13 AI 医疗

中国工程院院士董家鸿：智慧医疗——大健康，新生态

整理：智源社区 苗洪江

在第二届北京智源大会的 AI 医疗专题论坛中，中国工程院院士、清华大学临床医学院院长、精准医学院院长董家鸿做了题为“智慧医疗：大健康，新生态”的演讲。

董家鸿，肝胆胰疾病精准外科治疗、肝脏移植方面的专家，同时也是美国外科学院 (ACS) 院士、法国外科学院 (FAC) 外籍院士、国际肝胆胰协会（IHPBA）学术委员、国际消化肿瘤外科医师协会（IASGO）执行委员。

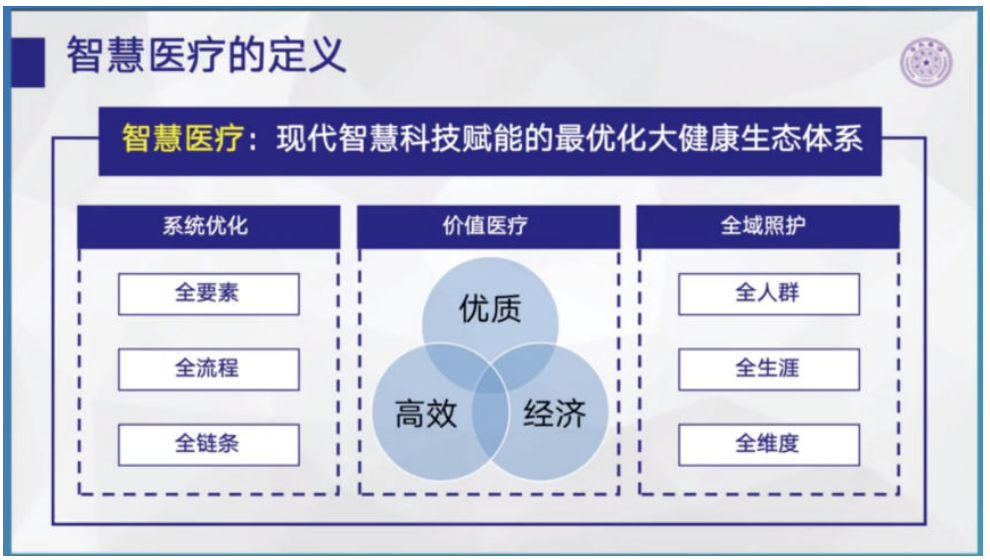


图 1：智慧医疗的定义

董家鸿提到，智慧医疗是现代智慧科技赋能的最优化大健康生态体系，通过全要素、全流程、全链条的系统优化，能够达到全人群、全生涯、全维度的全域照护，最终实现优质、经济、高效的医疗。同时，董家鸿提出了增强健康医疗服务技术能力 (Enhancement)、提升医疗服务效率效能 (Efficiency)、优化医疗服务体验 (Experience)、拓展医疗服务的时域、空域和领域 (Extension) 的“4E 效应”，从而实现精准医疗、精诚服务、精益管理的“三精”医疗为核心理念的价值医疗。

智慧医疗具有丰富多彩的应用场景，能够从健康管理、疾病预测、医学影像分析、辅助诊断、药物研发、精准用药、自动稽查审核、医院绩效管理等多层面全方位地为当前健康医疗的困局提供解决方案，是解决我国医疗工序矛盾、提高成本效益的必由之路。对于重塑未来医疗体系、实现以人为本的最优化医疗服务体系具有重要价值。

我国医疗目标人群庞大、场景多样，人工智能和大数据学科发展迅猛、转化应用高效，在国家政策强有力的推进下，智慧医疗逐渐形成了贯穿诊前、诊中、诊后的健康管理体系。预计到 2030 年中国数字医疗的市场规模将达到 2–7 万亿人民币，占整个医疗行业收入的 45%。

董家鸿也认为，在智慧医疗蓬勃发展的同时，我们更需要理性思考其发展策略和方向，不盲目跟风，牢记以治病救人为本的宗旨，以智慧技术直击医疗痛点，实现“4E 效应”。在产业应用中，清华长庚医院国产化脑起搏器、世界首例精准 3D 打印高位骶骨、清华大学医院智能精准肝胆手术规划系统、国家肝胆疾病标准数据平台、5G 驱动的无线医疗等十余个案例则是“4E 效应”在实际应用里的体现。

对于目前智慧医疗面临的挑战和可行性应对措施，董家鸿提出了以下几点： 首先，AI 技术的黑箱效应难以用人脑的思维逻辑进行解释，在应用于医疗时需公开其执行细节，如训练集的性质、目标边界的界定等，并对医师进行充分的培训； 医疗 AI 同样受到学习集框架的限制，因此相关研究的规范化和审批尤为重要；AI 与医生应不应该是竞争关系，而是应该形成一种人机共存、人机增强的模式，让医生站在 AI 的肩膀上，为患者提供最佳的医疗服务体验、营造有温度的医院。

图 1： 国家政策助力智慧医疗

在过去五个月里，智能医疗临危受命，赋能抗击疫情最前线取得的卓越成绩。清华大学不仅派出智慧医疗团队驰援武汉，而且多院系联合推出了 COVID-19 智能防控全息系统，该系统囊括了自测评估、辅助分诊（服务超 95 个国家、辐射用户超 3 亿）、智能诊断辅助（灵敏度 99.3%）、移动生理参数检测、隔离病房巡诊机器人、消毒机器人、远程集成协同诊疗平台、康复病人智能护航等，每一项子系统都成绩斐然。

最后，董家鸿分享了对智慧医疗带动全生态体系创新的展望： 科技将推动需求和供给的双侧革新，改变中国的医疗模式，促进整个医疗健康行业运营模式的转型。同时，他也为大家概括了清华智慧医疗的发展蓝图： 推进特色医工融合，打造新型智慧医院，实现“4E”应用效果，构建“三精”医疗体系，助力健康中国伟业。我们相信 AI 将为医疗插上智慧的翅膀，助力实现健康中国的宏伟梦想，完成中国民族的伟大复兴。

在问答环节中，董家鸿认为，智慧医疗的新技术如何高效的让使用者认知、得到管理者认可同样是需要 AI 从业者关注的问题，其中数据标准 / 接口难以共通，数据隐私脱敏都是需要大家努力解决的难题。

国家神经系统疾病临床医学研究中心副主任王拥军教授：脑血管病的人工智能——从临床到临床

整理：智源社区 李雪菲

国家神经系统疾病临床医学研究中心 副主任、首都医科大学附属北京天坛医院常务副院长王拥军教授的报告主题是《脑血管病的人工智能： 从临床到临床》。王拥军认为，医学人工智能要以解决临床问题为导向，以标准和高质量数据库为开发基础，重点验证对临床和患者的帮助效果，即以临床为主导、技术深度参与。

在报告中，王拥军介绍到，脑血管病位列中国居民死因第一位，其疾病负担日趋升高（如图 1 所示）。

脑血管病的医疗是一个连续的过程，从患者发病、入院前急救，到进入急诊室、住院治疗，最后回归社区，整个医疗过程都需要高质量的医疗照顾，才能改善患者预后。而所谓的高质量医疗是指把目前已有的技术，如临床指南，运用到临床实践中。但是，目前临床指南和临床实践之间存在着巨大的鸿沟，亟需发掘提高医疗质量的科学方法。而最好的方式就是融合人工智能与专家的经验建议弥补鸿沟，进而提高脑血管病的医疗质量，降低中国脑血管病的疾病负担。

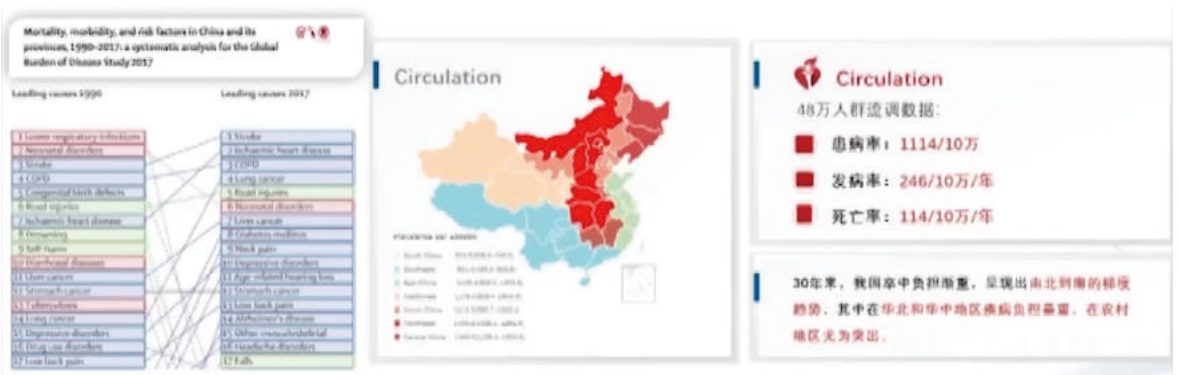


图 1： 中国脑血管病病负担日趋升高

一、从临床到临床

涉及脑血管病治疗的人工智能系统主要关注脑血管病的急性期治疗及病人的长期管理。目前在这个领域中，国际上最炙手可热的人工智能公司有三家： 美国的 RAPID、Brainomix 以及 iz.ai。它们的主要产品都涉及到在急性发病期用正确的方式帮助医生识别可以挽救的病人。其中，目前国际上最具引领作用的就是 RAPID，它是从临床需求开始研发新产品，并通过临床试验、推荐进入临床指南。

我们通过 RAPID 的成长之路机器现在的主要动向可以了解脑血管病人工智能的发展。RAPID 最早是用于帮助急性脑梗死患者识别可挽救脑组织（如图 2 所示）。

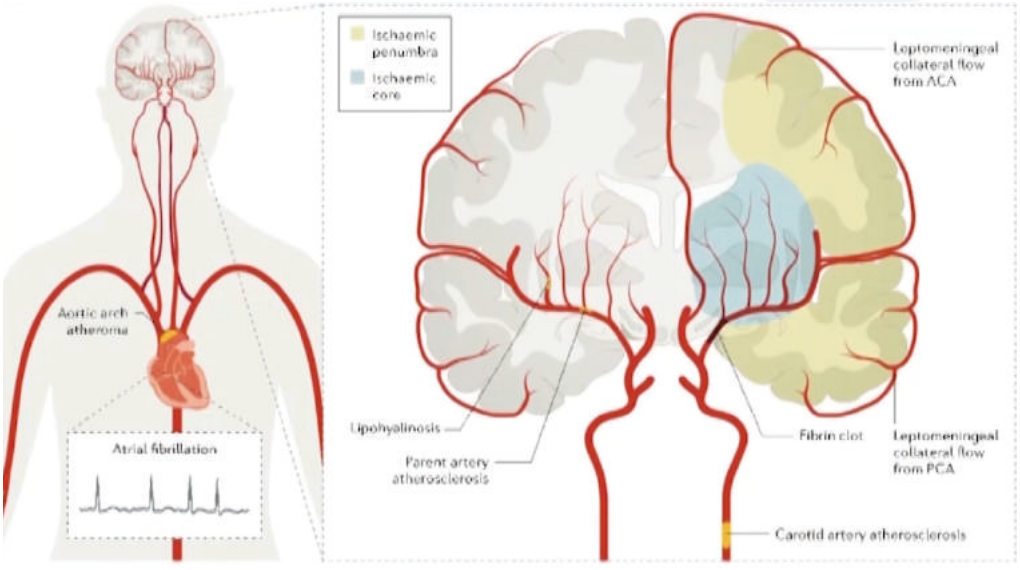


图 2：识别急性脑梗死患者可挽救脑组织

RAPID 的主要推进人是一位临床医生 Gregory W. Albers，斯坦福医学中心卒中中心主任，(图 3)。2008 年，Albers 教授开发出了 RAPID 帮助临床医生快速识别半暗带，同时得到了瓦伦丁红杉资本投资，RAPID 得以市场化；2009 年，Albers 教授拿到美国 NIH 的项目，使得 RAPID 软件迅速在美国和欧洲投入使用，并进入临床研究；2012 年，Albers 教授注册了一家公司，并从斯坦福大学购买了 RAPID 软件技术，利用独立资本进行开发； 同年，DEFUSE2 发表文章证明了 RAPID 软件可以很好的预测临床预后，帮助医生解决临床问题，同时，RAPID 运用在了当时国际上大型的临床试验中，这些临床试验奠定了现在脑血管病临床研究的基础，也使 RAPID 软件在 70 多个国家得到推行。

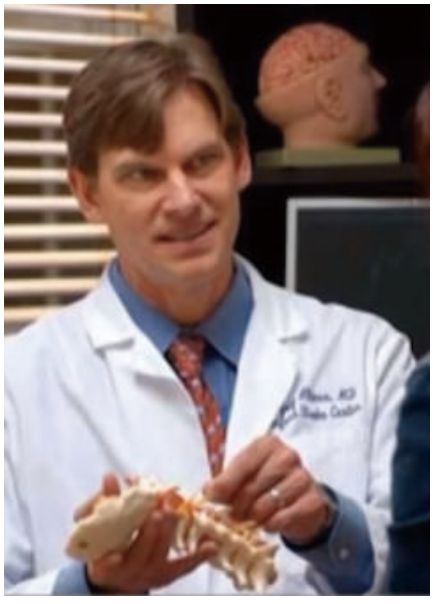


图 3：Gregory W. Albers，MD

2013 年，RAPID CTP 和 RAPID MRI 通过了 FDA 批准，允许在全美医院进行使用；2014 年，临床正式使用 RAPID 软件识别半暗带；2015 年，《美国指南》和《国际指南》把发病 6 小时内的取栓治疗列为新的治疗金标准，RAPID 软件覆盖超过 100 家医院；2016 年，RAPID 软件资助把黄金 6 小时向外进行了扩展；2019 年，在 RAPID 阮软件的支持下，《美国指南》和《国际指南》借助两个大型临床试验成功将 6 小时向外扩展到 24 小时；2020 年，RAPID 软件在全球超过 1500 家医院投入使用，帮助 65 万患者进行临床治疗。

人工智能的研发以临床为起点，也以临床为终点。最初需要考虑临床需求，依靠相应的数据库和标准进行临床试验，从而得到监管部门的批准，最终进入临床指南。

二、脑血管病诊疗辅助决策系统

2019 年，国家中心推出“天泽”系统，如图 4 所示，但由于没有临床效果评价，因而还未进行大规模的推广。这个系统主要有三个功能：AI 影像分析、自动化病因分型以及指南意见推荐。

具体来说，“天泽”系统首先通过 AI 影像分析，发现供血区域推测病因，同时自动识别血管狭窄，然后给出完整的发病机制诊断清单，最终为病人提供个体化治疗决策。目前，国家中心推出金桥工程 2 去证实“天泽”系统的效果。金桥工程 2 是一种多中心、开放标签、平行、整群随机对照的干预研究，能比较患者最终的治疗效果。

图 4：“天泽”系统

首都医科大学附属北京同仁医院王佳伟：神经感染免疫疾病与联邦学习创新平台的建立

整理：智源社区 詹好

在第二届北京智源大会的 AI 医疗专题论坛上，来自首都医科大学附属北京同仁医院神经内科主任兼医院中心实验室主任王佳伟，做了名为《神经感染免疫疾病与联邦学习创新平台的建立》的演讲。

一、创建创新平台的意义

在演讲的一开始，王佳伟首先介绍了神经感染免疫疾病与联邦学习创新平台的建立意义。王佳伟指出，在常见的危重感染中，大约 90% 的病因是不能完全明确诊断。由于不能明确诊断，治疗容易受到影响，导致致残率和致死率的上升。

例如，在脑膜炎和脑炎的临床分型当中，常见的有感染性和免疫性的，以及有癌性的脑膜炎；而在感染性的脑膜炎当中，有病毒感染、细菌感染、真菌感染和寄生虫等不同的病源种，大概有近万种的病源体。在免疫性疾病当中，有抗神经元表面的受体的自身免疫性脑炎，也是涉及近百种不同的抗体；有癌性脑膜炎，原发的，或继发的，很多种都跟肿瘤有密切的关系。

图 1：脑膜炎和脑炎的临床分型多种多样

在临床诊断当中，特别是神经系统感染性疾病，传统的诊断技术——如细胞的染色、细胞的培养、病毒的培养、细菌的培养、ELISA 方法，PCR 方法等——对于病源学的诊断，其实是远远达不到临床医生要求的。而由于病源学的追溯不明确，就导致了诊断的不明确，最终引起了致残率和致死率的上升。这就对于新的方法和技术提出了需求。

随着下一代测序技术的发展，特别是蛋白芯片、组学的芯片、免疫技术的发展，这一问题逐渐得到了解决。采用高通量，高敏感的技术，可以大大提高临床感染性疾病的诊断率（目前可以达到 40%）。

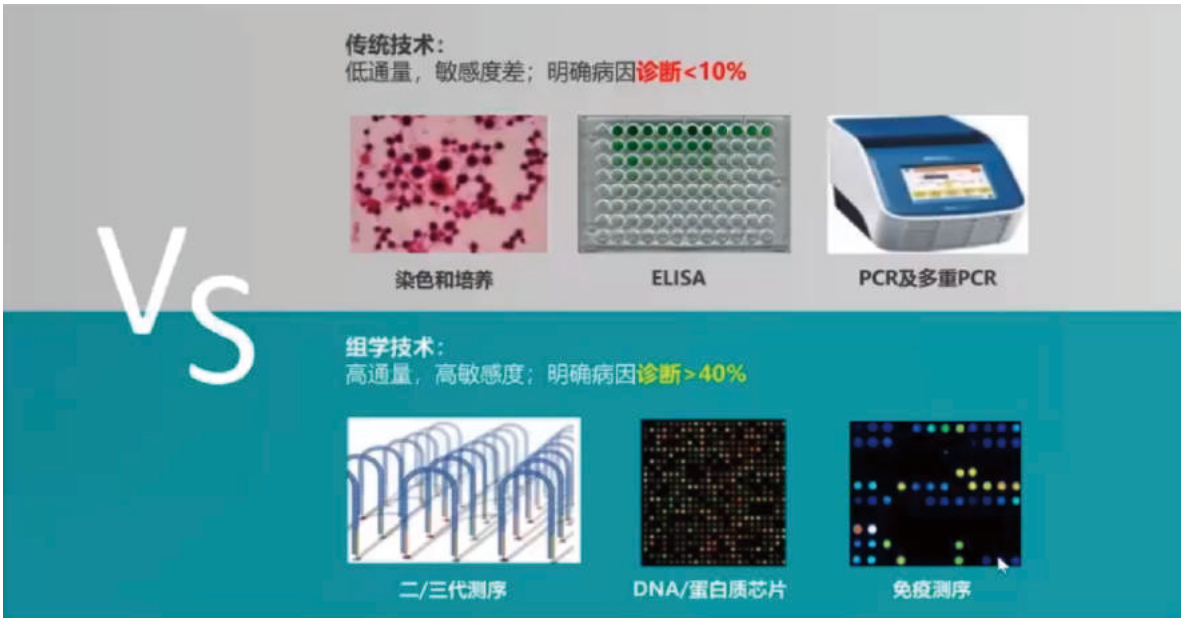


图 2：传统诊断技术 VS 组学技术

作为一个神经感染的专科医生，不但要明确病人感染临床的表现，如发热、头疼、癫痫、意识改变等，还需要查看病人有没有脑膜征、脑和脊髓的改变，同时还要取病人的脑脊液来看看中枢神经系统有没有感染。这对于鉴别不同的脑炎具有重要的意义。

王佳伟指出，从常规的诊断到经验性治疗，到精准的诊断和精准的治疗，这不仅是一个临床的技术的改进，同时也是从传统的诊疗模式，向数字化诊疗模式的改变，这就为人工智能的推进和采用提供了一个非常有力的依据。这是建立神经感染免疫疾病与联邦学习创新平台的首要意义。

创建平台的另一意义，与病人的临床数据有关。由于只有将病人的临床症状、体征、常规检查，以及基因组学大数据检测结合在一起，才能实现对疾病的精准诊断和正确治疗。除此之外，一些相关的高科技公司，也收集了包括免疫组学在内的很多微生物组学的数据。

然而，这些在现实中，我们通常很难同时使用这些数据，主要是出于在临床方面，对病人安全性及隐私的考虑。特别是这次新冠病毒疫情爆发以来，常常会出现在数据安全与数据隐私领域的纠纷。

例如，我们平时所使用的健康宝或其他一些软件，它们收集了检查对象的大量信息，而这些信息一旦泄露，轻则被中介公司所掌握，导致大量的骚扰电话，重则引起其他更严重的安全隐患。

出于安全性的考虑，临床的数据难以与微生物数据进行融合。要填补这两者之间的鸿沟，需要搭建一个重要的桥梁。王佳伟指出，现在智源研究院通过联邦学习的模式建立创新平台，就是搭建桥梁的良好示范。在这个基础上，建造一个创新性、研究性的平台，能够提高诊断的精准性。这就是创建神经感染免疫疾病与联邦学习创新平台的另一个非常重要的意义。

二、平台概况

在后半场的分享中，王佳伟首先为我们介绍了神经感染免疫疾病与联邦学习创新平台的初期、中期和长期的计划。

在初期计划中，平台试图通过神经系统的免疫学数据、微生物组学数据，以及一些联邦学习在临床的应用来进行实验。其中，这些数据包括了临床的检验报告、病例以及影像学的资料。

在中期计划中，平台尝试采集京津冀等周边一些地区患者的感染样本组学的数据，并对数据进行溯源分析。

在长期计划中，平台将尝试开展脑血管病 RAPID 技术的国际化的研究。在建立了相应的模型之后，就可以展开国际合作，建立一个诊断模型和风险预测模型。这也是项目组的一个结合临床的研究项目，以实现更好地为临床进行服务。

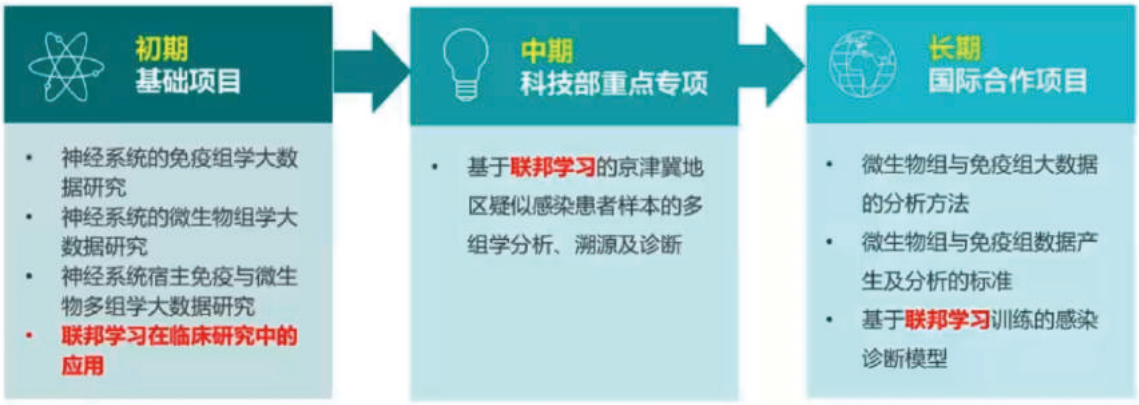


图 3：创新平台的初期、中期和长期计划

接下来，王佳伟介绍了创新平台的基本概况。创新平台由北京同仁医院、北京智源人工智能研究院团队、联邦学习团队以及予果生物团队联合构建。这个平台是推进跨学科、高水平的产学研的项目。

王佳伟指出，学科交叉是人工智能的一个重要的创新点，这个创新平台也是基于一个多学科的联合创新所打造的一个项目。在构建平台方面，项目组有重要的一些工作基础，包括“十三五”精准医学的重大病源微生物检测的项目等。另一方面，在多学科交叉方面，平台有着国际一流的专家团队，包括人工智能方向、医疗方向和生物组学、基因组学方向的专家团队，以及智源研究院联邦学习的大数据处理平台和相关学者等。以上都是这一平台能够得以顺利创建的保证。

目前，创新平台还在前期准备的阶段，团队已经联系了国内外专家，组织开展了多次线上讨论会，并制定了线上项目的启动方案。当前已经开展了一批小样本的对照研究，预测在年内就会形成初步的研究结果。

三、总结

王佳伟认为，神经感染免疫疾病与联邦学习创新平台，是为了实现精准医疗、构建智慧医疗、产生更多的临床研究成果。借助这个平台，更多的研究者会加入进来逐步推进这项研究，产出更多的临床成果，为临床服务。王佳伟对北京智源研究院、予果生物公司所提供的帮助进行了致谢，并期待能够和更多的同行进一步合作。

北京协和医院朱庆莉：超声 AI 新技术助力乳腺癌早诊早治

整理：智源社区 罗丽

在 2020 北京智源大会 AI 医疗专题论坛中，北京协和医院超声医学科主任医师，教授，博士研究生导师朱庆莉分享了超声人工智能在乳腺癌临床诊疗中的重要研究和应用，她的报告题目为《乳腺癌早诊早治，超声人工智能的新领域》。

朱庆莉在乳腺超声领域具有 20 年的临床工作经验，报告中，朱庆莉从临床医生的角度，介绍了中国乳腺癌诊治现状，以及在临床和整个乳腺诊治阶段遇到的一些瓶颈式问题，同时也分享了人工智能新技术在乳腺癌筛查、诊断和治疗、监测中的应用。在乳腺癌全周期诊疗过程中，与人工智能、基因组学和大数据等联合起来组成影像新技术，对实现创新的临床应用转化具有重要价值。

朱庆莉的演讲主要包括以下三个方面:

(1) 中国乳腺癌诊治的现况
(2) 人工智能在乳腺癌筛查中的应用
(3) 影像基因组学的应用

一、中国乳腺癌诊治的现况

乳腺癌是一种对人体危害性比较大的疾病，也是中国女性发病率最高的恶性肿瘤。最近的研究表明，除澳大利亚和美国等国家，中国乳腺癌的诊治效果也获得了非常不错的成绩，五年净生存率已位列世界前茅，而这些成绩的获得与乳腺癌的早期诊断、早期发现和早期治疗密切相关。

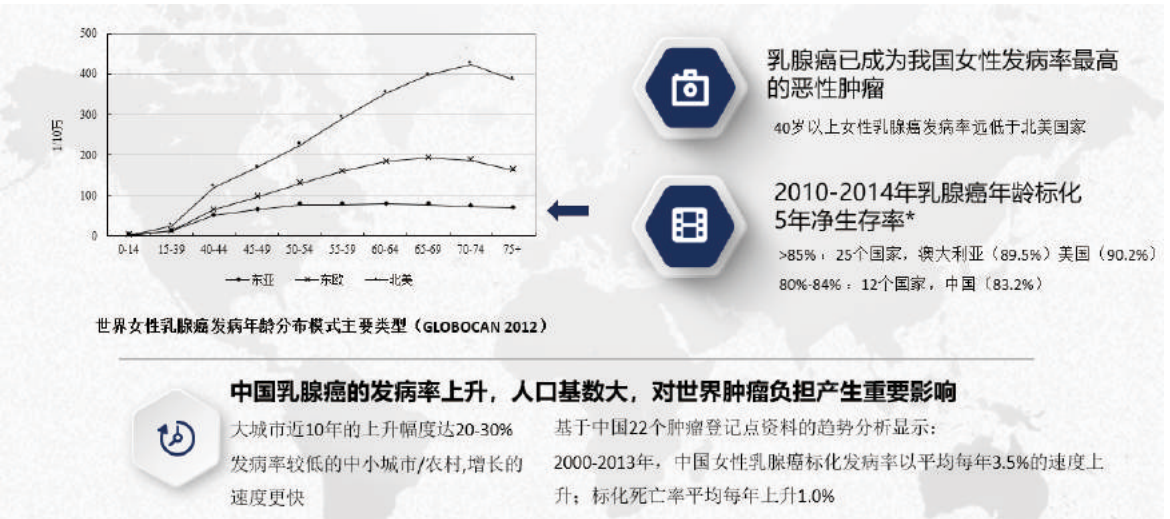


图 1：乳腺癌患病现况

从上图可以看到，东亚乳腺癌的发病率虽明显低于欧美，但也具有一定的上升趋势，中国人口基数大，中国乳腺癌的诊治对世界肿瘤诊治具有非常重要的影响，因此，我国非常重视乳腺癌的早诊早治工作。2009 年，我国启动了国家医改重大卫生专项——农村妇女乳腺癌检查项目，之后的多个政策性文件中，对“两癌”（乳腺癌、宫颈癌）的筛查和诊治均提出明确要求，并安排专项基金对“两癌”妇女进行救助。

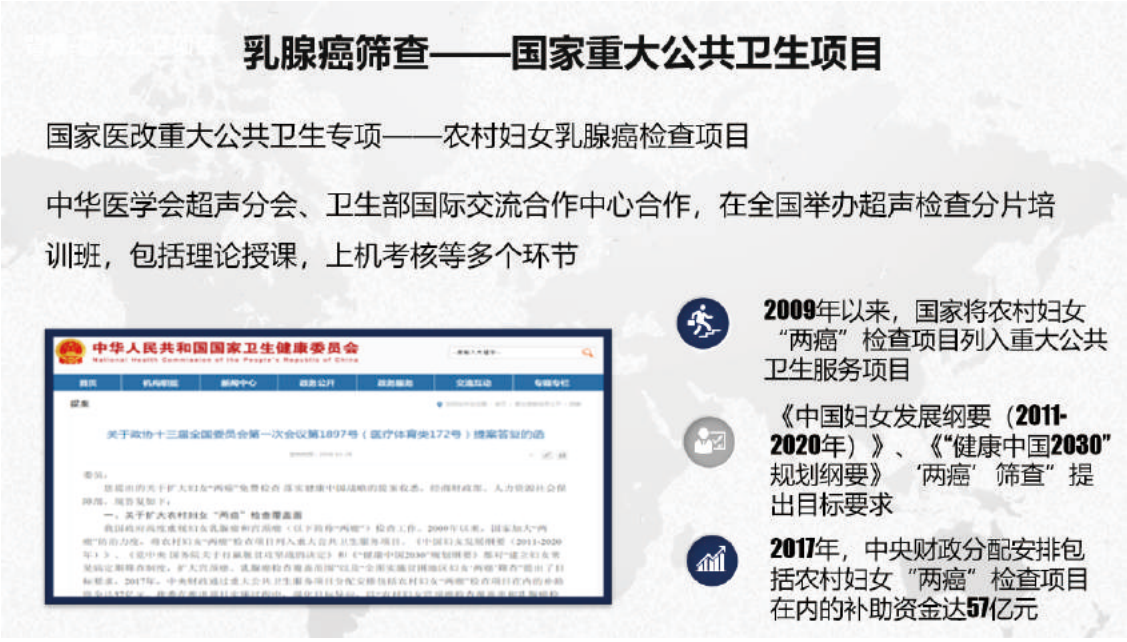


图 2：中国乳腺癌防控措施

2016 年国务院印发的《“健康中国 2030”规划纲要》中提出，针对癌症高发地区，及时开展早诊早治工作，同时推动肿瘤的机会性筛查。机会性筛查是指患者主动到医疗机构进行乳腺癌的筛查，与此相对应的是全体筛查，全体筛查是指只要达到了一定的人口都要进行乳腺癌的筛查。中国是一个人口基数非常大的国家，医疗资源有限，“2030 纲要”明确提出，现阶段中国乳腺癌的筛查方式是机会性筛查。针对中国女性乳腺腺体特点，以及超声价格低廉，设备普及率高等特点，超声成为机会性筛查的首选方案。

而超声作为乳腺癌筛查方法，也存在着一些问题:

(1) **诊断的特异性比较低。**根据不同检查人，有时会出现“假阳性”案例，即把一些良性疾病、良性结节误诊为恶性，造成了不必要的手术和活检，造成了医疗资源的浪费，也增加了个人和社会的经济负担。
(2) **治疗模式的转变。**早诊工作推动了早治工作的转变，早期乳腺癌的手术主要是根治术，或改良根治术，手术复杂难度大，而随着早期乳腺癌在临床上被发现，手术变得越来越简单。早期乳腺癌的治疗模式已经从外科手术为主转变为个体化综合治疗，以平衡局部治疗和全身化疗的优化方法。
(3) **全周期管理给临床工作提出更多工作要求。**患者术后恢复、生存时间延长等问题的出现，使得在整个乳腺癌诊治过程中，需要进行全周期、全方位的管理，肿瘤之外的健康问题包括心血管疾病、生育和心理等方面也需要进行关注。

影像学在易感人群的筛查、疾病早期诊断与治疗、个体化治疗方案的制定、疗效检测、随访等乳腺癌全周期管理中发挥着重要价值，那么，如何把乳腺癌基因检测、生物标志物研究成果等新的临床研究结果和影像学结合起来呢?

二、人工智能在乳腺癌筛查中的应用

有研究表明，人工智能在影像领域的作用主要有三大类:

⑴ **病灶的自动识别 (Detection)。**病灶的自动识别对减少临床工作负担具有重大影响。
⑵ **病灶的精准诊断 (Characterization)。**人工智能能够提高诊断准确性，减少漏误诊； 能够进行术前无创分期(个体化诊断)；在影像组学中，影像表现与基因组学相关，能够对肿瘤的特征进行精准描述。
⑶ **病灶随访监测 (Monitoring)。**人工智能能够监测病灶变化，进行治疗后的监测。

2.1 乳腺癌筛查

从上个世纪 90 年代开始，病灶自动识别就开始应用于乳腺癌癌腺的筛查，随着可识别的影像范畴的不断拓展，其应用领域逐渐延伸到超声、磁共振和癌腺的断层成像中，研究人员通过应用人工智能做自动病灶的发现和自动诊断。

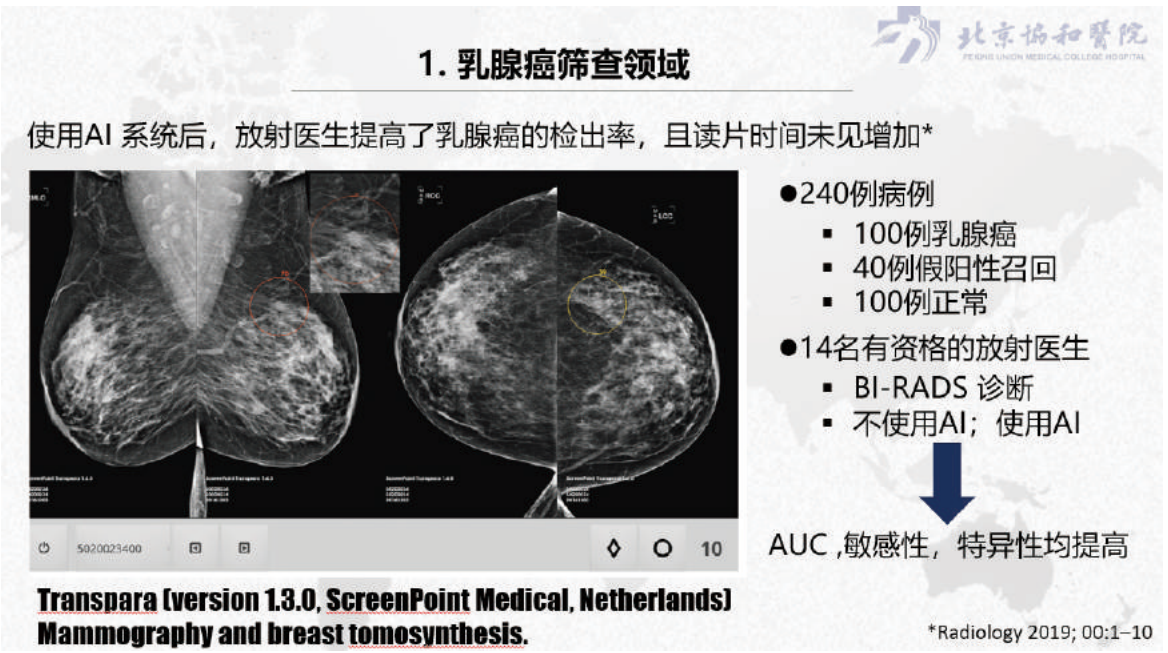


图 3：AI 乳腺癌诊断软件示例

图为人工智能乳腺癌诊断软件，在北美和欧洲应用广泛。研究和临床试验都表明，通过人工智能辅助诊断后，乳腺癌整体的诊断准确性和敏感性都有明显的提高。

今年发布在《Nature》上的文章“*International evaluation of an AI system for breast cancer screening*”中的实验中，研究人员在美国和英国分别做了两组不同的训练集和验证集集合，实验结果在训练集和验证集上均

表现良好，其突出表现是同时降低了对“假阴性”和“假阳性”的检测，在和六个真正的放射科医生的 PK 中，AI 系统均完美胜出。

而在超声领域也有类似的筛查方式——自动乳腺容积成像。

自动乳腺容积成像与我们所熟悉的常规超声不同，它可以自动获取整个乳腺的容积数据，不需靠人工扫查就能获得乳腺图像，也可以通过自动诊断对容积数据进行离线数据分析，通过软件自动把可疑的癌病灶标识出来，供放射科医生进一步确认。

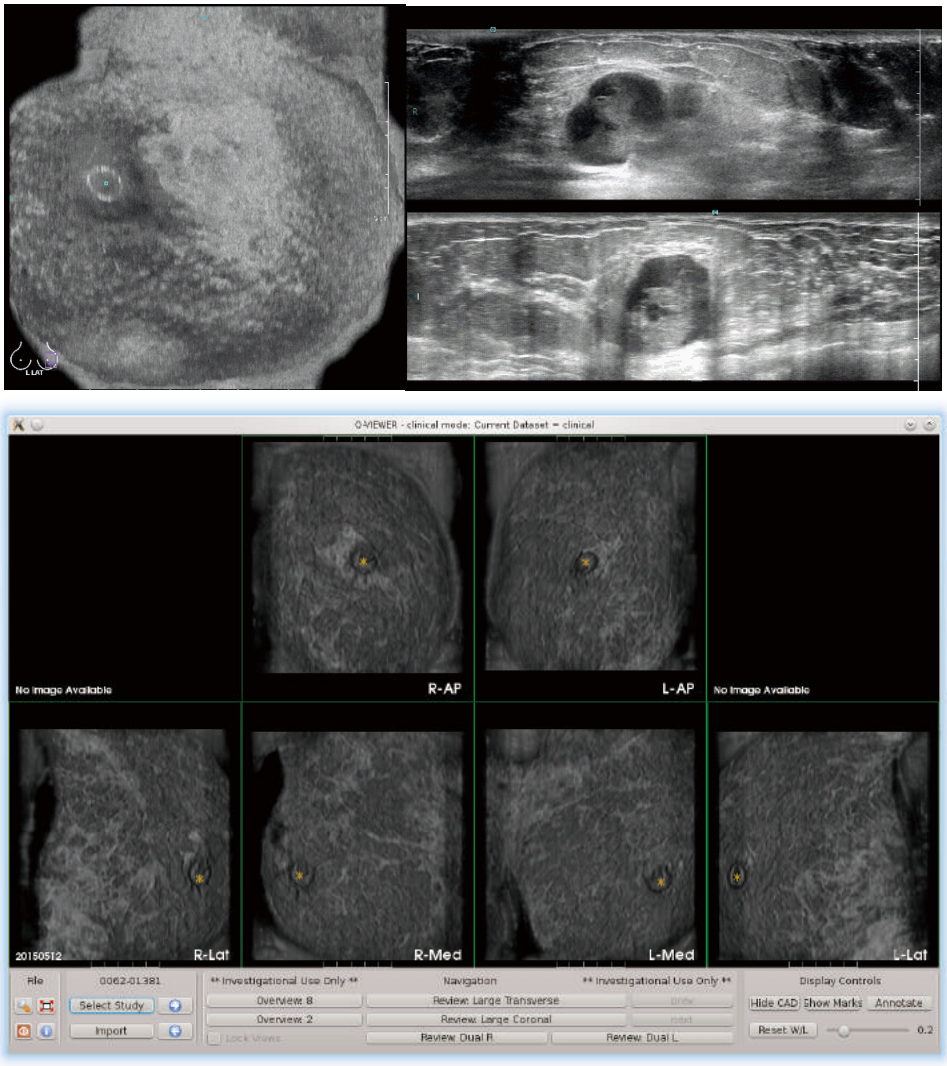


图 4：自动乳腺容积成像软件示例

自动乳腺超声技术手段在美国被批准用于致密乳腺的乳腺癌筛查。超声在乳腺癌筛查当中的地位和价值是毋庸置疑的，AI 软件可以从比较多的容积数据当中直接对可疑病灶进行标识。目前开发的软件，是在常规超声自动扫查过程中对癌病灶进行自动识别和勾勒。

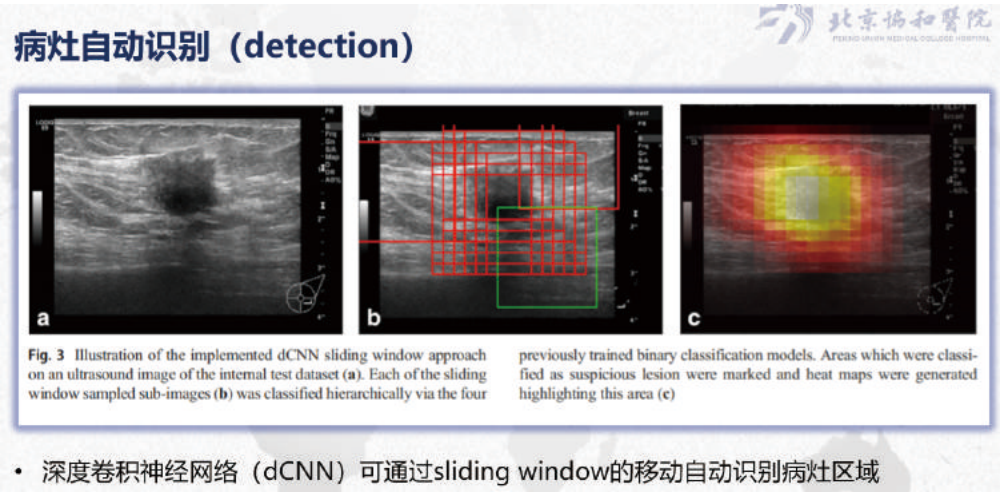


图 5：病灶自动识别软件示例

2.2 乳腺癌病灶的精准诊断

从 X 线到超声，再到磁共振，乳腺癌病灶的诊断工作进展得非常快。图为超声自动诊断软件，它可以对已经采图获得的病灶作出自动诊断，从实验结果来看，AI 病灶自动诊断软件具有临床实用价值。

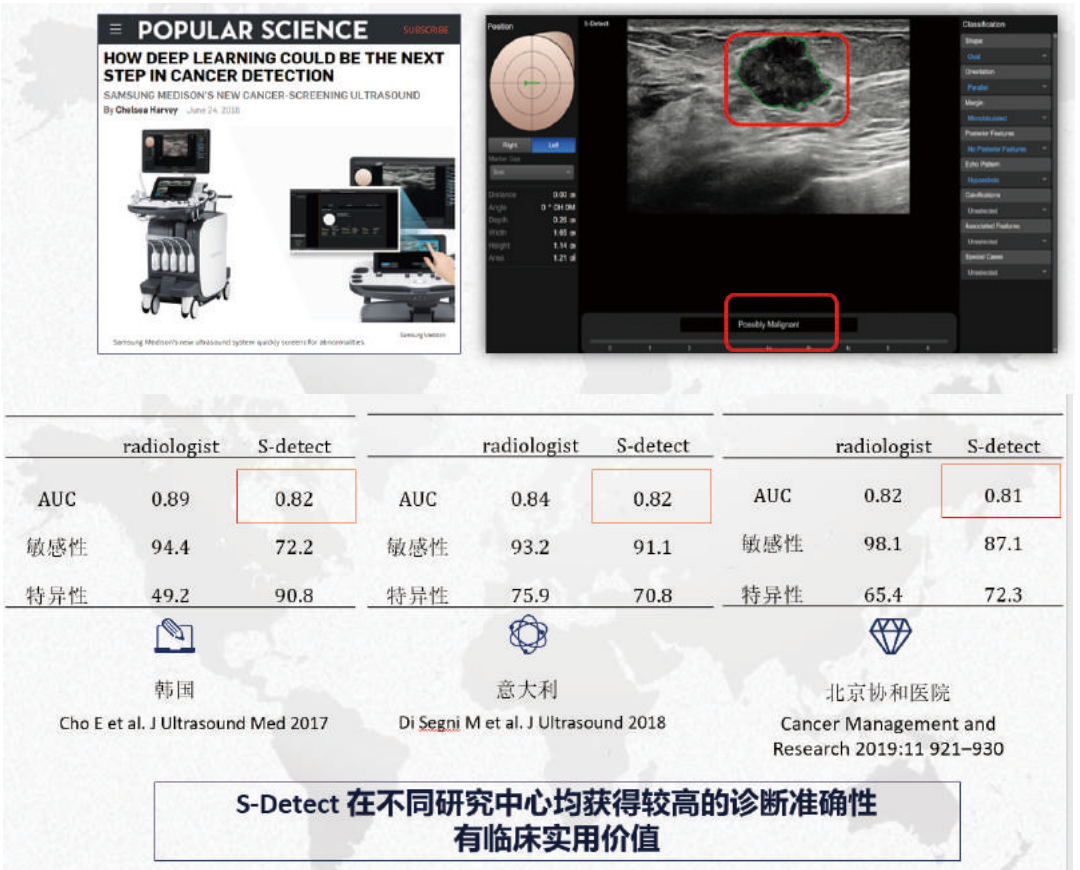


图 6：软件 S-Detect 及其应用

三、影像基因组学的应用

在临床研究中，病理是诊断的“金标准”，随着影像技术的发展，研究人员认为，可以将影像作为无创的疾病“观测器”，或是载体影像的一种方法，以对疾病进行诊断，包括形态分析和功能判断。影像学目标的改变为整个影像学研究和影像技术提供发展动力。

基因组学是通过高通量的基因测序比对提出的，它与疾病的预后相关，提出有临床价值的基因上的改变。**影像组学**是相对基因的改变来提出的，能够和疾病的预后形成良好的相关性。近年来，研究者把影像组学和基因组学结合起来，提出**影像基因组学**，为疾病的个体化预测提供更多研究价值。

基因组学的研究方法是通过一个高通量的测序来检测突变或基因的改变。在临床中，常用的乳腺癌的分子分型是基因组学的简化版，乳腺癌分成四种类型：Luminal A 型、Luminal B 型、H 型、三阴性，分子分型和病人的治疗反应以及生存密切相关，可以依据分子分型来指导临床决策。

而基因组学也有其局限性，首先需要通过有创检测确定肿瘤的分子分型，其次，肿瘤局部活检代表性欠佳，无法反映肿瘤的整体信息，将导致低估高风险肿瘤或过度诊断、过度治疗惰性肿瘤等问题的出现。因此，在临床中，迫切需要一种准确无创的手段来确定乳腺癌的分子分型。而影像组学就是这种诊断方式的产物，影像组学通过高通量的手段，通过组学的研究，与大数据和人工智能多维度、多平台的分析，能够找到影像和分子之间的关联性或影像和基因联合的作用，以服务于临床，是后基因组学时代非常重要的进展。

“Images Are More than Pictures, They Are Data”，影像内部分析的提取非常重要，影像组学能够克服肿瘤的异质性，对于疾病的风险分层、个体化治疗监测，以及病灶变化的及时识别等具有重要作用，也可用于无法进行活检的恶性肿瘤。基因组学数据的获取是通过一些兴趣区的识别来提取特征，通过对特征进行量化，建立模型，以进行临床预测。有研究表明，影像组学评分（LASSO 分析）对三阴性乳腺癌和纤维腺瘤的鉴别诊断有较高准确性。

在临床中，不同分子分型的乳腺癌术后复发的转移率，以及复发转移的高峰时间和位置均不同，因此，应该具有不同的个体化随访和治疗策略。影像基因组学在临床当中具有长链非编码 RNA，在乳腺癌发展过程当中会引起下游大规模调控改变，转移的发生率会增加，另外一方面，磁共振技术能够把两个计算机定量提取的 MRI 表型 – 测序确定长链非编码 RNA 的关联，以预测患者的早期转移。

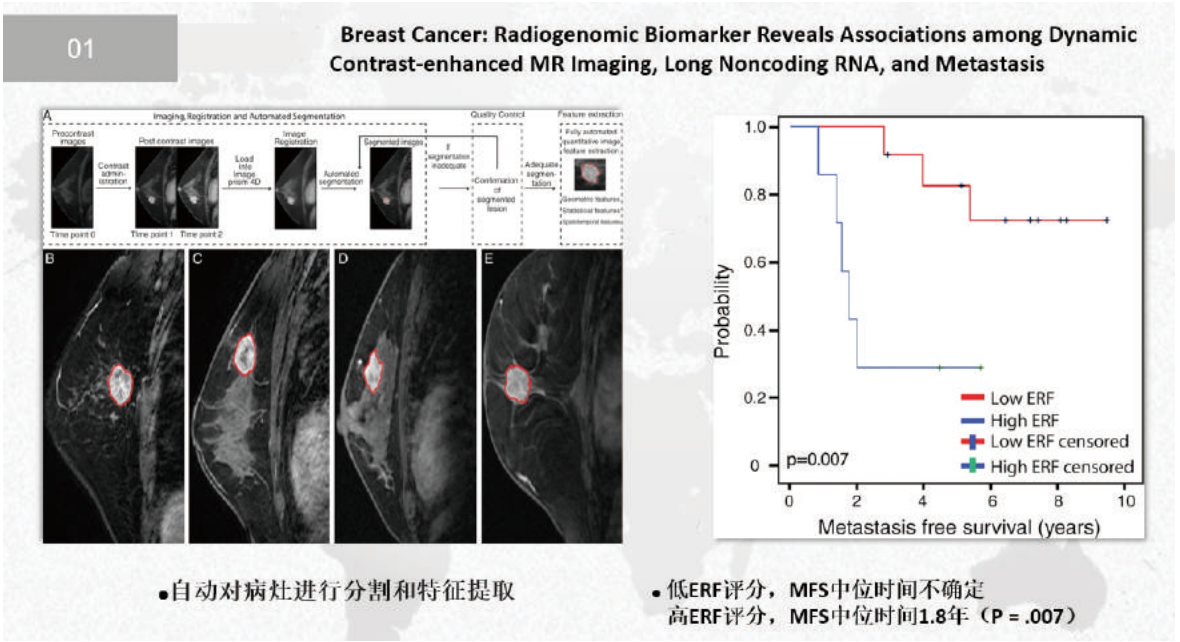


图 7：磁共振图像及特征的提取

图为磁共振图像，图像自动提取及特征提取，从右侧曲线中可以看到，在磁共振上提取的特征，确实在远期预后中发生了显著的差异。

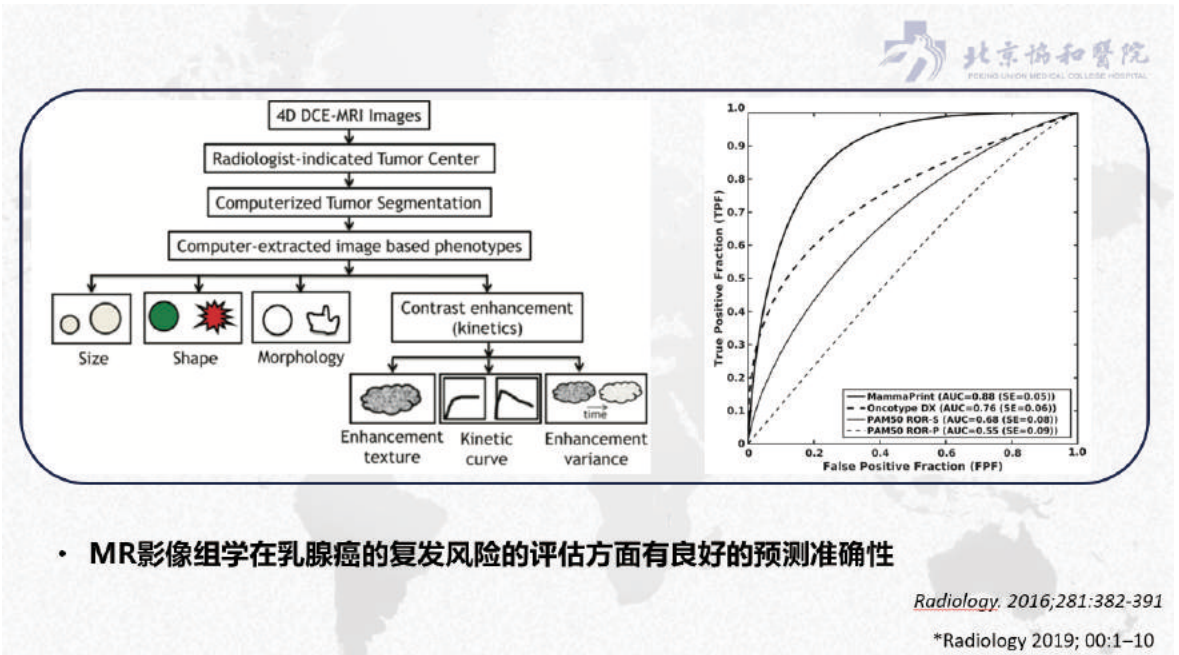


图 8：MR 影像组学评估乳腺癌复发风险

影像基因组学具有良好的预测准确性，图为 MR 影像组学方法评估乳腺癌的复发风险，研究采用多个试剂盒，用微阵列的方法去检测多个基因突变的改变，并与影像中的特征进行相关性比较。可以看到，影像基因组学在

复发风险评估方面，其 ROC 曲线有明显的提升。

可以看到，人工智能对乳腺癌良、恶性鉴别诊断，乳腺癌筛查有非常明确的辅助作用，对于优化诊断流程，实现高效的临床诊疗有很大的帮助。从临床未来的发展角度来看，朱庆莉表示，她更期望能够看到影像基因组学能发挥更大的发展和应用前景，以实现乳腺癌临床诊疗中个体化精准诊疗的目的。

四、结语

乳腺癌是中国女性发病率最高的恶性肿瘤，是一个亟待解决的关键临床问题。朱庆莉表示，从临床的角度来说，乳腺癌的诊疗研究应着眼于乳腺癌患者的全周期管理，在全周期诊疗过程中，影像学有其独特优势，它能够与人工智能、基因组学和大数据等技术联合起来组成影像新技术，在乳腺癌的诊疗研究和应用领域，如果能够充分发挥影像新技术的技术优势，相信就一定能够实现创新的临床应用转化，为广大乳腺癌患者带来新的希望。

商汤科技研究院副院长张少霆：新基建，新医疗，新机遇—新形势下的 AI——赋能临床医疗的视觉中枢

整理：智源社区 李雪菲

在第二届北京智源大会的“AI 医疗”专题论坛中，商汤科技研究院副院长、上海交通大学清源研究院副院长张少霆发表了题为《新基建，新医疗，新机遇 – 新形势下的 AI： 赋能临床医疗的视觉中枢》的报告，对智慧医疗的前景和智慧诊疗平台 SenseCare 进行了详细介绍。

张少霆指出，智慧医疗、健康的涵盖范围是非常广的（图 1）。围绕这些版块进行人工智能赋能，也有比较多的应用场景： 在医疗机构进行辅助诊疗和远程会诊的支持； 在患者端提供慢性病管理和用药监控的支持； 在药企端帮助新药研发；在医保和保险端进行智能支付等工作。

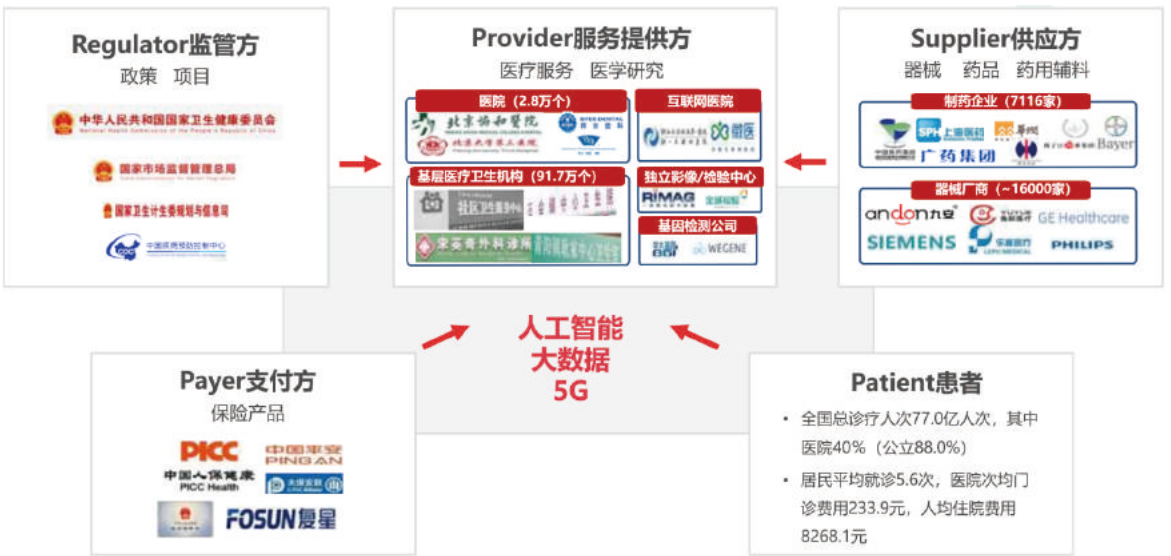


图 1： 智慧医疗关键角色互动图

SenseCare 智慧诊疗平台是针对医院板块的 AI 赋能产品，其目标是在赋能医疗影像生成的同时也赋能给对应的临床医生； 另一方面是在诊断、治疗、康复等全流程上为医院赋能（如图 2）。张少霆介绍，将 SenseCare 智慧诊疗平台装备到医院的科室里，全院的的临床医生只需要一个能浏览网页的电子设备就可以使用其所有的人工智能功能和影像三维分析等功能，并且能做到实时体验，依据不同的数据启动不同的工作。

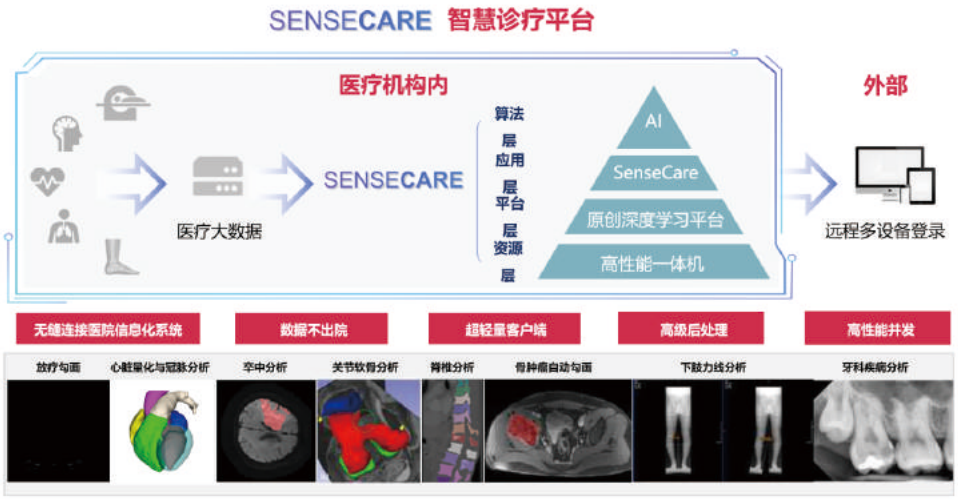


图 2：SenseCare 智慧诊疗平台

但在这种模式下如何保证数据安全呢？核心技术就是高并发的三维渲染。所有的医疗影像临床分析都需要三维渲染技术，在数据不外传的情况下，SenseCare 在服务器端完成渲染从而进行远程提供，进而实现交互分析。在使用过程中，SenseCare 可以同时保证 160 个用户进行三维高清渲染和交互，如果不考虑同时的情况，其能支持上千个用户量级，确保赋能全院的医生，且具有高度数据安全保障。

基于 SenseCare，AI 医疗影像完成了一系列应用，一个例子是肺部检测。除了常见的肺结节检测、肺结节良恶性分析，还提供了三维支器官镜的手术规划、虚拟内窥镜漫游显示，能对这些数据进行更深层次的分析，制定更佳的治疗方案。在新冠疫情期间，在 SenseCare 肺部功能基础上，还火速上线了新冠肺炎的分析功能，包括量化分析、针对新冠肺炎的分析、复产复工时的体检内容分析，驰援一系列的地区。第二个例子是骨科相关工作，主要是针对病人拍摄的 CT 和核磁共振，抓取多模态的骨头和肿瘤数据信息，然后对其进行多模态的融合、分割、配准等工作，最终打印出 3D 模型，帮助医生完成后续的手术规划（如图 3 ）。

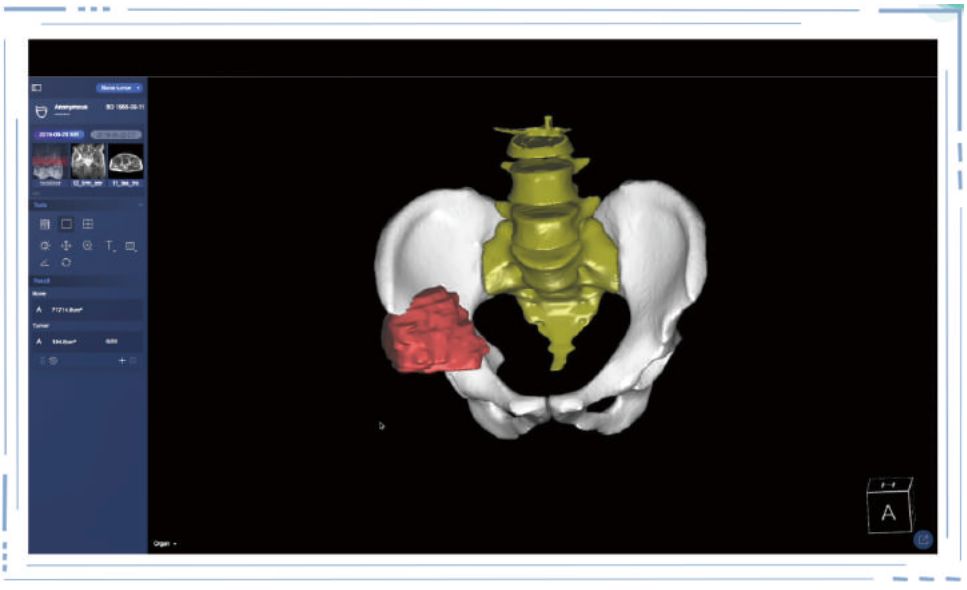


图 3：SenseCare 骨盆肿瘤 3D 打印规划

基于 SenseCare，在保障数据安全、网页浏览环境的前提下，还有助于实时发现潜在的肿瘤区域（如图 4）。在上万例病人的试验中，SenseCare 没有发现一例漏检情况，其性能效果非是可观的，目前由卫健委牵头已经在部署中心集群，将进一步部署到不同的医院。

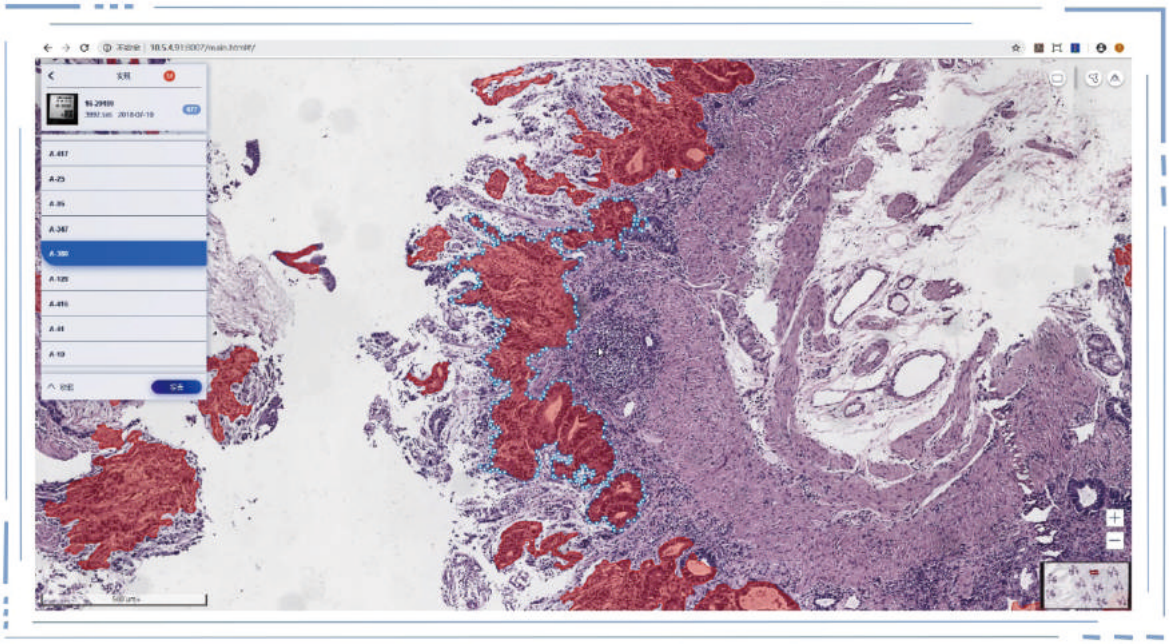


图 4：SenseCare 消化道病理诊断分析

借助临床医疗我们可以一窥 SenseCare 平台，再融合包括人工智能、大数据以及 5G 在内的一系列技术支持，可以极大赋能不同的行业，这将带来巨大的发展机遇。

智谱 AI 张鹏：知识疫图 AI+ 大数据在新冠肺炎知识智能服务中的应用

整理：智源社区 詹好

2020 年 6 月 23 日，在第二届北京智源大会的 AI 医疗专题论坛上，来自智谱 AI 的张鹏博士，做了名为《知识疫图 AI+ 大数据在新冠肺炎知识智能服务中的应用》的演讲。张鹏分别从数据汇集、智能预测和知识图谱三个方面想我们展示了“知识疫图”这一系统。

一、“知识疫图”平台

2019 年年底开始，新冠肺炎的疫情在中国开始爆发，现在已经扩展到全球，在疫情期间，学术界很早就开始积极动员，寻找科研成果在抗疫中的用武之地。其中，张鹏团队发布了名为“知识疫图”的疫情专题平台（网址：https://covid-19.aminer.cn/）。“知识疫图”项目主要围绕三个目标展开：

1. 汇集全世界最全面的，与新冠病毒相关的开放数据源；
2. 基于数据源进行大数据的智能预测，帮助人们预测疫情的走势；
3. 基于数据和智能 AI 技术，构建冠状病毒的知识图谱，使其积累形成易被使用的“知识”，以便更好地服务于后续的工作。

“知识疫图”项目基于 AMiner 平台而构建。AMiner 平台是一个大规模的科技知识图谱平台，在该平台中，可以通过海量的知识文献，发觉其中隐含的关联关系，实现从文献到知识的转化，并且通过快速的算法实现知识的智能服务。

而基于这一平台所构建的“知识疫图”项目，总体上说可以实现三方面的功能：首先是数据汇总的工作，其次是数据挖掘与预测的工作，最后是知识的获取、集成以及其他智能服务的工作。

二、“知识疫图”平台的数据汇总功能

张鹏首先介绍了平台在数据汇总方面所做的工作。“知识疫图”项目汇集了世界上最全面的新冠肺炎开放数据源（包括 400 多项开放数据），并且还在不断地更新中。目前，平台数据的范围涵盖了疫情、科研、知识、媒体、政策等各个方面。

其中，主要的数据源是疫情实况数据，已经超过了 260 项；科研方面的数据也占较大比重，接近 100 项；与新冠知识相关的数据也有近 100 项。此外，还包括约翰霍普金斯大学发布的 JHU CSSE 数据集，以及一些医疗方面的开放的数据，如临床数据的开放数据集、一些民间的志愿者组织提供的开放数据等。

图 1：疫情数据库

不仅如此，“知识疫图”还基于学术研究方面的数据，绘制了一个学术成果的时间线，筛选了与疫情相关的、知名的、重要的学术成果文献。不仅如此，还在此基础之上，邀请了相关领域方面的专家来对这些文献进行解读分析，最终汇聚成的时间线能有效帮助民众了解疫情相关的学术成果。

图 2：“知识疫图”中的学术时间线功能

在政策方面，“知识疫图”绘制了全国范围的政策地图，提供了基于地图的政策查询和搜索、分类的索引功能。同时也邀请了专家来对疫情相关的政策进行解读，并提供了智能匹配和推送的服务。甚至，用户只需要输入自己企业的名称，就可以非常快速地匹配到跟自己的企业、地区相关的一些疫情相关的政策。

在开放的新闻数据方面，“知识疫图”收集了大量疫情相关的主流媒体报道数据，分析其中的事件、实体、话题，并融合百科的知识作为背景，实现了基于语义和知识的新闻事件的分析，最终通过可视化结果予以展示。在此基础上，还实现了对社交媒体的用户心理的分析，通过对不同情感倾向内容的关注度和变化的趋势的分析，以实现心理上适当的安抚与干预，防止出现民众大面积的心理问题。

三、智能预测功能

“知识疫图”的第二个功能，即基于大数据的“智能预测”功能。

“智能预测”试图预测疫情趋势的走向，包括新冠肺炎的感染人数的预测等。在今年 2 月，“知识疫图”联合一些单位，组织了一次线上的关于疫情数据的预测比赛。这次竞赛吸引了全球来自中国、美国、日本、英国、德国等 15 个国家和地区的一千多支队伍参加。

比赛最终获奖的一些预测模型达到了非常好的预测效果，如获得第一名的模型利用了深度学习的 LSTM 模型进行序列数据的预测。“智能预测”将这样的一些模型集成到疫情 Dashboar 系统中，以构建全球新冠疫情风险评估和辅助决策的系统。此外，该系统还提供了多级别、细粒度风险指数评估。

四、知识图谱功能

最后，张鹏向大家介绍了“知识疫图”的第三个重要的功能，即知识图谱功能。

平台收集了网上开源的相关知识数据，联合“知识疫图”的自身数据，构建了 COVID-19 开放知识图谱。这个开放知识图谱覆盖了医疗、健康、物资、防控、科研和人物等各方面的知识，有超过 500 个概念，390 多个属性，2 万多个实例。这个知识图谱展示了众多与新冠肺炎相关的知识，如病毒与肺炎之间的关系，病毒与其他的病毒、症状、疾病之间的关系等。

除了这些关于新冠肺炎常见的知识以外，“知识图谱”还针对冠状病毒相关的科研成果进行知识的抽取和集成，以发现过去对于冠状病毒研究的脉络和隐性的知识，如冠状病毒主要攻击人体细胞的方式与 ace2 的基因片断的关系等。

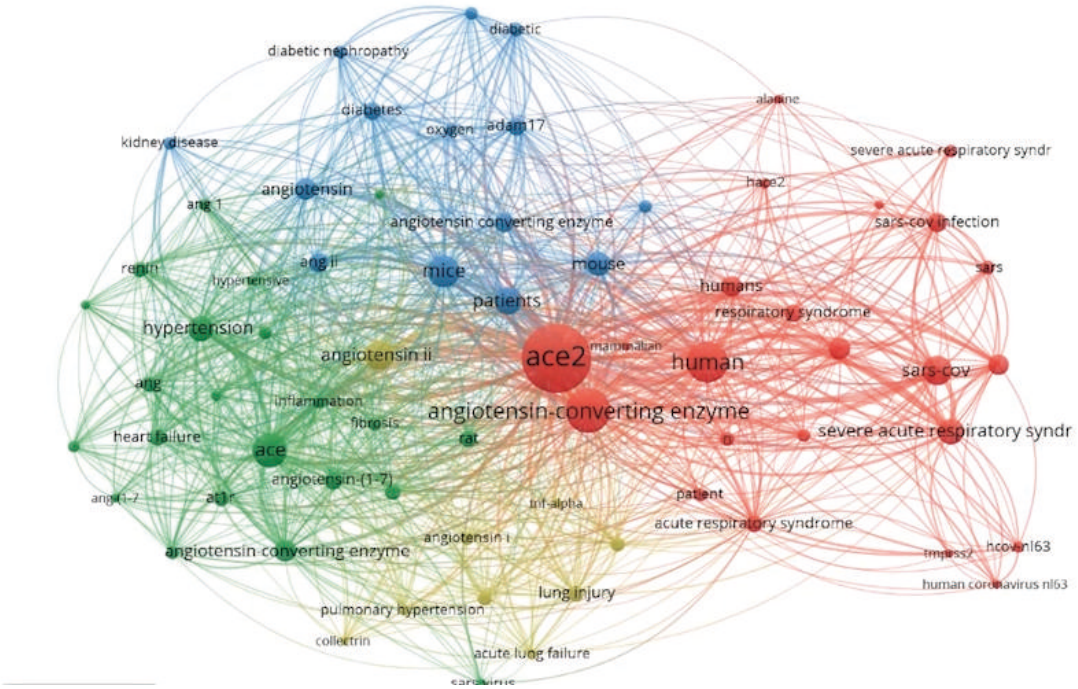


图 3：“知识疫图”中的“知识图谱”功能

目前，“知识图谱”通过“知识疫图”系统面向全世界的研究者开放。感兴趣的用户可以通过系统上提供的查询入口，通过关键词的方式查询和阅读知识图谱中的内容。此外，“知识疫图”也提供了多种格式的图谱数据直接的下载。

五、总结

最后，张鹏总结道，“知识疫图”试图打造了一个技术开发的社区，希望有更多的团队可以加入进来，尝试或使用“知识疫图”所提供的服务进行数据预测或其他科研工作。例如可以基于舆情的数据进行深入语义的分析和发觉；进行舆情安全方面的研究工作；或是结合交通的数据，讨论全球疫情对于交通的影响等。

AI TIME：AI 是医疗的下一个十年吗？

转载自：AI TIME 作者：田志远

医疗事关人身安全，要求极高，容错率极低，因此，知识壁垒和技术壁垒都很高。过去，AI 系统更多的是服务于终端，辅助医生诊断、决策。但是，医疗很复杂，直接切入终端问题很多。未来十年，AI+ 医疗会碰撞出怎样的火花，AI 对医疗产业、医护人员、患者等会产生怎样的影响？

对此，AI Time 联合北京智源大会，特别邀请了**首都医科大学附属北京同仁医院神经内科主任兼医院中心实验室主任王佳伟；商汤科技研究院副院长、集团副总裁，兼任上海交通大学清源研究院副院长张少霆；清华大学创新领军工程博士、智谱 AI CTO 张鹏；予果生物科技（北京）有限公司创始人及 CEO 夏涵；AI Time 负责人何芸，**共同推出了“人工智能是医疗的下一个十年吗?”特别论坛。

几位不同背景、不同岗位的大咖对 **AI+ 医疗**有什么独到的见解？让我们一起来看看吧。

一、AI 在抗疫中的作用

2020 年，新冠病毒突然而至，医疗机构成为战疫的前沿阵地，医护人员成为治病救命的无畏战士，AI 成为疫情预警、病情诊断的神兵利器。AI 与医疗两个与我们息息相关的领域以意想不到的方式紧密结合。那么，大数据、AI 对疫情期间的医疗检测等方面的作用有多大？未来还需要在哪些方面提升？

新冠疫情是百年不遇的重大公共卫生事件，堪比 1918 年西班牙大流感，但与之又有诸多不同。王佳伟主任首先提出了自己对新冠疫情的看法，并列举、分析了疫情发生以后国内外诸多模型的优劣势和特点，重点介绍了约翰·霍普金斯大学提出的模型的特点，认为 AI 对研判感染性疾病非常有价值，能够对感染人群情况分析、疾病溯源提供很大的帮助。并重点强调：**只有基于临床病人、基于流行病学的真实情况、数据，才能建立可靠的模型。**

在新冠疫情期间，**AI 技术响应速度快、介入的力度大**，帮助推出了 CT 辅助诊断系统、个人自我诊断系统，并帮助医生快速熟悉了新冠的特点，了解和掌握了诊断和筛查标准，提升了诊断的信心。但是，张少霆指出新冠期间也暴露出来了数据来源各异、标注水平不一、对隐私保护不健全的问题，以后可以针对相应问题进行有针对性地改进，迭代并部署模型，以预警疫情，提升诊疗效率。

其实，早在 2008 年，就出现了谷歌流感趋势，对当时的医学界、公共卫生界产生了很大的震动。张鹏据此提出了**用数据、AI 技术辅助医疗体系、公共卫生体系**的思路。

二、AI 对医务工作者的价值?

近年来，AI 不断进化，专家通过病历数据库中的海量数据不断训练 AI，让它学习诊断各种疾病。那么，以后病人能否在家一键诊断？医疗工作者能否远程诊疗？ AI 如何取得病人和医生的信任?

一键诊断、居家诊疗是目标，有着广泛的价值。王佳伟主任首先表达了自己对未来 AI 诊疗系统的期盼，并指出这其中的巨大价值。但是，实现这种效果存在很多困难与挑战：**(1) 海量数据的处理存在困难**，需要 AI 技术人员与医生一起发现、抓取特征数据。**(2) 要特别重视隐私和伦理问题**。未来，AI 在某些方面会超过人脑，但是基本不可能取代人。

目前，很多医务工作者已经接触过 AI 系统，介绍、推广 AI 系统的阻力大幅较少，要想让医生相信 AI 的结果，张少霆认为可以从三个方面入手：**(1) AI 技术人员要和医生一起开发产品；(2) 要在第三方监管机构的监督下去做；(3) 需要保障数据安全、注意可解释性。**

医学是一个比较复杂的情况，涉及各方面的内容。张鹏通过网络支付的例子指出安全问题是核心问题，**相比于支付涉及的财产安全，医疗涉及的人身安全问题更严肃、更重要**。AI+ 医疗不仅是一个技术问题，更是一个社会学问题。因此，在满足需求的过程中，路程还很漫长，需要解决的问题还很多。

三、AI 会给医疗产业带来什么变化?

随着 AI 技术的发展，未来抓取医疗 AI 所需数据的难点在哪里？数据量大小如何？如何保护数据安全？如何合理利用基因、蛋白质、代谢等多组学信息提高诊断准确率和效率？如何保证算法公平性，让算法具备可解释性？AI 将如何改变新药研发的理论与实践?

新冠爆发以来，新药研发人员利用根据特定靶点，对很多新药进行了筛选和验证。面对 AI 药物筛选与临床实际应用的距离越来越短，王佳伟主任表达了自己的乐观看法。

目前，清华大学已经有学生在利用计算机模拟药物分子反应（AI Time 的 B 站账户中有相关的分享视频，欢迎大家观看、点评），从而降低药物筛选的成本、缩短筛选的的时间。张鹏通过介绍真实医生学习、成长的过程指出了小样本学习甚至零样本学习的价值，并介绍了数据的价值。AI 诊断涉及的伦理问题很复杂，目前提供辅助诊疗的系统在技术上不存在困难，但是最终的诊断还需要医生来出具。

AI 医疗产品涵盖的领域众多，张少霆根据领域的不同，指出了不同产品的监管要求不一致，面临的挑战也不一样。如果产品最终目标是用到医生给病人下诊断书的阶段，产品的需求会更加复杂，需要平衡数据安全、数据

量等内容。产品在设计之初就需要努力避免医疗纠纷，考虑监管要求。新药研发领域更多的的 B 端需求，要平衡需求和风险，最终**实现降本增效的效果**。

四、AI+ 医疗，未来的机会在哪里?

今天，我们看到了 AI 的实际落地。未来十年，AI 在辅助诊断、辅助治疗、新药研发 、医疗数据挖掘、智能健康管理、医疗保险等领域会如何发展?

未来十年，AI+ 医疗有很多机遇和挑战，王佳伟主任通过用 AI 技术治疗失明患者的典型例子介绍了 AI 给医疗领域带来的新思路与新方式。此外，很多技术已经发展了很久，这些技术转变成民用值得我们期待，我们也应该能在不远的未来看到。

上述每一个领域的都是很有前途的领域，张少霆表达了自己的乐观态度，并指出医疗领域的不同的板块应该不是完全割裂开来的，它们互相联动很可能带来新的机会。

对于未来十年，张鹏建议我们应该思考 AI 能不能帮助我们找到目前无法治疗的疾病（如癌症）的病因，能不能提出治疗手段，从而惠及医疗工作者、惠及普通人、惠及整个社会。

14 AI 创业

北京市海淀区区长曾劲在 2020 北京智源大会“AI 创业”论坛上的致辞

在“AI 创业”论坛上，北京市海淀区区长曾劲出席并致辞。下面是致辞全文。

各位专家、投资家，各位同仁，女士们、先生们，朋友们:

大家上午好!

非常高兴受邀参加 2020 北京智源大会“AI 创业”论坛。首先，我谨代表海淀区委、区政府，对论坛的成功召开，表示热烈的祝贺！对一直以来关心支持海淀人工智能产业发展的各界人士，表示衷心的感谢!

创新发展历来是海淀的“金名片”“座右铭”。创新发展成就了海淀，海淀一直致力于创新引领，立足科技创新出发地、原始创新策源地、自主创新主阵地三大功能定位，加快中关村科学城建设，推动人工智能、区块链、大数据等一批高精尖产业健康发展。人工智能作为新一轮产业变革的核心驱动力、经济发展的新引擎，已成为中关村科学城的“硬核产业”。

这里有 AI 创业的“ 源头活水”——资源禀赋优势明显。有北大、清华等 27 所高校和中央党校 (国家行政学院) 等国家重要培训机构； 有以中科院为代表的国家级科研机构 99 家、国家工程研究中心 23 家、国家重点实验室 50 家； 在海淀工作或居住的两院院士 605 名，占全国的 36%； 区域每年大学毕业生近 20 万。海淀是我国人工智能创新的源头聚集地： 清华、北大、中科院等高校院所在人工智能领域处于全球顶尖水平，智源研究院、海华研究院等新型研发机构蓬勃发展； 是全国人工智能从业者的聚集地： 拥有近 4 万人工智能从业人员； 是全球人工智能企业最密集的区域之一： 拥有全国近 20% 的人工智能企业。

这里有 AI 创业的“ 深厚根基”——经济呈高质量发展。近年来，海淀经济社会持续健康稳定发展，取得了可喜成绩。2019 年地区生产总值接近 8000 亿元，已连续四年位居全市第一，经济总量和增长贡献均保持全市首位。经济结构高精尖特征明显，信息服务业、科技服务业、金融业和教育业四大行业对经济增长贡献率超过 90%； 高新技术企业总收入超过 2.6 万亿元，占中关村示范区约 40%； 发明专利授权量约 2.7 万件，占全市超过 50%，万人发明专利拥有量达 405 件； 国家级高新技术企业超过 1 万家，占全市约 40%； 有“独角兽”企业 40 家，占全国约五分之一。

这里有 AI 创业的“ 生态雨林”——发展环境不断优化。海淀是中关村的发源地，国家一系列科技创新的改革政策举措在此先行先试，是全国科技创新的先行者和试验田，现有国家级科技企业孵化器 14 家、大学科技园 19 家、留学人员创业园 21 家。区域政产学研金用等要素有机融合，形成了特有的创新创业生态体系。2019 年，我们发布加快人工智能创新引领发展的 15 条措施，突出支持重大原始创新、关键核心技术突破和开源开放平台建设。强化驻区高校院所在原始创新方面的“压舱石”作用，服务智源研究院等重大创新载体建设，推进人工智能、高端芯片等前沿研究储备和新技术突破。针对 AI 技术缺乏落地场景的难题，率先开放智慧医疗、智慧社区、科技公园等应用场景，并建设海淀“城市大脑”，为 AI 技术提供综合应用场景，推动生态发展。不久前，

我们还发布了《中关村科学城新时期再创业再出发提升创新能级的若干措施》和《中关村科学城北区发展行动计划》。当前，我们正以“新基建”为契机，加快推进公共算力平台、算法测试与数据共享平台等一批人工智能基础设施建设，为创业者提供基础研发资源和便捷研发服务。下一步，我们将进一步发挥政府组织优势和产业生态优势，与智源研究院联合，设立 20 亿元的人工智能科学家基金，持续升级智源生态，实现创新、空间、人才、资金等发展要素的系统支持。同时，我们将通过引导基金，引导创投机构投早、投长、投原创，共同培育人工智能创新企业。此外，我们还将规划不少于 100 万平方米的空间，用以建设人工智能集聚区。

海纳百川，积淀为雄。这是海淀的胸襟，也是海淀的姿态：我们诚挚欢迎全球创新合伙人前来海淀这片创新创业的沃土，追求远大理想、成就非凡人生！

最后，预祝本次论坛取得圆满成功！

谢谢！

创新工场创始人李开复：AI 赋能时代的创业

整理：智源社区 贾伟

2012 年至今，在深度学习推动下，这一波人工智能的蓬勃发展已有近十个年头。

在初期，一系列由 AI 科学家创建的初创公司，经过大浪淘沙，如今已有多家脱颖而出成为独角兽企业；榜样在先，于是有不少 AI 领域的学者，也寄望于自己在该领域深厚的研究功底，想乘风破浪，闯出一番事业来。

但人工智能的创业环境早已发生变化，单靠科学家挂帅就开辟一片天地的时代一去不复返。在进场之前，AI 科学家需要对当前 AI 创业形势有充足认识和准备，否则真可能热血而来，冷场而归，落得科研、商业两头空。

那么，在 2020 年这个时间节点，人工智能创业的大风向是什么？在如今环境，AI 创业有哪些特点？ AI 学者是否应该入场，以及该如何入场？

在北京智源大会“AI 创业专题论坛”中，创新工场创始人兼 CEO 李开复博士针对这些问题，做了一场深度演讲“AI 赋能时代的创业”。

演讲分为三部分。李开复先是对 AI 创业的时代背景做了详细分析，指出 AI 已经从“发明期”进入“应用期”，AI 创业的大环境已发生巨大变化。随后，他对欧美科技巨头成功经验进行分析，提出科学家型创始人在主导关键技术之外也需要理解商业，需要补齐产品化、商业化的能力。在最后，李开复谆谆告诫，AI 科研人才不要盲目入场创业，发挥价值的道路千千万万条。

以下，智源社区对李开复博士的演讲内容做概要整理，以飨读者。

一、AI 创业，大环境已变

过去 5 年，AI 已正式地从发明期进入了应用期。

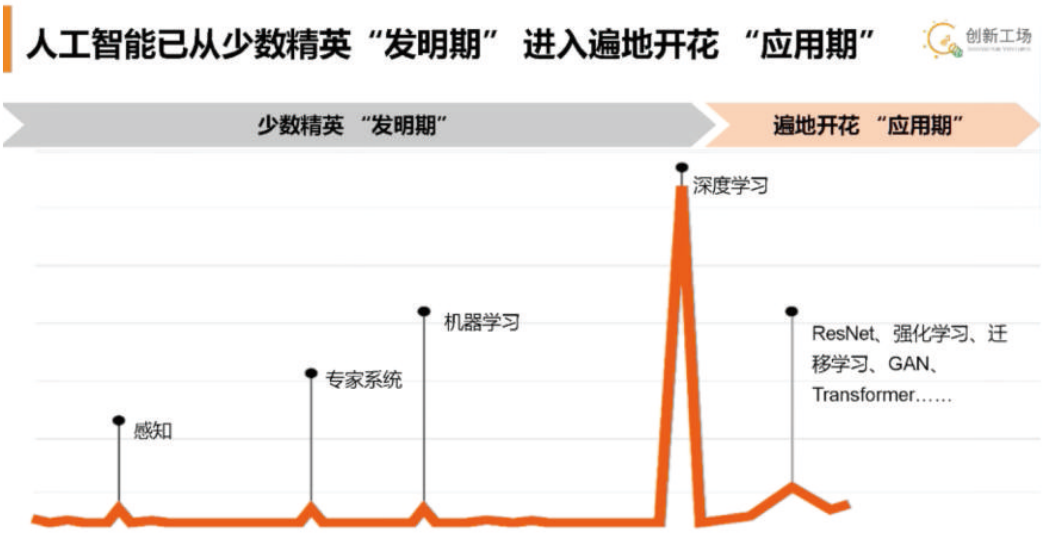


图 1：人工智能已进入遍地开花“应用期”

回顾人工智能六七十年的历史，早期有很多人在里面摸索碰撞，发明了很多东西，但大部分最后都证明是没有用的。

随着深度学习的兴起，一切都改变了。深度学习在很多领域都产生了巨大的效果提升以及相当的商业价值，把很多应用从不可用变到了可用，从勉强可用、狭窄领域可用变成很方便、很普及的可用。除此之外，还有一个改变是，10 年前真正懂深度学习的人可能只有几百上千个，而今天已经有几百万的工程师在使用深度学习。

所以今天的人工智能进入了一个新的时代。

AI 工程师	1,000’s	100,000’s	1,000,000’s	10,000,000’s+
AI 开发难易程度	不可能的任务	困难	懂点AI的工程师	大多数工程师
CEO	有经验的博士	CEO = 商业+ CTO = 科技	传统公司 + 首席AI官	传统公司
绝对价值创造	低	中等	高	高

图 2：在应用期，AI 成为了重要的基础设施

回顾过去这十年 AI 的发展，我们会发现，AI 是一个从黑科技到 B2B、再到 AI 赋能传统公司、然后进入无所不在的过程。

这个过程跟互联网很像。互联网在刚兴起的时候大家也感觉像黑科技； 后来出现了包括阿里巴巴这样的 B2B 公司； 再随后便是赋能传统行业。当时微软成立了一个互联网部门，专门寻找可以用微软的技术和产品进行互联网赋能的场景； 几年之后，这个部门就被解散了，因为互联网已经无处不在了。通过这个镜鉴可以看到，很多高深的技术大体会走这四个步骤。

在 2012 年的时候，AI 创业是一个纯技术的时代，许多 AI 技术人员成了创业者和 CEO，他们以技术为本，去寻找潜在的应用场景。

图 3：在发明期，AI 背后的科学家团队

几年后，技术发展了，AI 进入了 B2B 时代，先后涌现了许多 B2B 公司，他们的技术会用在金融、银行、保险或零售制造等领域，但因为每个行业使用 AI 的方法不一，每个公司在得到 AI 赋能时，都会遇到复制化的瓶颈。因此现在来看，AI 赋能传统行业，应该是 AI 领域迎来的最大机会。每个公司应该去分析自己对 AI 的需求，分析 AI 能够带来什么样的增益或成本降低。

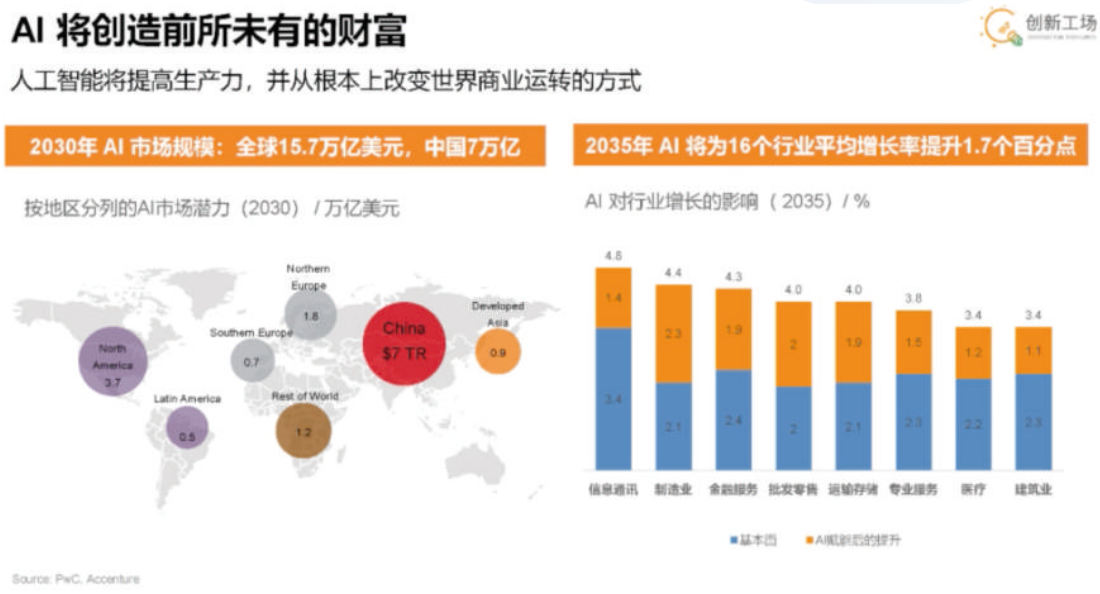


图 4：人工智能将显著提高生产力

另一方面，根据普华永道的分析，2030 年全球范围内的 AI 市场规模将达到 15.7 万亿美元。这 15.7 万亿美元并非来自 AI 独角兽，而是来自传统行业——信息通讯、制造、金融服务、批发零售、运输存储、专业服务、医疗和建筑业等与 AI 的深度融合。AI 的赋能可以让它们取得近一倍的增长。因此传统行业去了解 AI，用 AI 来改造、提升、赋能，找合适的人或合作伙伴帮助自己提升效益，现在是一个巨大的机会。

从另外一个角度来看，由于 AI 已经不像以前那样稀缺，所以靠一批懂 AI 的人了解一个传统行业后，去颠覆这个行业并成为领跑者，现在看来已经不那么现实了。更可能的情况是，传统行业学会并掌握 AI，利用 AI 来扩张自己。

那么，AI 可以赋能哪些传统行业呢?

图 5：AI 四波浪潮将重塑各行各业

李开复博士认为有四个相关领域:

第一波是互联网智能化。因为互联网的数据最多，所以能得到的价值最多。目前，最大的 AI 巨头其实也是互联网公司。

第二波是商业智能化。所有的商业都有数据，从大数据的累积、结构化、创造价值、分析，直到 AI，这是一个水到渠成的流程。

第三波是实体世界智能化。AI 能够感知（听、看……），而且已经达到甚至超过人的水平。更厉害的是 AI 可以介入各种传感器，它可以感知许多人类不能感知到的信息（例如温度、湿度，或黑暗中的事物），还能够进行三维重建等等，这些都是人类不能做到的。而 AI 能够把 IoT 中各种的传感器组织起来，把多模态数据融合起来，这代表以后的 AI 在感知上将全方位超过人的能力。

第四波全自动智能化。当 AI 能动起来，有了手、脚、轮子的功能，有了无人驾驶、智能农业、智能制造、机器人等等，这又会再提升到一个新的层次。

另一个问题是，如何利用 AI 赋能传统行业?

