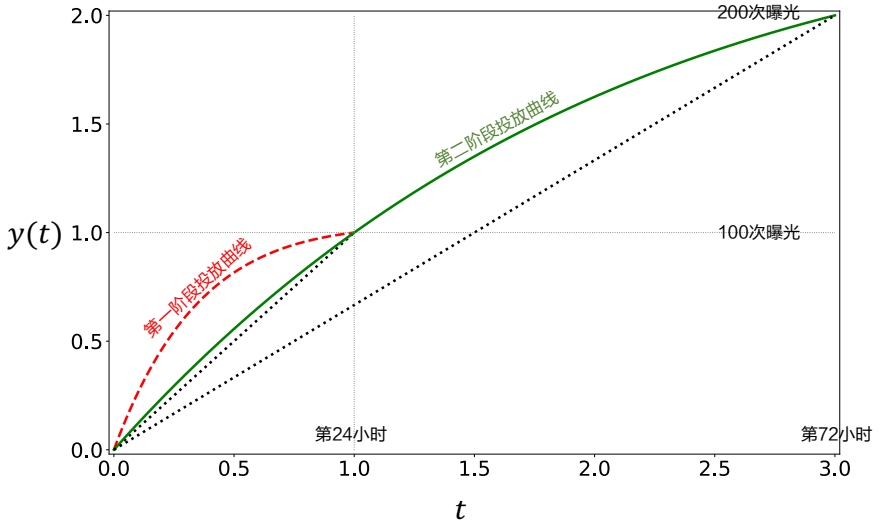
$$\text{提权系数} \quad = \quad \max\left\{g\big(y(t) - x\big),\ 1\right\}.$$

如果实际投放量 x 低于投放曲线 $y(t)$，则应该加速投放，即提权系数更大。但即使 x 远大于 $y(t)$，提权系数也不会小于 1，至少要让新物品获得自然流量。

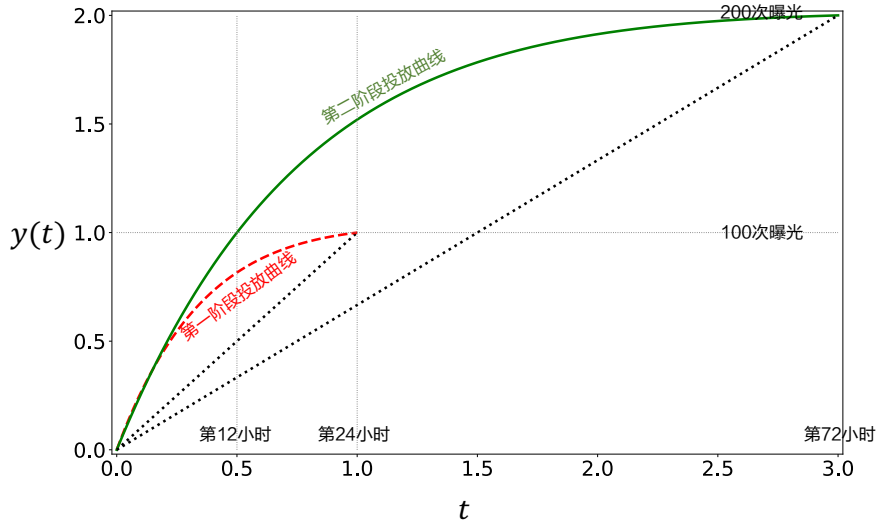
多级保量。 假设保量分为两阶段：第一阶段是前 24 小时，保量目标是 100 次曝光；第二阶段是 72 小时，保量目标是 200 次曝光。在完成第一阶段保量目标之后，立刻开始第二阶段保量。如图 3.2(a) 所示，假设某物品在第 24 小时的曝光次数小于等于 100，那么第二阶段的投放曲线应当通过 $(1, 1)$ 和 $(3, 2)$ 这两个点，这样可以计算图中绿色的投放曲线 $y(t) = 2 - (2 - \frac{2t}{3}) \cdot \exp[-(\ln \frac{4}{3})t]$。如图 3.2(b) 所示，某物品提前达到 100 次曝光，比如在第 12 小时达到 100 次曝光，那么第二阶段的投放曲线应当通过 $(0.5, 1)$ 和 $(3, 2)$ 这两个点，可以相应计算出绿色的投放曲线为 $y(t) = 2 - (2 - \frac{2t}{3}) \cdot \exp[-(2 \ln \frac{5}{3})t]$。有了投放曲线 $y(t)$，就可以根据 $y(t) - x$ 来确定提权系数。

