

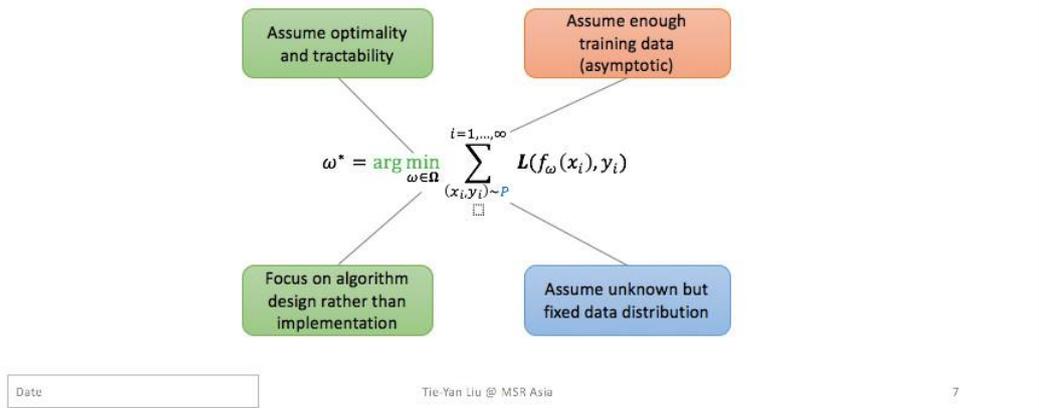
解决现实痛点做有用的研究

——形成机器学习研究的闭环

刘铁岩

今天非常荣幸能和大家分享人工智能和机器学习方面的话题，我报告的主题是“形成机器学习研究的闭环”。这并不是一个纯粹的技术讲座，而是饱含着经验分享，是有关这些年我们如何通过对于机器学习各个侧面进行 360 度的思考，从而形成研究的闭环。

Lessons We Learned: Big Gap between Research and Real-world Applications



让我们通过这个小公式来展开今天的分享。它看似简单，却涵盖了一大类的机器学习问题。这个公式中 x_i 和 y_i 是从某一个分布 P 中采样得到的训练数据样本， \sum 是对训练样本求和， L 是损失函数， f_ω 是需要训练的机器学习模型。机器学习的过程就是在训练数据上最小化损失函数，从而得到一个最优的模型 ω^* 。其实这个过程中，蕴含了一些假设。比如：假设数据分布是事先给定且静态不变的，假设我们有足够的数据可以达到训练的渐进性能，以及假设我们不需要为实际应用中算法的部署和运算复杂度而担忧。然而，当用机器学习来解决真正的现实问题时，这些假设并不成立，我们将会面临很多新的挑战——包括来自数据规模和动态性的挑战，算法易处理性和最优性之间的平衡，以及算法效率和可扩展性的挑战等等。

Motivating Fundamental Research by Real Challenges

Tackling Data Challenges

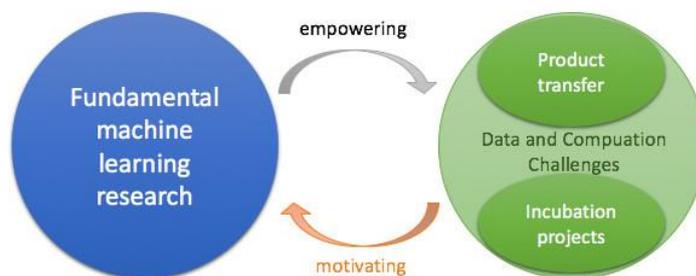
- Data labeling cost
 - **Dual learning**: leveraging structural duality to generate feedback signals for learning, so as to reduce labeling cost
- Data dynamics
 - **Game-theoretic learning**: learning and simulating the dynamics in the learning process (environment or other agents)

Tackling Computation Challenges

- Efficiency
 - **Lightweight and distributed learning**: designing extremely efficient and scalable algorithms
- Tractability and optimality
 - **Coopetitive learning**: trading off tractability and optimality

这些挑战可能大家在写论文的时候可以选择回避,但是当技术要落地、要与产业结合的时候,就无法回避这些问题了。换言之,我们必须以应用难点为动机,摒弃实际中不合理的假设,建立整个机器学习研究的闭环。

We Need to Keep these Challenges in Mind!