图 6：AI 赋能传统产业

李开复博士提出四点:

1. 单一环节降本提效。AI 可以取代许多传统行业中需要人重复劳动的工作，这将在很大程度上节省人力成本。例如某公司有近 4 亿美元的潜在坏账，传统方法需要雇佣数百名信贷员进行检查，但如果引入 AI 技术，只需要几名全职 AI 工程师就可以解决了，这不仅能够降低成本，而且还能在很大程度上降低违约率。

2. 单一环节优化赋能。例如在教育行业，教育不外乎是课堂学，回家练，考试测，然后老师评。在这四个过程中，老师的部分角色是可以用 AI 取代的。例如在学的过程中，可以用虚拟老师（例如卡通人物）来教学前的孩子，会更有趣一些； 在练的过程中，用 AI 来纠正英语发音，这样就可以有一个无所不在的老师帮你讲更标准的

英语；在测的时候，可以用 AI 改卷，或自适应题库等；而在评的时候，可以用 AI 智能纠错，或合成点评，从而能够对孩子一对一的建议。这些优化，并不改变原来的流程，只改变流程中的某一个事情。

3. 流程智能化赋能。这方面的代表是智能零售。如下图所示，围绕零售的全过程，利用 AI 技术精准预测每一家店哪种商品会在什么时间点卖出多少，分别对仓库（仓储调度）、工厂（生产研发制造）、零售商、经销商等整个商品生产、销售流程进行优化。同样的情况也适用于医疗行业。

4. 重构整个行业规则。这一步是最伟大的，也是最困难的。一定程度上，我们可以说今天的 AI 已经开始重构安防领域了，也可能重构了互联网领域，对于其他领域可能会相对更困难一些。但我们还是可以看到一些机会，当一个行业正在快速变革的时候，比如说从线下到线上教育的过程中，是不是有可能重构整个行业规则？或者在智能制药方面，是否能够用机器学习来提出制药效率？

总结来讲，李开复博士认为，当前环境下，AI 已经度过了由少数精英引领的“发明期”，而进入了遍地开花的“应用期”。在这一阶段，AI 赋能传统行业将是一个新的机遇。而在这个机遇中，最主要的将是传统行业主动拥抱 AI，而非 AI 颠覆传统行业。

二、AI 科学家创业需要理解商业

为了探究 AI 赋能时代创业的特点，李开复对 64 家海外科技巨头（北美 44 家，欧洲 15 家，以色列 5 家）的创业模式做了深度分析。他发现以下六条规律:

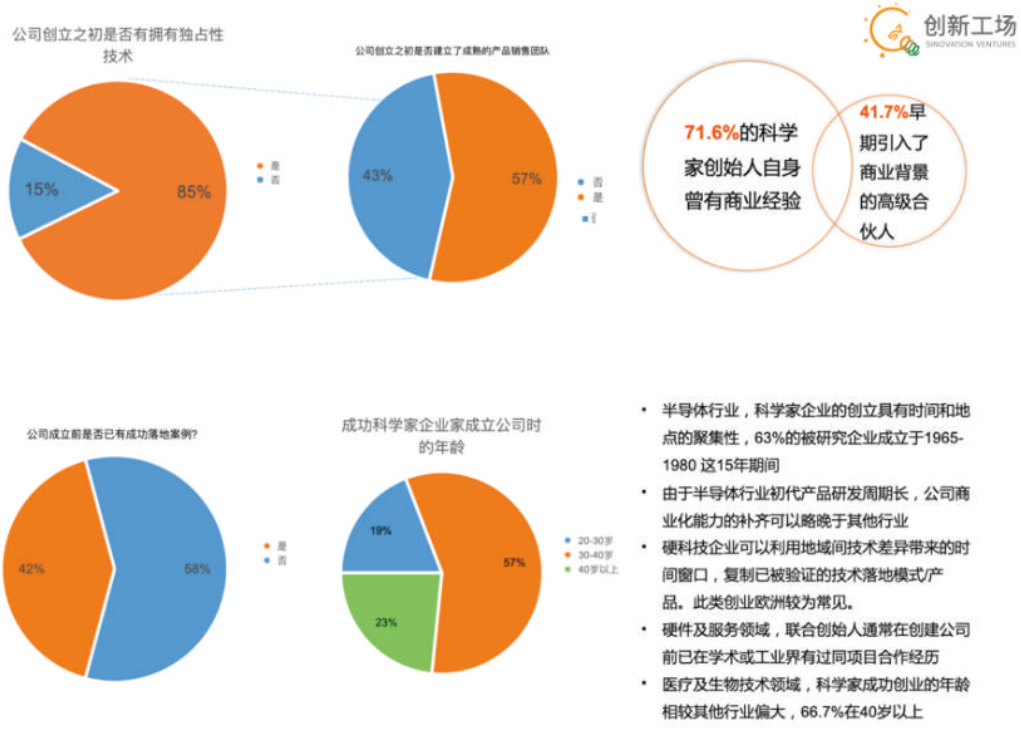


图 7：对 64 家海外科技企业创业模式的深度分析

1. 成功的科学家企业，拥有技术独占性和领先性的硬科技公司为主流。
2. 拥有技术领先性的硬科技公司也需要强大的产品和销售团队。
3. 成功的科学家企业，通常有两类： 科学家创始人自身曾有产品商业经验，或者早期引入了商业背景的高级合伙人。
4. 成功的科学家企业，在成立企业前已有成功的技术落地案例占很高比例。
5. 成功创业的科学家，30–40 岁创业的比例最高。
6. 部分行业成功的科学家企业具有典型行业特征。

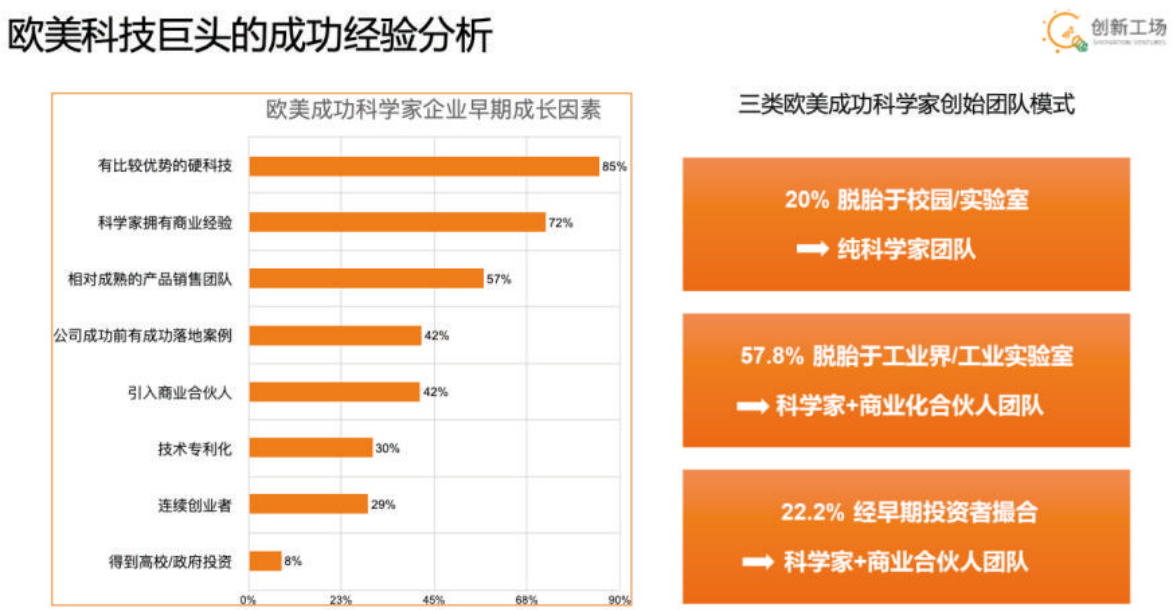


图 8：欧美科技巨头的成功经验分析

比较有意思的一点是，通过比较这 64 家企业，李开复发现，只有 20% 的成功企业脱胎于校园 / 实验室，而接近 60% 来自于工业界 / 工业实验室，另外有超过 22% 的是经过投资者撮合，也即将一个技术强硬的科学家与一个商业合伙人组成团队。

李开复指出，从投资者的角度来看，他们更倾向于最后一种，“**因为很多科学家可能自认为可以做，但我们要投资钱进去之前，还是要看他的商业经验是否充足，许多科学家本身并不很擅长商业。所以如果他没有，就要找一个商业合伙人。**”

精益创业之父 Steve Blank 培训过 500 个科学家团队，辅导过 261 个成型创业项目，他得出一个结论便是： 科学家往往很不愿承认自己并不具备把技术商业化的洞察与能力。

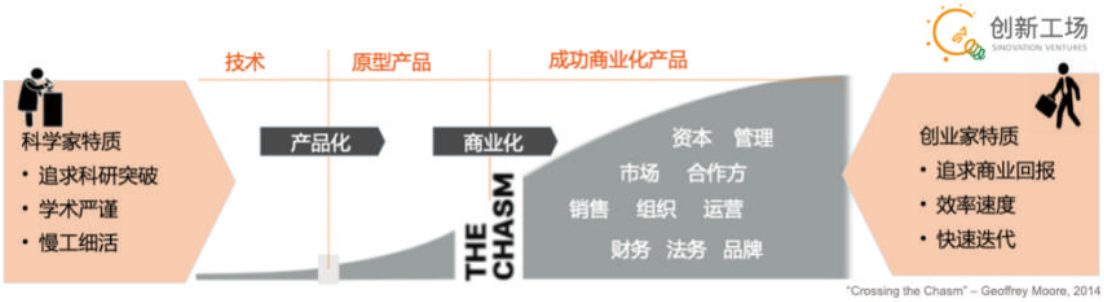


图 9：科学家与创业家的特质对比

科学家有自己的特质，从读博的时候就要求追求创新突破，要求学术严谨，慢工出细活，写篇论文可能要五六年的时间。然而企业家的要求是务实地追求商业回报，要求效率速度，希望产品快速迭代。这两种人本质上是完全不同的类型。一个科学家做 CEO，如果他自己不是很理解和尊重商业化的重要性，没有找一个重要的合伙人来管理公司，没有恰当地分配股权，那么他就可能面临灾难。这也是为什么我们看到许多有很强技术的初创公司在产品化、商业化的时候掉进了死亡谷。主要原因就在于，在搭建整个团队的时候，他们没有足够地尊重商业化人才的重要性。

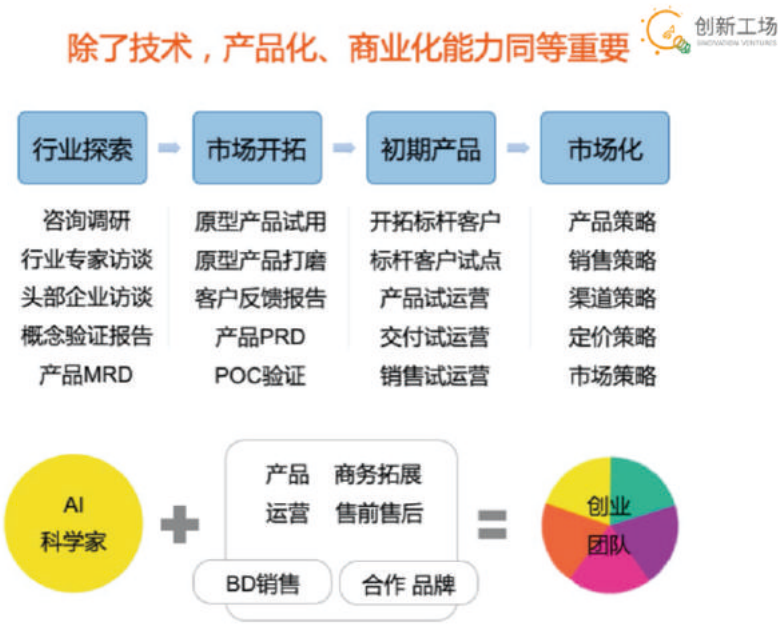


图 10：产业化、商业化能力的重要性

因此，李开复呼吁：“科学家主导关键技术之外，还需补齐产品化、商业化的能力。”

在技术研发之外，一定要重视商业化的能力，这并不是找个人来打工就好，而是需要多元化地进行行业探索、市场开拓、初期产品、市场化等，这可能需要好几种不同的人。一个创业团队里，科学家固然是关键，但产品运营、商务拓展、售前售后、BD 销售合作等也同样非常重要。

回归到 AI 创业本身，认清当前的创业环境特别重要。李开复指出，AI 技术产品化、商业化的门槛已经大大降低，这主要得益于以下四个因素:

1. 软件层面：

1）TensorFlow 和 PyTorch 为代表的深度学习框架已经成熟;

2）绝大多数深度学习模型及核心开发工具都以开源形式发布，这大幅简化了科研与工程复杂度。

2. 硬件层面：

1）Nvidia 的 GPU 系列，Google 的 TPU 系列，华为昇腾系列等 AI 加速芯片构成的硬件生态日趋完善;

2）服务器端和边缘计算端目前都拥有成熟的 AI 加速方案。

3. 集成层面：

1）云平台、容器、虚拟环境等技术大幅降低了 AI 算法的实施与部署成本;

2）现有的大数据平台、商业智能平台或传统商业系统与 AI 算法之间的连接越来越容易。

4. 人才层面：

1）纯科研型的人才结构已经转变为科研型、工程型、产品型、商业型的复合人才结构;

2）工程型、产品型、商业型人才在人工智能落地的过程中，越来越居于关键位置。

这就导致 AI 已经不再是 Rocket Science。从 CNN 发明到成功商业化，花了 30 年时间； 而谷歌从提出 Transformer 模型到大规模商用仅用了 2 年。

这说明，新技术成功商业化的时间越来越短了。

任何人都不能期望因为是自己发明的新技术，别人就学不会。大公司有的是技术，有的是人才，有的是资金，初创公司如果不能在两年内成功商业化，就很难具备竞争优势。

“我们可以看到现在整个行业有巨大的改变，我们必须要尊重这个环境。AI 已经度过了发明期，进入了应用期，这是一个很大的跳跃，所以我们要用不同的心态来看待 AI 创业。”

李开复博士正、反两面举了六个例子来说明情况:

1. 旷视科技：从游戏探索到商业落地。旷视科技创立于 2011 年，时值 AI 的“发明期”。旷视科技的创始团队是一支科研团队，在初期没有可以借鉴的行业经验，他们利用领先的科技优势尝试过不同的产品领域，例如 To C 类产品“乌鸦来了”、“相面大师”等，尽管这些产品的商业价值有限，但他们有足够长的时间保持竞争优势，来做商业探索；后来在创新工场等机构伙伴的帮助下，他们找到了更具价值的 To B 商业场景，营收得以大幅提升。

2. 创新奇智：以商业落地为根本，充分利用 AI 技术。创新奇智成立于 2018 年，这个时候已经是 AI 的“应用期”，AI 公司林立，巨头们也已经进入。这个时候成立公司，就应该意识得到除了 AI 技术领先性，商业落地也很重要。因此，创新奇智提出“技术产品”+“行业场景”双轮驱动模式，深挖应用场景，打造面向业务价值的

人工智能产品及解决方案，2019 年营收相比 2018 年实现 5 倍多成长。

3. 河小象：AI 是赋能教学评测端的强大工具，AI 可以提升教育质量，降低整体成本。需要注意的是，教育的核心仍是优质内容。河小象是一家 AI 教育的典型公司，AI 是它的加分项，而精心打造的内容才是决定是否成功的关键，也是最深的护城河。

4. 艾登科技：医疗行业先明确商业模式，再利用 AI 赋能。艾登科技是一家医疗 +AI 的公司，它发现了医疗行业中存在的几个痛点，例如诊疗数据质量不过关、医院间信息无共享机制，同一病症的医疗治疗方案和支出在不同地区差异巨大等。于是艾登推出了一套 SaaS 软件，这个软件能解决以上的痛点，而且定价也很合理，目前，3000 多家医院已经在使用这套软件。更重要的是，医院日常使用企业软件的过程，就是在帮助企业用脱敏数据来训练算法和模型，从而帮助医生来选择最佳的诊断方案。艾登的这种商业策略，不仅能够以充足的理由获得脱敏数据，而且医院也愿意为之付费。如果是一位 AI 科学家来做，一个很大可能的方案是去和某一家医院签一个独家合作，甚至要付出很大的费用才能获得医院的数据，渗透会很有限，规模化落地也会受限。

5. 反面案例：医疗影像读片技术公司，难以找到商业落地。当前，CV 技术的发展如火如荼，在许多领域 AI 的识别精度都已经超过了人类，但我们却发现医疗影像读片公司都发展得很困难。为什么？首先如何拿到数据是一个大问题。训练 AI 需要大量数据，这需要与多家医院进行合作； 而另一方面，医生的标注水平决定了机器学习的结果；AI 也只能达到部分病症标注，这极大地限制了 AI 的发挥空间。其次，医院普遍不会为软件买单，而生产硬件（读片机器）成本却非常高，医院同样不想购买。所以这些公司现在都面临着商业的困境，虽然技术足够好，但仍难以发展。

6. 反面案例：教育公司尝试前沿 AI 技术，却脱离市场需求。这是创新工场曾 PASS 掉的一个项目，这家教育公司有非常前沿的 AI 技术，他们希望做一个真的机器人老师。这个技术非常酷，应该也是最难的 AI 问题之一。但他们没有想到市场的需求在哪，在什么场景取代老师？是谁来付费买单？家长心理上是否接受?

总结来讲，当前已经不再是那种草莽初创的时代，AI 技术已经没有太高的壁垒，AI 科学家创业，必须要充分理解商业，才能避免掉入死亡谷。

慎之！

三、AI 科学家创业：扭转心态，做擅长的事

在报告的最后部分，李开复博士针对想要创业的 AI 科学家们提出了若干建议，如下:

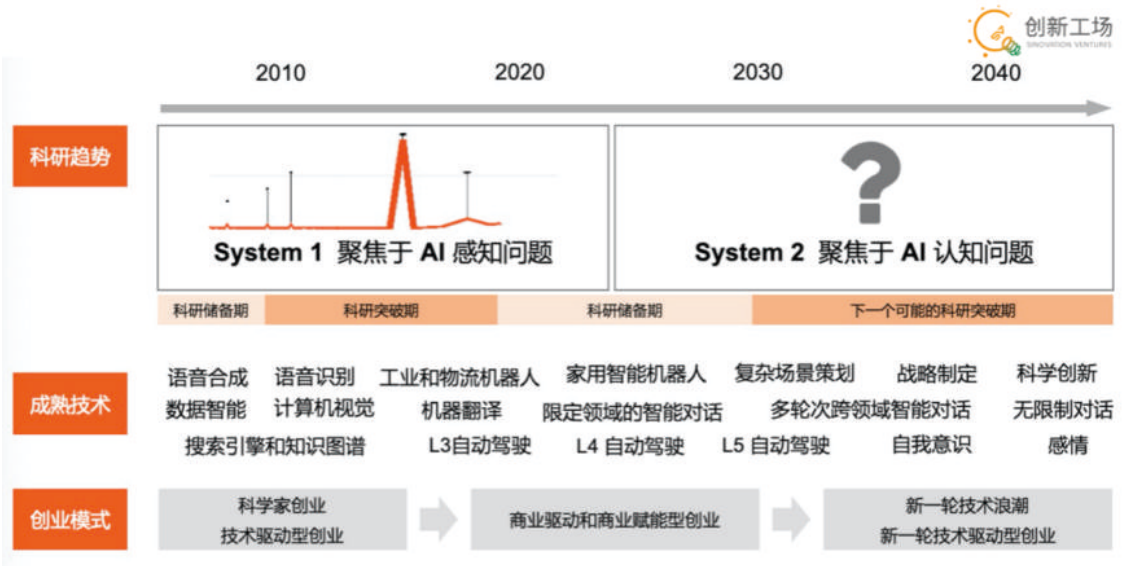


图 11：AI 当前的科研趋势、成熟技术与创业模式

1. 科研的问题还非常多，如果喜欢做科研，可以尝试做 System 2 的问题。System 1 中 AI 技术的“发明期”已经过去了，如果想要创业，想要做伟大的技术，就要针对 System 2 进行科研储备，一旦这些技术成熟，你便有一次机会做“发明期”的事情了。但这个有可能需要非常长期的投入，因为我们花了 60 多年时间的才让感知达到科研突破期，下一次是井喷是什么时候没有人能够确定。

图 12：AI 科研人才的职业道路：创业

2. 对于真的想参与创业的 AI 科学家，要放低姿态，理解商业。投身 AI 赋能的方式有几种：1）像吴恩达那样，撸起袖子创业，但必须要意识到现在已经不再是发明期了，在应用期创业难度会更高，所以一定要找懂行的合

伙人；2）加入传统公司，前面提到 AI 赋能传统公司将是未来一大机遇，但这时候需要考虑你是否能融入传统公司的企业文化等问题；3）加入 AI 赋能公司，去帮助传统公司做 AI 赋能。

图 13：AI 创业的几点建议

3. 如果真的决定撸起袖子创业，李开复博士给出四点建议。1）扭转心态，你的上帝是用户，要做有用并且有市场的创新；2）做擅长的事，如果不擅长比如商业化等领重要领域，就要找擅长的人加入核心团队；3）科研突破与商业回报并重，强调效率速度，快速迭代，创业就要有创业者的速度；4）要找到懂科技又懂商业的投资人，这可以补足你可能存在的需求和短板。

图 14：AI 科研人才的职业道路：留校

4. 有许多 AI 专家并不想创业，但仍然希望能够将自己的研究产生实际价值。李开复博士也总结了三种模式，分别为：1）Hinton 模式。Hinton 自己专注于理论研究，希望能够推动下一轮的 AI 发展，但是他会让他的学生去企业，帮助他们做 AI 应用，而自己并不受市场、竞争等因素的干扰；2）李凯模式。李凯教授自己出去创业，创办了 Data Domain 公司并上市，开辟了数十亿美元的新市场，成功之后回归学校，在技术与商业层面指导学生继续创业；3）李飞飞模式。身在学术圈，但利用学术休假等机会在企业兼职参与创业，之后再回归学术。这三位大师的模式，事实上也是一种可以让你参与 AI 创业或创造价值的方式。

道路千万条，对于 AI 科学家，重要的一点在于认清现实，认清自我。如此，才能有效利用自己的专长，做更有价值的事情。

清华智能产业研究院院长张亚勤：智能产业新浪潮

整理：智源社区 徐武涛

2020 北京智源大会“AI 创业”专题论坛上，清华大学智能产业研究院院长、清华大学“智能科学”讲席教授张亚勤博士作了题为《智能产业新浪潮》的报告。在报告中，张亚勤从三个方面对 AI 产业进行了介绍：

第一，AI 变革的三大方向；
第二，三大新兴行业；
第三，清华大学智能产业研究院。

以下智源社区编辑整理的张亚勤演讲报告要点。

一、AI 变革的三大方向

IT 行业在过去四五十年最大的变化就是数字化。

第一阶段始于上世纪 80 年代中期，数字化 1.0 致力于内容数字化，包括语音、图片、视频和文档。

到了 90 年代中期，开始了第二波数字化浪潮。数字化 2.0 主要聚焦于企业以及消费者互联网，前者包括客户关系管理（CRM）、供应链（Supply Chain）、商业智能（BI）、数据库和云计算等，后者包括搜索（Search）、社交（Social）、电子商务（E-commerce）、共享经济（Sharing economy）、通信（Communications）、数字货币（Digital Currency）和移动支付（Mobile Payment）等。

这两个阶段的特点均为信息数字化。

进入到数字化 3.0，我们开始对物理世界和生物世界进行数字化改造。物理世界中，我们的车、路、家庭和工厂等都在数字化，以前提到的信息高速公路，现在我们将其放入了互联网中，使之成为了数字世界的一部分。生物世界也是一样，大脑、身体器官、基因也都在数字化。3.0 阶段的数字化带给世界的影响远远超过前两个阶段，产生的数据量也出现了爆炸式增长，例如自动驾驶，每辆车每天产生的数据量约为 3TB；一次基因测序也会产生约 3TB 的数据量，与前两个阶段相比有多个数量级的差别。另外，这几年深度学习也有了很大的进步，包括 LSTM、CNN、GAN、BERT 等的发展，在语音识别、人脸识别、物体识别等领域已经达到了和人类相近的水平，并在知识理解方面也取得了很大进步。

总体来说，由于第三次数字化带来信息数据的爆炸式增长，深度学习的不断发展对算力的要求也呈现指数式的提高，因此传统的计算架构和通讯架构遭遇了瓶颈。

我们首先回顾一下过去五六十年指引产业发展的计算与通讯方面的三个重要定律和限制。

- 一是香农定律，包含三个方面，熵、信道容量和失真情况下压缩极限，包括 5G 的发展在内，目前已经非常接近这三个极限了。
- 二是摩尔定律，指每十八个月，芯片密度加倍。从这几年芯片的发展来看，摩尔定律也有逐步失效的趋势。

- 三是冯诺依曼计算机架构。在硬件方面，CPU/GPU/FPGA/ASIC 等在过去几年都有很大的变化。算法方面，由于速度和效率两方面的问题，目前的冯诺依曼架构并不非常适合运行。像谷歌、百度、寒武纪等等都推出了人工智能专用的芯片。另一方面，物理世界的数字化产生的很多数据都在设备上，处于边缘状态，5G 的出现使得我们可以把很多的智能决策放到边缘上去。

总的来说，分布式的智能、大量数据的产生以及新的硬件架构使得目前的 AI 产业有了一个新的发展。

二、三大新兴行业

智能产业的发展不仅提供了传统行业产业升级的机会，还能创造更多新需求、新岗位。在未来的五到十年，自动驾驶、工业互联网、智慧医疗这三个产业会遇到大的机遇。

在谈论自动驾驶前，我们先看一下人是如何驾驶的。通常我们将驾驶过程分成三个部分，看到——决策——动作，有几个不同的理论对此进行了解释。例如 Paul MacLean 的三体脑理论。Eric Kandel 的精确 – 非精确记忆的概念，从神经科学的角度解释了人在驾驶过程中是如何进行判断的。Daniel Kahneman 的系统 1 与系统 2 的理论，则是从行为科学的角度尝试进行了解读。

自动驾驶是一个很有趣的领域。从技术上讲，它融合了很多的技术创新；从行业发展的角度来看，由于对计划、位置、通讯设施等有很高的要求，因此在自身发展的同时能够带动其他行业的发展。从实现的难易度来说，自动驾驶面临很多的技术困难，不过让人感到安慰的是自动驾驶作为一个任务可以被分解为多个小任务分别进行攻克。因此虽然困难，但是假以时日仍然是可能取得成功的。从效益上讲，自动驾驶一旦实现，将极大地减小交通事故的发生，挽救更多的生命，还可以大大缓解交通堵塞的情况、改善空气质量。对国内相关行业来说，这样一个万亿规模的产业是一个很好的机会。

第二个是工业互联网。物理世界中通过各种各样的传感器将设备连接到云中构成了一个网络。5G 高速传输数据以及处理大数据的能力使得这一行业有可能产生真正的价值。目前我们利用各种独立的传感器从环境中搜集大量的数据，数据中包含大量的随机噪声，通过特征提取从数据中找出感兴趣的信息。更好的方式是将物理模型结合进去，使得分析数据后得到的结果更具有可解释性。

第三个方向是智慧医疗。以冠状病毒为例，它有许多变种。当我们想要寻找一种有效的药时，不可能对其一一进行验证，这不现实。所以我们会利用机器学习的方法来加速这个过程。同时，当我们对其变异机制有更多了解时，还能利用机器学习加速新药以及疫苗的研发。

三、清华大学智能产业研究院

最后我们谈一下正在筹建的清华大学智能产业研究院。

建立清华大学智能产业研究院的使命是利用人工智能的技术来创新、赋能产业，推动社会进步；目标是面向第四次工业革命，建立一个国际化、智能化、产业化的研究机构。我们会吸引大量人才，开发关键的核心技术，培养具有国际视野的领军人物，使其成为产业技术战略的智囊团。目前我们正在大量招聘人才，包括研究员、博士后和博士生，欢迎关注。

奇绩创坛创始人陆奇：AI 创业发展趋势：机会与挑战

整理：刘燕（InfoQ）

2020 年 6 月 23 日，在第二届北京智源大会的“AI 创业”专题论坛上，奇绩创坛（原 YC 中国）创始人兼 CEO 陆奇作了题为《AI 创业发展趋势： 机会与挑战》的演讲。他分享了 AI 创新创业的发展趋势以及现阶段 AI 创业所面临的一些挑战，并为 AI 创业公司应该如何把握创新机会提供了建议。

以下内容根据陆奇的演讲整理。

一、AI 技术的本质与 AI 价值的产生模式

首先，陆奇从 AI 技术的本质与 AI 价值的产生模式出发来分析 AI 创业的趋势，同时讨论整个业界应该如何帮助创业者更好抓住 AI 带来的创业机会。

他表示，现代 AI 技术的内核是基于深度学习的新计算基实； 在分布式重叠向量空间中学习特征表达能有效解决多种任务任务特征表达，本质上是知识的获取。

基于此作为基石，再加上工程化的能力，可以建立一个“三体合一”的系统架构，“三体”是指感知体系、思考体系、行动体系。三体合一的架构是任何智能体系的核心架构，因此 AI 系统的核心是通用的，AI 技术是获取知识，使用知识来达到目标的通用能力。

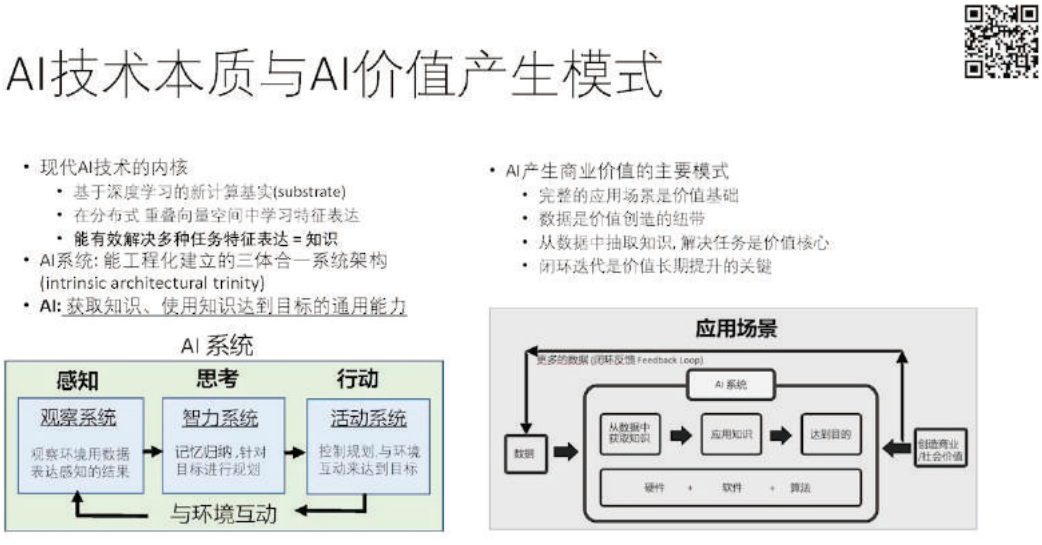


图 1： AI 技术本质与 A 价值产生模式

AI 产生商业价值的主要模式是怎样的？陆奇认为，首先要有完整的应用场景，这是其价值基础； 其次，数据是价值创造的纽带，此外，从数据中抽取知识、解决任务是整个的价值核心，最后，能有更多数据产生闭环迭代是价值长期提升的关键。

二、AI 商业化的宏观趋势

陆奇表示，从信息工业化发展的历史去看从 AI 的核心技术、主流商业模式，可以推演出 AI 商业化的宏观趋势。主要体现在四个方面:

1. 建立新的 IT 基础。具体包括，

- 传感器及 on-sensor 计算（芯片 + 软件 + 模型);
- 新的芯片技术栈，其对于开启垂直化时代的到来具有重要意义;
- 新的软件技术栈 software stack : 从底层到 fabric 到 middleware 到 device OS，再到应用，到工具链。

2. 开发应用。目前已经逐步转型到娱乐、制造、金融、医疗、教育、零售等所有产业和医生、分析师、客服、医生、教师等等所有职业。

3. 打造未来智能平台及相关产业生态，如，

- 如主系统（自动驾驶、机器人），新移动;
- 智能化场所：包括新工作与生活的空间和时间等;
- 个人助手：个人助手未来将是规模巨大的产业生态。

4. 形成产业发展基础环境，需齐备人才资本、金融资本、数据等主要生产资本、基础设施、及政策扶持等要素。

在明确了趋势和方向后，AI 创业公司应该如何推进商业化进程？陆奇认为，创业创新是发展 AI 商业化的核心路径。

创业创新包括三大要素：AI 技术、需求和市场。AI 技术是创新的核心驱动力； 需求是创新落地的基础； 市场是创新成长的环境。

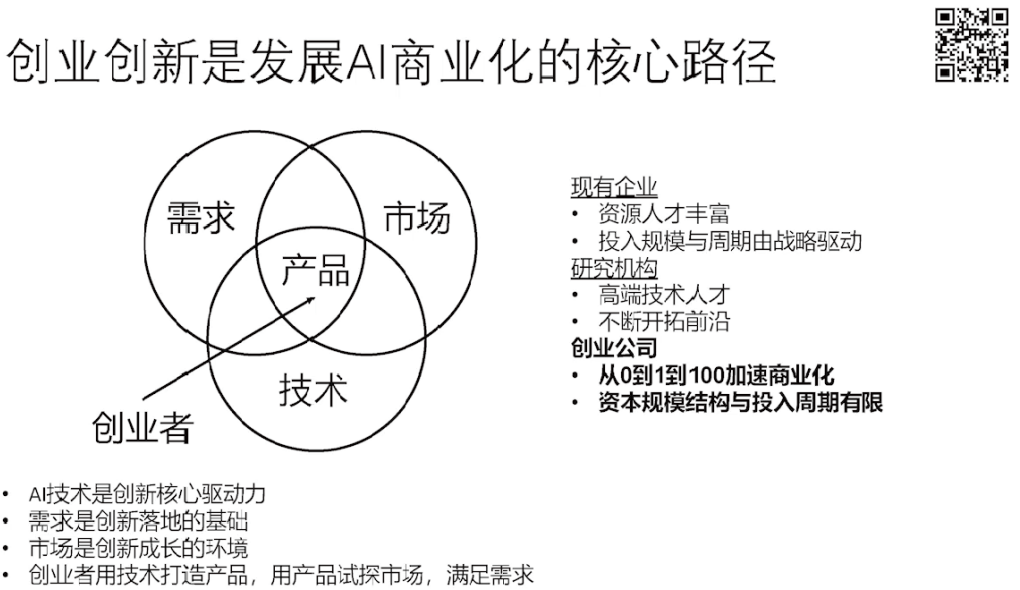


图 2：创业创新是发展 AI 商业化的核心路径

创业者通过利用 AI 技术来打造产品，用产品试探市场，满足用户的需求，让新的产品发挥出商业价值。

AI 商业化需要不同的实体一起合作，AI 的发展过程中需要大量的技术投入，现有的大企业拥有丰富的资源和人才，基于其战略驱动可以做大量的、长周期的投入； 现有的研究机构拥有高端的技术人才，也在不断开拓和探索前沿的 AI 技术。

在 AI 发展的过程中，其实创业公司是“主力军”的角色，它们比较灵活，能“见缝插针”，能够从 0–1–100 加速 AI 技术的商业化进程。当然需要注意的是，受限于资本规模结构和投入周期限制，并非所有的工作都适合创业公司来做。

三、哪些趋势创业公司可以把握住?

早期创业创新的趋势可以系统地从数字化进程发展的生态结构和趋势来推演。

工业数字化发展过去 60 多年的进程有节奏和规则的，基本上每隔 12 年就会出现新的平台和生态，这些生态有结构化的发展趋势。数字化发展进程的模式是由不同时代的计算平台所驱动，早期比较关注基础技术 — 早期的应用开发 —建立平台，形成生态，— 在生态环境下引发产业繁荣创新，在这个过程中核心驱动力是数字化的广度和深度。

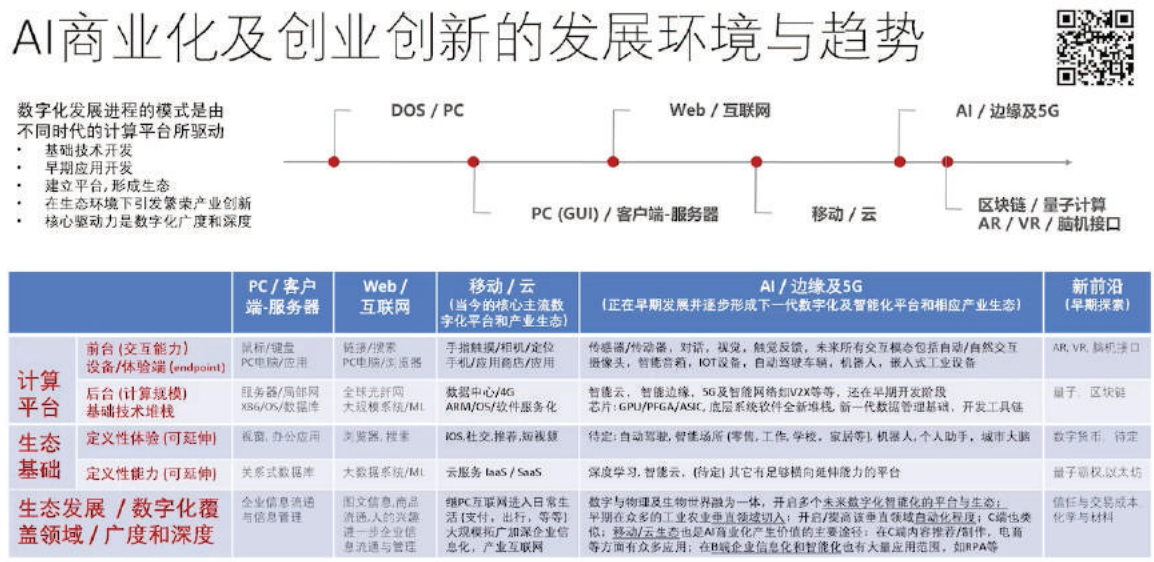


图 3：AI 商业化及创业创新的发展环境与趋势

数字化的深层次架构，生态核心是计算平台，包括前台，如交互能力，交互设备和体验端； 后台，指计算规模，其支撑是基础设施的堆栈、服务器和服务网等，后台的能力深度学习是核心，智能云也有可能成为定义性能力。

在计算平台上有早期应用，到了大的应用后就可以建立生态了。早期开发应用诞生了很多个生态，具有广泛商业价值，未来有可能智能驾驶、智能场所、零售、机器人个人助手等早期应用有足够宽度成为未来的生态的技术。这些都是很大的 AI 早期应用，都是创业公司可以参与进入的新的领域和趋势。

云和移动是目前数字化创新的主流生态，AI、边缘及 5G 是正在早期发展的并逐步形成下一代数字化及智能化平台和相应产业生态。在 AI 之后，数字化进程，有新的技术在探索，如 AR，脑机接口等技术是驱动新前沿发展的驱动力。

目前 AI 创新创业的前沿领域有很多，例如在 AI 基础前沿技术、AI 交互能力、AI 前端、AI 未来产业生态、垂直行业、移动 / 云生态应用、数字化前沿应用等领域，很多创业公司非常活跃，都在积极参与。一些领域如智能云、AI 前端等领域虽然是大企业的战场或者较适合大的公司，但对于创业公司来说仍然有很大的机会。

AI创业创新的前沿领域

创业前沿领域	创业细分领域	创业创新状况	创业生态环境
AI基础前沿技术		芯片GPU/PFGA/ASIC，底层系统软件全新堆栈，新一代数据管理基础，开发工具链 智能云所需的核心技术，智能边缘所需的核心技术，5G及智能网络所需的核心技术	IT基础工业生态
AI交互能力	传感器/传动器	各种光传感器如Lidar激光雷达，惯性传感器，声音传感器如麦克风阵列，热传感器， 空气传感器，卫星载体，低空(无人机)载体，定位（室外，室内）等等	目标应用行业生态： 如汽车供应商
	新交互模式与应用	对话交互，对话机器人在企业信息化自动化中落地应用；视觉交互早期探索	企业信息化/Saa5等
AI前端	设备端	摄像头，智能音箱，IOT设备，自动驾驶车辆，机器人，嵌入式工业设备	消费电子，工业设备等
	体验端	个人助手，虚拟人，3D，AR，新体验往往在以手机为主要使用端	移动/云生态
AI未来产业生态	AI赋能的产业生态	自动驾驶，智能场所(零售，工作，学校，家居等)，机器人，城市大脑，智能药物开发	相应的行业生态，2G
	AI技术基础生态	智能云，智能边缘，深度学习为主的开发平台，其它有充分横向延伸能力的平台	IT基础工业生态
垂直行业应用	B端	行业垂直细分领域如AOI用视觉提高检测效率等等，往往是设备+软件+服务+解决方案	其目标应用行业生态
	C端	生活细分场景如在家健身，用视觉帮助用户提高效益，往往是设备+软件+服务	其目标应用行业生态
移动/云生态应用	B端	企业信息化/智能化(各种职能)和产业互联网中有大量应用，短期RPA开始落地	企业IT生态
	C端	内容推荐，内容制作，内容/游戏体验如视频理解与交互，电商智能导购，定价等	移动互联网生态
数字化前沿应用	前端和后端	AR/VR，区块链，脑机接口，量子计算应用	风投早期探索生态

图 4：AI 创业创新的前沿领域

四、AI 创业面临的挑战

陆奇表示，现阶段的 AI 创业还面临一些挑战。

从技术上看，AI 技术的最大弱点就是太脆弱了，特别是在一些特定的场景很难达到效果。算法层面鲁棒性不够；数据上获取比较难，数据标注的成本和代价高，此外，还面临着数据孤岛、数据割裂的问题。此外 AI 技术门槛高，例如自然语言处理技术等 AI 技术往往需要高端人才多年的积累，一些 AI 公司并没有核心技术，依赖第三方公司。

在产品层面，从体验上看，C 端应用针对效应往往不及格，B 端客户满意度较低。在交互方式是哪个，定制化过多，难以产品化和平台化，集成商生态不足。

市场层面，在上游，供应链资金和时间要求在某些生态对创业公司造成困难；在下游，往往销售周期长，渠道资源稀缺，2B 和 TG 的资源是成功要素。

人才层面，在技术上，聘用有效技术人才耗时耗资，内部管理效益需要提高；从行业上看，对 2B 细分行业需

要聘用有深度行业能力的销售和 BD 人才。

在资本层面，AI 公司成长周期长，一些创业公司因为切细分赛道，天花板不够高，很难获得融资。

对于如何解决这些挑战，陆奇也提出了自己的建议。

在技术上，要提供新一代数据管理技术； 要通过系统化的开放数据集、服务接口、软件体系等，将技术门槛大大降低。

在产品层面，要针对产品和体验上做很多工作，管理用户预期，可借鉴搜索引擎模式； 在服务 B 端的要切的更细，可以从阶段性的流程上切入，从客户需求端切入。在交付方式上，通过项目合作累计平台能力，降低边际成本，提高集成商的能力。

市场层面，要帮助帮助创业公司利用政策环境，如“新基建”等抓住发展机遇。

人才上，要帮助创业公司聘用和管理技术和行业人才。要聘用技术核心人才，这些人才需要足够深的行业能力，了解 B 端企业，最好是在甲方做过的。另一方面加强对大专院校、研究机构人才的投入与引进。

资本上，帮助 AI 创业公司对接风投资金、银行贷款等，此外，风险投资机构也需要做适应调整，适应 AI 公司长期成长的特性，目前有很多 AI 公司虽然短期发展不足，但长期看，存在很大的价值。

圆桌论坛：人工智能创业和投资的未来十年

文字整理：蒋宝尚

在第二届北京智源大会“AI 创业专题论坛”上，启明科技邝子平、创新工场李开复、奇绩创坛陆奇、清华大学张亚勤、奇绩创业营曹勖文进行了题为“人工智能创业和投资的未来十年”的圆桌讨论。

各位嘉宾先是回顾了过去十年间，中国人工智能企业取得的发展，并对中国 AI 发展的优势进行了盘点，同时也对 AI 未来十年的投资和创业环境进行了展望。

在论坛的最后，面对当前 AI 人才短缺，如何构建负责任的 AI 企业，各位嘉宾也都纷纷给出了自己的建议。

以下是论坛的文字在整理:

一、过去十年：中国 AI 发展得分八十

邝子平：这次圆桌讨论的话题是“中国人工智能的创业和投资”主要内容是 AI 投资领域未来十年的前景如何。在展望未来之前，想请各位嘉宾回顾一下过去十年人工智能领域的投资以及创业情况。也对中国过去十年的发展情况进行评分，百分制，如果美国拿到八十分，那么中国能拿到多少分?

李开复：如果和美国对比，中国可以拿到百分制里的八十分。无论是独角兽企业的数量、投资金额以及价值创造都非常令人满意。例如，当前计算机领域的四只独角兽（商汤、云从、依图、旷视）在应用场景下累积了海量的数据，训练出了有价值的初始应用，然后也寻到了愿意付费的买家。从而得到了更高的估值，拿到了更多的融资，业务范围也增加了很多应用，因此不断地扩张，目前在计算机视觉方面处于“领跑世界”的位置。

AI 在其它领域，包括银行、客服、语音、无人驾驶也有很大的进展。但是缺乏好的数据和落地环境，企业级软件也不如美国发展得那么好，综合得分也能达到 80 分。

如果时光倒流，回到十年前，我们对中国的期望值可能只是 10 分，现在达到了 80 分，所以我们应该非常自豪。

张亚勤：我同意开复，中国得分至少应该是八十分，和美国打平手。刚才谈到视觉方面的四小龙，其实，讯飞、地平线、寒武纪等公司，在教育、健康和自动驾驶等领域借助风险投资的支持发展的也很快。虽然有些公司估值过高、存在一些泡沫，但是整体来讲非常有成效。综上，过去十年是中国人工智能技术发展最快的十年。

陆奇：我不知道满分（100 分）是什么样子，所以无法进行打分。另外，我认为这个问题应该至少过十年再来回答。以互联网为例，其从 1995 年左右开始，要是在 2005 年对发展情况进行评分，那时候的亚马逊的、Google、facebook 根本不知道能够成长为什么“样子”，但是在以“那时”为起点，经过十年的发展，就能够看到别样精彩的局面。所以，我的判断衡量指标是：十年、二十年以后，中国和美国两个大的创新体系当中，有多少人工智能企业站在世界第一梯队？因此，现在“评分”为时过早。

另外，开复和亚勤观点我非常认同。中国在计算机视觉、芯片、无人驾驶以及机器人领域都有不少尝试，也有很多进步。另外，还有一些垂直行业当中的应用（例如“用计算机视觉完成检测”）虽然赛道都比较窄，但是对企业的价值越来越明显。因此，总体上有一定程度的进展。

中国经过十年的发展，个人认为带来最重要的价值是：清晰了今天中国人工智能创业面临的挑战。因为接下来的十年，可以整合生态，从而把创新的壁垒和挑战的程度降低，帮助人工智能创业公司发展得更快。

如果从业界的角度能够把创新的门槛降低，那么，未来十年中国“驱动”的处于世界第一梯度的人工智能企业的数量会非常可观。

二、中国优势：数据 + 应用场景

邝子平：在过去十年，人工智能的几个重要驱动力，包括算力、数据等等，具有中国特色的是哪几个？另外，放眼未来十年，哪些中国元素能够驱动中国的 AI 跻身世界第一流。

陆奇：驱动人工智能发展的因素主要还是技术推动、需求拉动。未来十年，主要还是这二者的组合，即良好的需求和技术进展。

另外，未来十年我认为一个比较值得关注的是替代进口，因为中国现在逐渐进入需要自建技术产业生态的阶段。其中，IT 工业有很多机会，工业自动化在各个品类下，也有很多创业公司开始拥抱趋势，

中国前十年的发展过程中，重要的优势是数据。但数据的“联通”还有很多工作要做，今天大部分的数据存在状态是“孤岛”。如果想完全把这些数据打通，则需要技术平台的能力以及政策上的扶持。

十年之内能够实现数据资产化。一旦数据可以进行资产化，那么，数据的流通、数据的互动会极大地驱动人工智能产业的发展，特别是医疗和金融等等行业会大规模受益。

张亚勤： 过去的数字化更多的是“内容的数字化”、“信息的数字化”，现在和未来的数字化是“物理世界”和“生物世界”的数字化，到时产生的数据会是现在的上千倍或者上万倍，例如，自动驾驶汽车每天所产生的数据是 TB 级别。

大量的数据是一种优势，因为会使得 AI 算法更容易使用，同时也能够让场景衔接更加“自然”。例如，在自动驾驶方面，大量的数据会成为汽车以后超过人的重要因素。毕竟，人用眼睛只能看到有限的数据，汽车有各种各样的传感，可以感知到更多的数据。所以，大量的数据是中国 AI 的一个优势。

为什么我特别看好自动驾驶？自动驾驶是汽车行业百年来的大机遇，一百年来，汽车主要依靠燃油机和引擎，现在电气化和智能化让中国的人工智能超越了别的国家。另外，实现自动驾驶还需要各种各样先进的传感器，也需要各种各样新的芯片，需要定位的系统，需要智能的决策，因此这是一个大产业、有很大的体量，需要很多的技术，AI 也在里面起到很大的作用。所以，未来的十年不管是数据还是产业机会，包括人才等等整个的体量都是十分令人激动的。

邝子平： 刚才提到的这些非常有前景的具体行业，这里包含多少中国特色、中国优势、中国元素？

张亚勤： 符合中国特色的第一个是数据，因为这些数据所产生、所使用主要是中国的用户。也让我们从信息社会内容过渡到了物理社会和生物世界。因此，我认为这是中国的元素：由于人多所以数据量比较大，再就是产业本身大的体量。

李开复： 我来谈一谈中国元素对四个产业可能带来一些特别独特的机会，首先是智能制造和工业互联网。因为中国是世界的工场，所以我们有最好的制造的流程和技术，同时中国的人力在过去的二十年也涨了十倍，所以现在有些产业在流失。再加上产业链的调整，因此，我们是有非常大的必要让这些生产，尤其是高端的生产留在中国。

想要达到这样的目的，必须要把人力成本降下来，所以自动化的质检、自动化的制造，整个流程上的无人驾驶的叉车等等出现了。另外，整个工业自动化的过程对国家和经济是有必要性的，可以得到政府和民间的双重推动。

第二，同意是亚勤说的无人驾驶，技术方面我都非常赞同，但是中国也有一个很大的特色，中国车拥有量的比例远远低于美国，所以更适合在大家还没有形成买车习惯的时候展望未来的无人驾驶的出租车、无人驾驶的接驳车、无人驾驶的货车。

不需要经过办公交的状态，即我想买车、需要买车，买车是人生的目的。我们甚至可以想像公交可以定点制造，或者是像高铁一样，让其在高速公路上面，把人从一个城市带到另一个城市，但同时不需要轨道，因为无人驾驶是有道路和建设的加持。

另外，美国在讨论无人驾驶时候，一般路就是路、城市就是城市，必须要用 AI 解决非常多变化不可预测的新环境，但如果在中国新基建的过程当中能够把道路变得更聪明，把城市建设变得更聪明。例如，让道路能够看出来汽车可能要开出道路的范围，或者是在城中心把行人和汽车分流，这些对美国或者欧美来说都是特别高的成本投入。而中国在新基建的背景下，能让国内的无人驾驶把美国难落地的技术安全地推出。

第三，再看医疗。从全球的角度讨论，整个医疗 +AI 是疫情过后看到的热点，但是针对中国的特色来说，一定程度就是我们有机会获得后发优势。就像过去信用卡在中国还没有那么流通的时候，我们的移动支付能够有后发的优势。

医疗在中国现在还有很多不完善的地方，所以有更大的动力去拥抱新的技术，例如用大数据进行 AI 辅助诊断；把 AI 用在放射科、制药方面。现在我们也面临着大环境的医改、药改，所以有非常大的动力把 AI 数字化。过去在中国的医疗 IT 化不足、数据化不足，当然也很难做 AI。但是通过改革可以一次性地把 IT 化、数据化、AI 化三者的红利一起获取。

另外，为什么中国有特别大的机会？就是因为欧美的隐私法律过度严格，即便脱敏的数据也很难聚合共享，所以我认为现在虽然中国的医疗是落后美国的，但我认为因为这些因素，未来的十年理应由中国公司领跑世界医疗。

最后谈教育。中国的教育科技一直走在美国前面，因为中国家长过去“独生子”的政策，望子成龙、望女成凤的心态，愿意投入教育费用。美国没有这种课外辅导额外付费的习惯，基本是期待着上正规的课，所以做教育的科技创业就只能卖给学校，这个就让美国的教育科技很难发展，所以未来中国教育的发展可以更多地靠家长付费的意识，提出更多的创业方向，比如用 AI 帮助英语的发音，帮助自动修改作文，把学习变得更加游戏化等等。因此，中国教育企业领跑世界的机会也非常大。

三、未来十年：行业平台机会涌现

邝子平：刚才大家提到若干未来 AI 能够有垂直发展的领域，意味着将来 AI 是无处不在，很多行业都会有 AI 赋能的事情发生。那么，未来的十年 AI 平台还有机会吗？换句话说，假如医疗是 AI Drug Discovery Platform，还是用 AI 专门研制某一个疾病治愈的药物。因此，AI 赋能各行各业到底是各方面的细分还是平台仍然有机会？

张亚勤：要看怎么定义平台，大的云智能平台对初创公司来说机会比较小，关于云智能平台，美国可能就是微软、亚马逊、Google；国内就是 BAT 和华为，也不会超过五个。但是在这个大的平台之上可能会有一些行业平台，上面还有一些服务 SaaS，大部分初创公司是在 SaaS 领域。要看美国过去十年，最近几年发展最快的都是 SaaS 公司，AI 方面相信会按照同样的模式。所以一方面也会有小平台，另一方面，很多很深的 Deep Tech 公司，并不一定是细分某个领域，但是可以解决一些通用的问题。比如传感器现在也有很多机会，包括各种触摸传感器，3D 传感器等等。

一个初创公司要有很强的技术、很强的壁垒，具体解决一些问题，并不一定都是平台，也不一定非要是很细分

的领域。初创公司一开始也不要把平台作为自己的目标或者商业计划，因为平台不是这样成长起来的。刚开始一定是聚焦解决具体的问题，然后可以平台化。

李开复：我对 AI 的前景是非常看好的。在经济各个行业方面，几乎每一个传统行业都可以用 AI 对接，而且大部分行业可以迟早用智能化重新赋能，带来的产业升级是 AI 最大的机会。

那么到底是通过 AI+ 来做还是 +AI 来进行？ AI+ 当然是过去的主要模式，也就是旷视、商汤和视觉从一个切入点进去，然后根据第一个应用： 人脸识别和安防，做出更多的应用。从中可以逐渐找到更大的市场，技术的融合性不断提升，客户越来越满意，布置得越来越快，商业价值发挥得更明显，然后就不断地滚动，可能潜在成为某一个平台。

另外，如果有“平台梦”，可以参照旷视和商汤的路径，但即便是这两个公司也很难说就会成为巨大的平台公司，毕竟 AI 本身是赋能，还是要和行业进行对接。综上，伟大的平台一定都是用单一的应用切入，得到成功以后不断滚雪球滚大。

+AI 就是传统行业拥抱 AI，已有一定程度的平台，无论是企业级应用、工业医疗等等平台，看到有这样一个 +AI 的机会，无论是收购一个 AI 公司还是自己雇佣一个 AI 团队，能够打造成为一个传统行业 +AI 的平台，个人认为这一类的平台会有更大的机会，理由就是今天主流被用的到 AI 技术的门槛不断下降，所以传统行业的领跑者已经有了很大的品牌和客户的优势，加入 AI 的难度要远远比一个 AI 公司去学传统行业挑战巨头容易很多，所以我认为 +AI 是主要的模式，带来的平台可能还是以行业平台为驱动，AI 作为重要的技术辅助为主，AI+ 也有机会，但我认为是可遇而不可求。

陆奇：平台从商业的角度来讲需要相对比较分散的供应。如果是相对集中，平台很难抽象出来。人工智能早期技术渗透还不够，在早期大部分的人工智能应用都进行“端到端”重新设计。但是等到人工智能应用特别是行业应用普及以后，横向在某一个层次创新，特别是某一个行业的平台机会是会相对越来越多的。

即使是横向的平台，今天能够看到的人工智能早期应该也有机会，例如如何把数据孤岛打通。目前我们虽然有很多大的云服务，但是越来越多的企业数据已经分散在几个“云”上面。另外，如果应用很集中，也有大的企业垄断这个行业的话，那么平台的成功概率比较小。但是，早期平台的机会也存在； 长期，行业平台的机会可能越来越多。

邝子平：例如 Tensorflow，如果在中国，这种有雄心的、庞大的平台，会考虑投资么？

陆奇：判断标准是： 平台是不是明确解决了客户痛点。假定一个创业者在做类似的平台，我们最关注的是： 客户没有被其它的替代品很好地满足； 另外，需求有增长的趋势么？如果痛点很明确，且不容被替代满足，那么很值得早期投入和扶持。

四、新基建：发力降低 AI 创业门槛

邝子平：过去的十年中，中国的政府在安防、城市管理等等方面给 AI 的企业提供了巨大的落地场景，现在新基建也有大的投入，各位能给政府一些提议么？即未来新基建当中，政府有哪些投入方式？如何帮助 AI 行业在未

来的十年很好的发展?

曹勖文： 我个人认为开源技术能够带来很多生态效益，所以希望政府能够更多地支持开源 AI 的技术，可以分为两部分： 第一是供给端，比如支持高校开源： 研究的项目应该尽早开源从而获得业界的反馈，然后让开发者、工程师也能够参与提供一些支持。另外，学生可以尽早投入开源，锻炼实战能力，同时可以支持大型企业开源已有的项目，成立以开源技术为核心，通过开源模式获利的主要初创公司的模式。

第二是需求端，希望为开源的 SaaS 购买提供税收方面的优惠，中国会有不少 AI SaaS 公司，SaaS 在中国非常难生存，难点主要是在销售，除非客户是偏互联网和技术型的公司，可以比较自然地以类似 C（消费）端的产品方式切入。不然基本上是 B 端（企业），周期太长，不太利于迭代，中小企业能力比较弱，销售成本太高，可能入不敷出，这是 AI SaaS 企业普遍遇到的通病。

陆奇： 我们非常关注降低创新的门槛，当前开发者面临的情况是： 不需要写很多代码，过去三十多年累积的开源软件和开放接口，把整个移动和云生态的创新代价降得非常低。

但是人工智能时代其实门槛非常高，政府应该多做降低门槛的工作。具体而言，政府适合做的是启动、补选和引导。

对于人工智能创业企业来说，比较需要的有以下几点，第一是好的落地场景，尤其是企业的第一个落地场景和未来的闭环迭代至关重要，新基建其实可以起到非常大的作用，特别是国家能够影响和控制的企业场景非常多，如果可以在一定程度上充分利用好这些场景资源，创业公司可以更好地建立闭环的迭代，创新的速度会快很多。

第二，中国企业的 SaaS 渗透低。人工智能目前从创业的角度来讲，B 端相对来讲比较难切入，主要是中国企业的 SaaS 渗透不够、数据不够多，一旦企业 SaaS 渗透率高，人工智能创业公司的机会越来越多。因此，可以从政策层面引导鼓励更多的企业采用 SaaS，毕竟，这可以为人工智能创业公司带来更多的数据资源。

最后，创业环境中 AI 创业公司会经常遇到资金问题。有些公司的（细分）行业从传统风投的角度来讲，天花板太低。但是这些企业长期可以运行得非常好，所以如何提供银行贷款或者其它形式的资金资源就变得非常重要。

李开复： 刚才两位介绍了初创阶段的 AI 公司，我来讲一讲 AI 公司从运营到扩张的过程当中遇到的一些问题。AI 公司在很多新的技术刚刚落地的时候，存在的问题是价位偏高。例如新能源汽车，刚开始可能就是太贵了，政府补贴之后能够量产，量产之后价格下降。

在 AI 层面，例如工厂进行的智能制造，无论是 AGV 取代人力的搬动，或者是采用智能手臂进行抓取，工厂的老板都知道使用 AI 自动化的技术可以节省人力成本，但是，考虑到用机器替代，要很多年才能收回买机器的成本，于是就不会采用新技术。因此，政府的补贴能够更快地引入 AI 技术，然后实现量产。

所以，工业互联网、自动化制造、智能仓库、智能工厂等 AI 企业的难点在于能不能把最开始的成本降下来。

另外，新基建会给 AI 很多机遇。以无人驾驶为例，在国外很多公司背后都是有巨头公司支撑，例如，Waymo

背后有 Google。国内是非常特殊，顶级的无人驾驶公司都是在风险投资支持下“运营”，国内也有大公司开发无人驾驶，但是毕竟 Google 这样的体量目前还达不到。那么，国家大力支持的新基建，能不能让有些城市有更宽松的法律或者有更好的道路让无人驾驶更早地运行起来，毫无疑问，这样也会推动无人驾驶的发展。

最后，政府的引导对医疗意义重大。因为在国外医疗和保险当中，国家的参与度还是相对较低的，国内是相对较强的。医疗和保险这两个行业都有大量的数据，如果政府能够引导对接数据，这对病人、对用户都是巨大的好消息，因为可以得到更好的医疗、更好的医生、更好的诊断。

张亚勤： 政府首先应该在基础研究方面下功夫，例如针对 AI 新的理论、新的算法，下一代超越深度学习等等，因为这种基础研究企业投资意愿可能不强烈。

另外，政府应该关注人才的培养。现在很多高校都有 AI 专业，所以，应该鼓励 AI 专业招收更多的博士生和研究生。在未来建设的重点“新基建”的 7 个项目中，有 4 个都和 AI 有关。

其次，政府还要推动数据的共享，例如健康数据、保险数据和公共数据，各种各样的数据如果能够公开，尊重隐私安全的条件下，政府应该推动共享。我们的公共数据目前的数量和开放的程度是远远低于英国或者美国，所以，政府还有很多能够做的。

最后，初始企业还是要把商业模式通过市场化进行发展，不能光靠政府，政府的项目太多会让企业麻痹，政府也不要单独扶持几个企业，可以扶持行业，提供公平竞争的环境。

五、人才之痛：应用型人才缺乏

邝子平： 有众多文章指出，美国 AI 的主力之一是从国内到国外读书的留学生，它们大多数都有国内本科的经历。所以，我们展望未来十年，由于地缘政治很多的不确定性，大家认为中国的 AI 企业有没有人才危机？优秀人才将来会来自于哪里？企业到哪里去寻找这些人才？

陆奇： 大部分的初创公司主要是： 应用已经发明的算法框架到具体场景从而实现落地。其实，更重要的是人才，主要指能够从技术、产品和客户的需求几个方面，进行有机融合的人才。

大专院校培养出来的人才实际操作能力会弱一些。所以，我们需要把创业人才引进大专院校，毕竟，现在我们需要的是创新的能力。

拿微软举例，微软本质上更是一个技能大学，优秀的程序员、优秀的产品经理，如果在微软工作过两三年，其能力基本上就能够培养起来。希望以后的高校有越来越多创新的氛围和创新能力的培养，黑客文化的精神也能够让越来越的企业成为“人才大学”。

另外，一部分创业公司确实需要前沿算法，那就要跟科学家团队对接。所以，存在一定的挑战，因为科学家团队往往对行业对技术想得比较深，如果和产业相结合就需要专门的人才进行组合这些科学家，从而将些前沿的场景落地。

李开复： 人才危机肯定还是有的，AI 人才永远都是短缺的，但是不像过去那么短缺。我们应该创造更多的机会让海外的科学家、工程师回来。

虽然现在有很多的传统行业不需要顶级的 AI 人才，但寻找合格的 AI 工程师也不容易。所以，高校应该更加重视应用型人才的培养。

我们曾经和高校办过一些培训的项目，主题为应用型人才的训练，但是很多高校老师都不赞成，他们表示我们需要培养研究型人才。其实，应用型人才是非常短缺的。创新工场投资的一家公司就是看到很多还不是 AI，主要就是编程，程序员在高校当中得到的培训并不立即适合对接到一个就业的机会，所以需要重新培训。因此，希望高校提高对应用型人才培养的重视度。

张亚勤：以后通用型 AI 人才中国应该不会缺，因为很多学校都开设了 AI 专业，比较稀缺的是系统化思维的 AI 人才，要求其不仅仅能看到某个技术模块或者算法，而是通过系统化思维把框架从头到尾规划出来，然后找到合适的人执行。

曹勖文：国内不太缺初级工程师，甚至初级工程师有点泛滥，高端的工程师在任何行业都是稀缺的。

AI 需要更多的理论，理论固然重要，国内主要还是缺实际操作经验，高端的工程师需要做过大项目，解决别人没有解决过的难题才能锻炼出来，高校可以给理论基础，更多的还是要在业界大公司中的大项目进行锻炼，因为很多的特殊场景、规模只有大公司才有。

六、构架负责任 AI，造福全人类

邝子平：AI 作为一个新生的技术给人类带来了很多的好处，但是也一直有些争议，作为 AI 行业的投资人、领军人物和整个中国 IT 行业发展的意见领袖，希望几位给未来十年 AI 企业的创业者、企业家提出一些建议，如何能够增强我们企业的社会责任感，能够让 AI 确实造福人类。

李开复：我非常认可一句话：权力越大，责任越大。AI 是有史以来所有计算机科技当中权力最大的，因为它帮助人类甚至替代人类做出的判断是会影响别人“前途”，例如贷款、就业，甚至医疗还有很多领域存在健康和生命的后果。

所以我们的权力非常大，怎么才能有更强的责任心？一方面是要制造好的工具。另一方面也要让 AI 从业者和工程师都看到我的数据量可能不足，可能无法解释，可能会带来灾难。更重要的是对所有的 AI 从业者、AI 工程师都要有更多对社会、对人文的关怀，也要了解自己的责任，只有把多方面融合起来才能做出更负责的 AI 企业。

张亚勤：AI 带来的社会变革是有史以来从未有的，我们必须要负责任。无论做什么事必须要有底线。

我自己的原则是：我们都有孩子，我们不希望未来孩子发生战争，那么，就不要把 AI 用作武器；我们不希望小孩吃有污染的东西，那么就要推进有机食品；我们不希望孩子用毒品，那么就不能投资大麻公司等等，按照这个原则作为投资或者从事技术研究的指导，便能构建负责任的 AI 社会。

陆奇：首先建议做 AI 产品的工程师和产品经理要有“站在历史对的一面”的心态，因为今天的法律、今天的社会价值观往往没法预测未来，我们很多 AI 产品其实在开拓未来新的生活和工作的环境，无法等政府和法律管理，因此在做产品的过程当中有底线、有价值观、有责任心。

15 AI 交通

中科院自动化所研究员王飞跃：交通 5.0 — 何以实现智能交通到交通智能？

整理：智源社区 任黎明

王飞跃，中国科学院自动化研究所研究员、复杂系统管理与控制国家重点实验室主任。他的主要研究领域为复杂系统、智能控制、智能机器人、无人驾驶等。他曾先后当选 IEEE、INCOSE、IFAC、ASME 和 AAAS 等国际学术组织的 Fellow，并且主持完成多项国家重大项目。曾获国家自然科学二等奖、IEEE SMC 诺伯特·维纳奖。

王飞跃的演讲主题是《平行交通与交通 5.0：从智能交通到交通智能》。在本次演讲中，王飞跃对人工智能与智能交通的发展现状和未来趋势进行了系统分析，并重点分享平行交通和交通 5.0 的基础理论、关键技术及最新进展。随着交通系统从机械化、电气化、信息化、网络化到智能化的不断完善和提高，以区块链为核心技术的交通 5.0 时代为智能社会奠定了基础。为了实现交通 5.0 和交通智能，王飞跃团队提出基于 ACP 的平行交通系统体系和研究开发了交通管控云网端协同平台，他和团队的研究成果已经成功应用于广州、青岛、杭州等城市的交通管控中并获得了显著的效果，并且在演讲的最后，王飞跃对人工智能的新未来进行展望。以下为演讲全文。

一、来自 AlphaGo 的启示

王飞跃从 AlphaGo 将去向何方的问题引出对人工智能在交通领域重要性的探讨。目前，很多人认为 AlphaGo 已经无新技术可以研究，而王飞跃则认为 AlphaGo 是一个具有里程碑性质的工作，AlphaGo 的出现把我们从 Church–Turing Thesis 推向 AlphaGo Thesis 的新时代，这个时代具备以下三个特征：

- 平行世界：真实 VS 虚拟，现实的虚拟，虚拟的现实。
- 从牛顿到默顿：从牛顿的“大定律小数据”到默顿的“大数据小定律”，按照默顿自我实现运营的一个新时代；
- 智能活动的三部曲，即从**小数据生产出大数据，从大数据凝练出深度智能**。

如何从大数据中提炼出深度智能，AlphaGo 就是一个很好的样例。AlphaGo 从人类的 80 万例博弈开始，自我对抗“生产”出 7000 多万例新的博弈，并利用强化学习提炼出“深”智能的二张网，价值网和对策网，战胜人类的围棋大师。在此基础上，AlphaGo 进一步升级，成为 AlphaGo Zero，人类博弈的小数据几乎为零，除了博弈规则之外，一例不用，仅凭自我对抗产生的不到 3000 万例博弈，就炼出一张智能更深的“小智能”网络，将过去的二张网合二为一，回头以 100:0 的战绩横扫 AlphaGo。后来 AlphaGo Zero 再升级为 AlphaZero，不但围棋可下，其它棋也可以下。这些深度智能使得 AlphaGo 之类变得“聪颖无比”，所以 AlphaGo 之类将成为未来智能决策及智能产业范式转移的示例和基础。

二、大趋势：三个三与五个五

接着，王飞跃介绍了 AI“三个三，五个五”的大趋势。三个三中的三个 IT 分别对应三个世界和三个轴心时代，具体为：

人工智能的大趋势

New Logic，New Development，New Philosophy

图 1 ： 人工智能的大趋势

“三个三”：

- “老”IT 工业技术是开发物理世界的工业时代的主要工具，其对应人性大觉醒，以哲学突破为核心的第一轴心时代；
- “旧”IT 信息技术是开发心理世界的信息时代的主要工具，其对应理性大觉醒，以科学突破为核心的第二轴心时代；
- “新”IT 智能技术是开发人工世界的智能时代的主要工具，其对应智性大觉醒，以技术突破为核心的第三轴心时代。

“五个五”：

- 大 5G：从 Grid 1.0 到 Grid 5，即交通网，能源网，信息网，物联网及智联网；
- 大 5G 的建设促使社会形态发生的巨变：五个范例，交通变成社会交通，能源变成社会能源，计算变成社会计算，3D 打印机器人使制造会变成社会制造，最重要的是智能变成社会智能，最终社会变成智能社会，智慧社会。
- 大 5G 建设完成后会形成大网，它把三个世界紧密联系在一起。并且在智能科技时代将数据的力量，计算的力量，算法的力量，网络的力量，区块链的力量融合在一起，形成“**五力合一**”。

其中，区块链带给平行智能的技术特点为：**真（TRUE）（可信、可靠、可用、高效）+ 道（DAO）（分布式的去中心化、自主性的自动化、组织化的有序性），从平方道 $D^2A^2O^2$– 平行道迈向平行智能。**要实现平行智能必须要有一个五度空间才可行。

- 五度空间（CPSS 物理空间，网络空间，人工世界，心理世界，物理世界），并将人与社会因素放在核心的位置，人是万物的度量，人必须是这五度空间的主人公。
- 五类产业形态（工业 1.0,2.0,3.0,4.0）很自然转变为工业 5.0，认为我们仍在第三工业革命之中，它包括工业 4.0 和工业 5.0 二个阶级，虽然工业 4.0 和工业 5.0 的核心都是 ICT+CPS，但是工业 4.0 是以工业自动化思维为基础。它们之间最主要的差别为从工业自动化向知识自动化的转变（图 2）。王飞跃在 2000 年和 2004 年

的一篇题为《平行系统方法和复杂系统管理与控制》的文章正式引出了平行系统及工业 5.0 的概念。

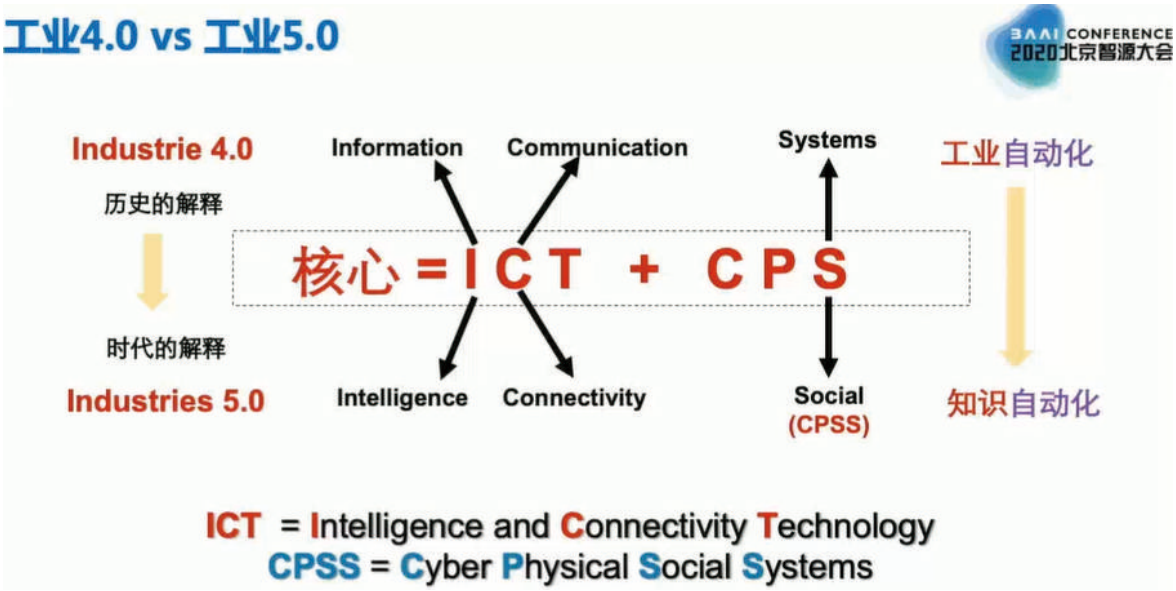


图 2：工业 4.0 迈向工业 5.0

三、新理论： CPSS 和 ACP

然而，若想实现智能化就必须从 CPS 转变为 CPSS，并且智能化的核心为知识自动化。即 AR，VR 和人工智能之外，还要是通过平行系统实现的自动化智能。未来的机器就是一个平行机（图 3 所示），这个平行机把物理的牛顿机和软件定义的默顿机合二为一，把物理，社会，网络空间打通，把云端和边缘串起来，通过小数据生成大数据，把大数据变成小智能。因此，这个平行机可能给我们带来一系列新的工作，如决策、法务、评估、学习工程师等。 图 4 为平行系统的理论计算框架（其中包括控制部分）。

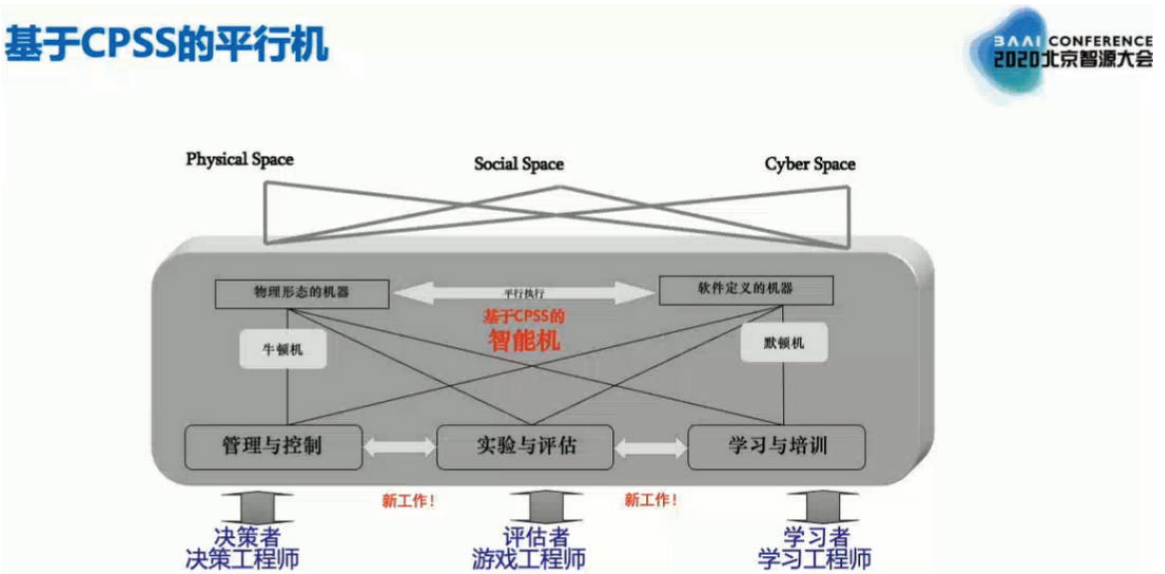


图 3：基于 CPSS 的平行机

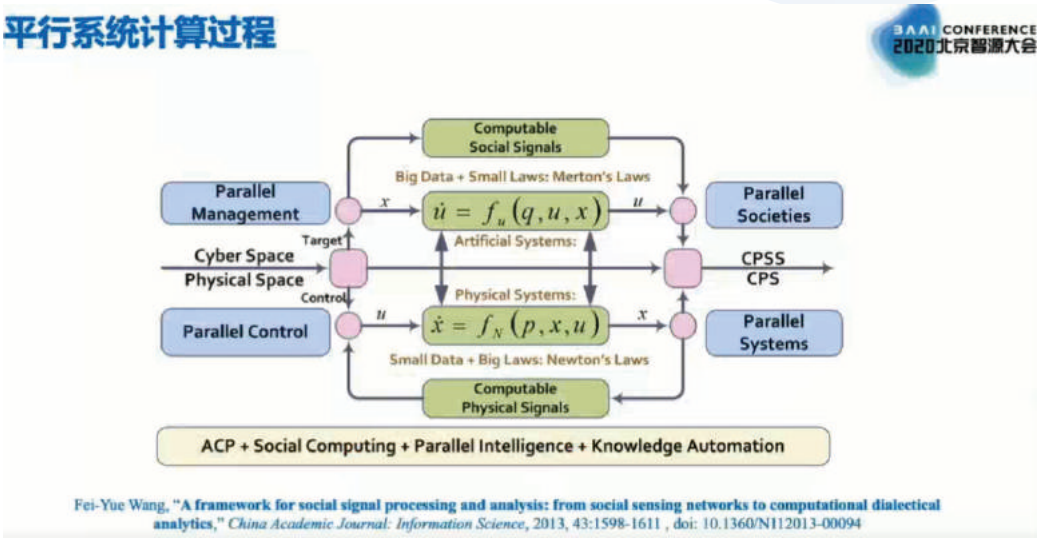


图 4：平行系统理论框架

2011 年，复杂系统管理与控制国家重点实验室成立，其研究核心为发展平行智能与平行科技，主要研究平行管理与控制、平行机器人，平行制造、平行医药、平行健康、平行社会，平行生态等等。为什么要研究平行？回顾使人工智能陷入十年寒冬的 Lighthill 报告，当时，Lingthill 认为人工智能的研究已经很久，但还在研究 ABC 水平的问题。有一部分学者研究先进自动化 A，另一部分学者研究计算机仿真 CNS，C，而这两部分跨度太大，如何可以使两个世界联系更加密切呢？这就来了第三波人，利用机器人建“桥”，Bridge，就是 B。但是，干了 25 年，桥还是建的不好，还在水下，不行，无法跨越“认知鸿沟”。王飞跃提出通过大数据填充鸿沟并提炼平行智能，再由平行系统架桥实现端到端的联结，跨越认知的鸿沟（图 5 所示）。

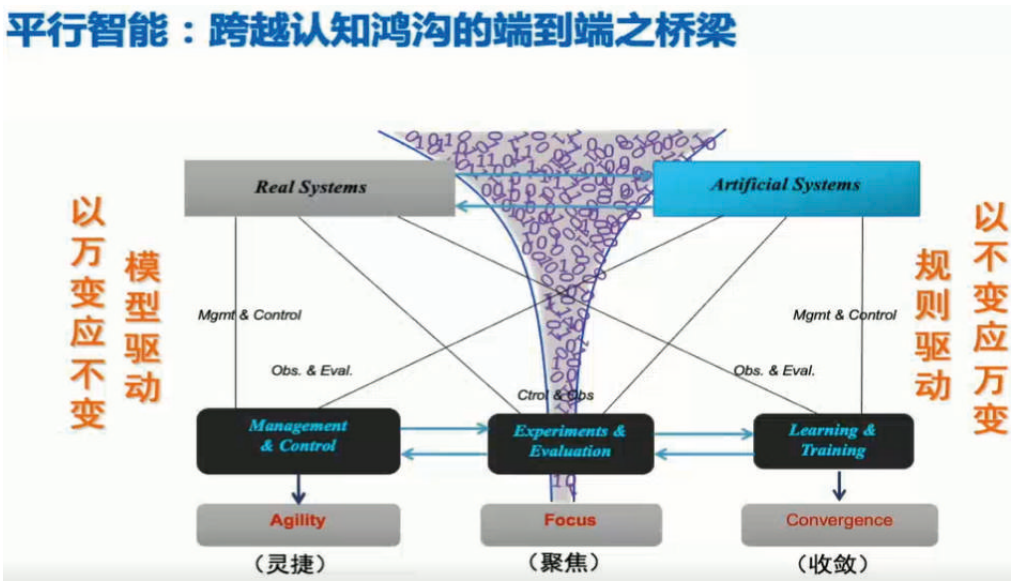


图 5：平行智能：跨越知识鸿沟

为什么大数据和平行可以合在一起？首先，大数据的实质为**“ 数据说话”,“ 预测未来的最好方式就是创造未来”**:

- 数据说话多了就变成了人工社会（A）及软件定义的社会，变成社会的数字孪生，即描述智能；
- 预测未来就是计算实验（C）把小数据变成大数据，把大数据变成小智能，即预测智能；
- 创造未来就是虚拟世界与现实世界合二为一，通过平行执行（P）实现虚实空间之间的反馈闭环，即引导智能。

通过上述大数据的三点本质可以实现从以前在物理世界“吃一堑”、在知识世界“长一智”，变到在知识世界“吃一堑，吃多堑”、在物理世界“长一智，长多智”，通过大数据和平行智能达到在物理世界低成本高性能高智能的目标。

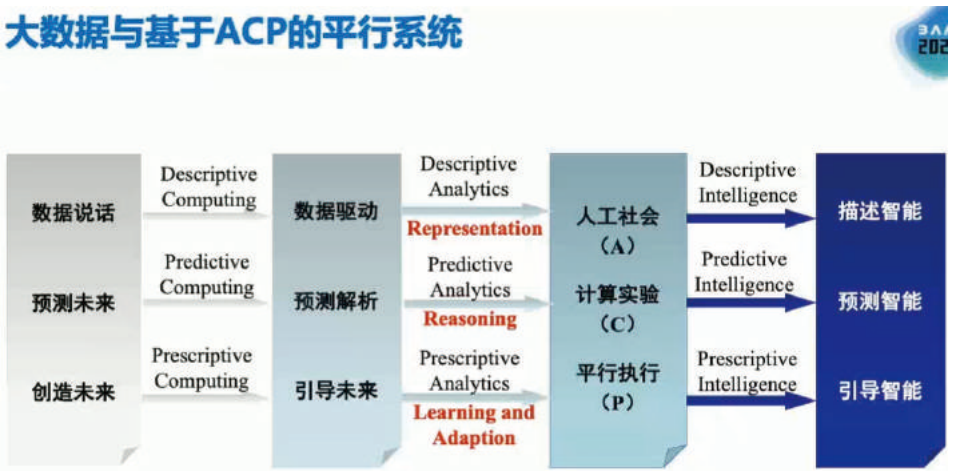


图 6： 大数据与基于 ACP 的平行系统

四、智能交通系统的新时代：从平行交通到交通 5.0

随后，王飞跃介绍了如何将平行智能应用到交通领域。交通 50% 是工程复杂性，50% 是社会复杂性，所以交通领域是一个天然应用平行智能的场景。图 7 为平行交通系统体系，PTMS（平行交通管理系统）既包括真实交通系统又含有虚拟交通系统，它使得计算机变成交通实验室用来进行实验评估、学习与培训和控制管理，然后把相应的硬件合成起来变成社会交通，图 8 是平行交通系统的软件接口。

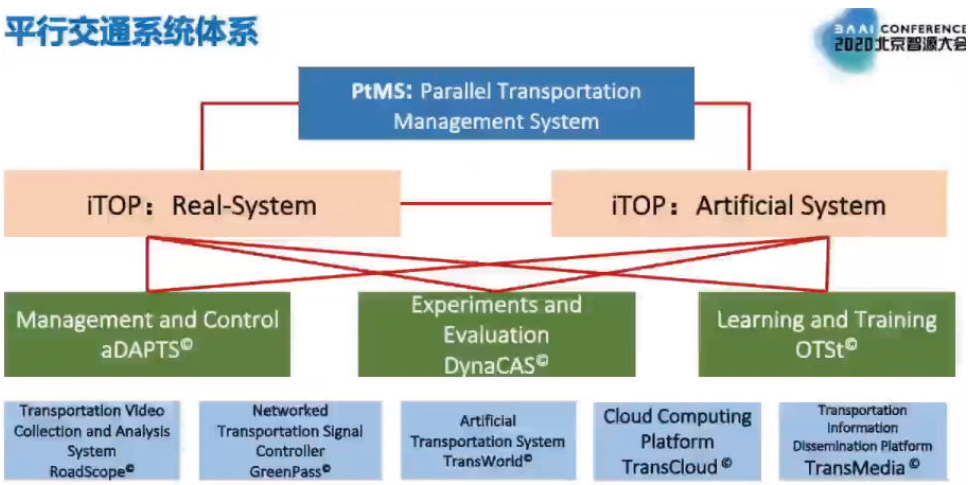


图 7： 平行交通系统体系

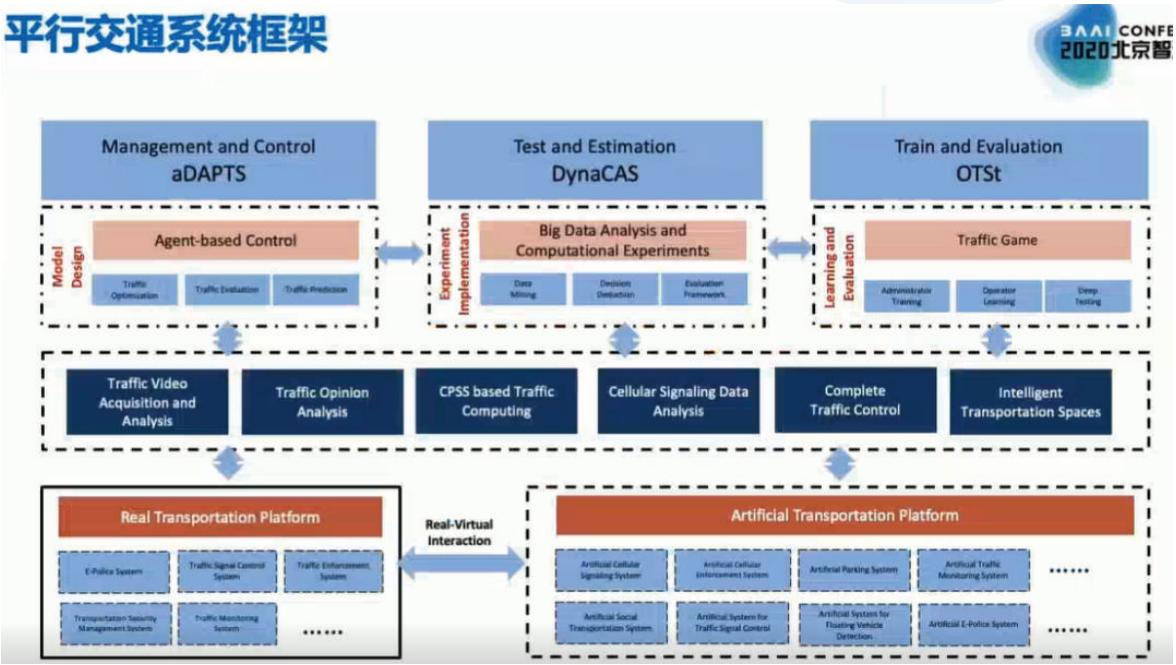


图 8： 平行交通系统软件接口示意图

上述虚实互动平行交通管理体系架构与技术可以解决交通领域的以下难题:

- 应用人工交通作为交通数据输出器可以解决交通领域存在交通参与主体众多，影响因素复杂等研究难题，
- 将计算机作为交通实验室，把小数据变成大数据，大数据变成小智能解决交通领域实验成本高，可重复性低的难题;
- 通过虚实空间平行执行及双闭环控制解决交通领域决策效率低，控制质量差的问题。

虚实互动平行交通管理系统的最终目标是建成可认知，可计算，决策优的智慧交通系统。为实现这个虚实互动的平行交通管理系统，王飞跃提出了基于实验设计、自适应动态规划的大规模路网交通预案实验和优化方法；构建了交通实验场景生成和预案评估的计算引擎平台实现软件定义的交通场景； 此外，他提出的基于人机混合增强智能的交通推荐技术 , 攻克了城市交通管控决策过程复杂、效率低、可靠性差等问题。

而针对传统交通感知系统面临适用环境单一、安装条件受限、设备成本高、系统化程度低、无法满足复杂交通场景的精细刻画和管控需求等一系列难题，王飞跃提出了交通平行视觉感知技术，这个技术可以产生一个从少量真实场景快速生成大规模虚拟场景（人工场景）的方法 , 这个方法提高了虚实互动交通视觉模型的精度和鲁棒性，并且有效的解决了复杂交通场景数据难获取、标注成本高等问题。

在基于无线传感网的城市交通空间综合感知技术应用方面 : 王飞跃构建了融合多模式交通行为特性的传感网络拓扑结构设计与优化方法（图 9），并提出了多源异构交通数据分层关联融合方法，这些方法大大提升了交通感知范围广域化和感知要素精细化水平。

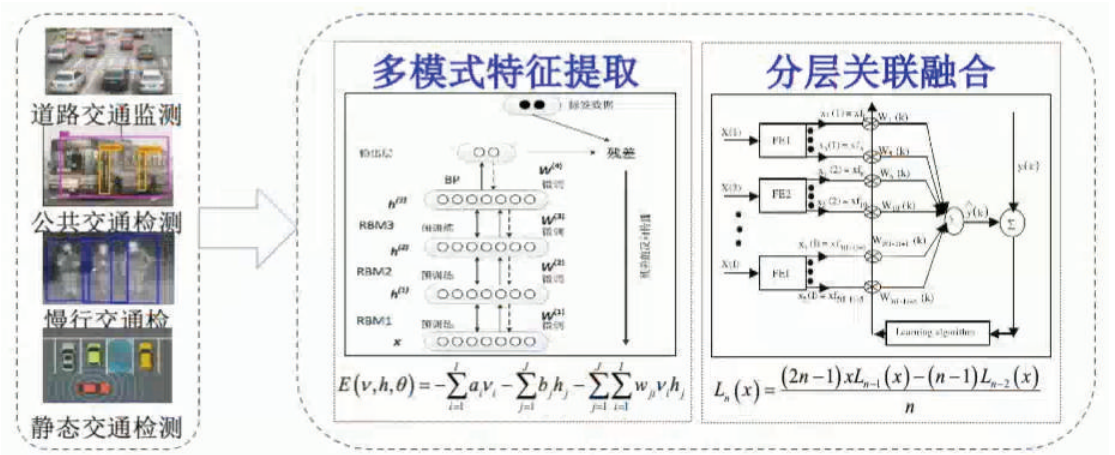


图 9： 多模式交通行为特性传感网络架构

针对城市交通管控平台技术标准不统一的问题，以及我国城市交通在交通流组成、路网结构、出行习惯等方面的独特性，王飞跃通过基于交通云端模糊神经元网络与边缘侧模糊规则融合模型和城市道路混合交通智能协同控制关键技术开发了集主动控制、防溢流控制、关联控制于一体的交通管控云网端协同平台（图 10），这个平台的原则是当地简单，远程复杂。

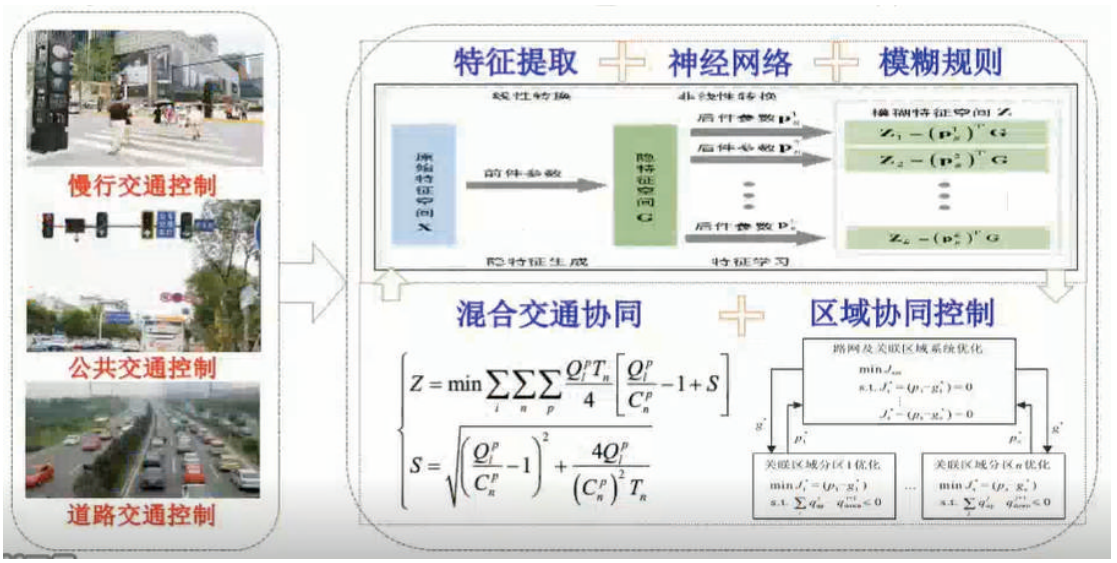


图 10： 云网端协同网络化交通平台关键技术

这个平台可以实现实际交通的按需控制。目前，这个平台主要应用的城市有青岛，苏州，广州等城市。

- 平行交通： 济南人工交通系统。这项应用主要是通过仿真进行交通压力测试，即假如城市拥有一百万辆车时实际交通到底怎么样？ 09 年的仿真实验结果表明只要路网中的车辆数目达到设计量约 15% 就会出现交通拥堵情况，而两年前杭州市的实测车辆数据显示当车辆数约等于设计量的 15% 会出现交通堵塞，这个数据印证了济南人工交通系统仿真结果的真实性。

- 广州亚运会公共交通平行管理系统。这个系统可以把所有公共交通出行报告和方案在计算机实行进行评估，以优化公交的调度。这个系统特点是它采用平行控制理论，通过实际系统与人工系统的相互连接，通过对二者之间的行为进行对比和分析，完成对各自未来的状况的“借鉴”和“预估相应地调节各自的管理与控制方式；这个系统的应用效果是它可以和智能公交监控调度系统无缝接驳，实现对全市 60 多条线路 8000 多台公交车以及 400 多台中小巴平均每天 130000 条发班班次的实时优化与管理。
- 青岛平行交通系统。这个系统可以实现人工交通和实际交通互动，该系统的实施效果为：主干道通行时间减少 20%，主干道车辆停车次数减少 45%，关键路段的早高峰拥堵里程减少 30%，车辆平均行驶时间减少 25%，路网通行效率提高 43.39%，显著改善了青岛的交通环境；
- 杭州西湖做交通推荐系统（实时配属系统）。王飞跃首次提出交通推荐系统的概念并将其应用到智能交通领域，这个交通推荐系统大大减少了拥堵报警，错误报警的次数，并且大大降低报警事件的平均处理时间（大约为一个红绿灯交替时间）。

接着，王飞跃讲述平行驾驶可以将虚拟驾驶和实际驾驶同步起来，提高交通运行效率。关于如何通过 AlphaGo 理论，实现智能交通系统的未来 ––– 从平行交通迈向交通的 5.0，王飞跃把交通领域的发展划分为一百年。目前，他认为交通也进入了第五代系统，从以前的机器能源（交通 1.0），电动（交通 2.0），信息化（交通 3.0），网络化（交通 4.0），到即将迈进的平行交通（智能化交通，交通 5.0）。若想实现交通 5.0，区块链技术必不可少，通过区块链把五个交通合成交通 5.0（图 11），把城市、公共、物流、静态、社会交通合二为一，打通部门之间的利益交割，做到即保密又公开，区块链可以解决各部门之间的矛盾，做到即安全又可靠，所以区块链技术为交通 5.0 的核心。并且未来社会的发展一定要是通过智能交通迈向智慧城市。

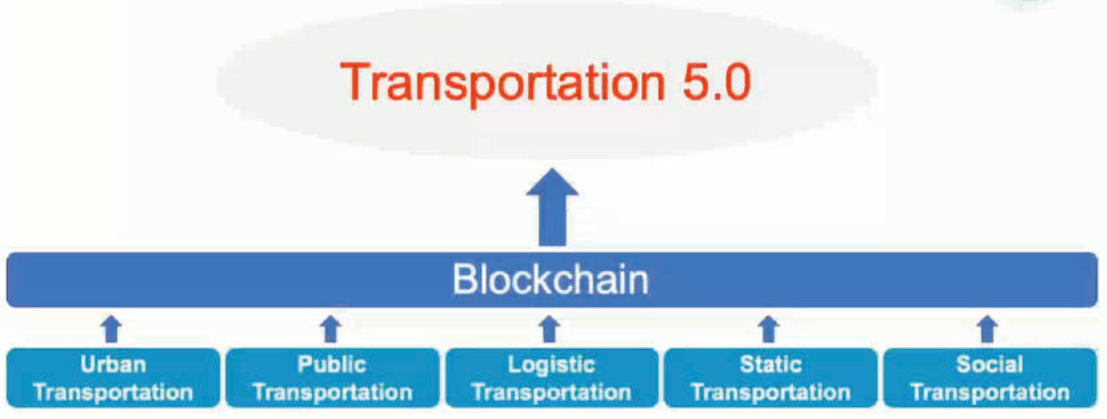


图 11 ： 交通 5.0 的核心技术 ––– 区块链

五、结语及展望：AI 新未来

演讲最后，王飞跃对人工智能的新未来进行展望。关于人工智能可能会威胁人类的这一说法，王飞跃并不认为人工智能对人类会产生威胁。正如 Godel 定理所述，Godel 不相信机器、计算机能超过人，除非数学不是人类发明的，就算数学不是人类发明的，计算机机器也超不过人的大脑。王飞跃把算法总结分为三个层次，第一个是算法智能，第二个是语言智能，第三个是想象智能。并且**算法智能 << 语言智能 << 想象智能**。正如爱因斯坦所言，智能的真正标识不是知识，而是想象。王飞跃相信**人工智能及“ 新”IT 智能技术是人类的朋友，相信人工智能会使人类社会更加开放、更加公平。**并且智能科技是时代的召唤和科技发展的必然结果，它不是人类的威胁，我们应以激动心、敬畏心和平常心面对人工智能的发展。此外，王飞跃希望人工智能只是过去的冬天和夏

天，还要有春光明媚的春天和硕果累累的秋天。中国在人工智能的研究方面要自己的话语权，力争创造“人工智能的直道，在直道自然行车，别强调什么超车。就是超过什么人什么国，也与你我或中国无关!”。

参考文献：

[1] Fei-Yue Wang, Jun Jason Zhang, Xinhu Zheng, Xiao Wang, Yong Yuan, Xiaoxiao Dai, Jie Zhang, Liuqing Yang, Where does alpha Go go: from Church-Turing Thesis to Alpha Go thesis and beyond”, IEEE/CAA Journal of Automatica Sinica 2016,Vo.3,No.2,pp.113-120.

[2] Fei-Yue Wang. Wang Xiao, Li Li et al Steps toward Parallel Intelligence. IEEE/CAT JLS, 2016. 3(4): 345-348.

[3] Fei-Yue Wang, “ Parallel Control and Management for Intelligent Transportation Systems: Concepts, Architectures, and Applications. “in IEEE Transactions on Intelligent Transportation Systems, vol, 11, no. 3, pp. 630-638, Sept. 2010.

[4] Wang. Fei-Yue. Five Transportations in One-A New Direction for ITS From Qingdao[J]. IEEE Transactions on Intelligent Transportation Systems 2015.

[5] Yuan Yong, Fei-Yue Wang. Towards blockchain-based intelligent transportation systems[C]//2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2016: 2663-2668.

[6] Fei-Yue Wang, A framework for social signal processing and analysis: from social sensing networks to computational dialectical analytic[J]. 中国科学信息杂志, 2013, 43: 1598-16l1, doi:101360/N112013-00094.

