

一文看懂机器学习与大数据风控

备注：来源于雷锋网（2016-11-04 发文）

一个普遍的看法是，机器学习等人工智能技术会最先在金融领域落地。金融行业是最早实现信息化的行业，有丰富的数据积累，且对于用技术提升效率有更多的需求。

现在也有越来越多的公司开始使用机器学习技术实现自动风险管理与放贷。但机器学习在风控中的作用究竟如何，有哪些关键技术，其优势与缺点又有哪些呢？本期硬创公开课，雷锋网邀请百融金服风险总监郑宏洲，来讲讲机器学习与大数据风控的那些事。

公开课实录：

雷锋网：今年人工智能很火，机器学习与深度学习等词甚至被很多非业内人士熟知，那金融行业对机器学习的态度是怎么样的？

郑宏洲：讲这个话题之前，我觉得我们需要先把一些名词稍微界定一下。我们今天讨论的金融行业，主要讨论的是零售信贷行业。机器学习这个概念也比较大，简单的说是利用计算机模拟或实现人类的学习行为，解决实际决策问题的方法论。深度学习属于机器学习中的一种，广义来说，像信贷评分中的逻辑回归等统计方法，也可认为是机器学习中的一种。而我们今天谈的机器学习主要是狭义的概念，即基于非统计原理的数据挖掘方法。

那么信贷行业对机器学习的态度可以说既拥护又谨慎。现代成熟的信贷企业，更多是依赖自动化的方式。例如：信贷风险管理，其核心是量化风险。在量化风险过程中，实际采用了相当多的统计分析技术。以信贷评分卡为例，方法论上和今天讨论的机器学习有很多共通之处，它都是解决分类问

题。只是金融信贷行业可能会从业务的角度去出发，关键是寻找解决问题的方法，对新方法和理论有很多期待，因此金融信贷行业从来对机器学习是拥护的态度。另外一方面，因为金融和货币挂钩，在很多关键技术上的使用上会比较谨慎，对安全性和规范性要求更高，因此从这个角度上看，会表现为对新技术上的谨慎态度。

雷锋网：机器学习在金融中的应用有哪些？

郑宏洲：机器学习在金融中的应用很广，例如：投资领域会用来做量化投资、高频交易；保险行业做营销获客和精算定损；信贷信用管理做信贷评分卡、风险策略等等；信贷反欺诈用它做人脸识别和语音识别等等。机器学习几乎在每一个有数据的场景都有应用。它主要是区别于纯粹人工经验去做决策。

雷锋网：目前来说，机器学习在大数据风控中是怎么样的地位？作用多大？

郑宏洲：我们知道，风控是信贷管理业务中的重要组成部分。风控按形式，可以分为传统人工风控和量化风控。大数据风控是量化风控的一种新形式，出现主要的条件是，现代社会是一个信息社会，在信息和数据上极大的膨胀，这给我们有更全面衡量个体风险的机会。

大数据风控，这是依托于海量的数据去判断借款人的信贷风险，这就决定了它比传统方法更依赖于技术方法去处理，同时大数据时常伴随着高维度稀疏性等特点，这决定了机器学习是实现这一场景的核心方法。

区别于传统风控技术，大数据风控是在方法论上做了相应的革新。风险，即不确定性。风险管理实际上就是做量化风险。大数据风控是将贷款主体各个方面的属性维度做全面风险的量化。它的主流技术渗透到量化风险的整个流程中去，包括贷前、贷中、贷后以及营销获客等全生命周期的管理。机器学习作为大数据风控的显著特征出现，充当着重要的技术更新角色。

通过它去解决传统方法无法解决的问题，它是大数据价值变现的重要工具，机器学习的技术水平在某种程度上是一家大数据公司的核心竞争力。

雷锋网：机器学习用于风控，有哪些较为成熟的技术方案吗，主流的技术途径又有哪些？

郑宏洲：机器学习按大类分监督学习和非监督学习。用于风控领域，实际上这两种都用到了，其中监督学习通常作为主要手段解决问题，非监督学习主要作为辅助方法。对于监督学习中，根据分类器选择不同又形成不同的方法，监督学习中目前比较成熟的，包含决策树、支持向量机、随机森林、adboost、gbdt 等技术方案。而主流的技术，像随机森林、gbdt，目前被业内广泛应用。它们各自适用于不同的具体数据情况，在特定的业务场景上会发挥独特的效果。

雷锋网：您个人比较看好哪些机器学习技术（用于金融领域）吗？

郑宏洲：机器学习仍在发展中，个人比较看好深度学习。目前深度学习主要还是应用在解决非结构数据的分类问题上。例如图像识别、语音识别等领域，包括像我们熟悉的人工智能领域的 AlphaGo。深度学习比其它机器学习能构造出更多的特征层，更有效地发现模式和规律。

每项技术都伴随业务发展需要而体现自身的价值。对应到信贷领域，人脸识别、语音识别被广泛用在反欺诈验真环节。在金融领域，反欺诈实际上有更多机器学习发挥的空间。这是因为反欺诈的特点在于行为的隐蔽性、稀释性。群体坏样本小量但聚集，对传统方法提出了很多挑战，除了验真环节，反欺诈模型上也更适合使用机器学习方法。它对模型的精准度和误判率都有相当的要求，在稳定性上有挑战。