Closing the loop of machine learning research

下面我给大家分享几个案例,看看我们是如何从实际挑战中激发研究问题,以及这样的研究又是如何反过来对实际应用有所帮助的。

对偶学习 Dual Learning

[对偶学习](#)解决的是实际应用中训练数据不足的问题。当我们没有充足的有标签数据的时候，想要进行有效的训练，就需要寻找其它信号来驱动训练过程。对偶学习利用的信号是天然存在于人工智能任务之中的，但是很少被人利用，我们称之为人工智能任务的结构对偶性。所谓结构对偶性指的是一个人工智能任务的输出恰好是另外一个任务的输入，反之亦然。例如，在机器翻译中，中英翻译和英中翻译是一对对偶任务；在语音信号处理中，语音识别和语音合成是一对对偶任务。

那么有了结构对偶性，对偶学习是如何进行模型训练的呢？我们以中英机器翻译为例。假设我们只有单语的数据，即无标注的英文文档和无标注的中文文档，和两个能力很弱的初始翻译模型。我们的任务是利用无标注的单语数据不断地学习、提高初始模型的能力，最后得到非常强的翻译模型。

为了实现这个目的，我们可以拿一个无标签的英文句子，利用初始模型将其译成中文，然后再利用反方向的初始翻译模型把这句中文译回英文。通过比较原始的英文句子和翻译回来的英文句子，以及中间的翻译结果的语法和词法，我们可以得到一系列反馈信号，来更新初始模型，周而复始，使之不断提高。当我们有海量的单语数据时，对偶学习可以不断地提升翻译模型的性能，达到很高的水准。[微软亚洲研究院 2018 年 3 月在中英新闻翻译任务上达到了媲美人类的水准](#)，对偶学习就是其背后的秘密武器之一。

对偶学习之所以有效，是因为两个对偶任务背后有着非常强的概率联系——它们的机器学习模型分别对应于联合概率的两种不同的展开方式。正因为这种联系，两个机器学习模型可以互相帮助，使对偶任务的学习更出色。目前，我们已经对对偶学习在有监督、无监督、推断、迁移学习、多智能体学习等各个层面上进行了深入的研究，在学术界产生了一定的反响，很多学者开始将对偶学习的思路应用在他们的目标问题中。

博弈学习 Game-Theoretic Learning

机器学习的另一大挑战，是数据由智能体产生，其分布是动态的，并且会随着机器学习的过程发生变化。智能体之间的互动，可以用博弈论来刻画。然而博弈论也存在自己的局限性，它假设智能体完全理性，而且进行的是最坏情况的分析。

[博弈机器学习](#)就是要取二者所长，得到一个能够解决实际挑战的方法。我们仍然关心智能体的策略行为，但是这种行为是用基于数据驱动的马尔科夫模型加以描述的。具体而言，在博弈机器学习的框架中有两个模型，一个模型用来学习智能体的行为，用它可以预测在未来新的情况下智能体会做出什么样的反应，产生什么样的数据；第二个模型用来解决目标的机器学习问题，它所用的部分数据由第一个模型产生，换言之，我们不再假设所有数据是由预先给定的分布产生的。

我们以广告拍卖机制设计为例来讲解一下博弈机器学习的流程。在广告的拍卖过程中，广告主们会对关键词或者广告位进行竞价，拍卖的胜者将得到广告机会；在这个过程中，广告费和广告的相关性都会起作用。当广告机制在这两种因素之间权衡的时候，广告主会有感觉，并且相应地调整自己的出价以及广告内容，以期获得拍卖的胜利。很显然，广告主的行为数

据是随着广告机制的变化而变化的，而不是从某个固定的分布中采样得来的。博弈机器学习包含不断学习的迭代过程，在广告拍卖机制更新后，广告主的行为会发生变化，我们需要相应地调整行为模型，行为模型再产生新的广告数据，而这些数据会被用来训练新的广告拍卖机制。这个过程不断重复，直到整个过程收敛，得到一个在均衡态下最好的机制。

竞合学习 Coepetitive Learning

竞合学习要解决的问题，是把一个复杂的优化问题转化为局部优化，每个局部问题用一个智能体来解决，并通过局部智能体之间的约束，保证局部优化和全局优化之间有非常强的联系。每一个智能体在做决策时，与其它智能体之间既是共享信息的合作关系，也存在对公共资源的竞争关系，形成合作与竞争并存的机制，最终实现全局最优化。

这一研究的背景是[我们与东方海外航运公司 \(OOCL\) 的合作](#)。在航运的应用场景中，每个港口都是局部智能体，每个港口都要对自己的物流状况作出决策，各个港口之间是上下游关系，有很强的联系；同时它们之间还存在对轮船载重资源的竞争与冲突。那如何有效地建模这种竞合关系呢？首先我们用一个图神经网络来对合作关系进行建模，其次，我们用拍卖来对竞争关系进行建模，通过求解一个次模优化问题，来决定轮船给相关港口分配怎样的资源。通过这种竞合学习，最后我们得到的局部优化和整体优化的结果非常接近，且运行效率提高了多个数量级。

