

# 概率编程能否扭转算法“痼疾”

■本报记者 张双虎

“算法”已悄无声息地“占领”了人们的生活。

前段时间,市场监管总局、国家网信办等七部门联合发布《关于落实网络餐饮平台责任切实维护外卖送餐员权益的指导意见》,其中要求,网络餐饮平台不得将“最严算法”作为考核要求,并通过“算法取中”等方式,合理确定订单数量、准时率、在线率等考核要素,适当放宽配送时限。

而在近日,麻省理工学院(MIT)的研究人员开发出一种新的概率编程语言(SPPL)。开发者称,它可以更准确、快速地评估算法的公平性,相关研究已在美国计算机学会编程语言专业组(ACM SIGPLAN)《编程语言设计与实现国际会议论文集》上发表。

概率编程能否维护外卖送餐员权益,能否解决大数据“杀熟”等算法“痼疾”?

## 概率编程“登场”

麻省理工学院的研究人员发现,司法系统、银行和商家正一步步依赖算法,做出各种影响人们生产、生活的决定。遗憾的是,这些算法有时存在“偏见”。譬如,当有色人种和低收入阶层者申请贷款或找工作时,甚至当法院决定他们在等待审判前该缴纳多少保释金时,都会因算法问题产生不同的结果。

“SPPL针对某些模型进行了优化,因此它能以原来数千倍的速度,提供更公平的解决方案。”该论文第一作者、麻省理工学院电气工程和计算机科学博士 Feras Saad 说。

这种概率编程是编程语言和人工智能交叉的一个新兴领域,旨在使人工智能系统更容易开发。研究者称,SPPL的工作原理是将概率程序编译成一种称为“和积表达式”的专用数据结构,并进一步使用概率电路实现高效概率逻辑的表达。因此,它为概率推理问题提供了快速、准确的解决方案。例如,对“向40岁以上的人推荐贷款的可能性有多大”这样的问题,SPPL可以对可能的推荐对象收入、信用、工作稳定性等分类方式的概率模型进行编码,从而解决不同肤色及社会经济地位者被推荐贷款的概率差异问题。

“理论分析和大规模实际验证均表明 SPPL 是实用的。”波士顿学院副教授、甲骨文实验室前科学家 Jean Baptiste Tristan 说,“由于编程语言的表达能力、精确而简单的语义以及精确符号推理引擎的速度等优势,SPPL 在这类具有挑战性的问题上,有更高的灵活性和可信度。”

## 概率编程虽精确但适用范围有限

“MIT 开发的这个系统是在既有概率编程模型之上,对计算效率机械优化的产物。理论上,这类公平问题大部分机器学习方法都是可解的,只不过统筹解决问题的效率偏低。”清华大学软件学院副教授邓仰东告诉



麻省理工学院的研究人员开发出一种新的概率编程语言,可以更准确、快速地评估算法的公平性。图片来源:unsplash

“机器学习问题的求解通常体现为对概率分布的操作,概率编程使得人们可以直接对概率分布进行计算,从而简化了程序设计。”

《中国科学报》,“相对而言,SPPL 可以实现一部分问题的精确验证,从而保障公平性。”

邓仰东解释说,程序的核心要素是“变量”,传统程序中的变量在一定时间点上取一个固定的数值,该数值由计算流程和输入确定,多次执行时,只要输入固定,其中变量取值也是固定的。但在概率编程中,“变量”可以是服从某种概率分布的“概率变量”。当程序执行到某个时间点,即使其他所有条件都一样,概率变量数值也不是固定值,但其取值遵循一定概率分布。例如,人们取一个高斯概率变量,程序“跑”上万次、几十万次后,如果把把这个变量的取值画成曲线,就可以看到这些取值会分布在高斯钟形曲线附近。机器学习问题的求解通常体现为对概率分布的操作,概率编程使得人们可以直接对概率分布进行计算,从而简化了程序设计。

机器学习有几大流派,包括符号学派(以符号逻辑为基础)、联结学派(以神经网络为基础)、控制学派(以控制论为基础)等。目前影响较大的是联结学派,代表性方法是使用深度神经网络进行机器学习,而且其最成功的应用体现在监督式学习任务中。监督式学