不同时间段差异化投放速率。 在例 3.1 中，物品在凌晨发布，发布 6 小时后，实际的 $t = \frac{\text{发布时间}}{\text{目标时间}} = 0.25$。如果采用均匀投放策略，是否该要求此时物品获得 25 次曝光呢？答案是否定的，原因是夜间流量很小，不容易完成均匀投放的目标。在控制投放节奏时，必须要考虑到不同时间段流量的差距。

我们可以统计每个时间段的曝光次数，以此作为控制投放速率的依据。对发布时间（介于 0 到 24 小时之间）做归一化，用 $k \in [0, 1]$ 表示。对曝光次数做平滑和归一化，用 $f(k)$ 表示，它满足 $\int_0^{24} f(k)dk = 1$，如图 3.3 所示。设 k_0 为发布物品的时刻，k_1 为当前



(a) 某物品在第 24 小时的曝光次数不超过 100



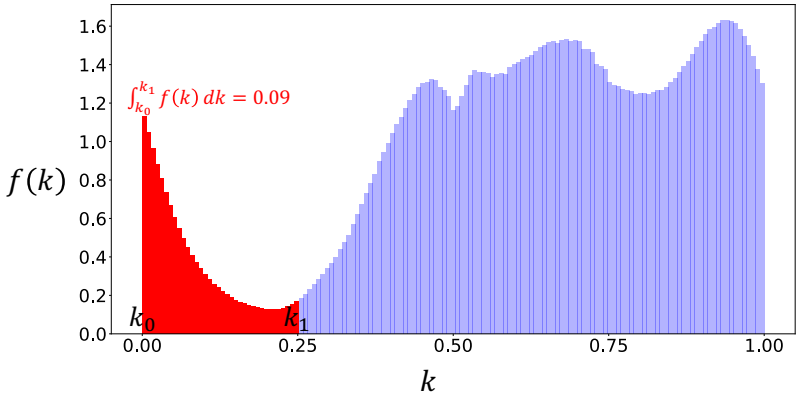
(b) 某物品在第 12 小时的曝光次数达到 100

图 **3.2:** 多级保量的投放曲线

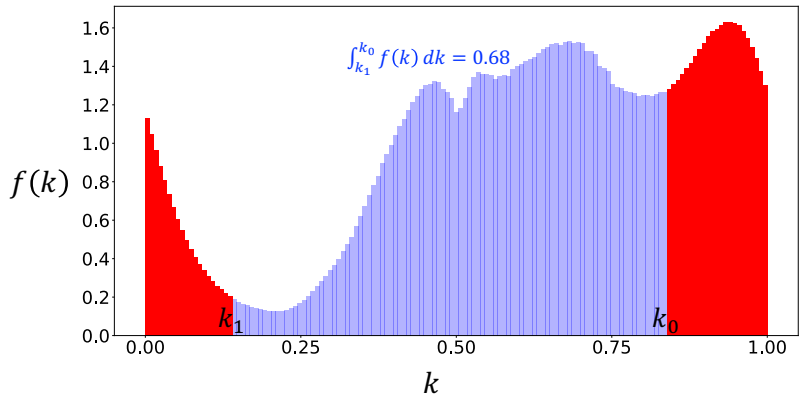
时刻，并计算：

$$t' = \begin{cases} \int_{k_0}^{k_1} f(k)\,dk, & \text{如果 } t_0 \le t_1; \\ 1 - \int_{k_1}^{k_0} f(k)\,dk, & \text{如果 } t_0 > t_1. \end{cases} \tag{3.1}$$

用上式算出的 t' 代替物品实际的 $t = \frac{\text{发布时间}}{\text{目标时间}}$。如图 3.3(a) 所示，设物品是凌晨发布，到了早上 6 点，$t = 0.25$，而 $t' = 0.09$，相当于晚上流量小，因此时钟变慢。如果采用匀速投放策略（即投放曲线的 $\theta = 0$），设定 24 小时保量目标为 100，那么从凌晨到早上 6 点，目标投放量是 $t' \times 100 = 9$ 次曝光，而非 $t \times 100 = 25$ 次曝光。