滴滴出行副总裁叶杰平：AI 赋能智能出行新时代

整理：智源社区 任黎明

在第二届北京智源大会 AI 交通专题论坛中，滴滴出行副总裁、滴滴 AI Labs 负责人叶杰平教授做了《AI 赋能智能出行新时代》的主题演讲。

叶杰平，滴滴出行副总裁、滴滴 AI Labs 负责人。密西根大学终身教授及大数据研究中心管理委员会成员，IEEE Fellow，智源学者。叶杰平主要从事机器学习，数据挖掘和大数据分析领域的研究。担任包括 IEEE TPAMI、DMKD、IEEE TKDE、NIPS、ICML、KDD 等多个国际顶级期刊编委及国际顶级会议程序委员会主席和领域主席。曾获得 KDD 和 ICML 最佳论文奖，以及 2010 年获得美国国家自然科学基金会生涯奖（NSF CAREER Award）。2019 年带领团队获得年度瓦格纳运筹学杰出实践奖（Daniel H. Wagner Prize）。

随着 AI 与各行各业的深度融合，它加速驱动世界经济从“互联网 +”迈向“智能 +”。此外，新一代人工智能的发展对各行各业的带动和影响作用将更为深刻，NEW AI 逐渐成为我国赢得全球科技竞争主动权的重要战略抓手，具有“头雁”效应。在交通出行领域，AI 正在推动交通出行的智能化变革。滴滴作为全球领先的移动出行平台、全球智能出行技术的探索者，近年来，持续大力投入 AI 基础研究，加速技术和经验开放，与合作伙伴一道共同推动 AI 在交通出行领域的变革。本次报告中叶杰平将分享滴滴的 AI 技术如何赋能智能出行发展、如何加速智能出行时代的变革。以下智源社区编辑对叶杰平演讲进行的要点整理。

滴滴作为全球领先的一站式出行平台，它具有极其丰富的出行数据，通过对出行数据的分析优化为全球用户提供出行服务。滴滴拥有的出行轨迹数据不仅数量大，而且非常完整（如滴滴在北京的出行轨迹数据已经覆盖北京大部分道路超过 400 多次）。这些出行数据为滴滴通过人工智能和大数据技术改善交通、为用户提供更便捷更舒心更安全的出行服务、为智能出行的愿景提供了强大的数据支撑。基于此，叶教授分享自己及其团队在智能出行领域的探索。

叶杰平认为未来交通出行（智能出行时代）主要从以下三个层面发生变化：

- 智能交通基础设施（智能化、网联化、协同化），交通基础设施会越来越智能，包括智能路网、智能信号灯，车路协同。
- 智能交通工具（电动化、智能化、高效化），交通工具由电动化、自动化。未来会取代现有的车辆。
- 共享出行（体验化、共享化、综合化），共享出行在未来会越来越受欢迎。

上述三个巨大变化中最关键的变化为智能，所以 AI 是智能出行的核心技术。目前，AI 已经应用于智能出行的多个场景，如括智慧交通，智能交通工具，智能运营，智能调度，智慧供需预测，智能派单等（图 1）。此外，在出行安全方面，地图中的路况预测、时间预估及路径规划中都需要用大量的 AI 技术。客服每天需要解答海量的问题，叶杰平开发了一套基于 NLP– 知识图谱及语音的智能客服系统。这套系统可以满足大部分用户的需求，极大提升了客服的效率，并且为 AI 赋能社会提供基础。

图 1：智能出行

一、AI 赋能交通基础设施

滴滴基于其独有的交通出行大数据，建设了一套集合分析中枢，控制中枢，感知中枢，数据中枢的交通大脑，这个交通大脑包括交通拥堵的实时展示，交通需求和出行规律的分析挖掘，交通拥堵原因探索及信号灯的控制优化等功能。此外，滴滴通过对政府数据，行业数据，众包数据，互联网数据的感知，开发了集大数据研判、实时预警、交通规划、度量体系于一体的城市交通分析工具，这个工具可以实现智慧信控、AI 派警、交通诱导及车路协同等城市化的方案（图 2）。

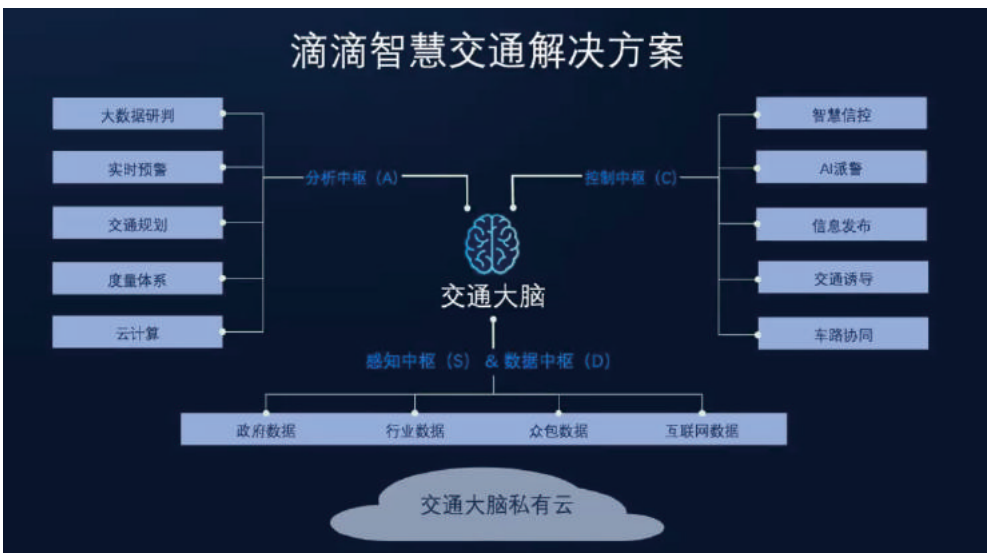


图 2：滴滴智慧交通解决方案

接着，叶杰平介绍了智慧交通项目，该项目由滴滴与政府和城市一起合作，应用滴滴平台的大数据和 AI 技术进行优化分析以形成智能信号灯。具体案例如： 基于滴滴现有的交通运行轨迹数据，结合 AI 和大数据分析算法，滴滴可以对每个十字路口各个方向的车流量进行预测，基于各个方向车流量的预测，交通管理部门就可以智能

地进行信号灯的控制。目前，该项目已成功应用于济南等 20 多个城市，优化了超过 2500 多个信号灯，在优化后的区域，车辆平均行驶时间降低了 10–20%，该结果表明这个项目可以极大的改善城市交通的运行效率。

二、AI 赋能智能车载

随着交通工具越来越智能，滴滴在智能车载方面研究开发的系统会让未来出行更加智能、安全和舒适。

2.1 智能座舱系统

滴滴基于语音智能（包括语音识别、语音合成、语音唤醒、声纹识别）技术开发了一套智能座舱系统。该系统以深度学习算法为内核，以保障驾驶安全为技术主线，支持驾驶员行为识别，身份验证及多模态智能交互功能。智能座舱系统可以提供低成本高性能的智能出行解决方案。针对复杂的车载环境，融合车辆信息，及时识别驾驶隐患，为司机预警，旨在为智能出行提供更安全更高效的出行体验。

2.2 高级辅助驾驶系统

高级辅助驾驶系统是基于 AI 视觉智能（包括人脸识别、人体识别、文字识别、车辆识别）技术开发的一套系统，这个系统与司机行为识别功能共同构成车辆主动安全体系。这个主动安全体系主要包括前期碰撞预警，车道线偏离预警，行人碰撞预警等预警功能。并且在车辆行驶危机时会发出警告，辅助驾驶员减轻或避免碰撞危险，从而增强驾驶的安全性。通过报告中的视频演示可知，该系统会根据驾驶员的错误驾驶操作、不良习惯（未系安全带、驾驶中抽烟，手持接听电话等等不良驾驶状态进行语音提醒，并且可以在斑马线处识别行人并主动减速停车。

2.3 自动化网络剪枝优化视觉系统

由于视觉系统是基于深度卷积神经网络，而深度神经网络的最大的缺点是主干网络非常庞大（如 AlexNet，VGGNet，ResNet 等都超过几百兆）而嵌入式资源又非常有限。这个不足给视觉系统带来巨大的挑战，针对这个挑战，滴滴研发了自动化网络剪枝方法（图 3），该方法可以在识别精度基本一致的情况下使深度神经网络模型的大小压缩了 50–100 倍，极大提升了系统的性能，具体细节参考 [1]。

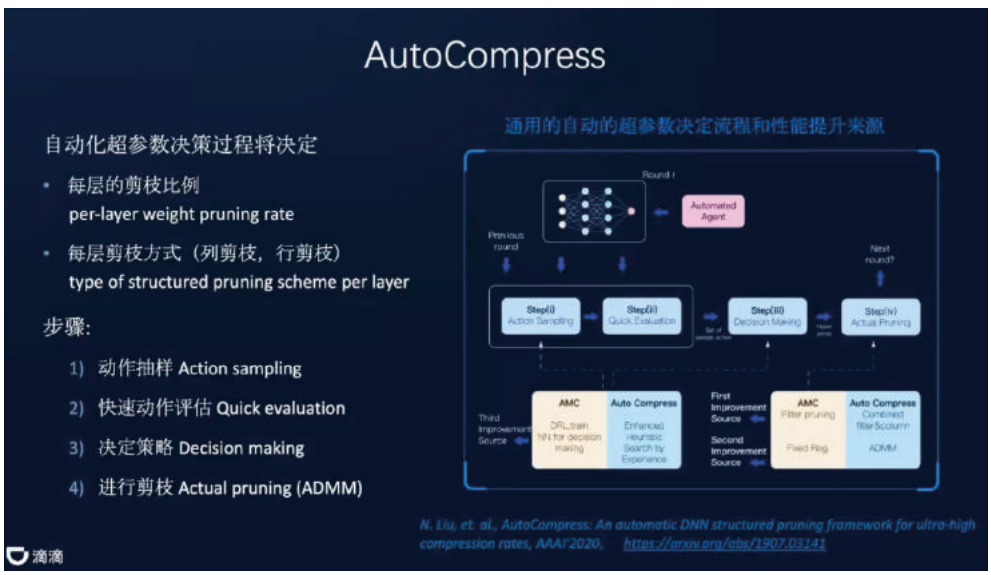


图 3： AutoCompress 方法

2.4 基于语音交互的接单系统

在语音技术应用方面，以前，司机需要通过手动点击屏幕进行订单的处理，包括接单，取消订单，导航等，这些手动操作不仅会导致出行体验差，而且增加了出行途中的不安全指数及驾驶的危险系数。基于此，滴滴研发了一套基于语音交互的接单系统，司机可以直接通过语音进行接单等进行操作，目前这个系统已经应用于日本、澳洲等国家，通过报告中的该系统在日本的应用场景视频演示可知，当订单成功后，司机可以通过语音实时了解乘客的位置及乘坐时间，大大提高了出行效率。未来，语音交互系统将支持包括接单，取消订单，信息查询，主动联系乘客或客服，加油充电维保等全方位的语音交互服务，为乘客和司机提供全行程的智能化服务。

三、AI 赋能共享出行平台

3.1 AI 赋能出行交易市场

滴滴的共享出行平台通过网络把世界和乘客连接起来，为乘客提供全方位的出行服务，满足乘客的多元化出行需求及高质量的服务体验，同时也提高司机的收入及减少空驶以提高交通出行效率。这个共享出行平台服务主要包括发单，派单，接驾和送驾等流程。AI 技术在这个服务流程中贯穿始终，如为乘客推荐上车点及订单预估价，订单供需预测与调控，订单派单，车辆调度，出行安全保障，ETA 及路径规划等（图 4）。

图 4： AI 赋能出行

3.2 基于二分图的派单算法

如何通过 AI 进行派单、调度及订单时间预估？其中，订单分配是滴滴最核心的业务之一。目前，滴滴平台每两秒可以做一次订单分配，滴滴订单分配具体步骤为（图 5）：首先，构建一个将所有司机、所有的乘客订单聚合在一起；然后，构建一个订单与司机两两相连的二分图。这个二分图的核心是两两相连后的权重，将这个权重构建一个矩阵，行表示乘客，列表示司机，矩阵中的值表示司机与乘客的订单匹配度。这个匹配度通过计算司机与乘客的距离及订单行驶时间来确定，如果司机跟乘客的距离越近，行使越短，匹配度的值越高，其中，匹配度的值在 0 到 1 之间。这个匹配度矩阵的二分图可以用经典的 Kuhn– Munkres 算法求得最优解，这个最优是在确保接驾体验的基础上，在 2 秒内最多的满足乘客的订单需求。

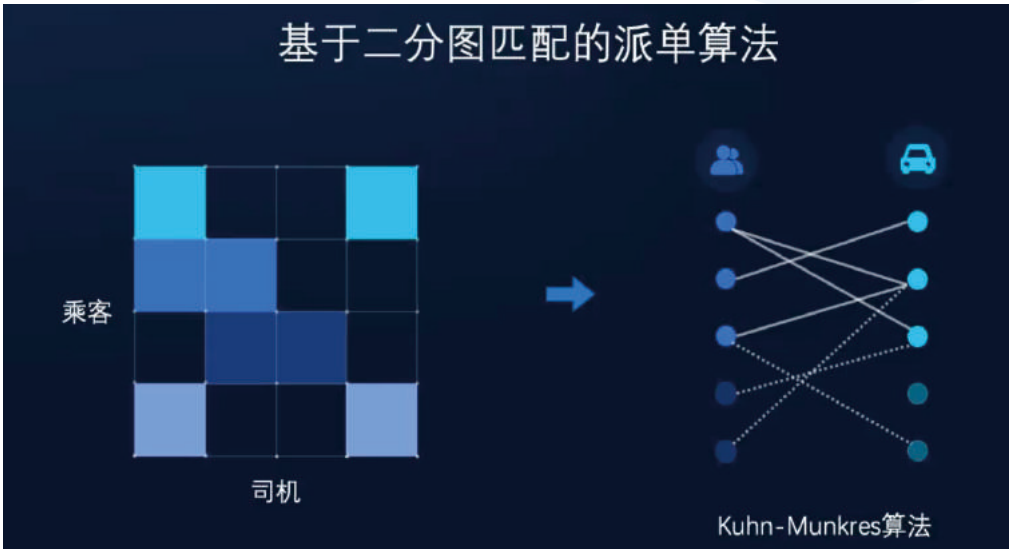


图 5： 基于二分图的派单算法

因此，基于二分图匹配的派单算法最核心的内容包括路径规划和预估到达时间（ETA）。其中，路径规划指表示从起点到终点需要经过的路线，预估到达时间表示预估从起点到终点的需要行驶的时间。在预估到达时间的研究方面，滴滴研发一套基于深度学习的时间预估系统，这个预估系统模型的核心是把出行轨迹用序列描述，因此，预估到达时间就可以用 LSTM 进行建模，再结合 Wide 和 Deep 模型（具体细节可参考 [2]）。通过这个深度学习系统可以使算法的精度有了显著的提升，通过报告中的该系统的应用场景视频演示可知，滴滴应用深度学习打造了新一代线上地图平台，其中 AI Labs 基于神经网络和强化学习技术针对路径规划（RP）和到达时间预估（ETA）问题研发了准确性高，计算速度快，占用资源少的新一代深度学习模型，这个模型可以在复杂的移动出行场景中确保车辆实时调度与订单分配的准确性，并根据实时突发路况进行计算反馈以快速整合生成最优出行方案，同时，该平台会根据乘客与司机的地理位置信息及路况信息、出行数据、司机信用评级进行动态匹配最佳订单和路径策略选择（图 6）。

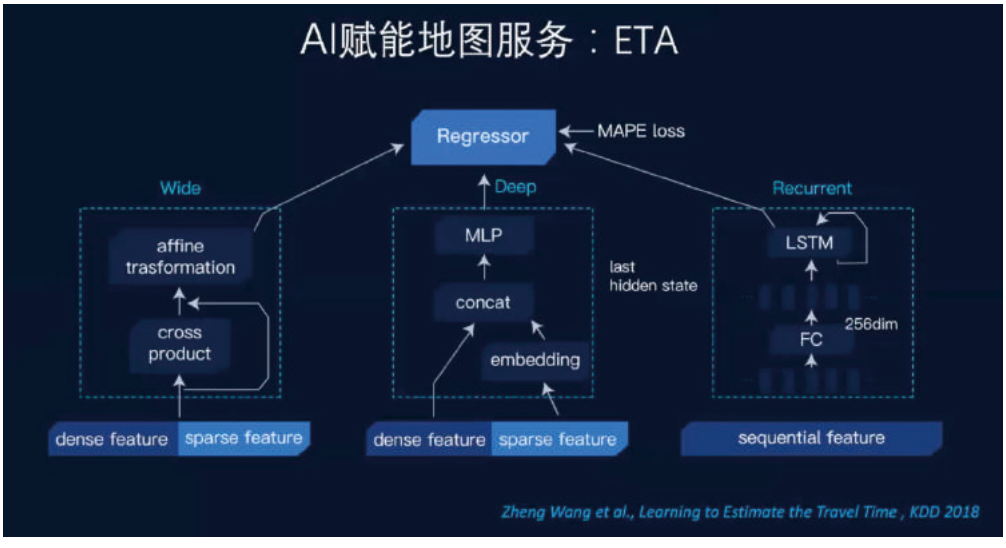


图 6： AI 赋能地图：ETA

基于 Kuhn– Munkres 的订单分配算法虽然可以在两秒内找到最优解，但如果结合 AI 技术对未来交通的预测信息，在两秒钟之内，该算法可以满足更多的订单需求及提升订单分配的效率。

3.3 基于强化学习的智能派单

由于每个订单分配的决策会对未来司机（车辆）的分布产生影响，所以可以用时间序列决策问题表示订单分配，这个基于时间序列的订单分配问题可以用马尔科夫决策过程（MDP）求解，通过 MDP 求解后，该问题的目标将从短期收益最优转变为长期收益最优。如图 7 右下角所示，MDP 中每个司机是一个 agent，状态（state）表示司机所处的位置（location）和当前时间（time）。动作（action）表示司机订单匹配，无论司机和乘客订单匹配与否，都会产生一个 action。奖励（reward）表示对每个 action 的激励（假如司机和某个订单匹配成功，reward 为该订单的价值，没有匹配 reward 为 0）。基于强化学习和组合优化方法充分考虑了每次派单对未来的司机分布的影响及基于全天车辆供需与出行预测，它把订单分配决策问题从两秒最优变成长期（如一天）最优。因此，基于 MDP 的订单分配系统 2017 年在全国 TOP20 城市上线，在确保用户体验的基础上，显著提升了司机的收入，具体细节可以参考 [3]。

图 7：基于强化学习的智能派单

3.4 基于 V–Net 的智能派单

基于 MDP 订单匹配的缺点是状态太少，只是一个时间或一个空间，导致许多非常有价值的状态信息没有得到充分运用，针对这个缺点，叶杰平应用深度强化学习来求解订单分配问题。· 基于深度强化学习的派单本质上是用深度神经网络直接学习价值函数（图 8），通过神经网络引入更多的特征（时间，空间，实时供需，实时天气等）能够增强神经网络的泛化能力及深度强化学习的有效性以提升订单分配的精准度和效率。此外，通过迁移学习可以有效提升多个城市的订单分配训练学习任务来提升订单匹配的效率。具体可以参考 [4]。并且，基于强化学习的网约车派单解决方案获得 2019 年 INFORMS Daniel H. Wagner Prize，该奖项为企业应用运筹学领域最高奖之一。

图 8：基于 V–Net 的智能派单

3.5 基于强化学习的司机 AI 助手

在真实的出行场景里，新手司机会由于错误的订单决策导致长时间没有接到订单。针对这个问题，叶杰平及团队开发了基于强化学习的司机 AI 助手（图 9），该 AI 助手主要利用时空价值来帮助司机做最优的决策，提升平台效率及司机的收入。通过报告中的视频演示可知该 AI 助手基于深度强化学习和最优决策理论技术，司机助手可以同时考虑基于时、空间的长期优化目标基础上，利用深度神经网络进行价值估计，为司机提供更准确有效的调度指引，该助手可以有效地将司机指引到订单热区以缩短空驶时间，在助手的帮助下，平台司机可以高效的在城市出行服务运行，更好地满足用户出行需求，最大化城市供需时空分布并且提升出行效率。该司机 AI 助手已经在小范围进行测试。实验结果表明基于 AI 司机调度能够显著提升司机收入和平台效率。

图 9： 基于强化学习的 AI 司机助手

3.6 AI 赋能驾驶安全

在 AI 赋能社会（AI 赋能驾驶安全）方面。滴滴围绕人、车、路三个核心交通要素，采集了与驾驶员相关的基本信息数据通过大数据和 AI 技术进行数据特征挖掘以消除交通隐患（如根据轨迹 MMU 来识别急加速急转弯急变

道，行驶过程玩手机，疲劳驾驶等危险行为）。此外，滴滴通过对平台发生的交通事故进行了深度的复盘分析包括超速，减速让行，高速路况速度过快，疲劳分心等为最严重的隐患行为，及时发现这些隐患行为并警示提醒司机是保证出行安全的关键点。通过对海量的数据分析进行路况预估，在一些特殊的高危路口，如果车的行驶速度超过某阈值，发生车祸的概率会显著提升，如果识别到此行为与路况，会有“前方路口事故多发，请注意减速”的警示提醒（图 10）。AI 赋能驾驶安全可以显著降低了路口交通事故的数量。

图 10：交通事故高隐患组预警

四、结语

本次演讲最后，叶杰平对 AI 在三个层面赋能智能出行新时代做了简要的总结（图 11），未来 AI 终将促使交通行业发生巨大的变革，即从智能交通基础设施； 智能交通工具到共享出行的不断变革。目前，交通出行几乎是一个世界性难题，因为它不仅与每个人的日常生活息息相关，还与经济发展和社会进步密不可分。所以，叶杰平希望有更多的研究者参与智能出行的建设，用人工智能改变未来交通出行。

图 11 ： AI 赋能智能出行新时代

参考文献：

[1] Liu N, Ma X, Xu Z, et al. AutoCompress: An Automatic DNN Structured Pruning Framework for Ultra–High Compression Rates[C]. national conference on artificial intelligence, 2020.

[2] Wang Z, Fu K, Ye J, et al. Learning to Estimate the Travel Time[C]. knowledge discovery and data mining, 2018: 858–866.

[3] Xu Z, Li Z, Guan Q, et al. Large–Scale Order Dispatch in On–Demand Ride–Hailing Platforms: A Learning and Planning Approach[C]. knowledge discovery and data mining, 2018: 905–913.

[4] Tang X, Qin Z, Zhang F, et al. A Deep Value–network Based Approach for Multi–Driver Order Dispatching[C]. knowledge discovery and data mining, 2019: 1780–1790.

百度集团副总裁李震宇：车路智行，打造面向未来的交通

整理：智源社区 杨依帆

在 2020 北京智源大会“AI 交通”专题论坛中，百度集团副总裁、智能驾驶事业群总经理李震宇发表了名为《车路智行，打造面向未来的交通》主题演讲，他指出，**智能交通的核心驱动力在于“ 自动驾驶 + 车路协同”，“ 车、路、行”三驾马车齐头并进，才能在保证安全出行的基础上实现终极“ 无人驾驶自动化”的目标。**百度认为“自动驾驶 + 车路协同”，将成为中国发展智能交通的制高点，助力实现真正的“交通强国”。百度 Apollo 推出 ACE 智能交通引擎，以自动驾驶和车路协同为双引擎，支持智能车联、智能信控、智能公交、智能货运、Robotaxi 等众多应用场景，“面向未来、兼容当下，让交通出行更简单、更美好”。

图 1：百度副总裁、智能驾驶事业群总经理李震宇正在演讲

李震宇，百度集团副总裁，智能驾驶事业群总经理。历任百度多个基础技术部门和业务部门的负责人，带领过产品、研发、商业合作等不同类型的团队，有丰富的管理经验。在首批国家新一代人工智能开放创新平台名单中，“依托百度公司建设自动驾驶国家新一代人工智能开放创新平台”名列榜首。

下面是智源社区编辑整理的李震宇演讲要点。

一、智能车路协同对自动驾驶产生的价值

1.1 降低成本

目前自动驾驶车辆成本居高不下，并且多数是实验型车辆，而真正达到量产车型需要进一步增加成本。车路协同可以降低传感器成本、计算单元成本、安全冗余成本，将单车成本转移到路侧，从而降低更多车辆的成本。从宏观层面判断，车路协同的收益效率也是非常高的。

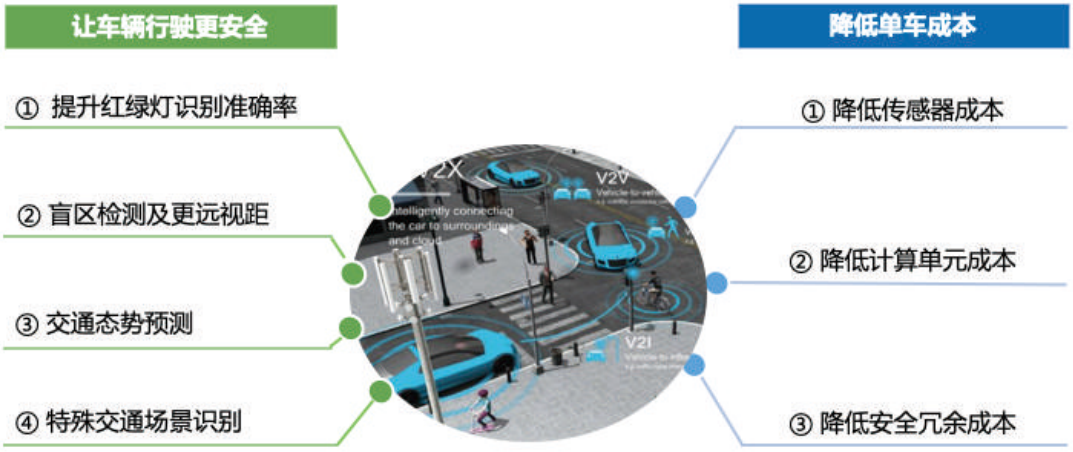


图 2：自动驾驶 + 车路协同，中国智能交通发展的制高点

1.2 保障自动驾驶安全

在红绿灯识别、盲区检测、更远视距、特殊场景识别以及交通态势预测中，车路协同能够发挥重要作用——如识别一辆大卡车后面横穿出的“鬼探头”的小汽车；路边停靠着一辆汽车，提醒远方车辆变道；进行路面的“井盖”等离散障碍物的识别；十字路口更远视距的识别等等。车辆和道路协同识别，能够增强识别效果，使得自动驾驶更具安全性。

二、智能车、路、行融合的三条必经之路

下图中的三维坐标直观地展示了车、路、行三者综合发展的轨迹，共分为三个阶段：数字化、网联化与自动化。

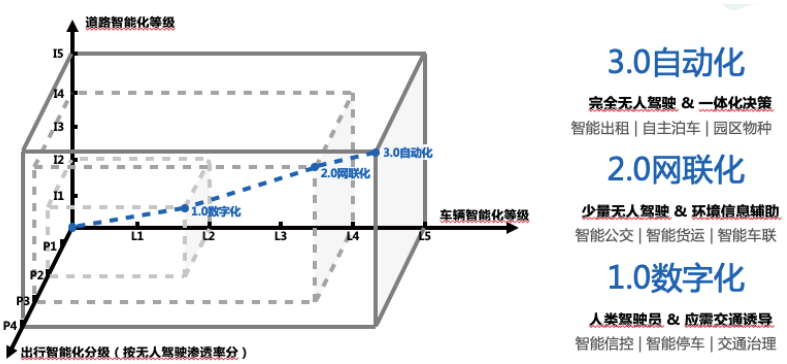


图 3：车路智行融合，是交通发展的必经之路

2.1 数字化

数字化是智能交通的初级阶段，比如司机可以通过智能识别和导引完成智能停车，交通控制系统通过人工智能技术进行交通治理等。

2.2 网联化

5G、IOT 万物互联等基础设施、通信与物联网产业的发展可以带领我们实现网联化的目标。网联化能够驱动智能驾驶、辅助车联等状态，如公交车联网后可以看清和听懂红绿灯的指示信息，从而与红绿灯进行联动。

2.3 自动化

自动化是智能交通的终极状态，即达到完全无人驾驶的程度。百度在此理论基础上推出了面向未来的 ACE 交通引擎——A：Autonomous driving 自动驾驶，C：Connected Road 车路协同，E：Efficient Mobility 移动出行。

三、ACE 交通引擎核心驱动力：自动驾驶 + 车路协同

ACE 交通引擎的主要构成为： 一个数字底座，两个智能引擎，N 个应用生态。数字底座将车、路、云、图进行数字化； 智能引擎分为 apollo 自动驾驶引擎与车路协同引擎； 应用生态为开发人员与合作伙伴提供平台，开发数字化、网联化与自动化的相关应用。

图 4：百度智能交通：1（数字底座）+2（智能引擎）+N（生态应用）

ACE 交通引擎适用于多个场景：自主泊车、Robotaxi、智能信控、智能货运、智能公交、智能车联等。

四、城市如何通过智能交通受益

智能信控：智能信控的主要作用是调节道路拥堵，提高出行能力，从而降低道路建设成本。

智能停车：过去人们对于停车收费的体验并不良好，现在，我们可以通过人工智能的方式得知车辆何时来到，何时离开，最后通过 APP 或者小程序的方式进行停车收费。

图 5：智能交通：释放 GDP 增长潜能，促进产业升级

智能公交：智能公交可以提高准点率、降低事故率，提高乘客体验。

智能货运：智能货运能够降低长途运输等路途中的事故率，同时降低货车油耗。

李震宇最后总结道，中国拥有稳定的制度优势及强大的基础设施建设能力，基于 5G、IOT 及人工智能相关技术，切实结合人们实际出行需求，解决道路交通出行难题，我们一定能够实现真正的“交通强国”！

北京市交通信息中心副主任杜勇：打破孤岛，用大数据驱动交通融合发展

整理：智源社区 任黎明

杜勇本次的演讲主题是《打破孤岛，用大数据驱动交通融合发展》。

杜勇，北京市交通信息中心副主任。长期从事智能交通关键技术研发和应用推广工作，先后主持或参与完成了 863、国家科技支撑计划等多项国家及省部级重大科研项目。科研成果获省部级科学技术奖 9 项。先后获得“全国交通运输青年科技英才”、“北京市百千万人才工程”、“北京市高层次创新创业领军人才”等科研称号。

在本次演讲中，杜勇回顾了过去十年北京市交通信息中心在北京交通行业大数据资源整合共享和开发利用方面所开展的工作，并基于工作实践，总结了交通大数据的典型特征及面临的困局。对于市民对更高品质出行服务提出的新需求，以及不断涌现的新技术、新业态，他介绍了以“深化交通大数据开放应用，推动交通运输服务协同创新”为主线的北京智慧交通提升行动计划，包括该行动计划的发展愿景、业务架构和技术架构等。以下为智源社区编辑整理的杜勇演讲要点。

一、交通大数据的困局

1.1 交通大数据方面开展的工作

以交通大数据的困局为出发点，杜勇介绍了过去几年来在交通大数据方面开展的工作及对他对交通大数据的理解和体会，从 2009 年开始到现在，他在交通大数据领域的主要工作经历了以下三个阶段。

- 从 2009 年到 2010 年是数据汇聚阶段，探索建立了交通行业数据中心，实现了交通委内部各个系统数据的接入共享和交换，实现交通行业数据中心从无到有的突破；
- 从 2010 年到 2017 年是数据管理阶段，开展了三个方面工作，第一是数据介入范围不断扩展，从交通行业内部的公交、地铁、出租等行业，拓展到了铁路、民航、气象部门。第二，实现了交通委内部和北京市其他的政府部门以及交通运输部之间常态化的数据共享交换，随着数据量的增大及业务部门对数据的依赖，建立了规范化的管理体系保障数据中心稳定平稳运行；
- 从 2017 年到现在是数据应用阶段，而传统的关系型数据库已经无法满足数据的存储和计算的实际需求，因此，将数据中心升级为并行计算和分布式存储的大数据中心，围绕相关实际应用场景开展大数据应用示范工作。

1.1.1 交通大数据的数据来源

目前，从交通行业大数据中心整合数据可知，交通大数据主要有以下三个来源（图 1）：

- 委内的数据：包括了北京市运输行业的从业人员，营运车辆和经营业户等基础信息；路政行业审批执法数据和公路交通流量数据及交通执法的检查和处罚数据；
- 行业数据：包括了地面公交、轨道交通，出租汽车以及货运、客运等传统的交通行业的数据。也包括了近几年新兴的网约车、共享单车等新的交通业态数据。数据类型包括轨道站点，公交线路站点车辆等基础信息，包括了卫星定位刷卡，扫码，计价，售票，排班以及订单等动态运营数据。

• 外部数据，从民航部门整合了机场的到离航班等信息。从气象部门介入了实时气象数据。

来源	数据类别	数据范围
委内数据	运输	从业人员、营运车辆、经营业户审批数据
	路政	路政审批与执法数据、公路交通流量数据
	执法	交通执法检查与处罚数据
行业数据	地面公交	公交刷卡/扫码数据、公交车卫星定位数据、公交基础数据
	轨道	轨道刷卡/扫码数据、轨道站点数据
	出租	出租卫星定位数据、出租计价器数据
	公租自行车	公租自行车车辆借还数据
	营运车辆	危化车辆、省际车辆、旅游车、重载货车卫星定位数据
	省际客运	长省际客运排班数据、实名售票数据
	新业态	网约车、共享单车的订单信息和车辆运行位置信息
外部数据	铁路	火车站日到发车次、客流统计、晚点信息
	民航	机场每日到离港航班、客流数据、晚点信息
	运营商	接入三家电信运营商手机信令数据
	交管局	交通事件、微波检测器采集的交通流量信息
	气象局	气象预报信息

图 1 ： 交通大数据的数据来源

1.1.2 交通大数据的数据特点

在数据管理层面，北京的交通行业大数据管理具有以下三个特点。

- 广聚合，实现了接入交通行业内外相关信息系统，汇聚数据每日达到 5 亿条；
- 强管理，按照 ISO20000 管理体系，实现了中心全流程，可视化规范管理；
- 重服务。开展大数据分析挖掘，支撑交通运行检测规划决策出行服务等交通重点业务工作。

杜勇介绍，通过对交通大数据进行清洗、计算、分析，并且利用可视化技术对交通相关业务进行服务，目前，交通大数据逐渐支撑了四类服务。如图 2 所示，左上角和左下角分别是轨道交通站点的客流换乘量以及地面公交的线网运行速度。通过这两个系统，监管部门可以实时了解交通运行情况，从而对公交线路优化和规划的政府决策提供数据支撑。右边两个图是实时公交信息，每辆公交车的到站时间和距离以及满载率，地铁的站与站之间的客流满载率。把这些数据信息发送给高德、百度等互联网企业，让出行者通过相关 APP 可以查询他们所需要的出行信息。此外，这些信息数据对互联网企业开展精细化调度提供了坚实的数据支撑。

图 2 ： 交通大数据的应用服务

1.2　交通大数据方面开展的工作

杜勇认为交通大数据如果要发挥作用，必须要经历精细化的数据管理； 精准化的交通特征计算； 智慧化的交通决策分析等三个主要工作。

从基础化的交通设施接入交通的动态运行情况，再应用深度学习，数据挖掘和人工智能等技术对交通大数据进行深层次处理，此过程如用 X 光给人体检一样，通过对交通大数据的深度挖掘能够发现交通的运行情况，交通的问题，有利于开展精细化的开展交通治理工作（图 3）。

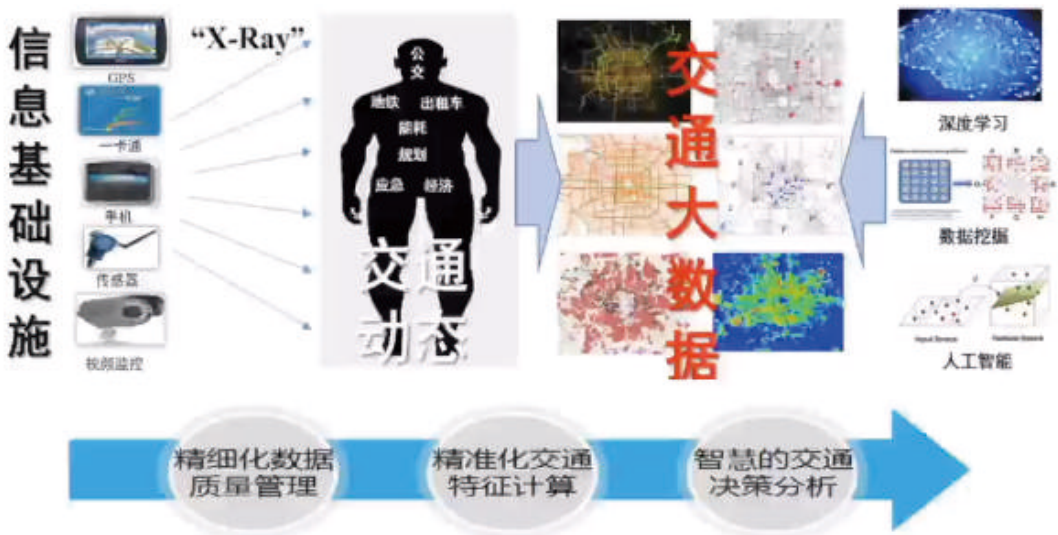


图 3： 交通大数据的处理工作

1.2.1　交通大数据主要有四方面的特征：

- 全面：交通大数据的数据量大而全，其涉及到 PB 级数据量。百亿级的数据记录及涉及的相关领域众多；
- 混杂：交通数据价值高低并存，包括了交通调度指令、客票信息及监控影像等动态和静态的数据信息；
- 关联：交通行业大数据必须实现跨行业的关联，数据的汇聚实现系统与行业关联及业务协同；
- 多样：在数据结构上存在异质多样的特征，包括结构化和非结构化及流动式等多个样式的数据。

1.2.2　交通大数据应用方面存在的主要问题：

（一）在信息孤岛层面，交通数据存在**行业孤岛，区域孤岛及开放不畅**等三个方面问题:

- 从行业孤岛来看，交通数据主要体现为行业数据的整合还是不全面；
- 从区域孤岛来看，交通大数据存在着不同省市交通部门之间的数据没有完全互联互通；
- 从开放不畅来看，虽然有交通大数据，但是面对社会企业、社会公众包括研究机构等开放的渠道不是很畅通，使交通数据的价值没有得到很好的发挥。

（二）在质量差层面，交通数据存在着以下四个方面问题:

- 标准不统一，比如出租车的卫星定位终端设备没有按照统一标准来生产制造；
- 数据不完整，所采集到的数据有许多核心数据字段存在数据缺失问题；
- 精细化程度不够，如公交站台位置不是很精准，全市企业对站点的编码不统一；
- 稳定性不够，很容易出现数据中断问题。

因此，杜勇认为交通行业的大数据应该更加重视数据层面的标准建设和质量管理工作，近年来，在交通行业大数据方面做的工作包括统一了北京市出租汽车车载终端的统一技术要求，建立了全市层面的统一的站点线路的编码规则及利用卫星定位数据精准化矫正位置。

（三）在分析弱层面：交通数据主要包括浅、虚、乱等不足（图 4）；

- 浅是对于交通行业数据的统计分析多，对于深层次挖掘以支撑决策的工作比较少；
- 虚是学术理论研究相对较多，对实际交通问题并且解决实际问题的研究比较少；
- 乱是大多数人站在自己角度，利用自己掌握的数据进行分析得出相关结论，但真正站在全市的角度利用跨部门的数据进行客观分析，得出全局性结论较少。

图 4： 交通大数据分析弱困局

二、交通大数据的分析与应用：

通过对去年北京市交通的现状、问题及未来的发展趋势，杜勇介绍了北京交通委制定的智慧交通三年行动提升计划。在智慧交通新时期、市民对更高品质出行服务的新需求日益迫切、同时，新技术和新业态正在不断涌现、北京智慧交通的建设亟需把握新机遇、整合提升智能交通设施、深化数据开放应用、推动交通运输服务协同创新、从而使北京交通运输步入一个新的发展阶段。

2.1 智慧交通计划的聚焦方向

未来的交通是以预约共享系统最优为主要特征的方向。为了更好地聚焦未来交通的方向，从实现路径上应该重

塑道路资源，运输资源和城市空间资源的分配模式，实现交通运输全局优化，系统协同与智能可控。在技术应用方面要充分利用大数据，人工智能，5G 通信，自动驾驶带来的技术变革机遇、从而通过技术创新来推动机制创新。

2.2 智慧交通计划的工作目标

接着，杜勇从该行动计划的工作目标方面仔细讲述了通过推动智能化技术与交通业务的深度融合预期实现的三类目标（图 5）:

- 第一类目标: 提升交通运输整体运行效率; 具体体现为让百姓的公交出行更准时，乘坐地铁更舒适，出租车更便捷，不同交通运输方式更协调;
- 第二类目标: 实现平衡调节交通系统供需关系; 具体体现为交通供需信息匹配，能够合理引导百姓出行需求，使百姓出行可规划、可计划、可选择、可预期;
- 第三类目标: 着力增强智慧交通治理能力，具体体现是是信号灯能够实现智能调控，交通执法能够实现线上线下一体化执法，通过技术和机制两方面能够充分动员社会力量参与北京市的交通治理工作。

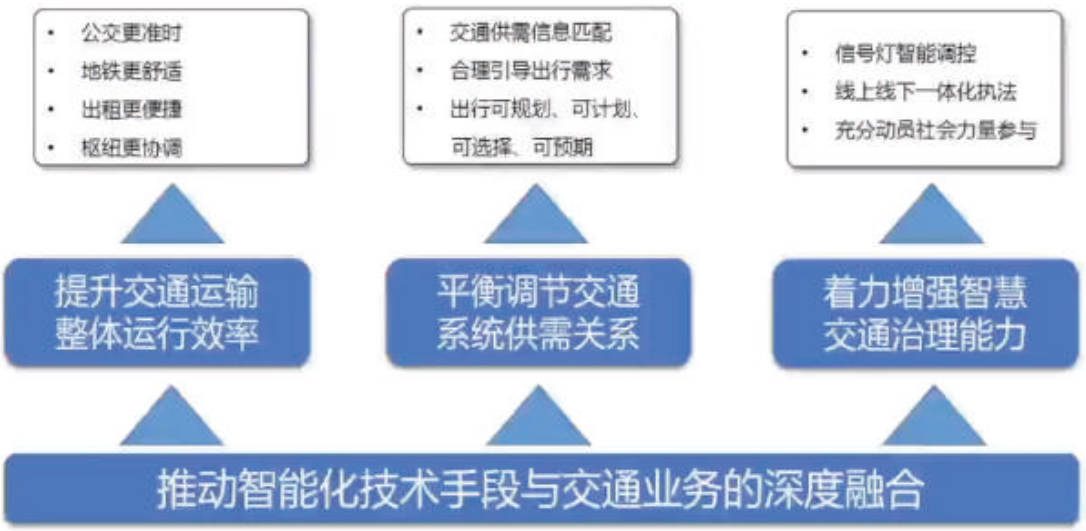


图 5： 智慧交通的工作目标

2.3 智慧交通计划的业务架构

然后，杜勇讲述了该行动计划感知层、数据层、应用层和业务层等的业务架构（图 6）。总而言之，智慧交通计划以智慧感知设施为基础，全面整合政府、企业、社会化数据，搭建交通大数据平台，实现交通要素的全景全量采集，打造集交通运行监测、指挥调度、决策支持、综合信息服务为一体的交通大脑、构建运营、管控、执法、服务等智慧交通应用场景、围绕优供”、“控需”、“强治”的交通综合治理思路，该计划的最终目标为公共出行提供便捷、高效、安全、绿色的服务。

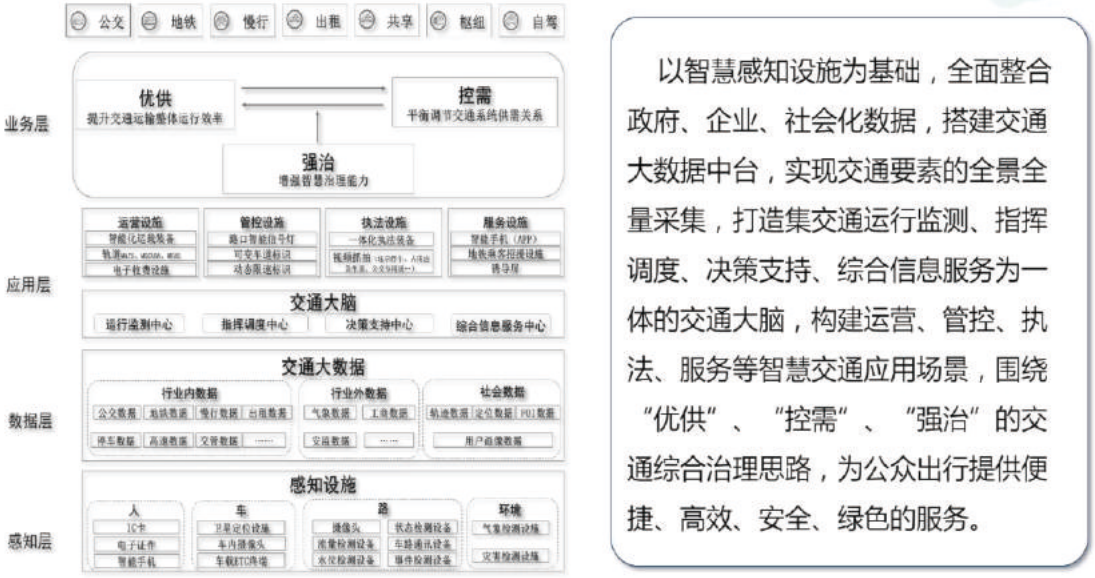


图 6： 智能交通的业务架构

2.4 智慧交通计划的技术架构

从技术架构方面，该智慧交通计划以边、端、云为主线的技术架构（图 7）。根据北京市交通的特点，该计划形成了地面公交，轨道交通，运输服务道路管理等领域的端边云的技术架构。在这个架构的基础上构建北京市统一的交通运输云和交通大脑。这个技术架构主要包括以下四个方面。

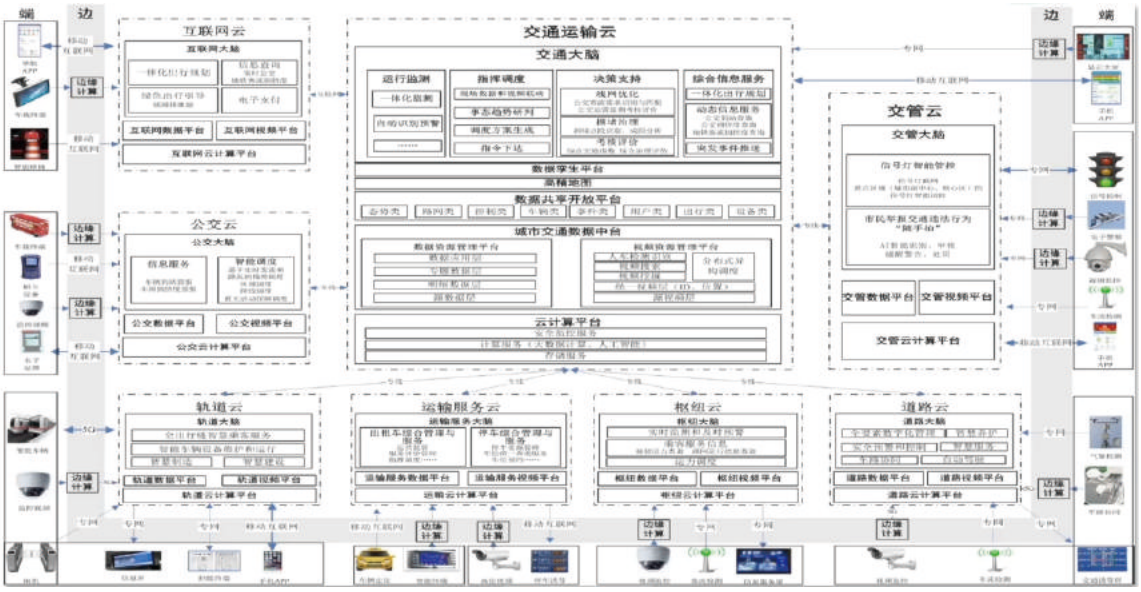


图 7： 智慧交通的技术架构

- 建设“1+1+6”的云架构体系： 统筹政府、行业、社会各自的资源优势，打造“一个交通运输云为中心，一个交管云为协同、六个交通行业为支撑”的云平台架构；

- 建设“一套标准、统一表达、多元融合”的大数据管理体系：整合全景全量的大数据资源，建设城市交通数据中台和数据共享开放平台，实现交通大数据的共享和深化应用；
- 建设“端”、“边”、“云”三层架构的视频资源分析管理体系：整合全市交通视频资源，统一管理，建设云计算和边缘计算一体化的分布式异构调度体系，通过机器学习和人工智能技术，实现车牌识别、人脸识别、行为识别的视频大数据智能化分析挖掘；
- 建设基于高精地图平台和数字孪生平台的城市交通大脑：构建全市统一的交通高精度数字地图库，探索利用物理模型、传感器数据、运行数据建设北京交通数字孪生仿真平台，在此基础上，建设完善北京市城市交通大脑，实现体化监测、自动识别预警、现场数据和视频联动、公交线网优化、智能考核评价、体化出行规划、动态信息服务等业务。

2.5 智慧交通计划的行动路线

最后，杜勇把智慧交通计划的行动路线总结为以出行者为中心，开放式建设发展（图 8）结束本次智源大会报告。该计划行动路线的内容为将公交到站时间、公交地铁客流拥挤度、停车位、交通事件、移动支付等动态出行数据向互联网平台开放、采用政企合作的模式、面向 C 端共同打造门到门的一体化出行服务 (Maas) 平台。充分融合互联网平台在人工智能、视频分析等领域的大数据中台能力、赋能交通大脑、面向 G 端共同打造用数据驱动、与视频联动、和现场互动的新一代交通运行监测预警和指挥调度平台。

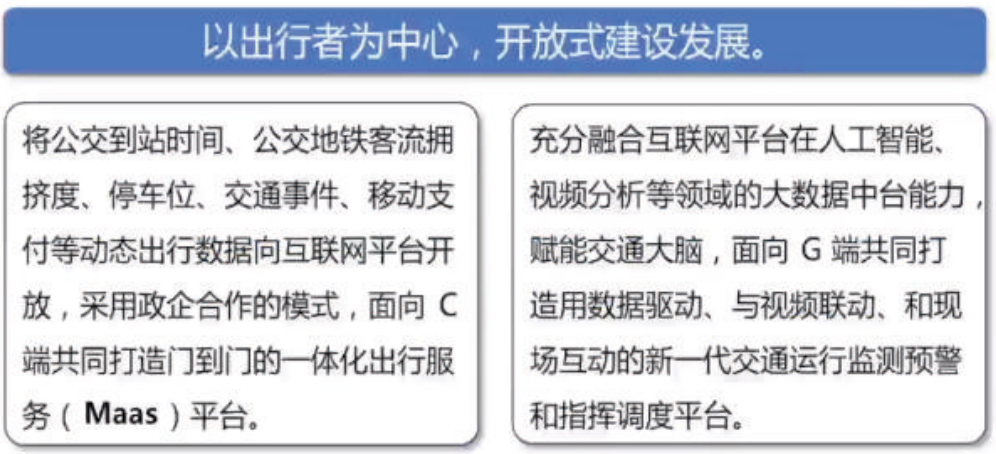


图 8： 智慧交通的行动路线

北航教授杜博文：基于广义时空数据挖掘的交通复杂行为认知 - 从研究到工业

整理：智源社区 任黎明

在第二届北京智源大会 AI 交通专题论坛中，北京航空航天大学杜博文教授做了《基于广义时空数据挖掘的交通复杂行为认知 – 从研究到工业》的主题演讲。

杜博文，北京航空航天大学教授，博士生导师，国家自然科学基金委优秀青年基金获得者。现就职于软件开发环境国家重点实验室、综合交通大数据应用技术国家工程实验室及北京脑科学高精尖中心。他的主要研究方向为广义时空大数据挖掘与认知、工程大数据、人工智能与机器学习。围绕这些研究，他主持了包括国家自然科学基金优青、重大、国家重点研发计划等 10 余项项目 / 课题，共发表包括 KDD、TKDE、Networks、TITS、TC 等国际期刊 / 会议论文 60 余篇，授权发明专利 10 余项，荣获国家科技发明二等奖（排名 3）及国家技术进步二等奖（排名 3）各 1 项，省部级科技奖项 5 项。杜博文研究团队的网站是 https://www.brilliantasus.com。

本次报告中，杜博文重点介绍了他团队对交通领域的单源时间序列数据、二维时空数据及高维时空数据等方面的探索，包括探讨了如何将相关研究成果应用于具体交通问题的改善等。

以下为智源社区编辑整理的杜博文演讲要点。

一、研究动机

1.1 研究背景

从改革开放至今，我国的交通运输方式已经巨大的变化，这些巨大的变革标志着我国已经成为交通大国。近年来，随着国家对交通领域发展目标的不断明确及在交通领域的研究不断深入。交通系统诸如多主体、多交通方式、多分布等多因素问题，网约车调度、公交车调度、共享单车调度等散决策问题以及意外交通事故、城市交通拥堵指数、恶劣气象等强干扰问题也逐渐凸显出来，这些问题造成了交通供需的解析难度增加，车流、客流聚集等一系列严重现象。这些现象意味着庞大而复杂的交通系统正在面临如何更加高效、精准，智能等关键挑战。

1.2 研究新机遇

随着大数据技术与交通的深度融合，大数据正成为交通智慧化发展和社会精细化治理的重要技术支撑。数字中国建设等大数据协作方案，为我们解决交通领域的难题与挑战指明了方向和方法，如通过物联网技术让获取全时全域的城市交通数据成为可能。而这些大数据不仅是城市建设新常态的需求也是社会服务效能提升的重要基础。基于大数据为交通领域发展提供的重要机遇，杜博文主要研究时空数据（如航空高铁公路、城市地铁的变化数据可以映射到空间维度上； 而历史状态突然变化、居民跨越空间位置的移动行为可以映射到时间维度上； 这些数据统一归结为时空数据）。目前，现有交通领域的时空大数据存在复杂时变及多元异构的缺点，这些缺点给交通领域的研究造成以下三大严峻挑战。

- 群同行为的多扰动与随机性会导致路网通行状态的辨识能力弱；

- 移动目的多样性与多变性会使群体移动行为非常复杂;
- 不同数据源的差异性与离散性会导致不同维度的特征关联性弱。

针对上述挑战，如何对城市交通的复杂行为进行动态认知和响应成为交通领域研究的主要科学问题。基于这个研究问题，杜博文及团队主要对基于广义时空数据挖掘的交通复杂行为认知 –– 从研究到工业进行深入研究。他从以下三个阶段开始本次主题演讲。

二、第一阶段：单源时间序列

现有交通领域的研究者及交通应用实践者在最开始时都是对某一个空间路网的运行状态进行研究。比如，我们在开车过程中，常常看到信息提示屏上对某一个段面的交通流量统计的结果。并且其通常使用 ViSSUM 和 TransCAD 等仿真软件。然而，通过这些软件进行研究工作的最大的缺点是**被动感知**，并且感知的范围极其有限，它仅局限在某条道路的几个断面上。这就引发了因位置绑定而难以形成全局感知的问题。针对难以全局感知的难题，杜博文在研究思路中将车辆视为移动传感器，该移动传感器可以实现交通数据来源从固定检测到移动采样的巨大变革，同时也实现了**交通数据由小样本到交通大数据的转变**。这个巨大的变革从研究思路上实现从对交通领域的研究从**一维空间向二维空间的迈进**。但是，在真实研究中直接使用移动检测器会受到数据扰动性及误差的随机性影响，这些影响必然导致**辨识结果的误差偏差大**。基于此问题，杜博文建立了将多个路段关联成一个区域，然后将各路段时空关联数据进行融合，再通过建维去扰、缺失补偿及融合校验的方法来提高路网运行状态的辨识准确率。具体步骤如下:

首先，针对多元检测器检测结果不一致或者相互冲突的问题构建了区域级的面向多元异构数据的多层级适配融合模型（图 1）。该模型通过数据源之间的相互校验及关联关系来提高计算结果的准确性，实验结果表明与单元数据相比，误差降低了 10.3%，保证了数据的稳定性（图 2）。

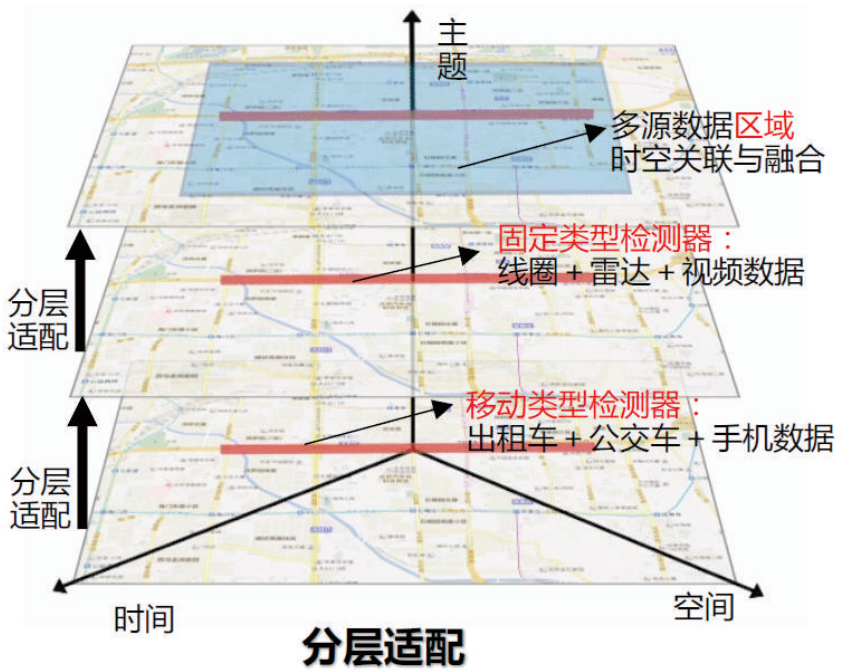


图 1：面向多源异构数据的多层级适配融合模型

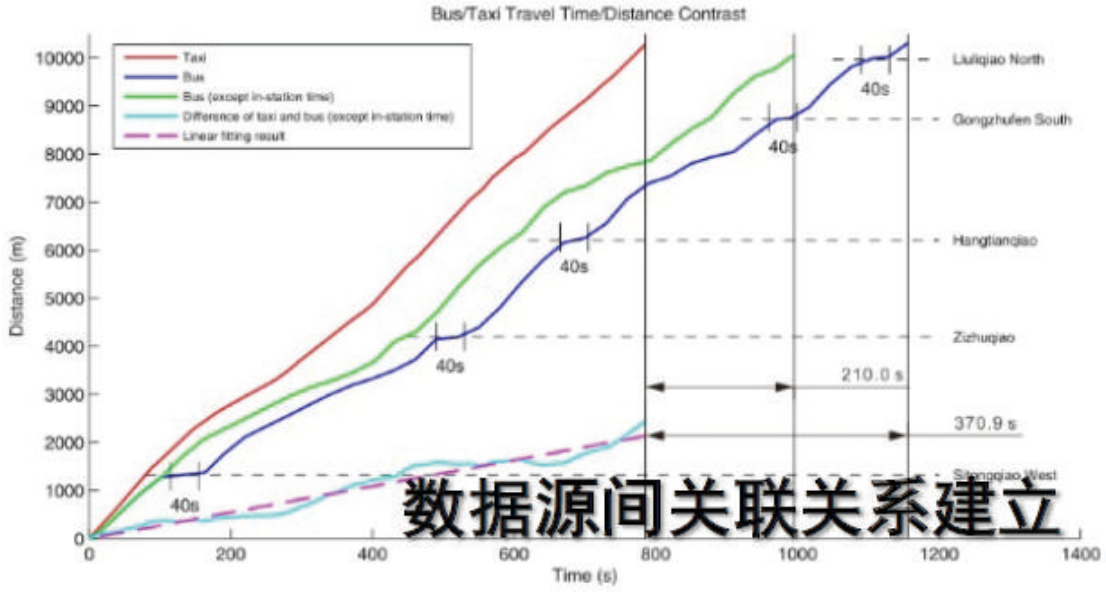
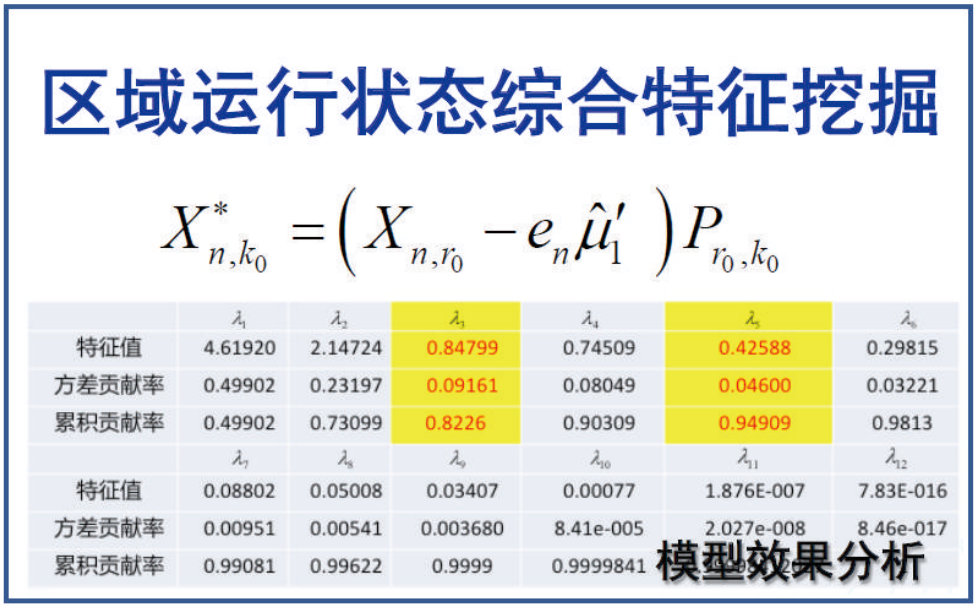


图 2：多元异构数据的多层级适配融合模型实验结果

其次，针对移动检测器位置随机分布产生的部分信息缺失的问题，杜博文受到指纹识别的启发提出了基于稳健特征空间映射的稀疏数据补偿模型。通过对区域运行状态综合特征挖掘及大规模实时数据投影映射转化的方法保证了数据的完整性。与国际先进方法相比，基于广域空间位置的时序数据补全方法的交通信息覆盖率增加了 7%，达到了 82%。因此，基于移动位置数据的城市出行信息服务关键技术与应用项目获得 2016 年国家技术发明二等奖。



	λ_1	λ_2	λ_3	λ_4	λ_5	λ_6
特征值	4.61920	2.14724	0.84799	0.74509	0.42588	0.29815
方差贡献率	0.49902	0.23197	0.09161	0.08049	0.04600	0.03221
累积贡献率	0.49902	0.73099	0.8226	0.90309	0.94909	0.9813
	λ_7	λ_8	λ_9	λ_{10}	λ_{11}	λ_{12}
特征值	0.08802	0.05008	0.03407	0.00077	1.876E-007	7.83E-016
方差贡献率	0.00951	0.00541	0.003680	8.41e-005	2.027e-008	8.46e-017
累积贡献率	0.99081	0.99622	0.9999	0.9999841	[illegible]	

图 3：稳健特征空间映射的稀疏数据补偿模型研究结果

在对第一阶段的研究进行总结时，杜博文发现在实际交通应用中，如何根据交通路网运行状态的实时客流量变化来动态调度公交车的运力及对路网的参数进行设计优化改进都是未知的。所以，单源时间序列的研究方法，在时空二维表征认知能力方面有限，并且非通勤群体行为复杂、关联特征弱、出行轨迹非连续及个体出行行为不确定性等问题导致单源时间序列难以对路网运行状态的本质进行真正解析。

目前，路网运行状态最关键的研究指标是 OD 量（起始地到目的地之间的群体流量）。通过研究关键位置检测器状态变化对于路网运行状态辨识的研究可以看作是在欧拉坐标系下开展的，并且欧拉坐标系对于固定空间位置研究是有效的。然而，如果要解析路网运行状态就要对群体移动行为进行研究，然而群体移动对于交通的供需是未知的，则欧拉坐标系就不再适用解析路网运行状态。基于这个挑战，杜博文应用拉格朗日坐标研究二维时空数据。

图 4： 研究思路的变革 欧拉坐标系 – 拉格朗日坐标系

三、第二阶段：二维时空数据

在拉格朗日坐标系中，路网运行状态辨识检测传感器的关联关系从空间位置转化到研究移动轨迹间的关联关系，这一转变使交通领域的时空数据研究从被动感知转为主动认知，而这个转变的主要难点在于如何在移动的检测传感器间建立关联关系。因此，交通数据也从单一的二维空间数据转化为二维时空数据。

3.1 居民群体出行路径解析方法

3.1.1 基于时空相关性特征的通勤客流聚集成因与溯源方法

由于城市交通卡与手机位置数据可以全面反映城市居民出行规律，近年来，许多学者利用这两大数据通过研究通勤群体行为来辅助企业预测出行及辅助公交车调度。然而，这两大数据存在数据稀疏且不连续的重大问题。针对此问题，杜博文提出了基于时空相关性特征的通勤客流聚集成因与溯源方法。首先，该方法通过分段式动态时间弯曲方法识别出关键出行路径并且进行通勤客流分析（图 5），然后引入多任务学习预测客流及演示路径及常态化的出行需求（图 6）。通过实际测试结果表明该方法误差为 11.15%，比现有方法降低了 50%（图 7）。

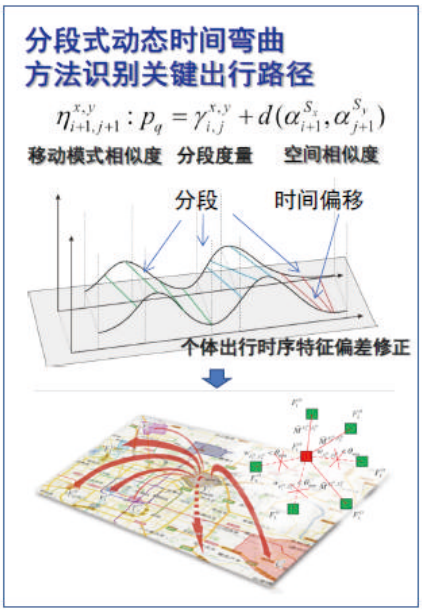


图 5： 分段式动态时间弯曲方法

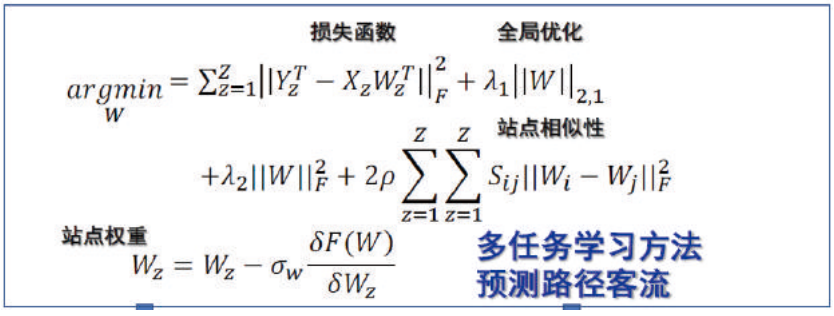


图 6： 多任务学习方法

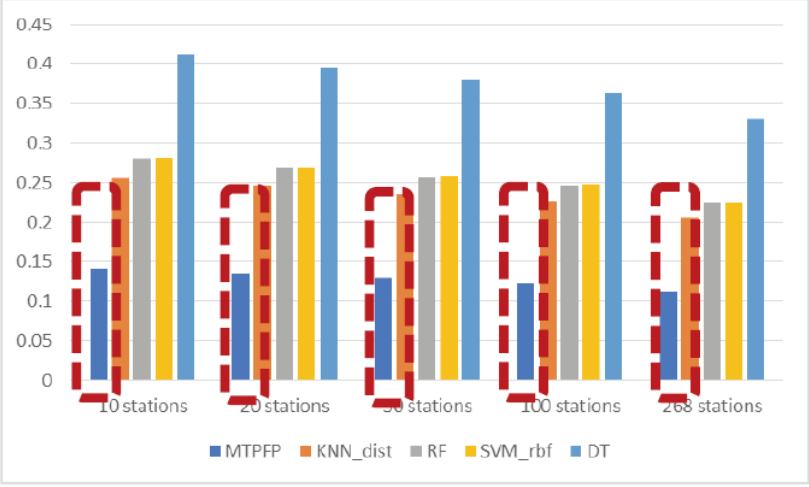
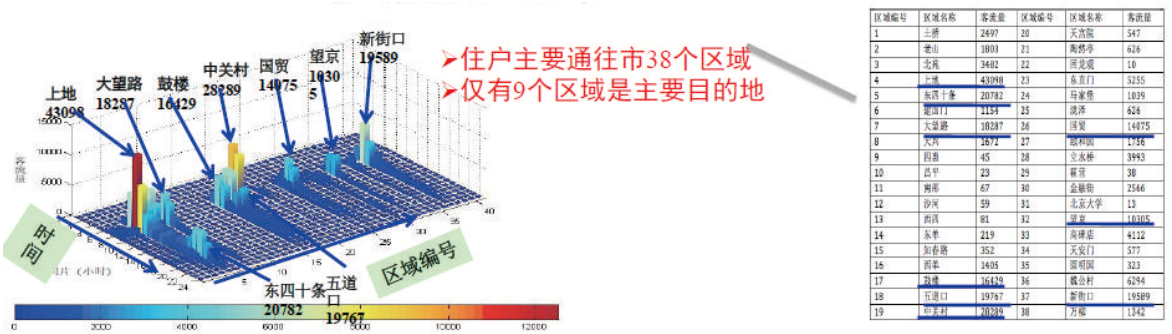


图 7：实验结果误差率对比分析

将基于时空相关性特征的通勤客流聚集成因与溯源方法应用于北京天通苑区域的通勤群体流量进行预测实验，该实验研究发现在与天通苑连接的百余个区域，有九个区域为公交客流的主要通勤区域，通过该方法得到的数据为公交车调度优化提供了数据支持（图 8）。



区域编号	区域名称	客流量	区域编号	区域名称	客流量
1	土桥	2497	20	天宫院	547
2	老山	1803	21	陶然亭	626
3	北苑	3482	22	回龙观	10
4	上地	43098	23	东直门	5255
5	东四十条	20782	24	马家堡	1039
6	建国门	1154	25	洪泽	626
7	大望路	18287	26	国贸	14075
8	大兴	1672	27	鼓楼园	1756
9	四惠	45	28	立水桥	3993
10	昌平	23	29	霍营	38
11	南邢	67	30	金融街	2566
12	沙河	59	31	北京大学	13
13	西四	81	32	望京	10305
14	东单	219	33	南锣店	4112
15	知春路	352	34	天安门	577
16	西单	1405	35	圆明园	323
17	鼓楼	16429	36	魏公村	6294
18	五道口	19767	37	新街口	19589
19	中关村	28289	38	万柳	1342

图 8：研究方法应用实践

3.1.2 非通勤群体出行关键路径识别方法

在出行的城市居民中有高达 40% 的非通勤群体，这些非通勤群体具有非规律性出行性且群体占比小、特征弱等特点，这些特点大大增加了对于非通勤群体的出行行为机理的研究。针对这个难题，杜博文提出基于无监督加半监督的混合监督学习方法（图 9），这个方法可以动态识别非通勤群体的出行路径及识别旅游、购物客流的出行规律。

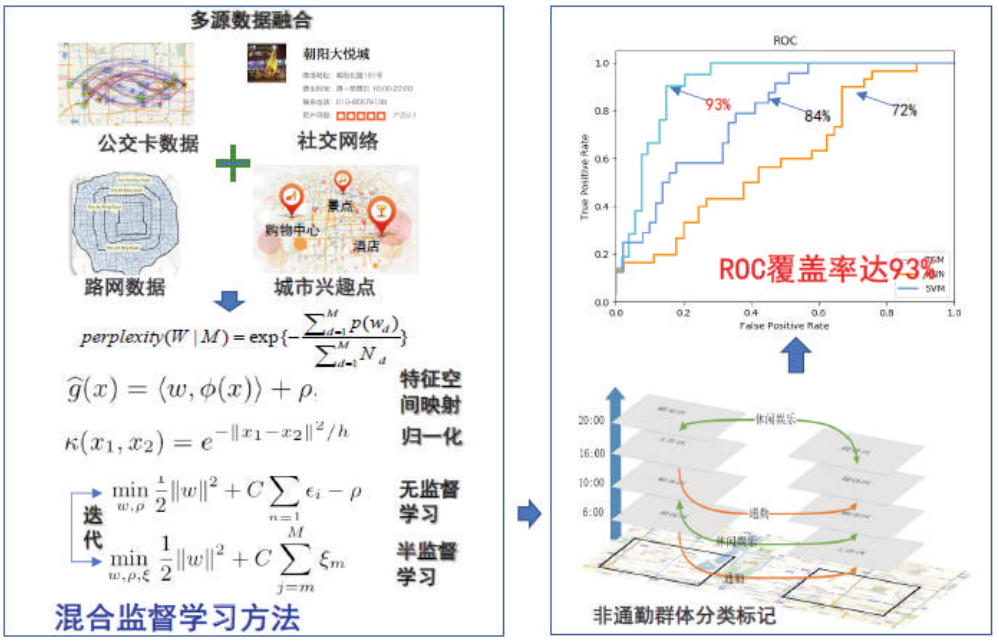


图 9： 混合监督学习关键路径识别研究方法

3.1.3 基于移动行为规律的群体识别方法

杜博文在 2016 年的 KDD 和 2019 年的 KEED 上的文章中 [3]，通过混合监督学习方法把扒手群体移动模式行为识别作为典型异常轨迹的应用场景，利用无监督学习的异常值检测方法，在规律性出勤群体和非规律性出勤群

体的基础上，使用 One Class SVM 再次进行分类，进而应用由监督分类模型识别异常轨迹，通过在同一空间位置的频繁返回模式、逗留模式、徘徊模式等刻划出了有别于规律性非规律性出勤群体异常移动行为，这个方法可以实现公共交通系统中的扒手识别。通过社交媒体公布的信息与一卡通信息数据进行匹配，建立混合监督学习方法训练与测试数据集。然后结合一卡通通行数据进行认证，最终实验结果表明混合监督学习方法的准确率接近 93%（图 10）。

Algorithm	Precision	Recall	F-score	Run Time(s)
		CM Methods		
DT	0.002	0.451	0.004	44.81
LR	0.003	0.476	0.006	36.72
SVM	0.005	0.512	0.009	21.31
LOF			0.009	300+
OCSV			0.029	39.67
		TS Methods		
LOF+DT	0.011	0.780	0.022	301.18+
LOF+LR	0.016	0.829	0.031	301.16+
OCSVM+DT	0.053	0.878	0.099	41.19
TS-SVM	**0.071**	**0.927**	**0.133**	**41.05**

准确率近93%！

图 10 ： 混合监督学习异常群体识别方法研究结果

3.2 基于时态集合的复杂交通行为建模

由于上述的三个内容都是从某一个状态到下一个状态的转移，所以可以将其归类为简单的时序。但在交通实际参与中，交通状况与出行行为是耦合的关系且交通路况与出行行为的影响因素更为复杂及数量多。基于此，杜博文将复杂交通序列数据预测建模为时态集合预测问题。这两者的主要区别在于时态集合是一组状态而不是一个状态。通过时态集合的价可以对复杂的交通事件进行建模。然而时态集合数据具有结构复杂、各因素属性各异特点，不同因素之间语义关联，特别是同集合中的元素之间还存在时序依赖的难题（图 11）。

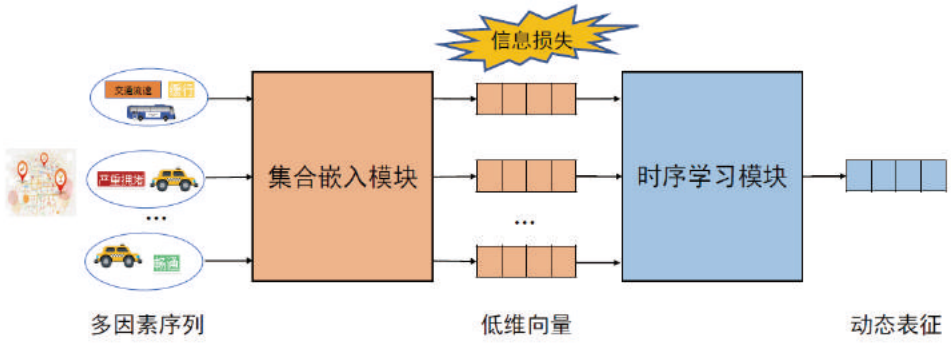


图 11 ： 时态集合的问题挑战

现有时态问题的解决方法是把这些状态都向一个低维特征空间进行映射，如 KDD2016，2019 以及 SIGIR2016 年的研究工作，这些研究工作大多数依照时间序列和时态事件预测思路（利用集合嵌入模块集合的低维特征表示）。在两阶段策略中第一阶段的低维表征直接作为第二阶段的输入，此方法会导致大量的特征信息损失，致使模型的预测精度降低。

针对上述问题，杜博文抛弃了对每个因素集合学习低维表示的阶段，他提出直接以集合中各元素为研究对象并且尽可能多地保留元素自身信息。该方法具体如下： 首先，通过元素与元素间、集合与集合之间的关系学习发现一种语义关系学习； 然后，通过引入注意力机制学习同类元素间的时间依赖关系，再利用门控机制融合静态与动态信息的表征信息作为最后输出的结果来提升预测模型的精度（图 12）。

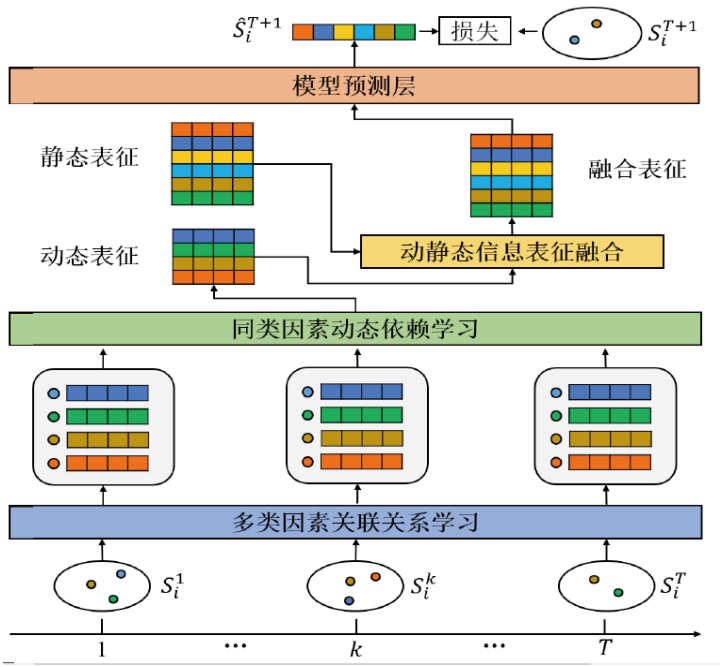


图 12 ： 动静态信息融合的复杂交通行为建模

在 2020 年 KDD 的《Predicting Temporal Sets with Deep Neural Networks》的文章中，通过大规模的实验表明，该预测方法（即 DSNTSP）在多个数据集中的各项衡量指标平均都超过现有方法的 10%，这个优异的结果验证了该思路的有效性（图 13）。

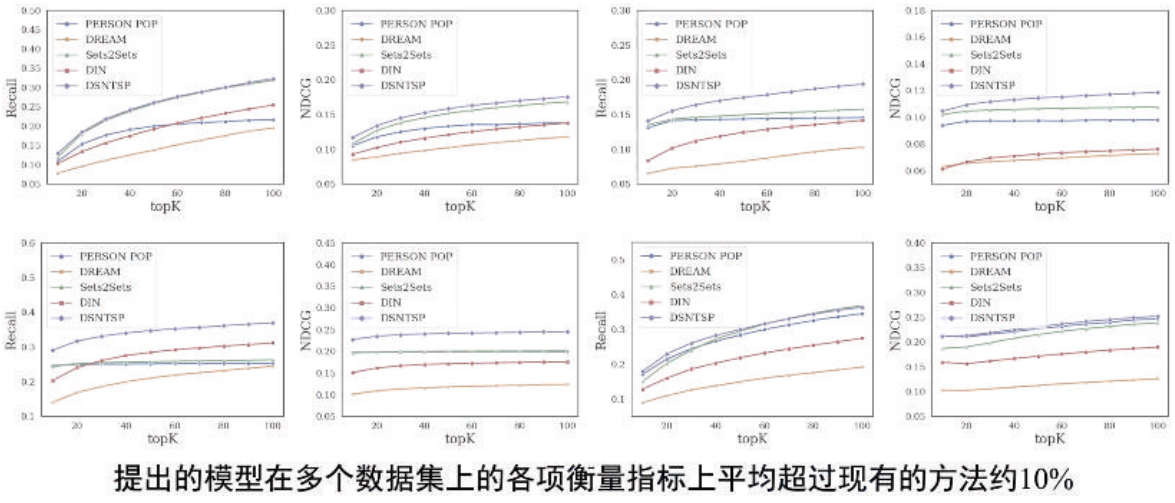


图 13 ： DSNTSP 研究实验结果

由于城市在不断演化，使交通领域的**研究范围由城市内变成城市群，居民出行范围不断扩大，出行距离不断增长，出行模式增多，**行为复杂度提高**且交通模式同时变成综合交通模式等巨大的研究挑战。**针对这两个挑战，主要有以下两种研究来解决个体行为的非连续性群体移动规律持续变化性及运行状态不确定性等复杂性问题。

- 移动行为变化，群体的单移动行为变成了群体的多模式移动行为。比如公交换地铁，公交换地铁以及地铁换单车的积蓄出行。
- 同一空间维度，单种交通资源需求量变为多种交通资源需求量的协同变化。比如现在地铁站附近到底需要多少辆共享单车，实际上是由共享单车本身以及网约车、地铁、公交所共同决定的。如果只用共享单车的数量预测单车的需求量一定是不准的，因为会受到出租车、公交等复合影响。

上述两种主要研究表明二维时空数据很难描述连续性出行模式。由此，交通领域的研究问题由二维时空数据上升到高维时空数据。

四、 第三阶段：高维时空数据

美国亚利桑那州立大学周教授认为交通行为可以形式化为空间、时间、状态三个部分。通过对这三个部分的时空数据深度挖掘可以分析出行者的行为模式，交通状态的演化规律。然而，真实场景中交通状况肯定是个多维度的，比如在某一时间和空间上，既有出租车行为状态，也有公交车的行为状态、共享单车的行为状态。杜博文把一个状态的多影响因素、多维度特征都映射到对应的状态点上，即通过高维特征建模来刻画学习行为解析这个状态点（图 14）。

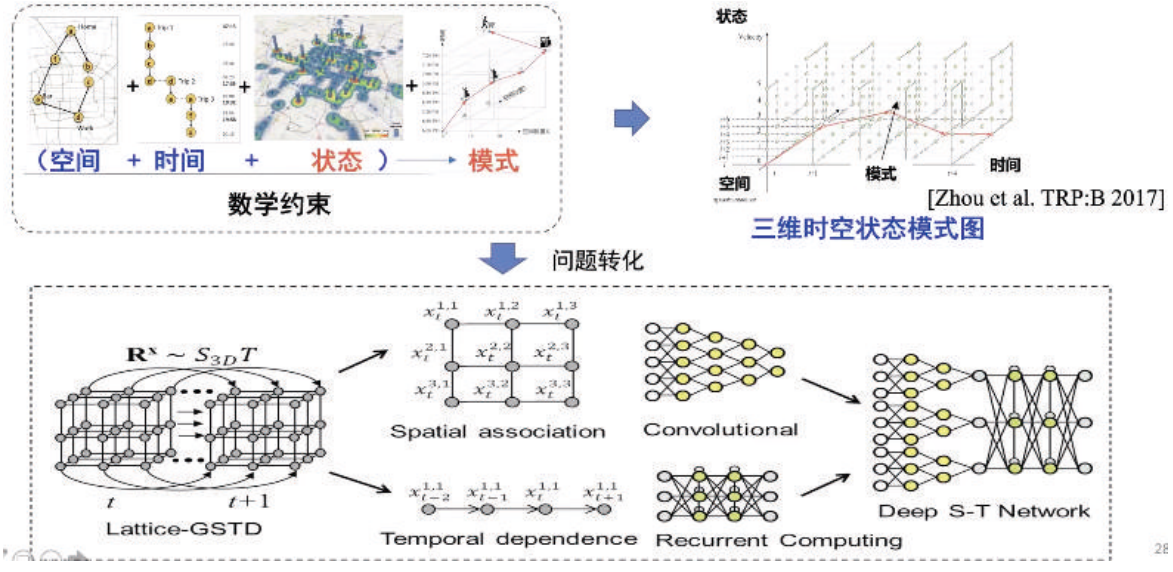


图 14： 研究思路的转变

4.1 基于 CoST–NeT 模型的交通需求量联合预测研究

目前，交通需求量的预测研究方法主要针对单一交通方式，这些方法缺乏对多模态交通需求量之间相关性的分析与挖掘。然而，实际上在不同出行方式的交通需求量之间，存在较强的关联性。因此杜博文提出基于多模态交通需求量的联合预测方法，首先，将高维时空数据中的每个时间点上不只是单一的交通需求量，而是多种交

通需求量的综合； 再挖掘不同交通方式在时间和空间维度上的关联关系； 最后，将多模式交通需求量预测建模为高维时空数据预测问题进行交通需求量的预测。

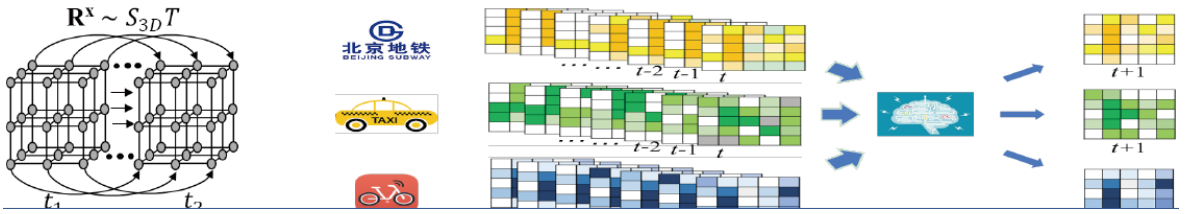


图 13：高维时空数据深度关联与融合预测

现有的研究方法主要应用 CNN，RESTENT 等神经网络模型来获取某一个时刻的交通状态。这些方法的不足是没有对交通需求量空间分布关系深入挖掘。杜博文提出了通过挖掘单种交通方式供给需求与多种交通需求量共性联合的方法以提高多模式交通需求量预测模型的精度。首先，从微观角度对交通需求量进行分解，从宏观对多模交通需求量进行融合； 再应用 CoST-NeT（采用多层基于卷积神经网络的自编码来进行单种交通需求的特征分析和异质 LSTM 模型将多种交通需求的特征进行融合)； 最后，应用 CoST-NET 模型学习单种交通需求的不变性和多种交通需求量之间的共性以实现多种交通方式的联合预测（图 14）。

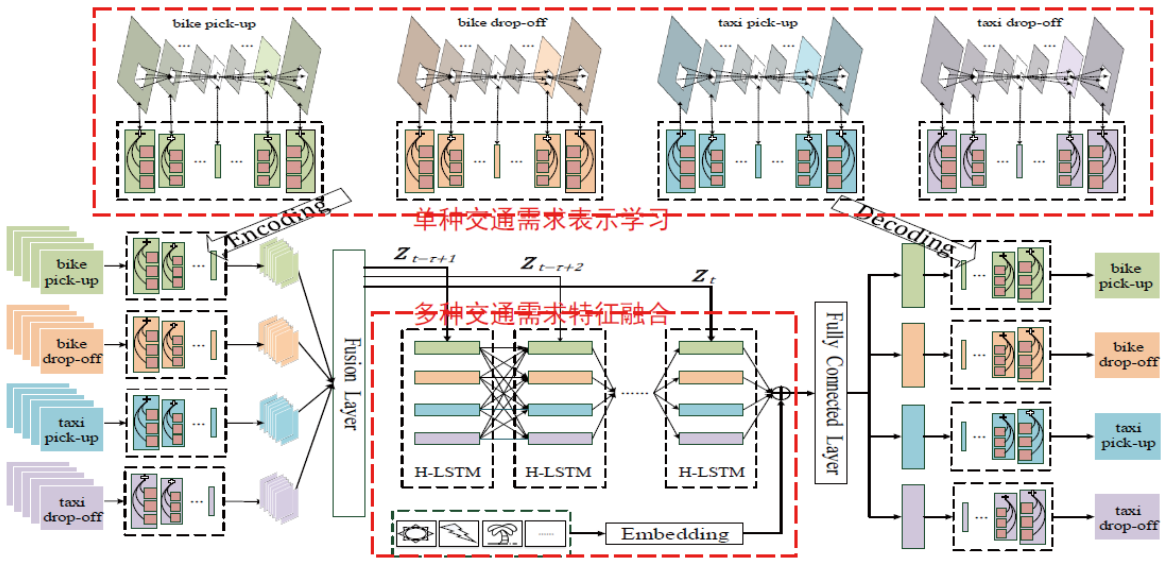


图 14： 基于 CoST-NET 模型的多种交通方式的联合预测

在 KDD2019 的《Co-Prediction of Multiple Transportation Demands Based on Deep Spatio-Temporal Neural Network》研究中，CoST-NET 模型预测精度达到 12.5%，并且该模型具有鲁棒性高泛化性强的特点（图 15）。此外，这篇文章也是就目前看到而言最先开展高维时空下多模态交通需求量预测的文章。在实际应用方面，基于 CoST-NET 模型验证了北京首条自行车“高速”建设的合理性。

Method	NYC Citi Bike		NYC Taxi	
	Pick-up	Drop-off	Pick-up	Drop-off
HA	5.4801	5.4672	22.6326	21.5601
ARIMA	6.4427	4.9956	10.2461	9.1361
LR	8.1028	8.1767	34.6678	33.6617
SAR	3.7536	3.5412	15.4175	13.5590
XGBoost	2.7166	2.5306	9.8231	7.9314
MLP	2.9364	2.6273	13.1985	11.4133
ConvLSTM	2.8726	2.7443	10.7542	10.3004
DeepST	2.7358	2.5506	11.2670	10.1583
ST-ResNet	2.7776	2.6219	10.5112	9.1331
CoST-Net	2.4819	2.2522	8.3853	7.4696

Method	NYC Citi Bike		NYC Taxi	
	Pick-up	Drop-off	Pick-up	Drop-off
HA	0.6659	0.6684	0.8391	0.8208
ARIMA	0.1058	0.1050	0.0073	0.0122
LR	0.8047	0.7917	0.7917	0.7742
SAR	0.5331	0.5459	0.4119	0.4003
XGBoost	0.7985	0.7930	0.9549	0.9453
MLP	0.6871	0.5139	0.9522	0.9079
ConvLSTM	0.7397	0.7248	0.9412	0.9253
DeepST	0.7593	0.7560	0.9539	0.9430
ST-ResNet	0.7941	0.7901	0.9537	0.9494
CoST-Net	0.8040	0.8027	0.9611	0.9535

图 15： CoST-NeT 预测实验结果

4.2 基于动态图卷积神经网络的交通需求量预测研究

截止 2019 年，交通需求量研究的最新预测方法主要基于深度学习的思路，基于深度学习的方法将交通网络建模成网格，并使用卷积神经网络 CNN 来获取空间相关性。然而，实际交通存在道路的不规则性和交通需求量在空间分布的不均匀性等特征，这些特征导致使用规则的网格进行交通需求量预测建模时存在着难以准确描述交通需求量的时空分布的问题。因此，杜博文提出了基于动态图卷积的交通需求量预测方法（图 16）。通过构建动态的需求转移矩阵以准确描述历史出行交通需求量及出行规律；在时空分布方面，将门限循环单元中矩阵乘法替换为动态图卷积，并动态提取交通需求时空依赖关系解决了难以同时考虑交通时空依赖的难点。

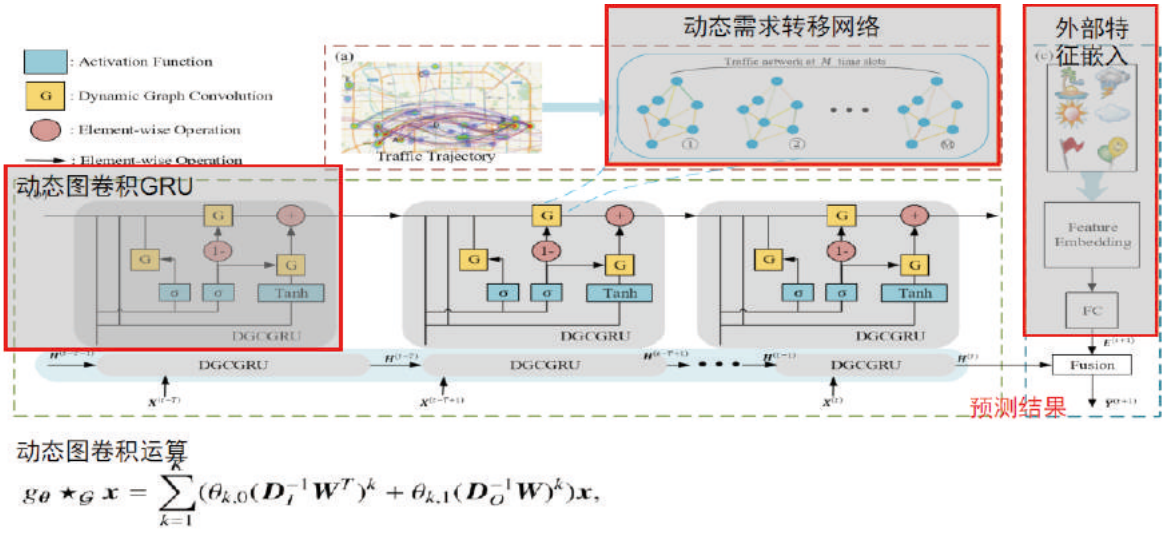
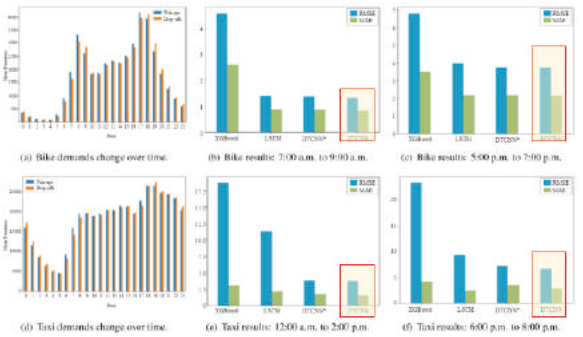


图 16： 动态图卷积的交通需求量预测方法

在 2020 年发表于 TITS 的《Traffic Demand Prediction Based on Dynamic Transition Convolutional Neural Network》的研究文章表明了在综合考虑时空依赖关系及外部环境因素对交通需求量的进行预测时，尤其是对出租车需求量的预测，动态图卷积的交通需求量预测方法与现有最好方法的 DCRNN 相比，RMSE 精度提高了 50%。此外，通过对分时段的预测结果进行比较，无论是早高峰还是晚高峰，DTCNN 具有更好的预测精度（图 17）。

Table 3: Results Comparison

Method	Bike-NYC			Taxi-NYC		
	RMSE	PCC	MAE	RMSE	PCC	MAE
HA	3.906493	0.541540	1.991092	38.663564	0.673600	9.529034
VAR	20.118131	0.329602	7.208243	16.209607	0.954641	3.083265
XGBoost	3.512882	0.561269	2.007128	16.973139	0.925507	2.955025
Basic RNN	3.864767	0.779739	1.872700	15.390889	0.951026	3.749574
LSTM	3.897652	0.788945	1.850340	13.077499	0.965589	2.930318
GRU	4.295366	0.719893	2.162775	13.429137	0.963306	3.289154
DCRNN	3.550321	0.815017	1.739865	19.918039	0.842173	4.801315
DTCNN*	3.444087	0.820051	1.740992	8.023104	0.987517	3.084475
DTCNN	**3.436808**	**0.820185**	**1.703449**	**7.778874**	**0.988342**	**2.8996 9**



在出租车数据上提高50%;

早晚交通高峰实验结果

图 17：DTCNN 交通需求量预测方法实验结果

此外，将该研究应用在深圳的交通数据集进行了验证，验证结果表明 DTCNN 方法能够反应居民的实际出行需求，可以为公交路线优化提供精准数据支持（图 18）。

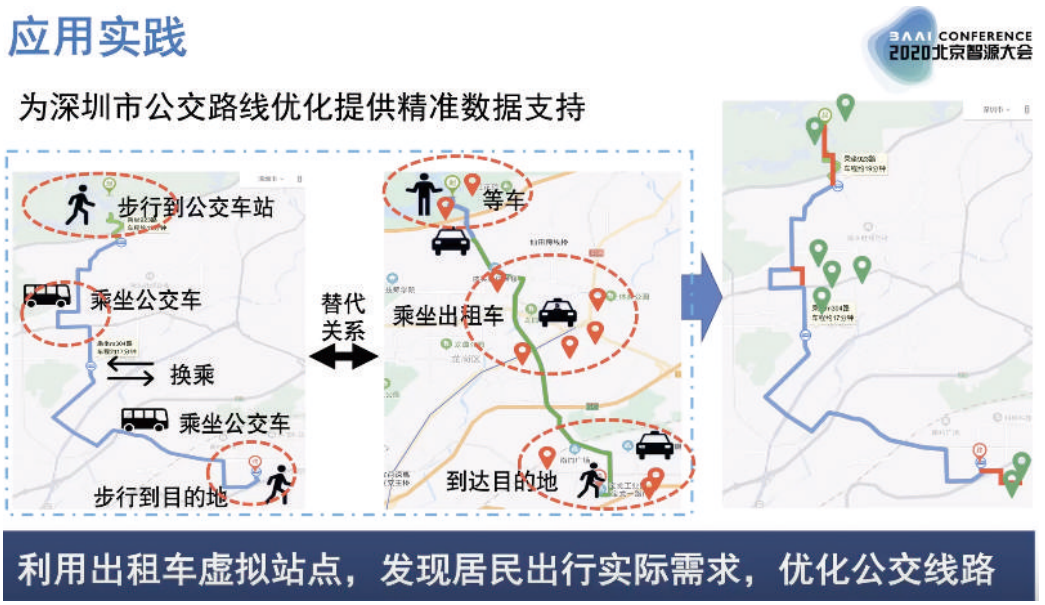


图 18：DTCNN 的实际应用案例

五、结语

最后，杜博文介绍到上述研究的交通时空数据都属于广义时空数据挖掘的框架（图 19），如从在最开始提到的固定位置的数据研究，可以映射到最简单的 a 这种结构化数据，地铁线路数据可以映射到 b 这种一维空间数据，

基于网格的交通数据可以映射到二维的空间数据 (c) 等。该研究框架还可以发现交通系统的通用特点，比如说除了路面交通数据、大量的地下基础设施检测数据、桥梁检测数据也符合这个框架。此外，广义时空数据挖掘框架还可以扩展到类似土木工程、桥梁工程、高铁线路等检测领域。

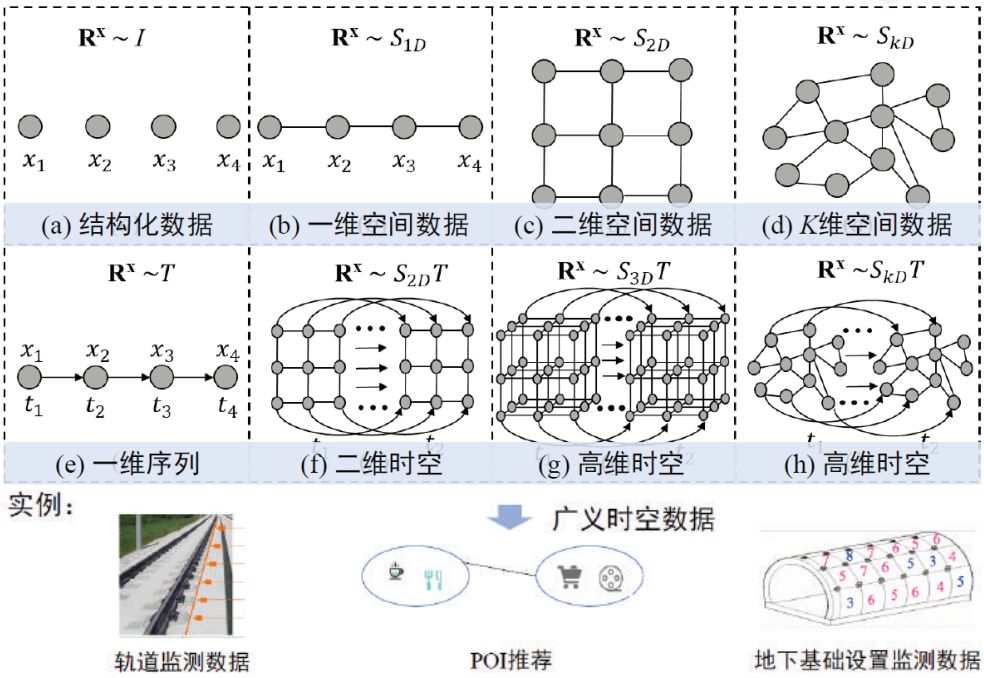


图 19 ： 广义时空数据挖掘的框架

参考文献：

[1] Transit Pattern Detection Using Tensor Factorization, INFORMS Journal on Computing, 2019.