习需要人先给机器学习样本打标签,而该过程就会掺杂主观因素。比如,判断一个人是否好看,亚洲人、非洲人和欧美人会有不同的标准,这就造成了人工智能的“算法偏见”。

“深度神经网络中,样本的偏见是固有的,无法消除也无法验证的。而 MIT 的 SPPL 相对来说验证模型准确,但适用的范围有限。在解决某些概率或机器学习方面的问题上,概率编程确实可以从数学逻辑上验证它是否相对公正。”邓仰东说,“它有利于解决一些能够精确评估概率的公平性问题,例如在金融欺诈预测问题上精确评估数据和模型的准确性,但和我们当前说的‘算法取中’、解决大数据杀熟是两码事。”

## 算法公平仍需通过监管实现

“算法可以通过获得的数据判断人的身份、消费习惯等,如果商家依据此类信息进行差异化营销,对不同的人推荐不同的产品、不同的方案,甚至对部分人屏蔽一些信息等,就会出现大数据‘杀熟’现象。”中国计算机学会秘书长唐卫清对《中国科学报》说,“我个人理

解,技术无法完全解决大数据‘杀熟’的问题,解决这类问题还要靠严格的监管。”

邓仰东同样认为,国内送餐、快递行业目前面临的“严格算法”问题,部分 App 的大数据“杀熟”问题,“本质上不是技术方面的问题,可能还是管理制度和社会监督方面的问题。”

“快递平台进行‘数据压迫’时,它的数据是准确的,是不带‘偏见’的。”邓仰东说,“送同样的路程,大部分人需要 10 分钟,但确实有人能够做到 3 分钟就送达,管理者不能用最快的 3 分钟要求所有的人,不能使用‘最严算法’。”

邓仰东解释说,比如有 20 个快递员,其中最快的用 3 分钟完成,但是所有人完成送件的中间值是 10 分钟。“算法取中”就是用中间值来要求所有人,它肯定比用“最严算法”要求的 3 分钟好很多,更公平一些,但事实上还存在一些问题。

“中间值是 10 分钟完成,就是说有 50% 的人在 10 分钟完成,还有另外 50% 的人 10 分钟是不能完成的。”邓仰东说,“假如所有的快递员都努力加快速度,都在 10 分钟之内完成了,那么这个‘中间值’就又变了,这同样会造成要求越来越严格。所以‘算法取中’只是相对好些,并不能解决所有的问题。”

邓仰东认为,解决网络平台对快递员的“数据压榨”及 App 的大数据“杀熟”等问题,还需要监督和制衡的机制。快递平台也需要有激励和考核办法,如果中间值取得太高,可能会导致整体送餐效率降低,消费者满意度会下降。这实际上是三方的一种博弈,要兼顾消费者、快递员和数据平台的公平和效率问题,需要监督和制衡的机制来解决。

8 月 17 日,十三届全国人大常委会第三十次会议在京召开,审议个人信息保护法草案(三次审议稿)(简称草案三审稿),后者对大数据“杀熟”等问题作出规制。

“当前,社会各方面对于用户画像、算法推荐等新技术新应用高度关注,对相关产品和服务中存在的信息骚扰、大数据‘杀熟’等问题反应强烈。”全国人大常委会法工委发言人臧铁伟在日前举行的记者会上表示,个人信息保护法草案立足于维护广大人民群众的网络空间合法权益,对利用个人信息进行自动化决策作出有针对性规范。

草案三审稿规定,利用个人信息进行自动化决策,不得对个人在交易价格等交易条件上实行不合理的差别待遇。同时,充分赋予个人自主选择是否接受自动化决策的权利。

此外,草案三审稿还对大型互联网平台和小型个人信息处理者进行了区分,规定大型互联网平台应当遵循公开、公平、公正的原则,制定有关个人信息保护的规则;授权网信部门针对小型个人信息处理者制定相关规则。

相关论文信息:  
<https://doi.org/10.1145/3453483.3454078>

# 中国自主研发求解器首获国际 SMT 比赛冠军

本报讯(记者胡珉琦)近日,形式化验证顶级会议 CAV 2021 会议公布了第十六届国际可满足性理论验证比赛(SMT-COMP 2021)结果,中国科学院软件研究所研究员蔡少伟带领团队研发的求解器获整数差分逻辑(QF\_IDL)组冠军。这也是中国队首次在 SMT-COMP 比赛中获得冠军。

“可满足性理论问题(SMT)是特定背景理论下的一阶逻辑公式判定问题,是计算机科学和人工智能研究的核心问题之一,SMT 求解器也是形式化验证的基础引擎。”蔡少伟表示。