(a) 某物品在凌晨发布，当前时刻是早上 6 点，算出 $t' = 0.09$



(b) 某物品在晚上 8 点发布，当前时刻是早上 3:20，算出 $t' = 1 - 0.68 = 0.32$

图 3.3: 不同时间段的流量差异显著，在控制投放速度时应当考虑到这一点

保量的难点。 在确定保量目标时，需要做一个简单的算术题。设每日新发布物品数量为 n，如果把保量目标定在 100 次曝光，则平台每日需要将 $100n$ 次曝光用于保量。如果 $100n$ 远小于平台每日的总曝光次数（俗称总流量），那么保量 100 次曝光是可行的，否则需要降低保量目标。事实上，即便 $100n$ 不到平台总曝光次数的零头，保量成功率也无法接近 100%，即有相当一部分新物品无法在前 24 小时获得 100 次曝光。

保量有几个困难之处。第一，召回和排序对新物品优化得不够好，部分新物品难以

被召回、难以通过漏斗。第二，新物品的提权系数优化得不够好，导致部分新物品曝光不足。第三，线上环境不断变换，比如新的召回和排序策略开小流量实验，会干扰新物品获得的曝光量。

如果把新物品提权系数设置得非常大，一旦达到 100 次曝光，就停止提权，这样保量 100 次曝光的成功率会很高，而且实现远比前面讨论的方法容易。但为什么不用这种简单粗暴的方法呢？原因是粗暴提权效果不如精细的提权。提权对新物品既有利也有害。提权可以让新物品获得更多曝光，增加热度。但提权会让新物品被曝光给不适合的用户，不利于点击率、点赞率等指标。如果提权过猛，新物品的点击率、点赞率等指标会偏低，在冷启结束之后会遭到推荐系统的打压，不利于物品持续获得曝光机会。

3.3 差异化保量技术

差异化保量的意思是对于不同的物品，设定不同的保量目标。举个例子，对于普通物品，系统设定的保量目标是 100 次曝光；对于优质物品，系统设定的保量目标是 100 到 500 次曝光。差异化保量是比简单保量更先进的技术，让流量向优质物品倾斜，因此有利于挖掘出高潜物品，可以提升内容侧指标。

第一阶段保量目标。 在物品刚刚发布时，需要给物品设定保量目标。此时物品几乎没有曝光，我们无法根据点击率、交互率、完播率等观测指标判断物品是否优质。我们可以根据物品内容预测物品的高热概率，并把高热概率作为设定保量目标的依据之一。在小红书，我们用多模态模型根据笔记的图文内容预测热门概率，比如点击量和点击率是否能达到 top 10%。模型的 AUC 较高，说明根据笔记内容预测热门概率是可行的。制定保量目标的另一个依据是作者质量。如果作者历史上发布的物品成为热门的概率很高，则他未来发布的物品也有较高概率热门。

下一阶段保量目标。 随着物品的曝光次数增加，它开始获得点击、交互、完播。当曝光次数较多时，点击率、交互率、完播率等观测指标可以较为置信地反映出物品是否优质。在完成第一阶段保量目标后，根据观测指标制定下一阶段的保量目标，制定类似图 3.2(b) 的投放曲线，开始下一阶段的差异化保量。

3.4 总结

- 流量调控是优化物品冷启动的重要抓手之一，它决定流量（即曝光机会）如何在新老物品之间分配。如果流量调控做得好，可以在几乎不伤害用户侧指标的前提下提升作者侧指标和内容侧指标。
- 工业界的流量调控技术经历过这几个发展阶段：强插 → 简单的提权 → 保量技术 → 差异化保量技术。本章重点介绍了保量技术与差异化保量技术。
- 保量技术有助于提升作者侧指标和内容侧指标。本章介绍两种方法——极简的提权公式、投放曲线——它们都可以动态计算提权系数。两种方法计算提权系数的依据都是发布时间、目标时间、已有曝光、目标曝光这四个值。

3.4 总结

- 差异化保量技术有助于提升内容侧指标。通过对物品的点击次数、点击率等指标建模，可以在物品发布时根据它的内容预测它成长为热门的概率，以此制定第一阶段的保量目标。在物品获得一定曝光之后，可以根据它的实际表现，制定下一阶段的保量目标，助力其成长为热门。

参考文献

[1] A. Radford, J. W. Kim, C. Hallacy, A. Ramesh, G. Goh, S. Agarwal, G. Sastry, A. Askell, P. Mishkin, J. Clark, et al. Learning transferable visual models from natural language supervision. International Conference on Machine Learning (ICML). 2021 8748–8763