雷锋网：在考虑使用机器学习做风控时，有哪些评判指标及技术指标？

郑宏洲：机器学习的方法有很多，在风控管理上的应用也有很多种场景。对于每一种机器学习技术，其评判的指标和技术标准都不一样。我们下面来举一个常见的应用场景，风险评分，它预测一个事件在未来是否会发生。像这样的场景，无论是机器学习还是传统统计方法，评判指标并没有太大的差别。主要差异是分类器的差别（在分类问题上），区别的是变量，对于结果来讲是类似的判断标准。

这里要讲常见的一些误区，比如凡是风险模型都看 KS，AUC 等指标。经常有人说，某模型 KS 达到 50 或 60，而你的模型 KS 可能才 40，并因此说你的模型不如别人。模型的区分度首先是和样本很有关系，它很容易伪造效果。比如我将模型区分不准的样本做剔除，那么它可能突然可以从很低的 KS 提升到很高。又比如说将业务上的静止客户做剔除，KS 也会有很大的变化。

举这个例子是说，技术指标首先需要在相同的样本下比较才有意义。另外一方面，KS 并不是衡量一个模型好坏的关键要素，只是因为它最直观，可以粗略知道模型的区分度，它的意义类似于变量 IV 值的作用。很多时候模型的稳定性要比 KS 这些指标更为重要，同时还看你业务应用的范围上群体的效果。

雷锋网：机器学习应用于风控，优势与弊端是什么？

郑宏洲：机器学习对于风控来说，优势是带来了新的技术革命。在自动化审批、区分精准度、开发效率等方面都比传统的风控方法有更多的可能性，这是它的优势。而弊端是，新技术在完备性上很多时候还不成熟，很多方法论仍处于探索阶段，在解决方案上没有形成完整的闭环。例如：风控模型的可解释性。传统模型入选若干变量，每个要求有很好的解释性，而机器学习会入选成百上千的变量，这些变量不是很直观。这是任何新技术都会类似产生的问题，它需要时间去探索和修正，可以说道路是曲折的，前景是光明的。

雷锋网：您对机器学习应用于风控模型时缺乏可解释性怎么看？这一问题又该如何解决？

郑宏洲：机器学习应用于风控模型时，缺乏可解释性是一个普遍的问题。

首先，为什么会出现缺乏可解释性？我们说了机器学习风控模型区分度上往往有更好的表现，然而它的问题是复杂度远要高于传统方法，因为机器学习拟合进去更多非线性关系，人类去理解很多非线性规律交织在一起是有难度的，这就造成了我们说的缺乏可解释性的现象。

其次，这种缺乏可解释性可不可取？这里面实际可以再细分为两种情况。非线性关系其中一种可能只是噪音，而另外一种实际的非线性规律。我们在做机器学习时，如果太迷信技术方法的本身，处理太粗糙可能会将更多的噪音拟合进来，这个问题也是很多统计学家通过很多算法不断去调优机器学习算法的初衷之一，并且随着新技术的不断更新会越来越优化。另外一种实际的非线性规律，这就是某些机器学习方法在特定场景下会比传统统计方法效果更优的主要原因。逻辑回归本身是一种广义的线性模型，它放弃了很多非线性的关系。传统统计方法并不是不如机器学习，而是对建模的人水平要求更高，一个建模大师，他也许要费比机器学习更多的精力去做这件事情，但结果仍然可以和最好的机器学习分类方法媲美，并且具备机器学习不具备的优点。

那么既然机器学习好像更容易更快的解决问题，传统统计方法的意义又在哪里？传统统计方法通过牺牲掉一小部分的区分度效果，换取数据的可解释性。实际上是将复杂问题简单化，将复杂的现实世界分解为更为容易理解的模式，这和人理解复杂的现实世界方法是相符的。这种处理方式的好处是业务更容易调整和监控，并且容易避免数据噪音干扰。

部分技术专业人士会觉得把技术做得很好就行了，但如果能把模型做得特别好，一定是技术与业务兼顾。模型实际上是整个风险应用线条上的一个

节点，所有的规律和发现是服务于业务的，这导致不可解释性会没被采用，而会用更容易理解的特征去把握风险。

机器学习的不可解释性实际上无法根本的解决，一般会有两种变通的方式：第一种，将机器学习作为传统方法的辅助，帮忙人去发现数据上难以发现的非线性规律；第二种，分解到单一维度去理解非线性关系。

雷锋网：机器学习做风控中，人工的地位与作用是怎么样的？

郑宏洲：目前一些传统的信贷企业，在规模还较小的阶段，仍存在很多通过人工审批和风控经验去完成整个风控管理。然而当信贷规模庞大的情况下，特别是额度较小的信贷业务，纯粹靠人工去做风控变得很艰难。一方面是成本效率上的问题，进件量大的时候要付出相当多人力成本和时间成本；另外一方面是人工匹配和主观判断容易导致出错，并且在业务优化和积累难以传承。