[2] Bowen Du, Chuanren Liu, Wenjun Zhou, Zhenshan Hou, Hui Xiong. Detecting Pickpocket Suspects from Large–Scale Public Records. IEEE Trans. Knowl. Data Eng. 31(3): 465–478(2019).

[3] Bowen Du, Chuanren Liu, Wenjun Zhou, Zhenshan Hou, Hui Xiong. Detecting Pickpocket Suspects from Large–Scale Public Transit Records. IEEE Trans. Knowl. Data Eng. 31(3): 465–478 (2019)

[4] Le Yu, Leilei Sun, Bowen Du, Chuanren Liu, Hui Xiong, Weifeng Lv, Predicting Temporal Sets with Deep Neural Networks, KDD, 2020.

[5] Ye J, Sun L, Du B, et al. Co–Prediction of Multiple Transportation Demands Based on Deep Spatio–Temporal Neural Network. Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery Data Mining. ACM, 2019: 305–313.

[6] Bowen Du, Xiao Hu, Leilei Sun, Junming Liu, Yanan Qiao, Weifeng Lv, Traffic Demand Prediction Based on Dynamic Transition Convolutional Neural Network, IEEE Transactions on Intelligent Transportation Systems, 2020.

“AI 交通”圆桌论坛：强基建、重研发、促融合，政产学研携手，创造立体耦合智能交通网络

整理：智源社区 杨依帆

在 2020 北京智源大会“AI 交通”专题论坛的圆桌讨论环节，百度集团副总裁兼智能驾驶事业群总经理李震宇、北京市交通信息中心副主任杜勇以及北京航空航天大学教授杜博文参与了交流。三位专家针对主持人所提出的问题积极交换了意见，分别从政、产、学、研角度出发，提出了智能交通网络、数据知识融合、数据隐私保护等方面的相关架构设计解决方案。

图 1：2020 北京智源大会“AI 交通”专题论坛

主持人：首先请三位专家畅想一下未来的智能交通。

李震宇：未来智能交通主要有三点： 一是无人驾驶技术的突破； 二是相关政策法规的突破； 三是智能网联道路基础设施建设。

杜勇：智能交通需要完善智慧感知基础设施，针对城市道路资源、空间资源进行优化，让百姓的出行可规划、可预期。我们要变革传统交通运输调度方式，通过技术创新来带动机制和服务创新。

杜博文：智慧交通需要城市交通大脑进行决策，外加可控制的末梢神经系统配合运作。人、车、路协同耦合需要构建一张立体网络，基础设施保障能让出行更加安全可靠。

主持人：请谈谈交通大数据和智能交通服务之间的关系。

李震宇：大数据可以衍生出交通服务，交通服务也可以产生大数据。广义的交通大数据与交通服务可以有许多重叠的部分。

杜勇：大数据处在中台，用于支撑上层的各类智能交通服务。数据应用能力成熟度越高，代表支撑能力越强；反之，数据应用能力越低，服务对数据的依赖程度就越低。

杜博文：如何令数据知识驱动服务？关键点有四个：感知、认知，协同和预知。感知是感知当前状态；认知用于追根溯源，通过数据挖掘手段分析感知到的状态由何原因引起；协同是运用“群知”的手段，通过机器学习、迁移学习等方法构建协同网络；最后，预知可以判断演化趋势，实现智能交通精准服务。

主持人：今天几位专家组成了一个政、产、学、研的专家团队，请问过往工作经历给诸位何种启发？

李震宇：随着协同融合需求的增加，我发现大家的合作共识非常一致，未来政、产、学、研能够更加紧密地跨领域协作，共享数据信息。

杜勇：政府推动交通信息服务可分为三个阶段：主导、引导和督导。前期联合科研机构与企业实现关键技术突破；中期鼓励上下游企业开展合作；后期建立标准规范，加强监督工作，推进产业健康有序发展。

杜博文：科研方面一定要深入行业，弥补技术短板。政府接收反馈自学术界与产业界的数据知识，不断循环迭代，碰撞火花。

主持人：数据隐私保护主要有两种方式：一种是为数据增加噪音或扰动，让数据进行有损传输，另一种是当前热门的联邦学习——大家彼此保留数据，只开放访问权，互相传递加密参数，共同建模。请问这两种方式哪种更好？

李震宇：这两种方式我们在实践中都用到过。在共享前做一些必要的数据脱敏，使得数据流动起来，只有数据流动起来，创造的价值才不可限量。

杜勇：我们将公交线路站点等原始静态数据全部开放，而个人出行相关的隐私数据通过信息平台加密处理，将处理后的信息服务向企业开放。有损传输和联邦学习这两种技术方式都值得探索和引入。

杜博文：联邦学习是非常关键的技术，通过 DES 把数据包装成服务形式提供给用户，同时区块链配合进行加密追溯和智能合约签订。通过“数据即服务”的方法将数据链接起来，形成可总控的虚拟通道。数据在使用过程中是透明的，用户并不知道数据来源于何处，而区块链的追溯功能可以追溯到谁使用了数据。

16 机器学习

AAAI 主席 Yolanda Gil：思虑周全的人工智能——为数据科学和科学发现构建新型合作伙伴关系

整理：智源社区 罗丽

在北京 2020 智源大会机器学习专题论坛上，AAAI 主席、南加州大学信息科学研究所副主任 **Yolanda Gil** 作了题为“Thoughtful Artificial Intelligence: Forging a New Partnership for Data Science and Scientific Discovery”（思虑周全的人工智能：为数据科学和科学发现构建新型合作伙伴关系）的主题报告，为我们介绍了“Thoughtful AI”在零散数据整合和跨学科研究中的重要作用，同时提出了设计 AI 系统需要遵循的七条原则或七大研究领域对构建有效的 AI 合作伙伴关系的重要影响。

Yolanda Gil，南加州大学信息科学研究所副主任，美国人工智能协会（AAAI）第 24 任主席，美国计算机协会（ACM）会士，人工智能特别兴趣小组前任主席，毕业于卡内基梅隆大学，曾在美国国家科学基金会计算机科学与工程理事会咨询委员会任职。

正式演讲前，**Yolanda Gil** 首先介绍了“Thoughtful Artificial Intelligence”的概念、人工智能的应用以及人工智能在科学领域的发展和研究现状。

Yolanda Gil 表示，人工智能应该具有具备推理和思考其正在采取的步骤和过程是否合理的能力，以便它可以传达其思想、改善思想，并提出新的思维方式和学习思考问题的方式，**Yolanda Gil** 认为，“Thoughtful Artificial Intelligence”是研究 AI 系统如何成为数据科学和科学研究合作伙伴的一个好方法，在接下来的几十年，她非常希望能够看到 AI 科学家的出现，以及 AI 科学家、数据科学家、工业界和不同学科的科学研究人员的合作。

推荐系统、无人驾驶汽车、足球机器人、IBM Watson、问答游戏、帮助改善搜索的针对性最佳人类知识图谱以及 AI 会话系统等机器学习系统和机器人技术是已经成熟的人工智能技术。AI 成功的前景中，有两种不同的线程

彼此互补且相互作用，一个是数据线程，数据线程是从大量数据和大量的观察中学习； 另一个是有关世界知识、有趣的实体知识和任务知识的知识线程，如 IBM Watson、知识图和会话系统，知识对于启用 AI 应用程序具有强大作用。

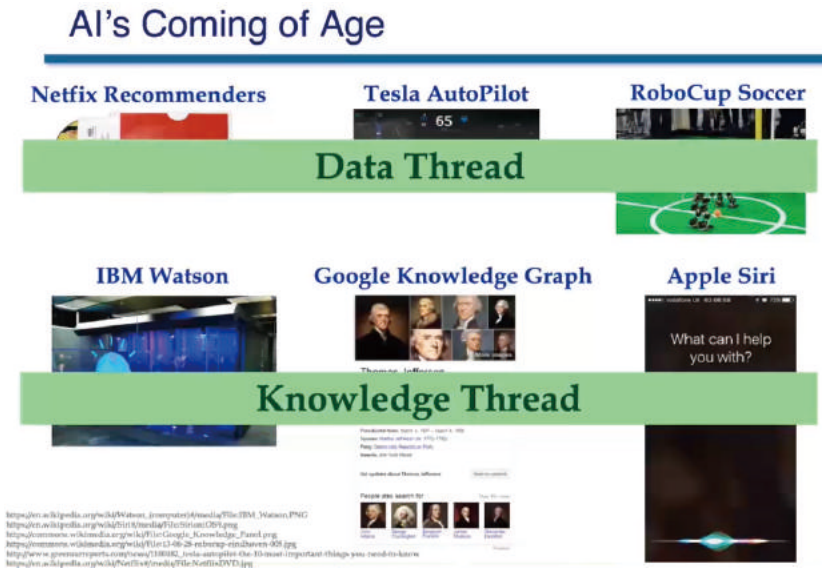


图 1： 成熟的 AI 应用

科学中人工智能的应用是 **Yolanda Gil** 的研究重点。例如，推荐系统技术在勘测气候数据时非常强大； 位于海底的自动驾驶机器人能够自动进行实验并收集数据； 通过生物学和化学方法可以实现实验室设备自动化的机器人自动化； 科学知识图谱中的大量工作文本提取，解决了工厂的大项目，其中包括许多不同的兴趣实体，整合制药公司，解决问题并理解科学的工作流程。

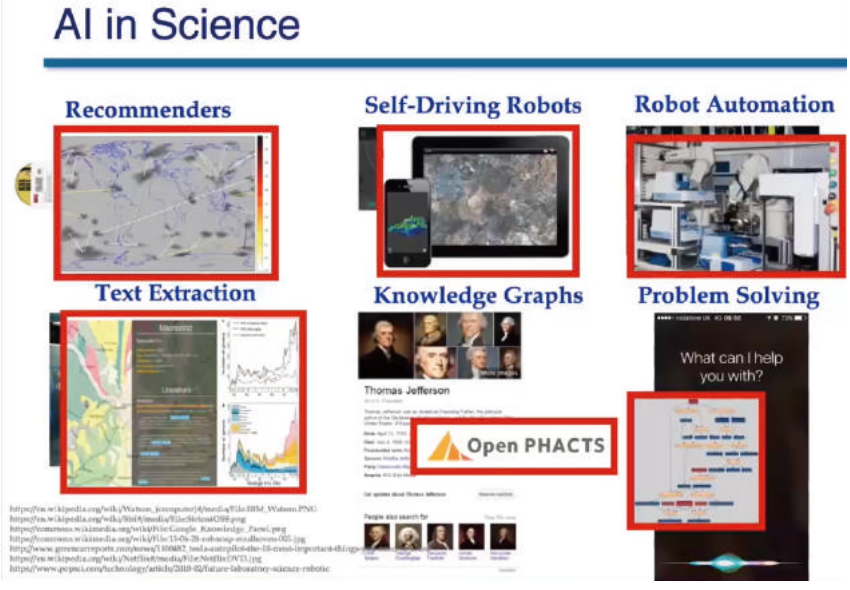


图 2： 科学中的 AI

科学中的 AI 跨越了两个传统，在数据线程和知识线程中有着悠久的历史，在数据分析和知识推理方面也具有悠久的发展历史。

AI 的先驱者 Herb Simon, Feigenbaum 和 Bruce Buchanan 等人以不同方式的两个方面研究从 AI 的角度看待科学，如图 (3) 左图所示。之后，**Yolanda Gil** 介绍了不同科学杂志中有关“AI Transformations Science”的研究，如图 (3) 右图所示。其中，左上方的研究是，致力于计算可持续性和环境可持续性的数据线程，使用机器学习和约束优化技术研究自然环境； 右上方的研究是，用深度学习改善蛋白质结构预测； 左下方的研究在 AI 中使用知识图谱的知识线程，以及毒理学推动知识发现的研究。右下方是关于词的文本学习，以获取大量文献知识的研究。可以发现，人工智能是一门贯穿所有领域的渗透科学。

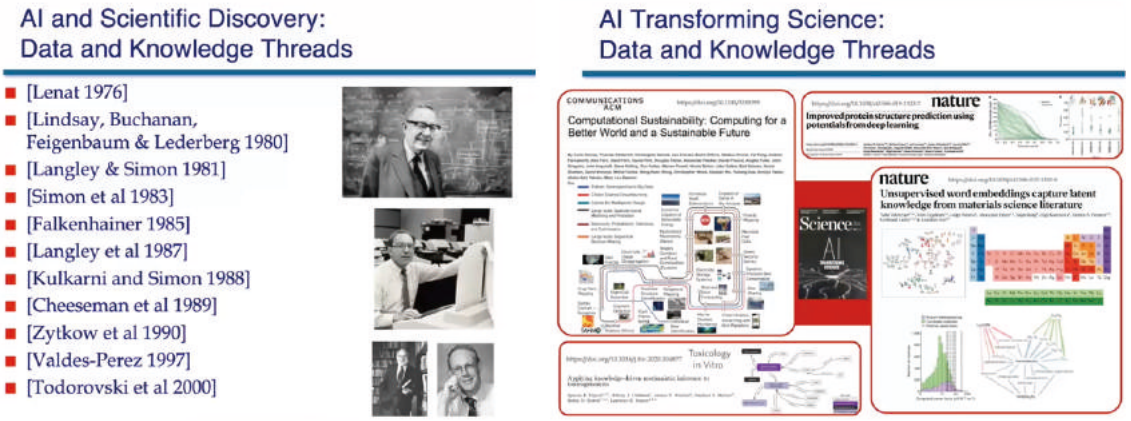


图 3： AI 研究学者与研究文献

Yolanda Gil 的演讲内容主要包括四个方面:

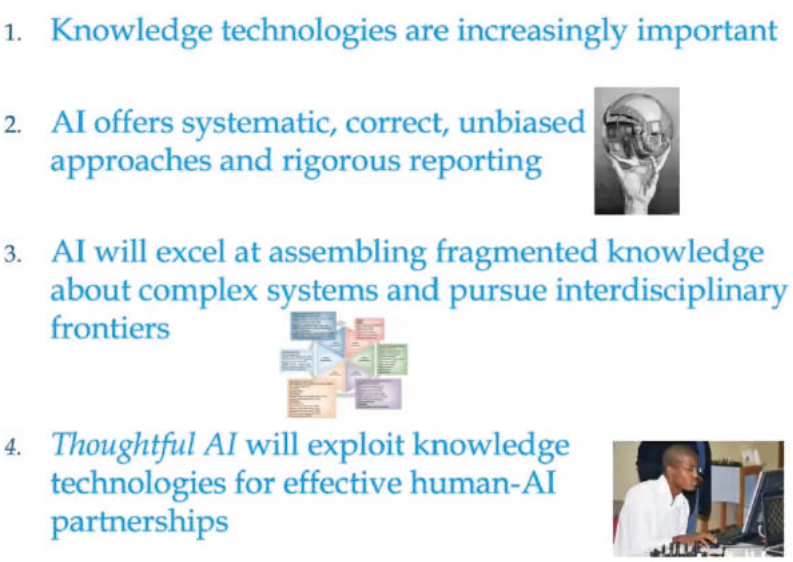


图 4：**Yolanda Gil** 的演讲内容

(1) 知识技术越来越重要
(2) AI 提供系统的、正确的、无偏见的方法和严格的报告
(3) 人工智能擅长整合有关复杂系统的零碎知识，追求跨学科前沿
(4) “Thoughtful AI”将利用知识技术建立有效的 AI 伙伴关系

一、知识技术越来越重要

知识技术越来越重要，一方面是通过大量的大规模知识库的工业采样，知识库能够捕获不同类型的知识，这些知识与不同目的和应用相关，所以它非常强大。**Yolanda Gil** 认为可以将数据作为开放的知识库，开放的知识库对科学具有重要的影响，是一种非常重要的知识工艺。在越来越多的应用研究中，工业规模知识图谱、知识库和自然语言等被得以广泛地应用。在过去 3、4 年中，从文本常识知识中提取常识成为了一种新的研究热点，**Yolanda Gil** 所在的研究所在这些领域中已经做了很多研究。**Yolanda Gil** 表示，在计算机视觉的研究中，知识标题的提取将忽略对图片的描述，视频使得研究者对对象以及所观察到的关系的准确表示变得越来越困难。在机器学习和数据科学中，需要使用用户能够理解的知识和术语来解释系统在做什么，它是理论指导数据科学的重要方向，也可以通过使用物理知识来约束机器学习系统正在学习的内容，使它满足相关的物理定律。

在某些领域的理论研究中，越来越多的知识技术贯穿其中，因此，在获取知识和保持知识更新方面仍存在很多挑战。研究人员表示，具有“维基百科知识量”的理论研究中，这种规模的资源扩展和状态更新将是一项非常艰巨的任务。因此，可以考虑尝试获取与某个领域相关的知识，或与总体有关的兴趣实体的知识。获取所有知识是一个巨大的挑战，但是拥有像 Wiki 数据之类的资源，或者像 Wiki 数据一样获取大量知识的资源对某种理论研究是很有用的，这也表明了知识技术的重要性。

二、AI 提供系统的、正确的、无偏见的方法和严格的报告

人工智能提供了一种非常独特的方法来查看任何领域的数据和知识。那么人类是如何研究和使用数据的？其中又存在着哪些问题呢？

1. 人类是非系统的。有一项研究表明，使用文本提取系统来编译化石记录中已知的所有内容，然后将它们与自动化系统进行比较时，发现人工提取需要大约 10 年的时间，与手动提取数据相比，即使文本提取仍是一种不完美的技术，但人工智能系统仍更具系统化、更加完善，机器能够从人类错过的文章中提取很多有用东西，不完善的 AI 系统比人类做得好。

2. 人类会犯错误。在一篇文献中，作者在整理影响不同国家经济衰退的因素时，实际上将一些国家排除在外，这使得一些偶然的重要信息可能被排除在分析之外。

3. 人类存在偏见。Yolanda Gil 引用另外一个实例说明了人类在数据研究中存在偏见。一个观察古气候记录的视觉和人工智能系统能够观察到过去几个世纪的气候数据，并提出一些可以解释气候趋势的假设，这些是正在研究相同数据的科学家的论文中从未提及的。而当 **Yolanda Gil** 问及科学家有关假设时，得到的回答是，“这是一个很好的假设，我只是没有提及它，我认为我在论文中讨论的那些假设足够好。”可以看出，在某种程度上，研究人员确实存在偏见，而我们拥有很多可能性并且能够加以探索。

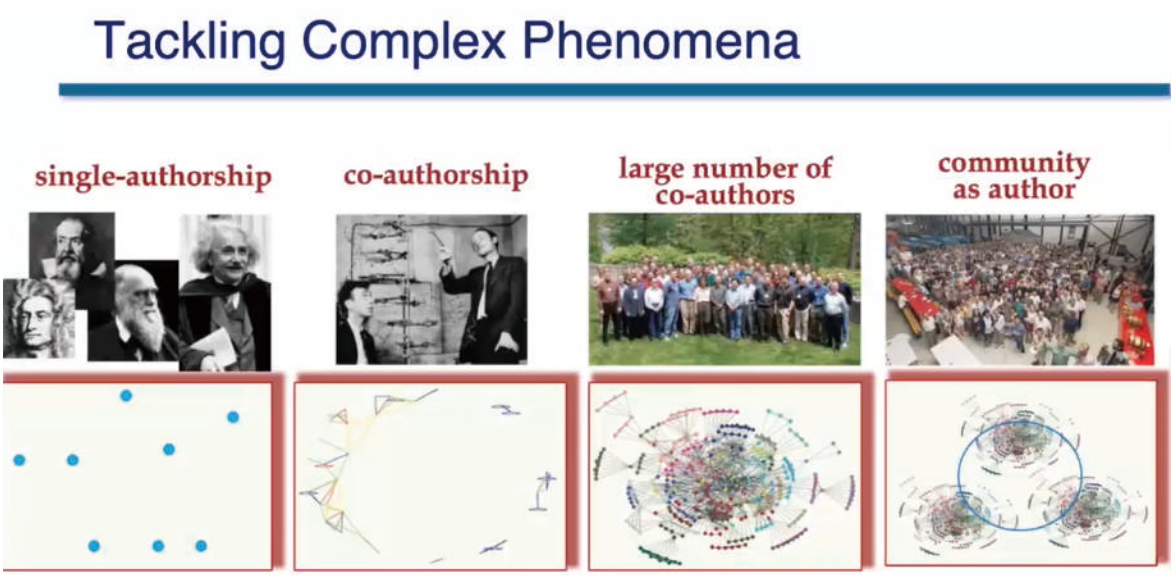
4. 人类会遗漏重要信息。实际上，人们写论文时会漏掉许多重要信息，**Yolanda Gil** 将其称为不良报告。书面论文很难再现和复制，**Yolanda Gil** 及其团队已经做了一些研究，用于量化复制论文的工作量。人工智能系统的科学遗产或出版物可以进行某些数据分析和研究，这些研究可以以更加系统、正确和公正的方式提出一些可能的解释和假设，并能够对 AI 系统的运行进行严格的实际报告。就保持严格性而言，人工智能系统确实可以改变规则。

Yolanda Gil 认为，虽然我们离拥有极富创造力的 AI 系统还很遥远，但是在很多领域中，人工智能系统可以以更好的方式帮助我们做研究。在蛋白质组学和基因组学的研究中，AI 系统会自动提供一个假设，并自动查看可用于检验该假设的数据类型和方法，并得到结果，AI 系统能够对结果进行推理，然后生成修订的假设（如果适用）以及该假设的一些置信度值。在这些研究中，人类分析很难做得透彻，而 AI 系统可以做到真正尝试测试每个搜索引擎，检查每个可能的选项并在搜索和优化科学方面做得更好。

那么，我们是否可以认为，如果机器能够执行指令，那么如果我们给机器以科学的指导，它们就可以更加彻底而正确地分析大量可用数据。答案是否定的，我们还需要花费了大量的时间来阅读文章和书籍，以了解科学家是如何提出问题，如何回答问题以及需要考虑采用哪种机制。**Yolanda Gil** 表示互联网人工智能科学家设计的真正的“Thoughtful System”，需要经历研究科学并彻底实现科学的运动。

三、人工智能擅长整合有关复杂系统的零碎知识，追求跨学科前沿

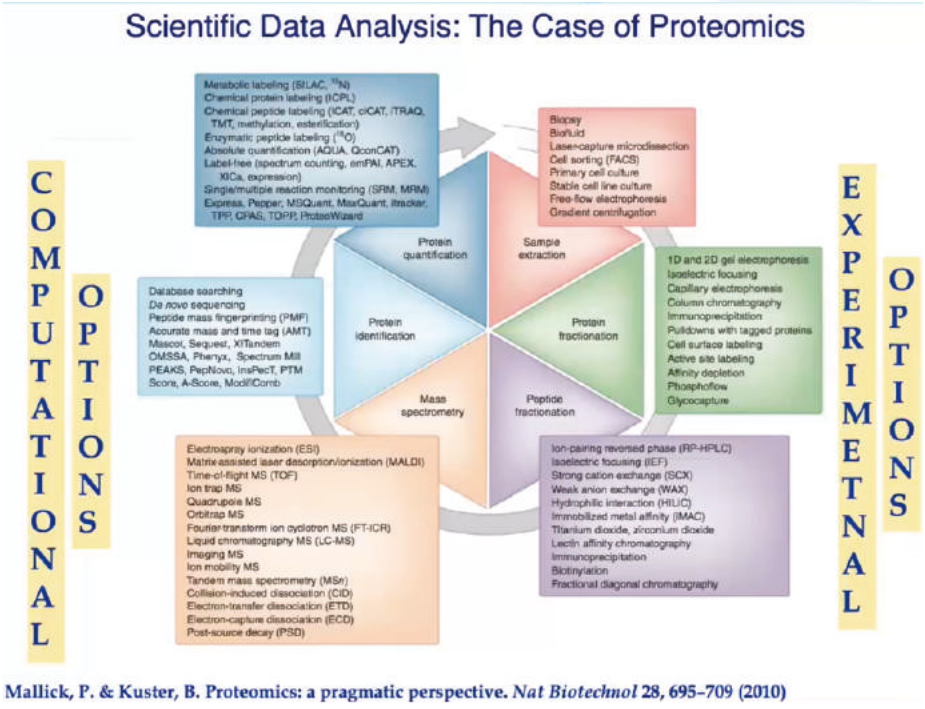
人工智能不仅会对分析特定学科的数据产生巨大影响，也会使科学研究发生巨大变化，零碎知识和系统是非常复杂的，需要从事跨学科研究，这对人们来说是非常具有挑战性的。所以，如果想要了解大脑区域复杂系统，比如了解大脑，或了解地球健康的生态系统，亦或是了解宇宙历史，为了整合各种知识和数据，我们需要非常认真地对待 AI。



Evolution of the scientific enterprise from [Barabasi, 2005] extended with the ATLAS Detector Project at the Large Hadron Collider [The ATLAS Collaboration, 2012].

图 5：合著网络演化

一个世纪以前，一位科学家只对应一篇论文一位作者，而在二十世纪初，出现了共同作者和简单的合著网络，之后又出现了越来越多的合著团体。科学正变得越来越复杂，那么 AI 如何帮助我们解决问题?



Mallick, P. & Kuster, B. Proteomics: a pragmatic perspective. *Nat Biotechnol* 28, 695–709 (2010)

图 6： 蛋白质组学研究

图为蛋白质组学图片，每个颜色不同的区域分别表示不同的蛋白质组实验室的不同专业见解，每个不同的方框展示了不同的实验方法。可以看到，没有一个实验室能结合所有方法进行研究，而人工智能具备各种专业领域的知识。在进行科学审查时，要求科学家拥有其团队成员所具有的所有专业知识，而大多数人是需要合作分析数据。而 AI 系统可以与人类合作，帮助我们收集零散知识并进行跨学科科学的研究。

以 **Yolanda Gil** 及其团队的项目研究为例，为了解食物供应及短缺，**Yolanda Gil** 及其团队在项目研究时整合了不同的学科模型。渔业取决于气候，依赖于水模型、农业模式以及农作物经济价格，每个学科的模式都是不同的，而集成模型或中等模型的建立需要花费数月或数年的时间，而且大部分是手工完成的，并且需求量在不断增加，它们在本质上有很大的不同，**Yolanda Gil** 发现需要从回答模型建立方式的问题，考虑的变量，使用的数据类型以及模型的运行方式等方面来思考模型的构建。而人工智能能够跨越不同学科，每个不同模型可以代表不同的过程，如何使用模型？一个模型如何从其他模型获取什么样的数据？哪些参数可以探索？可以用某个模型研究哪些物理变量等，人工智能能够把复杂问题组装起来，在科学上以更有效的方式整合模型，帮助我们研究跨区域因果关系。在不同实验室、不同群体和不同学校的研究中，高度交叉的学科和知识是分散的，很难将其整合起来，而 AI 系统能够在整合有关复杂系统的零碎知识中发挥更大的作用。

四、人工智能的研究方向

演讲的最后一部分是关于**“ Thoughtful AI”** 的研究方向，**Yolanda Gil** 认为，**“ Thoughtful AI”** 的研究将真正改变 AI 系统与人类的合作关系。

对科学家来说，拥有科学合作伙伴会带来一系列更严格的要求，因为他们想要进一步真正地理解、解释和辩论一些问题，而人机交互是其中最重要的问题，在人机交互中，人类可能在某些任务上做得好，而计算机更擅长

其他任务。以 Garry Kasyanov 提出的自由式象棋为例，Garry Kasyanov 曾表示，一个玩家可以是任何人与计算机的组合，任何超级计算机和任何数量的人，这些人将代表整个团队中的一个计算机，而人类又将与另一个玩家竞争。

那么我们如何设计出人机交互的最佳玩家呢？很明显，人机交互的最佳玩家并不是拥有最好的计算机和最优秀的大师的最佳组合团队，而是对国际象棋具有中等知识并且知道应该由那个人来制作那个游戏，应该使用哪个计算机程序来制作所要玩的游戏，以及一个好的流程来确定谁负责整体玩家的进步。因此，需要用最好的计算机，在最先进的算法中使用最优秀的人，人机交互的最佳玩家是人机互动和相互补充产生的最佳结果。那么，在 AI 系统中拥有科学合作伙伴需要遵循什么原则？人工智能系统需要做什么来帮助我们解决这些大的问题？

演讲中，**Yolanda Gil** 详细阐述了**“ Thoughtful AI Systems”**所包含的 7 条原则，并表示，在科学研究和数据科学中，这些原则将帮助我们建立有效的 AI 伙伴关系。

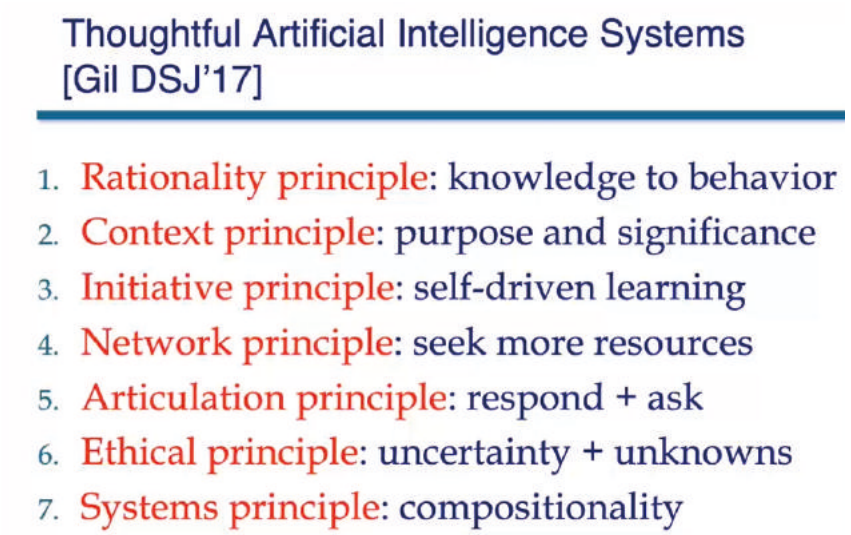


图 7：**“Thoughtful AI Systems”**所包含的 7 条原则

1. **理性原则。“ Thoughtful AI Systems”**的第一个原则是理性原则，它要求 AI 系统具有确定其行为的知识，这意味着它们必须具有一定的可预测性，必须能够理解系统从知识到行为的运行方式。AI 科学家使用的知识是与特定行为相关联的知识，这样才能回答诸如 AI 系统是否理解水流理论或其他任何理论，并确定其答案的问题。
2. **语境原则。**在科学中，AI 系统包含他们正在执行的任务，提供的数据集和算法等其他指标，AI 系统对他们所要回答的问题的类型，问题的相关性，问题的目的和意义具有“自己的想法”。在科学中我们可以提出什么样的问题？这些问题遵循什么样的模式？不同学科遵循的方法是什么？思考科学家回答不同问题所遵循的过程和问题是什么？他们会看到什么样的数据？遵循什么样的方法？这些都是非常重要的问题，但它们不仅仅是一个问题，更重要的是要了解有关问题的来源。
3. **主动原则。**AI 系统能帮助我们解决非常复杂的问题，而且并不需要我们教他们所有知识，并向他们解释一切，AI 系统在学习方面具有非常强的自我驱动能力。他们能够在每天晚上学习所有知识，并从头开始阅读文献，然后重建他们所知道的一切知识。他们能够将自己从文献中学到的新知识整合到已知的知识中，并能够运用

判断力将所有知识整合到该系统的工作方式中。AI 系统能够通过自我指导和自我询问学习和回答一些问题，能够在新方法出现时能刷新自己的知识。

4. **网络原则。**AI 系统应存在于一个包含网络资源和科学资源的知识网络生态系统中，他们可以在其中自由地访问服务，访问数据库，访问不同类型的工作流知识，即各种不同的知识方式，无需某种连接性和能力，以便他们及时回答正在出现的问题，而且可以将结果放入该科学记录网络中。能够与其他事物建立联系非常重要。
5. **衔接原则。**在科学中，解释 AI 系统中的重要信息是非常有必要的，科学家们不仅希望能够听到有关结论的解释，而且还希望能够听到这一发现与文献中所知信息之间的联系，这就是扩展。扩展对科学非常重要，而 AI 系统应该能够阐明联系并把他们的发现传达给不同的听众。AI 系统可以从不同的角度展示来自不同工作领域的人的回答，可以将其与其他研究或已知的方法联系起来，AI 系统了解自己的发现背景，发现的重要性以及如何与其他工作进行对比和整合的方式。
6. **伦理原则。**伦理原则非常重要，涉及范围也相当广泛。对 AI 系统来说，其行为和运行产生的结果会受到伦理的范围和局限性的约束。只能访问某种类型的数据或某种特定类型的观点在科学中尤其重要，因此，将知识融入观念非常重要。
7. **系统原则。**系统原则是 AI 系统的第七大研究领域，是为特定任务或目的创建系统。研究者可以通过训练系统使其完成多个任务，但在将 AI 系统视为应该能够组成的系统或者将其作为不同层次的抽象系统等方面仍有很多工作要做。链接不同的 AI 功能非常重要，而 AI 科学家能够解释，提出，设计和计划这些系统应该具备的多个功能。因此，能够将不同 AI 系统集成在一起非常重要。

Yolanda Gil 表示，这 7 条原则是人工智能研究中非常重要的研究领域，它们将使 AI 受益并推动 AI 成为科学和 AI 系统的有效合作伙伴，具有更广泛的范围和应用空间。

五、结语

机器学习是人工智能领域的研究热点，其目标是希望计算机能像人一样进行学习，从样本数据中学到知识和经验，然后用于实际推理和决策。人工智能数据科学中数据驱动的研究使我们进一步了解到知识技术的重要性，人工智能系统可以为我们提供更系统的正确的、无偏见的方法来分析任何数据和知识，并进行科学的、严格的报告，在整合复杂系统零碎知识和跨学科研究中，人工智能系统具有重要作用，**Yolanda Gil** 提出的设计 AI 系统需要遵循的七条原则或七大研究领域对构建有效的 AI 伙伴关系，分析有关数据信息和知识具有重要作用。

Q&A:

主持人：有教授表示，情感是人类智能中的一个重要因素，那么您认为，在 AI 系统设计中是否可以将情感作为一个重要原则。

Yolanda Gil：我认为这是一个非常有趣的观点，事实上，在演讲中我谈到人类是有偏见的人，在某些场景中，我认为有一种情感在科学中是非常重要，那就是顽固，这种决心和顽固的情感在某些研究和系统设计中或许是最重要的情感。但在通用智能中我认为这个问题是非常具有针对性，比如有研究人员已经开发出情感驱动的框架，这对开发虚拟人类非常重要，特别是在医学领域。

卡耐基梅隆大学邢波：一个标准化、可组合的机器学习蓝图

整理：智源社区 孙超

邢波本次的演讲主题是《A Blueprint of Standardized and Composable Machine Learning》(一个标准化、可组合的机器学习蓝图)。

邢波，卡耐基梅隆大学机器学习系副主任，美国新泽西州立大学分子生物学和生物化学博士，美国加州大学伯克利分校计算机科学博士，主要研究集中在机器学习和统计学习的方法论和理论，大规模计算机系统和架构的开发。邢波曾经担任过美国统计协会期刊应用统计年鉴的副主编，同时也是机器学习杂志和机器学习研究杂志的执行主编，曾经在 2014 年担任 ICML 的主席。

在报告中，邢波总结了自己近几年的研究工作，详细向我们介绍一套关于机器学习的底层理论应用公式，他从机器学习的微观层面，包括损失函数、优化器、模型架构、理论知识，构建了一套机器学习的蓝图理论，并将其实例化，应用于人工智能领域。

下面我们对邢波的这套机器学习蓝图框架作详细介绍。以下是智源社区编辑整理的邢波报告内容。

一、机器学习蓝图是什么样的：How about a blueprint of ML

众所周知，AI 已经被用于解决很多任务和问题，如目标识别、内容生成、计算生物学、健康保健，自动驾驶汽车等，如图 1 所示。人们对机器学习寄予很高的期望，很多学者致力于研究机器学习，他们采用了各类神经网络模型，如图 2 所示。然而机器学习需要处理大量的数据，并且往往很多数据会超出你的认知范围，有时候单点数据也可能需要大量的经验积累。所以，对于机器学习研究者而言，即便有丰富的研究经验，想要做好机器学习研究，也需要大量的工作。

图 1：机器学习应用场景

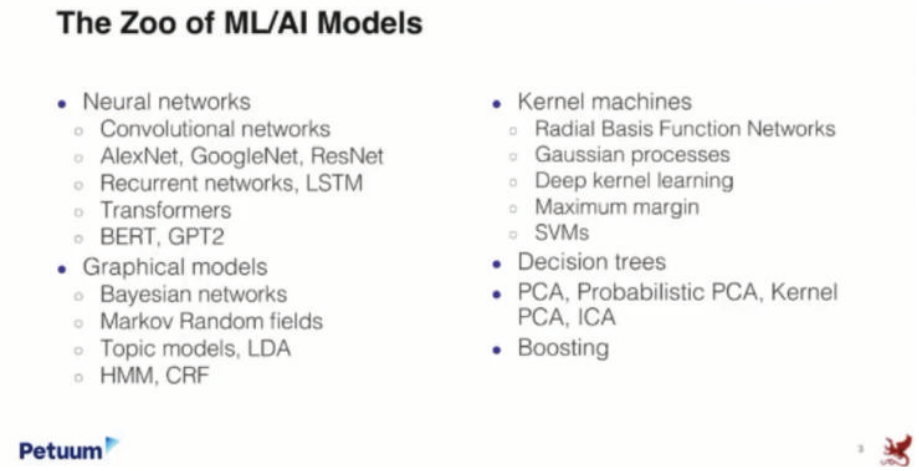


图 2：常见神经网络模型

人们很难根据个人经验或创造力在一些事情上进行导航，如迷宫。但是可以假设一套关于机器学习的设计蓝图，通过不同的算法及相关公式去处理不同的问题。基于此，邢波建立了一个蓝图支架，该支架包含 3 个分量，如图 3 所示： 一个是损失函数，给系统训练设定目标； 一个是模型架构，神经网络需要非常大的库，需要设计模型架构来进行探索； 再一个是优化器。作者用这样一些简单的维度和理论去绘制一个机器学习蓝图，应用于现在或者将来，从而避免随机或者费时的相关工作。

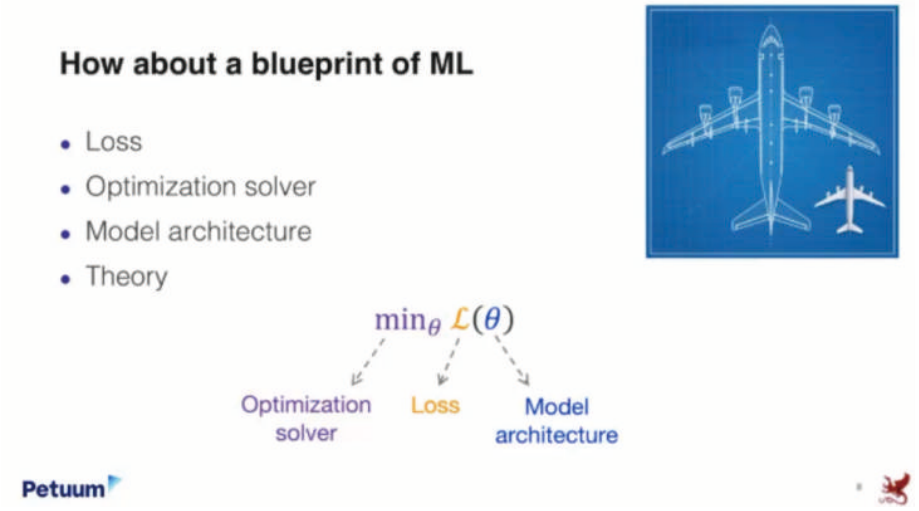


图 3：机器学习蓝图组成

二、机器学习标准公式：The standard equation

邢波根据相关实例提出了标准公式，如图 4 所示： 第一个公式定义了一个损失函数，给出了目标分散和作为参考量的差值计算，然后需要一个约束条件整合各类不同的数据和实践，该条件可以用于某个规则或者作为其它的限制条件或者成为分隔边界等。等效地将约束条件公式写为最下行公式的形式，可以看到该公式包含 3 个部分，第一个部分为经验，包括外来的正则化、数据样例或者计算规则等； 第二部分是分歧项，实际上是建立一个训练中的动态，像老师和学生之间的相互作用，把一个模型当作老师，另一个模型当作学生，学生会逐渐学

习靠近老师，达到一个收敛的效果，老师当然对自己的知识存在不确定性，因此第三部分是一个熵的术语。邢波从物理相关的研究中获得启发，得到该公式，并运用该标准公式以一个简单的方式进行了重现熟知的算法工作。

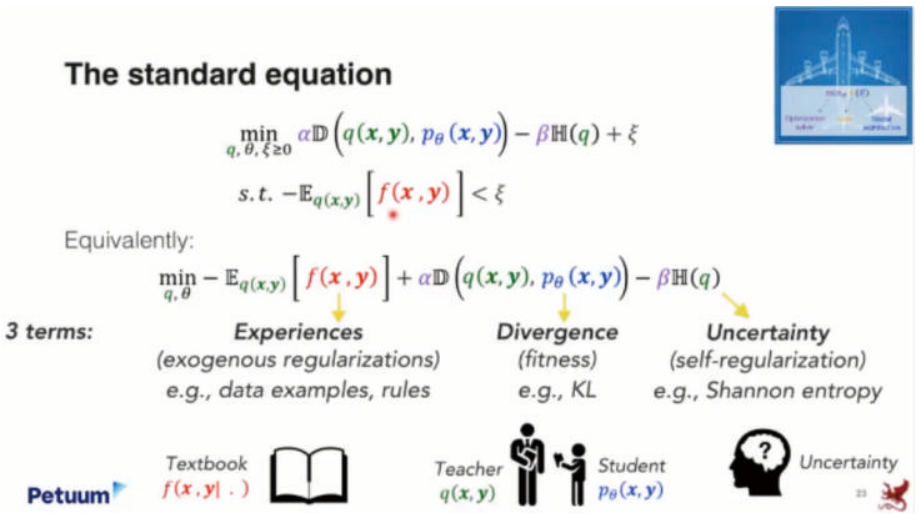


图 4 标准公式

三、基于标准公式下的一些机器学习算法介绍

接下来，邢波列举了在标准公式基础上实现的相关算法，主要涉及主动学习、增强学习、对抗学习。假设存在一个非常庞大的学习框架需要主动学习，在标准公式下，主动学习有一套新的公式和理论，但是和其他公式没有太大的区别，只是需要重新定义这些特征函数和经验函数。如图 5(a) 所示的一个区间函数，确定了数据的存在和缺失，在一些数据库中，缺失数据出现后将会造成一定的不确定性，需要通过预测调整。图 5(b) 为增强学习，同样证明了标准方程的普遍性。增强学习不局限于数据，还拓展到环境空间等状态，根据质量及要求增加了奖励函数，事实上使用增强函数，重点需要做的是重新定义经验函数和质量函数的关系。在虚拟学习方面已经变得非常流行的对抗学习，如图 5(c) 所示，也是在标准公式下构建的，它主要利用概率下降函数，被广泛应用，包括内容生成方面的应用。

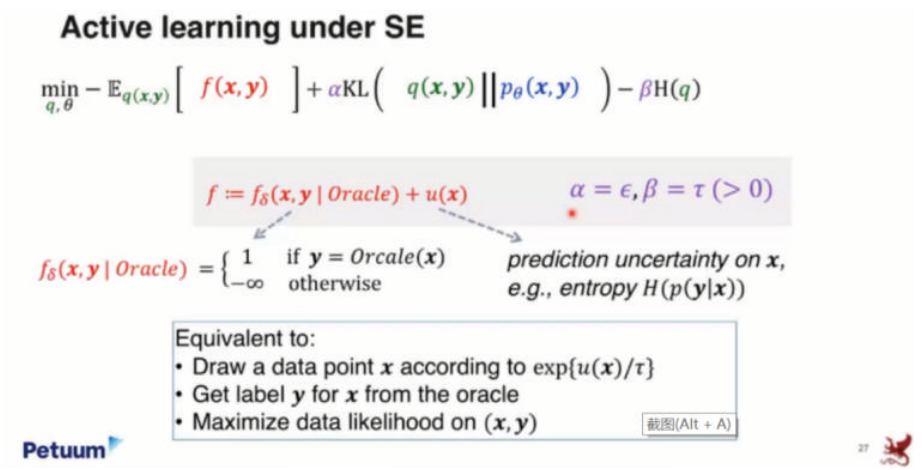


图 5(a)： 主动学习

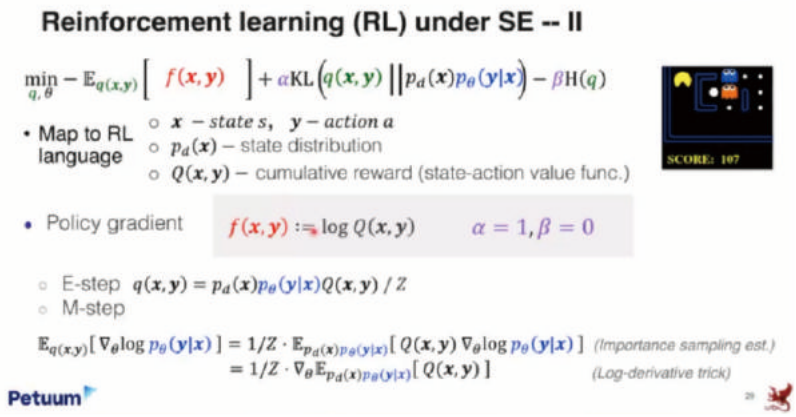


图 5(b)：增强学习

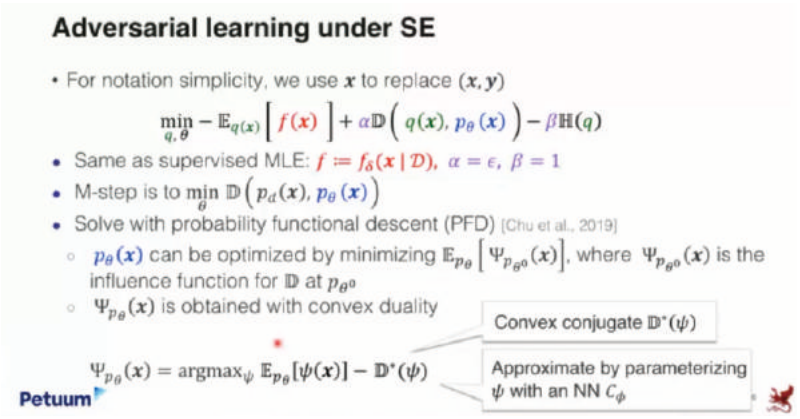


图 5(c)：对抗学习

邢波列举出很多使用标准公式的算法例子。如图 6 所示，包括数据扩充、重新加权、约束驱动学习、好奇心驱动、知识升华等，本质上他们都是以标准公式为基础，只是会因为定义以及经验函数的不同导致一定的差异。

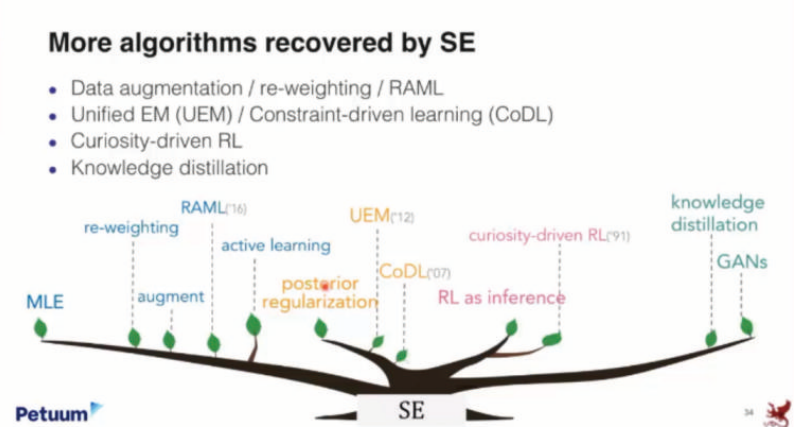


图 6：基于标准公式的算法复现

关于优化求解器方面的介绍如图 7 所示，优化求解器现在还无法像标准公式一样作为很多应用的主损失计算。但目前为止，在某些方面已经比较接近了，像梯度下降函数可以提供一个简洁的公式作为解算器，缩小计算的损失。目前优化求解器的算法主要有反向传播、凸对偶性拉格朗日算法、整数线性规划以及梯度下降函数等。

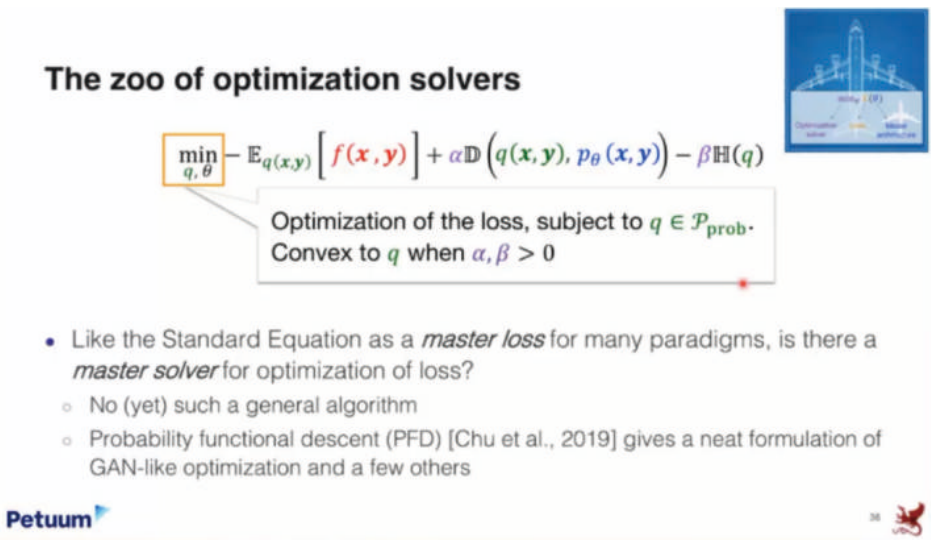


图 7 优化求解器

四、模型架构

机器学习蓝图的最后一部分为模型架构。模型架构主要包括三个部分，分别是神经网络设计、图像模型设计以及组成架构。如下图所示，图 8(a) 显示各神经网络组成部分之间互相联系，编码器、解码器、嵌入器等可以通过输入 FFNetwork、RNN、Transformer、WordEmbeder、PositionEmbeder 等生成分类器、编码解码器等，同时用一种非常简单的方式将他们进行组装； 图 8(b) 为图像模型设计，人们较为了解可以通过小的组块构建更大的模型； 图 8(c) 多组结合构建深度神经网络，有时会集成神经网络和图像网络，得到混合图像或者多因子图像，形成一个多模型或者多目标的网络架构。

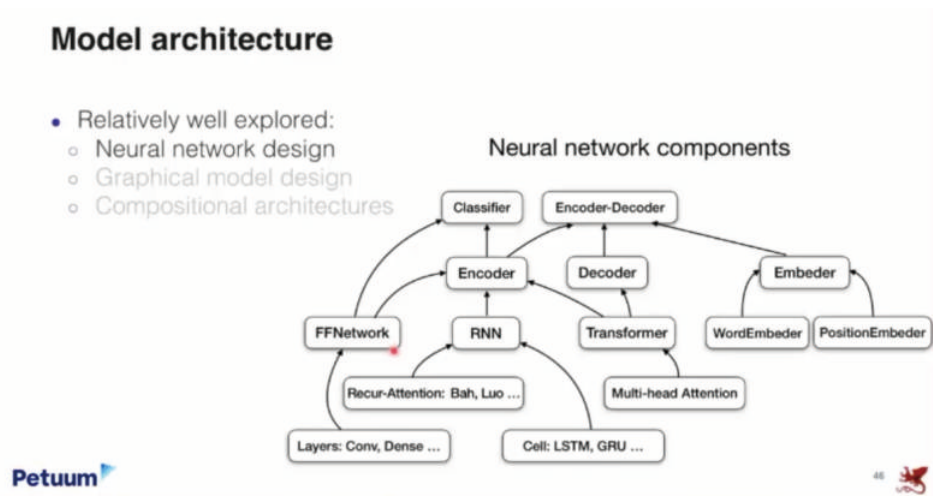


图 8(a)：神经网络组分

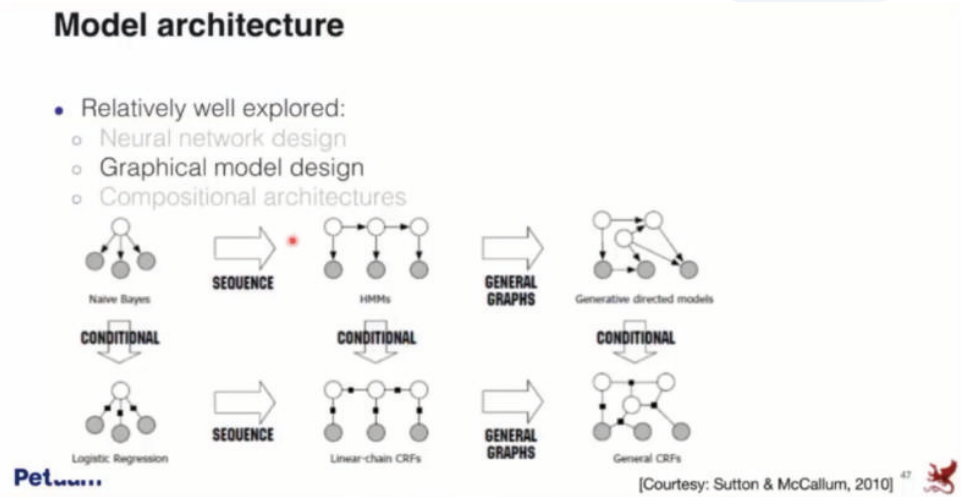


图 8(b)：图像模型设计

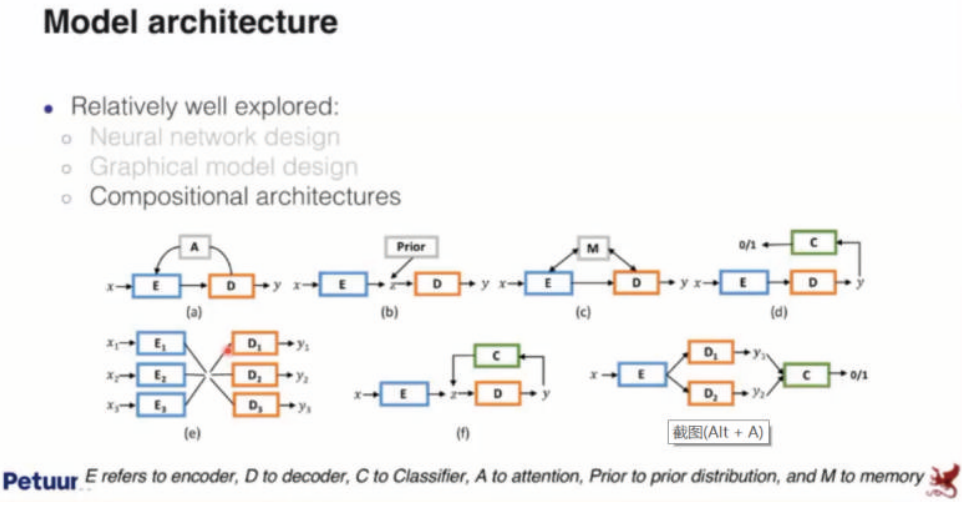


图 8(c)：模型架构

五、机器学习蓝图综述

综上，如图 9 所示，机器学习蓝图主要包括 4 个部分： 首先是函数，本文最起初谈到的标准公式，也是该蓝图的核心部分； 再者是算法，在标准公式基础上的可替代优化算法、梯度下降函数等； 再一个是模型架构； 有了以上三点，再结合相关理论，构成了本文的所描述的机器学习蓝图概念。从目前来看，这个蓝图还只是重现之前的一些经典算法，但是或许在将来，机器学习可能会从这个公式开始构建，以这个公式的损失函数、收敛性等，构建更多的实践和算法。

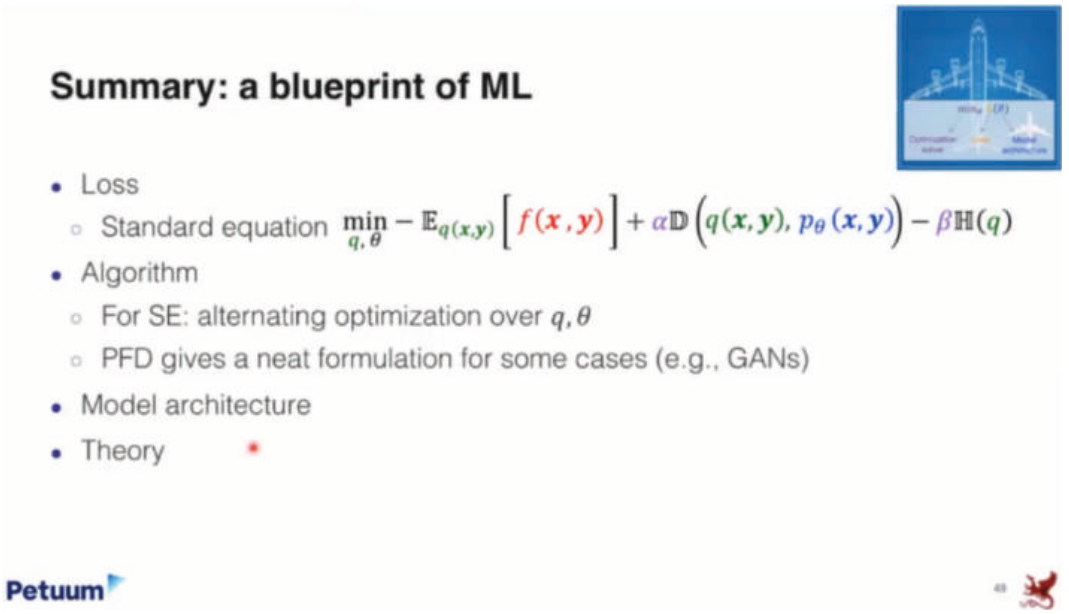


图 9 机器学习蓝图综述

结语

邢波老师的这场关于机器学习蓝图框架的演讲，实际上非常深入地向我们解释了机器学习的底层架构，让我们更加深层次地认识到我们平时所用到的机器学习是如何实现的，各个计算方程、函数无不经过大量实验，最终得到可以被应用的结论。

哥伦比亚大学 John Wright：几何学及对称学在非凸优化问题中的应用

整理：智源社区 钱小鹅

John Wright 本次的演讲主题是《Geometry and Symmetry in (some!) nonconvex problems》(几何学及对称学在非凸优化问题中的应用)。

John Wright，哥伦比亚大学电气工程系副教授。他于 2009 年 10 月获得伊利诺伊大学香槟分校 (University of Illinois at Urbana Champaign) 电气工程博士学位，并于 2009–2011 年在微软研究院工作。他的研究领域是高维数据分析。最近，John Wright 的研究集中在开发从不完整和损坏的观测中稳健地恢复结构化信号表示的算法，并将其应用于成像和视觉的实际问题。他的工作获得了许多奖项和荣誉，包括 2009 年因其在人脸识别方面的工作而获得的伊利诺伊州莱梅尔森创新奖、2009 年 UIUC 马丁研究生优秀研究奖、2008–2010 年微软研究奖学金以及 2012 年柯尔特最佳论文奖。

在研究方面，John Wright 正在开发高维数据稳健分析工具，并将其应用于视觉数据分析问题，如图像和视频压缩、人脸和对象识别。其工作强调寻找即使在数据不可靠 (噪声或损坏) 的情况下也能表现良好的方法，并且这些方法带有正确性的证明。

本次讲座，John Wright 为我们分享了从卷积中恢复信号的反卷积问题。盲反卷积应用非常广泛，包括神经科学、显微镜技术、天文学、信号处理等，他在分享中提到，利用基于非凸优化的方法，在一定条件下，可以将目标短信号和稀疏信号恢复到该模型固有的符号移位对称性。这种对称性在形成反卷积的优化过程中起着核心作用。

图 1: John Wright

一、盲反卷积及非凸优化

盲信号处理 (BsP) 是目前信号处理中最热门的新兴技术之一，它具有稳定的理论基础和许多方面的应用潜力。Bss 的目标是在没有任何或很少关于源信号和混合知识的前提下，从一组混合 (观测) 信号中恢复原始的信号。在考虑时间延时的情况下，观测到的信号应该是源信号和通道的卷积，对卷积混叠信号进行盲分离通常称为盲反卷积。

为什么将其称为盲反卷积呢？我们不妨从它的数学定义上入手。不妨设 $y = a_0 * x_0$，其中 a_0 为短信号，x_0 为较长的稀疏信号，随着计算机视觉的发展，我们发现在图像去模糊中出现了一个非常相似的结构，其中 y 为模糊图像，a_0 为模糊核，x_0 为目标清晰图像，由于使得目标更加模糊，因此我们将其取名为盲反卷积。不难看出，如果我们已知 y 来计算 a_0 和 x_0，那么该问题将会有多解出现，因此，在计算之前，通常需要添加一些约束条件来控制解的唯一性亦或其他的性质，从而使得得到的数值解更具有物理意义。

John Wright 本次分享的约束条件主要为：a_0 的稀疏性条件以及 x_0 简短性条件，称之为 Short-and-Sparse-Deconvolution (SaS)。SaS 模型出现在许多应用中，一类应用涉及到在数据集中寻找基础的模体（在有重复数据集中寻找到一组构建该数据集的基础集合），这个模体问题一般会出现在脑神经科学研究中的细胞外棘突分类和钙成像，其中观察到的信号显示重复的短神经元兴奋模式，该兴奋模式关于时间或空间具有稀疏性。类似地，在纳米材料研究中产生的电子显微镜图像常常显示重复的模体。SaS 反卷积的另一个重要应用是图像去模糊。通常，模糊内核相对于图像大小（短）较小。在自然图像去模糊中，通常假设目标图像具有相对较少的锐边，因此具有稀疏导数。在科学图像去模糊中，例如在天文学和地球物理学] 中，目标图像通常是稀疏的，无论是在空间域还是小波域，这又导致了 SaS 模型的变体。SaS 反卷积问题的变体也出现在工程的许多其他领域。例如通信中的盲均衡，声音工程中的去冗余和图像超分辨率。

所有这些应用都导致了稀疏盲反卷积问题的推进和研究。稀疏盲反卷积的主要算法方法涉及非凸优化。反卷积的非凸公式可以通过几种概率形式（ML/MAP、VB 等）导出，也可以简单地从启发式中导出。例如，在图像去模糊中，内核 a 可以建模为驻留在单纯形上。这些单独从建模来看是很自然的，但在优化方面存在问题：单纯形上反卷积的自然公式允许全局最小值（对应于尖头卷积核 $a=\delta$），它们没有提供关于基本事实的信息。解决这个问题的实际方法包括利用额外的数据优先级或通过边缘恢复或多尺度优化进行初始化，以避免不重要的尖头全局最小值。

相比之下，出于对 MAP 和 VB 方法的仔细比较，[1,2] 建议用 Unit Frobenius norm 来代替 a 的约束，也就是说，考虑约束在高维球体上。这个选择可能更适合某些科学应用，比如显微镜，在这些应用中，内核 a 可以有负数。对于图像去模糊，可以假设 a 是非负的，并且从建模的角度来看，球体约束似乎不太自然。

John Wright 首先为我们分享的即为球面约束稀疏盲反卷积的几何性质，其目标是了解基于非凸优化的简单算法何时能够准确地恢复卷积核 a 和稀疏信号 x。这一目标是由上述应用（尤其是显微镜数据分析）驱动的，在这些应用中，信号 x 存在着强烈的物理稀疏性，且求解得到的数值解具有很好的物理意义。

这些应用激发了大量关于 SaS 问题变体的算法工作。相比之下，能够解释算法何时以及为什么成功的理论相对较少。John Wright 在这些方面做了很多工作，假设 a 是短核，x 是稀疏随机支持的情况下进行算法展开，通过对某些（理想化）案例的理论分析和大量的数值实验证明，在满足这些假设的情况下，所提出的算法能够正确地恢复一个，这些结果源于球面约束稀疏盲反卷积的一个显著的几何性质：尽管问题仍然是非凸的，但每个局部极小值 a 非常接近于基真核 a_0 的有符号移位截断。这一观察结果为球面约束如何促进稀疏盲反卷积提供了一个几何解释。

John Wright 提到，本次分享的基于非凸优化的算法，核心是在球体上最小化目标函数 φ，使用的优化方法为 bilinear lasso。John Wright 将这个过程抽象为数学中的非线性优化问题，不妨假设 $\varphi(a)$ 为目标函数，那么如

果使用 bilinear lasso 方法进行优化，那么有如下表达式:

Bilinear Lasso. Our starting point is the (natural) formulation

$$\min_{\boldsymbol{a},\boldsymbol{x}} \underbrace{\tfrac{1}{2}\|\boldsymbol{a}*\boldsymbol{x}-\boldsymbol{y}\|_2^2}_{\text{Data Fidelity}} + \lambda \underbrace{\|\boldsymbol{x}\|_1}_{\text{Sparsity}} \quad \text{s.t.} \quad \|\boldsymbol{a}\|_2 = 1. \tag{2.1}$$

We term this optimization problem the *Bilinear Lasso*, for its resemblance to the Lasso estimator in statistics. Indeed, letting

$$\varphi_{\text{lasso}}(\boldsymbol{a}) \equiv \min_{\boldsymbol{x}} \left\{ \tfrac{1}{2}\|\boldsymbol{a}*\boldsymbol{x}-\boldsymbol{y}\|_2^2 + \lambda \|\boldsymbol{x}\|_1 \right\} \tag{2.2}$$

denote the optimal Lasso cost, we see that (2.1) simply optimizes φ_{lasso} with respect to $\boldsymbol{a}$:

$$\min_{\boldsymbol{a}} \varphi_{\text{lasso}}(\boldsymbol{a}) \quad \text{s.t.} \quad \|\boldsymbol{a}\|_2 = 1. \tag{2.3}$$

图 2: 数学模型表达

在图 2 中的 (2.1)–(2.3) 中，约束 a 具有 l2 范数。这个约束打破了 a 和 x 之间的尺度模糊性。此外，约束流形的选择对计算有着惊人的强烈影响: 如果 a 被约束到单纯形，问题允许全局最小值。相反，球约束公式的局部极小值通常对应于基本真实值 a_0 的移位 (或移位截断) 。

bilinear lasso 方法优化目标函数已广泛应用于图像去模糊，在研究的过程中，学术界对稀疏反卷积的几何结构逐渐有了较为全面和深刻的见解，特别是对 A 的各种约束对伪局部极小值存在与否的影响。在图像去模糊中，通常使用的单纯形约束 ($a \geqslant 0$ 和 $\| a \|_1 = 1$) 由问题的物理结构自然产生。令人惊讶的是，单纯形约束的反卷积允许极小的全局极小值，在这个极小值处恢复的核是一个尖峰，而不是目标模糊核。

随后，科研人员将 l2 正则化应用于 a，并观察到这种替代约束给出了更可靠的算法，以及球面上简化目标 φ 的几何性质，证明了在 x_0 有一个非零项的稀释极限下，φ 的所有严格局部极小值都接近 a_0 的符号位移截断。通过在球面上采用不同的目标函数 (基于 l4 最大化)，科研人员证明了在球体的某一区域上，每个局部极小值都接近于 a_0 的截断有符号位移，即 $s_l[a_0]$ 对窗口。John Wright 的核心优化问题与此非常相似，然而，在更简单的移位非相干假设下，John Wright 提出的算法得到了 a_0 和相对稠密 x_0 的更精确数值解。

John Wright 为我们展示了他及其团队在该领域的研究成果:

1) 单移位几何

为了直观的了解 φ(a) 的性质，我们首先将图 2 中所抽象出的目标函数形象化的在 a_0 真实值附近叠加一个单移位。如图 3，即为 φ(a) 的函数图，其中:

- 目标函数在 a_0 上是强凸的;
- 在非常接近 a_0 的单移动区域 $s_l[a_0]$ 处有一个局部极小值;

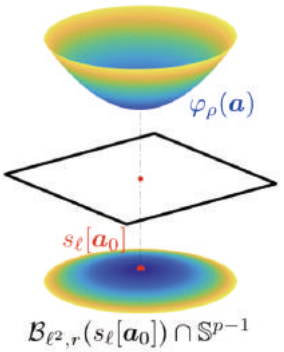


Figure 3: Geometry of φ_ρ near a shift of a_0. Bottom: a portion of the sphere $\mathbb{S}^{p-1}$, colored according to φ_ρ. Top: φ_ρ visualized as height. φ_ρ is strongly convex in this region, and it has a minimizer very close to $s_\ell[a_0]$.

图 3: φ(a) 的目标函数单移位示意图

2) 双移位几何

接下来，我们在 $s_{l_1}[a_0]$ 和 $s_{l_2}[a_0]$ 两个不同位移的线性跨距附近可视化目标函数 φ(a)。更精确地说，我们在球面 Sp_1 和线性子空间的交点附近绘制 φ(a) 及其线性子空间。

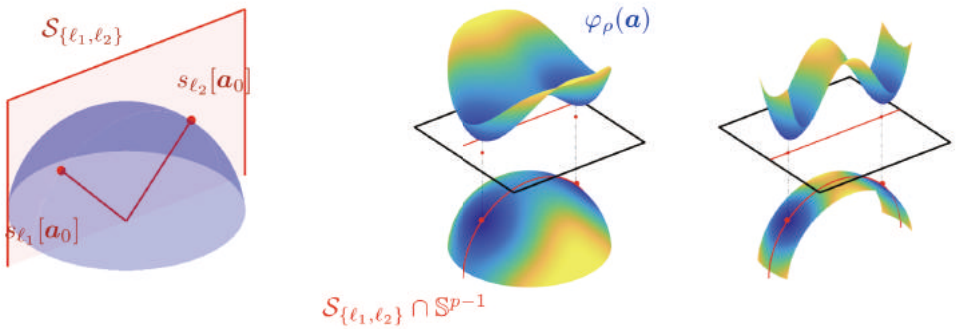


Figure 4: Geometry of φ_ρ near the span $\mathcal{S}_{\{\ell_1,\ell_2\}}$ of two shifts of a_0. Left: each pair of shifts $s_{\ell_1}[\boldsymbol{a}_0]$, $s_{\ell_2}[\boldsymbol{a}_0]$ defines a linear subspace $\mathcal{S}_{\{\ell_1,\ell_2\}}$ of $\mathbb{R}^p$. Center/right: every local minimum of φ_ρ near $\mathcal{S}_{\{\ell_1,\ell_2\}}$ (red line) is close to either $s_{\ell_1}[\boldsymbol{a}_0]$ or $s_{\ell_2}[\boldsymbol{a}_0]$; there is a negative curvature in the middle of $s_{\ell_1}[\boldsymbol{a}_0]$, $s_{\ell_2}[\boldsymbol{a}_0]$, and φ_ρ is convex in direction away from $\mathcal{S}_{\ell_1,\ell_2}$.

图 4: φ(a) 的目标函数双移位示意图

同样，我们观察到:

- 在每个移位 $s_l[a_0]$ 附近有一个局部极小值;
- 这些是 $s_{\{l_1,\ l_2\}}$ 附近唯一的局部极小。特别地，目标函数 φ 在任何 $a_1 s_{l1}\left[a_0\right]+a_2 s_{l2}\left[a_0\right]$ 的迭加处沿 $s_{\{l_1,\ l_2\}}$ 呈现负曲率，其权重 a_1 和 a_2 是平衡的，即 $|a_1|\approx|a_2|$;
- 函数 φ 在远离子空间 $s_{l_1,\ l_2}$ 的方向上显示正曲率;

3) 多移位几何

最后，我们在多移位几何上做目标函数 φ 的构想，如下：

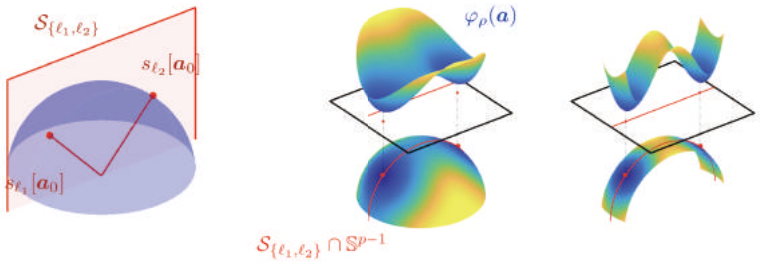


Figure 4: Geometry of φ_ρ near the span $\mathcal{S}_{\{\ell_1,\ell_2\}}$ of two shifts of $\boldsymbol{a}_0$. Left: each pair of shifts $s_{\ell_1}[\boldsymbol{a}_0]$, $s_{\ell_2}[\boldsymbol{a}_0]$ defines a linear subspace $\mathcal{S}_{\{\ell_1,\ell_2\}}$ of $\mathbb{R}^p$. Center/right: every local minimum of φ_ρ near $\mathcal{S}_{\{\ell_1,\ell_2\}}$ (red line) is close to either $s_{\ell_1}[\boldsymbol{a}_0]$ or $s_{\ell_2}[\boldsymbol{a}_0]$; there is a negative curvature in the middle of $s_{\ell_1}[\boldsymbol{a}_0]$, $s_{\ell_2}[\boldsymbol{a}_0]$, and φ_ρ is convex in direction away from $\mathcal{S}_{\ell_1,\ell_2}$.

图 5: φ(a) 的目标函数多移位示意图

同样，在每个有符号移位附近有一个局部极小。在位移的大致平衡叠加下，目标函数呈现负曲率。因此，唯一的局部极小值接近有符号位移。

4) 子空间并集几何

结果表明，这些性质在每一个子空间上都得到，这些子空间跨越了几个移位 a_0。实际上，对于每个子集定义线性子空间均满足上述的结果。

如图 6，假设子空间 τ 是由集合 τ 索引的移位 $s_i[a_0]$ 的线性跨度构成，那么由几何理论表明，在概率很高的情况下，φ(a) 函数在 τ 不太大的任何 S_τ 附近都没有虚假的局部极小值，例如 $|\tau| \leq 4\theta p_0$。将所有这些子空间组合成一个几何对象，定义子空间的并集：

$$\sum_{4\theta p_0} = \bigcup_{|\tau| \leq 4\theta p_0} S_\tau$$

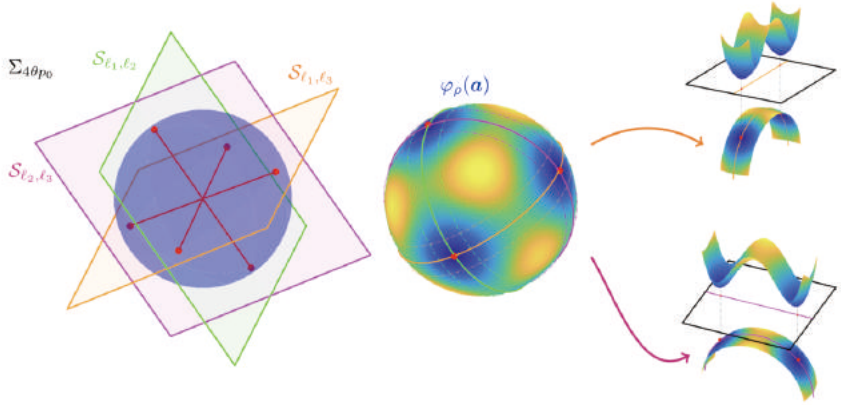


Figure 6: Geometry of φ_ρ over the union of subspaces $\Sigma_{4\theta p_0}$. Left: schematic representation of the union of subspaces $\Sigma_{4\theta p_0}$. For each set τ of at most $4\theta p_0$ shifts, we have a subspace $\mathcal{S}_\tau$. Right: φ_ρ has good geometry near this union of subspaces.

图 6: φ(a) 的目标函数子空间并集几何示意图

图 (6) 给出了该组的示意图。我们声称:

- 在$\Sigma_{4\theta p_0}$附近，所有局部极小值都在符号位移附近。
- φ 的值在远离$\Sigma_{4\theta p_0}$的任何方向上增长。

John Wright 根据上述的四个几何结果，最终解释到：在两个关键假设下，上述观察结果中可以看到两个通用的结果:

第一，稀疏率 θ 足够小（相对于 p_0 的移位相干 μ);
第二，信号长度 n 足够大;

二、两步算法及实验结果

受 φ 的每个局部最小值都是地面真实值 a_0 的有符号移位截断的几何性质的启发，John Wright 提出了一个可靠恢复真实值 a_0 的两阶段算法。在第一阶段，算法恢复一些有符号移位截断的真值，下一阶段从该部分恢复中推断出真值。具体算法如下:

Algorithm 1 Nonconvex Sparse Blind Deconvolution

Ensure: Observation data $\boldsymbol{y}$, regularization parameter λ_0 and $\lambda_{\min}$, continuation parameter $\beta > 1$

Solve $\boldsymbol{a}^{(0)} = \arg\min \varphi_{\lambda_0}(\boldsymbol{a})$ on $\mathbb{S}^{k-1}$ with random initialization

Set $\lambda_1 = \lambda_0$, zero pad $\boldsymbol{a}^{(0)}$ to $\boldsymbol{a}^{(1)}$ and $\boldsymbol{a}^{(1)} \in \mathbb{S}^{k'-1}$ $(k' > k)$.
while $\lambda_k > \lambda_{min}$ **do**
    Solve $\boldsymbol{a}^{(k+1)} = \arg\min \varphi_{\lambda_k}(\boldsymbol{a})$ on $\mathbb{S}^{k'-1}$ with initialization $\boldsymbol{a}^{(k)}$.
    $\lambda_{k+1} = \lambda_k/\beta$
end while

图 7：非凸稀疏盲反卷积算法

最后，John Wright 为我们展示了算法在合成数据和真实数据上的性能。

- 无噪声数据:

通过循环生成 m=256×256 的无噪声观测信号 an ∈ Sk−1 xn 2 n=1 n=1 大小为 k 卷积核与具有伯努利分布的随机激活信号之间的卷积。

我们在图 8(a) 的左边绘制了不同内核大小 k 和稀疏度θ的内核恢复误差。图上的每个点是 20 个独立测量值的平均值。该算法在蓝色区域表现出色，但在红色区域开始失败，在红色区域，要么内核大，要么底层激活信号密集。在典型的 STM 测量区域的下方是白色虚线，在该区域内，提出的算法获得了令人满意的性能。

- 噪声数据:

用 m 维随机激活映射对 k 维（k/m=0.14）的固定核进行卷积，并叠加高斯噪声。研究测试了该算法在不同稀疏度 θ 和噪声功率下的性能。结果如图 8(b) 所示：在满足稀疏性约束的情况下，该算法实现了信号恢复，并对噪声具有鲁棒性。

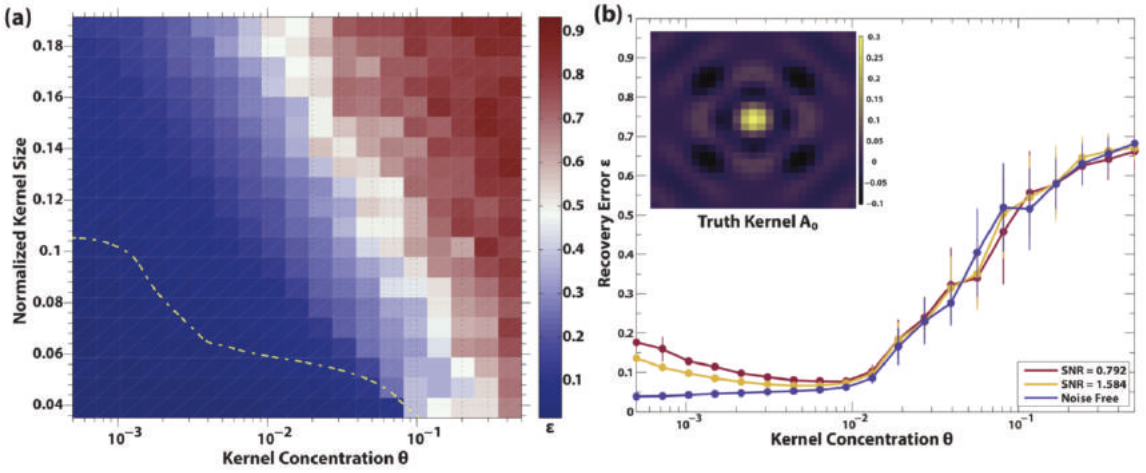


图 8: 噪声数据评价

• 显微镜数据分析

将该算法应用于从 NaFeCoAs 获得的实验显微镜数据。我们在图 9 中显示的结果表明，所提出的算法设法恢复缺陷傅里叶域中波纹的缺失细节，这些波纹编码了工作中电子的物理散射过程。

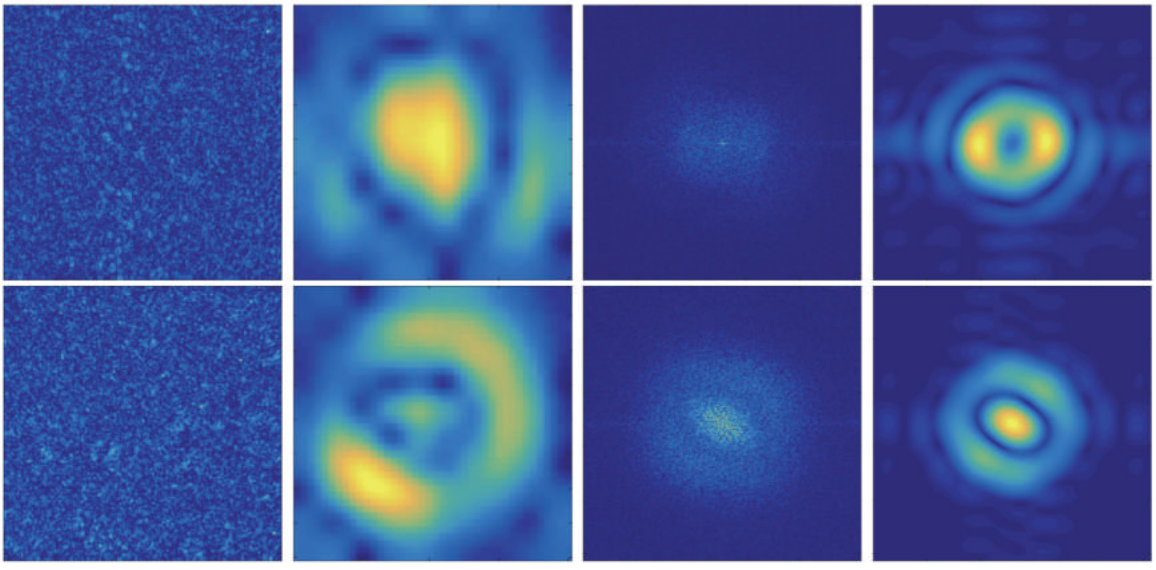


图 9:STM 数据分析

从左至右：显微图像，提取卷积核（缺陷模式），以及它们各自的傅立叶幅度图像。

• 图像去模糊

在图像去模糊数据集上测试该算法，通过求解来恢复卷积核。为了明确区分算法的不精确性和通用模糊核模型，对三类模糊图像进行了实验：（i）由锐化图像和模糊核卷积生成的合成模糊图像；（ii）在干净的合成模糊图像中加入高斯噪声产生的噪声模糊图像（信噪比 =100）；以及（iii）使用相机抖动拍摄的真实模糊图像。由于移位的模

糊性，我们考虑了所有可能的移位，对恢复的模糊核的精度进行了评估。核恢复误差累积分布如图 10 所示。

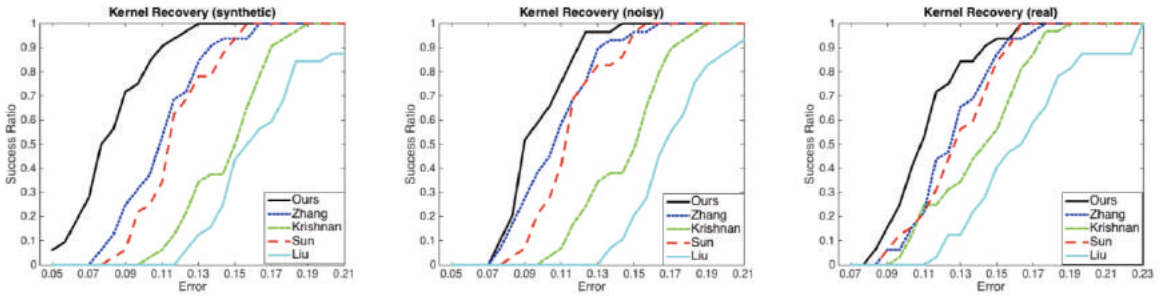


图 10: 图像去模糊数据分析

从合成（左）、有噪（中）和实（右）模糊图像中恢复的模糊核误差的累积分布

结果显示，该算法对这三类图像都有较好的卷积核恢复效果，但对去模糊图像的改善不明显，尤其是对真实图像。这可能是由于 (i) 该数据集中的卷积核在图像上不是严格一致的，(ii) 非盲反卷积算法利用自然图像梯度的重尾分布，对恢复的卷积核的精度不太敏感。

三、结语

本此讲座，John Wright 主要为我们分享的内容为： 当核函数为单位 Frobenius 范数时 SBD 非凸优化问题的全局几何性质。在这种情况下，John Wright 发现所有的局部极小值都是良性的，在某种意义上，它们接近于基真值的符号移位截断。基于这一认识，John Wright 提出了一个两阶段的算法，利用隐藏在局部极小中的信息来恢复真实解。

这个问题揭示了在用几何方法分析 SBD 问题时所面临的挑战。对于具有更强对称性的问题，类似的方法产生了对函数几何和恢复保证的全局理解。John Wright 指出，SBD 中的弱对称性将对这个问题遇到的困难做出重要贡献。

最后，John Wright 为我们展示了诸多实验结果，其对局部极小值的刻画贯穿于卷积字典学习问题，并且通过对所提出的算法稍加修改，也可以有效地解决卷积字典学习问题。然而，该部分的理论证明尚未完整，他提到，大家有兴趣的话可以继续深入研究，希望通过完整的证明过程了解可以有多少种内核，或者哪些类型的内核是可恢复的，这可能是字典学习问题中常见的假设。

在科学测量中，通常我们还会遇到的另外两个问题是分辨率极限和测量误差，这启发我们考虑 (i) 是否有可能将盲反卷积和超分辨率过程结合在一起；(ii) 是否可以提出一种鲁棒的盲反卷积算法来自动排除噪声条目。

参考文献

[1] David Wipf and Haichao Zhang. Revisiting bayesian blind deconvolution. arXiv preprint: 1305.2362, 2013.

[2] Haichao Zhang, David Wipf, and Yanning Zhang. Multi-image blind deblurring using a coupled adaptive sparse prior. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), January 2013.

北京大学教授林宙辰：基于学习的优化算法

整理：智源社区 沈磊贤

在第二届北京智源大会“机器学习”专题论坛中，北京大学信息科学技术学院林宙辰教授做了题为《Learning based Optimization》的报告。林宙辰是 IAPR/IEEE Fellow，中国图象图形学学会机器视觉专委会主任，获国家自然科学杰出青年基金资助，曾在 2015 年 ImageNet 大规模视觉识别竞赛（ILSVRC）场景分类项目上获得冠军，他的主要研究方向为机器学习、模式识别、计算机视觉、图像处理、数值优化等。

在报告中，林宙辰简要概述了基于学习的优化算法工作原理，以及在图像去噪、非盲反卷积等方向上的应用；他认为在传统优化算法的基础上引入学习机制，算法的收敛速度可以得到显著提高。以下是智源社区编辑整理的林宙辰演讲内容要点。

以下是智源社区编辑整理的林宙辰演讲内容要点。

一、优化问题的复杂度

众所周知，在传统优化方法中，对于不同类型的问题，解决这些问题的复杂性存在下界，尽管某些场景中下界尚不准确，但是无论如何，问题复杂性的下界一定是存在的。例如，对于广泛应用在不同类型问题中的确定性梯度下降和随机梯度下降（凸或非凸），它们的下界都显示在下表的底部。

- Optimization problems all have complexity lower bounds if solved in traditional ways (some are still unknown)

Methods	Non-strongly Convex		Strongly Convex	
	Non-Acc	Accelerated	Non-Acc	Accelerated
(1a)-(1b) [87]	$O\left(\frac{L}{\varepsilon}\right)$	$O\left(\sqrt{\frac{L}{\varepsilon}}\right)$	$O\left(\frac{L}{\mu}\log\frac{1}{\varepsilon}\right)$	$O\left(\sqrt{\frac{L}{\mu}}\log\frac{1}{\varepsilon}\right)$
(2a)-(2c) [87]	$O\left(\frac{L}{\varepsilon}\right)$	$O\left(\sqrt{\frac{L}{\varepsilon}}\right)$	$O\left(\frac{L}{\mu}\log\frac{1}{\varepsilon}\right)$	$O\left(\sqrt{\frac{L}{\mu}}\log\frac{1}{\varepsilon}\right)$
(3a)-(3d) [4]	$O\left(\frac{L}{\varepsilon}\right)$	$O\left(\sqrt{\frac{L}{\varepsilon}}\right)$	not given	not given
GeoD [9]	not given	not given	$O\left(\frac{L}{\mu}\log\frac{1}{\varepsilon}\right)$	$O\left(\sqrt{\frac{L}{\mu}}\log\frac{1}{\varepsilon}\right)$
PEP [11]	$O\left(\frac{L}{\varepsilon}\right)$	$O\left(\sqrt{\frac{L}{\varepsilon}}\right)$	not given	not given
Lower Bound	$O\left(\sqrt{\frac{L}{\varepsilon}}\right)$		$O\left(\sqrt{\frac{L}{\mu}}\log\frac{1}{\varepsilon}\right)$	

Complexity comparisons between different accelerated deterministic gradient methods and their non-accelerated counterparts.

Method	Individually Convex	Individually Nonconvex
SGD	$O\left(\frac{\sigma^2}{\mu\varepsilon}\right)$ [101]	$O\left(\frac{\sigma^2}{\mu\varepsilon}\right)$ [101]
VR	$\tilde{O}\left(n+\frac{L}{\mu}\right)$ [18]–[20], [24]	$\tilde{O}\left(n+\frac{L^2}{\mu^2}\right)$ [96], [97]
VR+Momentum	$\bar{O}\left(n+\sqrt{\frac{nL}{\mu}}\right)$ [26], [29], [31], [90], [100]	$\bar{O}\left(n+n^{3/4}\sqrt{\frac{L}{\mu}}\right)$ [90], [93], [99]
Lower Bound	$\bar{O}\left(n+\sqrt{\frac{nL}{\mu}}\right)$ [34]	$\bar{O}\left(n+n^{3/4}\sqrt{\frac{L}{\mu}}\right)$ [102]

Complexity comparisons between different variation reduction (VR) based accelerated stochastic gradient methods and the plain SGD.