会使用高级语言(如 Pascal、C)编程的人,一定不会对可满足性问题感到陌生。在编程语言中,用于条件语句的布尔表达式由变量通过运算符以及“与”“或”“非”等逻辑连接符组合而成,给每个变量一个值,很容易判断出整个表达式是否为真。但反过来,给定一个表达式,是否能为每个变量找到值,使得整个表达式成真?这就是 SMT 的一种形式。

蔡少伟介绍,作为一种工具,SMT 求解器在工业领域尤其是软硬件验证中具有广泛的应用。比如 Windows 操作系统驱动程序的验证就用到了 SMT 求解器。

在此次 SMT-COMP 比赛中,蔡少伟团队自主研发了基于 DPPL(T)和随机搜索混合的方法,打破了传统 SMT 求解器框架,在强数值约束的差分逻辑算例中取得了显著效果。

据悉,该研究团队长期从事约束求解器研究,进行 SMT、命题逻辑可满足性问题(SAT)等计算机科学经典问题求解算法及工具的研发,并在相应领域国际大赛中多次获奖。其提出的约束求解技术和研制的 SAT 求解器已应用于华为公司的电路验证、腾讯地图优化、微软 Azure 云平台的虚拟机预配置和异常检测,以及美联邦通信委员会的频谱分配等项目。

## 速递

### 国务院公布《关键信息基础设施安全保护条例》

本报讯 日前,国务院公布《关键信息基础设施安全保护条例》(简称《条例》)。该《条例》将于 9 月 1 日起施行。

《条例》对关键信息基础设施认定、运营者责任义务、保护部门开展工作,以及相关法律责任认定给予详细说明。

《条例》指出,任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动,不得危害关键信息基础设施安全。运营者应当优先采购安全可信的网络产品和服务;采购网络产品和服务可能影响国家安全的,应当按照国家网络安全规定通过安全审查。(袁一雪)

### 华科师生团队获 2021 年图计算挑战赛冠军

本报讯 日前,华中科技大学计算机学院服务计算技术与系统教育部重点实验室组建的图计算团队获 Graph Challenge 2021 冠军。Graph Challenge 是图计算领域最具影响力的国际赛事之一,已举办五届。这是国内团队第一次在该赛事中获得冠军。

Graph Challenge 2021 包括静态图匹配、动态图划分和稀疏神经网络推理三个赛道,分别代表了图计算的不同典型应用场景,吸引了赛灵思、英伟达、劳伦斯利弗莫尔国家实验室、弗吉尼亚理工大学等国际知名高校、科研院所参赛。最终,华中科技大学和美国马里兰大学帕克分校两支参赛团队获得冠军。

华中科技大学参赛团队从去年年底开始备赛,选择稀疏神经网络推理作为主赛道,为加速人工智能应用提供新方案。这个赛道的任务是将神经网络的权重数据抽象为图数据,执行推理任务,是人工智能领域的典型应用场景。

图是一种用来建模事物之间关系的一种数据结构,可以应用于生产生活中的各个领域,从社交媒体、网页排序到科学计算、人工智能,都可以用图来表示。这些应用需要被快速处理,而图结构的不规则性则让这一目标变得很难。因此,图计算成为大数据和人工智能时代的核心挑战。(李芸 赵娜)

### “数字中国 2021 技术年会”云上开幕

本报讯 近日,由神州控股、神州信息、神州数码集团联合主办的“科技自强、数据融通、场景创新——TECH 数字中国 2021 技术年会”云上启幕。与会专家围绕云原生、数字原生、金融科技等技术话题发表精彩演讲。

会上,神州信息与华为公司携手发布了“分布式新核心联合解决方案”。该方案基于华为混合云底座包括鲲鹏服务器、高斯分布式数据库等,提供可靠和高效的平台;神州信息提供核心账务服务包括存款、贷款、支付、网贷、商城等各种互联网业务,以及定价工厂、产品工厂等基础组件,并且通过开放 API 帮助客户高效便捷地连接全场景。

当天,三家主办方还联合发布了“神州信创云”。神州信创云为企业数字化转型打造全栈自主可控底座,提供整体信创云规划及建设服务能力,助力企业实现数字化变革和价值创造。神州信创云整体能力框架由能力底座、能力引擎、能力中枢和能力市场四层组成,将持续整合数据化资源,扩展更多的生态和创新。(郑金武)