这些方面都会导致纯人工的方式难以支撑现代的信贷管理模式。另外一个角度，人工的方式实际上也有它的优点，它能在业务开展过程中实现很多感性认识和经验积累，是很多业务特征和模式的发现来源。很多场景下，仍然需要人工去主导做决策。

雷锋网：机器学习能在多大程度上替代人工的思考，在风控中是否会出现机器与人相冲突的情况？

郑宏洲：机器学习在未来能够在很多方面替代人工，但无法全面替代。机器学习是一种技术，是对人工的一部分工作进行优化，这种优化会融合和促进很多人工搭配机器一起工作的方式。

风控管理中可能会存在机器和人相冲突的情况，这种情况需要分开去讨论。在实际业务开展中，机器做的是发现历史的规律，它有很多的适用范围和噪音处理等问题，这时候就需要人去干预，不断优化机器学习的方法

和弥补其不足，所以说我们要求做风控的人才既要懂技术又要懂业务，是一种综合的人才。

而另外一方面，人的行为本身有很多主观的判断，会受情绪等非理性的因素影响，使决策结果失真，这时候机器又能理性地协助人的决策。所以这两者是相辅相成的作用，而不是简单的冲突。当机器和人不一致的情况发生时，往往是发现业务价值的时刻。因此要求风控专家对数据和特征有敏感度。

雷锋网：从机器学习算法到真正应用到产品中，其中需要跨越的挑战会是什么？

郑宏洲：实际上目前很多机器学习已经应用到真正的产品中，而且被大家广泛的使用。比如说人脸识别，比如说推荐算法。而在信贷风控领域，非统计方法的机器学习真正深入人心和被人所接收，则还需要时间。主要的挑战有以下几点：

- 1、传统统计方法仍然是主流的风控方法，业务应用模式适应业务发展，变更意愿不强。
- 2、新技术的不成熟性，新方法可能带来的新问题需要完整的体系去解决。

推动技术更新和应用永远是业务发展，传统的很多方式可能无法满足业务发展，就自然而然会被新方法所代替。例如像传统方法建模时间长，对经验依赖更多等问题，可能会被更高效的机器学习所替代。

雷锋网：百融金服在机器学习的应用上，有哪些实践经验可以分享？

郑宏洲：百融是一家金融大数据信息服务公司，其服务的对象是金融企业。这就决定了在技术探索和业务分析上会有很多的尝试。百融在很多前沿技术上都做过探索和创新，百融有自己的联合建模实验室和机器学习团队。

开发了百融 100brain 机器学习平台，它是一个分布式的纯 R 平台，在这个平台上做机器学习知识的传承和分享。我们内部还举办了各种技术大赛，去验证传统统计方法和机器学习方法的效果优劣。百融在反欺诈领域，我们也采用机器学习的方法，去识别特征异常的群体和规律。同时，我们信用风险领域构建完整的风险评分生态，全面去量化个体在各项信贷业务中的表现。应该说，探索一直在路上，保持不断技术创新的初心。

精彩问答：

逻辑回归可以实现评分分布的好坏比校准，机器学习如何实现？

逻辑回归评分的好坏比校准是一个调整准确性问题，回归输出的内容是预测概率，机器学习同样是有预测概率，方法论上是类似的。两个都可以将预测概率阶段转换成评分，因为校准是在评分刻度校准时实现的，两者是同样的方法论。

如果评分做得比较准，好坏的校准是不频繁的，频繁的校准可能是存在过拟和的问题，这需要在机器学习在分析初期，做变量的预处理和调整，再用机器学习去做。

关于模型冷启动，一般在还没有不良数据的时候，如何设置模型的初始参数？

这种情况下，一般依赖专家评分卡，较好的选择是评分卡有一个类似模式经过验证，如果是完全没经过验证，初始参数比较难以调整到符合业务。这种情况下，初始参数的绝对值没那么重要，因为模型的准确性是很难满足的，但可以关注的是变量维度是否符合业务场景，让初始冷启动模型整体具有排序性，它需要一个不断迭代的过程去实现模型的准确性。

对于风控团队来说，模型人员和策略人员，哪个更重要呢？策略需要经常调整，而模型可以外包出去很久不更新，策略人员不需懂太多复杂高深的算法等等，就可以完成审批、授信、反欺诈等日常业务，是不是风控团队中只需策略人员就可以了呢？

实际上两个角色都很重要。这两种角色分工一般在架构上有两种情况，一种是问题中提到的方式是分开的两个完全独立的团队，另一种是按业务流程搭配在一起。但业务模式和群体没有太大变动的阶段，模型的排序性持续保持，那策略人员不需要太去了解算法，可以完成审批和授信。

但现实中，很多业务发展中，模型会因为模式的变化而波动很大，这时调整策略是不够的，需要两者的整合。这个问题分不同的阶段，跟公司运营模式与所处阶段有关。当整体风险表现稳定时模型没那么重要，而在外包模式下，一旦发生模型变化，很难及时对业务很好的调整衔接。