图 1：优化问题的复杂度及其下界

表中可以看出复杂度的下界通常依赖于一些全局参数，例如目标函数梯度的 Lipschitz 系数 L、目标函数的强凸性（strong convexity）参数等。但很显然，仅凭这类全局参数无法从细节处展现问题的本质，无法提供局部特性的具体信息，因此，如果仅考虑问题的全局性质就无法使问题快速地收敛。

林宙辰总结了影响优化算法收敛性的几个因素。首先是优化问题本身的结构，约束还是非约束问题、凸问题还是非凸问题，这些差别都会导致最终的收敛性有很大的差异； 其次是优化算法中的参数选择，即使是相同类型

的算法，选择不同的参数也会带来不同的收敛性。例如，对相同的加速梯度下降算法，如下图所示，参数β的选择是否合适，会导致收敛速度存在$O(1/k^2)$和$O(1/k)$的差别。

$$\mathbf{y}_k = \mathbf{x}_k + \beta_k(\mathbf{x}_k - \mathbf{x}_{k-1}),$$
$$\mathbf{x}_{k+1} = \mathbf{y}_k - \frac{1}{L}\nabla f(\mathbf{y}_k). \qquad O(1/k) \text{ vs. } O(1/k^2)$$

图 2：加速梯度下降算法及收敛性对比

最后一个影响算法收敛性的因素是数据的特性。对于下图所示的弹性网问题（Elastic Net problem），如果 A 没有特殊性质，并且用交替方向乘子法（Alternating Direction of Method of Multipliers，ADMM）求解，则其收敛速度仅为$O(1/k)$，是次线性（sublinear）的。但如果 A 具有受限等距性质（Restricted Isometric Property），如下图所示，则可以证明收敛速度是线性的。

$$\min_{\mathbf{x}} \|\mathbf{x}\|_1 + \frac{1}{2\alpha}\|\mathbf{x}\|_2, \text{ s.t. } \mathbf{A}\mathbf{x} = \mathbf{b}$$
(Restricted Isometric Property) There exists $\delta_k \in [0, 1)$ such that
$$(1 - \delta_k)\|\mathbf{x}\|^2 \leq \|\mathbf{A}\mathbf{x}\|^2 \leq (1 + \delta_k)\|\mathbf{x}\|^2 \qquad \text{sublinear vs. linear}$$

图 3：弹性网问题收敛速度对比

在上述的三个因素中，由于所研究的问题是具体已知的，所以无法更改问题的结构，但是可以从另外两个因素入手，通过更改参数、考虑更多细节或数据特性，机器学习可以很好地改善优化机制求解问题的过程。这也是基于学习的优化方法的研究动机。

二、基于学习的优化算法：概述

林宙辰简要概述了基于学习的优化的工作原理。他认为，如果优化算法的某些部分与数据相关，那么它就可以称为基于学习的优化算法。基于学习的优化算法不同于自适应算法，自适应学习仍然需要在使用时自己确定一些参数，而基于学习的优化方法通常必须向算法提供数据，以更好地训练算法。

在基于学习的优化算法中存在几种范式，如下图所示。第 0 类范式直接学习优化算法。这种希望机器学习可以做任何事情的想法很明显是不可能的。因此这种范式下的工作很有限，但也确实存在一些现有研究，如下图的下方所示，通过强化学习或 LSTM 学习梯度下降，但上述工作中所用到的π函数和g_k函数非常复杂，很难对其进行分析，所以没有理论上的保证。只在一些非常简单的任务（例如回归问题）上仅获得了一些经验性的成功。

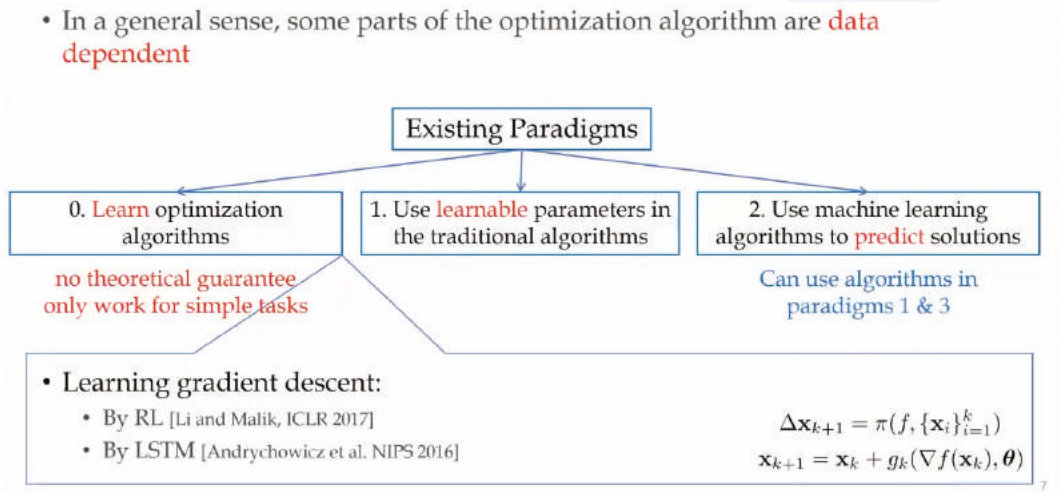


图 4：基于学习的优化算法的三种范式

第 1 类研究范式是在传统算法中使用基于学习的优化方法。实际上这种研究范式考虑了优化的基本结构，仅调整了一些参数，因此仍然可以确保收敛。第 2 类研究范式是使用机器学习算法来预测解。如果预测得到的结果很好，则接受，否则拒绝。这种思路仍在传统的优化框架中，但加了些纠正的措施，因此仍然可以保证收敛。这里用到的预测算法可以来自第 0 和第 1 范式中的方法。(PPT 中有 typo)

接下来，林宙辰对后两种研究范式做了详细阐述，并介绍了在这两个方向的研究工作。

三、基于学习的优化算法：第 1 范式

首先是第 1 范式： 在传统算法中使用可学习的参数。如下图所示，它包括三个步骤，首先将传统算法的迭代展开为 DNN 或更通用的计算图。每个 cell 上的计算不仅限于激活函数，附近 cell 之间的关系也可以像 DNN 一样不只是线性组合； 接着，在传统算法中引入可学习的参数，这意味着需要允许一些参数根据数据进行更改。最后一步是向算法提供一些数据进行训练，以便找到合适的参数。

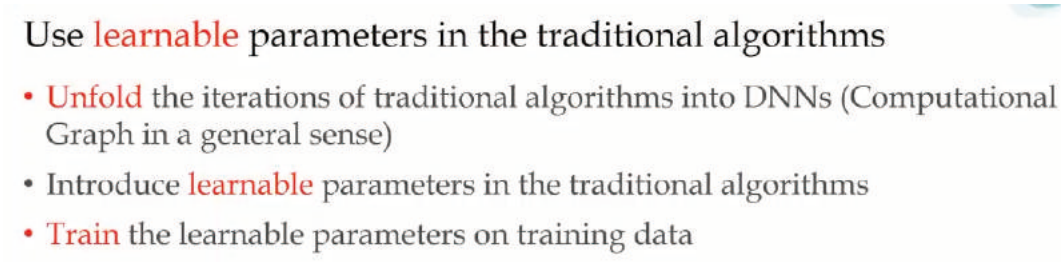


图 5：第 1 类范式的研究思路

林宙辰介绍了这方面的相关研究工作。如下图所示，将 RNN 用于 LASSO 问题 (Sprechmann et al. TPAMI 2015)； 将 LSTM 用于稀疏编码问题 (Zhou et al. AAAI 2018)； 使用一些受优化启发 (optimization inspired networks) 的网络来解决图像恢复问题 (Gregor & LeCun, ICML 2010; Zhang et al. CVPR 2018; Yang et al. NIPS 2016) 等。这类问题基本上都是稀疏表示的问题。

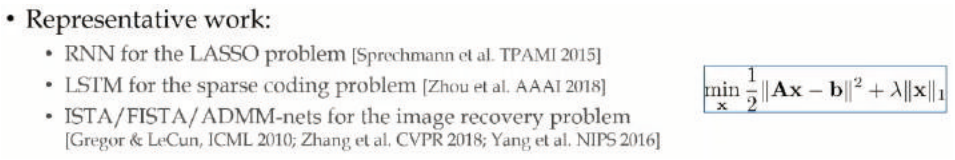


图 6：代表性工作

但林宙辰认为，现有的工作大多是启发式的。而对于分析基于学习的优化方法的收敛特性，这类研究非常有限，已有的有 Chen 等人在 2018 年的工作，但是该证明仅适用于 LASSO 问题，不能推广到其他问题，并且研究中考虑的大多数是无约束的问题。

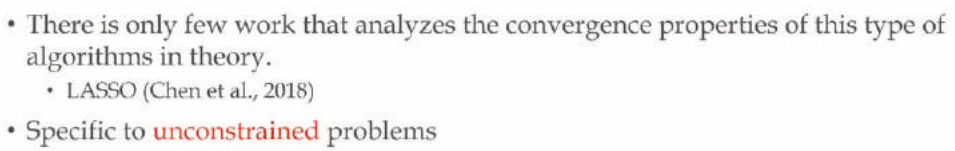


图 7：Chen 等人在 Lasso 问题上的工作

基于以上分析，林宙辰介绍了他在该方向的研究，如下图所示，考虑 $f(\bullet)$ 和 $g(\bullet)$ 都是凸函数的优化问题，且变量 Z 和 E 是线性耦合的。

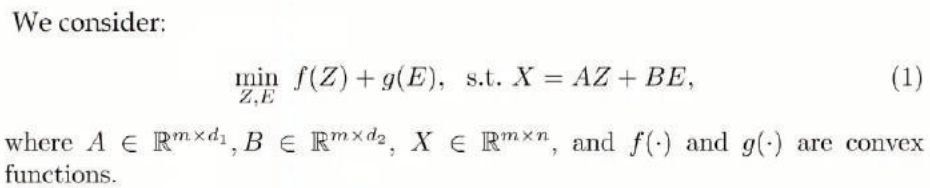


图 8：林宙辰在第 1 范式中的研究

使用传统的线性化 ADMM，可以通过如下图所示的五个迭代步骤中解决此问题。（由于时间限制，未对线性化 ADMM 进行详细介绍）。迭代步骤中有一个特殊操作 prox，称为邻近算子（proximal operator），具体定义见图右侧。给定输入 x，称 $prox_{\alpha f}(x)$ 为 $f(\bullet)$ 函数在 x 点的邻近算子。

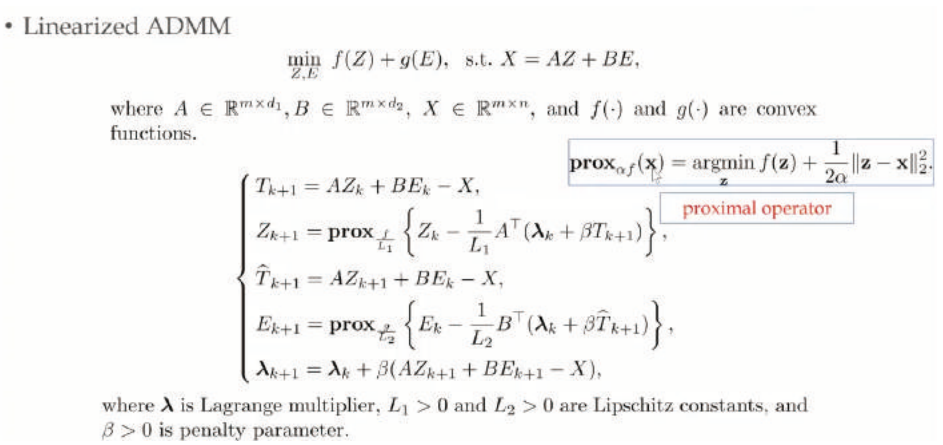


图 9：线性化 ADMM

接着，林宙辰介绍了将上述的传统方法变为 learnable 方法的思路。流程如下图所示。假设有优化问题 $\min_z f(z)+\frac{1}{2}\|Az-b\|_2^2$，首先对平方部分进行线性化，并得到迭代式:

$$z_k = prox_{tf}(z_{k-1} - tA(Az_{k-1} - b))$$

上式为函数 $f(\cdot)$ 的临近算子，而 $tA(Az_{k-1}-b)$ 是平方部分的线性化结果。容易证明临近算子是单调递增的，即输入增加，输出也将增加。而 DNN 中的激活函数通常是单调递增，至少单调不减的，因此，上述临近算子可以用来充当 DNN 中的激活函数。

将上式中的临近算子替换成任意单调不减的激活函数 ς，将固定的 tA^T 替换成可学习的矩阵 W_{k-1}，得到了更加宽泛的结果，如下所示:

$$z_k = \varsigma(z_{k-1} - W_{k-1}^T(Az_{k-1} - b))$$

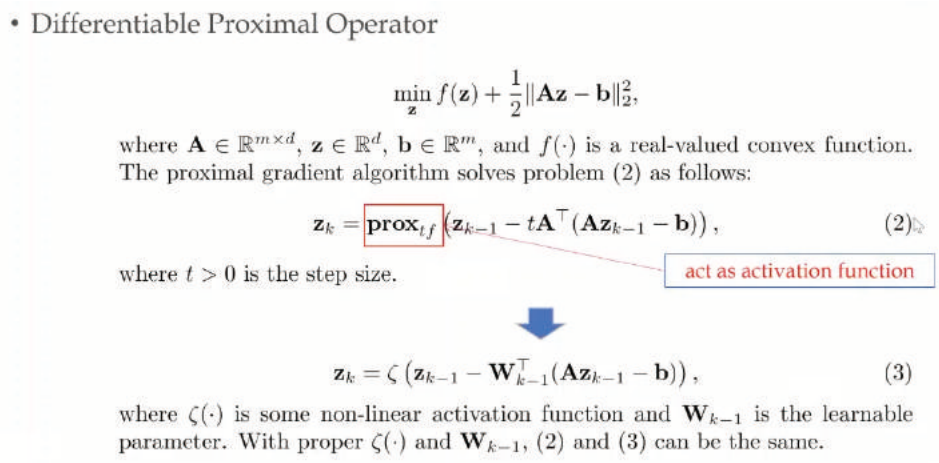


图 10：可微的临近算子

利用以上思路可以将传统的线性化 ADMM 更改为可学习的版本，两者的对比如下图所示，用参数化激活函数代替临近算子（实际上可以进一步放宽到更通用的非凸函数），将 A 替换为可学习的矩阵，并用逐元素乘法替换矩阵上的均匀缩放。总之，可学习的版本引入了更多灵活的变量，算法可以更好地适应给定的数据。

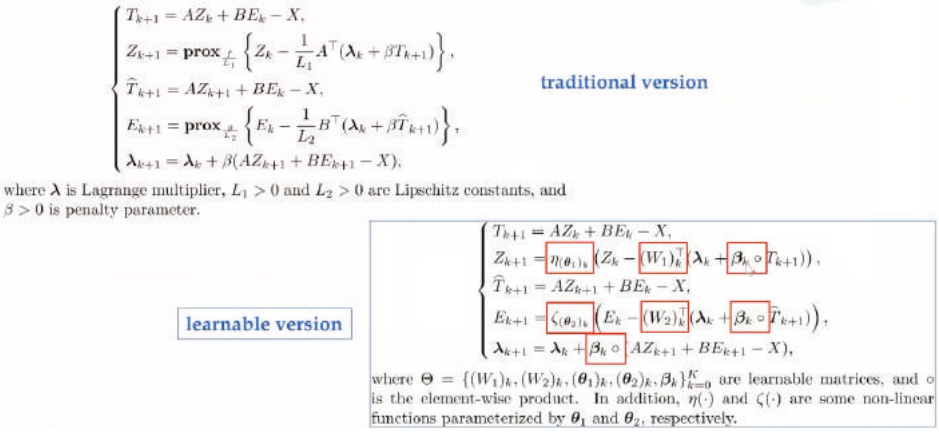
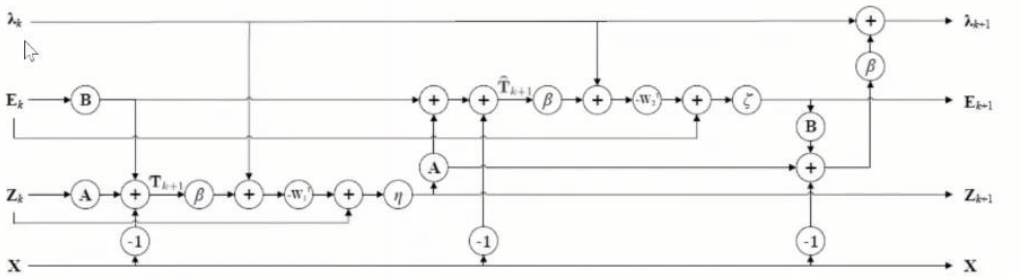


图 11：可学习的线性化 ADMM

下图给出了迭代过程的计算图。在输入端可以随机生成一些输入，或者将实际问题的数据作为输入； 至于输出为 dual gap。由凸分析可知 dual gap 总是非负的。如果 dual gap 变为零，则获得最优解。



Training Strategy:

$$\min_{\Theta} f(Z_K) + g(E_K) - d^*(\boldsymbol{\lambda}_K), \tag{4}$$

where $d^*(\boldsymbol{\lambda}_K)$ is the dual function of (1) defined as

$$d^*(\boldsymbol{\lambda}_K) = \inf_{Z,E} f(Z) + g(E) + \langle \boldsymbol{\lambda}_K, AZ + BE - X \rangle .$$

图 12：迭代过程

接着林宙辰进一步分析了上述算法，指出该方法与传统算法相比确实具有优势。主要体现在三个方面，如下图所示。首先，基于学习的方法每多迭代一次，网络的输出值与真实解的距离将减小，并且最终将减小为零。这意味着即使该方法是基于学习的，最终也可以获得真实的解。这是一个很好的理论保证。其次，在某些条件下，算法的收敛速度可以提高到线性。此外，如果传统方法线性 ADMM 和新方法都迭代 k 次，那么基于学习的算法提供的解将会一直优于传统算法给出的解。

Theorem 1 and Theorem 2 **[Convergence and Monotonicity]** (informal).

$$\underbrace{\text{dist}\,(\boldsymbol{\omega}_k, \boldsymbol{\Omega}^*) \geq \text{dist}\,(\boldsymbol{\omega}_{k+1}, \boldsymbol{\Omega}^*) \to 0}, \text{ as } k \to \infty.$$

$$\boldsymbol{\omega}_k \to \boldsymbol{\omega}^* \in \boldsymbol{\Omega}^*$$

Theorem 3 **[Convergence Rate]** (informal).
If the original problem satisfies *Error Bound Condition*, then

$$\text{dist}(\boldsymbol{\omega}_{k+1}, \boldsymbol{\Omega}^*) < \gamma \ \text{dist}(\boldsymbol{\omega}_k, \boldsymbol{\Omega}^*), \quad \text{where } 0 < \gamma < 1.$$

Theorem 4 **[Faster Convergence]** (informal).

Define operators: $\boldsymbol{\omega}_{k+1} := \mathcal{T}_{\Theta_k}(\boldsymbol{\omega}_k)$ for D-LADMM; $\boldsymbol{\omega}_{k+1} := \mathcal{T}(\boldsymbol{\omega}_k)$ for LADMM.
For any $\boldsymbol{\omega}$,

$$\text{dist}(\mathcal{T}_{\Theta}(\boldsymbol{\omega}), \boldsymbol{\Omega}^*) \leq \text{dist}(\mathcal{T}(\boldsymbol{\omega}), \boldsymbol{\Omega}^*).$$

图 13：基于学习的 LADMM 算法的优势

下图为模拟结果。绿色、蓝色和红色曲线表示传统的 LADMM 算法，黑色曲线表示基于学习的优化算法。可以看到基于学习的优化算法使用少于 LADMM 10 倍的迭代次数达到了更低的目标函数值，将速度提高了十倍以上。

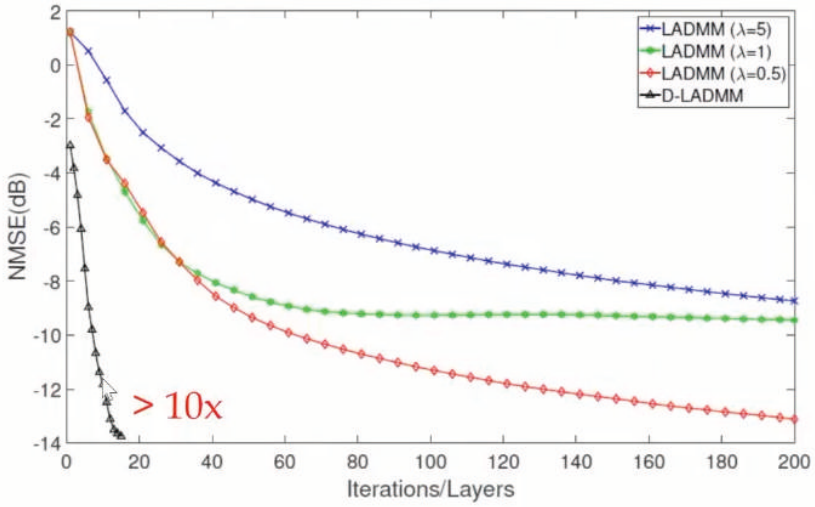


图 14：算法模拟结果

下图是对自然图像去噪的实验。可以看到，为获得相同的 PSNR，新方法仅用了 15 次迭代，这意味着将速度提高了大约 100 倍。从视觉比较上也可以看到基于学习的算法与传统算法之间的巨大差异。

• Natural Image Denoising

Table 2. PSNR comparison on 12 images with noise rate 10%. For LADMM, we examine its performance at a couple of different iterations. LADMM is comparable to D-LADMM only when it undergoes a large number of iterations.

PSNR	Images											
	Barb	Boat	France	Frog	Goldhill	Lena	Library	Mandrill	Mountain	Peppers	Washsat	Zelda
Baseline	15.4	15.3	14.5	15.6	15.4	15.4	14.2	15.6	14.4	15.1	15.1	15.2
LADMM (iter=15)	22.1	24.2	18.0	23.1	25.2	25.6	15.0	21.7	17.7	25.1	30.6	29.7
LADMM (iter=150)	27.9	29.8	21.6	26.5	30.4	31.3	17.8	24.3	20.5	30.0	34.5	35.7
LADMM (iter=1500)	29.9	31.1	22.2	26.9	31.8	33.2	18.0	25.1	20.7	32.8	36.2	37.8
D-LADMM (K=15)	29.5	31.3	21.9	25.9	32.5	35.1	18.8	24.5	19.3	34.3	35.6	38.9

~ 100x

(a) GND (b) Noisy image (PSNR=15.4) (c) D-LADMM (PSNR=35.1) (d) LADMM (PSNR=31.3)

图 15：自然图像去噪实验结果

四、基于学习的优化算法：范式 2

接着，林宙辰介绍了第二项工作，基于学习的优化方法中的第 2 类范式，即使用机器学习算法来预测解。主要包括以下步骤，首先预测解，然后，检查解的好坏，即存在一个监视条件，如果满足监视条件，则接此解； 否

则，将选择传统解。

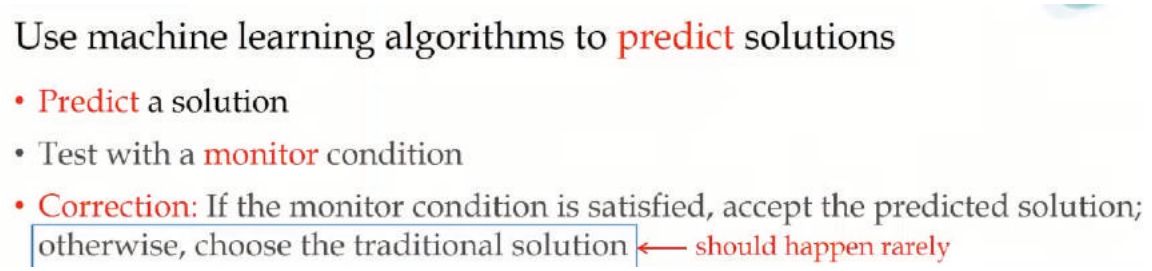


图 16：第 2 类范式研究思路

传统算法中已经有一些使用监视机制的工作，例如，对于非凸型 APG 问题，如下图所示，将临近算子 v_{k+1} 和 z_{k+1} 作比较，选择其中目标函数较小的方案。但是这类机制尚未在基于学习的优化方法中使用。

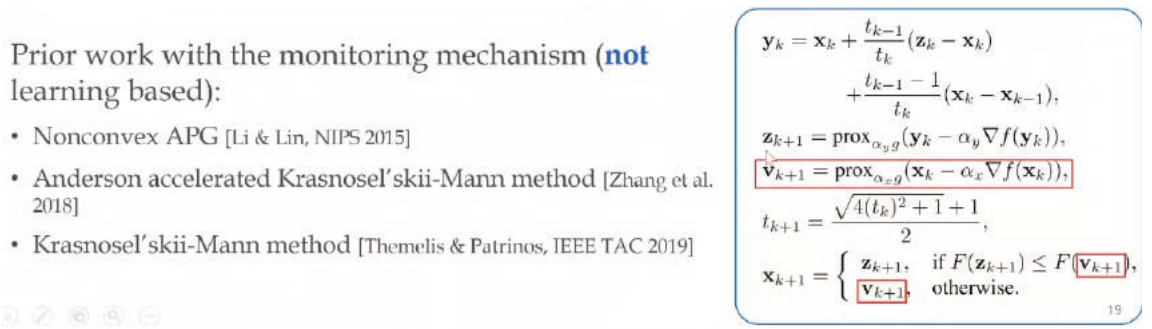


图 17：传统算法中的监视机制

林宙辰将基于学习的优化算法应用在逆问题的研究中。逆问题（inverse problems）研究的是如何在给定 y 和噪声 n 的情况下恢复真实数据 x。比如下面的照片为模糊的版本，即 $y+n$，为了将其恢复为清晰图像，即 x，可以制定一个抽象的目标函数 $f(\cdot)+g(\cdot)$，其中 $f(\cdot)$ 是数据保真度项；$g(\cdot)$ 是正则化，描述了 x 上的一些先验信息。

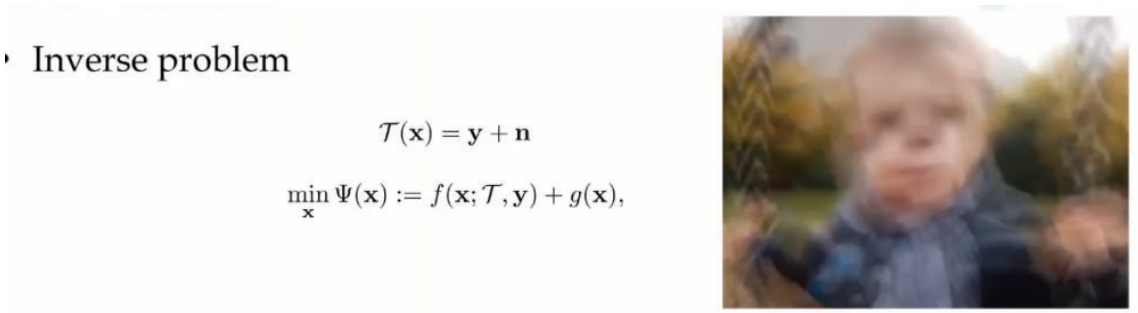


图 18：图像逆问题

传统的加速或不精确的近端梯度算法由 v^k 和 x 组成，如下图所示，v^k 可以加速或不加速，x 可以是精确的也可以是不精确的，因此它们之间将有四个组合。

(Accelerated/Inexact) proximal gradient algorithm:

$$\mathbf{v}^k = \begin{cases} \mathbf{x}^k, & \text{(A-1)} \\ \mathbf{x}^k + \beta^k(\mathbf{x}^k - \mathbf{x}^{k-1}), & \text{(A-2)} \end{cases}$$

$$\mathbf{x}^{k+1} \in \begin{cases} \mathrm{prox}_{\gamma^k g}\left(\mathbf{v}^k - \gamma^k \nabla f(\mathbf{v}^k)\right), & \text{(B-1)} \\ \mathrm{prox}^{\varepsilon_k}_{\gamma^k g}\left(\mathbf{v}^k - \gamma^k \nabla f\left(\mathbf{v}^k + \mathbf{e}^k\right)\right), & \text{(B-2)} \end{cases}$$

图 19：传统近端梯度算法

下图为近端梯度算法的结构。可将其分为前向更新和后向更新两个部分。其中，x^{k+1} 可以抽象地写作 $A_g \circ A_f(x^k)$，其中 A_g 和 A_f 为抽象算子，如果随机选择它们，显然不能保证算法收敛。因此，我们只将它们的输出结果作为优化算法预测的解。为了保证收敛，后续设置了纠正机制。

- Structure of the algorithm

Backward update

$$\mathbf{x}^{k+1} = \mathrm{prox}_{\gamma^k g}\left(\mathbf{x}^k - \gamma^k \nabla f(\mathbf{x}^k)\right)$$

Forward update

Abstraction:

$$\mathbf{x}^{k+1} = \mathcal{A}_g \circ \mathcal{A}_f(\mathbf{x}^k)$$

$$\mathbf{u}^k = \mathcal{A}_g \circ \mathcal{A}_f(\mathbf{x}^k)$$

predicted solution

But general $\mathcal{A}_g$ and $\mathcal{A}_f$ cannot guarantee convergence!

图 20：近端梯度算法的结构

下图为基于学习的优化算法的显式版本。包括三个部分： 预测 (predict)、监视 (monitor) 和校正 (correct)。由于在校正阶段显式地使用了目标函数来比较哪种解更好，称之为显式版本。如果经过比较，预测的解更好，就采用，否则，仍然选择传统解，并通过后向更新来更新。

- Explicit momentum Flexible Iterative Modularization Algorithm (eFIMA)

Algorithm 1 Explicit Momentum FIMA (eFIMA)

Require: $\mathbf{x}^0$, $\mathcal{A} = \{\mathcal{A}_g, \mathcal{A}_f\}$, and $\{0 < \gamma^k < 1/L\}$.

1: **while** not converged **do**

prediction

2: $\mathbf{u}^k = \mathcal{A}_g \circ \mathcal{A}_f(\mathbf{x}^k)$.

monitor condition

3: **if** $\Psi(\mathbf{u}^k) \leq \Psi(\mathbf{x}^k)$ **then**

4: $\mathbf{v}^k = \mathbf{u}^k$.

correction

5: **else**

In the worst case, $\mathbf{v}^k \equiv \mathbf{x}^k$

6: $\mathbf{v}^k = \mathbf{x}^k$.

7: **end if**

8: $\mathbf{x}^{k+1} \in \mathrm{prox}_{\gamma^k g}\left(\mathbf{v}^k - \gamma^k \nabla f(\mathbf{v}^k)\right)$.

9: **end while**

图 21：基于学习的优化算法（显示）

上述基于学习的优化算法是收敛的。从直觉上讲，最坏的情况下，算法总是选择传统的解，而传统算法是收敛

的。在一般情形下，如预测的解更好，则该算法应该也可以收敛。林宙辰也给出了一些严格的分析。下图证明了迭代具有足够的下降属性，借助该属性可以证明迭代的任何聚点都是目标函数$\psi(x)$的关键点，因此，在较弱的意义下算法可以认为是收敛的。

- Explicit momentum Flexible Iterative Modularization Algorithm (eFIMA)

Theorem 1. *Let $\{\mathbf{x}^k\}_{k\in\mathbb{N}}$ be the sequence generated by eFIMA. Then at the k-th iteration, there exists a sequence $\{\alpha^k|\alpha^k>0\}_{k\in\mathbb{N}}$, such that*

$$\Psi\left(\mathbf{x}^{k+1}\right)\leq\Psi\left(\mathbf{v}^k\right)-\alpha^k\|\mathbf{x}^{k+1}-\mathbf{v}^k\|^2, \tag{1}$$

where $\mathbf{v}^k$ is the monitor in Alg. 1. Furthermore, $\{\mathbf{x}^k\}_{k\in\mathbb{N}}$ is bounded and any of its accumulation points are the critical points of the objective function $\Psi(\mathbf{x})$.

图 22：算法收敛性证明

此外，林宙辰还介绍了基于学习的优化算法的隐式版本。它依然由预测，监控和校正三个部分组成。同样也可以证明迭代具有足够的下降特性，并由此可以证明收敛。但是如下图所示，预测和监控环节有所不同。

- Implicit momentum Flexible Iterative Modularization Algorithm (iFIMA)

Algorithm 2 Implicit Momentum FIMA (iFIMA)

Require: $\mathbf{x}^0$, $\mathcal{A}=\{\mathcal{A}_g,\mathcal{A}_f\}$, $\{0<2C^k<\mu^k<\infty\}$, and $\{0<\gamma^k<1/L\}$.

1: **while** not converged **do**
2: $\mathbf{u}^k=\mathcal{A}_g\circ\mathcal{A}_f(\mathbf{x}^k)$.
3: $\tilde{\mathbf{u}}^k\in\mathrm{prox}_{\gamma^k g}\left(\mathbf{u}^k-\gamma^k\left(\nabla f(\mathbf{u}^k)+\mu^k(\mathbf{u}^k-\mathbf{x}^k)\right)\right)$. — monitor condition
4: **if** $\|\mathbf{d}^{\tilde{\mathbf{u}}^k}_{\Psi^k}\|\leq C^k\|\tilde{\mathbf{u}}^k-\mathbf{x}^k\|$ **then**
5: $\mathbf{v}^k=\tilde{\mathbf{u}}^k$.
6: **else**
7: $\mathbf{v}^k=\mathbf{x}^k$.
8: **end if**
9: $\mathbf{x}^{k+1}\in\mathrm{prox}_{\gamma^k g}\left(\mathbf{v}^k-\gamma^k\nabla f(\mathbf{v}^k)\right)$.
10: **end while**

prediction

correction

$$\Psi^k(\mathbf{x})=f(\mathbf{x})+g(\mathbf{x})+\frac{\mu^k}{2}\|\mathbf{x}-\mathbf{x}^k\|^2,$$
$$\mathbf{d}^{\mathbf{x}}_{\Psi^k}=\mathbf{d}^{\mathbf{x}}_g+\nabla f(\mathbf{x})+\mu^k(\mathbf{x}-\mathbf{x}^k)\in\partial\Psi^k(\mathbf{x}).$$

图 23：基于学习的优化算法（隐式）

- Implicit momentum Flexible Iterative Modularization Algorithm (iFIMA)

Proposition 1. *Let $\{\mathbf{x}^k,\tilde{\mathbf{u}}^k,\mathbf{v}^k\}_{k\in\mathbb{N}}$ be the sequences generated by Alg. 2. Then there exist two sequences $\{\alpha^k|\alpha^k>0\}_{k\in\mathbb{N}}$ and $\{\beta^k|\beta^k>0\}_{k\in\mathbb{N}}$, such that*

$$\Psi\left(\mathbf{x}^{k+1}\right)\leq\Psi\left(\mathbf{v}^k\right)-\alpha^k\|\mathbf{x}^{k+1}-\mathbf{v}^k\|^2,$$

and

$$\Psi(\tilde{\mathbf{u}}^k)\leq\Psi(\mathbf{x}^k)-\beta^k\|\tilde{\mathbf{u}}^k-\mathbf{x}^k\|^2$$

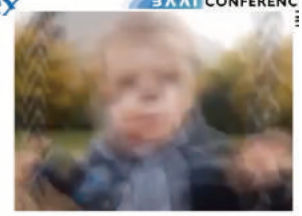
are respectively satisfied.

Theorem 2. *Let $\{\mathbf{x}^k\}_{k\in\mathbb{N}}$ be the sequence generated by iFIMA. Then $\{\mathbf{x}^k\}_{k\in\mathbb{N}}$ is bounded and any of its accumulation points are the critical points of Ψ.*

图 24：算法收敛性证明

林宙辰通过具体示例介绍了基于学习的优化算法在图像恢复逆问题上的应用。首先是非盲反卷积（non–blind deconvolution.），即给定模糊图像，恢复原本的清晰图像。在此问题中，非盲意味着模糊核是已知的。因此，y 是模糊核，z 是标注值（ground truth）。具体计算过程如下图所示。

Learning-based Iterative Methods for Nonconvex Inverse Problems



- Non-blind Deconvolution

$$\min_{\mathbf{x}} f(\mathbf{x};\mathbf{D},\mathbf{y}) + g(\mathbf{x}).$$

$$\mathbf{y} = \mathbf{b} \otimes \mathbf{z} + \mathbf{n}$$

$$f(\mathbf{x};\mathbf{D},\mathbf{y}) = \|\mathbf{y} - \mathbf{D}\mathbf{x}\|^2 \text{ and } g(\mathbf{x}) = \lambda\|\mathbf{x}\|_p \ (0 \le p < 1).$$

$\mathbf{x} = \mathbf{W}\mathbf{z}$, $\mathbf{D} = \mathbf{B}\mathbf{W}^\top$, where $\mathbf{B}$ is the matrix form of $\mathbf{b}$ and $\mathbf{W}$ is the wavelet transform matrix.

We update $\mathbf{z}$ by solving

$$\mathcal{A}_f(\mathbf{z}^k) := \arg\min_{\mathbf{z}} \|\mathbf{y} - \mathbf{b} \otimes \mathbf{z}\|^2 + \tau\|\mathbf{z} - \mathbf{z}^k\|^2$$

to aggregate principles of the task and information from last updated variable, where $\mathbf{z}^k = \mathbf{W}^\top\mathbf{x}^k$. Then $\mathcal{A}_f$ on $\mathbf{x}$ can be defined as $\mathcal{A}_f(\mathbf{x}^k) = \mathbf{W}\mathcal{A}_f(\mathbf{z}^k)$, i.e.,

$$\mathcal{A}_f(\mathbf{x}^k) = \mathbf{W}(\mathbf{B}^T\mathbf{B} + \tau\mathbf{I})^{-1}\left(\mathbf{B}^T\mathbf{y} + \tau\mathbf{W}^\top\mathbf{x}^k\right). \quad \text{easily computed by FFT}$$

Solve $\mathcal{A}_g(\mathcal{A}_f(\mathbf{z}^k)) := \arg\min_{\mathbf{z}} g(\mathbf{z}) + \tau\|\mathbf{z} - \mathcal{A}_f(\mathbf{z}^k)\|^2$ by a **deep network**.

图 25：非盲反卷积问题

下图是将基于学习的优化算法（显式和隐式版本）与邻近梯度算法进行比较的模拟。可以看到迭代次数比传统方法少得多。这意味着基于学习的优化算法实际上是线性的，而且传统算法只是次线性的。

Non-blind Deconvolution

TABLE 1
The number of iterations (including plug-and-play modules) in FIMA. "No. Iter." reports the number of whole iterations and "No. $\mathcal{A}$" denotes the times the plug-and-play modules $\mathcal{A}_g \circ \mathcal{A}_f$ has been performed by FIMA during iterations. We also report the number of iterations for standard PG in the rightmost column.

Image	eFIMA		iFIMA		PG
	No. Iter.	No. $\mathcal{A}$	No. Iter.	No. $\mathcal{A}$	No. Iter.
Fig. 4	13	11	22	21	542
Fig. 5	19	15	26	25	577
	linear		**linear**		**sublinear**

图 26：结果对比

下图是一些定量比较和定性比较，可以看出基于学习的方法比传统的图像恢复方法具有更高的 PSNR 和 SSIM，但计算所需的时间却少得多。

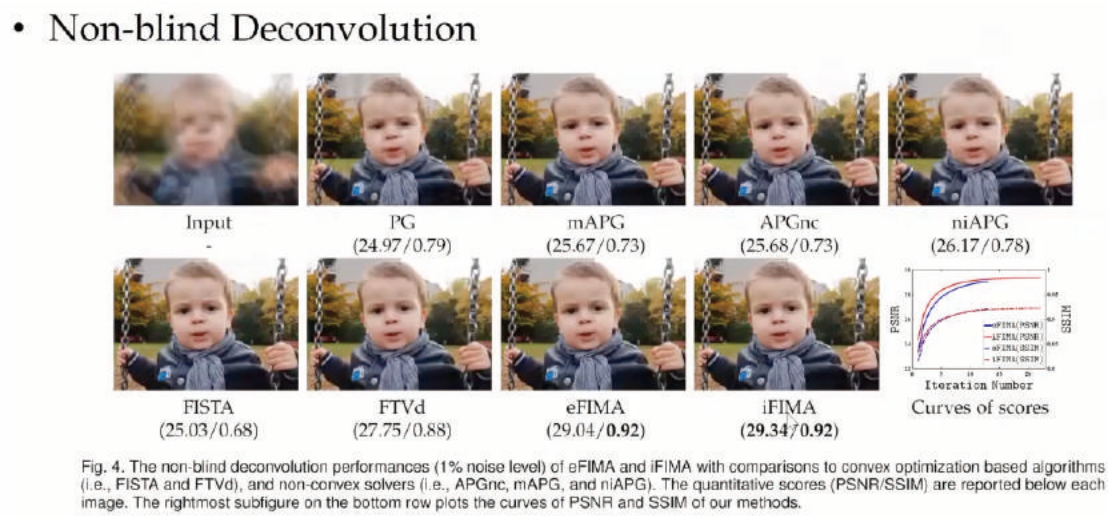


Fig. 4. The non-blind deconvolution performances (1% noise level) of eFIMA and iFIMA with comparisons to convex optimization based algorithms (i.e., FISTA and FTVd), and non-convex solvers (i.e., APGnc, mAPG, and niAPG). The quantitative scores (PSNR/SSIM) are reported below each image. The rightmost subfigure on the bottom row plots the curves of PSNR and SSIM of our methods.

图 27：非盲反卷积问题定性比较

• Non-blind Deconvolution

TABLE 2
Averaged PSNR, SSIM and Time(s) on the benchmark image set [24]. Here σ denotes the noise levels.

σ	Metric	State-of-the-art Image Restoration Methods					Classical Nonconvex Methods				Ours	
		IDDBM3D	EPLL	PPADMM	RTF	IRCNN	PG	mAPG	APGnc	niAPG	eFIMA	iFIMA
1%	PSNR	28.83	28.67	28.01	29.12	29.78	27.32	26.68	26.69	27.24	29.81	**29.85**
	SSIM	0.81	0.81	0.78	0.83	0.84	0.71	0.67	0.67	0.73	**0.85**	**0.85**
	Time(s)	193.13	112.03	293.99	249.83	2.67	20.36	13.02	7.16	5.29	**1.89**	2.06
2%	PSNR	27.60	26.79	26.54	25.58	27.90	25.61	25.20	25.28	25.63	28.02	**28.06**
	SSIM	0.76	0.74	0.72	0.66	0.78	0.63	0.60	0.61	0.64	**0.79**	**0.79**
	Time(s)	198.66	100.52	270.45	254.26	2.68	15.43	7.70	4.66	3.30	**1.90**	2.07
3%	PSNR	26.72	25.68	25.78	21.18	26.81	24.63	24.39	24.48	24.76	27.05	**27.07**
	SSIM	0.72	0.69	0.68	0.42	0.73	0.57	0.55	0.56	0.61	0.74	**0.75**
	Time(s)	191.25	96.32	257.94	252.47	2.68	13.89	6.44	5.37	2.63	**1.89**	2.07
4%	PSNR	26.06	24.88	25.27	17.95	26.10	24.05	23.88	23.95	24.14	26.20	**26.37**
	SSIM	0.69	0.65	0.66	0.28	0.70	0.54	0.53	0.53	0.59	0.70	**0.72**
	Time(s)	183.44	93.82	258.45	255.84	2.67	11.99	6.01	7.82	2.35	**1.89**	2.07

TABLE 3
Averaged quantitative scores on Levin et al's benchmark.

Method	PSNR	SSIM	ER	KS	Time(s)
Perrone et al.	29.27	0.88	1.35	0.80	113.70
Levin et al.	29.03	0.89	1.40	0.81	41.77
Sun et al.	29.71	0.90	1.32	0.82	209.47
Zhang et al.	28.01	0.86	1.25	0.58	37.45
Pan et al.	29.78	0.89	1.33	0.80	102.60
Ours	**30.37**	**0.91**	**1.20**	**0.83**	**5.65**

higher quality and much faster!

图 28：非盲反卷积问题定量比较

基于学习的优化算法同样也可以应用于盲反卷积，这意味着模糊核是未知的。从下面的对比图可以看出，所提方法产生了更加清晰的地面真实图像。

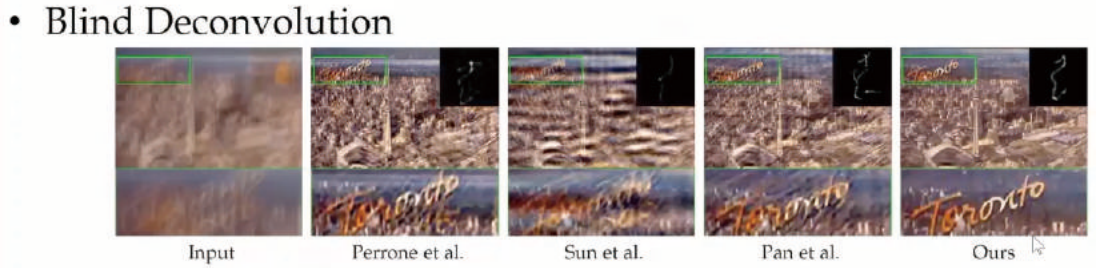


Fig. 7. Visual comparisons between mFIMA and other competitive methods (top 3 in Tab. 3) on a real blurry image.

图 29：盲反卷积问题结果比较 1

Fig. 9. The blind image deconvolution results of mFIMA with comparisons to state-of-the-art approaches on blurry facial image with 3% Guassian noise. The quantitative scores (i.e., PSNR / SSIM / KS) are reported below each image.

图 30：盲反卷积问题结果比较 2

基于学习的优化算法还可以用来去除图像上的雨水条纹。从下图可以看出，所提方法比传统算法和纯粹基于深度学习的算法要好得多。

- Rain Streak Removal

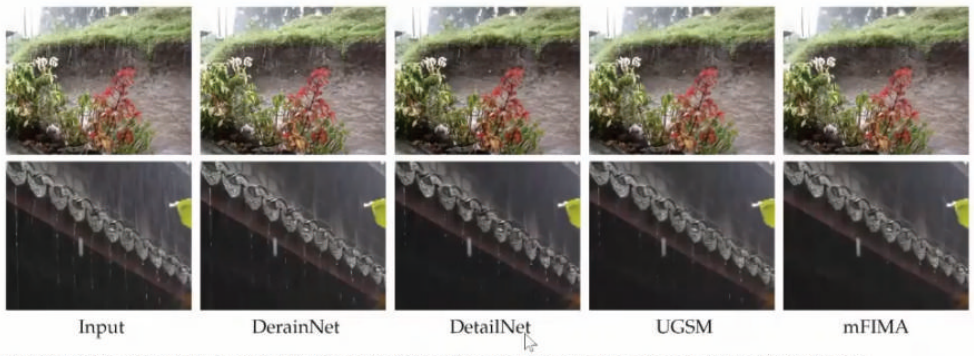


Fig. 10. Rain streaks removal results of mFIMA with comparisons to the state-of-the-art approaches on real-world rainy images.

图 31：雨痕去除问题结果比较

五、总结

最后，林宙辰对报告做了以下总结:

1. 长期以来，优化算法一直促进机器学习的发展，如今借助机器学习的思想也能帮助解决优化问题。优化算法和机器学习可以相互受益，两者之间的交叉融合可以使两个领域更健康、完整地发展。
2. 在传统优化算法的适当部分引入学习机制，可以显著提高算法的收敛速度并得到更好的信息处理效果。基于学习的优化算法能够更好地适应数据，将是传统优化算法的有益补充。
3. 如果研究止步于应用而没有任何理论分析，那么这些算法的价值是有限的，每个人都可以想到。但如果要有理论上的保证，那就困难得多。特别是对收敛速度的分析，是非常少见且重要的。

同时，林宙辰希望他在基于学习的优化领域汇报的成果，可以引起优化同行们的更多关注。

旷视首席科学家孙剑：视觉计算前沿进展

智源社区 季葛鹏

在第二届北京智源大会机器学习专题论坛中，旷视首席科学家、旷视研究院院长、西安交通大学人工智能学院首任院长、智源研究员孙剑博士，带来了《视觉计算前沿进展》的主题分享。

孙剑曾两次获得 CVPR 最佳论文奖 (2009 年和 2016 年)，谷歌学术引用超 14 万 (截止 2020 年 8 月)，拥有 40 多项美国或国际专利，于 2010 年被 MIT Technology Review 评选为全球 35 岁以下杰出青年创新者即 TR35。**深度卷积神经网络四大核心要素是什么？深度学习实践中的挑战有哪些？计算机视觉应用中的核心难点是什么？产品落地应用过程中关键性问题又有哪些？**让我们带着好奇与疑惑，同孙剑一起，就近期视觉计算领域的前沿技术展开深度研讨与思考吧！

图 1：视觉计算前沿进展

一、背景介绍

随着深度学习的进步、计算存储的扩大、可视化数据集的激增，计算机视觉方面的研究在过去几年发展可谓是日新月异，特别是在自动驾驶汽车、医疗保健、零售、能源、语言学等诸多领域，计算机视觉的应用都越来越广。视觉是人类获取信息的最主要的方式，在视觉、听觉、嗅觉、触觉和味觉中，视觉接受信息的占比高达 80%。早在 1966 年，一位人工智能领域的先行者，时任麻省理工学院教师的马文・明斯基 (Marvin Minsky) 教授，突发奇想地为学生布置了一个暑假作业：“让计算机看懂世界”。自此，这成为了像 Marvin 这样敢于创新的学者对于未知世界探索的一小步，也成为了人类对于计算机理解视觉信息的一大步。伴随着计算机领域基础设施的快速发展和人类对于计算机理解并处理视觉信息能力的无限向往，经过长时间的演变，计算机视觉已经无处不在。

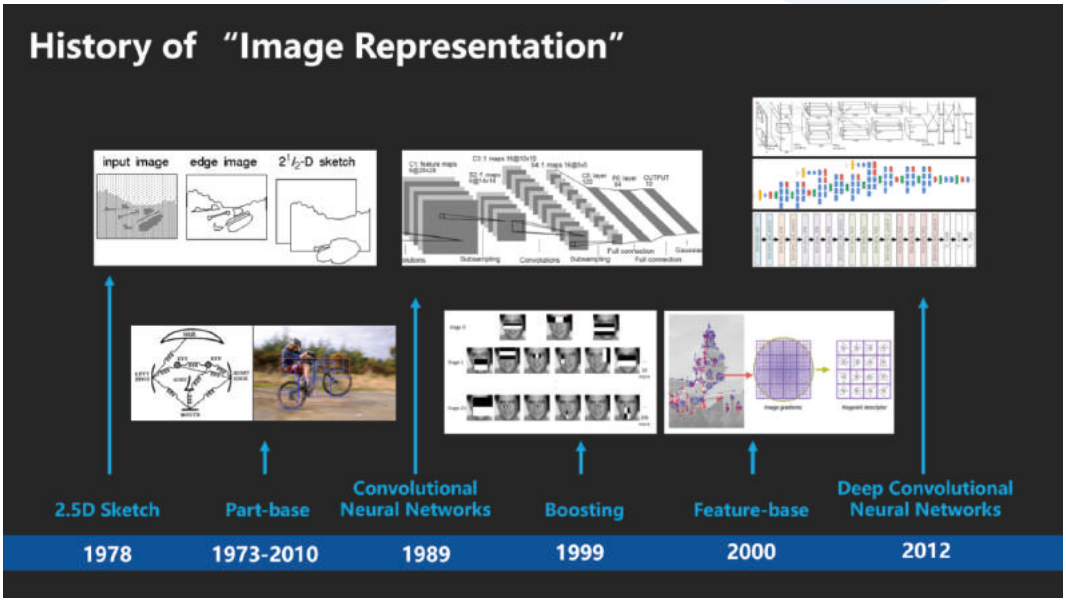


图 2：图像表示的历史发展

孙剑指出，计算机视觉中存在很多问题，最为核心的问题就是“如何识别图像中的物体”，而在这个过程中最为核心问题就是“如何求取一个图像的表示（Image Representation）”，以至于人类能够在计算机中完成这样一个使命。

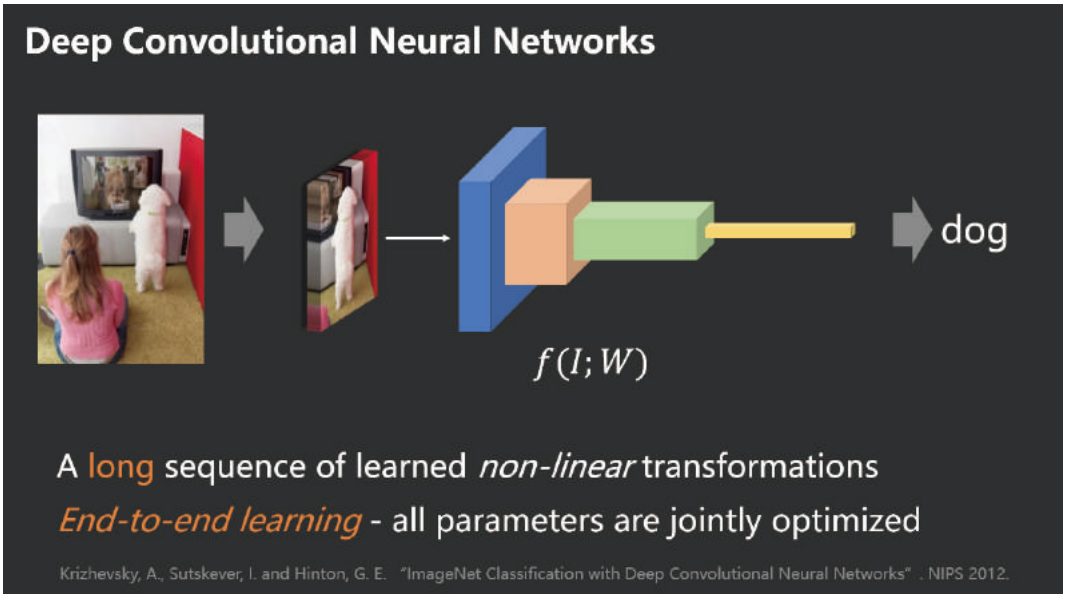


图 3：深度卷积神经网络

时至今日，最具统治力地位的方法就是我们所常见的**深度卷积神经网络（Deep Convolutional Neural Network）**，这种网络有两个显著的特点： 第一是包含多次非线性变换，即把一张图片变成计算机可以识别的东西； 第二是可自动学习的参数，即端到端的自动学习的任务。

二、深度卷积神经网络

深度卷积神经网络最早源于八十年代，是来自日本的 Fukushima 教授首次提出的。从第一次使用卷积神经网络完成数字图像识别，深度学习到今天已经成为了非常流行的工具，这经过了很长的发展历程（如图 4 所示）。

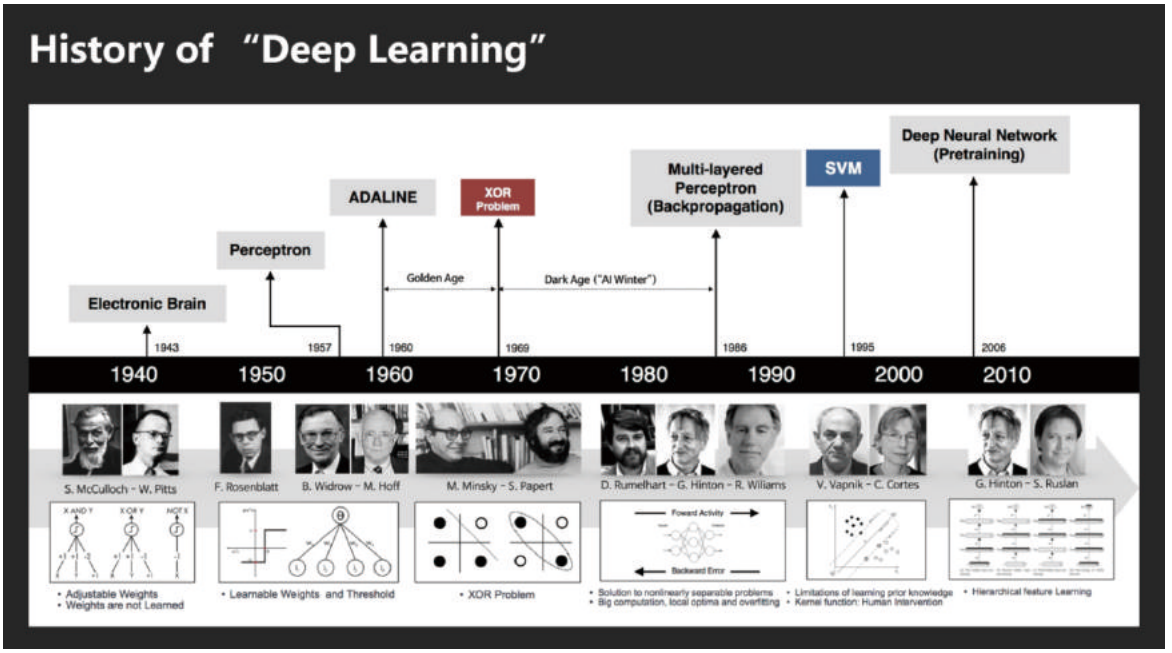


图 4：深度学习的历史发展

孙剑指出，深度卷积神经网络有**四个核心因素：卷积操作类型（Convolution）、整个网络的深度（Depth）、卷积层的宽度（Width）和输入的大小（Size）**。大多数的研究工作基于这四个因素展开。

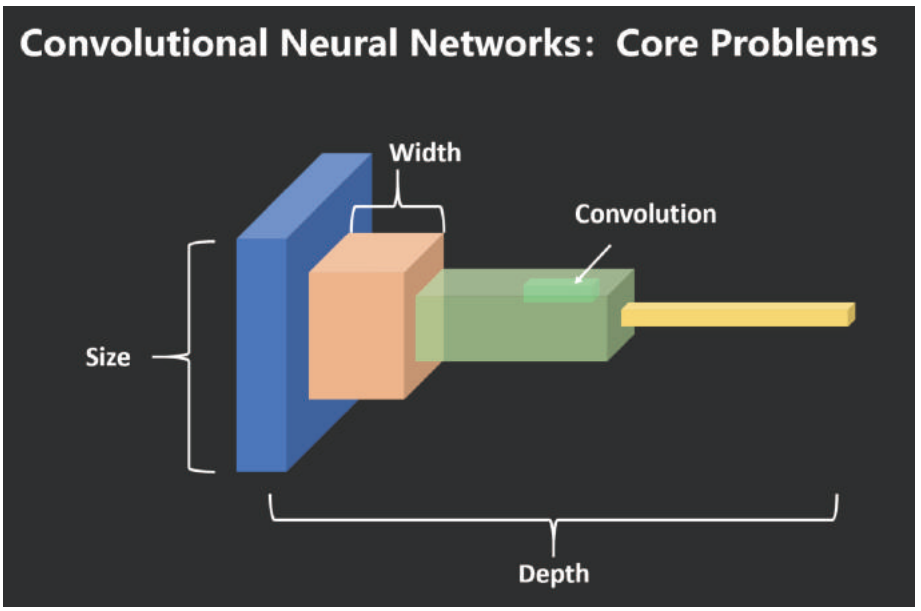


图 5：卷积神经网络：核心因素

2.1 卷积操作类型 (Convolution)

常用的基础卷积核大小有 5x5、3x3、1x1（如下图所示）；后来发现可以通过分组卷积（Grouped Convolution）将 3 × 3 卷积、1 × 1 卷积分成很多组，减少卷积操作中的冗余部分，使卷积更高效。另外一个近些年在卷积方面的思路是深度卷积（Depth–wise Convolution），可以把深度卷积看作是分组卷积的极致，在计算量小的网络非常高效。

基于之前的思想，旷视研究院提出了 ShuffleNet V1 [1] 算法，在 Grouped Pointwise 操作中引入 Shuffle 操作，用于交换通道之间的信息，同时保持十分低的复杂度（如下图所示）；

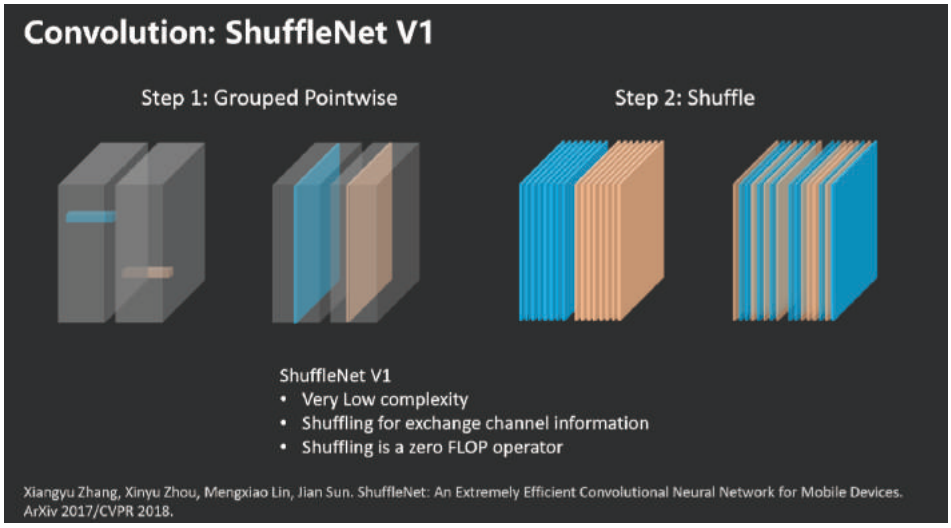


图 6：ShuffleNet V1 中的卷积

2019 年提出旷视研究院提出 ShuffleNet V2 [2]，在前者的基础上引入卷积平衡的概念，通过 Channel Split 和 Partial Convolution 的改进，有效避免网络的碎片化和减少元素级别运算的操作（如下图所示）。

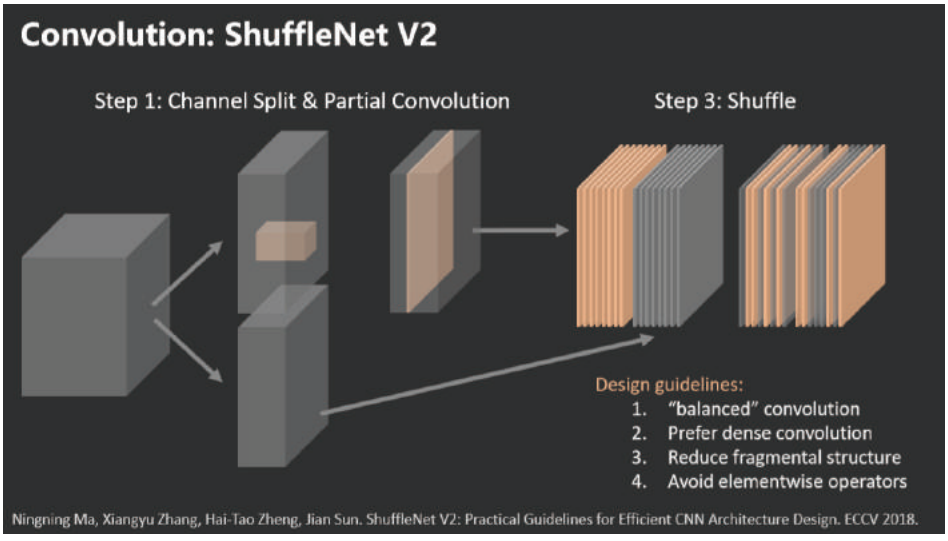


图 7：Shuffle V2 中的卷积

最新的卷积研究方向叫“动态卷积”。 动态卷积的卷积核和参数与输入特征是相关的。例如，在 Channel-wise Mixture [3] 工作中，引入了多个卷积核的线性组合，其系数是动态的（如下图所示）。

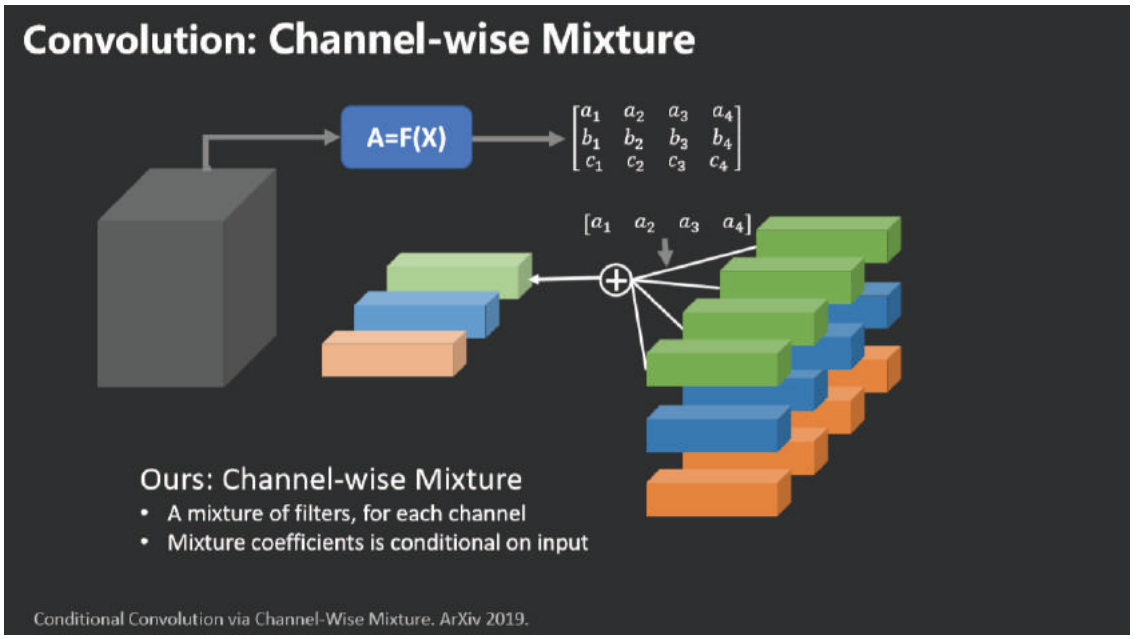


图 8：Channel-wise Mixture 中的卷积

2.2 网络的深度（Depth）

谈及神经网络的深度，孙剑介绍到，首先在历史上网络的深度曾经是深度神经网络研究工作中非常大的障碍，学者们发现深度神经网络非常难训，很多人相信深层神经网络是训练不好的。其次，就是若干年前大家很难重现深度神经网络的结果，这两点原因造成它当年不能被广泛使用。

网络深度的核心变革最早可以追溯到 2012 年提出的八层神经网络 AlexNet。AlexNet 斩获了 ILSVRC 2012 的冠军，其性能远远超过当时非神经网络方法。2014 年提出的 VGG 系列网络，实现了对于 19 层网络的突破，并斩获了当年 ILSVRC 2014 的亚军，而同年的冠军则由来自谷歌研究员提出的 LeNet 致敬版本——GoogLeNet 所拿下。

最具划时代意义的网络，要数来自微软亚研院（孙剑团队）提出的 ResNet-152，这也是第一个超过 100 层的神经网络。

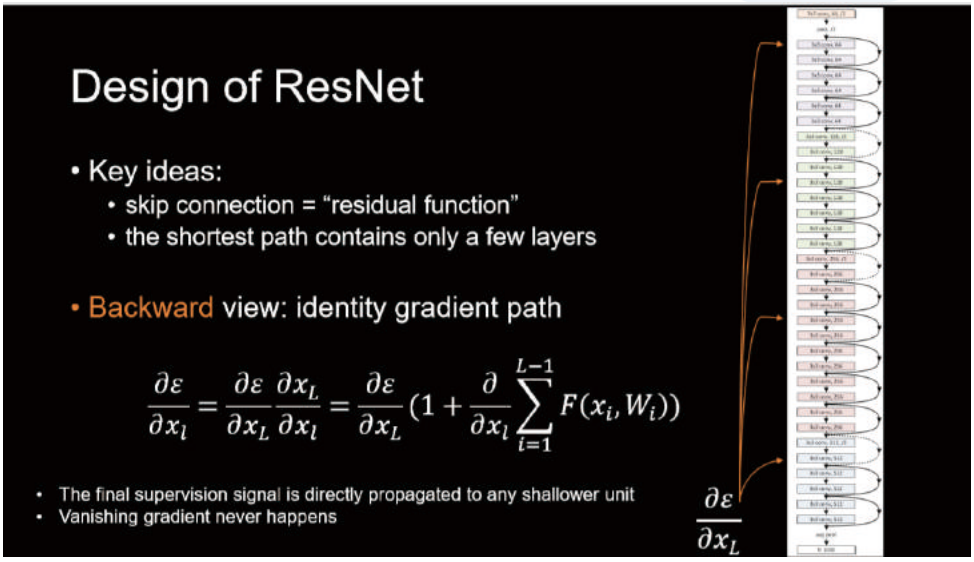


图 9：ResNet 的设计

ResNet 是一种残差（Residual）网络，其核心思想是残差连接（Residual Connection），即学习从一种信号到另外一种信息之间的变化量（残差映射函数），这样可以让优化任务变得更加简单，并有效避免当网络变深时，在梯度反向更新过程中的梯度退化问题。残差网络不仅可以用于图像识别，还被应用到了 AlphaGo Zero 象棋决策过程、NLP 领域（Transformer、BERT）等。

2.3 网络的宽度（Width）

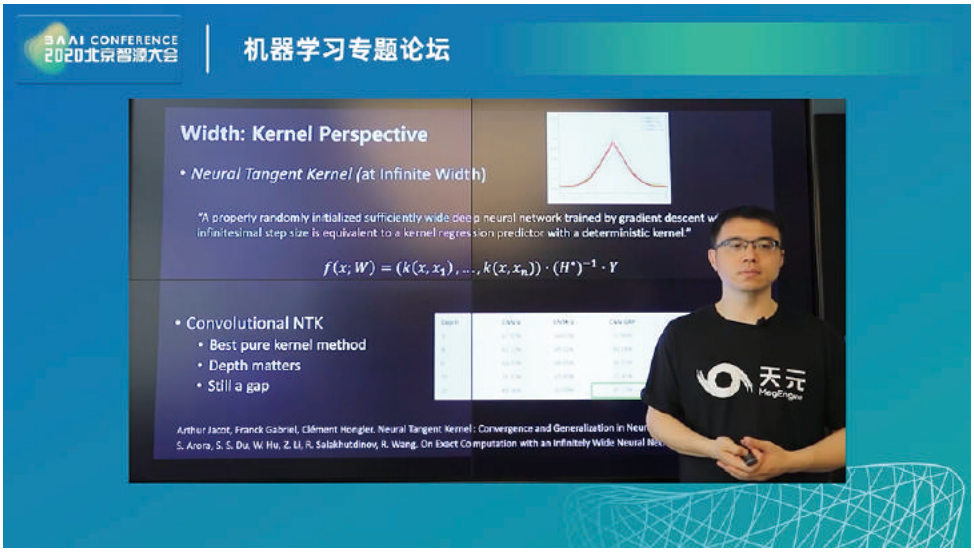


图 10：从 Kernel 角度看网络的宽度

深度网络的宽度指每一层有多少神经元和通道，即表达能力。最近的一项被称为 Neural Tangent Kernel 的研究 [4]，给神经网络提供了一个新的解释，该工作从 Kernel 的视角看待神经网络，指出一个深度神经网络如果

充分宽，则可以等效一个确定性的 Kernel 方法。这是一个很有价值的理论研究方向，值得进一步探索。

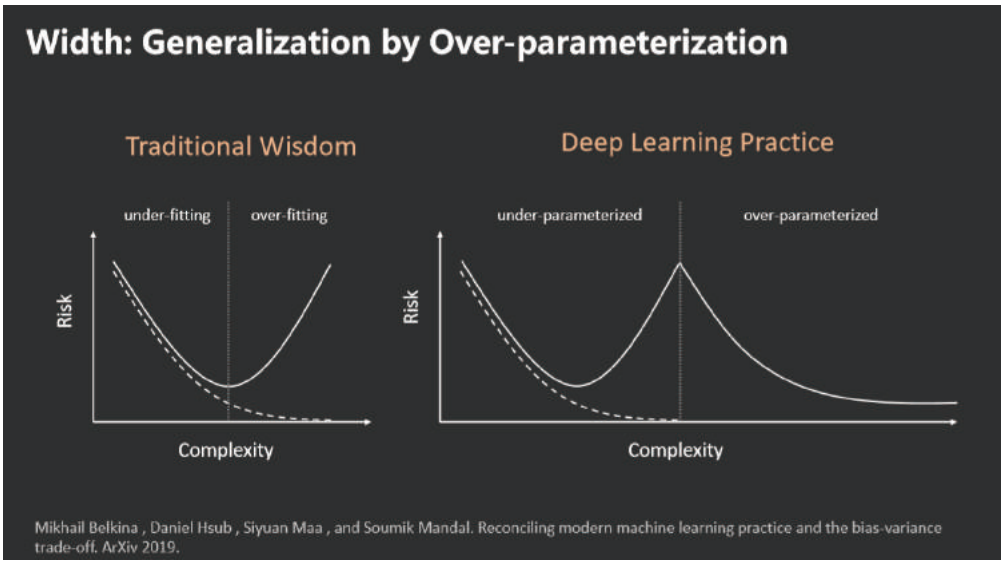


图 11：过参数化的泛化

在另外一项关于宽度的研究 [5] 中，研究人员发了一个区别于传统思维的现象，在传统思维中，如果网络容量非常小的时候会产生欠拟合（Under–fitting），过于复杂可能会过拟合（Over–fitting），但是如果继续增大且到达一个阈值时称为过参数化（Over–parameterized），这时训练与测试 error 会继续下降。这个现象的背后说明不能使用参数量来衡量网络的容量，而应追求更为本质的东西——是否具有更优的平滑特性。此外该研究也说明，使用更深的网络、增加数据、增大网络容量，神经网络的性能会不断的增加，甚至可能超过人的性能。 举个例子，旷视在 2015 年推出的刷脸支付，也被 MIT 在 2017 年评为“十大创新性突破技术”。人脸支付这个应用场景通过大量数据，首次超过人的性能。

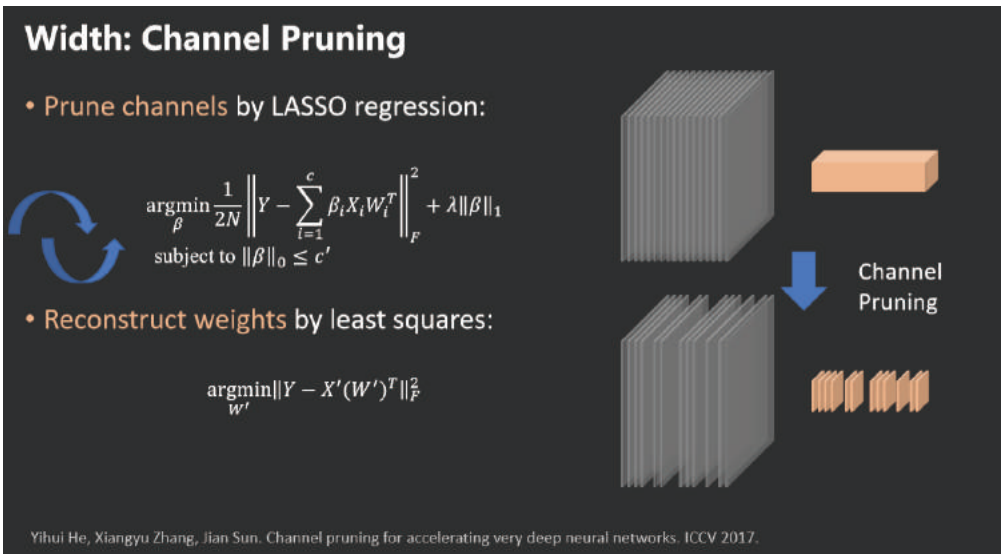


图 12：通道剪枝

Channel 数量的变大虽然会提升网络性能，但同样也会带来很高的计算复杂度，严重制约了实际应用。因此学者们希望降低 channel 数量，并同时保证性能，提出通道剪枝（Channel Pruning）技术去掉冗余的通道。

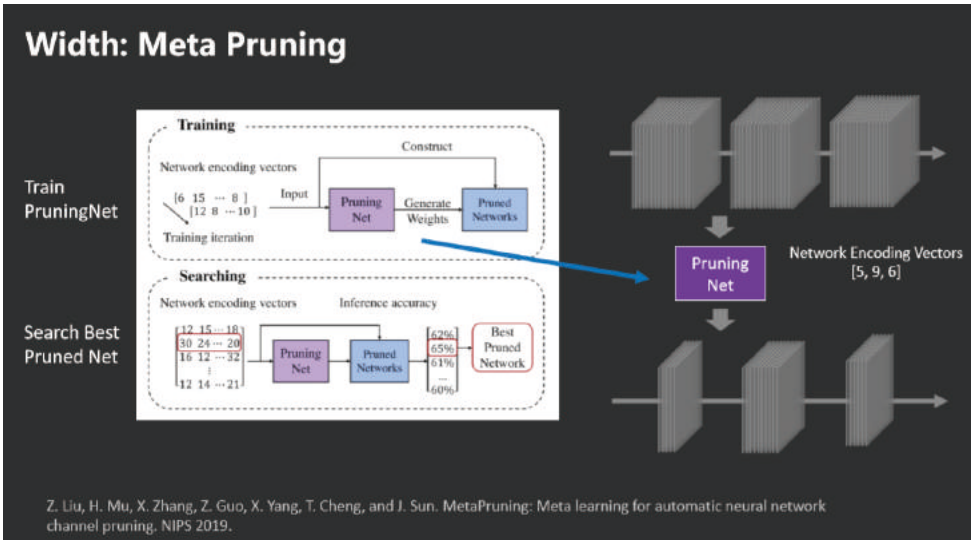


图 13：元剪枝

在发表于 NeurIPS 2019 的 Meta Pruning [6] 工作中，旷视研究院提出通过训练一种 Meta 网络，来学习如何去修剪另一个网络，这是操作另外一个网络的网络，该方法取得了非常好的效果。

2.4 网络的尺度（Size）

神经网络的 Size 指输入图像的大小，包括网络内部不同阶段特征图的大小。这个参数在标准的神经网络设计过程中一般都是固定的，而在旷视研究院去年的研究工作 [7] 中，我们发现可以动态改变网络在训练与推理过程中每一层的大小，非常利于性能的提升。

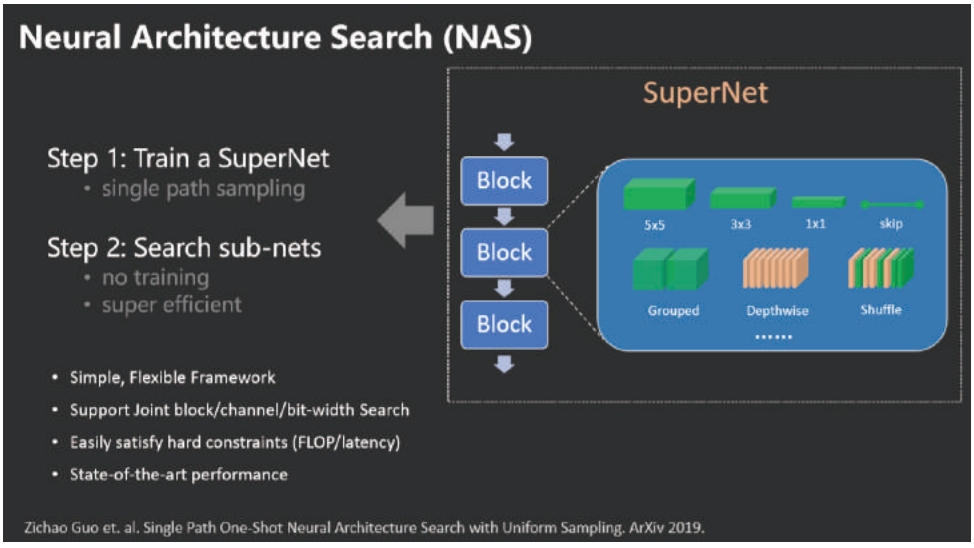


图 14：神经网络架构搜索

如果对以上 Convolution、Depth、Width 和 Size 四个因素进行联合优化，便有了一个全新的方向：神经网络架构搜索（NAS）。基于 NAS 思想孙剑团队还提出了非常大且容易训练的网络，名为 Singe Path One-Shot NAS[8]，该方法会首先训练一个 SuperNet，然后直接从中采样出一些子网路，它们可以直接继承 SuperNet 的权重，无需重新训练便可以找到很多性能优良的子网络。

三、深度学习中的关键挑战

在深度学习研究与开发中，保证网络结构、深度学习框架、计算设备三要素的协同设计，是决定整个系统能否高效运转的关键。旷视基于自身快速迭代的业务需求，从 2014 年开始研发深度学习框架天元（MegEngine），并于 2015 年投入使用。该框架凭借训练推理一体化、动态图静态图结合、兼容并包、灵活高效可拓展等特性，在 6 年来一直支撑着整个旷视的学术研究与工程研发。旷视所有算法均基于天元（MegEngine）进行。

旷视在 2020 年 3 月份把深度学习框架天元 Alpha 版本开源给人工智能社区内所有的开发者使用，6 月上线了 Beta 版本，并将于 9 月发布正式版本。

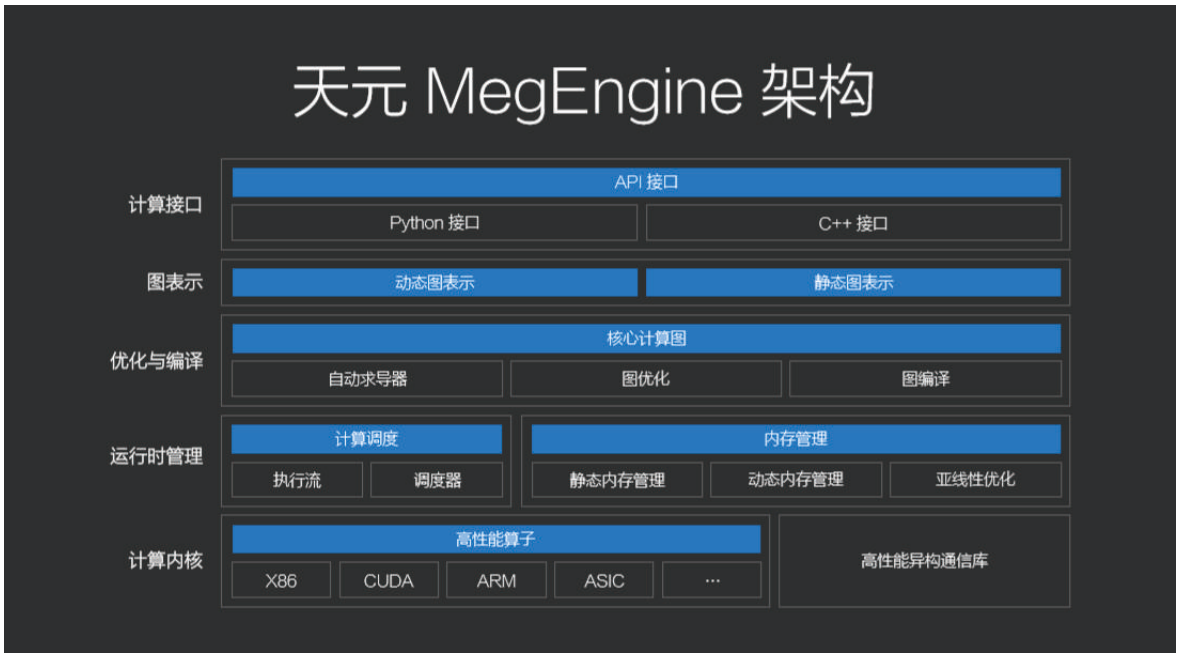


图 15：MegEngine 架构图

深度学习的研发挑战非常大，虽然人们对其给予厚望，但是它并不能实现大家对人工智能所有的梦想。为此，孙剑还列举了若干关键性问题和挑战：

第一，理论化的理解。如何解释在超大模型与相对于模型参数而言较少的数据的情况下，网络依然能够得到很好的泛化性能？这需要对今天的深度学习模型有更好的理论解释。
第二，架构设计：在今天大量研究人员的时间都花在调模型结构上。
第三，可解释性：深度学习模型被诟病的一点是说它是黑盒子，不具有很好的解释性。
第四，对抗攻击：涉及到模型可靠安全性的一些方面。

第五，联邦学习：当数据来源不同，又有隐私要求时，如何联合训练系统。

在深度学习可解释性问题上，孙剑还介绍了旷视研究院近期的最新工作——球面优化动力学理论[9]。该研究发现，在深度学习中，带批归一化和权重衰减的网络在优化过程中受两个“力”的控制，一个是离心力，另一个是向心力，它们分别受不同的机制来驱动。文章证明，在神经网络的训练过程中，一直在更新一个参数的角度，从而达到稳态。旷视研究院对这个参数角度给出了一个非常严格的推导公式，而且这个公式与大量的实验几乎完美吻合。

该工作的意义在于： 解释了 BN 对梯度消失或爆炸时的抑制； 同时也指出优化可以跳出小的局部极小； 很好的解释了在这种随机梯度下降的方法中，如果不改变学习率，为何网络不收敛。

四、机器视觉

机器视觉中的核心问题主要分成四类：分类、检测、分割和序列学习。

4.1 Classification（分类）

最经典的分类任务就是猫狗识别，即识别视觉场景中是猫还是狗。在这个领域中最大最经典的数据集之一就是 ImageNet。分类任务及其衍生应用非常多，包括交通监控、医学图像、自动驾驶和机器人等等。

4.2 Detection（检测）

检测任务中不仅需要识别物体类别，还需要提供物体的位置信息，即： 是什么？在什么位置？这是很多应用的基本前提。

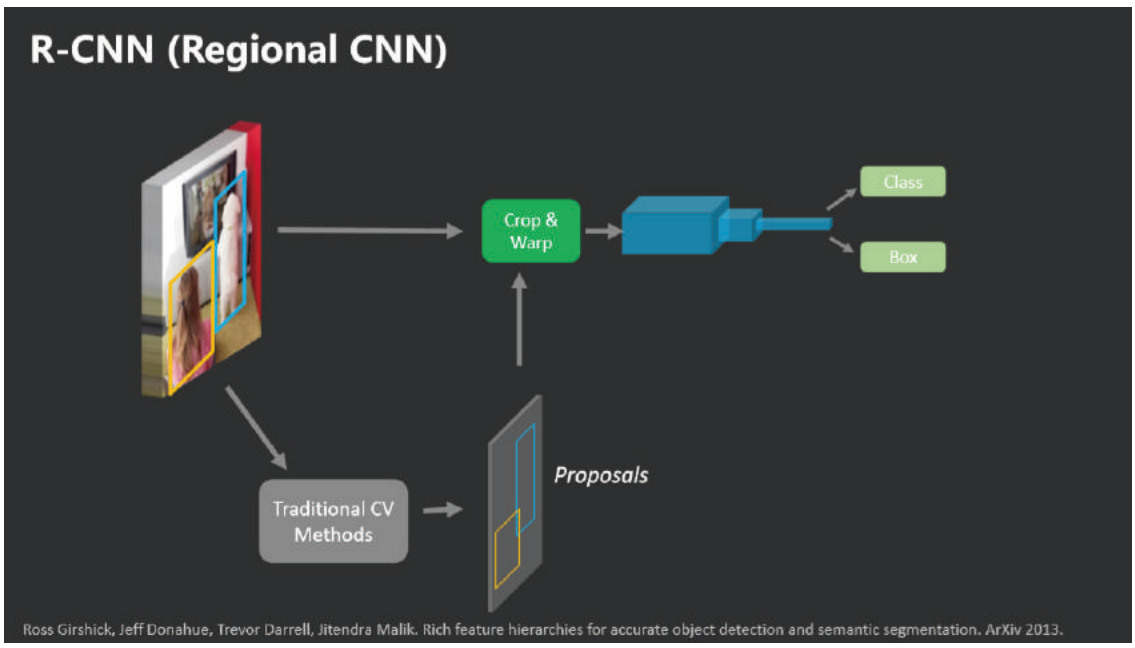


图 16：R-CNN

在深度学习领域，最早的检测任务方法是 R-CNN [10]。该方法首先基于传统方法将原图中所有可能的物体裁出来，然后将每个裁剪部分送入神经网络，判定其属于哪个类别，以及其边界框的形态。虽然 R-CNN 取得了非常不错的性能，但其弊端在于，每次操作都会有几千个框，计算量十分大。

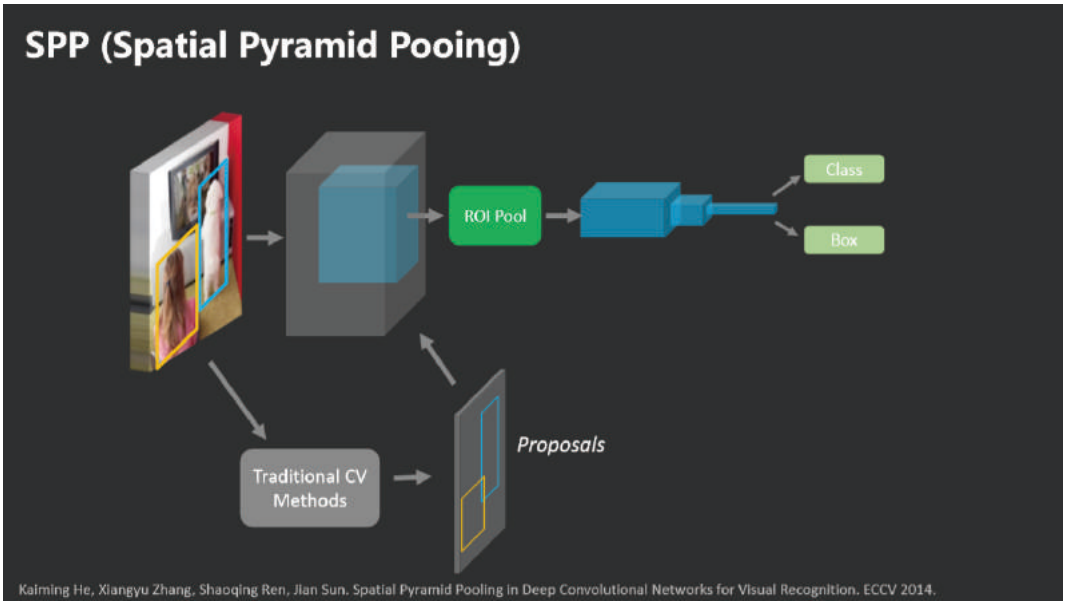


图 17：SPP

针对这个问题，孙剑团队在 2014 年提出 SPP [11]，缓解了 R-CNN 中计算量的问题。该方法无需对原图进行裁剪，而是先对图像进行一次卷积操作，进而对特征图进行裁剪。对于这些裁剪的特征，后面就可以接很小的神经网络，既达到了同样的性能，速度也提高了 100~200 倍。

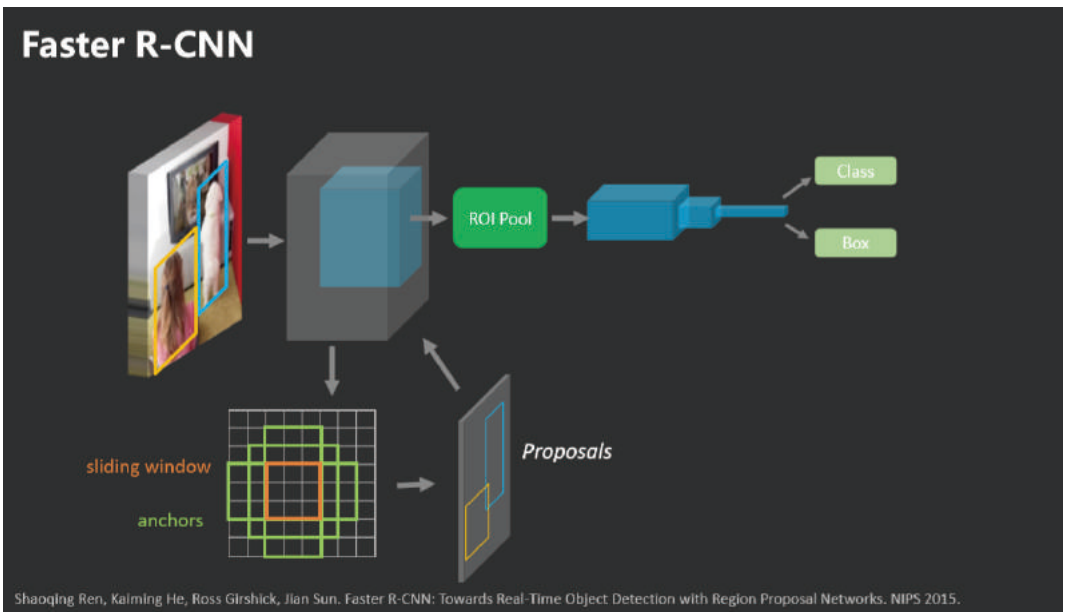


图 18：Faster R-CNN

之前提到的 Proposal 方法都是基于传统方法来做的，那么是否能够利用深度学习实现整个过程的自动学习过程？孙剑团队在 2015 年提出 Faster R-CNN [12]，实现了从 feature map 中直接获取 Proposals，并引入 Anchor 的概念让整个系统都可以使用深度学习来进行，这样的方法还能使得系统更加高效。当然，后面还可以接上掩膜（Mask），即何凯明在 2017 年的工作 Mask R-CNN，证明检测和分割同时做可以获取更好的效果。

除了之前提到的二阶段方法（Two-stage）外，另外还存在一阶段方法（One-stage）。这类方法以 SSD [13]、YOLO [14]、RetinaNet [15] 为代表，即直接回归物体的类别概率和位置坐标值，无需 Region Proposals，准确度稍低，但它因为其效率很高，且在硬件上容易实现，所以在工业界得到了最广泛的使用。

当然，最近 Anchor-free 的方法打破之前 Anchor-based 的禁锢，即丢弃掉 Anchor 的概念，对于图像中的每一个点进行回归和预测，同样取得了不错的性能。这类工作有 DenseBox [16]、FCOS [17] 等。

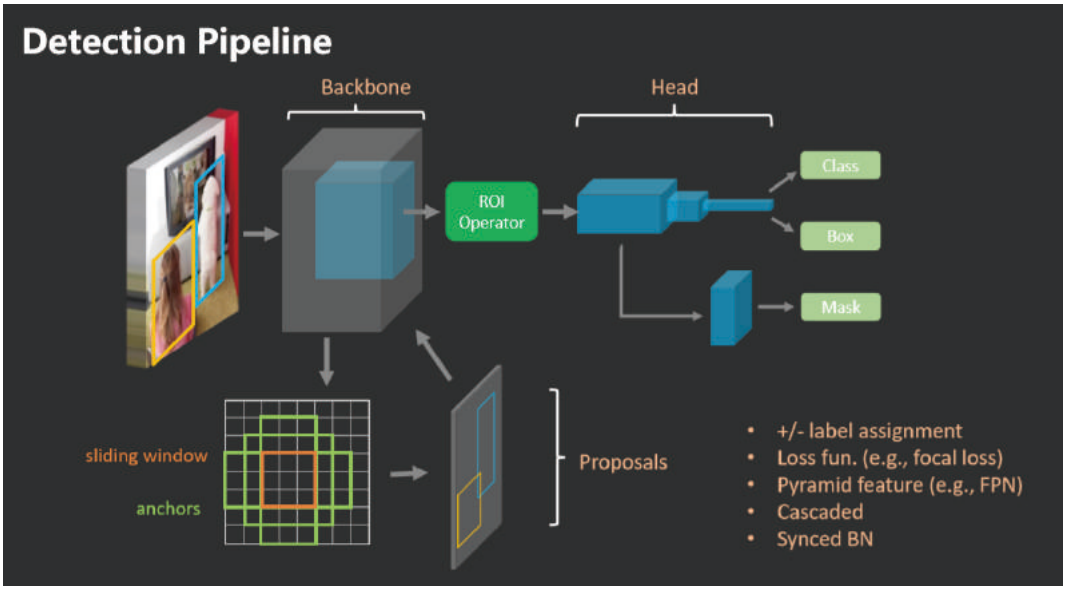


图 19：检测的基本流程

最后，孙剑对于检测流程进行了一个总结：基于上述基本检测框架，还有更细的技术创新，例如框的正负样本的定义、训练的损失函数，方是否使用多尺度、是否多机训练等。它们使得使得整个检测流程越来越丰富。

目前，衡量物体检测最权威的数据集是 MS COCO，它由微软创立。从 2013 年创建以来，到 2019 年，COCO 的精度不断提高。旷视在 COCO 挑战赛上取得三连冠，分别是在 2017 年（52.5 mAP）、2018 年（56.1 mAP）和 2019 年（61.2 mAP）。

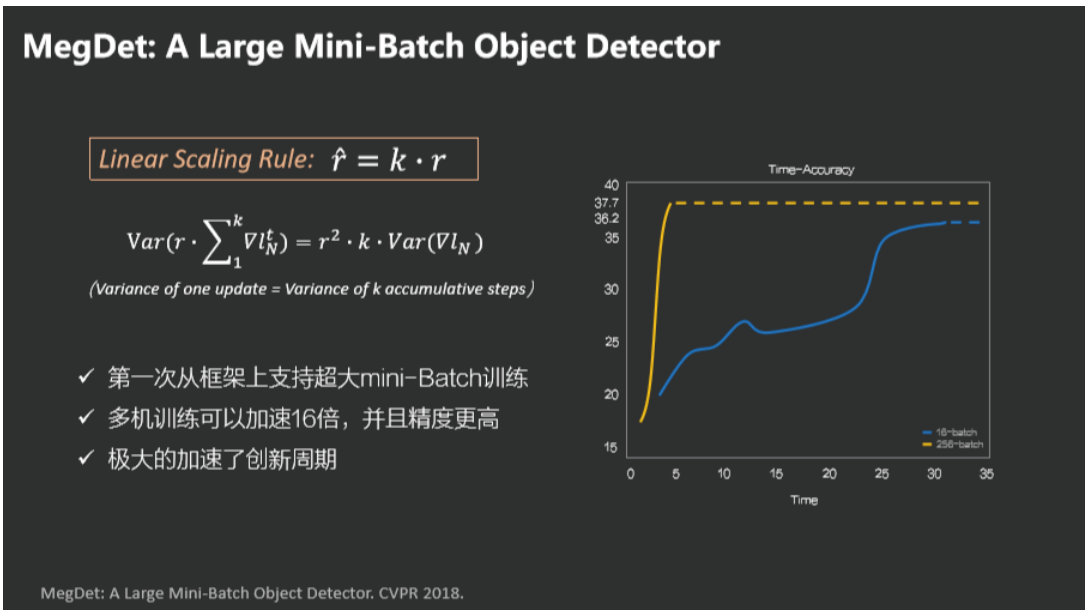


图 20：MegDet

2018 年，旷视提出第一个大 mini–batch 的物体检测器 MegDet [18]。它首次支持使用超大 mini–Batch 来训练物体检测器，能够在多机系统上加速整个训练系统 16 倍，从图中可以看到，这套系统大大加速了创新周期。

为进一步增大数据集容量，旷视与北京智源人工智能研究院一起创建了 Objects365 V2 数据集，它是目前世界上最大的精标物体检测数据集，包括 365 种常见物体，两百万张图像，三千万人工标注框。了解更多信息可以直击这里：https://www.objects365.org/。

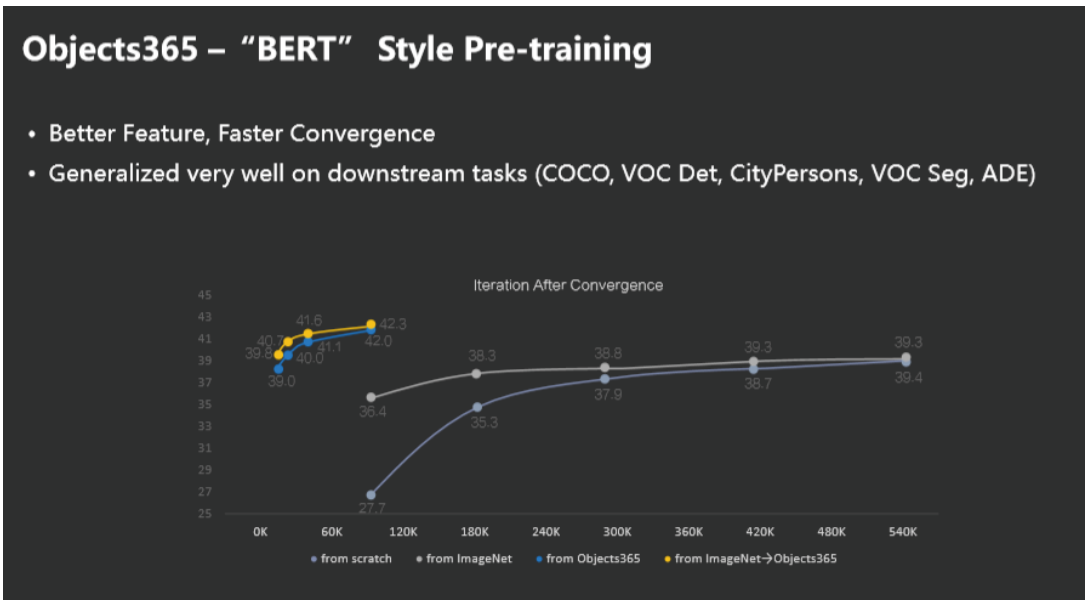


图 21: Object365 的 BERT 式预训练

那么如此大数据集是否能够带来大的收益？答案是肯定的。孙剑指出，经过类似于 BERT 的预训练工作，在 Objects365 上面得到的预训练特征可以在加速检测、分割等下游任务收敛速度的同时，显著提高其性能上界。

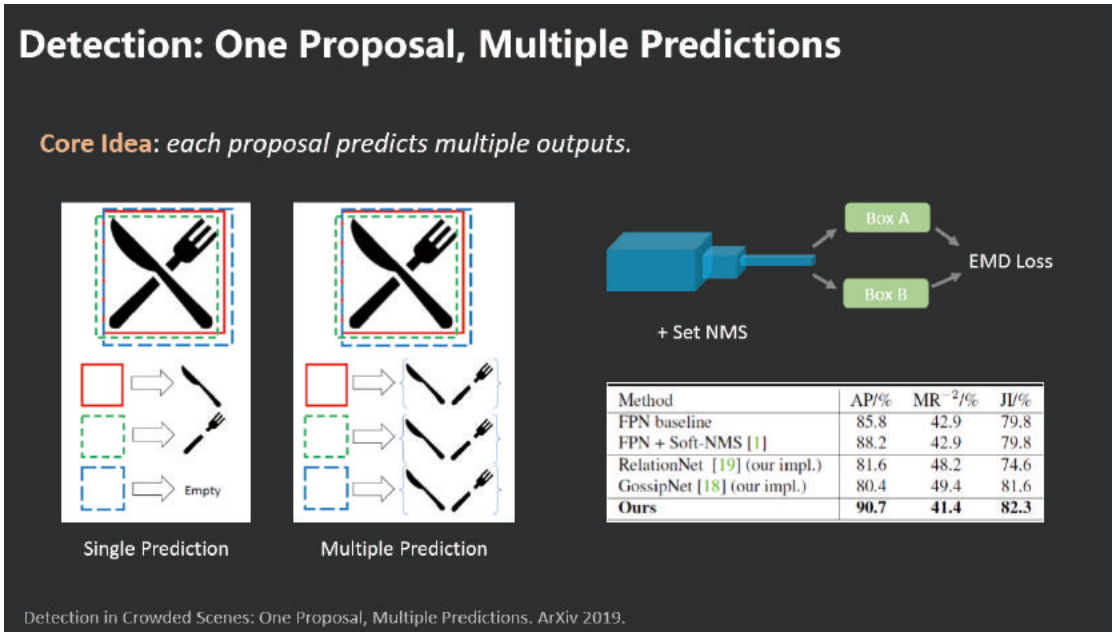


图 22：如何检测出多个预测

另外，值得一提的是，针对物体检测领域一个非常困难的问题——遮挡问题，孙剑团队在 CVPR2020 上提出一种模型 [19]，能够通过 1 个检测框预测多个物体，完美解决上图中的刀叉重叠问题。对此孙剑表示：“做好计算机视觉不仅仅是用深度学习这么简单，深度学习只是一个工具，面对具体问题的时候研究人员需要更好的理解问题、更好的建模，才能够把问题解决。”

五、机器视觉应用中的核心难点

在报告的最后，孙剑对于当前计算机视觉应用落地过程中存在的多个关键性问题，进行了总结:

1. **长尾分布问题 / 小样本问题**。因为机器学习方法并不能保证对很稀少的样本进行准确的分类，这也是人工智能之所以和大家期望有差距的核心原因之一。
2. **自监督学习**。背后的原因是标注训练样本太少，是不是可以通过没有人工标注的大量数据进行学习？如何通过定义自监督任务学习很好的特征，这是非常有希望的方向。
3. **遮挡问题**。虽然解决遮挡问题的方法有了一些进展，还是有很多问题需要解决。
4. **视频中做物体检测、跟踪的关联问题**。当前帧的物体和下一帧的物体如何能够关联起来？例如给定几辆车，如何在视频中跟踪几辆车，这个目前人工能力远远超过算法能力，在实际视频分析中非常有用。
5. **视觉控制问题**。尤其是在机器人这个领域，即不但要获取视觉信息，还要控制另外一个装置做一些行动，能和物理世界进行交互。
6. **极高精度的深度学习**。深度学习精度虽然很高，但是有些场合要求非常高的精度，那么怎么把它使用起来，依然值得研究。

Reference

[1] Shufflenet: An extremely efficient convolutional neural network for mobile devices. CVPR, 2018.