轻量学习 Lightweight Learning

最近这几年，学术界有一种“大力出奇迹”的趋势，用到的 GPU、TPU 越来越多。这种情况不仅会导致学术垄断现象，还会出现一种马太效应，一些研究的边界要通过强大的计算资源才能获取，而且他人没有计算资源就无法复现。

面对这种情况，我们做了一系列轻量机器学习的研究，我们希望告诉学术界，**有时候巧妙的算法比算力更重要，不需要那么多的计算资源也可以解决很大规模的问题**。在我们 2015 年发表 LightLDA 算法之前，最好的 LDA 系统是谷歌的 LDA，用 10000 个 CPU 训练了 70 小时，从文本里抽取出 10 万个主题。我们在算法上做了创新，首次提出了采样概率的乘性因子分解，在 60 小时内可以用 8 台计算机抽取 100 万个主题。

我们发表在 NIPS 2016 和 2017 上的 [LightGBM](#) 算法也提出了全新的优化思路，比如互斥特征捆绑技术和基于投票的轻量级并行框架，这些新技术让 LightGBM 比此前最好的 XGBoost 算法快一个数量级以上，精度也有所提升。LightGBM 开源后，在没有任何宣传的情况下迅速在 GitHub 上获得了 8000+ 星，过去两三年里很多算法竞赛、数据挖掘竞赛的冠军都使用了 LightGBM。由此可见，精巧的算法创新可以降低学术的门槛，让很多人不需要砸钱买上万块 GPU 或者 CPU 也可以做很了不起的大规模的研究。

分布式学习 Distributed Learning

当然，当数据和模型大到一定程度时，分布式运算不可避免。[分布式机器学习](#)也有很多问题值得深究，比如数据如何切分？局部节点之间如何通信？局部节点训练出的机器学习子模型如何复合？每一步听起来简单，做起来都很需要技巧。

比如说通信，最简单的是使用基于 MPI 的同步通信，但在成百上千台机器共同处理一个计算任务时，不能保证每台机器运算速度一致，这时同步通信就好似有短板的水桶，最后整个系统被短板拖垮。近年的热点是异步通信，但异步通信会受到延迟的困扰。当一个很慢的机器把它的陈旧的模型更新同步到全局服务器上时，可能毁掉那个被其它快机器更新了很多次的新模型。为了解决这个问题，我们在 ICML 2017 上发表的一篇论文，首次用数学手段对延迟进行了严谨的刻画，并且提出了消除延迟的补救方法。理论和实验均表明，新方法的收敛性能优于传统的异步通信，在精度方面接近单机算法。

除此之外，在分布式机器学习方面，我们还做了很多其它工作，也对这一领域做了较为全面的总结，整合为《[分布式机器学习：算法、理论与实践](#)》一书，推荐对分布式机器学习感兴趣的读者阅读。

解决现实痛点，做有用的研究

这五个研究方向看似不同，背后其实有共通之处——每一个研究都是来源于实际应用中的痛点分析，弥补了传统机器学习算法和模型的不足。正是因为如此，我们提出的这些新的研究方法，在现实的应用场景中取得了颠覆性的效果。

- 将对偶学习应用于中英机器翻译任务，我们在 2018 年 3 月率先达到了媲美人类的水平。
- 将博弈学习和深度学习应用于智能投资，我们得到了比所有市面上的基金产品的超额收益率都高很多的投资策略，而且在风险控制方面也满足了严苛的要求。
- 将竞合学习应用于集装箱调度，我们不仅在速度上有极大的提升，还能够减少约 10% 的运营成本，这相当于每年节省几千万美金的支出。
- 将 LightLDA 算法应用于微软的广告业务，我们在用户体验没有任何下降的情况下促成了 80% 的利润增长，收到了产品副总裁的高度赞扬。
- 将分布式学习应用于微软 CNTK 平台，我们在训练速度上与其它平台相比有了非常大的提升。

我想通过这五个实际案例向大家展示，如果我们在做人工智能、机器学习研究时，有针对性地去解决现实中的痛点问题，从中发掘关键的挑战，找到技术的难点，那么我们的研究将有机会对现实世界产生非常巨大的影响。所以，**从事机器学习的研究，不能闭门造车，要从实践中来，到实践中去，形成研究的闭环。**