# 数字孪生：用虚拟优化现实

■冯瑞

近年来,“数字孪生”概念正逐渐走入人们的视野。这个在上世纪 70 年代美国国家航空航天局(NASA)计划中提及的概念,直到 2010 年才正式在 NASA 另一个报告中给出了明确的定义:将真实世界的事物构建成为虚拟孪生体的空间,并对现实空间或物理空间进行指导和优化的过程。

经过多年发展,数字孪生已逐渐成为实现物理世界和数字空间双向交互的新范式。而随着其与人工智能、大数据等技术深度融合,数字孪生也成为全球信息技术发展的新焦点。信息技术研究和咨询公司 Gartner 曾连续 3 年把数字孪生列为十大战略科技发展趋势,并认为未来 5 年它还将产生颠覆性的创新。

目前,数字孪生已经上升为全球主要国家战略,各国纷纷重视其发展,加速推动制造业进入数字化和智能化的时代。例如,由美国国防部主导建立的国家数字化制造与设计创新中心,在 2018 年就把数字孪生列入战略投资重点;德国工业 4.0 也把数字孪生作为重要内容;英国在 2020 年发布国家数字孪生体原则,目的是统一各个行业对于数字孪生开发的标准,提升不同数字孪生体之间数据融合的价值。

我国也不例外。2020 年 4 月,国家发改委与中央网信办共同发布《关于推进“上云用数赋智”行动 培育新经济发展实施方案》,将数字孪生列为七大新一代数字技术之一,并提出数字孪生体创新应用,以期促进数字孪生的发展以及在先进制造业或者制造领域的创新应用。

由于数字孪生在制造业领域愈发受到重视,所以它成为我国新基建的重要组成部分,更是建设新型智慧城市的重要技术手段。目前,上海市、广东省与海南省等多地纷纷推出政策支持数字孪生发展,支持探索建设数字孪生城市。例如,雄安新区就率先提出打造全

球领先的数字孪生城市;上海市也面临数字孪生的重大发展机遇。目前,上海市正在进行城市数字化转型的工作与新型智慧城市和平安城市的建设,将为数字孪生发展提供更加丰富的应用场景。

有了政策,还需要考虑“政策落地”问题。笔者认为,数字孪生要更好地应用到国家发展中,离不开企业的支持。当然,学界是研究数字孪生的基础,企业却是其发展的核心,只有搭建两者间的合作桥梁,才能让数字孪生更好地发展。

而不论是哪一方研究与发展数字孪生,都需要从顶层设计开始。笔者认为,顶层设计中需注意以下几个问题。

首先,是关键共性技术的问题,即要先突破精准建模以及超大规模计算的技术。若有所突破,就要加强数字孪生基础理论和基础研究,促进数字孪生数据闭环的形成。

同时,要加强数字孪生工程应用技术的研究,促进智慧城市、平安城市重点领域的创新应用,还应面向数字孪生城市重点在交通、社区、服务等领域实现规模化落地,进而打造城市规划新模式。

其次,针对每个构建层所必需的基础软件依赖国外的问题,我国需要加强基础设施建设,比如高性能公共计算中心等。同时,要打造大规模知识库、模型库以及算法库,相关技术标准分析也需要进一步突破,并建立数字孪生不同模型之间统一的方法论。

除了上述问题,数字孪生评价体系指标以及科学统计体系方面还存在缺失,相关政策缺乏对数字孪生发展的科学规划和引导。而对于监管部门来说,数字孪生所涉及国家敏感的地理信息、数据安全与新的经济运转模式,都为其带来新的挑战。

眼下,数字孪生从最初集中于制造业单一应用领域,向大尺度、跨领域融合发展。譬如,随着数据量的不断加大,数字孪生城市模



蒋志海制图

“数字孪生从最初集中于制造业单一应用领域,开始向大尺度、跨领域融合发展。不仅如此,数字孪生还正在从对物理世界镜像映射转向多模型动态的反映。”

型将对模型建立的精度和效率提出更高的要求。不仅如此,数字孪生还正在从对物理世界镜像映射转向多模型动态的反映。

至于跨领域方面,数字孪生显然是各大技术的集大成者,例如数据模型会涉及到人工智能的技术,甚至包括数字孪生里非常重要的智能决策。人工智能的加入无疑会提高智能决策的可靠性、稳定性。