[2] ShuffleNet V2: Practical Guidelines for Effcient CNN Architecture Design. ECCV, 2018.

[3] Conditional Convolution via Channel-Wise Mixture. ArXiv, 2019.

[4] Neural Tangent Kernel: Convergence and Generalization in Neural Networks. ArXiv, 2018.

[5] Reconciling modern machine learning practice and the bias-variance trade-off. ArXiv, 2019.

[6] MetaPruning: Meta Learning for Automatic Neural Network Channel Pruning. NIPS, 2019.

[7] Resizable Neural Networks, 2019.

[8] Single Path One-shot Neural Architecture Search with Uniform Sampling. Arxiv, 2019.

[9] Spherical Motion Dynamics of Deep Neural Networks with Batch Normalization and Weight Decay. ArXiv, 2020.

[10] Rich feature hierarchies for accurate object detection and semantic segmentation. 2013.

[11] Spatial Pyramid Pooling in Deep Convolutional Networks for Visual Recognition. TPAMI, 2015.

[12] Faster R-CNN: towards real-time object detection with region proposal networks. NIPS, 2015.

[13] SSD: Single Shot MultiBox Detector. ECCV, 2016

[14] You only look once: Unified, real-time object detection. CVPR, 2016.

[15] Focal loss for dense object detection. CVPR, 2017.

[16] Densebox: Unifying landmark localization with end to end object detection. ArXiv, 2015.

[17] FCOS: Fully Convolutional One-Stage Object Detection. ICCV, 2019.

[18] MegDet: A Large Mini-Batch Object Detector. CVPR, 2018.

[19] Detection in Crowded Scenes: One Proposals, Multiple Predictions. ArXiv, 2019.

17 决策智能

清华大学张崇洁：高效协作的多智能体强化学习前沿研究进展

整理：智源社区 窦勇强

在第二届北京智源大会“决策智能”专题论坛上，来自清华大学交叉信息研究院的张崇洁助理教授以“*Efficient Collaborative Multi-Agent Reinforcement Learning*”为题进行了演讲报告。

张崇洁，于 2011 年在美国麻省大学阿默斯特分校获计算机科学博士学位，而后在美国麻省理工学院从事博士后研究。目前的研究专注于人工智能、深度强化学习、多智能体系统、以及机器人学，担任清华大学交叉信息科学院助理教授，博士生导师，机器智能研究组主任。

过去几年人工智能得到了很大的发展，机器学习特别是深度学习方面在实际问题上的应用使人工智能受到了极大的关注。然而随着人工智能应用的不断广泛化和复杂化，使得研究者对人工智能提出更高的需求。研究趋势也从简单的模式识别到更加复杂的智能决策与控制，从单研究智能体的问题，过渡到解决多智能体的问题。

在本次演讲中，张崇洁系统讲述了高效协作的多智能体强化学习研究的前沿进展。他抽丝剥茧般回顾了当前多智能体学习存在的挑战，通过引入通信和角色的方式逐步解决挑战达到最佳性能水平的研究历程。此外，张崇洁通过理论分析工作展望了对未来多智能体强化学习研究的趋势性看法，见解独到，相信会给大家带来很多启迪。

演讲正文:

一、多智能体强化学习简介 [1]

研究者通常把具有感知和决策的能力的个体称为智能体 (agent)。智能体基于它的感知，可以做出相应的决策以及行动来改变周围的环境，多个智能体可以通过协作式的行为实现一个整体的目标。例如，在机器人集群控制中，每一个机器人就可以看作一个智能体；在一个风力发电场，每一个风机就可以看作一个智能体。

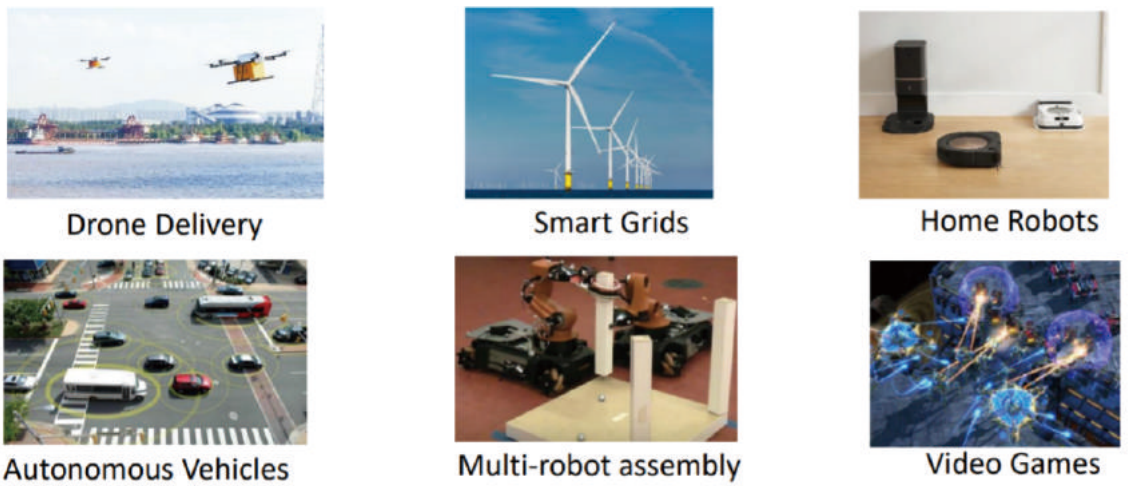


图 1：人工智能愈加复杂的应用场景

多智能体学习的问题可以分为三类：协作式多智能体，对抗式多智能体，以及混合式多智能体。其中，协作多智能体是一群智能体通过协同合作，来共同来优化整体目标的行为。

在大多数协作式多智能体问题中，环境往往是部分可观察的 (partially observable)：每个智能体只能观察环境的部分信息，而且环境的变化会存在一些随机性。这样一类复杂的多智能体协作决策问题，可以用一个较为通用的模型来刻画——部分可观察的 Markov 决策过程（Dec–POMDP）。

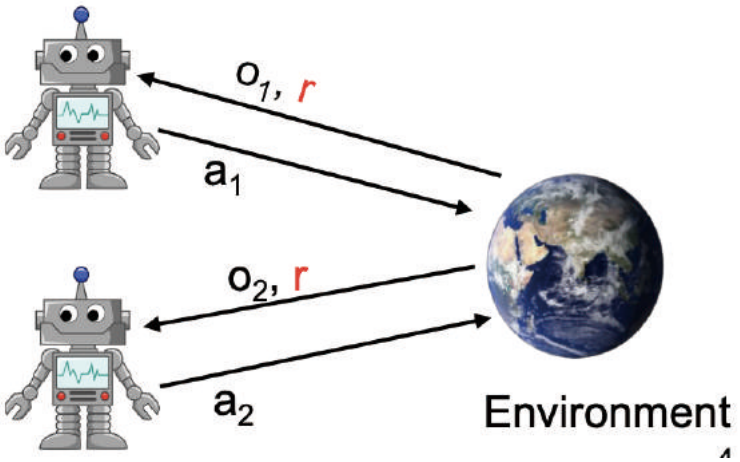


图 2：协作式多智能体模型 Dec–POMDP

Dec–POMDP 决策过程是非常通用的，它可以刻画大部分在不确定环境中多智能体决策的问题。从一种简单的角度来看，可将它视为把单个智能体的 Markov 决策过程过渡到多智能体的环境中。模型的运作方式如图 2 所示，在这个环境有两个机器人，在每一时刻，每个机器人都会根据它当前的感知输入选择某一个动作，执行这个动作之后将会改变环境中某一部分的状态。在这之后机器人通过进一步观察环境，得到新的观测。尽管每个机器人可能会有不同的观测信息，但它们会得到同一个反馈信号。因为这里整体的假设是协作式多智能体的范围，所以这个反馈称为联合的报酬 (joint reward)。在这类协作式多智能体问题中，研究者希望找到一组决策策略，使得智能体根据这个决策策略来执行它们的行动的时候，可以收获最大化的期望累计报酬。

- Objective: to find policies for agents to maximize expected cumulative rewards
- A local policy π_i for each agent i: mapping its observation-action history τ_i to its action
  - State is unknown, so beneficial to remember the history
- Joint policy $\boldsymbol{\pi} = < \pi_1, \ldots, \pi_n >$
- Value function: $Q_{tot}^{\boldsymbol{\pi}}(\boldsymbol{\tau}, \boldsymbol{a}) = \mathbb{E}\left[\sum_{t=0}^{\infty} \gamma^t r_t \mid s_0 = s, \boldsymbol{a}_0 = \boldsymbol{a}, \boldsymbol{\pi}\right]$
- Policy $\boldsymbol{\pi}(\boldsymbol{\tau}) = \text{argmax}_{\boldsymbol{a}}\, Q_{tot}^{\boldsymbol{\pi}}(\boldsymbol{\tau}, \boldsymbol{a})$

图 3：Dec–POMDP 形式化定义

这里寻找的决策策略，是指在前文定义的分布式 – 部分可观察的马尔可夫决策过程 (Dec–POMDP) 中，寻求一个映射关系，对每一个智能体把它的局部观察的历史映射到一个动作 (action) 上。而在 Dec–POMDP 的定义下，全局的环境状态是不可直接观测的。智能体往往需要记住一些历史的信息来辅助今后更好的决策。决策策略又称“联合策略”，所谓的联合策略是智能体策略的集合。为了更好的描述和解决多智能体决策的问题，研究者定义了一个值函数 (Q value function) 来量化任务中的执行目标，这个值函数是折扣的未来累计期望收益和 (Discounted future cumulative reward)。对给定一个任务如果能够学习出相应的值函数的话，那么智能体的最优联合策略也就相应得到。最优策略，可以直接从值函数中推导出来，即相对于行为变量 a (action) 取参数最大化 (argmax) 的结果。因此，求解协作式多智能体的 Dec–POMDP 问题，有两种途径：①直接学习一个最优的策略来最大化智能体的值函数（累积回报）；②学习出智能体的行为值函数，从值函数中推导出一个最优的策略。

在许多实际问题中，环境往往是非常复杂的，同时无法预先知道环境的模型。在这种情形下，愈加能够体现出强化学习的优势——不断试错：当环境不可知时，可以采用智能体与环境不断交互和探索的方式，在这个过程中建立关于环境的模型，进而进行动作的规划；也可以在环境学习奖励规则，在交互中直接学习智能体的策略。每个人的生活中都有强化学习的影子，在完成一个新的目标时，我们无法预先知道每一步该怎么走，而往往会有走完一步之后发现是好还是坏的反馈。人类学习的过程就是根据这种反馈信号来反思自己做出的行为，进而更好地面对未来的类似的场景。当后面遇到类似的情形时，一般会有两种做法：分析之前发生的类似经历，选择之前反馈最好的那个行为进行执行；同时可以尝试之前没做过的行为，如果新的动作比我们已知期望的回报要好，那今后就会要多做一些，如果比我们期望差，那么今后就会少做类似的行为。强化学习将这种试错 + 探索的方式，通过在贪婪选择目前已知的最优策略的算法中添加随机性来实现人类中学习的思想。

多智能体强化学习是在单智能体的基础上扩展到多个智能体的试错学习：在单智能体学习中，为单个智能体学习一个策略；多智能体学习则会选一组策略（也成为联合策略）为多个智能体服务。同时，在多智能体中一般有智能体之间是相互交互影响的而非完全独立的约束条件。在协作式多智能体中，智能体间的交互可以通过报酬来反映，每一个智能体的动作都会影响整体的报酬。那么，多智能体强化学习如何应用到多智能协作问题？又如何去学习最优的联合策略或者值函数呢？

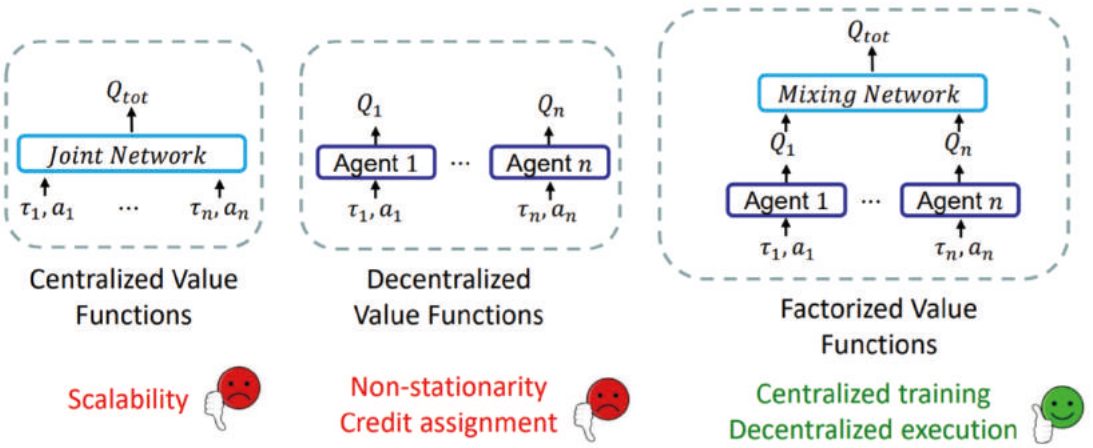


图 4：多智能体强化学习的三种范式

第一种方式是中心化的训练方法，将所有的智能体观测以及动作作为输入，建立一个联合的神经网络来输出联合值函数的函数值。中心化的方式存在的问题是： 不具有扩展性。在训练中观测空间是指数级增长的，即使神经网络表达形式特别强，可以学到这种映射关系，在执行过程中也会遇到通信的困难，要实时的去收集所有智能体的观测，做出决定之后再分配给所有智能体相应的决策动作。另外一种方式是分布式学习，每一个智能体有自己的网络，来实现学习的可扩展性。但分布式学习的问题在于当智能体在一个环境中共同学习的时候，环境成为非稳态的 (non-stationary)，不具有收敛性和最优性。另一个困难是不能很好地分配智能体获得的联合奖励，即信度分配 (credit assignment)。 因此，更好的方法是将这两种方法合并，称为可分解价值函数学习方法： 每个智能体都有其自己的行为价值网络或策略网络，并通过混合网络输出联合的实际价值。在这种情况下，每个智能体有分解的值函数也有共同的值函数。在执行过程中，每个只用仅仅通过个体的值函数或策略网络进行决策。 因此，它具有很好的可扩展性的同时解决了一些分布式学习问题，介于中心化训练和分布式学习两种方式之间的一种较好的学习范式。在具体的实现过程中，通过时间差分学习 (TD-learning)，将环境的反馈信息进行反向传播 (back propagation) 影响和更新每一个智能体的值函数，以解决环境的非稳态 (non-stationarity) 和信度分配的问题 (credit assignment) 的问题。

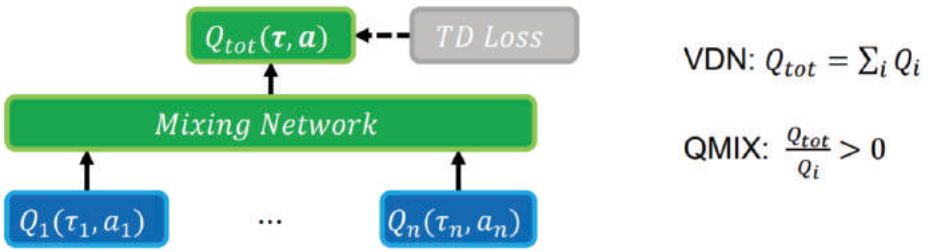


图 5：可分解的值函数学习范式（CTDE）

在中心化训练 – 分布式学习的范式之下，许多研究者提出一些结构约束假设的来实例化这种范式，其核心思想在于价值函数混合网络 (Mixing Network) 的确定。2017 年，领域研究者提出了价值分解网络 Value Decomposition Network (VDN)[2]，该方法通过简单求和的方式将智能体局部价值函数整合为联合价值函数。这种方式简单有效，但是限制了对于联合价值函数 Q_{tot} 的表达能力。

在此基础之上，研究者将 VDN 的较强假设进行了松弛，提出 QMIX[3]，它只假设总体的报酬对于个人报酬的偏导是大于零的。这样每个人提高自己的报酬就可以提高整体的报酬，以这样的方式实现 CTDE 范式。这一系列工作中，研究者提出了不同的假设来设计联合价值网络 (Mixing Network) (图 5 绿色部分) 进行中心化训练。同时在分布式执行过程中，把联合价值网络去掉，智能体通过自己的局部价值网络进行决策 (图 5 蓝色部分)，从值函数中推导得到相应的策略，来进行分布式执行。目前基于这种值分解的方法，在多智能体强化学习上取得一些前沿的一些结果，例如在星际争霸 2 的微操作游戏任务中，能学到很多有意思的策略，如放风筝策略，一个狂热者打两个海军陆战队，传统上海军陆战队是打不过的，通过不停“拉仇恨”的方法，就可以打败比自己强大的狂热者。

图 6：智能体学习到的放风筝战斗策略

目前值函数分解方法在一些复杂的问题上还存在着局限性，张崇洁给出了三点重要的方面。其一，前述方法不能很好地处理不确定性。因为当智能体学到自己的策略时，所有智能体进行完全分布的执行，随着环境的不确定，比如说状态不确定性等等，智能体间的协作则会变得不协调（miscoordination）。随着时间的推移，由于不能很好处理中环境的不确定性，这种不协调会得到积累进而导致较大的问题。此外，由于智能体间网络参数的共享（共享子网络或策略网络），目前的方式不能解决比较复杂的问题，智能体的行为趋向于单一化。即使参数共享的方式能够解决这样复杂的问题，也会导致庞大的网络的参数。此外，一些复杂的问题往往需要多样性异构智能体才能够解决。第三点，对这目前这些方法理论的分析，何时有效的理解有待深入。

针对上述三点挑战，张崇洁带领的团队近期进行了三方面的工作来解决。第一方面，通过通信优化的方式来解决不确定性的问题； 第二方面，通过这种角色涌现的方式来解决智能体参数动态共享的学习过程； 第三方面，关于线性值函数分解的理论分析工作。

二、引入最小化通信的多智能体协作 [4]

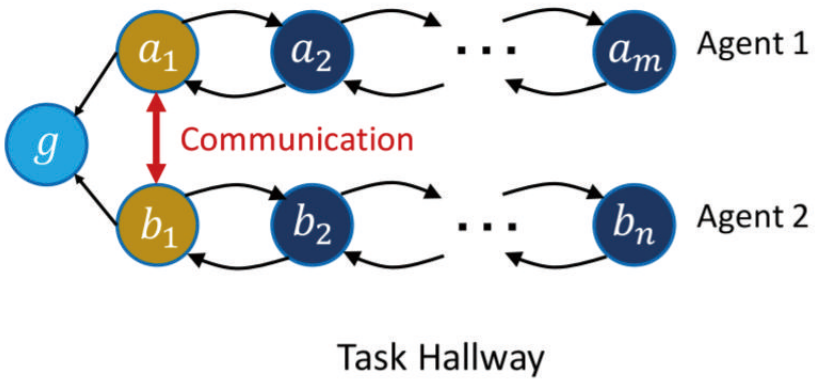


图 7：完全值函数分解存在的缺陷

图 7 中展示了完全值函数分解方法存在的缺陷，在该例中，有两个智能体分别位于长度不同的通道中，其中 a1 是智能体 1 所在通道出口的位置，b1 是智能体 2 的通道出口位置。当两个智能体同时到达通道出口目标 g 的时候，会收到一个报酬。如果两个智能体在不同的时间点到达目标 g，则不会收获报酬。假设初始状态是随机的，每个智能体初始位于不同的位置。由于智能体部分可观察的特性，即使中心化的训练方法表达能力非常强，最终两个智能体也只会以很小的概率同时到达收获报酬，因为智能体在执行的时候行为是完全确定的，向左走或者向右走，而互相不知道对方的初始位置，并且智能体间没有通信的交流，导致了之前的研究工作无法完成这类任务。如果考虑加入智能体间的通信交流，只要任意一个智能体快到达目的地之前，就是告诉其他智能体这个信息。并且等待接收对方同样到达目的地之前的信息，最后同时执行到达目标 g 来解决这个问题。

通信的加入可以解决此问题，但是这种通信不是长期需要的，比如说智能体 1 在位置时，无需进行通信向另一个智能体通报自己的位置。只有在离目标 g 最近的位置处进行通信的协调就可以，所以张崇洁团队提出在允许通信的同时需要最小化通信量。该方法称为近似可分解的值函数（NDQ）算法（图 8），该算法解决智能体通信的时间、内容以及通信对象的问题。

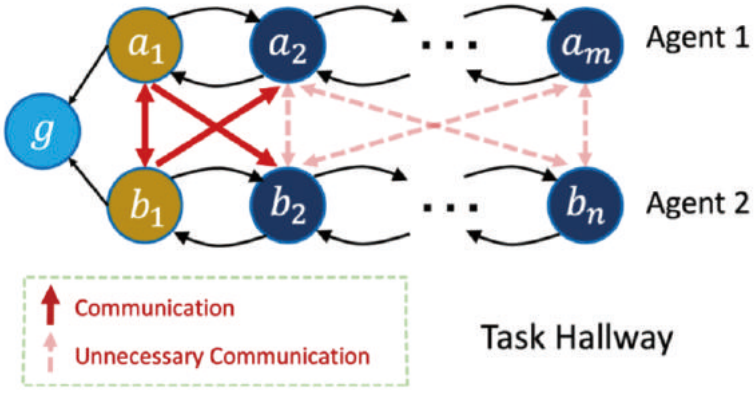


图 8：近似可分解的值函数方法 NDQ 解决的问题图解

NDQ 的框架如图 9 所示，传统值函数分解的结构下，每个智能体有自己独立的函数空间，基于智能体的局部观测历史进行优化。而 NDQ 则再此基础上进行改进，允许智能体之间可以相互发信息，智能体的策略不仅仅基于局部观察，还基于它收到的通信信息。

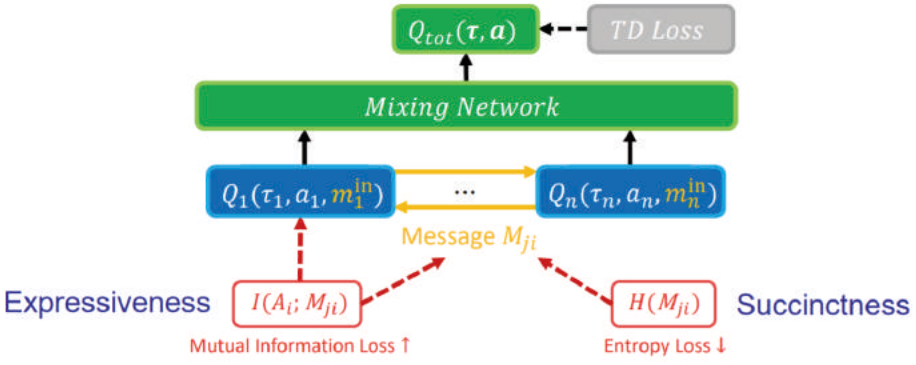


图 9：NDQ 算法框架结构图

然而，如果每个时间步，所有智能体之间都互相通信，则会变成了中心化的过程，不具有扩展性且浪费通信资源。因此，在该工作中，张崇洁团队加入两个约束条件来优化通信：①首先是通信消息的表达性约束，即希望这个智能体发送方到接收方之间发送的消息一定是对于接收方有帮助的，该约束通过最大化通信内容与智能体决策之间的互信息来实现。②信息简洁性约束，即尽最大努力缩小和减少信息的熵 (Entropy)，如果一条信息没有用，数值上的表现是 Entropy 很小，也就代表发送该条信息是没有必要的。因此通过两个约束，一是最大化互信息，二是最小化信息熵，保证了智能体之间的通信的简洁和有效。在实际实现中，无法直接优化这两个目标函数，所以通过借鉴变分推断中的思想，推导出了相应的变分下界来支持实际优化，有关具体推导过程感兴趣的读者可以参考 [4] 中附录。

- By deriving variational lower bounds, we get the equivalent communication loss:

$$L_c = \mathbb{E}_{M_j^{in},\mathrm{T}_i}[\mathcal{CE}[p(A_j|\mathrm{T})\|q_\xi(A_j|\mathrm{T}_j, M_j^{in})] + \beta D_{KL}[p(M_{ij}|\mathrm{T}_i)\|\mathcal{N}(0,1)]]$$

- Overall loss:

$$L = L_{TD} + L_c$$

图 10：NDQ 推导的优化目标函数

如图 10 所示，最终 NDQ 算法通过两个目标函数的结合进行端到端训练：第一个是训练混合网络的强化学习中常用的时间差分损失 TD loss，第二个是对于信息的通讯约束损失 communication loss。

在简单和复杂的任务中，NDQ 都表现出了非常优异的效果。首先，是传统完全值分解方法不能够解决的 Hallway 任务，NDQ 能够很好的学到最优策略。如图 16 所示，初始 t=1 时智能体在左 1 图中黄色的两个位置，此时由于它们没有到达通道出口，智能体间无需通信，NDQ 算法学习到了这个特征，因此此时没有信息的交流。这种不需要通信的状态持续到智能体 2 到达出口 b1 的时候，会向智能体 1 发送消息告知它已经到达出口 b1 的信息。最终当智能体 1 也到达对应的出口 a1 时，同样发送信息给智能体 2。因此 NDQ 算法在这个任务中学到了最优的策略。为了验证 NDQ 算法在复杂环境上的有效性，他在星际争霸 II 微操作管理的任务上同样进行了实验，本文主要显示六个实验结果（测试基准 Benchmark 是由牛津大学的团队提出，感兴趣的读者可以访问网站 https://sites.google.com/view/ndq 查看更多的实验结果。）

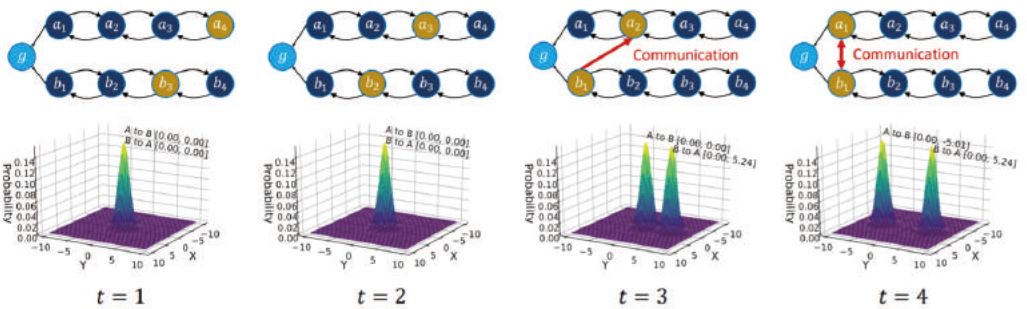


图 11：Hallway 任务中 NDQ 算法的表现结果

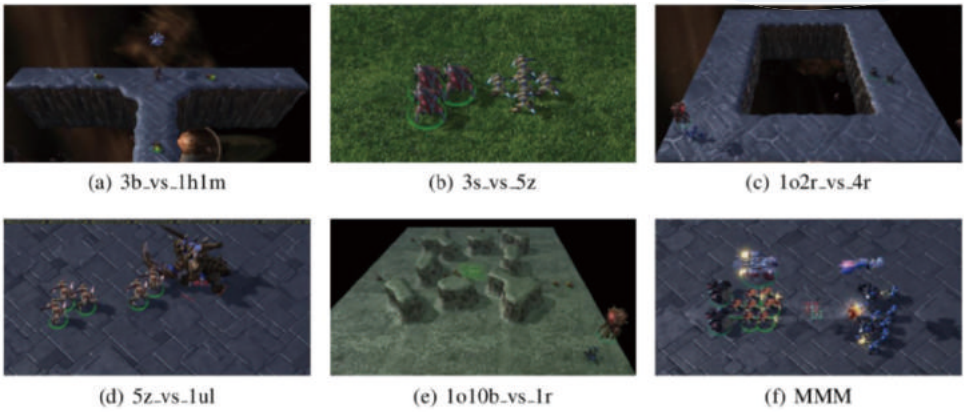


图 12：星际争霸 II 微操作管理实验 (https://sites.google.com/view/ndq)

实验的基线系统（baseline):

- QMIX[3]，完全值分解方法的代表实例。
- TacMAC[5]，基于注意力机制的通信的算法。
- 自行实现的 QMIX 与 TacMAC 的结合算法，测试 NDQ 的表现情况。

实验结果分析：TacMAC 是一个中心化的学习方法，它几乎在所有的复杂环境下都不能学习到好的策略；QMIX 在一些复杂环境中的表现不是很好； 当为 QMIX 增加通信的 Tarmac 算法时 , 性能表现有提高，但是与所提出的 NDQ 相比还是有一定的差距。基于注意力机制 Tarmac 算法的通信学习方法是一种软约束的学习方法，而 NDQ 则是显式地进行优化学习，能够很大程度提高和解决通信的优化问题。当对于通信进行剪切 (communication cut) 时，即将 80% 的通信信息进行丢弃时，接近可分解的值函数 NDQ 方法几乎没有受到影响，而对于基于注意力机制的 TacMAC 方法，则不能鲁棒应对信息丢失的环境的影响。

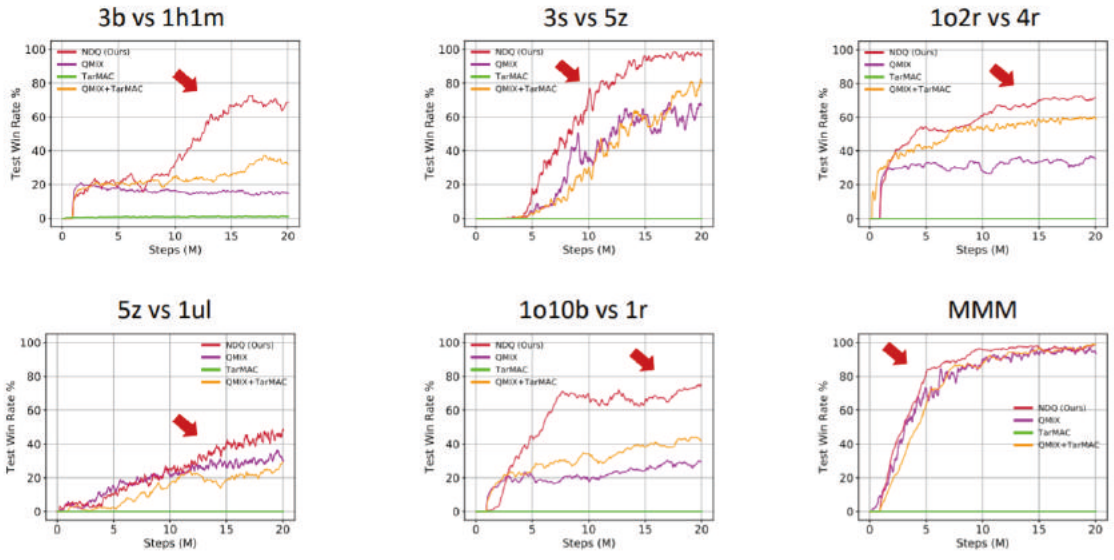


图 13：在星际争霸 II 中无信息丢弃的条件下的实验结果

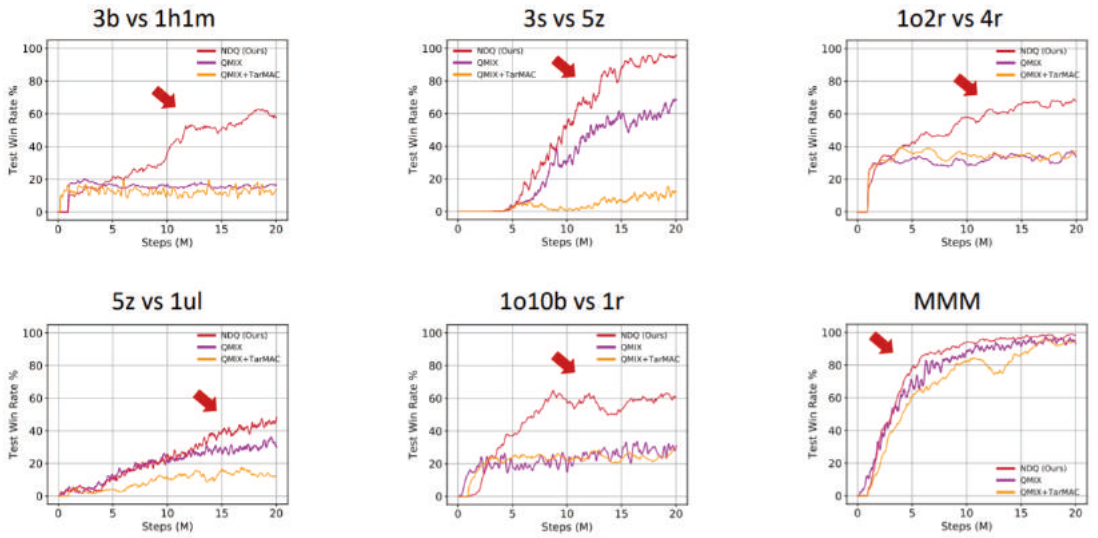


图 14：在星际争霸 II 中 80% 信息丢弃的条件下的实验结果

三、基于角色的多智能体强化学习 (Role-based)[6]

NDQ 算法通过通信的方式解决多智能体在执行过程中不确定性，本节的工作则是介绍通过如何通过基于角色的方式，来加速多智能体的学习。为什么需要动态的共享学习呢？原因是在很多复杂问题中，需要智能体有多样化的行为，或者甚至智能体本身必须为异构，即不能共享参数，因为不同功能的智能体不适合采用一个网络来表达。

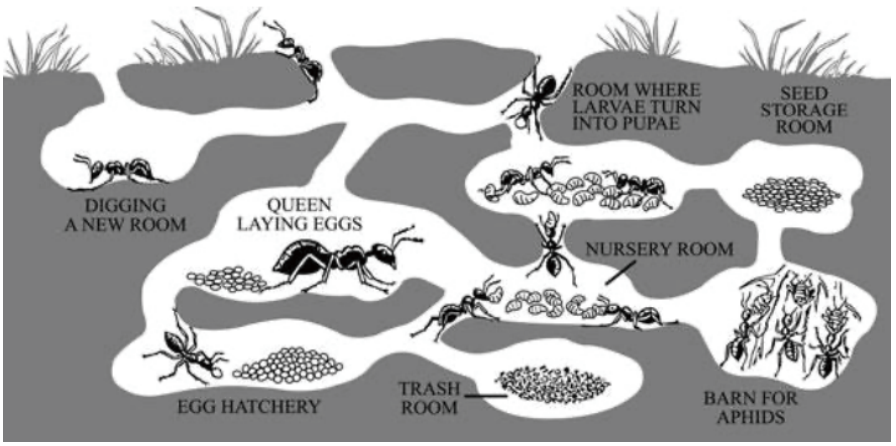


图 15：蚁群中不同蚂蚁有不同的角色

在现实生活或者自然界中有很多这样的情况，比如蚁群中不同蚂蚁有不同的角色，每个角色由不同的蚂蚁来执行——挖洞、寻找食物、搬运食物、清理垃圾、以及专门下蛋的蚂蚁 Queen。如果用一个网络来学上述所有行为，则需要通过全局搜索的方式学习一个很大的网络。学得智能体的行为多样性则会受限于网络的大小，过小的网络不能解决复杂的问题。与此同时，另一种方式是为每一个智能体学习一个独立的价值网络或者策略网络，这种方式也存在缺陷，因为智能体间或多或少可以通过共享个体学习到的一些知识来加速整体的学习。特别是在一些大型系统中，并不是每一个智能体都完全不同。因此，他的团队提出一种基于角色的多智能体强化学习

方法。他的基本思想是，如果智能体在任务中承担类似的角色，就分配类似的决策策略，从而共享智能体间学习的经验。而类似的决策策略意味着智能体在执行类似的子任务，它们将展现类似的行为。

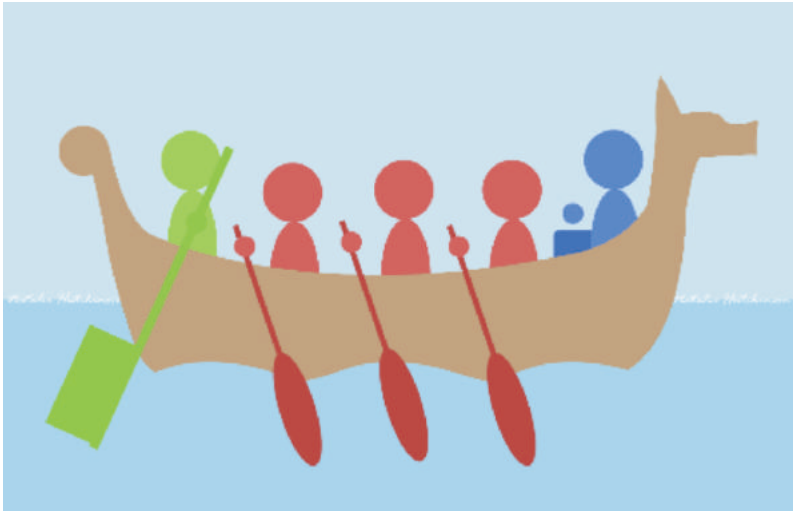


图 16：划龙舟，基于角色涌现的多智能体强化学习

可以从一个简单的示例理解动态共享参数的原因，以划龙舟为例（图 16），其中有三种角色，掌舵者，船员以及协调敲鼓者。显然，划船的船员策略高度一致，所以可以分享他们的学习经验。而掌舵者其他人策略是很不一样的，所以不一定需要有经验的分享。划龙舟的角色划分例子引入了人类的先验知识，但是解决很多问题之前，无法预先获知需要的角色，也无法划分相应的角色给不同的智能体，张崇洁的团队针对这个问题给出了一种巧妙的解决方案 ROMA（Multi-Agent Reinforcement Learning with Emerging Roles）。首先由于这些角色的非预定义性，设计的算法要能够自动学习出所需要的角色。具体的做法是通过推理的方式，根据智能体的行为推理它之前相应的角色是什么。每一个智能体的策略由他的角色所决定。如果智能体角色相同，那么它们的策略也相同； 如果角色不同，那它们的策略也会不同，这样就达到动态共享的一种方式。当然，智能体的角色不是一成不变的，一个智能体可以根据环境的不同来动态改变它的角色。

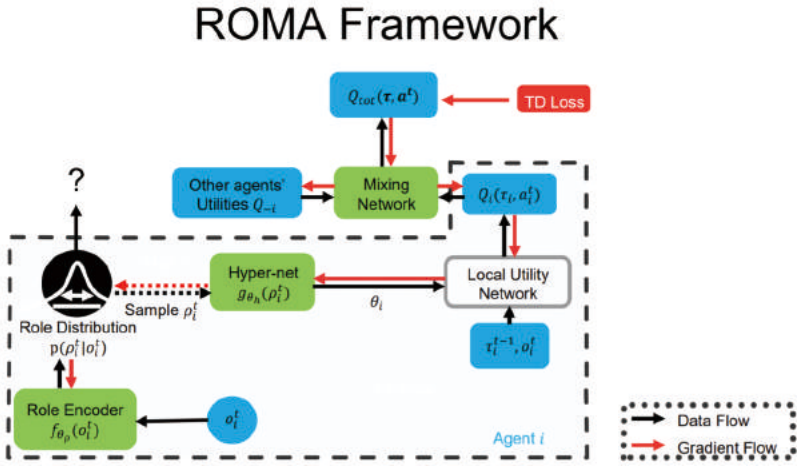


图 17：基于角色的多智能体学习框架 ROMA

ROMA 的框架如图 17 所示，在执行过程中，智能体 i 通过一个编码器把它的观测编码到一个随机的隐空间中，然后在这个角色的隐空间中进行采样，采样出当前智能体需要的一个角色。通过 Role Decoder 解码器（一种超网络 hyper network），解码输出智能体的局部效用函数的参数。该效用函数的输入为历史信息和当前智能体的观测，输出为该智能体的值函数 Q value，每一个角色都对应着智能体的每一种策略。训练过程中，每一个智能体把他们的局部值函数 Q value 输入到一个混合网络中（Mixing Network），该混合网络输出全局联合价值（Total Q value），这样可以通过时间差分 TD 的方式进行训练。

- We propose two regularizers to enable roles learning
- Identifiable by its behaviors (trajectory, role, observation)
  - Maximizing mutual information $I(\tau_i; \rho_i | o_i)$
- Capable of clustering agents
  - Either agents have similar roles;
  - Or they have different behaviors, which are characterized by the local observation-action history.

图 18：角色学习中的两个正则器 (Regularizer)

但是简单按照上述的做法很难学到较优的策略，为了保证学得的角色在空间上是有意义的，需要施加一定的约束条件。具体包括两个方面，一是角色跟它的行为的相对应性，一个角色对应某一类的行为，通过最大化角色在隐空间中的参数以及角色的经历（trajectory）二者的互信息实现；二是角色可以区分不同智能体的行为，如果智能体的行为类似，应该将它们的角色在隐空间中聚在一起，需要分化聚类的功能，不同智能体要么承担相同的角色，要么具有不同的行为。

- To formalize this idea
  - Introduce a learnable dissimilarity model d_ϕ
  - For agents, i and j, seek to maximize $I(\tau_j; \rho_i | o_j) + d_\phi(\tau_i, \tau_j)$
  - Minimizing the number of roles by minimizing $\|D_\phi\|_{2,0}$, the number of non-zero elements in $D_\phi = (d_{ij})$, where $d_{ij} = d_\phi(\tau_i, \tau_j)$
- The clustering loss:

$$\mathcal{L}_D(\theta_\rho, \xi, \phi) = \mathbb{E}_{(\boldsymbol{\tau}^{t-1}, \boldsymbol{o}^t) \sim D, \boldsymbol{\rho}^t \sim \rho(\cdot | \boldsymbol{o}^t)} \left[\left\| D_\phi^t \right\|_F - \sum_{i \neq j} \min\{ q_\xi(\rho_i^t | \tau_j^{t-1}, o_i^t) + d_\phi(\tau_i^{t-1}, \tau_j^{t-1}), U \} \right]$$

图 19：角色可聚类的损失函数

因此，整个损失函数由三方面组成，一是训练混合网络的 TD Loss，二是可区分角色的 Identifiability loss，三是不同智能体聚类的 Clusterability loss。

$$\mathcal{L}(\theta) = \underbrace{\mathcal{L}_{TD}(\theta)}_{\text{TD Loss}} + \lambda_I \underbrace{\mathcal{L}_I(\theta_\rho, \xi)}_{\text{Identifiability}} + \lambda_D \underbrace{\mathcal{L}_D(\theta_\rho, \xi, \phi)}_{\text{Clusterability}}$$

图 20：ROMA 整体的优化目标

实验结果表明，在具有挑战性的星际争霸 2 微操作管理任务中，ROMA 在越复杂的环境下表现地越突出，例如，在 27 vs. 30 个海军陆战队的场景中，智能体需要具有非常好的微操作才能以少数赢多数。在比赛初期，智能体大致采用相同的角色分布，而后期会根据血量的多少来承担不同的角色。

智能体的角色是动态的，在初期智能体会根据所处的位置选取角色，比如站在前、中、后的智能体将会具有不同的角色。角色相近的智能体随着打斗的过程中血量的变化承担新的角色，例如血多的向前冲，血少的向后退。

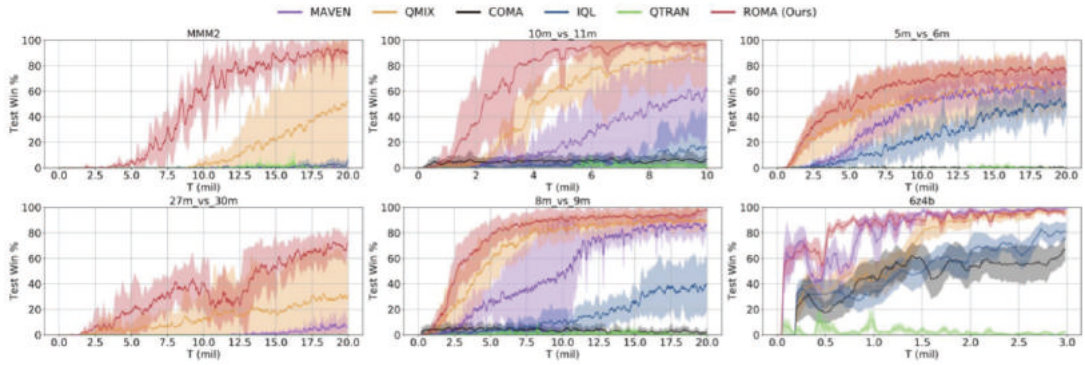


图 21 ROMA 在星际争霸 II 微操作管理挑战上的实验结果（https://sites.google.com/view/romarl）

图 21 和 22 展示了 ROMA 在星际争霸 II 微操作管理挑战上的实验结果，学习阶段初期时，智能体在探索不同的角色，随着学习越来越深入，角色功能的分化也会越来越好。因此角色和学习的过程是一个相互反馈的交互过程。上面是同构的情况，在异构的情况下也是相同，能够学出不同的角色，智能体的功能不同，角色也会不同。

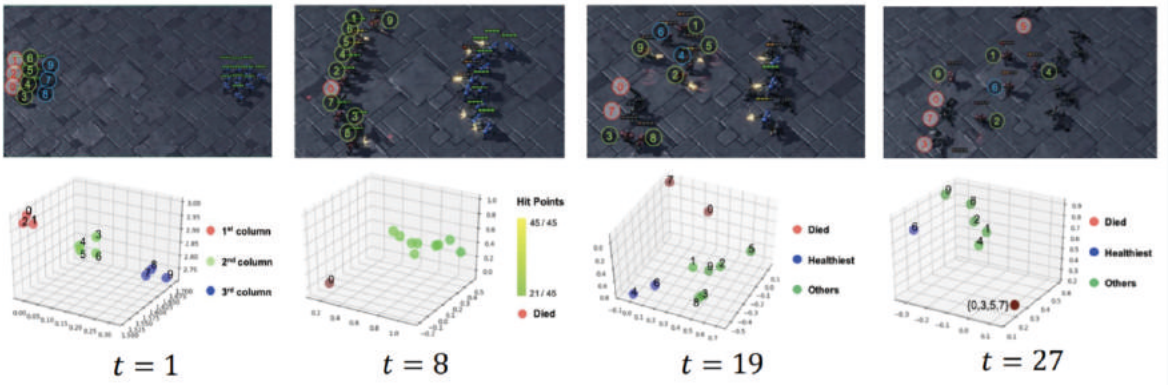
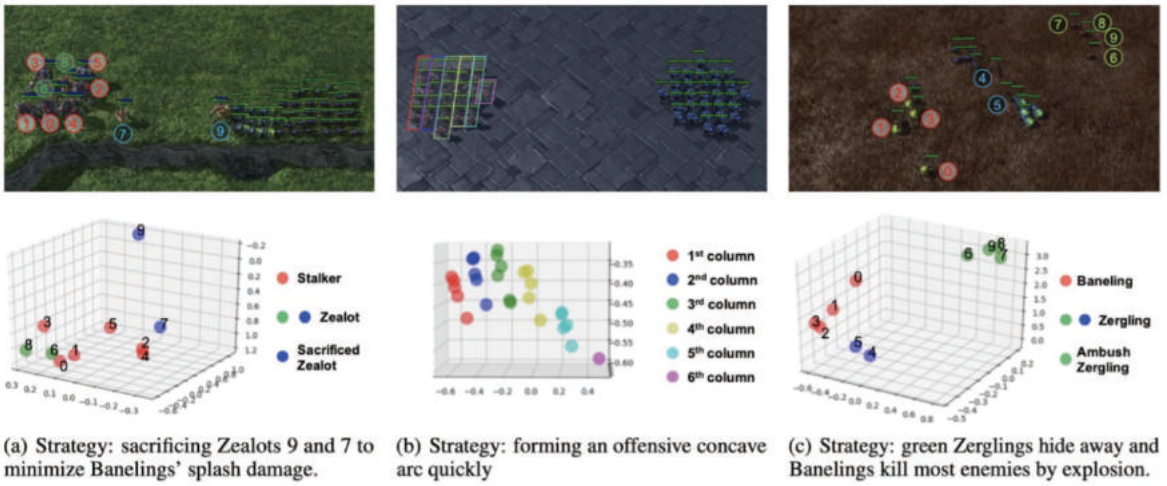


图 22：动态角色学习图解



(a) Strategy: sacrificing Zealots 9 and 7 to minimize Banelings' splash damage.

(b) Strategy: forming an offensive concave arc quickly

(c) Strategy: green Zerglings hide away and Banelings kill most enemies by explosion.

图 23：几个 ROMA 角色学习中令人兴奋的示例

总结前两项工作在多智能体强化学习研究中的位置，如图 24 所示，协作式多智能体主要由两个方面刻画。

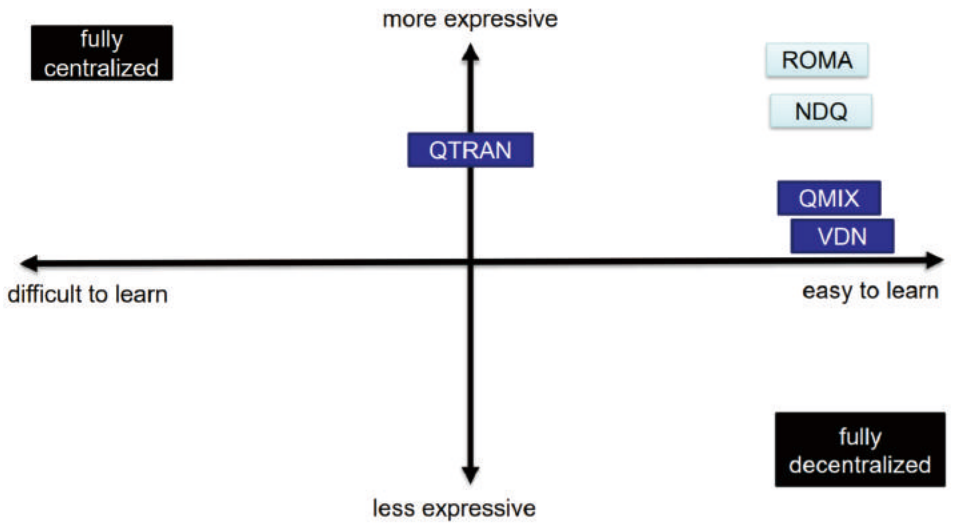


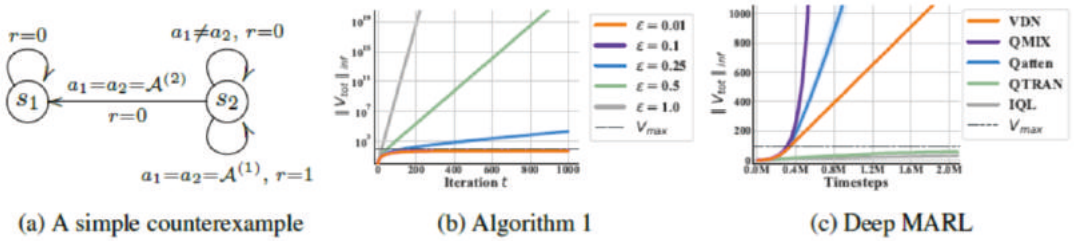
图 24：协作式多智能体研究工作总览

一个是方法学习的难易度；另一个是方法学习得到的效果，即表达最优策略的效果。显然完全中心化的学习方式 (Fully centralized)，具有很强的表达能力，但同时较难学习。而完全分布式的学习方式 (Fully decentralized)，具有较弱的表达能力，但是较为容易学习。在它们中间值函数分解 (Value factorization) 的方法，具有折中的表达能力以及中等的学习难度，从表现上讲相较于完全分布式的学习方式要好得多。上述介绍的接近可分解的值函数算法 NDQ 通过增加通信的方式具有更强的表达能力，而学习的难度相较于值函数分解的算法 (如 QMIX) 也相差无几。同时，基于角色的多智能体学习 ROMA 算法则有更多的多样性。

四、线性值函数分解的理论分析工作以及 Offline RL[7]

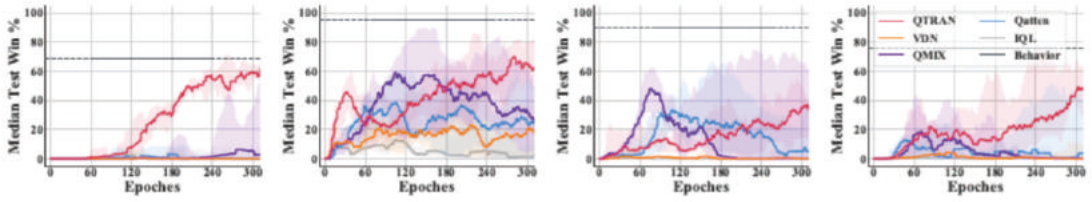
最后一节介绍张崇洁团队在线性值函数分解方面的理论分析工作，在该工作中意图解决的问题是：为什么多

智能体学习值函数的分解的算法（如 VDN,QMIX）能够取得不错的效果？在该工作中，他们设计了一个 Multi-agent Fitted Q-iteration 的理论框架，将单智能中研究函数近似（Function Approximation）下算法的收敛性以及最优性的表现的 Fitted Q-iteration 框架扩展到了多智能体领域（Multi-agent fitted Q-iteration）。从中推导出了闭式的更新规则（closed-form update rule），即 Empirical Bellman error minimization，基于这个闭式解，他们发现简单的线性值函数分解方法（linear value factorization），例如 VDN 中的局部值函数求和得到联合值函数，基于这样简单的结构假设以及混合网络的训练，它们隐式地实现了一个非常好的信度分配（credit assignment），一种联合报酬分配的机制，称为反事实的报酬分配。具体来说，单个智能体自己的报酬，等价于假想做随机的动作得到的整体的报酬，与做最优的策略行为得到的报酬之间的差值，将这个作为行为值函数 Q value，是一种非常好的方式。在现实生活中，如公司评价一个员工的贡献也是类似的做法，由此解释了值函数分解方法在多智能体学习的任务中具有较好表现的原因，同时该工作也证明了在智能体 on-policy 训练过程中的局部收敛性。



(a) A simple counterexample　(b) Algorithm 1　(c) Deep MARL

图 25：反例的构造与收敛性实验



(a) 5m_vs_6m　(b) 2s3z　(c) 1c3s5z　(d) 2c_vs_64zg

图 26：值函数分解方法及分布式训练方法 IQL 在离线训练中的实验

尽管有特定条件下局部收敛性的证明（图 25），但是目前的工作缺乏全局的收敛性保证。此外，而且在采用不同的策略得到的数据训练（Off-policy）时，线性值函数分解算法表现的不尽如人意，无法从示例中进行学习（learn from demonstrations）。如在图 25c 的离线训练实验中，当前许多最好的算法的价值函数都无法收敛，会发散。在复杂的环境下（图 26），如果 data 先通过一个好的策略收集起来（实验采用 QMIX 收集），用收集的数据来进行训练的方法也没有效果，即使采用 QMIX 的得到数据训练同类 QMIX 智能体，也无法得到很好的表现，这与常识中单智能体 Q-learning 是一个离线策略训练的观念相违背，非常值得进一步的探索。

五、结语

多智能体强化学习是一个具有很大前景的研究领域，本次演讲中，张崇洁从协作式多智能体的角度分享了前沿的研究工作，包括通过值分解的方法与通讯优化方式结合实现多智能体合作，有效地解决多智能体任务中的不确定性问题；通过基于角色学习的方法，通过动态共享智能体的参数提升可扩展性，使得在非常困难的任务中

相对于最好的方法也有极大的性能提升。谈到领域未来的发展方向，他指出在环境允许的条件下，支持分层的学习具有较大的前景。同时，针对线性值函数分解算法的理论分析工作，表明了当前算法对于离线训练(off-policy training)需要有较大的关注。离线训练不仅具有较高的学习效率，同时可以利用已有的示例数据，如自动驾驶中的经验数据，来进行策略的学习。未来离线多智能体强化学习将会成为重要的组成部分。

参考资料

[1] J. N. Foerster, "Deep Multi-Agent Reinforcement Learning," p. 205.

[2] P. Sunehag et al., "Value-Decomposition Networks For Cooperative Multi-Agent Learning," arXiv:1706.05296 [cs], Jun. 2017, Accessed: May 29, 2020. [Online]. Available: http://arxiv.org/abs/1706.05296.

[3] T. Rashid, M. Samvelyan, C. S. de Witt, G. Farquhar, J. Foerster, and S. Whiteson, "QMIX: Monotonic Value Function Factorisation for Deep Multi-Agent Reinforcement Learning," arXiv:1803.11485 [cs, stat], Jun. 2018, Accessed: Mar. 13, 2020. [Online]. Available: http://arxiv.org/abs/1803.11485.

[4] T. Wang, J. Wang, C. Zheng, and C. Zhang, "Learning Nearly Decomposable Value Functions Via Communication Minimization," arXiv:1910.05366 [cs, stat], Oct. 2019, Accessed: May 23, 2020. [Online]. Available: http://arxiv.org/abs/1910.05366.

[5] A. Das et al., "TarMAC: Targeted Multi-Agent Communication," arXiv:1810.11187 [cs, stat], Feb. 2020, Accessed: May 25, 2020. [Online]. Available: http://arxiv.org/abs/1810.11187.

[6] T. Wang, H. Dong, V. Lesser, and C. Zhang, "ROMA: Multi-Agent Reinforcement Learning with Emergent Roles," arXiv:2003.08039 [cs], Mar. 2020, Accessed: May 08, 2020. [Online]. Available: http://arxiv.org/abs/2003.08039.

[7] J. Wang, Z. Ren, B. Han, and C. Zhang, "Towards Understanding Linear Value Decomposition in Cooperative Multi-Agent Q-Learning," arXiv:2006.00587 [cs, stat], May 2020, Accessed: Jun. 15, 2020. [Online]. Available: http://arxiv.org/abs/2006.00587.

清华交叉信息学院吴翼：多智能体强化学习中的课程学习、演化与复杂性涌现

整理：智源社区 熊宇轩

作为 ACM–ICPC 领域的传奇人物之一，昔日的「姚班」少年吴翼在加州大学伯克利分校取得博士学位之后，加入了 OpenAI 从事通用人工智能研究。近年来，他发表了以 MADDPG 为代表的一系列高水平研究成果。在本届智源大会上，吴翼博士带来了以「多智能体强化学习中的课程学习、演化与复杂性涌现」(Curriculum,Evolution and Emergent Complexity) 为题的主题演讲。吴翼博士从哲学的终极命题「我们从哪里来?」出发，介绍了涌现出复杂群群体行为的条件，并结合 OpenAI 近期完成的捉迷藏游戏项目进行了详细的说明。

下面是演讲正文，智源社区编辑做了一定的编辑整理。

一、物种进化的启示

本次演讲，我主要针对人工智能研究领域最重要的任务之一——「构建通用人工智能」进行讨论。为了实现这一最终的目标，我们已经在深度学习、强化学习、规划 / 推理、搜索等方面取得了许多令人备受鼓舞的进展。这些伟大的技术用到了与机器学习和优化方法有关的诸多概念。在本次演讲中，吴翼博士主要从受人类自身启发的新型人工智能研究的角度进行了深入探讨。

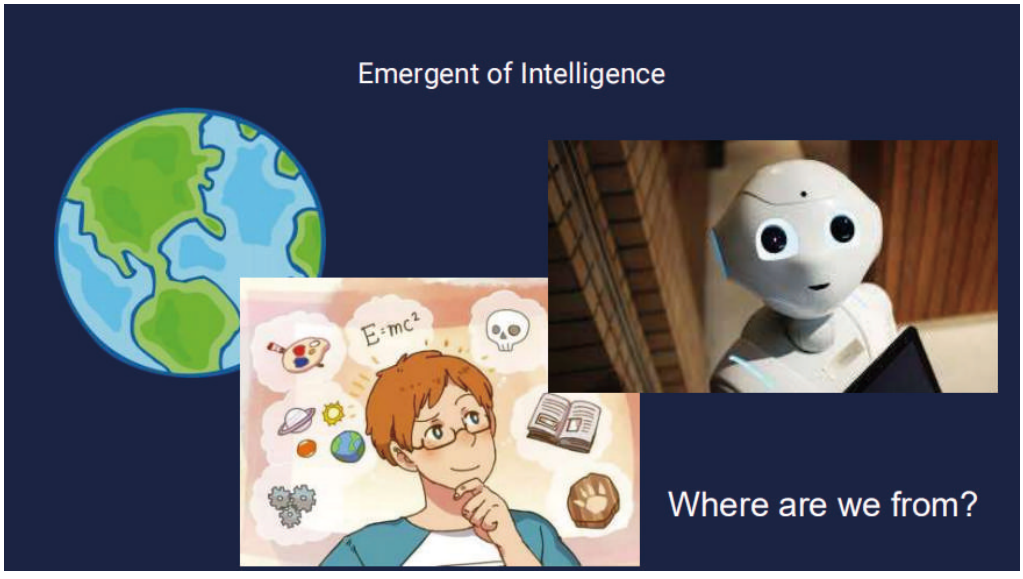


图 1：智能的涌现——我们来自何方?

该领域的研究要从人类智能的漫长历史说起。我们美丽的地球母亲拥有着神奇的生态系统，它最终孕育了人类的生命。在现代科学技术的帮助下，我们逐渐开始构建和人类有相似行为的机器。然而，在我们创造一类新型智能体之前，我们需要回答一个问题：我们 (智慧生命) 从哪里来?

「我们从哪里来?」这是一个经久不衰的问题。200 年前，一位名叫「查尔斯・达尔文」的年轻人也对这一问题产生了兴趣。1831 年，为了探寻该问题的答案，达尔文开始了他的环球航行。大约 4–5 年后，达尔文抵达了一处被称为「加拉帕戈斯」的群岛。如今，这里已经是一个自然保护区，成为了各种生物栖息的乐园。

在此后的数月中，达尔文环绕整个群岛进行了深入的考察，并受此启发撰写出了名垂后世的巨著《物种起源》。

在达尔文的环岛旅行中，最著名的故事莫过于「达尔文雀」的演化。他注意到，尽管所有的达尔文雀都起源于大陆上，但是分布在加拉帕戈斯群岛中不同小岛上的达尔文雀演化出了形状不同的喙，这是由于它们吃的食物不同。

除了鸟类之外，我们还可以在加拉帕戈斯群岛上发现许多有趣的现象，这些物种在数百万年间涌现出来的过程会令人感到震惊。例如，那里有生活在陆地上或者生活在水中的不同种类的蜥蜴，有生活在赤道上的企鹅，还有不会飞的鸟（鸬鹚）。这正是大自然的神奇之处，它们有着出人意料的极为多样的能力和行为。

因此，加拉帕戈斯之旅巩固了达尔文脑海中伟大的理论——「进化论」。达尔文在它的巨著「物种起源」中详细介绍了「进化论」，他认为这种物种的多样性并不是刻意设计的，而是进化（自然选择）的结果。有机生命会努力适应环境的变化，而只有那些最适合的种群能够在自然选择的过程中幸存下来。这些物种本身也成为了环境变化的一部分，使得各种不同的物种能够以合作、竞争等形式协同演化。人类作为地球上唯一真正具有「智能」的生物，能够得以诞生，本身也是生命的奇迹。

那么，我们能从物种进化的过程中得到怎样的启示呢？首先，生物体循序渐进地从简单形式演化到复杂形式；其次，各物种作为环境的一部分进行交互、合作、竞争，并协同进化； 第三，地球是一个复杂系统，进化的过程存在极大的复杂性，并且会产生意想不到的结果； 最后，进化发生在大量个体组成的种群中，在一个种群中会涌现出群体行为。

简而言之，对于强化学习来说，我们可以从物种进化的过程中得到以下启示：（1）我们需要构建一个足够复杂的仿真环境；（2）我们应该让智能体在该仿真环境下协同演化。

在上述要点的启发下，我们的工作主要涉及两个方面：（1）在符合规律的物理环境下根据简单的规则涌现出复杂性；（2）涌现出群体行为，以及如何实现这种行为。吴翼博士在本次演讲中仅仅介绍了第一个部分的工作。

二、捉迷藏游戏中的智能涌现

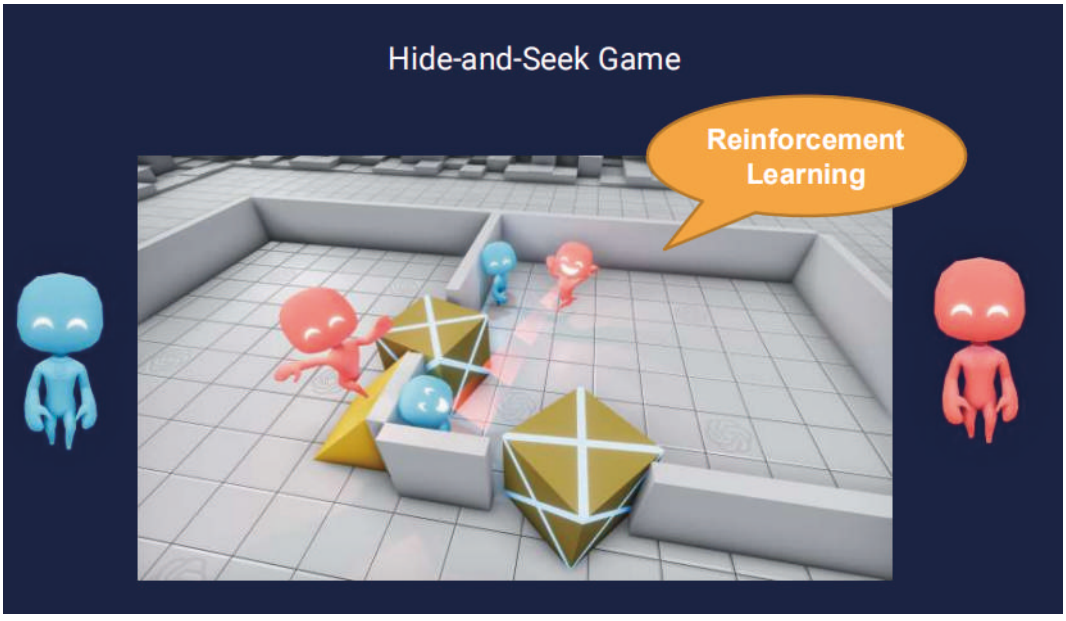


图 2：捉迷藏游戏的仿真环境

如图 2 所示，在捉迷藏游戏的仿真环境中，我们设置一些仿真物种（可爱的小智能体），还有道具物体、墙，这些智能体会在该环境中玩捉迷藏游戏。红色的智能体（seeker）需要找到蓝色的智能体（hider），hider 则需要躲起来而不被 seeker 找到。当红色的智能体找到 hider 时，seeker 会得到奖励，而 hider 则会由于被找到而受到惩罚。因此，通过执行强化学习让这些智能体能够协同学习，从而优化他们的奖励函数。

为了模拟自然环境下的演化过程，我们创建了数以千计的捉迷藏游戏，让智能体在仿真的物理世界中并行运行游戏。仿真演化实验的技术细节如下:

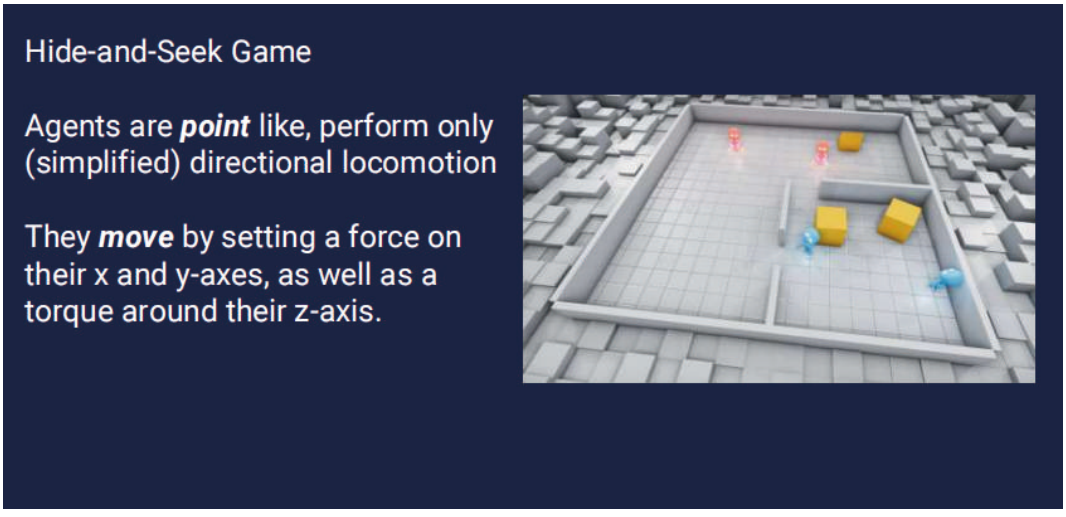


图 3：捉迷藏游戏的技术细节

为了简化控制过程，我们将智能体视为一个个点，它们只执行简化的定向运动。通过对智能体施加一个 x 和 y 轴上的力，以及 z 轴上的扭矩（让智能体旋转），使智能体移动。

图 4：智能体的视线

智能体可以看见正面的圆锥形视线（如图 4 中 seeker 正面的红色区域）中的物体和智能体，它只能接收这些可见物体和智能体的信息。

图 5：智能体的感知能力

智能体也可以通过类似于激光雷达的传感器感知到它们与物体、墙，以及其它周围的智能体之间的距离。因此，它们可以通过感知门和墙壁在该环境中进行导航。

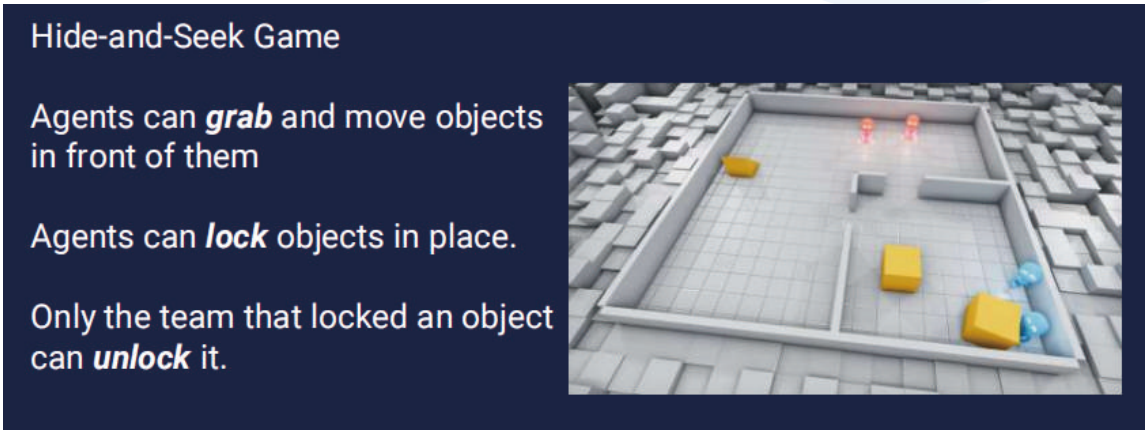


图 6：智能体的特殊行为

除了移动之外，智能体还能完成两种特殊的行为：（1）抓取（2）上锁 / 解锁。当智能体执行抓取行为时，它们可以移动面前的物体，并一直持有这些物体。当智能体执行上锁动作时，它们可以将面前的物体锁定在某个地方。请注意，我们进行的是有组别的锁定动作，如果 seeker 将某物体上锁，那么只有 seeker 能够将该物体解锁；反之，如果 hider 将某物体上锁，那么只有 hider 能够将该物体解锁。

此外，我们还设计了一些额外的细节。例如，设计了一种基于团队的奖励函数，来自同一个团队的智能体会得到同样的奖励。如果某 seeker 发现了任意的 hider，则红队奖励函数 +1，反之则 −1；如果某 hider 没有被发现，则蓝队奖励函数 +1，反之则 −1。

同时，我们还为 hider 设计了一个准备阶段，在此期间 seeker 不能移动，所有的智能体也不会得到奖励。在训练过程中，我们希望在随机环境下，通过并行的近端策略优化算法进行训练。我们将在并行的环境中随机初始化物体的位置、墙的结构，以及智能体的数量。在这里，我们也使用了参数共享机制，每一个智能体会共享相同的策略权值。我们向策略的输入中引入了智能体的类别信息，每个智能体知道它们是 seeker 还是 hider。在明确了这些技术细节之后，我们接下来将讨论涌现出的行为。

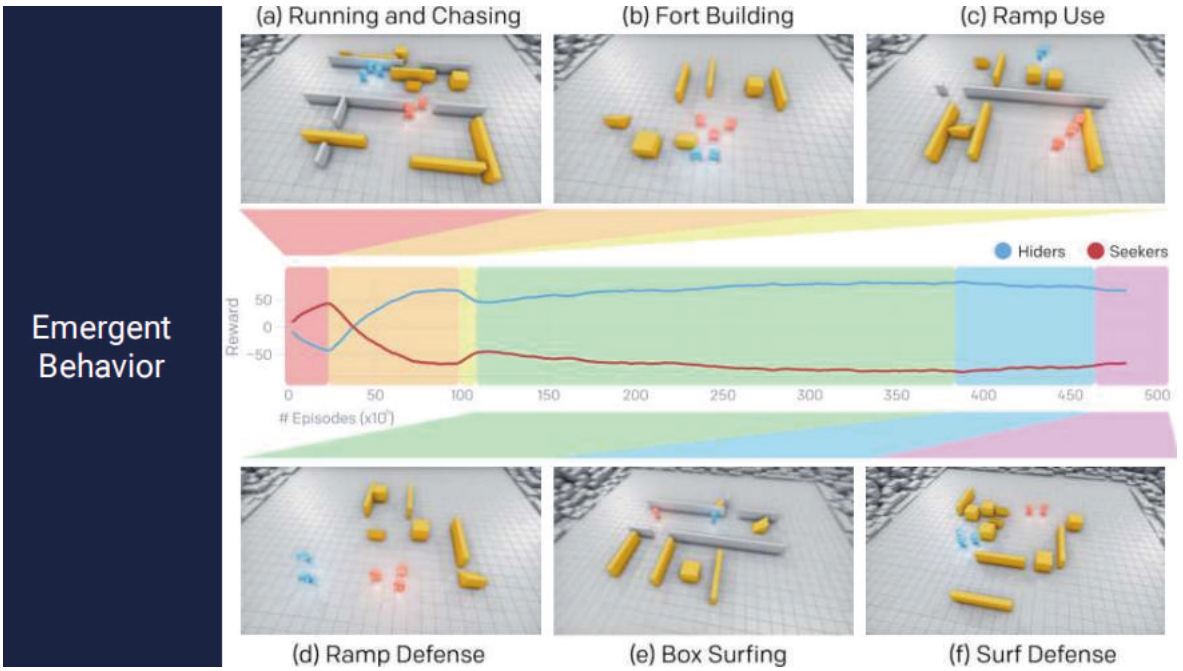


图 7：涌现出的行为——逃跑和追赶、构建堡垒、使用扶梯、防御扶梯攻击、箱子冲浪

如图 7 所示，我们一共总结出了 6 种涌现出的行为阶段，我们也展示出了各个智能体的奖励函数曲线:

阶段 1「逃跑和追赶」: 在训练初期，智能体基本上学习到的行为是「逃跑和追赶」，seeker 试图追赶上 hider，而 hider 试图逃跑。

阶段 2「构建堡垒」: 在本阶段中，hider 学会了在准备阶段使用环境中的箱子在它们自己周围搭建一个堡垒，这样一来，seeker 在准备阶段结束后就无法直接看到 hider。

阶段 3「使用扶梯」: 随着训练继续进行，seeker 很快就发现了一种对策，它们学会了将扶梯移动到 hider 构建的堡垒旁，然后爬上扶梯跳入堡垒，从而发现 hider。

阶段 4「防御扶梯攻击」: 在经过了长时间的训练后，hider 也会针对 seeker 的扶梯攻击找到相应的对策。Hider 学会了在准备阶段构建堡垒之前就锁上所有的扶梯，这样一来 seeker 就无法借助扶梯跳入堡垒了。我们曾经认为这就是群体智能涌现的最终阶段了，然而正如我们在视频中所展示的，在该阶段之后又发生了一些意想不到的现象。

阶段 5「箱子冲浪」: seeker 学会了将箱子移动到被锁定的扶梯旁，然后通过扶梯爬上箱子，站在箱子顶上向堡垒「冲浪」，最终跳入堡垒发现 hider。这是由于我们构建环境中的物理模型的方式所导致的 (尤其是抓取机制) ——当智能体抓取住某物体后，这二者之间的距离就固定下来了，因此当智能体站到箱子上之后，它可以同时执行抓取和移动两种行为，从而使箱子和智能体一起移动 (即「冲浪」)。这并不是一种漏洞，而是该环境的特性，智能体只是学会了利用这种特性。

阶段 6「防御冲浪攻击」: 最后，hider 学会了在准备阶段将包括箱子、扶梯在内的所有物体都锁上，从而防御箱子冲浪攻击。这也正是我们观测到的最后的阶段。

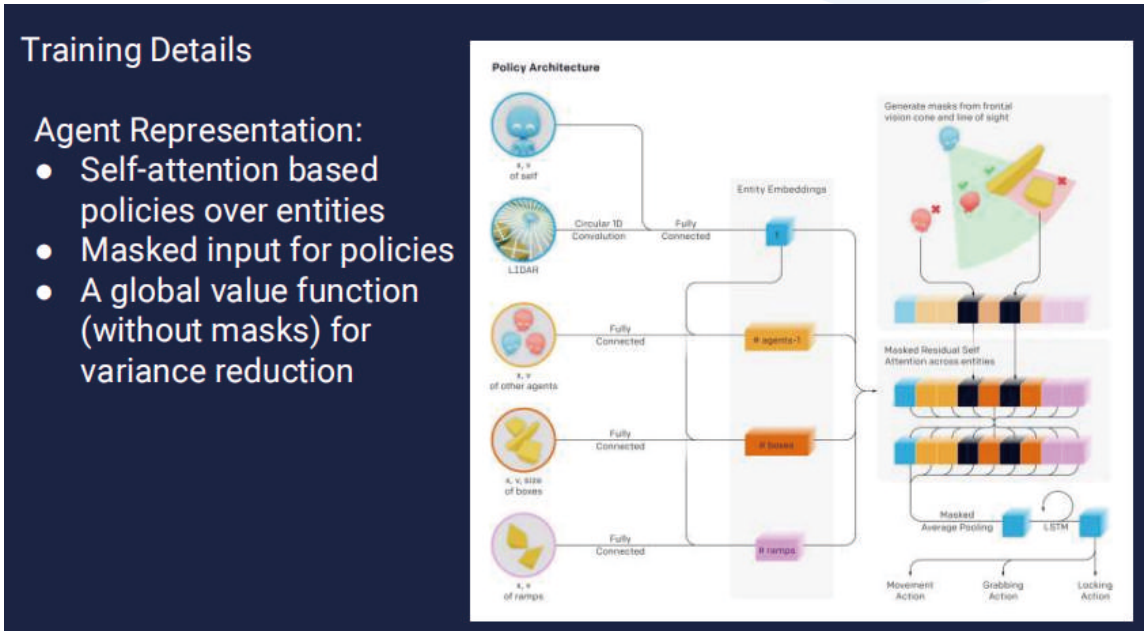


图 8：训练细节

下面，我们将讨论训练的细节。实际上，我们进行了大量的模型简化实验（又称「消融实验」），如果你想了解全面的训练细节，请参阅论文「Emergent Tool Use From Multi-Agent Autocurricula」(https://arxiv.org/abs/1909.07528)。

我们在实验中也观测到两个重要事实。

首先，对于智能体的表征是十分关键的。由于实验中会涉及到随机数量的物体，我们对各个实体使用了基于自注意力机制的策略。接着，我们通过掩模屏蔽了一些策略的输入，从而使智能体只能获取它们可以看见的物体的信息。对于值函数而言，我们使用了一种不带有掩模的全局值函数，从而减小了方差。

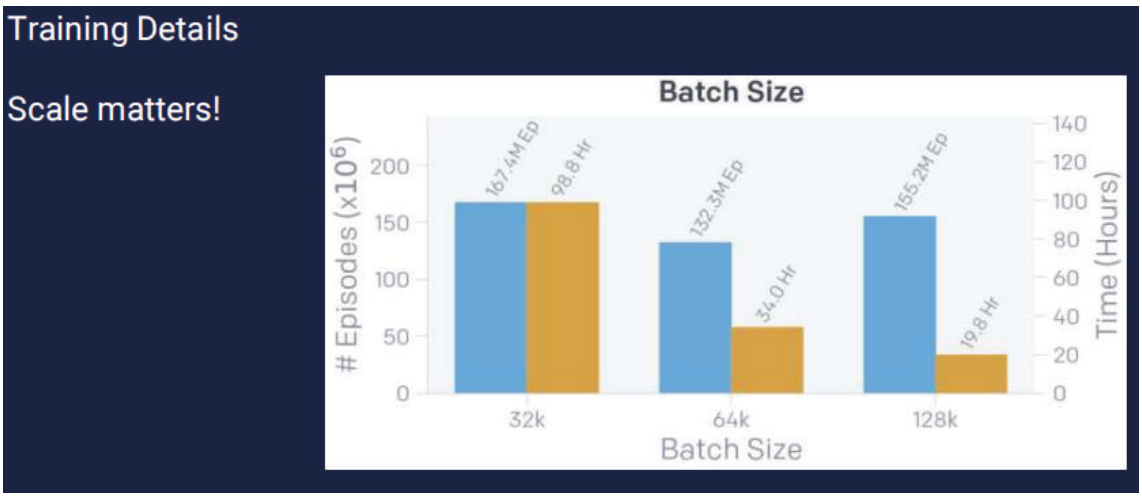


图 9：训练细节——训练规模

此外，我们还观察到训练规模也有很大的影响。我们使用了不同的 Batch size 进行模型简化实验，我们发现当 Batch size 较大时，训练速度会快很多。如图 9 所示，蓝色的部分代表我们采样得到的所有用于训练智能体的状态序列，黄色部分是训练时间。显然，随着 Batch size 增大，训练时间会缩短。

除了这六个智能涌现阶段，我们还有很多有趣的实验发现。首先，我们发现智能体可以学习到很棒的协作策略。例如，我们观察到智能体会相互传递持有的箱子，从而更高效地堵住门。在我们的实验中，也出现了一些意想不到的行为，这与地球上物种的自然进化十分相似。例如，在训练的初期，hider 实际上仅仅学会了不断逃向距离 seeker 无限远的地方，而这种行为会阻碍其它有趣的行为的涌现。因此，在最终的环境实现方案中，我们在围绕游戏场地中心的一定范围内设定了一个惩罚区域，这样一来就不会有智能体试图逃向无限远处。

实际上，智能体是非常聪明的，他们学会了利用环境中的一些漏洞。例如，hider 学会了通过非常明智的方式利用环境中的物理机制，这是由于在训练初期物理引擎中的某些设置情况造成的，我们需要在最终的环境实现中修正这些漏洞。同样地，seeker 也会利用一些环境的漏洞。例如，seeker 发现了它们可以利用扶梯爬到某些特定位置，然后飞到空中。这也是由于物理设定造成的，我们需要仔细地修正这些漏洞。

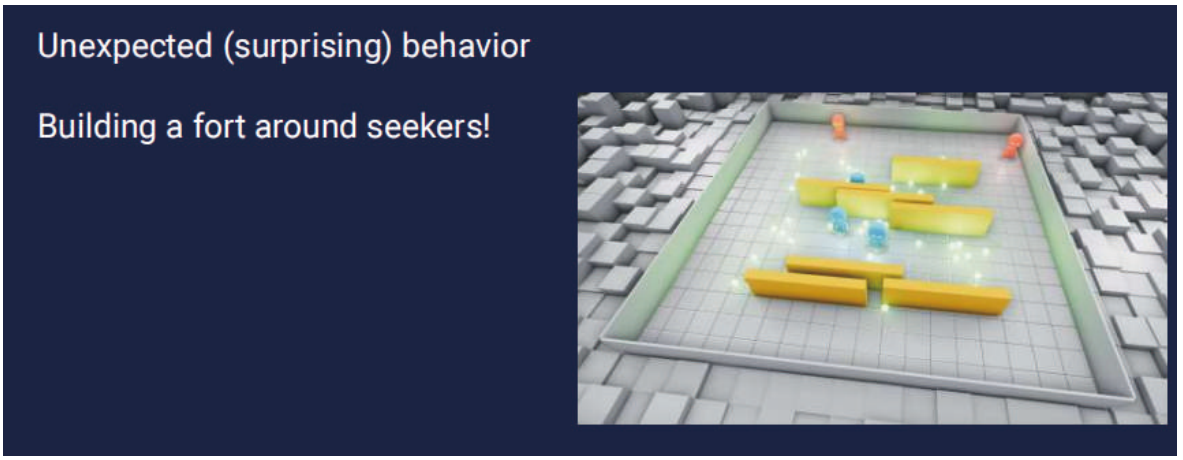


图 10：hider 构建一个堡垒将 seeker 围住

另一个令人意想不到的行为是，由于 hider 可以构建堡垒将它们自己包围起来，那么它们是否能构建堡垒将 seeker 围起来，从而让 seeker 无法出来抓 hider 呢？这是一种非常自然的策略，但是在我们标准的捉迷藏游戏中并没有涌现出来。但是在一些变体中，这种策略确实发生了。

在如图 10 所示的变体游戏中，绿色的发光点是一些奖励金币。Hider 不仅仅要防止它们自己被 seeker 找到，还要保护这些金币不被 seeker 捡到。因此，在这种情况下，仅仅构建一个堡垒将 hider 自己围起来并不足以保护这些金币。而这些 hider 非常聪明，它们找到了正确的应对策略：在准备阶段将 seeker 推到角落，然后使用箱子将这些 seeker 堵在这些角落中。有趣的是，hider 甚至使用了两层箱子加固这个陷阱，这种行为是非常出乎我们的意料的。这种变体是由吴翼博士本人发现的，这也是他本人最喜欢的整个项目中的一段视频。

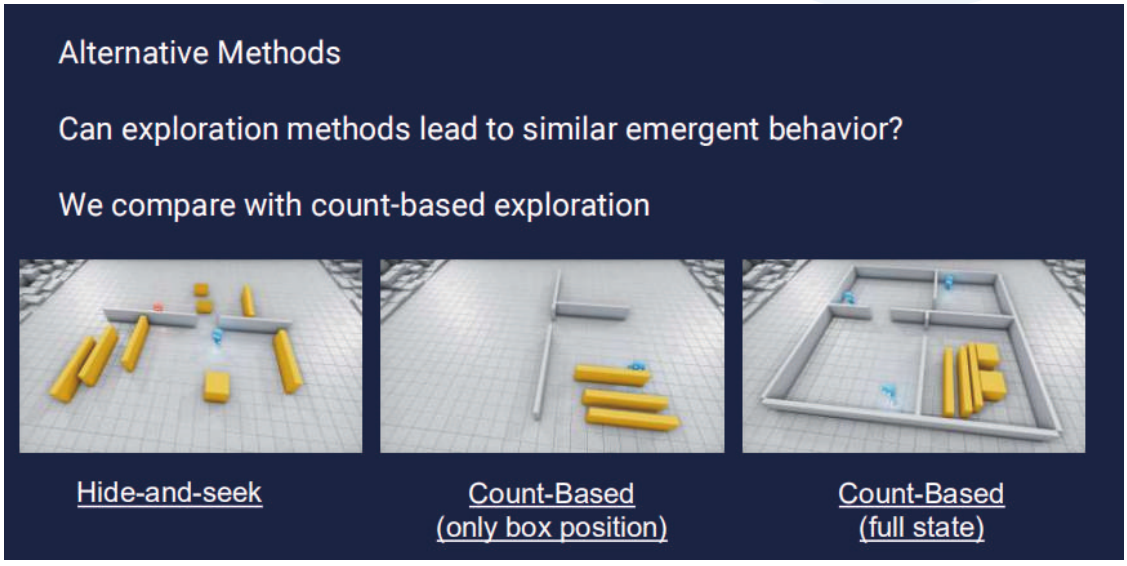


图 11：对比实验

那么，其它的方法也能够得到与我们相似的行为涌现结果吗？为此，我们也和其它方法进行了对比实验。具体而言，我们通过一种常用的「基于计数的探索」(count-based exploration) 方法进行了一系列对比实验。我们的多智能体强化学习框架发现的行为如图 11 最左侧的图所示。我们可以很容易地描述不同行为的强度，这些策略对于人类而言也是可解释的，很容易理解。

然而，在基于技术的探索中，我们可以观察到此时确实涌现出了某些行为。例如，智能体抓取到某物体，然后在环境中移动。但是此时出现的行为是比较低级的，即我们无法看到任何策略性的行为。

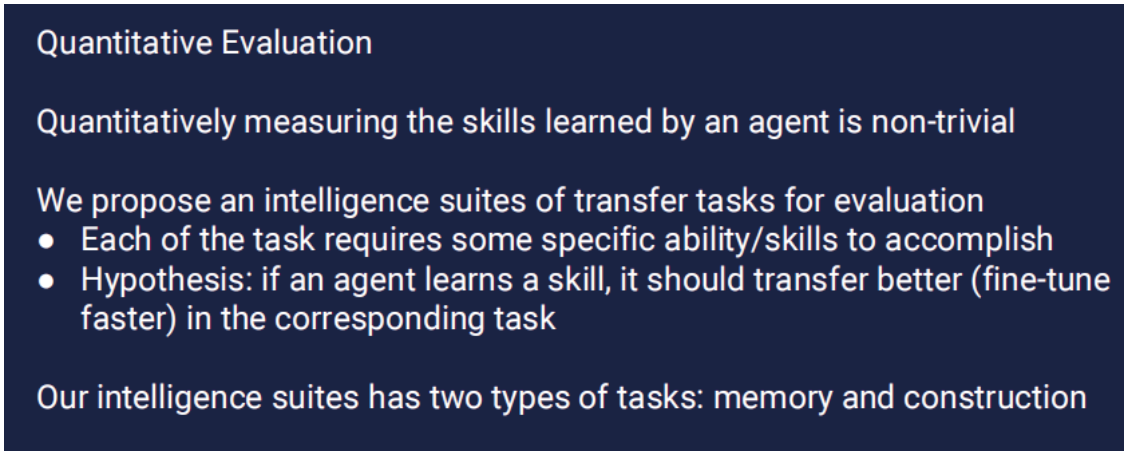


图 12：用于定量评估的迁移学习任务

除了观察涌现出的行为之外，我们执行了一些迁移学习任务，用于定量评估。由于捉迷藏游戏中的智能体学习到了一些复杂的技能（例如，导航、操作物体，建造等），那么我们能将这些技能迁移到其它的环境中吗？

为了实现这一目标，我们提出了一套由 5 个迁移学习任务组成的智能实验，将其用于定量评估。为了完成每项任务，都需要智能体具备某些特定的技能。我们假设，如果某个智能体学会了某种技能，那么它应该在相应的任务中能够更好地迁移这种技能（相对于从头开始训练调优更快）。我们可以把这 5 个迁移学习任务分成两类：(1) 记忆 (2) 构建。

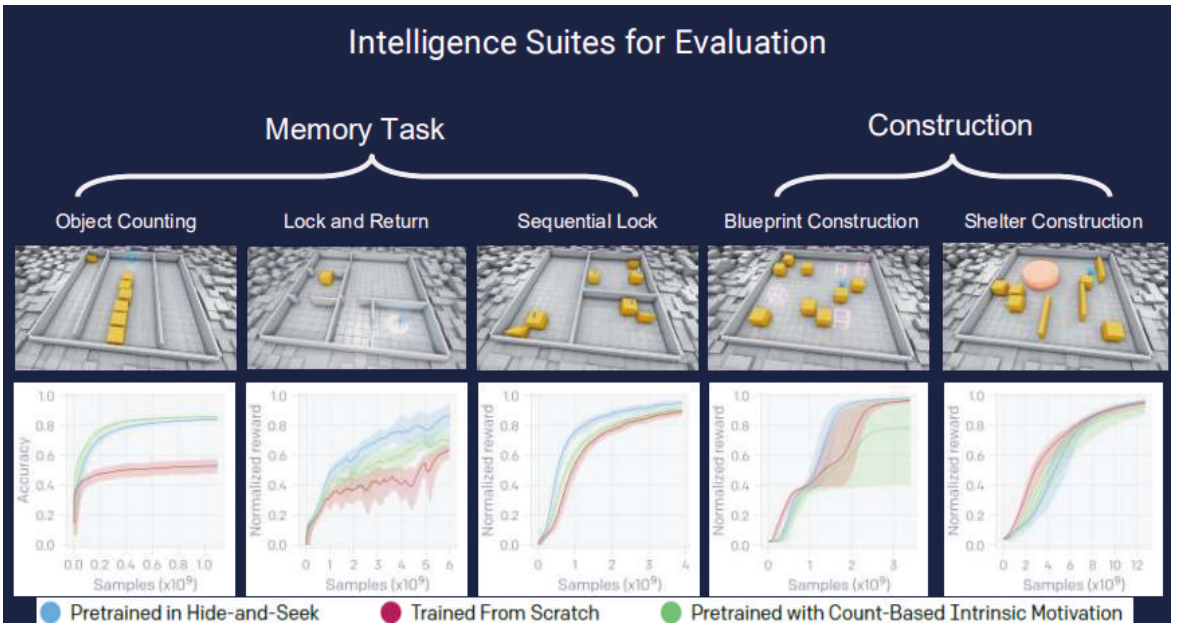


图 13：5 类迁移任务实验

5 类迁移任务如图 13 所示。其中，「物体计数」、「上锁并返回」、「顺序锁定」为记忆任务。为了完成记忆任务，智能体需要记住从环境中发现的关键信息。此外，「蓝图构建」和「遮蔽物构建」为构建任务。为了完成建造任务，智能体需要以一种特殊的方式操纵大量的物体。

任务 1「物体计数」：在该任务中，智能体不能移动。环境中有一些数量随机的箱子，这些箱子会随机向左侧或右侧移动。智能体需要观察这些箱子的移动情况，并且在状态序列 (episode) 的最后回答出有多少箱子移动到了左侧，有多少箱子移动到了右侧。因此，智能体需要记住这些箱子的移动过程。
任务 2「上锁并返回」：在环境中存在一个箱子，智能体需要找到这个箱子，将其上锁，并且自己返回到出生点。因此，智能体需要记住自己的出生点信息，而这种信息并不是输入的一部分。
任务 3「顺序锁定」：这是最具挑战的一类任务，环境中分布着若干箱子，智能体需要以特定的顺序锁定这些箱子，然而智能体事先并不知道这种顺序。因此，智能体首先需要对环境进行探索，然后记住箱子的状态，通过不断地试错最终完成任务。因此这是一种典型的长期收益 (long horizon) 任务。
任务 4「蓝图构建」：在该任务中，给定一个蓝图 (blueprint)，智能体需要将所有箱子移动到蓝图中规定的期望地点才能完成任务。
任务 5「遮蔽物构建」：在环境中有一个大的红色圆柱体，智能体需要用箱子将这个圆柱体包围起来，保护它不被环境所发现。

在实验中，我们在这 5 个迁移任务中执行了近端策略优化 (PPO) 算法，采用不同的初始化策略时的学习曲线如

图 13 下方所示。蓝色的曲线为使用我们的捉迷藏游戏初始化的策略的学习曲线，红色的曲线为从头开始训练的学习曲线，绿色曲线代表受到通过基于计数的方法启发的预训练方法。在所有的迁移任务中，捉迷藏游戏都要优于对比基线或与其性能相当。在记忆任务中，这种优势要更为普遍，尤其是对于那些需要导航技能的任务来说。但是，对于构建任务来说，这种差别就非常小了。我们至今还不明白为什么这种差距如此之小，这也是一个有待研究社区解决的开放性问题。

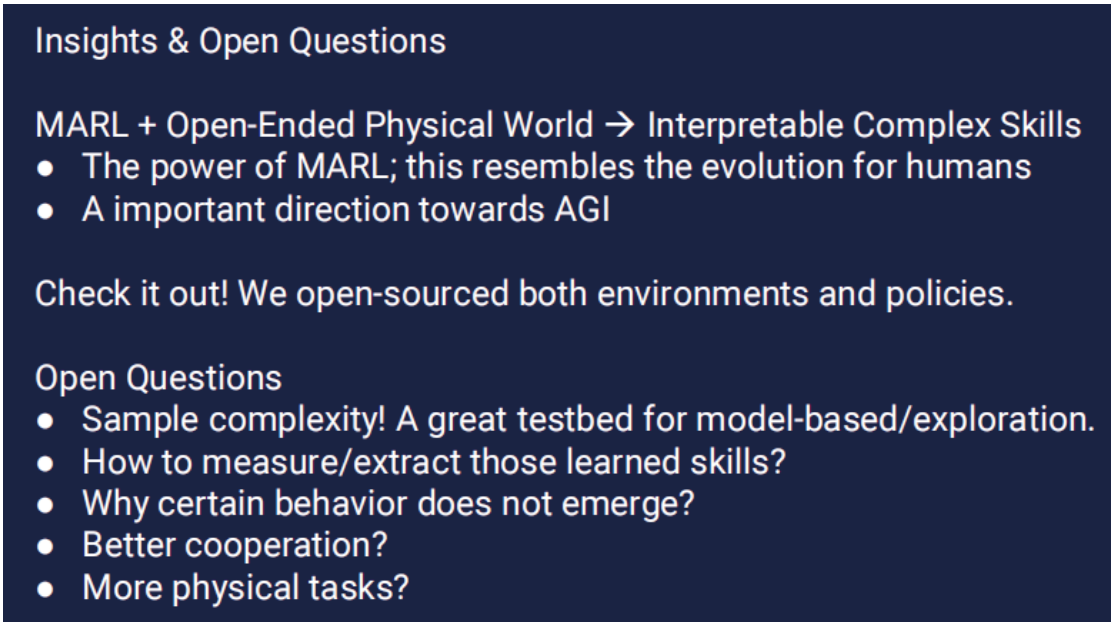


图 14：见解与开放性问题

那么，我们可以从捉迷藏游戏项目中学到什么呢？最重要的一点是，通过将多智能体强化学习与开放式的物理世界相结合，会自然地涌现出一些人类能够理解的复杂技能。这归功于多智能体强化学习的强大能力，而这种训练过程与人类的进化过程非常相似。我们相信，这是通向通用人工智能之路上的重要研究方向。该项目的环境与策略已经开源，感兴趣的读者可以通过以下链接获取相关资源：https://github.com/openai/multi-agent-emergence-environments

作为通向通用人工智能之路的阶梯，本项目也提出了许多开放性问题。例如，「我们是否能够减小采样复杂度」、「如何测量、提取出学习到的技能」、「为什么会涌现出某些行为，而为什么有些行为则没有涌现出来」。我们希望这些见解与开放性问题可以作为一个起点，帮助整个研究社区未来在该领域取得更大的进展。

三、结语

本次演讲的主题为「课程学习、演化与复杂性涌现」，我们认为，在演化机制与复杂环境的共同作用下，我们会发现涌现出了许多复杂的行为，而这些行为甚至对于人类来说也是可解释的。多智能体强化学习为学习复杂的行为提供了一种天然的自主课程，而这也与自然界中的演化过程相类似。在我看来，即使是对于现实生活或理解我们人类本身来说，这也是一个非常重要的研究领域。目前，这是一个非常活跃的使用强化学习技术理解人类社会的研究领域。

然而，「计算」是该研究领域中目前遇到的最大的瓶颈。我们必须承认，在这一项目中，我们使用了大量的计算资源。可能有人会认为，这是一件非常糟糕的事情，他们认为 OpenAI 过于依赖巨大的算力。但是，在我看来，这并不是一件坏事，因为这里的庞大计算量实际上意味着在未来还有巨大的提升空间。我相信，这个项目会成为该领域的一个对比基准，帮助那些激动人心的研究涌现出来。

最后，我想说，实现通用人工智能（AGI）是 OpenAI 的使命，我们对我们所坚信的道路非常有信心。我们希望，通用人工智能有朝一日能够真正得以实现，并造福于整个人类社会！

北京大学卢宗青：多智能体合作中的通信

整理：北京大学 姜杰川

第二届北京智源大会上，北京大学计算机系卢宗青教授做了《通信驱动的合作学习》的报告。

近年来，强化学习在理论和应用层面都有了很大的突破，但是在多智能体的情景下表现却不尽人意。自然界中的生物和人类社会都广泛地采用通信作为合作方式，这启发我们可以将通信引入多智能体合作算法。围绕通信的必要性和影响等方面，卢宗青教授分享了他们团队近年来的一些工作，包括通信如何帮助优化目标的提升和通信在多智能体情景中的应用。

以下为卢宗青教授的演讲正文:

一、通信作为合作方式：从自然界到人类社会

在自然界中存在着广泛的合作现象。例如在 Wood Wide Web 中，树根通过菌丝连在一起。森林中比较高的树，光合作用比较强，因此可以合成更多的养分，它可以通过菌丝把多余的养分传给旁边的小树苗，而一些将要死掉的树也会把养分传送给旁边的树。此外，当有害虫侵蚀植物时，它们通过树根之间的连接传递一些化学信号，提醒旁边的植物有害虫出现，这样这样旁边的树可以提前分泌特定的化学物质，从而抵御害虫。

另一个案例发表在 2013 年 Nature 上，研究者们发现在红海海底，石斑鱼可以与海鳗协同捕鱼。石斑鱼向海鳗摇摇头，然后一起游向珊瑚礁。海鳗身体比较柔软，可以进入珊瑚礁里边，而石斑鱼在外面等待。石斑鱼可以用头给海鳗提醒这个鱼藏匿的位置，从珊瑚礁里边被海鳗赶出来的鱼也会被石斑鱼捕食。

灵长类动物的合作就更高级了。在 Social Moneys 的例子中，猴子们通过不同的声音来提醒族群中其他猴子附近有捕食者。比如一只猴子看到了一条蛇，它就会发出声音提醒大家附近有蛇。

总结这三个例子，植物是通过分享一些化学物质来进行合作，鱼是通过一些特定的行为姿势，猴子是通过不同的声音。对于经过几千年进化的人类来说，我们的合作利用了所有这些方式，除此之外我们还进化出了更高级别的语言。这些合作方式可以概括为 Communication，这也是我今天要讲的的主题——研究如何通过 Communication 来更好地促进智能体之间的合作。

对于 Communication，学界的研究主要有两个方向，一个方向是 Information Sharing，智能体学习分享有助于算法训练和协作决策的表示或者其他特殊信息； 另一个方向是 Grounded Language，主要探究智能体之间所学会的由离散信号构成的语言是否与人类语言具有某种相似的特性。在这个报告中，我主要关注第一方面的 Information Sharing，重点介绍我们最近的一些工作。前两个工作主要是研究通信如何服务于强化学习的优化目标，后两个是研究如何通过简单的通信来使智能体更好地合作。

二、通信服务于强化学习优化的目标

通信的直观理解，是每个智能体都把自己的一些信息分享给其他的智能体。但是这样存在一些问题，首先是通

信代价比较大。另外简单的分享信息未必可以得到更好的效果，我们真正需要的是“必要的通信”，即能够对奖励带来增益的通信，这也是我们提出 ATOC 的初衷。

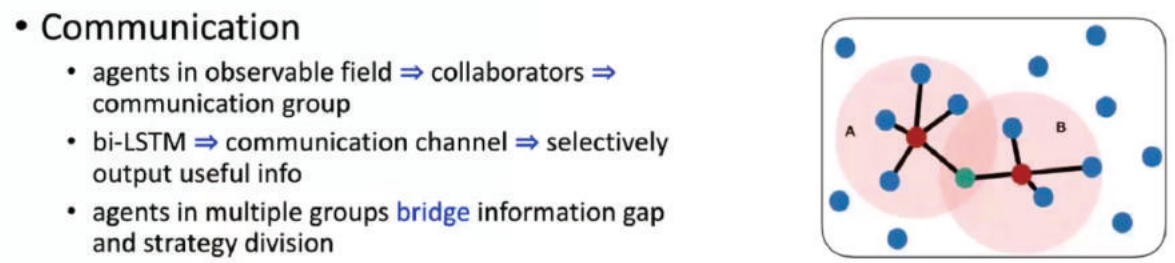


图 1： ATOC

ATOC 中的通信采用比较传统的设定，智能体可以与视野内所有智能体进行通信。通信的具体形式是，通过一个双向 LSTM 对信息进行整合。而何时与视野内智能体发起通信是通过一个门控机制来控制的。这个门控机制的学习采用的是反事实推断的思路，利用 Critic 计算通信或不通信所做出决策的 Q 值之差，差值越高说明通信对于奖励的增益越大，也就意味着越必要。将这个差值作为监督的信号训练门控机制，可以衡量通信在什么时候是有必要的。

图 3 中展示的是 Cooperative Navigation 实验中通信情况随时间的变化。绿色的虚线表示通信通道，方形智能体表示通信的发起者。可以看到随着智能体占据更多的 Landmark，通信会越来越少。最右边的图显示的是在四个智能体构成的一个通信组，黑色和黄色箭头分别代表有无通信时的动作。可以看到，加入通信之后，智能体会趋向于合作的动作。

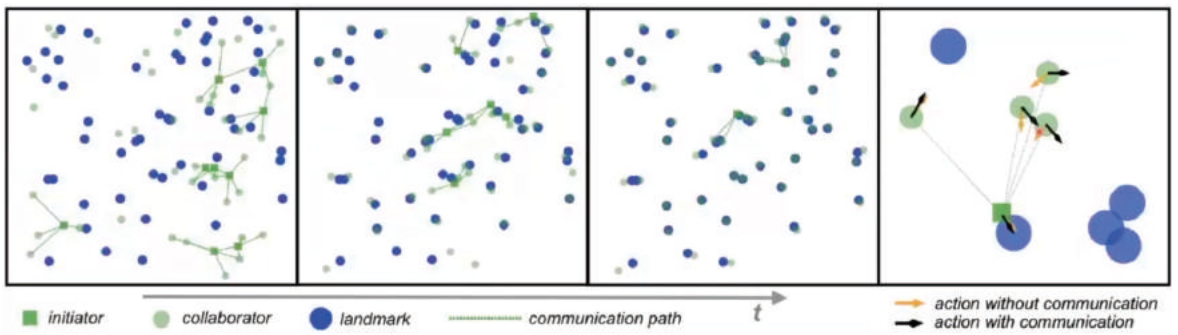


图 2: Cooperative Navigation

ATOC 以及之前的通信方法 CommNet、TarMAC、IC3Net，都是某种形式的 All to All、One to All 或者 One to Many 通信机制。但对于真正的网络通信或者人类对话，大部分情况下都是一对一通信。如何在中心训练分布执行的学习范式上进行一对一的通信，是我们接下来的第二个研究“I2C”的主要出发点。I2C 利用的是 Request–Reply 通信机制。智能体决定与视野内哪个智能体进行通信，并发送一个 Request，相应智能体的信息被传送给发出 Request 的智能体。

- **Learning Prior Network via Causal Inference**
  - Intuitively, an agent likely communicates with others who are potentially imposing influence on itself

$$\mathcal{I}_i^j = D_{\mathrm{KL}}(P(a_i|\boldsymbol{a}_{-i}, \boldsymbol{o}) \| P(a_i|\boldsymbol{a}_{-ij}, \boldsymbol{o}))$$

  - Joint action-value function can be exploited:

$$P(a_i|\boldsymbol{a}_{-i}, \boldsymbol{o}) = \frac{\exp(\lambda Q(a_i, \boldsymbol{a}_{-i}, \boldsymbol{o}))}{\sum_{a_i'} \exp(\lambda Q(a_i', \boldsymbol{a}_{-i}, \boldsymbol{o}))}$$

$$P(a_i|\boldsymbol{a}_{-ij}, \boldsymbol{o}) = \sum_{a_j} P(a_i, a_j|\boldsymbol{a}_{-ij}, \boldsymbol{o}) = \sum_{a_j} \frac{\exp(\lambda Q(a_i, a_j, \boldsymbol{a}_{-ij}, \boldsymbol{o}))}{\sum_{a_i', a_j'} \exp(\lambda Q(a_i', a_j', \boldsymbol{a}_{-ij}, \boldsymbol{o}))}$$

  - I2C can also serve as a component to reduce communication

$$\mathcal{I}_i^j = D_{\mathrm{KL}}(P(a_i|\boldsymbol{a}_{-i}, \boldsymbol{o}) \| P(a_i|\boldsymbol{a}_{-i}, \boldsymbol{m}_i, \boldsymbol{o}))$$

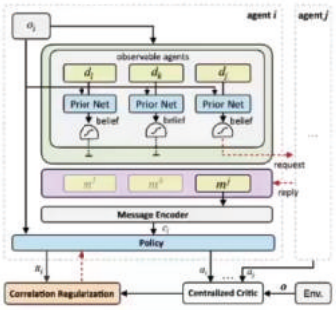
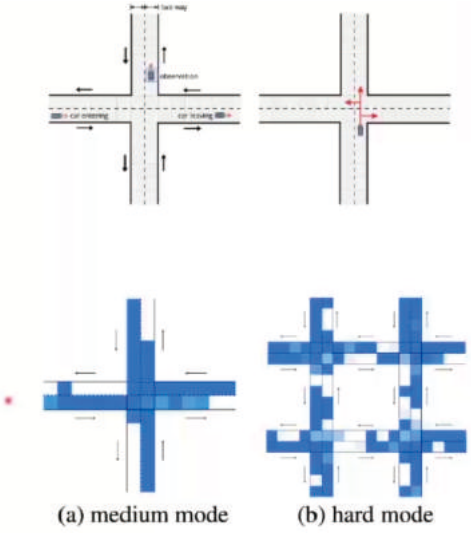


图 3: I2C

I2C 通过 Joint Action–Value Function 推断通信何时发生。在单个智能体中，通信对于奖励的提升容易衡量，但是这在 Joint Action–Value Function 中并不容易。我们的想法是，一个智能体应该选择与对自己影响比较大的智能体通信。对另一个智能体的动作考虑或不考虑这两种情况，我们将它们分布的 KL 散度作为智能体之间的影响。这两个分布通过 Joint Action–Value Function 计算得到，如图 4 中所示。计算所得的影响作为监督信号学习一个 Prior Network，用于在执行过程中决定通信与否。通过近似我们可以去除其他智能体动作的依赖，使得 Prior Network 能够独立工作，不依赖其他智能体信息。



(a) medium mode (b) hard mode

	MEDIUM	HARD
I2C+TARMAC	**97.92%**	**92.17%**
TARMAC	97.60%	89.24%
IC3NET	78.08%	40.47%
NO COMMUNICATION	79.19%	48.10%

+ Reduced communication with better performance 👍

图 4: Traffic junction

在 Traffic Junction 场景中，对比 TarMAC 和 IC3NET，I2C 取得了性能上的提升，另外 I2C 也有助于减少通信量。左下角的图显示的是通信的 Overhead，颜色越深通信越大，可以很直观地看到通信量显著减少。

三、通信在智能体合作中的应用实例

通信中如何衡量其他智能体信息的重要性？我们希望，通过智能体信息的编码计算出智能体之间的某种关系，并利用这种关系来衡量来自其他智能体信息的重要性。

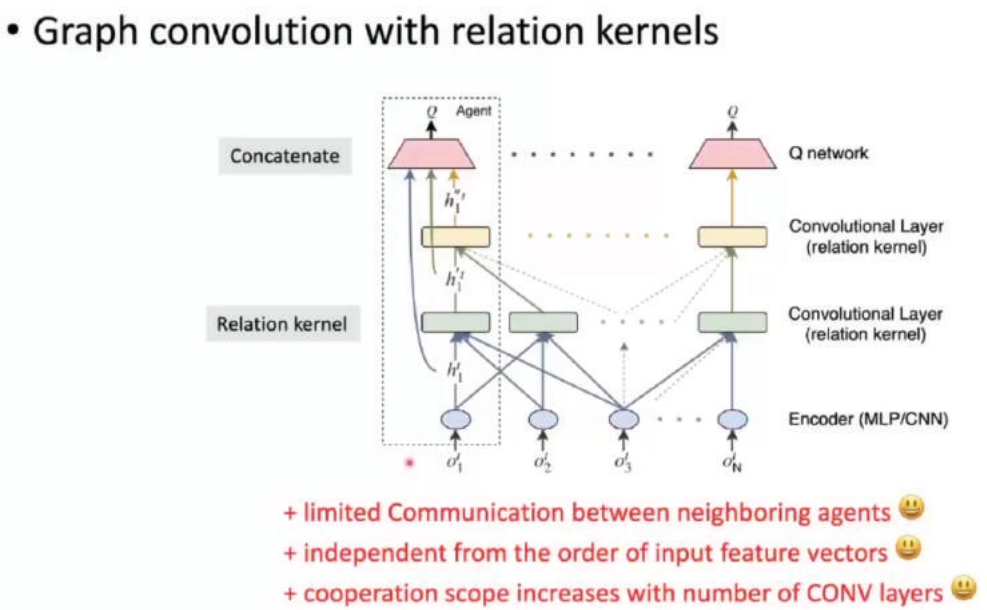


图 5: DGN

DGN 采用图卷积架构，并采用多头注意力机制作为卷积核，处理来自不同智能体的通信信息。每个智能体只与周围的邻居进行通信，通过多头注意力机制把信息整合在一起，发给下一卷积层。在下一层同样接收其他一跳内智能体的通信信息。这样随着卷积层的增加，所收集到的信息覆盖面积就会越来越大，从而使得智能体通过一跳内的通信机制获得更广泛的信息。

另外考虑在一些场景中，智能体高动态的变化，我们希望在这种情况下合作具有持续性。我们对前后两个时间步所计算的权重分布施加一个正则，促进权重在连续两个状态上尽量保持一致，从而提到合作的持续性。

最后一个研究中，我们探讨的是公平。公平对于我们社会有帮助的，但是我们想要的肯定不是绝对的公平，因为绝对的公平对系统性能没有帮助。在多智能体的系统中，我们想要的是公平和效率的权衡，这是多智能体中的经典问题。

• Fair-efficient reward

$$\hat{r}_t^i = \frac{\bar{u}_t / c}{\epsilon + \left| u_t^i / \bar{u}_t - 1 \right|}$$

$\bar{u}_t / c$: the resource utilization of the system, encouraging to improve *efficiency*

$\left| u_t^i / \bar{u}_t - 1 \right|$: the agent's utility deviation from the *average*.

Proposition 1. The optimal fair-efficient policy set π* is *Pareto efficient* in infinite-horizon sequential decision-making.
Proposition 2. The optimal fair-efficient policy set π* achieves *equal allocation* when the resources are fully occupied.

图 6: Fair–efficient reward

FEN 探讨的是如何通过简单的通信，来同时学习公平和效率。这是一个多目标优化问题，如果简单把两个目标融合在一起，这两个目标不是独立的，通过传统强化学习难以得到比较好的结果。

我们提出如图所示的公平 – 效率奖励 (Fair–Efficient Reward) 作为这个问题的优化目标，这一目标同时考虑了效率与公平。但是直接优化这一目标也比较困难，因此我们提出一种分层结构。上层的控制器的优化目标是 Fair–Efficient 奖励，控制器选择下层一个子策略执行策略。其中一个子策略的优化目标是环境给出的奖励，而对于其他子策略，我们提出一种基于互信息的奖励，使得不同的子策略行为不同，以提供给控制器多种选项。FEN 是分布式训练的，智能体之间只需要通过简单的通信获得平均效用即可。

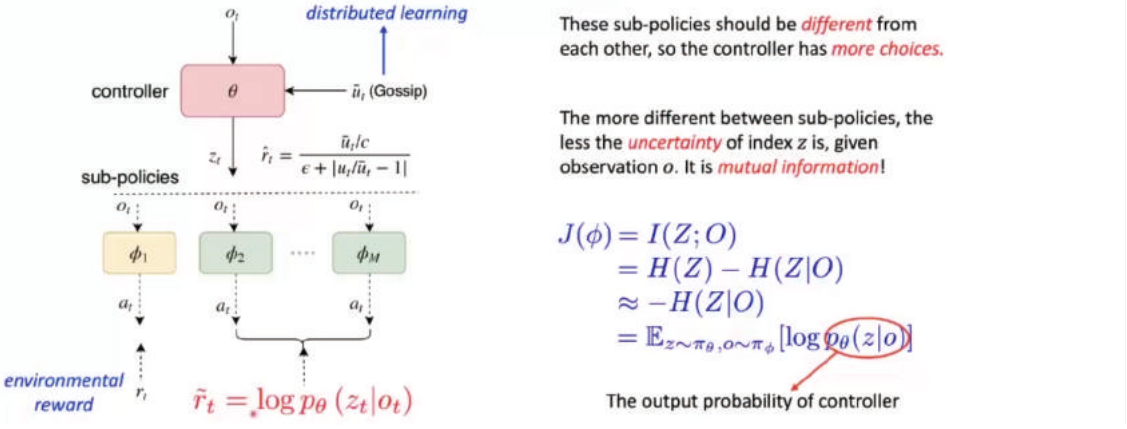
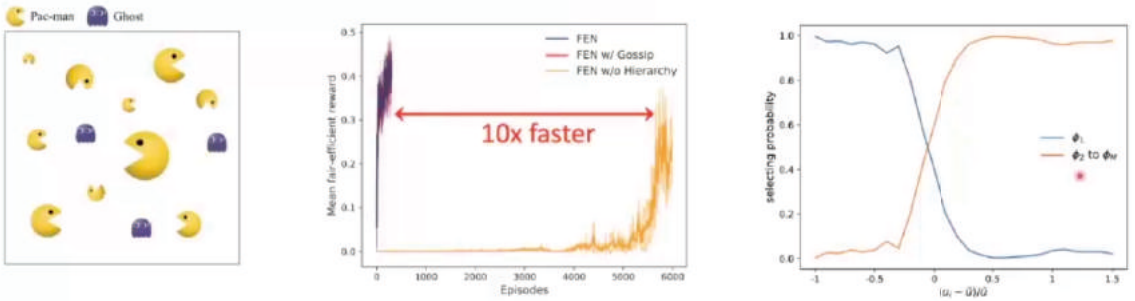


图 7: FEN

图中的实验情景模拟了马太效应，能力较强的智能体更容易吃到食物，因而能力变得更强。如果没有公平性衡量，会陷入强者更强的困境。FEN 对比其他基线方法，在公平与效率指标都是最优的，并且使用了分层结构比不使用分层结构的训练速度快了十倍。右图中可以看到当智能体的效用低于平均效用时，控制器倾向于选择优化环境奖励的子策略，反之则倾向于选择优化信息论目标的子策略，这与人类经验相吻合。



	social welfare	CV	min income	max income	episodes
Random	84 ±30	0.93 ±0.25	1	22 ±10	-
Independent	791 ±62	0.86 ±0.11	1	202 ±33	100
Inequity Aversion	702 ±90	0.80 ±0.16	2	152 ±18	1000
Min	18 ±8	2.04 ±0.66	0	7±4	6000
Avg	527±113	0.86 ±0.21	2	126±18	1000
Min+αAvg	441±75	0.85 ±0.18	1±1	103±16	2000
FEN	**830**±22	**0.06** ±0.01	**79**±2	94±3	300
FEN w/ Gossip	**841**±55	**0.07** ±0.01	**76**±4	95±4	300
FEN w/o Hierarchy	251±12	0.06 ±0.04	23±2	26±1	6000
FEN w/ Random Sub-policy	834±47	0.08 ±0.02	66±7	99±6	-

图 7: The Matthew Effect

四、结语

无论是对于智能体还是人类，通信的作用都非常大，因为通信能够改变学习的过程。从人类的角度来讲，我们很多语言性质，都反映了我们对事物的认知。关于通信如何去改变人类的学习以及人对事物的认知这一方面，当前的研究并没涉及。但随着我们进一步深入的研究，可能会探索到通信以及语言在人类认知、学习上所产生的更深远的影响。

中科院自动化所赵冬斌：从仿真到实体的深度强化学习方法

整理：中科院自动化所 朱圆恒

6 月 23 日，中科院自动化所研究员赵冬斌在 2020 北京智源大会“决策智能”专题论坛上做了《深度强化学习 – 从仿真到实体》的报告。赵冬斌是 IEEE Fellow，是多个国际计算智能领域权威期刊的编委，也是多个国际权威期刊的特邀编辑，担任 IJCNN2019 国际程序委员会的主席。其工作主要在计算智能，深度强化学习，自适应动态规划理论和方法，以及智能车辆、机器人等方面的应用。

在报告中，赵冬斌从三个方面展开介绍:

第一，研究探索更聪明，更智能的游戏 AI 算法。
第二，应用游戏 AI 的算法实现智能驾驶的安全、稳定决策。
第三，在视觉导航、环境探索、协作和博弈对抗领域实现机器人从仿真到实体的迁移。

以下是赵冬斌演讲全文:

今天的报告大家都提到深度强化学习，深度强化学习结合了强化学习的决策能力和深度学习的感知能力，这需要感谢 Google DeepMind 和 David Silver 提出的深度强化学习方法，这个方法也被列为了人工智能近几年几个里程碑的事件之一。

图 1：基于 DRL 的 AI 里程碑事件

图 1 列出了基于 DRL 的 AI 的里程碑事件，包括 2015 年谷歌提出解决 Atari 游戏的深度强化学习方法 DQN；2016 年的 AlphaGo 以 4:1 的大比分战胜了世界围棋顶级选手李世石；2017 年谷歌的 Alpha Zero 用人类的数据自学习，还具有泛化性，可以下国际象棋和日本将棋；2019 年包括谷歌的 Alpha Star 攻破星际争霸，CMU 的六人德扑 Bot Pluribus，这都是不完全信息的博弈，谷歌还将其扩展到三维的第一视角，做了雷神之锤游戏，微软也针对麻将做了一个麻将 AI Suphx，Suphx 的实力达到十段，人类基本在九段左右；2020 年谷歌又提出了 MuZero，既能玩游戏，还可以做围棋，进一步提高了算法的泛化性，也就是我们常说，更通用的人工智能。

我们早期的研究主要围绕强化学习和自适应动态规划，拿到了深度强化学习方向国家第一个自然科学基金；2016 年发表一篇深度强化学习的综述文章；2017 年 IEEE TCDS 论文获得了年度优秀论文（唯一）；2018 年组织深度强化学习的专刊，参加了 Robomaster 全球人工智能挑战赛，全部 4 次最高评价；2019 年参加星际争霸天梯赛，获得学生组冠军，参加 IEEE CoG Fighting AI 比赛，获得亚军等等。这次报告主要是挑选一些从仿真到实体相关的工作跟大家分享。

一、游戏 AI

首先跟大家分享就是格斗游戏的工作，格斗游戏动作空间比较大，动作和连招组合起来有 56 个动作，但是反应时间只有 16 毫秒。虽然对手的状态一目了然，但是对手是否能放大招却无法知道，因此这是一个不完全信息博弈问题。而且有三个对手，需要适应多种不同类型的格斗人物特性，对泛化性有一定的要求。

我们和英国 Simon 教授合作，利用 RHEA 决策和强化学习对手建模的方法做了一个通用的格斗游戏 AI。利用遗传算法的搜索能力强、强化学习对手建模能力强的优势，实现了算法的泛化性，适合不同的格斗角色。我们也和 2018 年排名靠前的 AI 做了一个对比测试，得到了一个效果（如图 2）。我们参加了 2019 年的格斗比赛，在比赛中，我们有对手建模学习的过程，一边和对手比赛，一边学习对手的策略，利用学习到的对手模型，更新策略网络，利用更新的策略获得了比赛的胜利。最终我们在比赛中获得了亚军。

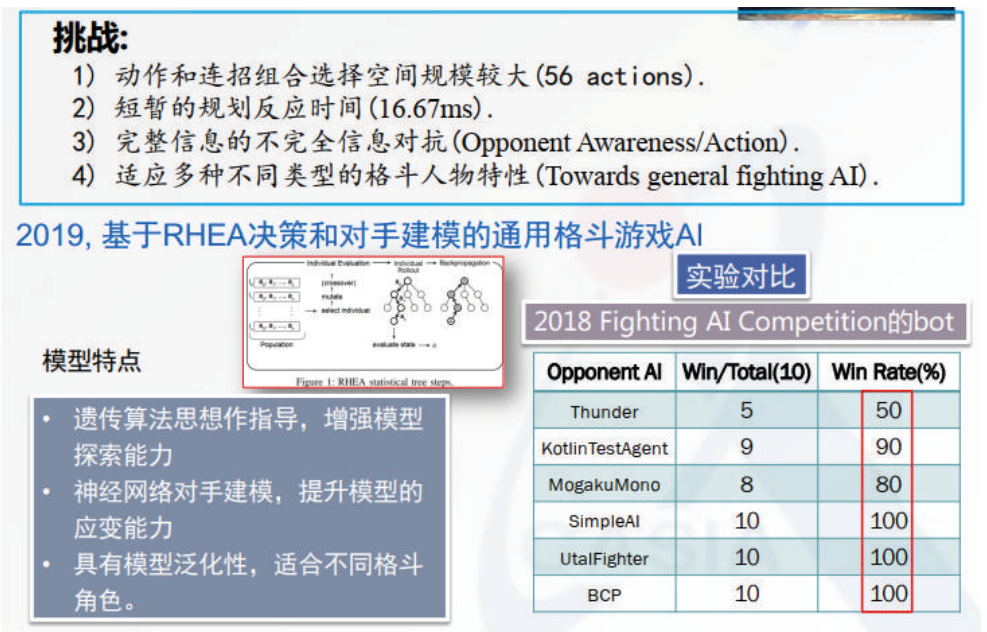


图 2：格斗游戏

前面的格斗游戏是一对一，星际争霸游戏则是多对多。我们针对星际争霸的研究也比较早，主要做星际争霸的微操，针对多智能体、不完全信息和实时决策的问题，我们定义一种高效的状态表示方法（如图 3），包括前一时刻的，自己的动作状态和对手以及队友的状态，输出移动或进攻动作。提出了多智能体梯度下降 SARSA (λ) 的方法来解决星际微操中多智能体的决策控制问题。相关文章发表在 IEEE TETCI 期刊上，得到 Popular Article，同时文章也被谷歌发表在 Nature 的 AlphaStar 论文引用。在游戏 AI 领域，我们发表两篇综述，2016 年发表在控制理论与应用的《深度强化学习综述：兼论计算机围棋的发展》，2017 年《深度强化学习进展：从 AlphaGo 到 AlphaGo Zero》，加起来下载量 1 万余次，也在中国自动化学会等官方微信里面分享了一些体会。组织了一个 IEEE 神经网络与学习系统汇刊专刊，主题为深度强化学习和自适应动态规划。和 Simon 和 Julian 这两位 IEEE ToG 的创刊主编和现任主编，一起组织了深度强化学习和游戏的专刊。

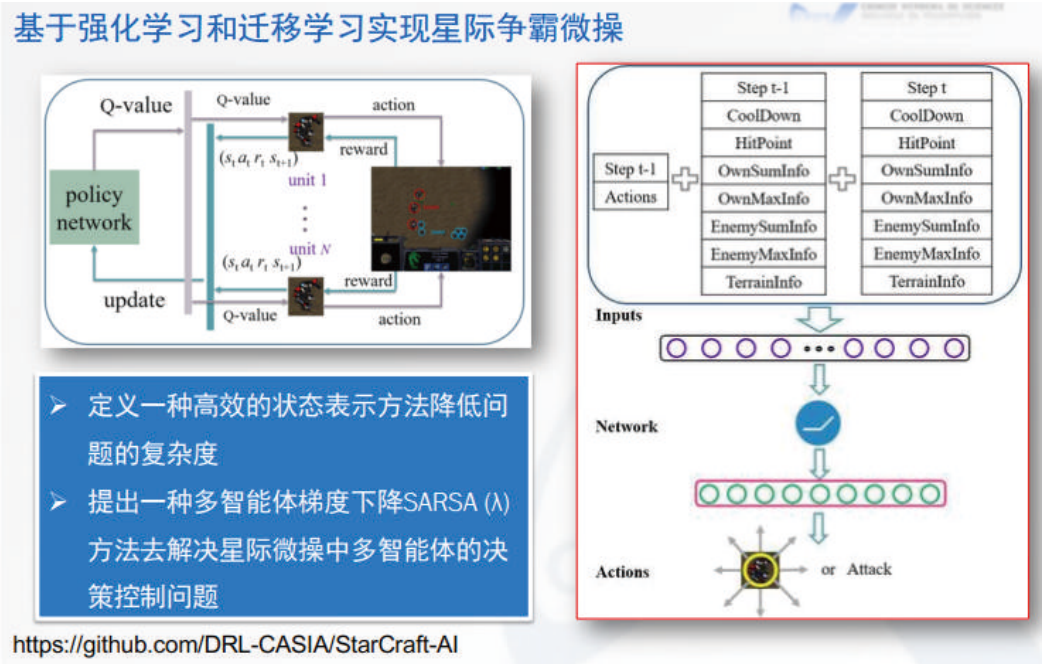


图 3：星际争霸微操

总结一下游戏 AI 的发展，我们分析谷歌和 Open AI 基本都是从游戏开始做，最终把它应用到实际，包括电力系统优化，机器人操作，机器人运动和机器人玩魔方。因为在游戏环境下学习验证，可以避免决策过程遇到的安全、伦理、数据高效和加速等等问题。我们自己做了一个游戏 AI 的发展趋势（如图 4），横轴从单个体到多个体，纵轴是二维到三维。在左下角的 Atari 游戏和围棋这类单个体完全信息问题，目前是解决的比较好的，最典型的包括谷歌的 MuZero。但是包括蒙特祖玛等关于推理的游戏还有待进一步的提升。第一视角三维的游戏，比如赛车、Minecraft 以及 ViZDoom 等还有许多需要做的工作。二维环境下，如星际争霸、DOTA2 等多智能体、不完全信息博弈问题，已经有很多优秀的工作，但是已有的工作对硬件资源需求比较大，如何能够优化算法，更好的把这些算法应用在实际的系统中，还有很多的工作要做。再结合起来就是三维多个体问题，这一块也更具挑战性。

图 4：游戏 AI 发展趋势

二、智能驾驶

我们将上述游戏 AI 的算法尽量应用到实际系统中，第一个考虑的就是智能驾驶。智能驾驶是对车辆通过相机、激光雷达等传感器获得的一些信息来进行周围环境的检测和物体的识别，在这个基础之上，我们再来做车辆的预测和决策的控制，整个链条比较长，这里我只是挑一些识别，还有车辆的纵向控制、换道控制等来跟大家分享一下。

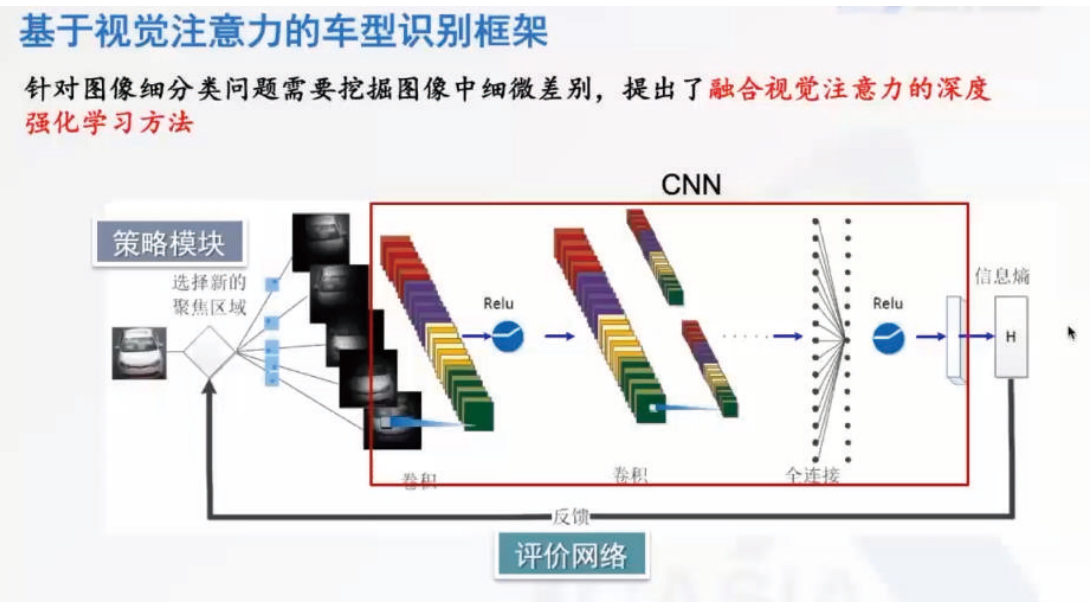


图 5：车型识别

我们在 2016、2017 年做了一个基于视觉注意力的车型识别框架（如图 5），针对图像细分类问题需要挖掘图像中细微差别，提出了融合视觉注意力的深度强化学习方法。人对车型识别时会关注车标、进气格栅、挡风玻璃和雨刷器等等，我们希望把注意力集中在这些位置，通过卷积网络来计算，利用识别信息熵做反馈评价。这种方法使得性能获得了很好的提升，相关文章发表在 IEEE TCDS 期刊杂志上，得到 Popular Article 第一位，被评为年度优秀论文。把这个方法用在实际的多任务学习，进行前方车辆检测和前车距离的检测，这两项我们参加中国智能车未来挑战赛，均获得了第一名。其他的工作包括交通信号检测、车道线识别检测，车道保持状态监测等也都参与了一些。

在得到了检测的信息之后，下一步的工作就是做智能驾驶的决策控制，其中有一个工作比较典型，就是车道保持。我们延续之前的工作，输入的是车辆观察到的图片，用多任务学习的方法得到车辆和车道偏离的距离，包括车辆的偏角以及车道的朝向。再把学习到的结果作为输入，利用 DDPG 方法进行决策，来控制方向盘的转角，进而实现车道保持的任务（如图 6）。

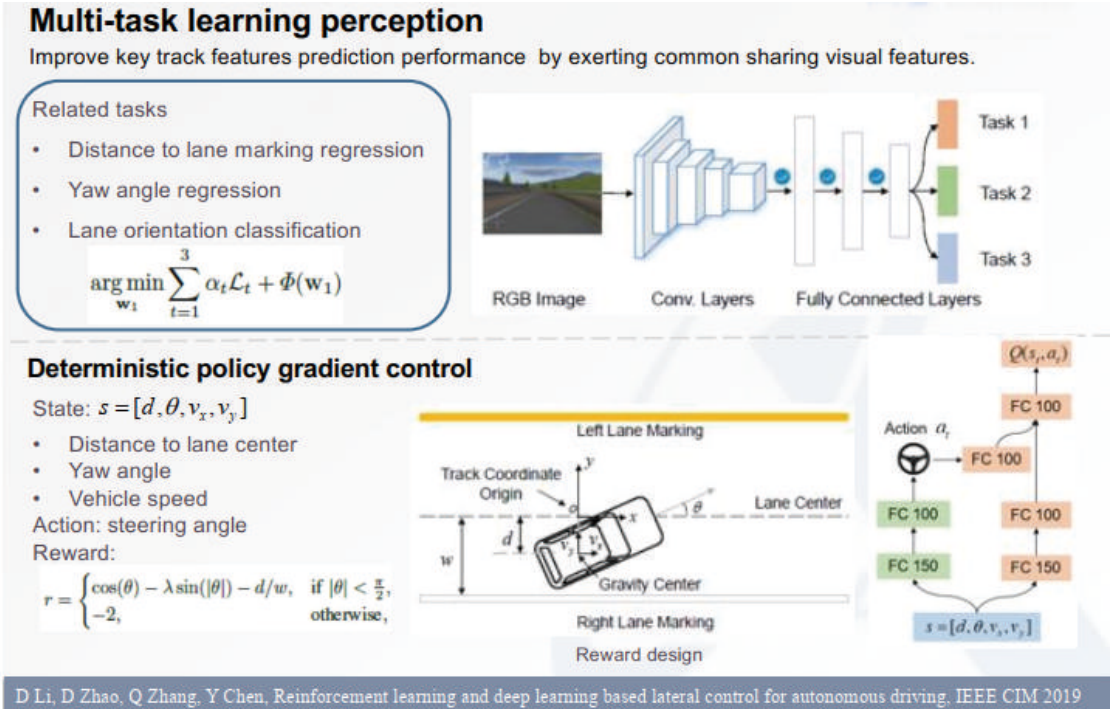


图 6：车道保持

从实验的结果来看，多任务的学习与单任务学习相比，经过不同任务的加权，可以得到更好的性能。将多任务学习与一些基线方法进行比较，结果也更稳定，同时可以泛化到新的赛道环境。总的来说，把多任务的感知和强化学习的控制结合起来，可以实现车道保持的控制，既可以看到自己本身的感知结果，还可以获得目标控制的结果，包括在单车道和三车道环境下的控制。

上面介绍的是单车道的保持，但是如果本车道有一辆开的比较慢的车或者事故车，我们就需要换道通行，这在车辆控制里面属于横纵向综合控制。我们设计了一个分层的强化学习（如图 7），上一层进行高层的决策，判断是否保持车道或是换道，下一层进行轨迹规划进而执行。测试过程中，算法首先在 Udacity 平台进行测试，从

实验结果中可以看到，当规则因素和深度强化学习相结合的时候，可以实现及时换道的功能，单纯使用规则的话，换道决策比较保守。为了验证算法的可迁移性，我们直接把算法迁移到另外一个更专业的仿真测试平台 VTD 里面，在迁移过程中并没有进行网络训练，但是效果非常好，这主要得益于之前设计的分层的架构。

把前面智能驾驶的感知和决策的工作结合起来，我们设计了一个无人配送车。这也是在今年的疫情之后，大家尽量避免在食堂集中就餐，由我们的无人配送车带着装有 200 斤盒饭的拖车，并将其送至我们所里面的两个大厦，让大家分散就餐。这个工作量还是比较大，无人配送车可以减少人和人的接触。无人配送车具有路人检测，路径规划，及时避障等功能。我们的无人配送车在自动化所开放日自动化之光进行了展出，也得到了今日头条的报道。

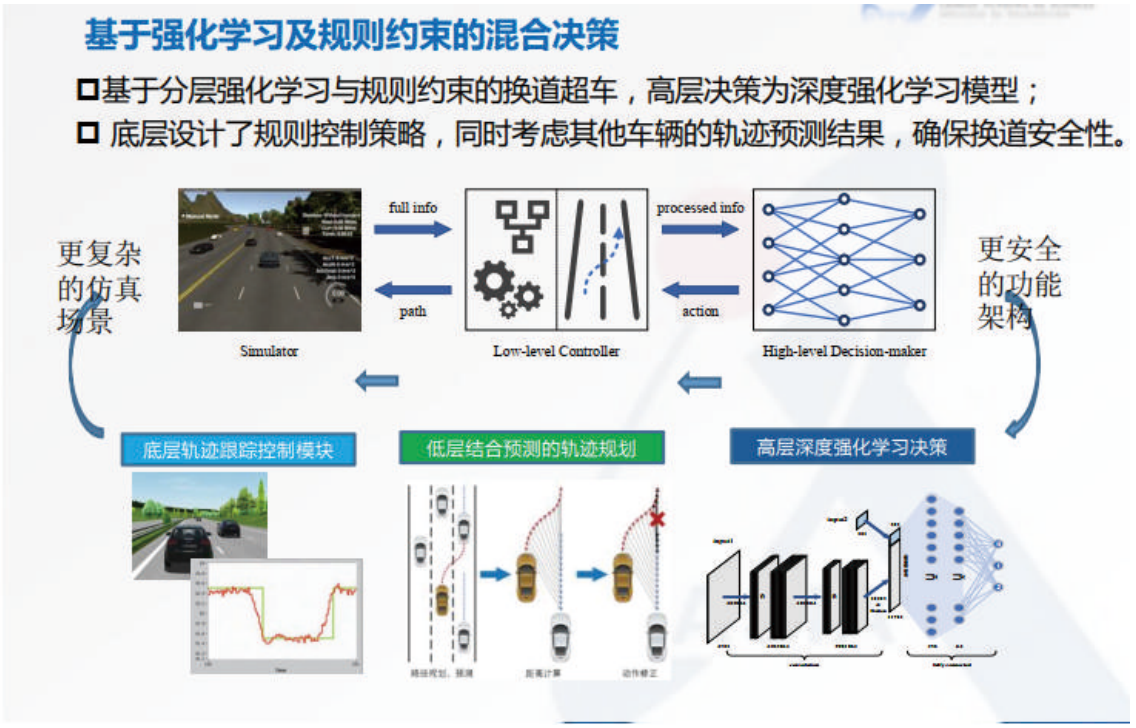


图 7：超车换道

在智能驾驶和深度强化学习领域，大家应该齐力为这个领域做一些贡献。因此我们也做了一些自己的工作，收集了深度强化学习相关的数据集，包括车道线检测和车辆检测、交通标志检测，并将我们参加的比赛和我们自己收集的数据集公布在开源的网站上（如图 8），欢迎大家更好的利用。我们自己的算法也进行开源，包括车道保持算法，希望对智能驾驶和深度强化学习领域有所推进。

数据集类型	数据集名称	大小	地点	时间	视频段个数	图片张数
车道线检测数据	Tusimple 数据集	58G	美国 San Diego (高速路场景)	2017年3月 2017年5月 2017年6月	2858 2321 1229	57160 48420 24580
	CULane 数据集	88.3G	北京 (城市环境)	2017年5月 2017年6月	489 782	55018 48217
	中国智能车未来挑战赛数据	10.9G	江苏 (城市和高速环境)	2017年	60	7268
	自主采集数据集 (未标注)	14GB	北京安立路 北京奥体中路 北京知春路 北京奥体中心附近路段 北京致真大厦地下车库	2017年9月 2017年9月 2017年9月 2017年9月 2017年9月		1945张（812M） 2523张（992M） 13101 张 (5.02GB) 15841 张 (6.06GB) 3268 张 (1.28GB)
深度强化学习数据	深度强化学习TORCS数据集	20G	TORCS仿真环境	2017年		12W张
	端到端学习TORCS数据集	124G (数据说明见附件1)	TORCS仿真环境 可训练E2E算法和Dagger算法模型	2018年		30个.h5文件
	CARLA城市环境数据集	23G	Carla仿真环境 可训练InfoGail算法、E2E算法和Dagger算法	2018年		包含人工采集13W张图片，2.3G，自动采集20G左右
车辆检测数据集	2018和2017年中国智能车未来挑战赛离线测试数据集-车辆检测数据集	3G	江苏	2018年 2017年		
交通标志数据	2018和2017年中国智能车未来挑战赛离线测试数据集-车辆检测数据集	6G	江苏，陕西	2018年 2017年	133	3174张

图 8：智能驾驶 – 数据公开

今年我们也参与了智能驾驶决策比赛 I–VISTA 的组织，大家感兴趣可以报名（如图 9）。一共有预选赛和决赛两部分，提供专业软件 VTD 让大家试用，参赛选手利用软件进行算法的调试，最终提供一个性能的测试报告，以此判断参赛选手是否可以参加决赛。决赛的时候，由主办方提供装有 VTD 的电脑，来做硬件在环的测试，考验参赛选手的算法是否更适合实际的应用系统。

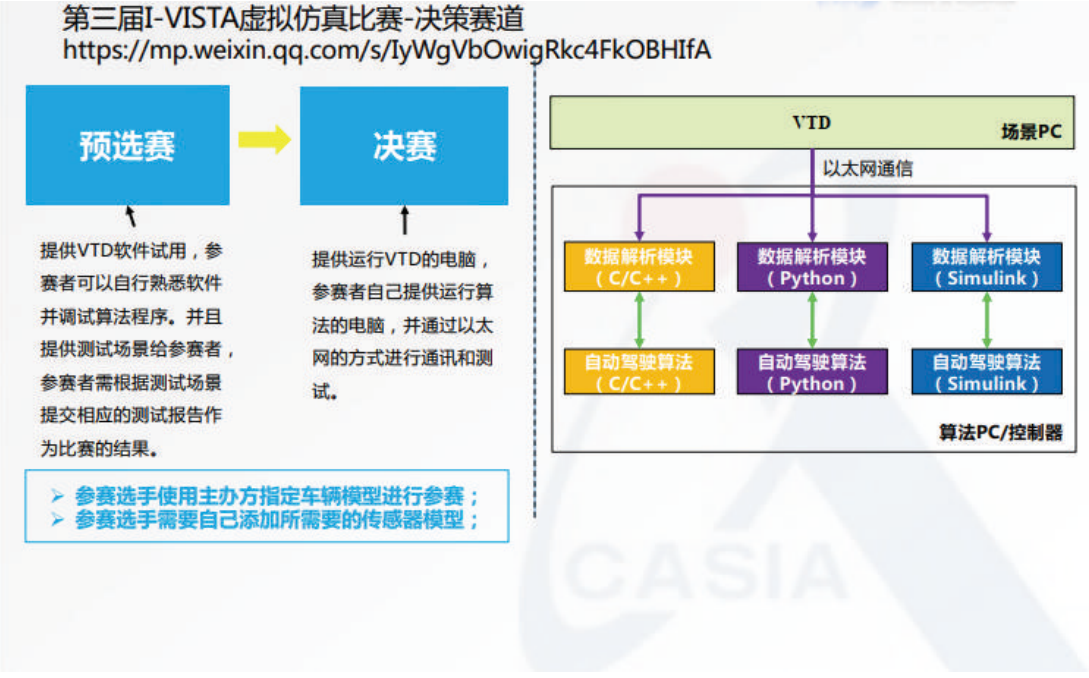


图 9：第三届 I–VISTA 虚拟仿真比赛

智能驾驶的比赛有很多，但是决策相关的比赛很少。前面我提出了对游戏 AI 的展望，针对智能驾驶领域，平台和算法方面也都需要很多的工作，需要大家共同参与。包括设计一个典型的测试环境，到底哪一种环境能够更好的对智能驾驶算法进行测试； 怎么进行交互，如何实现环境车辆的切入干扰，以此来检测算法的智能性，也就是环境和交互； 算法的智能该如何评价，目前比较简单的评价方式就是如果违规就扣一点分，但是这种评价的方式是否科学，是否评价出来的前几名真正代表了算法的智能水平比较高； 在 L4、L5 甚至无人驾驶里面，是不是能够细分更多的评价准则，这都还有很多的问题需要我们共同去解决。我们也希望在决策智能领域，可以做出一个平台提供给大家来进行学习测试。当然，智能驾驶的算法也有很多的工作目前还不是很成熟，主要针对复杂环境有很多开放的不确定的问题，比如有车有人随时出现。算法在智能驾驶里面一定要有可解释性，在一些干扰情况下，算法可能会出现一些误动作，包括各种场景的鲁棒性、泛化性，还有很多的工作要做。

三、机器人

最后跟大家分享一下我们在机器人方面的工作，包括视觉导航、环境探索以及实体的对抗。视觉导航是在室内的场景，通过视觉传感器，寻找一个物体，比如找微波炉，机器人能够发现它并能走到附近，就表示这个任务完成。常用的方法是 Slam 建图，然后定位，如果没有地图的时候，我们就用强化学习的方法来实现。但是传统的建图，对物体的位置信息要求比较严格，在新的环境里面可能不适用。我们提出了一个基于 Markov 网络和图神经网络的强化学习方法 MGRL。物体之间的关系，我们用 Markov 网络来表示，用图神经网络来推理，用强化学习的框架来训练。图 10 中，输入是摄像头拍摄的前向、左侧、右侧的图片，用卷积网络提取视觉的特征，同时用 Markov 网络来获得三张图片中离目标点的距离，得到三个具体的信息，把它们定义为系统的状态，用 Actor–Critic 的方式来计算 Value Network 和 Policy Network。

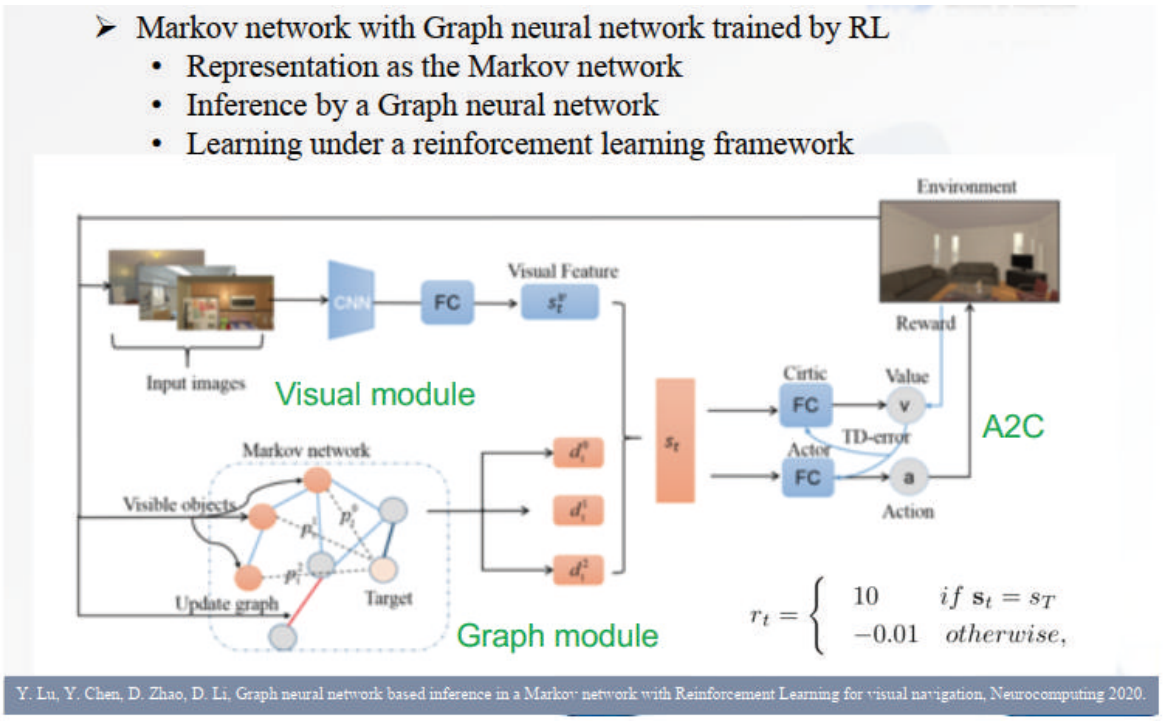


图 10：MGRL

在一个标准的测试环境里面，有四类的场景，包括一个厨房、起居室、卧室等等。我们应用图神经网络强化学习的方法，结合各种消融实验，跟 A2C 进行比较。图 11 右下角是学习到的物体之间的关系，假如物体之间没有关系，它就没有连接线。此外，我们将我们的方法和一些最先进的方法进行比较，比如 ICLR 2019 年的方法，在四个环境里面进行的测试，对比的方法针对每个环境需要一个模型，我们的方法总共只需要一个模型；我们的方法对动作的需求更低； 同时，我们的方法找到目标所需要的最大步数也更少。我们将这个方法迁移到实际的环境中，我们用一个机器人搭载几个摄像头，去找一个目标，通过简单几个步骤就可以找到目标的位置。

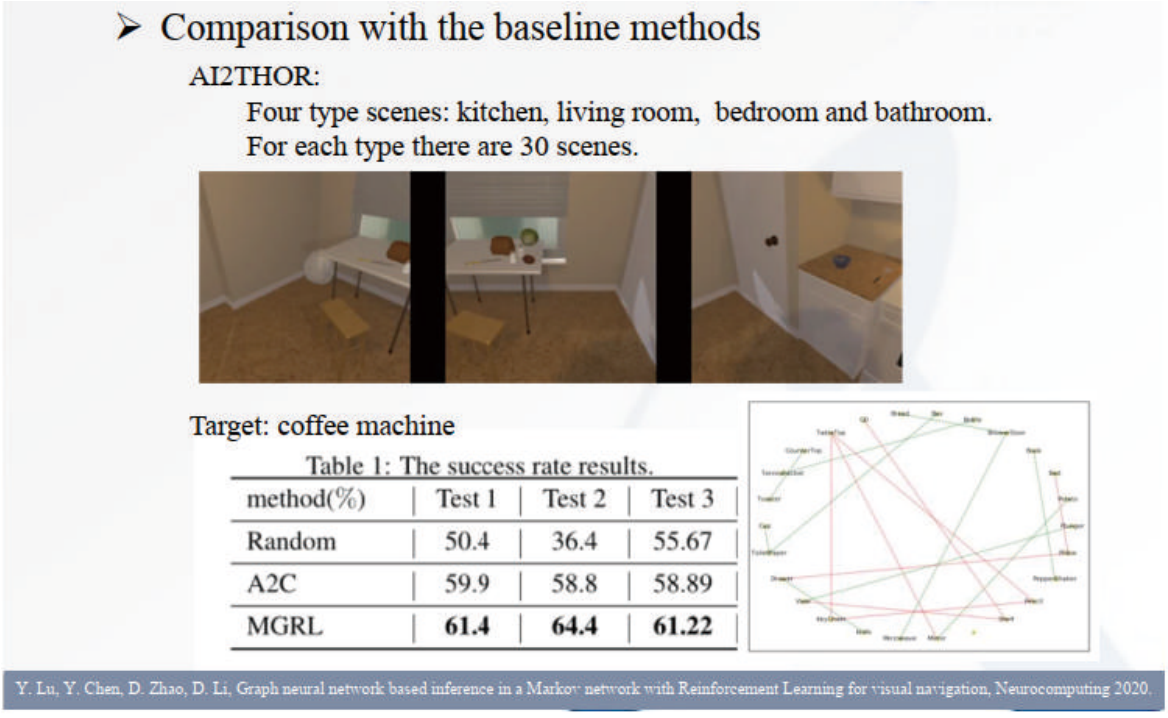


图 11： MGRL 实验结果

关于机器人，还想介绍一下未知环境探索，这也是智能驾驶和机器人等领域里面大家比较关注的问题。一般的方法，可以通过规则的方法来进行探索，但是对于比较杂乱的环境，这个方法就有一些局限性。也有人用端到端的学习方法，但是迁移性比较差，新环境需要大量的样本。我们提出一个深度强化学习的方法，包括几个模块： 决策、规划和建图（如图 12）。决策模块根据机器人已经走过的路径以及现在的地图，来确定下一个要走的位置的点； 规划模块，根据这个点用传统的 A* 方法规划出到达这个点的轨迹； 建图模块是在完成行驶轨迹的过程中，一边做动作，一边收集信息，来完成整个地图的更新。

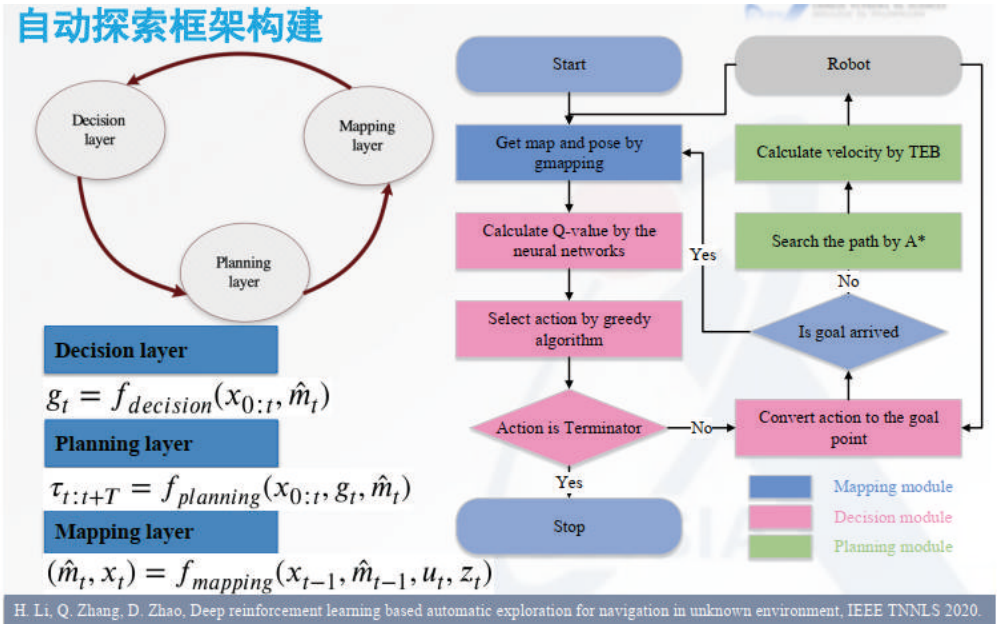


图 12：基于 DRL 的自动探索框架

我们采用一个全卷积神经网络，定义一个性能指标函数，定义地图和已知真值地图的差别。但是真值地图我们很难获得，因此我们将其替换为所获得地图的香农熵，也就是地图的不确定性。同时考虑建图所用的路径的长度，路径越短越好，结合机器人运动的约束，进而得到奖励的定义（如图 13）。

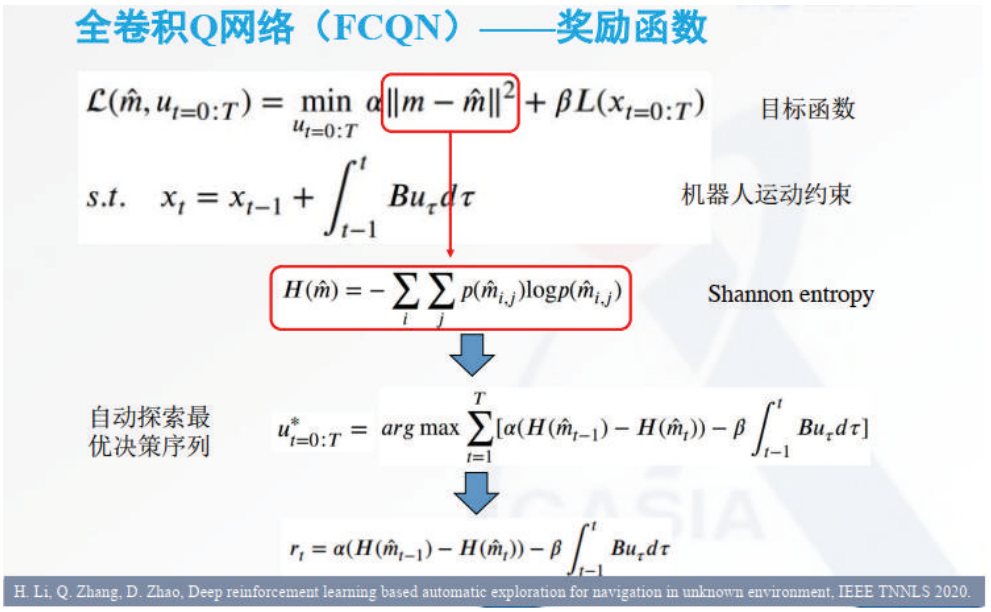


图 13：全卷积 Q 网络

我们设计了基于全卷积 Q 网络的辅助任务，输入地图的位置和边缘的图像，输出是优势函数和状态值函数。将地图进行离散化，判断网格点是否被占用，灰色的网格点是没有探索到的空间，辅助任务就是发现在建图过程

中得到的边缘图像，使得探索更有效率。在地图测试结果中，辅助任务的方法效果都是比较好的。

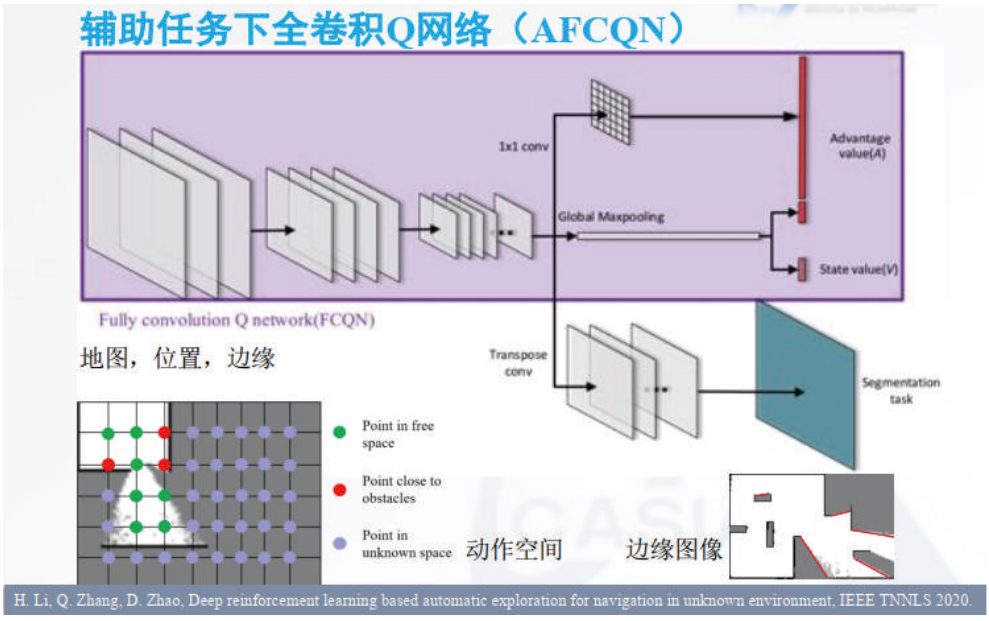


图 14：辅助任务

上述是在仿真环境里进行测试，同时我们也利用自己的比赛地图，来做实际的测试。图 15 可以看到性能的对比，从仿真到实际里面，可以看到算法性能有一点损失，但是大部分还是能够保持算法的效果。分析原因，我们觉得是因为算法的决策输出是一个目标点，而并不是机器人的具体的控制，具体的控制可能不确定性更大一点，而目标点是更中观或者宏观的指标，所以这个算法迁移带来的差异性更小一点。

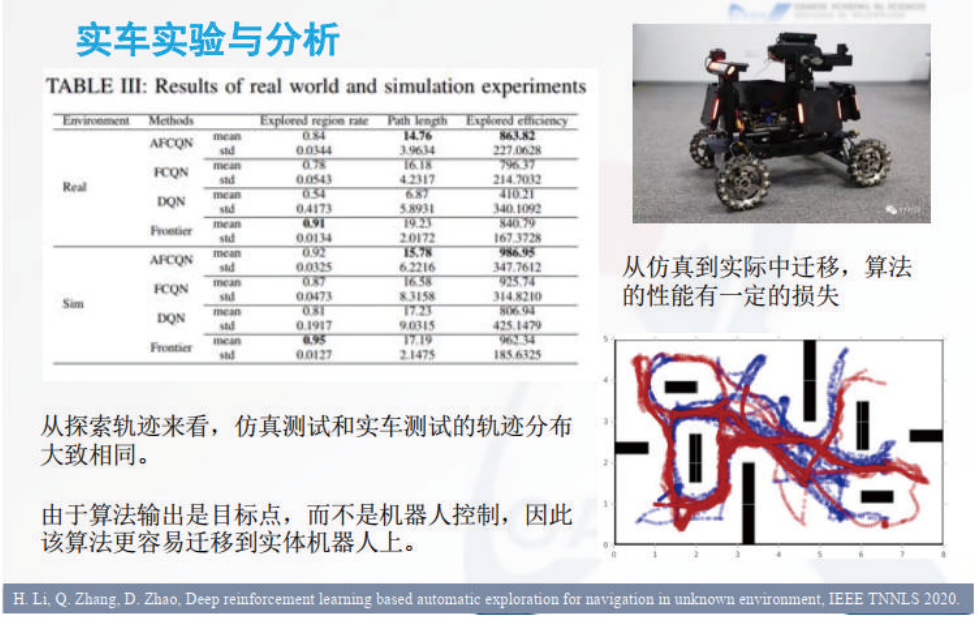


图 15：实车试验与分析

最后我来介绍一下我们在 Robomaster AI 挑战赛的工作，这是大疆在 2018 年开始的在 ICRA 会议上举办的一个比赛。每队有两个机器人，在一个 5 米× 8 米长的空间里面有一些障碍，互相寻找并攻击对方。机器人可以发射炮弹，需要攻击机器人的装甲板，机器人四周有四块装甲板，如果被击中的话，这个机器人就会掉血。在规定的时间里，哪一组机器人的血量保持最多哪一组就获胜。我们在 2018 年获得了算法的最高评价。在 2018 年的时候，大疆的机器人跟所有的对手来进行比赛，他们的机器人性能比较好，速度比较快，因此我们果断采取一个保守的策略。在打斗的时候如果发现装甲板在闪烁，就表示子弹打中对手，队友机器人立刻过来补刀，对手机器人没有灯了，就表示它已经死掉了，最终我们获得了比赛的胜利。2018 年大家的平台不一样，很难公平比较算法的优劣，2019 年都用了同样的平台来进行设计，也增加了一些难度，比如每辆机器人最开始没有子弹，需要到两个固定装弹区域进行装弹，每次装弹数量也是限量的，其他的跟 18 年基本相同。这个实体比赛会有很多不确定性出现，所以实体的比赛和应用还是有很多的难度，我们需要去克服，而且我们还有很多工作需要去做。

整个 Robomaster 比赛还是蛮复杂的，我们做了一个系统架构的图（如图 16），包括底层的驱动，如何根据它做运动； 包括相机、激光雷达这样的驱动，将得到的数据到输入感知层，实现机器人的定位； 前边车辆的检测，自己车辆的检测、敌方车辆检测，车辆检测的装甲板在哪里，根据检测结果融合、追踪和预测节点。接下来做规划，规划过程中要兼顾全局规划和局部的避碰，最终实现底盘的控制、云台控制以及射击控制，两个机器人之间的协作也会有一个学习的策略。

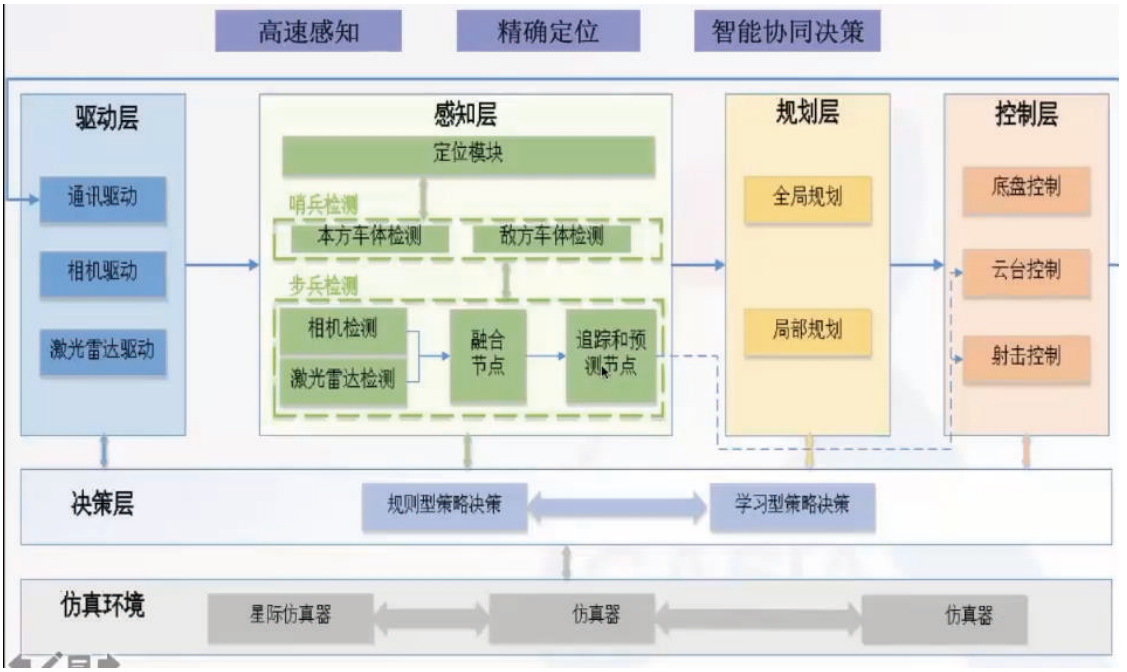


图 16：Robomaster 系统架构和关键技术

如果直接进行实体实验来完成上述工作，实验很难进行，因为实体实验经常发生碰撞，对机器人有损耗。所以我们开发仿真平台，仿真平台课题提供机器人汆的第一视角，能够为检测提供一些数据。在二维的环境下，可以来演练两个机器人协作的策略，验证包括瞄准、射击，提高射击的准确率。还包括整个全局协作的工作，后

续还将这些工作迁移到实体平台当中。如图 17 所示，我们针对仿真到实体的工作，将实体环境抽象简化，简化成二维的环境，我们用一个类似于星际的环境进行策略学习，学习两个机器人之间如何进行协作。再把它分层强化，在下一层的时候把策略转化为每个个体、每个机器人执行的任务，在执行的过程中进行路径规划、寻找目标、目标检测，最后迁移到实体里面。这也是一个多智能体强化学习协同博弈问题，这还是比较复杂的一项任务。

图 17：Robomaster—从仿真到实体

四、总结

我们主要在做深度强化学习相关的工作（如图 17），在游戏 AI 包括单个体格斗的游戏，例如星际争霸和 ViZDoom 等方面进行研究。游戏环境是基础，我们继续探讨更智能的游戏 AI 的算法，更具可解释性的算法。进而把这些方法应用到智能驾驶领域，包括车辆检测、车辆的保持和决策的控制，还包括机器人导航、位置环境探索，以及协作和博弈对抗的问题中。

启元世界高超：启元星际指挥官——基于高效平台训练的最高级强化学习智能体

整理：启元世界

6 月 23 日，启元世界技术副总裁高超在 2020 北京智源大会“决策智能”专题论坛上作了《启元星际指挥官：基于高效平台训练的最高级强化学习智能体》的报告。高超曾先后就职于易趣、百度、阿里巴巴等知名企业。在离开阿里巴巴前负责广告投放平台团队。 2018 年加入启元世界，任技术副总裁，负责强化学习平台产品的建设，在分布式系统、高性能计算、大数据等领域有 13 年的工作经验。

在报告中，高超从三个方面展开介绍：

第一，介绍启元星际指挥官达到职业玩家水平，其背后的技术要点
第二，介绍启元世界强化学习平台的设计要点
第三，介绍启元世界强化学习平台与产业的结合点

以下是高超演讲的全文：

首先，向大家介绍一则消息，6 月 21 日，启元星际 AI 顶级职业选手挑战赛中，启元星际指挥官以两个 2 ：0 的比分，分别击败了中国两位顶尖星际职业选手黄慧明和李培楠。其中，李培楠更是现役中国选手中排名最高的。这一成绩说明了启元世界已经具备解决强化学习领域最为复杂问题的能力，以及世界一流的技术水平。

一、星际争霸智是强化学习领域最为复杂的问题之一

星际争霸是电竞领域最为经典的游戏之一，也被认为是最具挑战的即时战略游戏。在该款游戏中，玩家需要同时考虑经济建设、基础设施建设、科技发展、战斗单元的建造。尤其是该游戏中各个兵种有相克关系，玩家在建造建设的过程中，还要综合考虑战斗规划、兵种配合、资源合理分配等要素，从而达到相对的战斗力最大化。最后，玩家还需要有快速响应的临场操控能力，指挥部队战斗。

启元世界从 2017 年 8 月，公司诞生之初就开始基于星际争霸的环境研究强化学习技术。在 2018 年 4 月，北京大学举办的第 42 届 ACM-ICPC 全球总决赛上发布了星际争霸人机协作挑战赛。2018 年 11 月，启元星际指挥官在 Mini Game 中达到职业选手水平，并受邀在加拿大举办的 AIIDE 会议上演讲。之后，启元星际指挥官全面进入 Full Game 的研究，并于 2019 年 9 月达到白金水平，3：0 击败人类黄金级选手。2019 年 12 月，达到钻石水平，并在同年的 NeurIPS 会议中展示 Demo，成为该届会议最火爆的体验项目。2020 年 6 月达到宗师水平，并于当月击败了人类顶级选手。

星际争霸是当今强化学习届最为复杂的问题之一，其决策复杂度对比围棋有数十个数量级的提升，其表现如下图：

图 1：围棋 AI 与星际 AI 对比图

1. 围棋是完全信息下的博弈，而星际是非完全信息的；
2. 围棋是回合制对战，而星际是毫秒级的变频决策；
3. 围棋仅对一枚棋子进行操作，而星际是要从上百个单位中选择若干；
4. 围棋仅有落子一种指令，而星际有建造、移动、攻击等上百种指令；
5. 围棋的指令目标在 19*19 的格子中选择一个，而星际的目标则要在 256*256 的区域，或者数百个单位中做选择；
6. 围棋平均每局只需要决策 100 次，而星际需要 2000 次以上的决策。

综合上述复杂度，围棋的决策空间是 361，而星际是 10 的 26 次方。

二、启元世界星际指挥官的算法实现要点

启元世界星际指挥官为了应对如此复杂的问题，设计了模仿学习、强化学习、演化学习三位一体的训练流程。

模仿学习可以以较低的成本初始化星际 AI 智能体，从而节约大量的、低效的智能体初期探索算力。模仿学习以少量人类数据作为输入，输出超过人类黄金选手水平的智能体。同时，以人类数据初始化的智能体，可以为后续的训练过程带来打法上的多样性，从而保证在与人类对抗中的鲁棒性。模仿学习的另一个好处是，可以构建一个快速验证算法策略的技术架构。

强化学习以模仿学习阶段输出的模型作为起始模型，使用带有 GAE 的近端策略优化算法（PPO）进行优化。为了在强化学习阶段保持人类多变的打法，会比较正在优化的策略分布与模仿学习策略分布的 KL 距离，并在损失函数中加入一个惩罚项。

为了在强化学习过程中演化出更为强劲鲁棒的打法，加入了智能体联赛机制，以期在智能体相互博弈的过程中，共同促进成长。在该联赛中，主要包括三类智能体。其一是 Main Agent，其目的为变强和变鲁棒。它会与联赛中的所有打法的智能体及其历史版本进行对抗。第二类是 Main Exploiter，其目的是发现 Main agent 的缺陷，并针对缺陷训练应对的策略，最终作为 Main Agent 的陪练，补强其漏洞。第三类是 League Exploiter，其目的是发现 league 中全体智能体的打法缺陷，并找到应对策略，最终作为 Main Agent 的陪练，补强其漏洞。

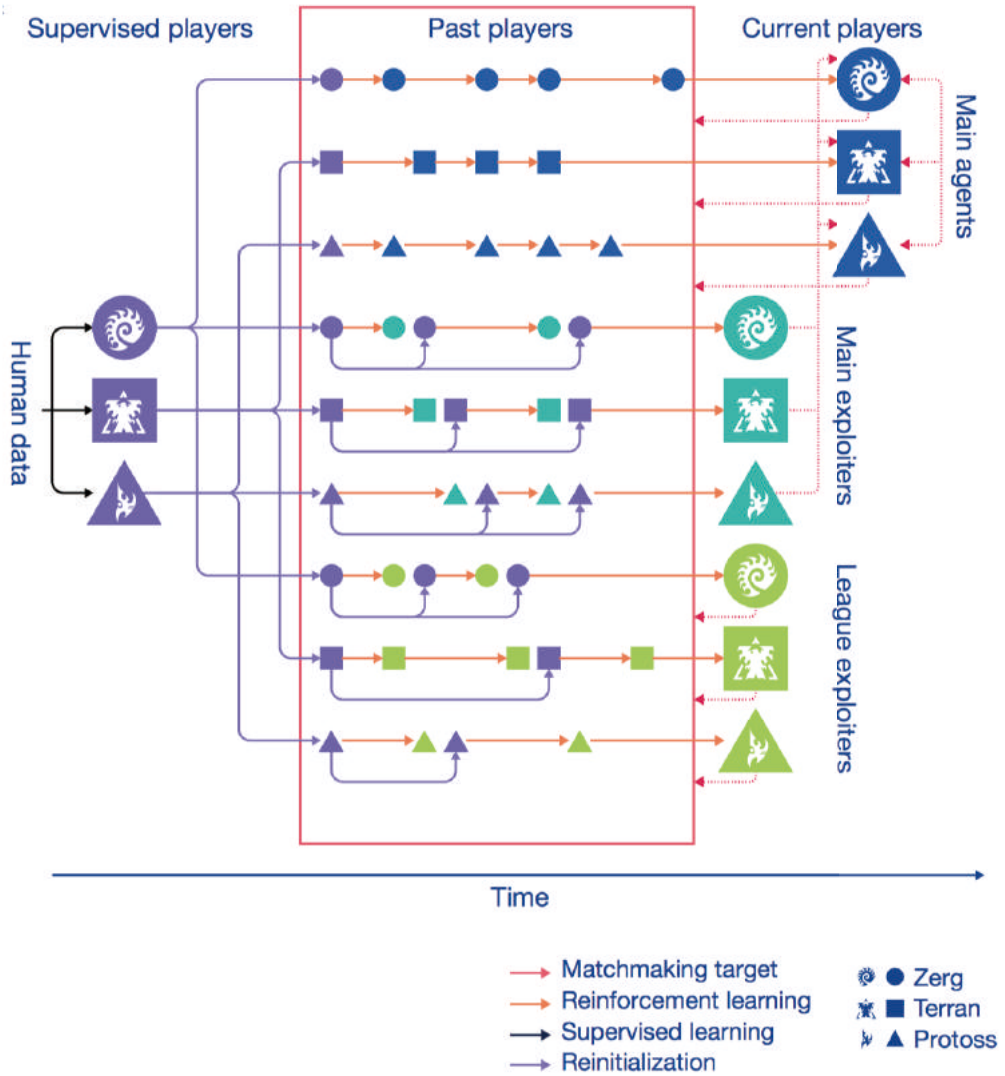


图 2：Commander Neural Network

启元星际指挥官使用了启元世界自主设计的网络模型 Commander Neural Network。这是一套类似于图像处理领域中 ResNet 等模型一样的标准化模型。它将输入、输出、奖励标准化，可以端到端的解决基于空间和时间特征关联的，博弈对抗类型的强化学习问题。

三、高效的智能体训练平台

启元世界从建立之初，就确定了一横两纵策略。通过竞赛项目或星际争霸类的研究型项目积累技术经验，并沉

淀到智能体训练平台中。通过平台的转化，输出给业务项目。而通过业务项目积累的行业经验再次反哺到平台中，为日后的项目节约解决方案上的成本。

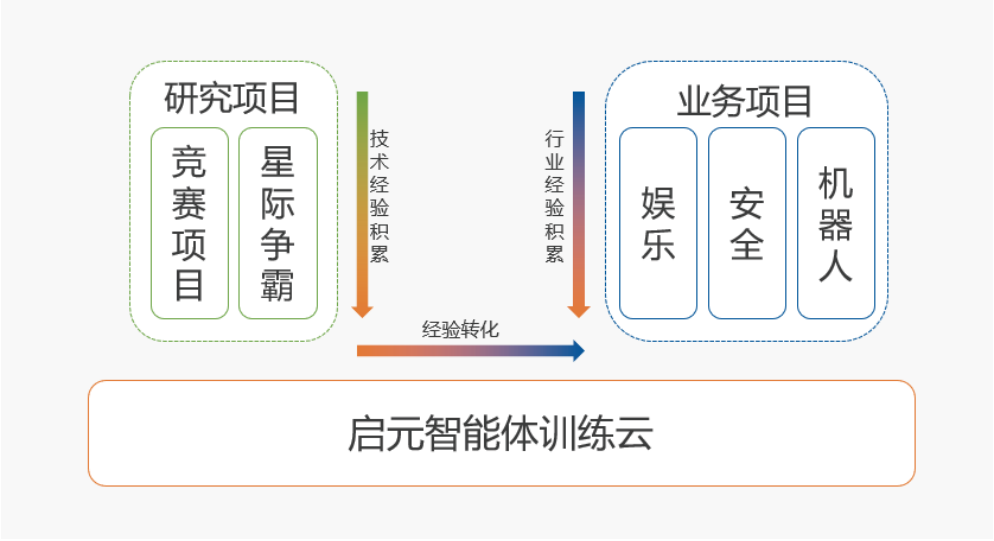


图 3：启元智能体训练云

启元世界面向于产业级大问题提供解决方案，通过大量案例的分析，将该类问题分解成两个关键要素： 问题规模和业务效果，其关系如下图所示:

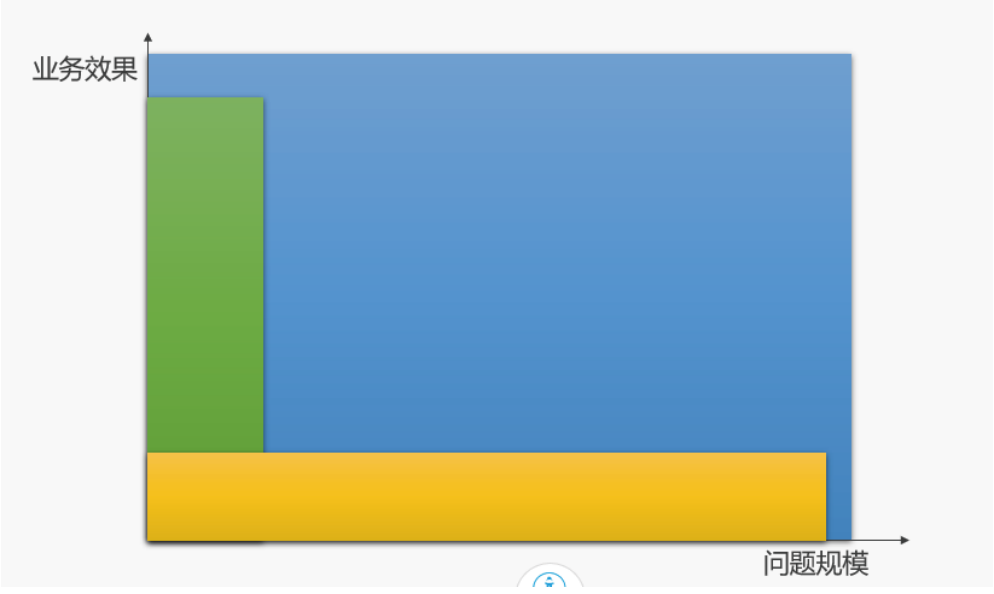


图 4：两个关键要素

问题规模主要依靠分布式技术解决，而业务效果主要依靠算法能力。启元世界在算法能力之上进行了进一步的抽象，总结了在相关领域的最佳实践，进一步提升了算法结合产业的效果。

根据上述要素，我们进一步分解，设计了五层系统架构，如下图所示:

图 5：对要素进行分解，设计一个五层系统架构

通过硬件架构的设计，提供了高计算密度、低通信延时的集群部署方案。通过分布式操作系统层的抽象，将众多服务器抽象成如同一台电脑的、可灵活分配的算力模型。最后通过四大引擎的计算抽象，将大规模算力转化为数据生产和消费的能力，从而简化了大规模算法的实施成本。

算法层涵盖了算法实施的全过程，包括原始数据处理的特征库、支撑强化学习优化方法的算法库、上面提到的标准化神经网络模型结构及组件的模型库，以及优化智能体鲁棒性的训练方法库。

最后，启元还将上述技术结合十余年的系统建设经验，构建了涵盖工程师从研发、调试、到模型训练、评估、部署，全周期的产品解决方案。

上述架构的运行逻辑如下图:

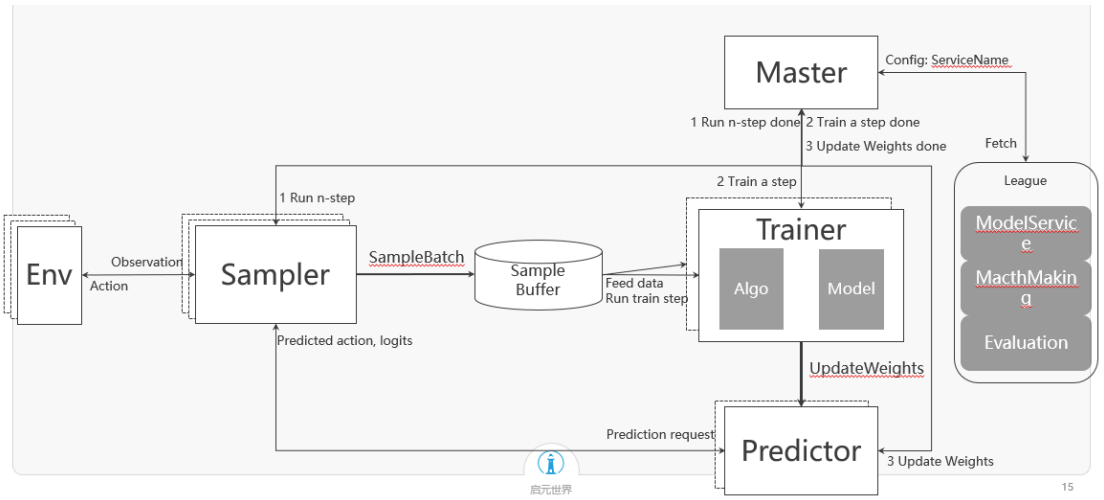


图 6：循环逻辑

四、启元智能体训练平台的技术优势

启元世界拥有业界一流的系统设计和实施能力，根据强化学习计算特点设计的计算模型、网络通信优化、数据 Pipeline 优化、计算优化、Placement 优化等多种手段，将平台的计算能力推高到开源实现的 10 倍以上。

另外，启元世界还开创性的提出了对抗博弈类的标准网络结构，Commander 网络模型（群体指挥控制）和 Hero 网络模型（多智能体协作）。配合标准化的训练方法（模仿学习、自博弈训练、联赛机制），可以产出达到甚至超过人类水平的智能体。

启元智能体训练平台于其它竞品的对比如下图:

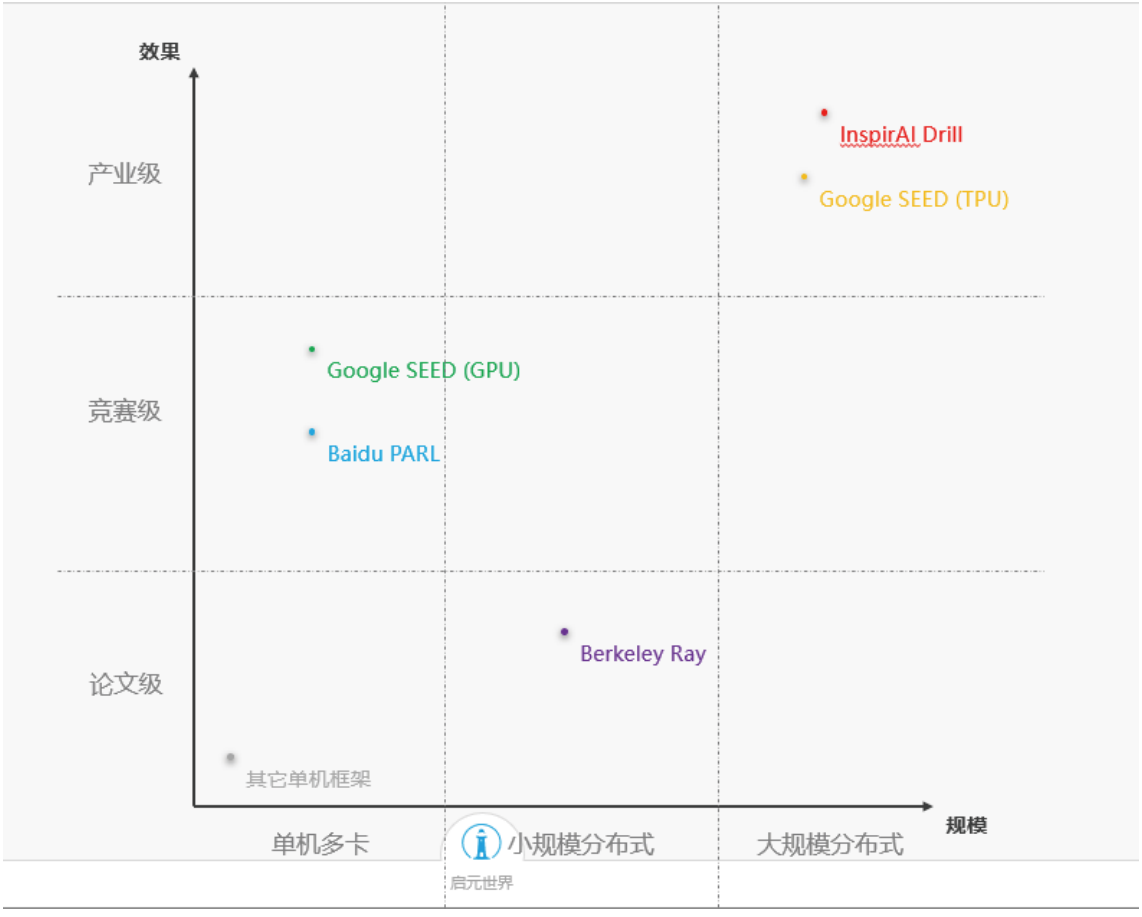


图 7：竞品对比

启元智能体训练平台和 Google SEED(TPU) 同属于产业级大规模分布式强化学习计算平台，因为二者都已经解决了该领域最为复杂的问题。如果 SEED 部署在 GPU 集群上，最多支撑单机 8 块 GPU，也就退化到单机多卡的领域，与其类似的是 PARL，从发布的信息上看，它们更多的是在解决竞赛问题。Berkeley Ray 可以较大规模的部署，但受限于分布式多进程的计算模型及实现，其规模扩展也受到限制，并且多用于研究领域。而其它的单机框架更是只能解决非常小规模的问题。

五、启元智能体训练平台的商业应用

启元世界依托于成熟的平台技术，凭借高强度的计算性能、大规模生产问题的算法能力、低成本的算法实施方案，可以将强化学习技术应用于诸多行业，如：智慧防务、数字娱乐、金融科技等。

图 8：平台产品：跨行业通用技术，市场空间极为广阔

六、结语

启元世界以星际争霸为平台，通过三年的潜心研究，将公司的强化学习技术水平推升至世界一流。并通过标准化、平台化，赋能于众多行业，为我们的生产生活带来巨大的社会和商业价值。

18 AI 防疫

帝国理工郭毅可：抗疫政策的评估，数据科学的应用

整理：智源社区 蒋宝尚

在第二届北京智源大会的“AI 防疫”专题论坛上，英国皇家工程学会院士、英国帝国理工计算机系教授郭毅可做了题为《抗疫政策的评估：数据科学的应用》的报告。

在报告中，郭毅可详细介绍了如何根据数据建立数学模型预测疫情。郭教授表示：传染病学、流行病学是一门标准的数据科学，同时数据科学并不一定非常复杂，换句话说，针对传染病的数据科学研究都是比较直观的。

在报告中，郭教授还具体介绍了动态和静态两种传染病模型的细节，也对之前的建模预测效果进行了展示，同时对中国和欧洲的两种抗疫政策进行了简单评价。

以下是文字整理：

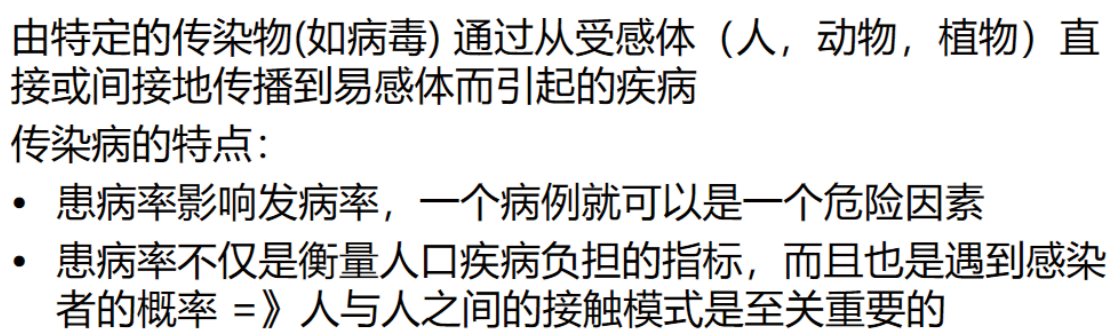


图 1：什么叫流行性传染病?

今天演讲的题目是《抗疫政策的评估：数据科学的应用》，我先从流行传染病开始谈起。传染病与普通疾病的最大区别在于：普通疾病的患者影响自己，传染病由于其传染性在，会进一步影响患病率，而患病率影响发病率，一个病例就可能是一个危险因素。另外，患病率不仅是衡量人口疾病负担的指标，而且也是遇到感染者的概率，其和人与人之间的接触模式高度相关。

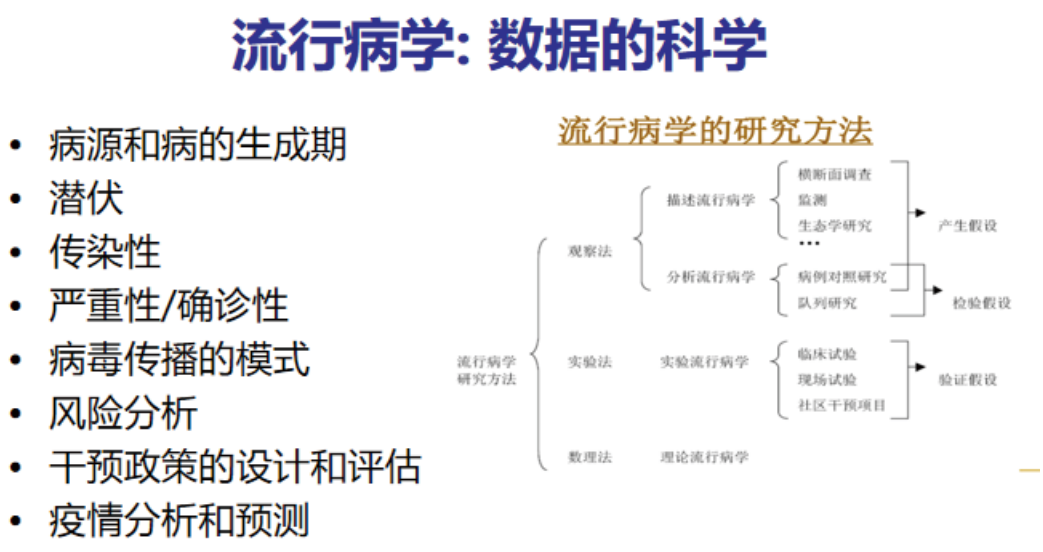


图 2：流行病学是一门关于数据的科学

因此，传染病一旦出现，没有患病的人们关心自己会不会受到传染，政府则关心如何让更少的人被传染。这时，首先需要进行的是数据科学研究，即通过观察有多少人患病（例如进行关于病毒的核酸检测），判断病毒的潜伏期、传染性和传播模式。政府也应出台相应的防疫政策，虽然政策能在一定程度上限制传染病的流行，但却给经济发展带来了风险，这时则需要对政策进行全面的分析和评估。因此，传染病学、流行病学是一个标准的数据科学。

一、静态传染病模型：求解概率方程

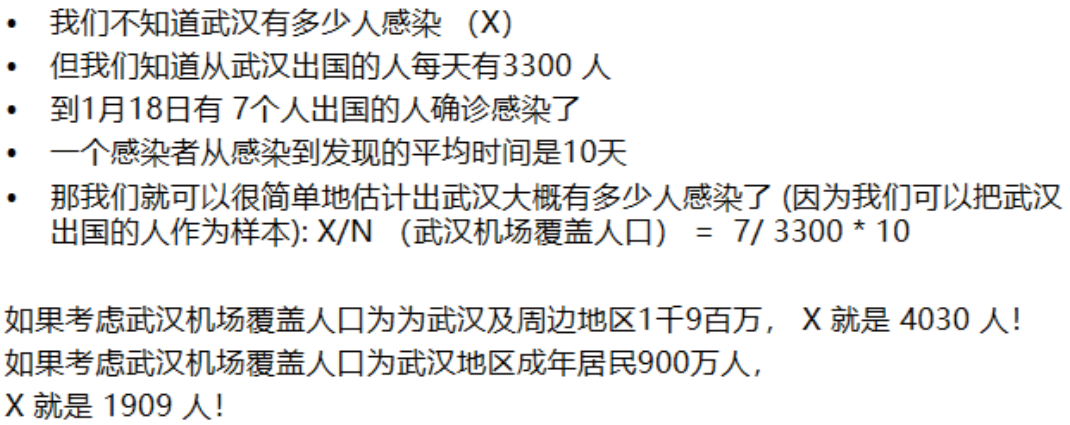


图 3：帝国理工对武汉疫情的早期预测

数据科学并不一定复杂，换句话说，针对传染病的数据科学研究都是比较直观的。例如帝国理工对武汉疫情最早的预测：我们不知道武汉有多少人感染，但我们知道从武汉出国的人每天有 3300 人；到 1 月 18 日有 7 个出国的人确诊感染了；另外，一个感染者从感染到发现的平均时间是 10 天，那么我们就可以简单地估算出武汉大

致感染的人数。因为我们可以把武汉出国的人作为样本，通过求解概率方程式就能得出感染人数。

具体而言，如果考虑武汉机场覆盖人口为武汉周边地区 1 千 9 百万，那么感染人数就是 4030 人，如果考虑武汉机场覆盖人口为武汉地区成年居民 900 万人，那么感染人数就是 1909 人。

2020-01-29 06:11 | 湖北省卫生健康委员会

2020年1月28日0时-24时，湖北省新增新型冠状病毒感染的肺炎病例840例（武汉市新增315例、黄石市新增33例、十堰市新增23例、襄阳市新增61例、宜昌市新增12例、荆州市新增30例、荆门市新增28例、鄂州新增27例、孝感市新增101例、黄冈市新增111例、咸宁市新增21例、随州市新增46例、恩施州新增13例、仙桃市新增5例、天门市新增11例，潜江新增1例，神农架林区新增2例）。全省新增死亡25例，其中：武汉市19例，孝感市2例，荆门、鄂州、黄冈、天门各1例。

截至2020年1月28日24时，湖北省累计报告新型冠状病毒感染的肺炎病例3554例（其中武汉市1905例、黄石市86例、十堰市88例、襄阳市131例、宜昌市63例、荆州市101例、荆门市142例、鄂州市84例、孝感市274例、黄冈市324例、咸宁市112例、随州市116例、恩施州51例、仙桃市32例、天门市34例、潜江8例，神农架林区3例），已治愈出院80例，死亡125例(其中武汉市104例,黄石市1例、宜昌市1例、荆州市2例、荆门市4例、鄂州市1例，孝感3例、黄冈市5例、天门3例，潜江1例)。目前仍在院治疗3349例，其中重症671例、危重症228例，均在定点医疗机构接受隔离治疗。累计追踪密切接触者22095人，尚在接受医学观察20366人。

注意： 当时一个感染者从出症状到入院确诊的平均时间是10天

图 4：2020 年 1 月 28 日湖北省新冠肺炎疫情情况

这个简单的预测非常有价值，因为当时抗疫政策的制定必须要知道感染的规模。该预测结果也在 1 月 29 日得到了验证，根据当时卫健委的报告，湖北省有 3500 人感染，武汉有 1900 人感染，由此可见当时的预估是较为准确的。

二、动态传播模型：用流动数据讲述生命

图 5：传播动态系统数学模型的发明者

上面是简单的数据科学，下面介绍复杂一些的动态变化。关于动态变化，传染病学最重要的一个工作，是所谓的 SIR，即传播动态系统的数学模型，由两个物理学家发明。此传染模型带有普遍性，是一个 General Model，其概括了传染过程中的三个人群：易感者、感染者，恢复者。

先来看一个简单的动态模型，即假设治愈的患者能获得“终身免疫力”，不再传染其他人； 再者，还要去除干扰因素。这时所研究的对象是两个部分，一是从易感者到感染者的传播速率，二是从感染者到免疫 / 死亡者的周期。针对这两部分，动态模型会描述三个状态： 易感状态、感染状态、治愈状态。

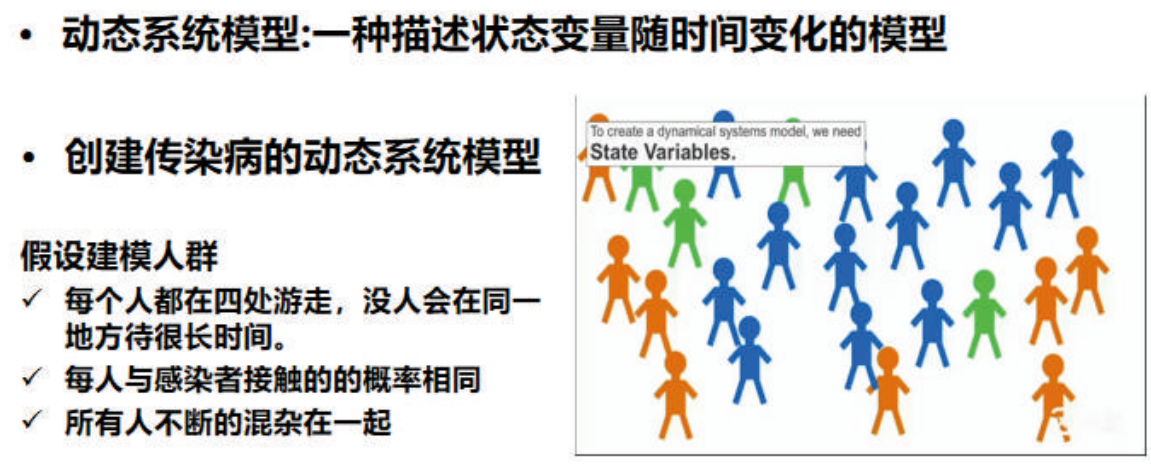


图 6： 传染病动态系统模型

另外，此动态模型对人群也有三个假设：1. 每个人都在四处游走，没人会在同一地方待很长时间；2. 每人与感染者接触的概率相同；3. 所有人不断地混杂在一起。

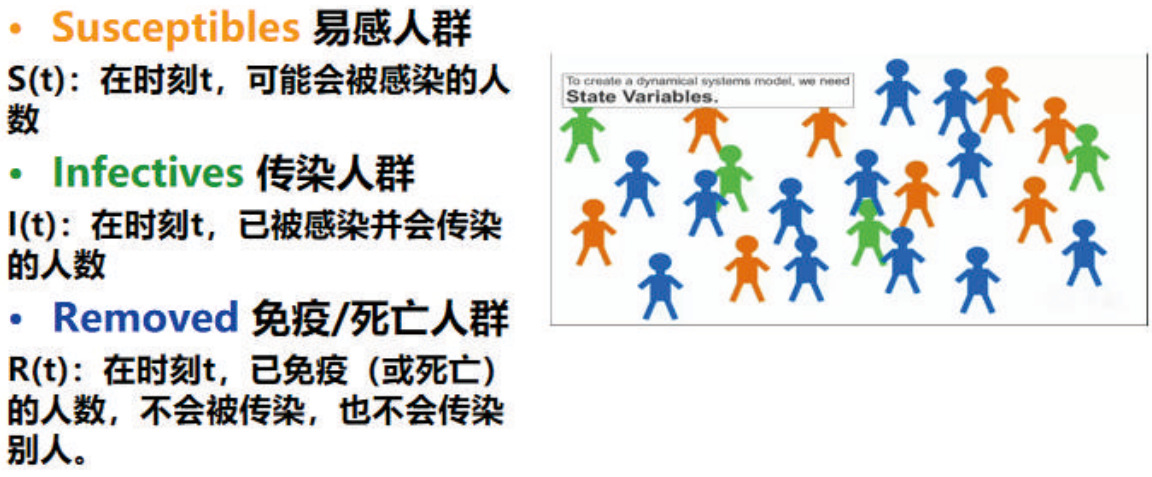


图 7： 三个动态变化的人群： 三种状态变量

三个动态变化的人群对应三种状态变量，其中易感人群： 在某时刻可能会被感染的人群； 传染人群： 在某时刻已被感染并会传染的人数； 免疫、死亡人群： 在某时刻已免疫（或死亡）的人数，不会被传染，也不会传染别人。

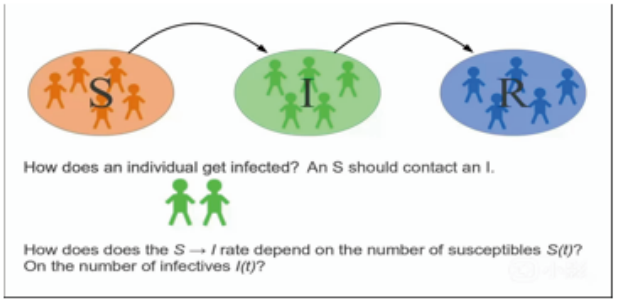
有了假设、变量之后，然后根据 SIR 模型找出动态变化规律，即需要确定个体状态如何转换、两个转化速率:

不感染到被感染、感染到治愈。

- S→I rate取决于什么?
- ✓ 单一个体被感染的可能性与I(t)感染人群数量成正比
- ✓ S→I rate也包含任意易感染者S(t)的影响
- ✓ 个体被感染的可能性与S(t)和I(t)的数量都成正比。
- 所以，在时刻t

$$S \rightarrow I \text{ rate} = b\,S(t)I(t)$$

*此处b为一个感染速率参数



- ✓ 参数b包含2方面影响：有效接触的可能性和接触导致感染的可能性
- ✓ b数值大对应人群比较活跃的社会互动，疾病高度传染的。
- ✓ b数值小对应隐居的群体，疾病难以传播。

图 8：感染速度：S → I rate

以上就是基本模型的基本思想，虽然会涉及一些数学，但非常简单。例如从易感到被感染取决于什么？当然取决于被感染人数，如果感染人数很多，或者很多人被感染，感染速度就会加快； 或者被易感暴露的人群很多，那么感染速度也会加快。

此外，还会涉及到一个参数，即针对速度的参数，其受两方面的影响，一是，有效接触的可能性； 二是，接触导致感染的可能性。也就是说，如果对应人群比较活跃的社会互动，那么参数就大； 如果对应隐居的群体，疾病难以传播，那么参数就小。

- I→R rate取决于什么?

只取决于感染的数量 I，I→R rate与I成正比

- 所以，在时刻t，

$$I \rightarrow R \text{ rate} = a*I(t)$$

*此处a为一个恢复速率参数: 如何让感染得不再感染了

图 9：恢复速率：I → R rate

上面是感染的速率，那么恢复速率由什么决定呢？其实，只取决于一个变量，就是感染的数量。

假定不考虑采取的医疗措施（因为医疗可以加快治愈率），感染的数量与恢复速率成正比。但是数学表达式中也

会有一个回复速率参数，取决于如何让之前感染的不再感染了。这里有两种方式，一种是治好，一种是死亡。

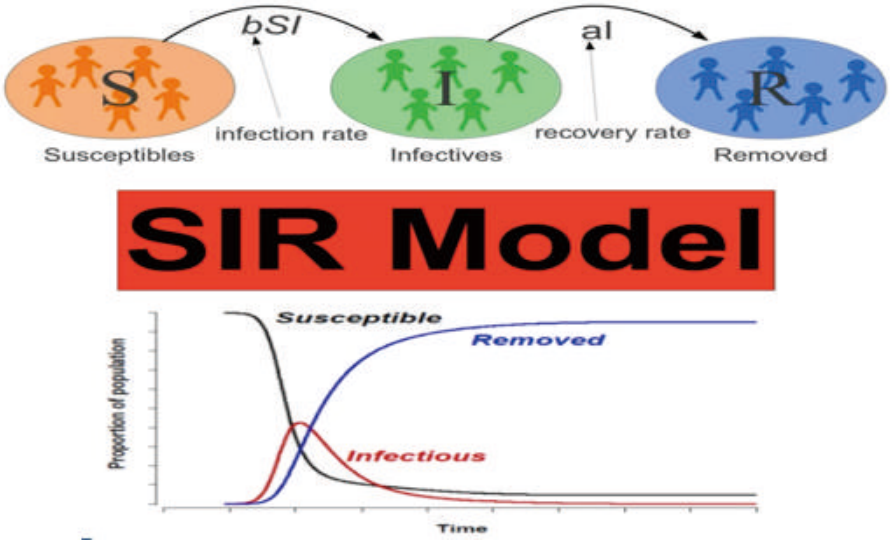


图 10：SIR 模型及转化速率

其实，这一非常简单的传染病模型预示着会有“疾病峰值”的出现： 刚开始的时候随着时间的推移，很多易感人群被感染了，感染率就上去了，到了一定规模以后所有人都生病了，没有人可以感染了，感染率就会下降，随后出现的都是治愈病例。其实，所谓的群体免疫基本上符合这种思想。

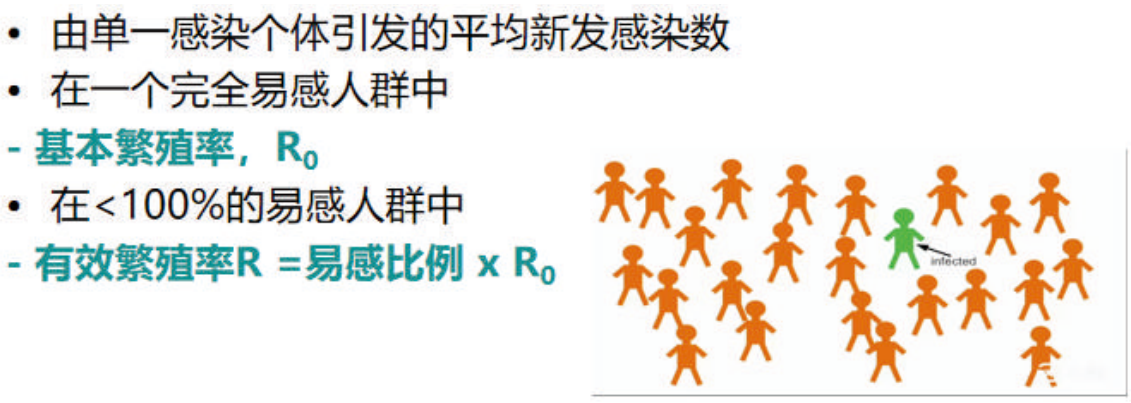


图 11：基本繁殖率

有了这个模型以后，其实可以做很多事情，其中一项非常重要的工作就是实时模拟各国现在处于各种各样干预政策中的传染率。这里会涉及一个重要的参数，叫做基本繁殖率 R0，即单一个体可以引起多少个新的感染者。

如果没有干扰政策，此 R 就是基本繁殖率，如果存在干扰政策，那么模型的易感比例就会改变，此时的 R 叫做有效繁殖率。

如果 R0 大于 1，那么传染模型就是指数型，R0 等于 1 则感染保持恒定，R0 小于 1 则感染消失。

对于一种直接人传人的病原体

$$R_0 = \beta c D$$

其中

β:每次受感染者和易感者之间接触后，病毒的传播概率
c: 接触率
D:感染持续时间

图 12：基本繁殖率的决定因素

R0 由什么决定呢？基本上是三个参数：1. 每次受感染者和易感人群接触后，病毒的传染率（因为接触不一定传染）；2. 接触率，接触的频率；3. 感染持续时间。而 R0 的数学表达式则是由这三个参数相乘。

具体而言，传染率如果是 0.15，接触的频率是 12，感染的时间是一周，那么基本繁殖率是 1.8。

三、干预政策分析：中国和欧洲对比

如果有了干预政策会改变什么呢？改变有效繁殖率，即把易感的人群控制住，把受感染的人群控制起来。

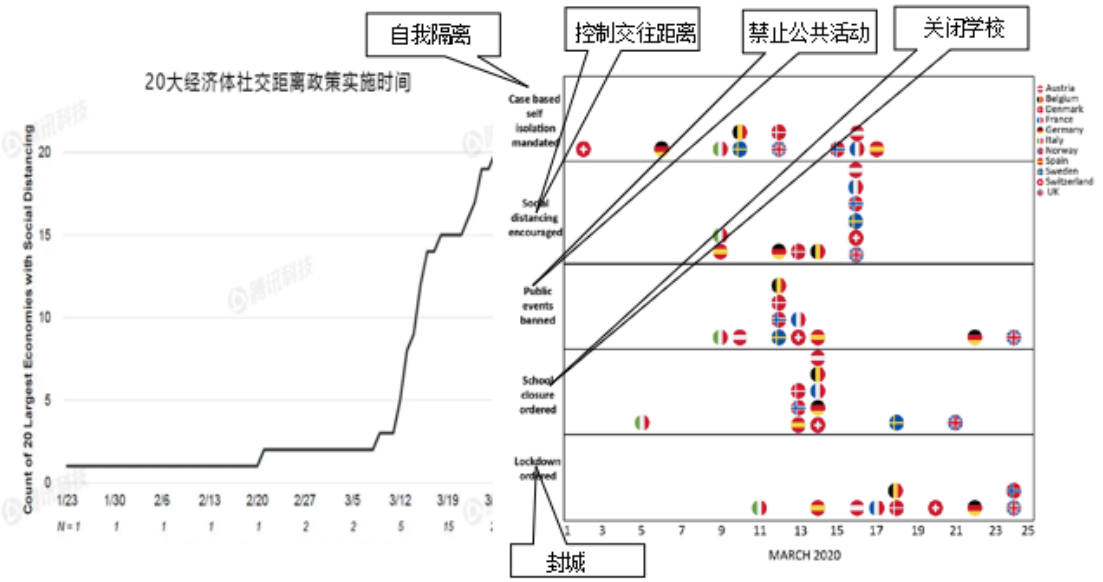


图 13：各国的干预政策

下面讲一讲对各国干预政策的研究。疫情爆发之后，二十大经济体社交政策各有不同。例如中国非常严格，瑞典、英国宽松。所有的政策都有其道理，即如何平衡生命与生活。举个例子，过马路有被车撞死的风险，但不能因为这个风险把交通封锁。因此，生命和生活平衡点的把握非常重要，如果照顾了生命死亡率和患病概率，那么人民可能在经济和人民生活上会有巨大损失，且其他原由的死亡率就会增加。

所以，这就要求我们仔细分析干预政策，然而定性分析无法得到想要的结果，最好是用定量分析，能够“互相比较”。定量之后，那么就能够将经济损失纳入模型，则会得到优化版本。当然，听起来非常科学和理性，但有的时候也很残酷，因为要考虑的因素非常多。

有多少干预政策呢？大概有自我隔离、控制交往距离、禁止公共活动、关闭学校，更严酷的就是封城。

图 14：通过人群流动的数据来决定干预政策

这二十大经济体中，干预政策的实施，在各国的基础是不太一样的。例如中国的有利条件是健康码，它可以帮助政策实施到细微处，即可以通过人与人接触的模式和个体的运动轨迹建立整个干预政策。所以这也是我们国家恢复正常秩序后没有出现太大疫情反弹的原因之一。毕竟，如果有一个人被确诊，那么其整个交往人群都能获知，则可以通过溯源对其进行控制，这样就不需要采取特别严控的政策来进行社交距离或者封城，经济可以更加放开一些。

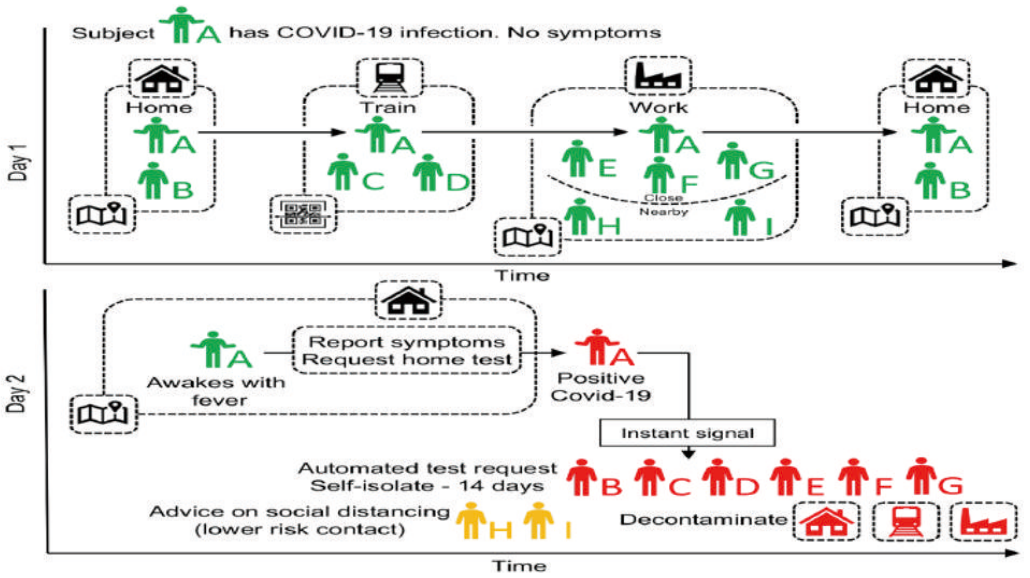


图 15：通过了解人与人接触的模式来优化干预

这种模式也存在缺点，即牺牲了个人的隐私。现在有很多研究都是希望通过在不影响隐私的情况下能够完成工作，例如通过 WiFi 可以建立联系基础（contact base）。

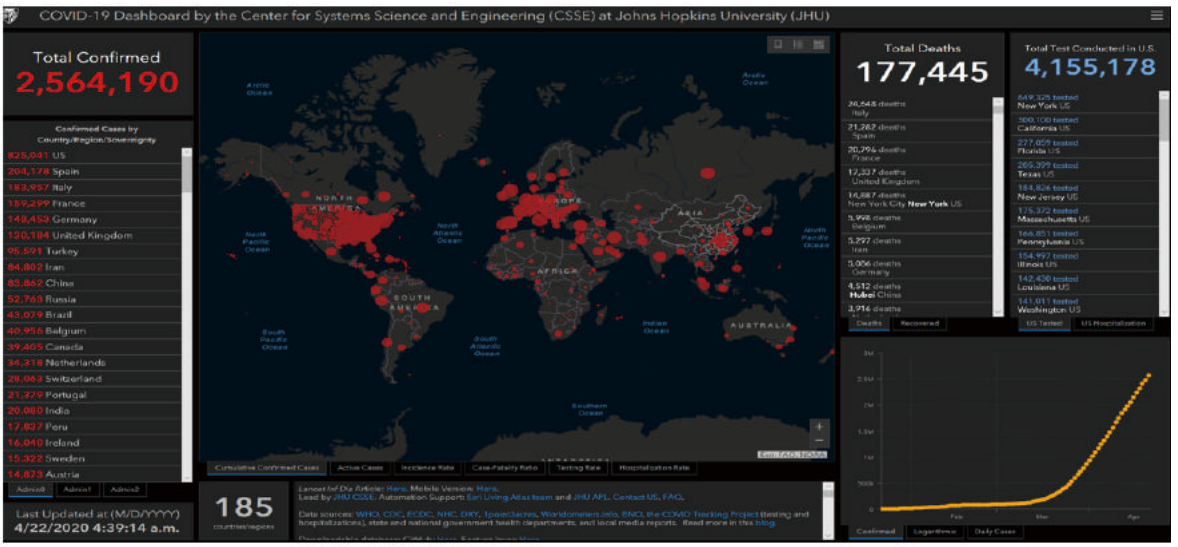


图 16：全球疫情网站

有了这些政策之后，便每天看上述网站，了解一下多少新增患者、新增死亡人数。最主要的是通过观察数据反推各国的政策有效性。

图 17：数据反映的政策干预结果：平均翻倍时间

其实，干预是有效果的。如上图所示，干预结果通过平均翻倍时间表现出来，即从 4000 人增长到 8000 人花费了多少时间。其实，封城之前基本上三天翻一倍，封城之后大概二十天才翻倍。这大大降低了病毒的传播率。

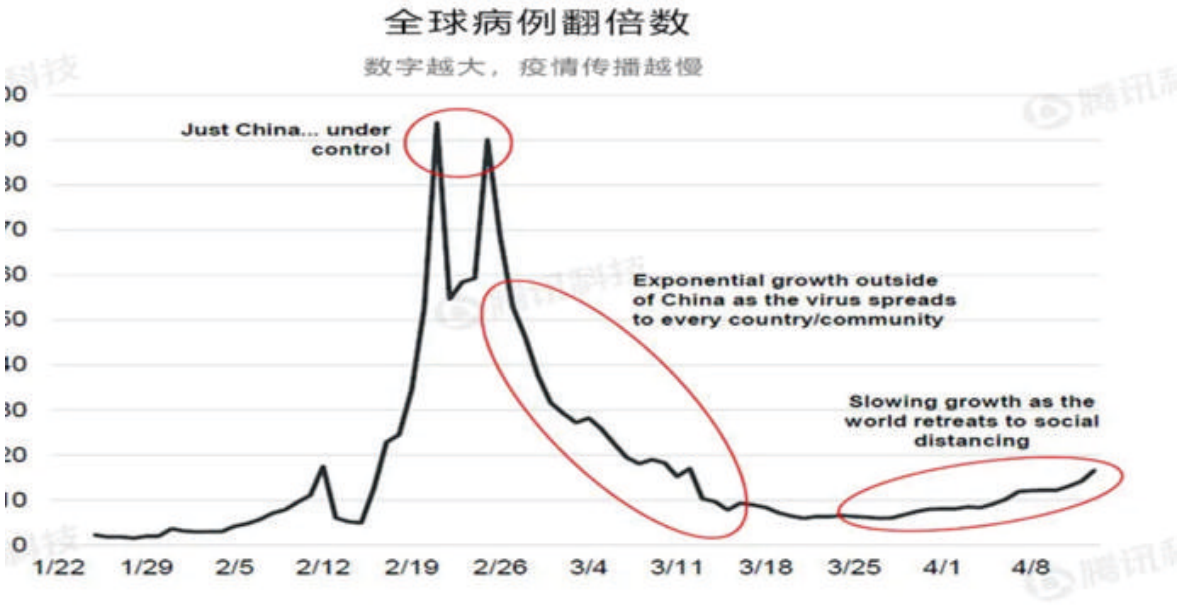


图 18：数据反映的政策干预结果：全球病例翻倍数

如上图所示，通过大规模的观察也可以了解这一现状。开始的时候“翻倍”花费的时间很短，大概为十天左右。2 月 1 日武汉封城，翻倍的时间增加到了 90 天。3 月初的时候欧洲爆发，翻倍的时间又缩短了。当然，这种衡量干预的方法都比较初级，并没有看到一个国家和一个城市的变化。

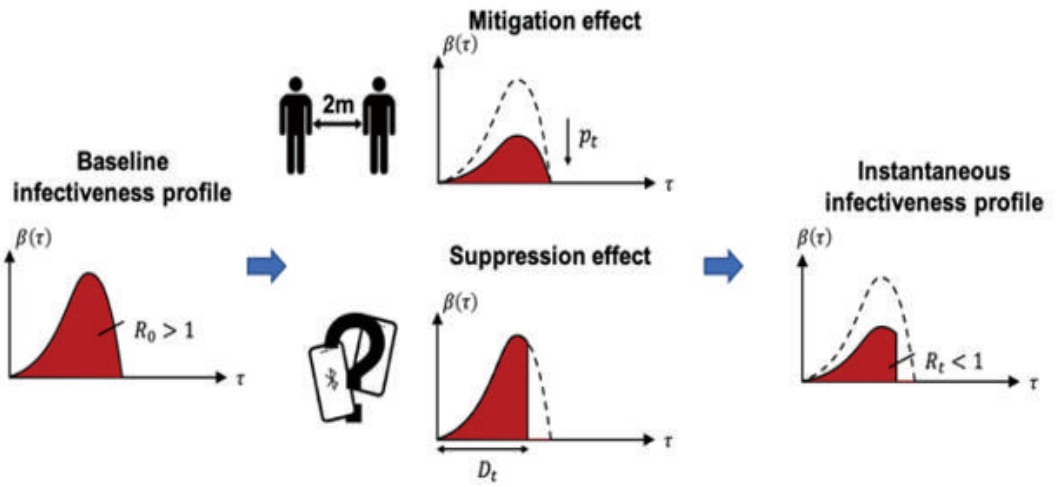


图 19：精确地量化干扰政策的作用

因此，为了精确地量化干扰政策的作用，我们用模型进行了模拟，模拟的结果就是 R 繁殖率（几何上表示的 R 就是传播曲线下的面积），即一定的时间内一个人能传播多少人。当然，传播的概率就是参数 B（Beta），下面的面积就代表传播的人数。

我们把政策的作用分成两大类：一类就是 S 到 I，只有缓和系数，就是我把 B 参数 降低下来，降低它的传染率。怎么降低？用保持社交距离、戴口罩等干扰方法。第二类是阻断，改变 I 到 R，即让 Dt 缩短（如果发现感染者，立即隔离，阻断其传染率）。

实际上任何一个政策都有两面性，既有阻断传染期的效果，也有降低传染率的效果，所以组合起来就是可以计算这个 R（繁殖率），希望能够小于 1。

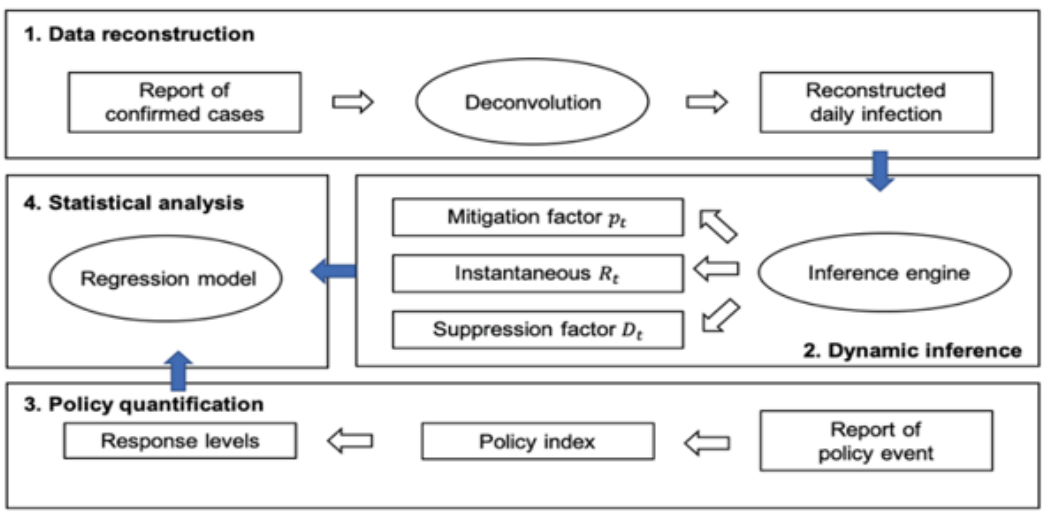


图 20：量化系统示意图

其实，整个观察以及模型结果就是报告的确诊病例。其实我们不可能知道这个国家到底有多少人感染了，除非做全民的测试，否则只能预测。那么如何从确诊病例预测全部感染者规模？我们的做法是把时间向后推，然后重建传染模型。

随后，就可以用贝叶斯的理论推断三个参数，一个参数是缓解系数（Mitigation factor），另一个是有效繁殖率（instantaneous），最后一个是阻断系数（Supperssion Factor）。

有了这些以后，就可以构建前面提到的 SIR 模型，从而把它和政策进行结合分析。即回答一个政策到底影响了哪些因素这些问题。

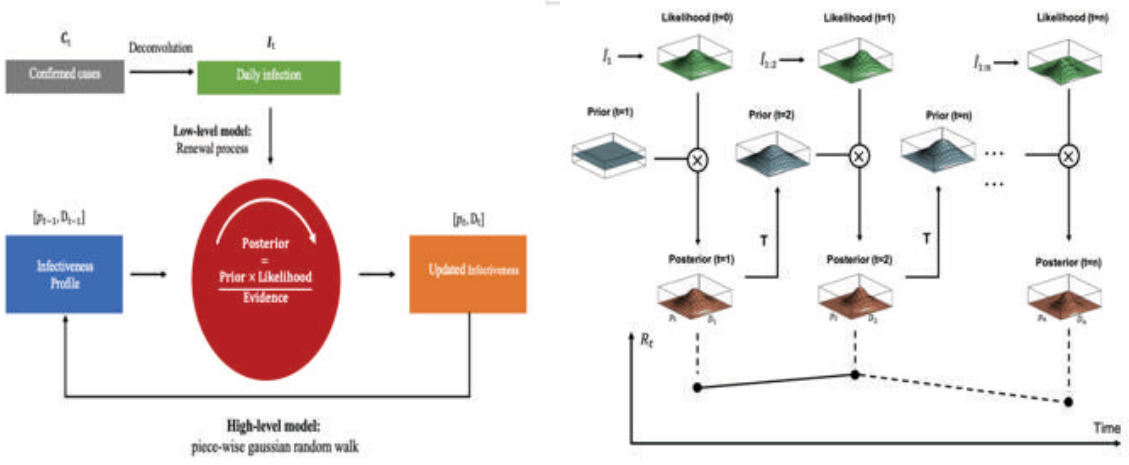


图 21：用贝叶斯估计来计算 Rt

整个模型最难的部分是用贝叶斯进行计算 Rt。毕竟，我们要求的对 RT 的估算是每天实时进行，所以由于政策具有延迟性，导致推算变得异常艰难。

这里我们采用的思想是：能够观察到的都是发生在过去的，所以还需要往后推。具体而言，我们通过贝叶斯的方法，通过顺序的学习，即根据前几天算出来的 RT 改变后验概率，也就是期望改变参数，把后验概率最大化。综上，整个过程等于是进行了一个顺序的贝叶斯推理。强调一下，我们并没有使用神经网络，而是运用贝叶斯的高斯过程。

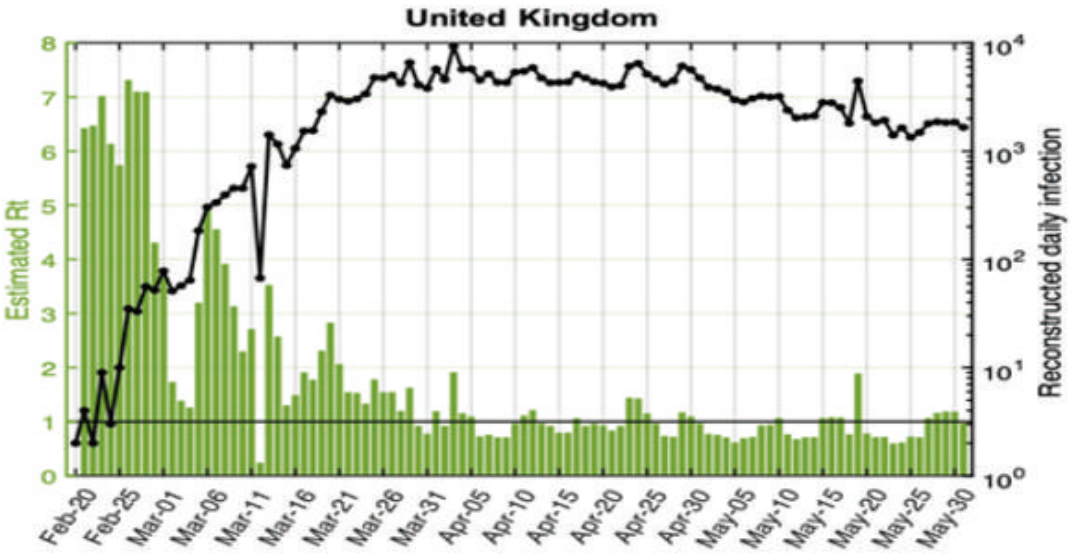


图 22：揭示伦敦的 Rt 变化

运用上述推理过程，就可以得到一个非常漂亮的关于各个城市的描述，如上图所示伦敦 RT 的变化，黑线就是根据确诊病例估算出的感染，可以看到伦敦到了 4 月 5 日以后的 RT 基本上在 1 以下，所以实际上传播已经开始控制住了。

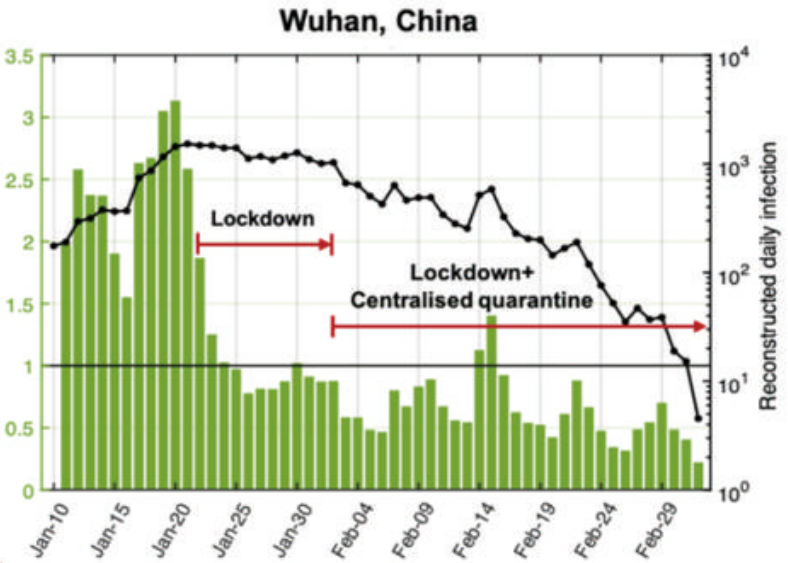


图 23：揭示武汉的 Rt 变化

武汉则更明显，封锁之前 R 值非常高，春节的时候 R 达到了 3。23 日封城以后 R 值迅速降低（因为采取的不仅是封城政策，还不让上街）。因此，1 月 23 日到 2 月 15 日中，实际上新患病的很少，几乎所有的病例都是前面感染的，只不过那个时候爆发了症状。

如上图所示武汉的 Rt 曲线有一个跳跃，因为武汉更换了市长，市长所采用的防疫政策是将过去的所有疑似都当成“确诊病例”进行控制，这作为一个人为的动作，发挥了很大作用。随后加上方舱医院的使用，可以看出武汉从 2 月 3 日疫情得到控制。这里我们也可以明确了政策对于整个抗疫的影响。

esponse	Representative Measures	Impact of measures R_t relative reduction	Suppression effect D_t relative reduction	Mitigation effect p_t relative reduction
evel 0 inimal response	No mandatory restrictions	0	0	0
evel 1 oft response	Closing schools, International travel controls.	35% CI:[25%, 45%]	22% CI: [17%, 27%]	29% CI: [18%, 38%]
evel 2 trong response	Cancel public events, Restrictions on gathering, Restrictions on internal movement.	60% CI:[54%, 65%]	26% CI:[21%, 30%]	56% CI:[50%, 61%]
evel 3	Close workplace, Close public transport, Stay-at-home requirements.	71% CI:[68%, 74%]	37% CI:[35%, 40%]	67% CI:[64%, 70%]
evel 4 mergent response		74% CI:[71%, 77%]	40% CI:[37%, 42%]	70% CI:[66%, 73%]

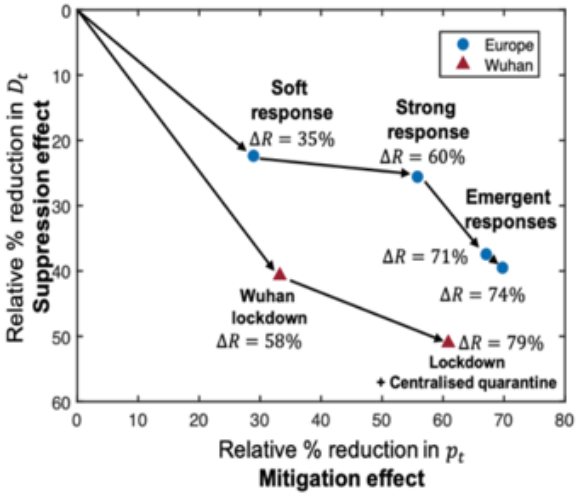


图 24：欧洲政策的评价结果

我们也对欧洲的所有政策进行了评估。其实，欧洲和中国采取两种不同的政策，欧洲的政策基本上没有强制性的封城，但也关闭了学校、工作场所，控制了交通。其实，每个政策我们都对应 R 的变化。其中，Soft Response 可以降低 30%，Strong Response 可以降低 70%，所以还是非常有效果。而中国的做法截然不同，因为中国采取的是非常严格的政策，“一下子”就把 R0 减掉 79%–80%。

因此可以看到各国政策的评价是不一样的。当然，我们没有分析具体“成本”，如果这个评价再加上“成本”，然后进行比较，可能就比较有意思了。

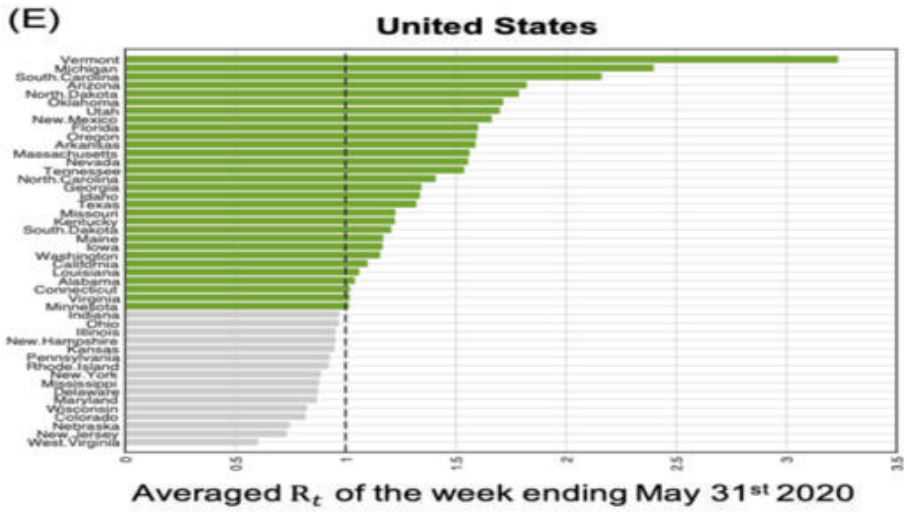


图 25：美国疫情的第二次爆发

RT 确实在一定程度上能代表预测性，例如上图我们在 5 月 31 日计算的美国 RT，那个时候就看到美国毫无疑问在面临着第二次爆发，因为其 Rt 的数值在 30 个州全部超过了 1。

由于当时 R 的效果在大概 10 天后才能观察到，所以到了 6 月 12–13 日的时候，30 个州当中的 29 个州都有第二次疫情爆发，其中 5 个州是高爆发（Record High），因此预测比较准确。

四、总结：模型参数改变，背后是人命代价

总结一下，将人工智能、数据科学应用在传染病防控当中，效果非常棒。什么叫做人工智能？就是用物理来描述一个世界，把它变成变量之间的转换，然后通过观察得到数据，通过观察推断模型，这才是真正人工智能的伟大意义。

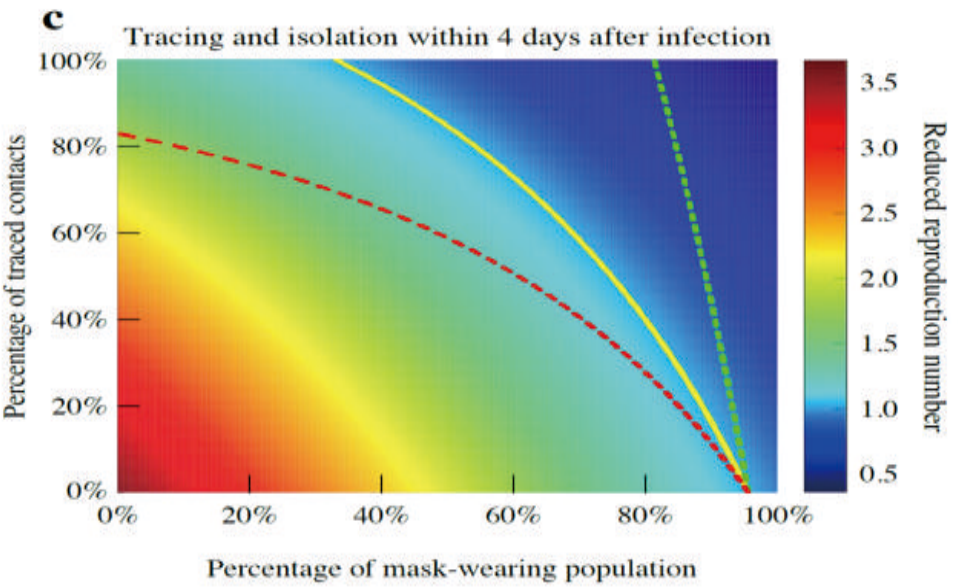


图 26：干预与否：改变的是模型参数

在建模过程中，我们需要更多的是关于模型的定义和模型参数的学习，例如上图戴口罩的模拟，通过戴口罩改变 R0、RT 的数值。

其实，干扰与否对于数据科学和人工智能来说，可能就是改变一些模拟的参数。但是对于社会，其背后的代价会是生命。

图 27：干预与否：代价是生命

如上图 4 月 20 日的数据，香港和纽约的面积差不多大，香港感染了 1000 多人，一共死了 4 个人，纽约 4 月 20 日的死亡是 1.3 万人，而整个大纽约最近的一个数字 3 万多，如果只看纽约城（New York City）这一数字也达到了 1.8 万。

那么如何评价强烈干预的政策？其实，这个问题是可以讨论的，如果是像香港这样非常强的干预，到今天为止还是封闭状态，与全世界不能正常交往。那么，这对香港的 GDP、经济、民生的副作用是非常大的。因此付出的代价换来了低死亡率，是不是完全合理？这个问题也是可以讨论的。

最好的做法是在生命和经济当中取得平衡，即在保证生命救助同时，也能保证生活。这种平衡也是我们想要的未来社会，要让城市有免疫力也要有抗灾力，如果有一套规矩，能够指导制定平衡政策，那么这座城市就是一个真正的智慧城市。

这一次我们对智慧城市的定义和理解有了很大的进步，以前我们理解智慧城市就是交通不堵，污染更少等等。实际上这些东西都是皮毛，真正一个城市的智慧在于能够抗灾，能够免疫，能够保证人民的生活，能够保护人民的健康，这才是最重要的。

人大教授文继荣：疫情突如其来，大数据人工智能如何沉着应对？

整理：人大高瓴人工智能学院

在 2020 北京智源大会“AI 防疫”专题论坛中，中国人民大学文继荣教授分享了题为《大数据人工智能技术 + 疫情防控：经验和反思》的报告。

文继荣，中国人民大学信息学院院长，中国人民大学高瓴人工智能学院执行院长，智源首席科学家。主要研究方向是互联网搜索与数据挖掘等，获得过 50 多项美国专利，同时在国际著名会议和期刊上发表了一百多篇论文，也是信息检索领域主要期刊 ACM Transactions on Information Systems(TOIS) 的副主编 (Associate editor)。

2020 年春节期间，新型冠状病毒疫情爆发，在智源人工智能研究院的部署下，文继荣教授和许多研发人员都参与到了北京市疫情防控的相关工作中，并研发出了新型冠状病毒肺炎防控智能追踪服务系统和时空足迹近距定位系统，为北京市的抗疫工作做出了一定贡献。报告中，文继荣教授分别介绍了两个系统的主要原理及功能。

一、新型冠状病毒肺炎防控智能追踪服务系统

该系统主要是通过汇聚用户散布在各个互联网公司的片段式数据，利用用户在移动互联网的“数字脚印”，从而围绕风险人员绘制轨迹信息，利用算法对高危人员进行分析、追踪与筛查，最终确定密切接触人员名单，达到快速定位到重点防范区域、防范人群的作用。自 1 月 28 日启动使用到 2 月 2 日运行生成首批数据，该系统已经持续发现疑似接触人超过 10000 名，并且能够根据人工智能算法自动生成活动报告，目前该系统仍然在持续为北京市的防控工作提供保障。

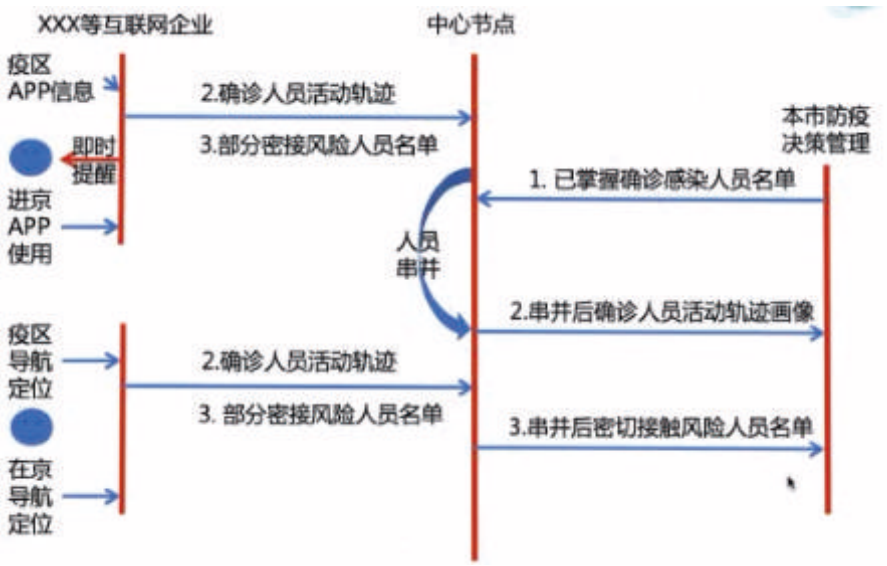


图 1：基本数据的处理流程

图 2：系统首页示意图

二、时空足迹近距定位系统

该系统是解决 GPS 在室内的定位问题，可以实现精准定位到城市中每个房间的风险防控服务，通过蓝牙、局域网信号、气压计等信号，对人员时空轨迹数据进行采集，追溯近距离接触人员，借助大数据和人工智能技术更精准的进行疫情防控，从而降低隔离成本，为企业复工复产提供支持和保障，因此，这个系统最典型的应用场景便是人员较为密集的室内办公场所。

另一方面，文继荣教授还提出了在此次疫情防控过程中所产生的三点思考:

1. 下一次公共卫生事件突发，我们能不能做的更好?

在应对此次新冠病毒疫情的工作之下，文继荣教授发现了暴露在疫情下的“数据孤岛”、“数据安全性”、“数据动态性”和“决策及时性”等问题，疫情虽然尚未结束，但我们已经要开始思考应对此类事件的解决方法和措施，保证数据信息的全面准确等，为未来的挑战做好准备。

2. 完全的隐私保护是不可能的!

文继荣教授以苹果谷歌联合推出的疫情追踪系统为例，虽然苹果谷歌在操作系统层面上进行设计该系统，并且声明不会泄露用户隐私信息，但是文继荣教授针对现实生活中人们获取隐私数据的一种经典方法的变形，提出了“完全的隐私保护是不可能的”这一见解。

3. 公共利益和个人隐私的让渡。

随着我们的世界从物理世界逐渐过渡到数字世界，在网络世界中会逐渐分化出另一个包含真实性格、记忆等的数字分身，而当用户的数据和信息在互联网中留下痕迹后，文继荣教授表示我们其实已经在不知不觉中让渡个人隐私，而对于公共利益和个人隐私的冲突问题，文继荣教授表示需要政策和法律来界定边界，并且需要公开进行讨论该问题。

北大教授宁毅：科学、精准的公共卫生 - 应对慢性病和传染病双重威胁

整理：智源社区 贾伟、王静

在智源大会“AI 防疫”专题论坛上，北京大学宁毅教授做了主题为“科学和精准的新公共卫生应对慢性病和传染病双重威胁”的报告。

宁毅教授是北京大学公共卫生学院教授、美年大健康首席科学家、公共卫生专家，并且在弗吉尼亚做过医学院的助理教授、博士生导师，也曾在跨国公司 GSK 任职。

报告中，宁毅教授提到，全球疫情不太乐观，如果能够较好地防控外源性输入的病例，中国境内疫情反复的压力就会急剧降低。这种防控范围较大，在斩断传播途径这样的过程中，每个个人、家庭以及单位发挥着重要的作用，甚至是主战场的作用，国家教育、健康促进、家庭行为改进等等，这些是保证生活和防够保持常态化的关键。相对来说，应当把防控做得更精准，可以局限到某些人群或地域进行防控。

以下演讲正文——

从去年一月份开始，一直到今天，疫情的变化每天都发生着戏剧性的变化，这吸引着我们每一个人。今天，我把近一段时间对于过去的一些回顾，以及我们对未来的一些思考与大家进行讨论。

一、疫情概况

首先看一看今天（2020 年 6 月 23 日）疫情的状况，全球如今有大约 907 万感染者，死亡 47 万人。过去的一个月，大家可能对这个数字已经麻木了，但我们还是需要去想，这样的数据究竟反映了什么？

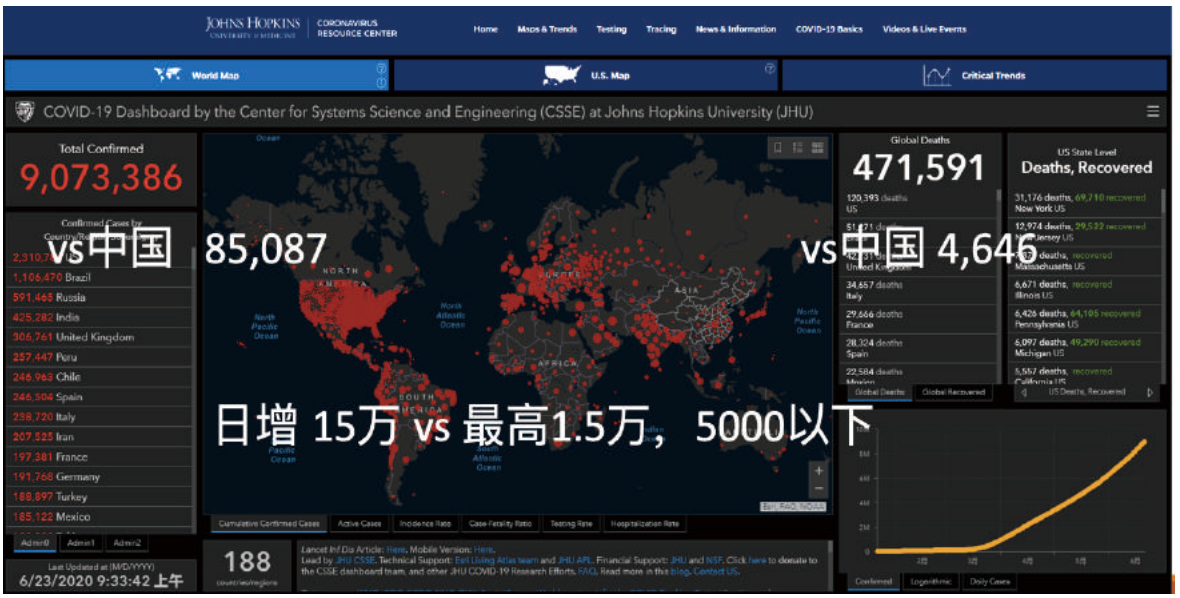


图 1：6 月 23 日，世界范围内的疫情对比（中国 vs 世界）

比较一下中国。中国在整个疫情期间一共有 8 万多人感染，但现在全球感染者已经是这个数字的 100 多倍了。按照这样的发展趋势，到本月底，感染人数将突破 1000 大关。从死亡人数上看，中国死亡人数是 4646 人，全球死亡现已超 47 万人，是中国死亡人数的 100 多倍。从新增感染人数上来看，目前整个世界还仍以每天 15 万人的速度增加； 而中国感染人数最高的一天达到 1.5 万，之前与之后大致都在 3000–5000 人之间变化，后来稳定在 1400–1200 人变化。从这个对比中，可以看出，现在全球疫情的压力非常大。之前我曾经讲过，中国能不能消灭或者消除这个疾病，不取决于中国自己，而取决于全球的疫情控制情况，所以到目前为止我们可以很肯定地说，这个疾病会长期和我们共存。

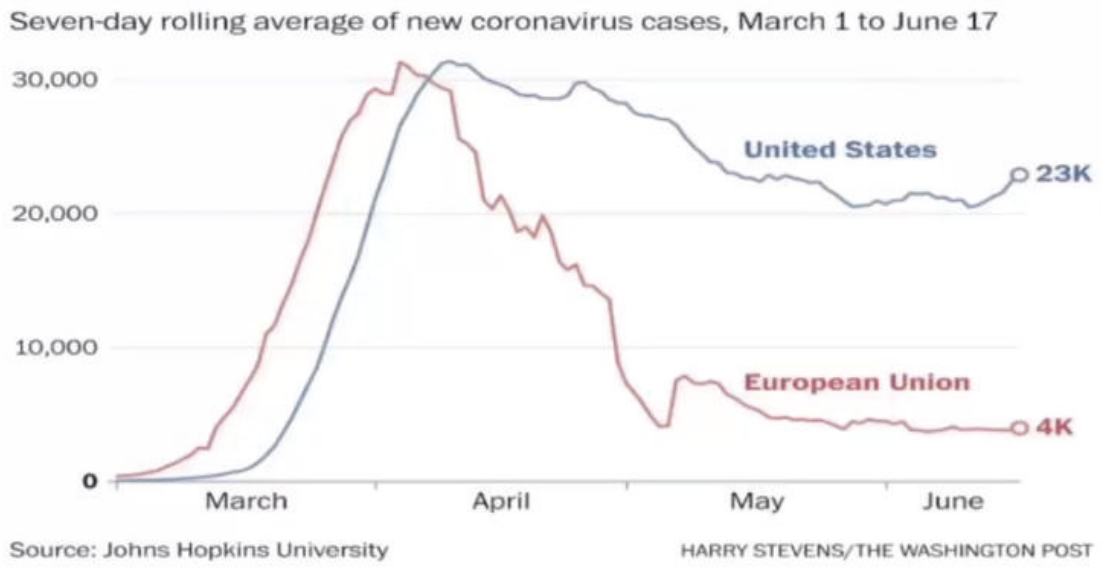


图 2：美国和欧洲的比较：相似的基础，不同的结果。

各个国家都采取了不同的措施，欧洲和美国在基本条件相似的情况下，两个国家的患病率和发病情况却表现得非常不一样。

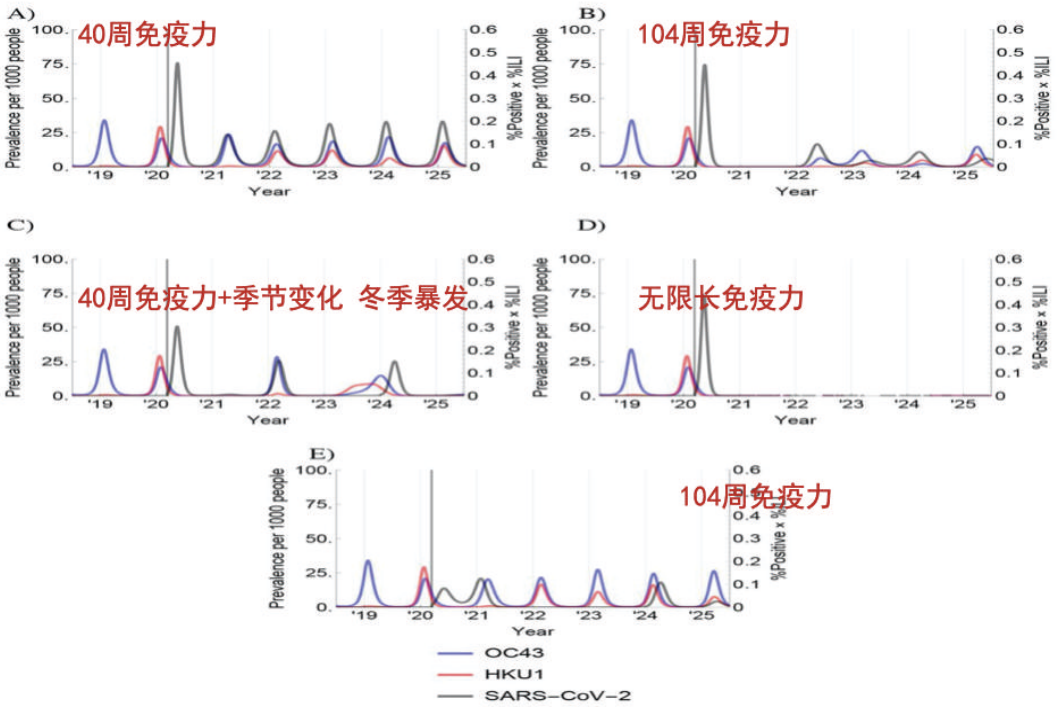


图 3：各种情况下新冠流行的预测

哈佛大学的研究小组进行了一个预测，即根据人们在产生病毒抗体之后能够维持的时间来预测疫情未来的发展。从现在的数据来看，真实情况更接近于左上角的数字变化，也即感染之后有 40 周的免疫力，预测结果是： 到 2025 年，新冠疫情仍会流行。这里提到 40 周的免疫力，也就是免疫力能够保持 10 个月； 但今天有些报道中又提到免疫力维持的时间只有 8–12 周，说明我们的抗体水平明显下降了，未来三到五年疫情很难看到明显的控制。

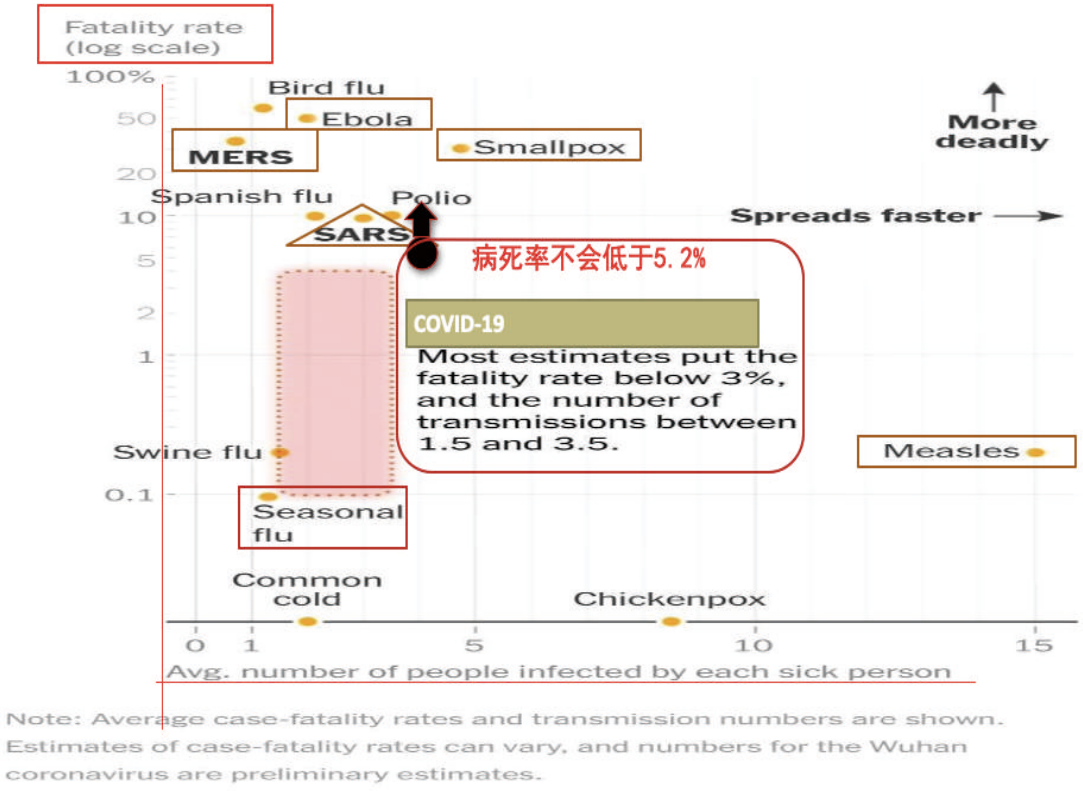


图 4：曾经和现在认知的基本参数：不支持中国群体免疫（国外不得已）

现在国内面临的最大争议是，中国要不要做群体免疫。我们必须回顾一下和其它疾病的比较。图 4 中横轴表示 R0，也就是传播系数，过去我们认为 COVID–19 的传播系数大约是 3–4，但现在来看，人口密集的情况下可能会达到 5.7。如果做出很好地控制，R0 可以接近 0。但 0 是有前提条件的，就是需要严格防控。我们曾经认为这是一个大号的流感。流感在美国的病死率是 0.1%，但目前 COVID–19 在美国的病死率是 5.2%，也就是说病死率是流感的 50 倍还要多；其他国家的情况也大体相近。针对我们国家疫情，早期我曾经判断病死率不会低于 3.5%，因为当时我们国家的数据还是低于 1%，当时“知识分子”采访我，问“为什么”，我给出的原因是“很多病重的患者还没有死亡”，随后统计上去之后应该能达到 3.5%。现在看来，当时还是比较保守，但那个时候也是国内甚至国际上，认为最高的一个估计。而现在，各个国家还都有大量的新发病人，相对第一波传播是比较发达的国家，第二波非发达的国家病死率会怎么样？我预计病死率会超过 5.2%。在这种情况下，任何一个国家思考群体免疫的时候都要想：发病阶段有没有足够的医疗资源去应对？这样的死亡率能不能接受？

回到动态的过程中来看各个国家的变化。我们国家继承原来苏联传统的疾病控制理论，提出了三点：控制传染源、切断传播途径、保护易感者。从图 4 中可以看到，这三点并不是相互独立的。传染源如果多，传播途径就要加力，也可以减少可能的易感者。

图 5：传染病的动态中，思考各个国家的疫情变化

现在来看，美国和欧洲的一些国家认为现在似乎达到了群体免疫，疾病得到了很好的控制，疾病的新增感染人数也下降了。但要注意到，这只是暂时的，因为前一段时间隔离措施比较严格，传播途径上有所着力，很多易感者并没有发病转化为传染源，从而使传染源降低了。一旦未来各个国家恢复到正常生活状况，疫情必然会再次反弹。

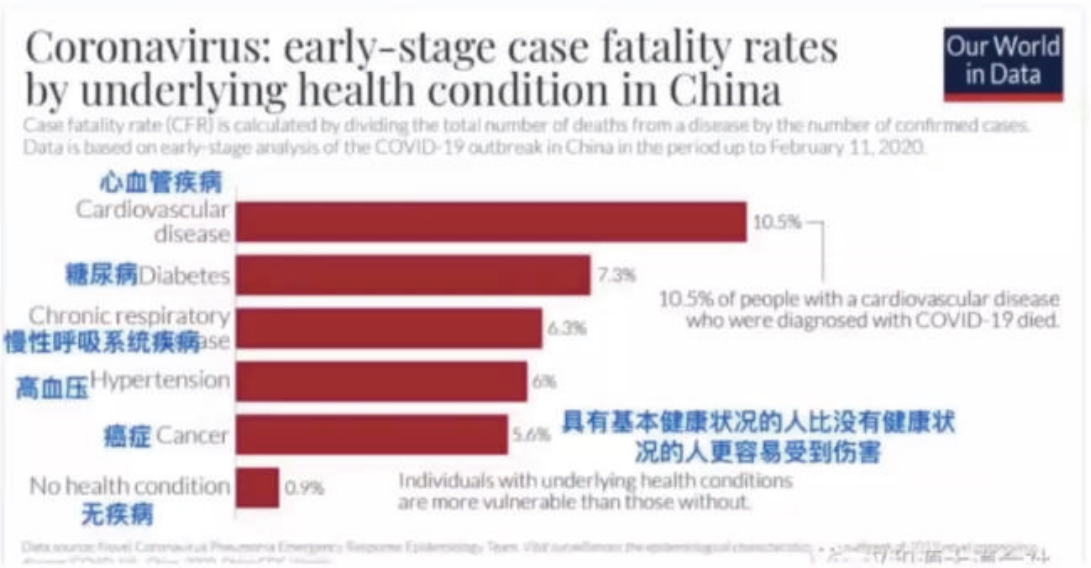


图 6：新冠中的脆弱人群

整个疫情易感人群主要是脆弱人群。心血管病的病人，世界各个国家的报道非常吻合，死亡率达到了 10%； 糖尿病、慢性病呼吸系统疾病、高血压和癌症晚期患者，也都达到了 5%–10%。相对来说，如果自身没有什么固

有疾病，病死率一般很低。

二、精准防控

我们来看，在北京这种情况下如何做到精准防控；或者在未来其他地方有疫情发生时如何做到精准防控。我们国家在防疫上的一个大的策略，基本上就是：外防输入，内防反复。我们从北京、黑龙江、天津的数据可以看出，基本上黑龙江、天津的病例都是输入的。

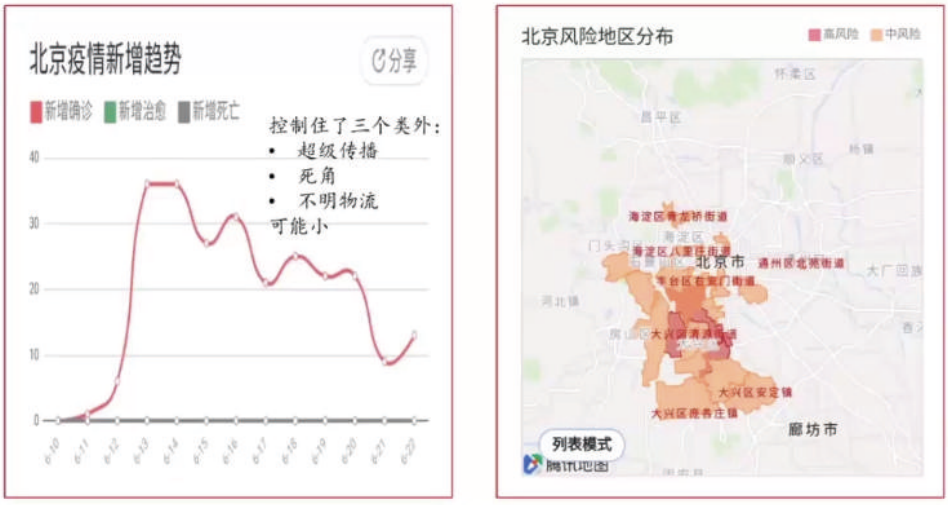


图 7：北京疫情的大致情况

我们从北京病例的基因序列发现，它和欧洲的基因序列更接近。具体是欧洲输入还是从吉林延展过来的，我们还不清楚。天津这边，已经发现了和北京的疫情有关联，因为在发病人群和北京流行的人群之间有一个无症状感染者。我们可以说，北京的疫情目前是处于积极的控制下，于 13–14 日达到高峰，之后就是稳定的下降了，18 日之后，CDC 专家谈到北京的疫情得到了很好的防控，为什么呢？因为 18 日之后，所有病人的发病和感染都确定是和新发地市场密切相关，后来发病的人群应该是间接接触，疫情的传染源是非常明确的。在这种情况下我们把新发地以及相关地区控制住，疫情防控就有保障了。从图中也可以看到，18 日以后我们看到疫情是相对稳定下降的。现在有三个意外情况可能会发生，1）出现超级传播者；2）出现监控死角；3）有不明原因的物流传播病毒。那么这会引起新的疫情，但这种疫情的可能性比较小。所以我个人支持已经看到希望的观点，让民众感觉到我们的疫情有控制的希望，让他们抱有乐观而不是恐惧的心态来面对疫情。

非常感谢文继荣教授和北京的团队，能够把不同的区域分为低风险、中风险和高风险，甚至局限在一些街道上，在不同的区域采取不同的防控措施。大家可以看到基本上在西南城区的丰台、大兴等地区的风险比较高。同时对于北京的疫情能够做到这样精准的防控，是非常不容易的，因为它的人流量非常大，而且短时间内流动快，流动半径大。这个时候追踪技术就发挥了重要、关键的作用。

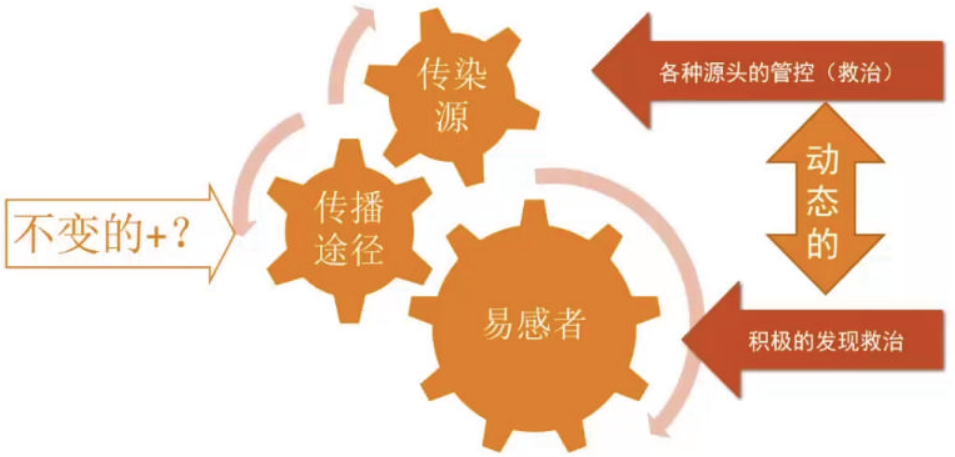


图 8：确定性中寻求突破口：传染病的动态 + 相互减压

什么叫科学？什么叫精准？怎样管控这次疫情？我们还是要回到传染源、传播途径和易感者来讲。对于传染源就是源头的管控； 易感者就是对重点人群，如年老、患病的人群，要进行重点保护。我们可以看到，基本上发病人群以及感染疾病未发病的人群是在一个动态的过程。在传染源的管理方面国家是非常发力的，每个小时都有可能有新的疫情发生，因此时间的动态是非常关键的，如何在传染源、传播途径和易感者之间减压，这是我们的一个思考。

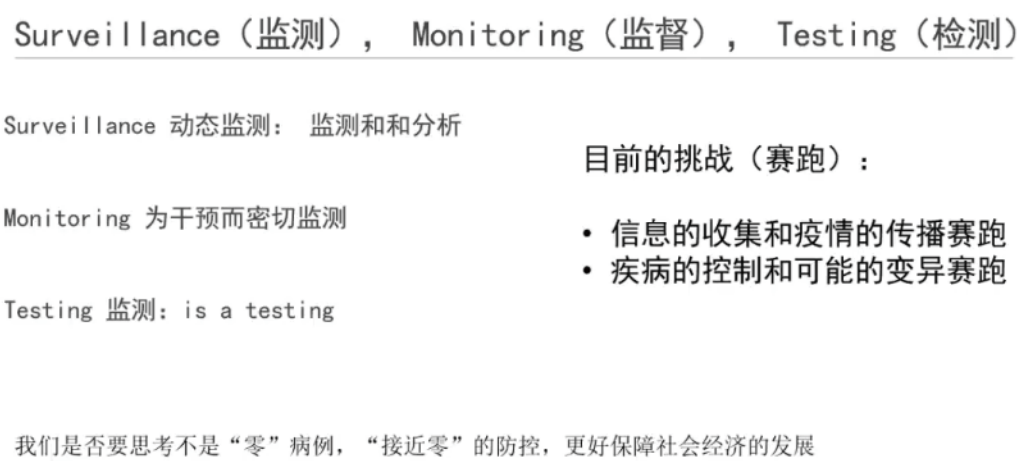


图 9：寻找精准的靶子：基础数据和信息

目前北京正在进行大面积检测，武汉也在进行全城检测，那么就要讲三个基本概念：Surveillance（检测），即要了解疾病现状； 另一个 Monitor（监督）对疾病的现状进行监督，甚至采取一些干预措施改变疫情的动态； 再就是我们常说的 Testing（检测），应该是监测和监督疫情的重要内容。但是我们从公共卫生的角度思考，如何在监测、监督这两个方面来下功夫，找到最关键的高危人群、最可能的传染源，然后有重点地实施公共卫生措施？疫情的变化基本上是每三到六天会感染一拨病人，每天的疫情分析、甚至时时刻刻的分析都非常重要。数据的收集和分析是就是在和疫情的传播赛跑，我们的控制措施也在和疫情的传播赛跑。今天有报道说我们的病毒株

在变化，对细胞的亲和力增加了 10 倍。中国这种情况下，如果能有效地控制疫情的发展，病毒变异的可能性就可以大幅度降低；如果疫情还在全球这样流行，那么变异的可能性就会增加。当然，我觉得一年以内大的变异还不会有，变异会随着传播力明显增加。其致病率是降低还是增加，现在我们还不明确，比较理想的状态就像流感这样，但现在我们还有不可确定的因素。

对于未来疾病的控制，我们一定要考虑对社会经济的影响。毫无疑问，我们控制疫情是保障社会经济的发展，所以现在的目标基本上是奔着“零病例”的方向发展，如果能够加强 Surveillance 和 Monitor，能不能考虑接近零病例的情况下让社会和生活正常运转？同时即使有小的疫情发生，我们也能够快速扑灭。当然，对于新发地这样的疫情属于难防难控，一般可防可控的情况下我们要控，同时也要防控相结合，这样能够减轻社会经济发展的压力。

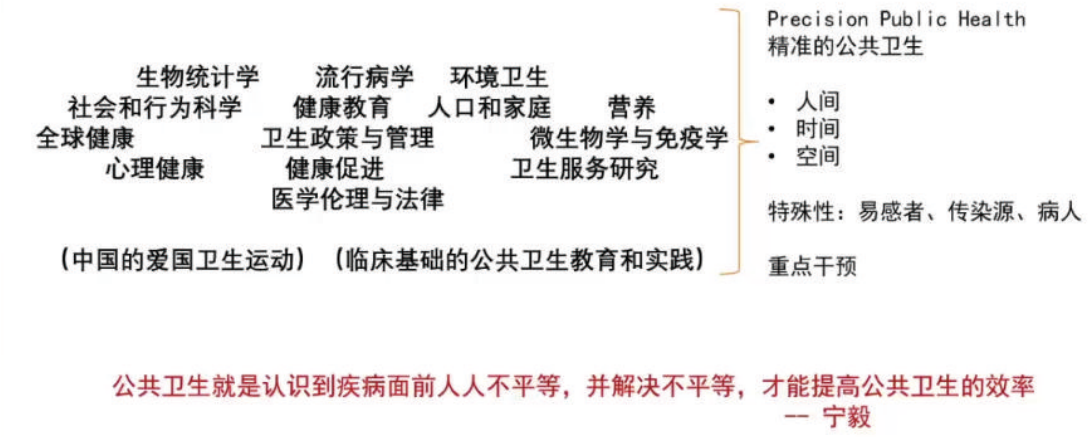


图 10：公共卫生到精准公共卫生

刚才提到我们通过监测以及监督来对高危人群、疫情可能的发展进行预判的时候，在公共卫生领域，对传染源和易感人群、传播途径的管理是不是可以做得更好？公共卫生包括生物统计流行病和环境卫生，可以看到这一次新发地疫情与环境是密切相关的，所以个人和家庭能不能考虑社会和行为学的干预建立起健康的生活习惯？如果有健康的生活习惯，我们就不用担心疫情的传播与危害。因此，如何让普通民众通过健康教育接受、强化这种健康行为？这就涉及到人口和家庭，后面再讲从营养上怎么支持这次疫情的控制，接着又涉及到全球疫情的防控、海关的管理、卫生政策的管理，还有对疾病的基本了解，包括一些社会学的因素等。这次三文鱼不能吃了，三文鱼产业在中国有多大，鱼类的产业有多大，肉食类产业有多大，这些都有很大的影响，我们应该怎么解决？同时，涉及到心理健康和健康促进等，如何防控人们的恐惧心理？每个决策者在每一次把控平衡这种精准和扩大范围防控的时候，也在把控会不会发生可能的一些风险。这就非常需要我们在专业上甚至是 Precision Public Health，涉及到什么样的人需要检测？在动态中如何把握？哪些空间要下功夫？涉及到易感者、传染源和病人，要运用怎样的综合公共卫生手段？在我看来，**公共卫生就是认识到疾病面前并非人人平等，我们解决公共卫生问题就是解决不平等的问题，提高公共卫生的效率。**对于高危人群、高危时间、高危空间、脆弱人群如何解决，要把这些问题解决得好，防控效率就会相应提高。

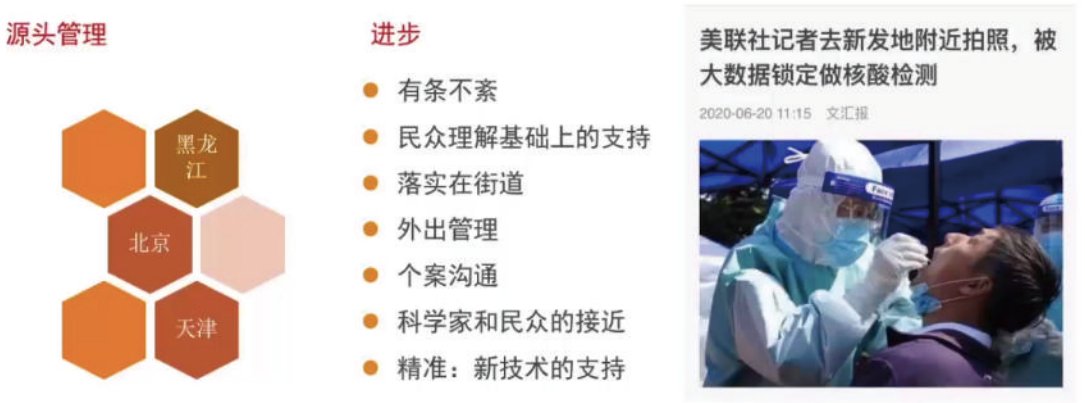


图 11：外防输入，内防反复：病毒流动和有序人口流动

从源头的管理来看，黑龙江、北京和天津都处于较难防控的状况，我们应该在控上下功夫，对于难防的部分以及重点的区域，比如农贸市场，现在对已经确定的重点区域要进行严格地管理，同时加强控制。在北京，我们感觉到有些防控还有进步的空间，表现在整个防控的过程当中太紧张，因为新发地是非常不一般的地方。不过整体来说是有条不紊的，民众能够理解和支持，并且能做到自愿去进行核酸检测，社区对于外出的管理也非常完善。另外在精准预防上，也运用了很多新技术，例如美联社的记者去新发地拍了张照片，结果被大数据锁定，要求他必须做核酸检测。

三、新冠和非传染性疾病

高发病率和高病死率是
- 老年人
- 基础疾病人群
- 社会脆弱人群

四个阶段

- 双重负担： A double burden of diseases
- 向慢性病倾斜： Shifting from infectious diseases to non-communicable diseases?
- 关键问题：卫生资源匮乏 In and Out of the basket of public health
- **殊途同归：解决慢性病舒缓传染病压力Common risk factors**

图 12：同时思考传染病和非传染病

这次疫情可以分为三个阶段： 疫情发生的阶段； 疫情发生之后现在大部分省份都处在缓冲期的黄金阶段； 接着在秋冬季来临时可能是疫情高发的阶段。

现在我们在想如何共同解决传染病和非传染病的问题。可以从这次疫情看到，高感染率人群以及高病死率人群基本上都是老年人、有接触疾病的人群和相对脆弱人群（经济收入各方面比较低）。在这种情况下，我们认为传

染病和慢性病共同构成了公共卫生的重要部分，尤其是中国这样的发展中国家，对于健康资源长期投入的不足，那么有限的资源究竟是优先覆盖慢性病还是优先覆盖传染病，这是公共卫生的焦点问题。回到今天，我们认为整个新冠疾病的高危人群就是慢性病的人群，这两个疾病都不能轻视。

图 13：疫情期、间歇黄金期、防控高压期（秋冬季节，或者提早）

在未来的疫情期、间歇黄金期以及防控高压期阶段，我们可以做哪些事情？首先，疫情防控在秋冬季会有大的压力，也就是防控的高压期。北京目前是处在疫情期，可以看到我们要建立和修正原来的一些健康习惯，比如戴口罩、勤洗手、少去拥挤的地方，保持 1 米以上的社交距离。针对防控的高压期，需要强化健康行为习惯，包括分餐、疾病预防康复，让一些疾病康复，从而达到理想的身体状况。

在夏季，我国一些地区发生了疫情反复，预计秋冬季的疫情防控压力会更大，每一波疫情的影响都值得我们关注，我们要改变一些行为，从而降低患病风险。我们也要体会饮食、心理状况、运动和社会交往对健康的影响。因为我本人是学营养的，因此我希望能够给大家推荐一些良好的饮食习惯，即三多两少。如下图所示。

图 14：生活方式建议

四、总结

对于本次演讲，总结如下:

1. 不能过度依赖国家的组织动员，要科学精准实施防控;
2. 重在外防，同时在内防中动态地思考防控使用公共卫生技术手段;
3. 发挥个人和家庭主战场作用，生活和防疫两个常态化;
4. 预防优先，思考慢性病和传染病的防控，管控风险。

精鼎医药冯胜：真实世界数据（RWD）和 AI 如何炒好临床研究这盘“菜”？

整理：智源社区 张弛

在 2020 北京智源大会“AI 防疫”专题分论坛中，我们邀请到了冯胜教授进行题为《COVID-19: Real-World-Data (RWD) & Advanced Learning in Clinical Studies》的分享。

冯胜，精鼎医药真实世界数据亚太区总裁。中国科技大学分子生物学学士，美国北卡州立大学生物统计和生物信息学博士。

在分享中，冯胜提出了真实世界数据和临床试验数据的两条相对独立的研究处理路径，而此次 COVID-19 疫情将两条数据处理路径错综复杂地联系在了一起。针对 COVID-19 疫情背景，并结合自身多年企业工作经验，冯胜对 AI 处理 RWD、RWD 进入政府和 RWD 进入药物公司三个方向展开阐述，分析了 RWD/AI 在 COVID-19 疫情中进入临床研究所面临的普遍、特殊挑战是什么，最后为 AI engineers 和 IT 行业从业人员等将真实世界数据和 AI 技术带入临床研究提出行之有效的建议。

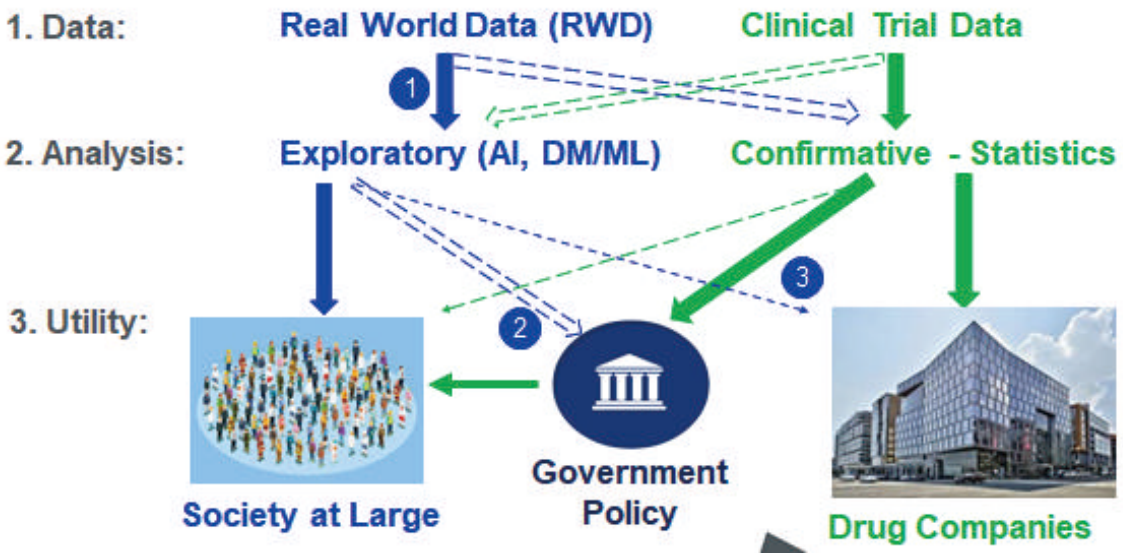


图 1：真实实验数据和临床试验数据的处理

一、RWD/AI 在 COVID-19 疫情中进入临床研究所面临的普遍、特殊挑战是什么？

值得一提的是，企业生产范围内所定义的 AI 除了包括学术范围内的神经网络、深度学习等，还包括数据挖掘、统计分析方法等，是广义的 AI，而在接下来的分享中也将在此基础上进行讨论。

1. RWD/AI 所面临的普遍性挑战——数据质量的划分

当我们从数据的应用场景横向展开，以数据质量标准（Data Quality Standard）、数据分析性质（Analytic Styles）、临床应用价值（Clinical Market Value）三个维度纵向进行分析时，我们会发现真实世界数据面向大众，主要应用于社交媒体、新闻等场景，且多为探索性数据研究，对于数据质量标准的划分并不明确，因而在临床研究中的价值甚微。然而在临床试验、公共政策制定等场景中所需要的数据多为确定性分析数据，要求对每一个数据都需要很强的质量控制，所以这些数据在临床研究中价值也是最大的。

Data Utility Scenarios	Newspapers, TV-Spotlights, Online blogs, Twitters/Facebook/WeChat	COVID-19 Scientific Papers FDA/CTAP Review, Clinical Trial Design Simulation	Public Policy Making, Clinical Trial Designs, Insurance Decision
Data Quality Standard	Mostly Unknown/untested; **no standard**	Varying: from low to high, **In general, in the mid-ground**	**Strong Quality Control** not good news for RWD/Big Data
Analytic Styles	Most Unknown. **For knowns:** **Exploratory 80%**: AI/DM/ML **Confirmative 20%:** Statistics	**Exploratory: 50%** **Confirmative: 50%**	**Exploratory: 5%** **Confirmative: 95%**
Clinical Market Value	$	$$$	$$$$$$$$$$$$$$$$$$$$ $$$$$$$$$$$$$$$$$$$$

图 2：数据在不同应用场景下的分析

2. RWD/AI 在 COVID-19 疫情背景下所面临的特殊性挑战

- COVID-19 疫情来势汹汹，在全球忙于应对疫情的情况下，收集到的数据质量参差不齐、无法控制，不同于癌症、糖尿病等数据集，疫情数据快速产生、变化迅速，这就给数据的采集和分析造成了很大的困难。
- 疫情初期，最好的数据分析师和最好的数据源之间存在鸿沟，存在于企业中的优秀的数据分析师无法获取到置于政府内的公共数据集，导致数据分析的滞后。
- 疫情突如其来，无法制定临床数据的标准，因而也就无法评判数据分析质量。
- 全世界优秀的数据分析师和强大的资源处于分散状态，无法集结起来进行数据分析。
- 疫情期间的一些虚假数据、探索性模糊数据和确定性数据交融错杂，而这些数据的不公开、不透明性导致无法辨别数据的真伪，这也就为数据处理增加了一定的困难。

分析完 RWD/AI 在 COVID-19 疫情中进入临床研究所面临的普遍和特殊挑战，冯胜介绍了一个数据集在临床研究中的应用例子，利用贝叶斯方法分析包括 local policy/law 在内的多个公共数据集，使得数据分析能够突破实时监测的限制，可以达到预测一个月后的效果。

二、政府在 RWD 进入临床研究中扮演的角色

2020 年 5 月 19——29 日，十天之内，FDA 对羟氯喹两次授权又取消，这次事件的背后，针对“羟氯喹对于疫情的治疗是否有用”这一观点出现了很多支持和反对的临床证据，而这些证据大多都表现出小样本、不严谨、发布于社交平台等特点，不符合严格的临床试验的特点，那么针对这个事件，冯胜提出问题：疫情之下，一定要大样本、随机、双盲、安慰剂对照的严格的临床试验吗？监管机构能够接受的最低力度证据（Minimal Strength Evidence）是什么？能否有指南 / 指导原则？真实世界数据到底行不行？

为了回答上面的问题，冯胜通过一个 RWD 应用于临床的例子——埃博拉和棕榈树平台试验进行说明。棕榈树实验是一个十分不严格的临床试验，它没有双盲，没有安慰剂对照，孕妇、小孩都可以入组，可以中途叫停，并将患者换入治疗效果好的组内，尽管如此，棕榈树实验还是大获成功。从以往多次惨烈的教训中，科学家、医生和世界的领导者们逐渐意识到，疫情爆发的时候，不是进行严格的药物临床试验的理想时机，如何快速的找到一种有效的药物治病救人才是首要任务。而在这次 RWD 成功应用于临床试验的例子中，人们意识到：RWD 到底可不可以应用于临床试验取决于多个因素，但是其中关键的一点是——“领袖”是否介入，通过国家或政府将有效的资源进行整合，这是 RWD 能够成功的关键。

三、RWD 应用于临床研究，AI engineers 应该怎么做

冯胜认为 AI engineers 和 IT 从业者们无法将 RWD 应用于临床的一个原因在于沟通不畅，AI 工程师在于临床医生交流时应该注重于物资分配、人员部署的讨论，而不是执着于介绍算法功能的强大，同时应该更多的需要了解适应性实验设计的要求，构筑起大数据和临床之间的桥梁，巧妙把握好实验性（Explanatory）和适应性（Pragmatic）是 RWD 助力临床试验的重要一环。

四、总结

RWD 要成功应用于临床试验，需要国家或政府的介入进行资源整合；AI engineers 要使 RWD 被临床医生所接受，便要将知识体系和思维架构逐渐向实用型临床知识过渡，掌握适应性实验设计的要求，使得科学型 AI 和实用型临床知识达到平衡，相信 RWD/AI 的助力一定会使未来临床试验的研究再创辉煌！

北大副教授边凯归：新冠疫情下接触者精准追踪技术的思考：如何最大化用户隐私的保护？

整理：智源社区 季葛鹏

在第二届北京智源大会“AI 防疫”专题论坛中，来自北京大学信息科学技术学院网络与信息系统研究所副所长、副教授边凯归，对团队近期关于“流行病接触者精准追踪技术”的研究工作做了一个详细的报告分享。整个报告分成四个主要部分，包括：流行病接触者追踪技术的基础概念和背景简要介绍，管控措施粒度与接触者追踪精度层次，产品落地过程中的三个约束条件，随后介绍了智源研究院开发的保护隐私的流行病接触者精准追踪系统——智源蓝保（Blue Bubble）。

一、流行病接触者追踪的技术背景

图 1：接触者追踪的定义

什么是**接触者追踪（Contact Tracking，CTC）**？其包含四个内容：第一个功能是追溯与感染者密切接触的人员；第二是所提供的结果是否支持对某些人员进行隔离；第三点是扩大对更多流调人员的支持力度；最后一点是需要使用更为高效的数字化的工具。**CTC 最终的目的是将密切接触者的近距离感染者找出来，保持一定的检测精度，尽可能地减少非必要隔离人员带来的损失。**

图 2：智源研究院启动流行病接触者追踪技术研发

智源研究院积极响应国家号召与社会即使需求，在二月底 3 月初便启动了接触者追踪技术的研发，用于解决复工、复产、复学过程中**精准追踪**感染人员的位置，**快速排查**与感染者有近距离接触人员，最终目的是**大幅度降低隔离人员比例。**

边凯归补充道，我们的技术方案经过几轮的迭代确定，最后决定采用蓝牙近距离感知技术方案，其有两种模式：一种是楼宇发现的模式，一种是个人发现的模式（后文会详细地介绍）。4 月 15 日这个系统已经部署在知春路智源研究院写字楼上，楼宇上面的边缘存储会有感染者以及近距离接触的蓝牙记录，通过比对数据就可以写字楼内部找出潜在的近距离接触者。一旦有人感染会把自己手机的蓝牙信息上报给疾控部门，部门会把包含曾经去过的地点的信息发回与上报者或相关部门，最终目的是降低隔离人员的比例。

图 3：新加坡 TraceTogether 系统

3 月 20 日新加坡上线了 TraceTogether 系统，每个人手机上安装了 App，两个人距离较近的时候手机会自动广播蓝牙信息，比如自动随机生成的个人 ID，这样的好处就是可以保护个人隐私，即便他人通过搜索蓝牙 ID 也无法获取个人信息。因为该系统上线较早，所以在一定程度上是有用的。边凯归接着指出其缺陷所在：“由于注册时需要个人手机号和身份信息，所以该技术在比较关注隐私的研究者的角度来看可能会有不一样的看法，后面会有专门的章节进行相关讨论。”

4 月 10 日 Apple 公司和 Google 公司宣布合作，将从底层打通个人设备和蓝牙的接口。由于两家不同的公司为保护用户隐私采用不同通讯接口的定义，终于 Google 选择迁就 Apple，计划统一接口为用于研发基于“个人设备蓝牙接口”的接触者追踪技术。但是在没有实现成功之时，就指出个人隐私信息存在被 iOS 和 Android 系统以及第三方应用截取滥用的风险，这也是当时无数学者批评该做法的原因。

4 月 19 日，来自全世界多所大学的 300 名国际学者针对基于蓝牙的近距离接触追踪技术发表联合申明，明确并提出四点要求： 第一，必须使用独立的系统开发具有独立功能的公共卫生检测手段，避免数据被第三方 App 滥用； 第二，解决方案必须公开透明； 第三，必须默认地最大化保护用户隐私； 第四，技术的使用必须是用户自愿的。这些研究者一致认为，必须使用**一个统一而又去中心化的计算框架**，这是给出的一些框架设计的原则。

图 4：Exposure Notification 框架的发布

5 月 20 日，Apple 与 Google 终于联合发布了名为 Exposure Notification 的框架，支持最新的 iOS 13.5 或 Android 系统，但不支持大陆用户。

6 月 15 日，德国也出了一套名为 Corona Warn 新冠警告系统，就是使用了 Apple 和 Google 公司在 5 月 25 日发布的框架，流程大致为：生成一个随机 ID，并且同时扫描和记录周围设备的 ID 也是把这个 Key 上传到中心服务器，服务器会将感染者的 ID 发给所有安装 App 的设备以示警告。

边凯归针对当前国内国际疫情局势发展进行总结：每一个国家都需要一套符合国家法律法规的、高度保护用于隐私的感染 AppAPP，而且由于数据安全因素，每个国家都需要使用自己的技术力量去完成这样一套独立于国外的东西。所以，基于当前市面占有率最高的两款操作系统（iOS 和 Android），我们亟待研发一套真正属于自己的通讯协议，做出属于自己的精准追踪产品。

二、管控措施粒度与接触者追踪精度

管控粒度	管控方法	借助技术手段	问题
城市级别	封城	无任何防备的情况下，难以提前进行技术部署	不得已而为之，经济损失巨大
街道 社区级别	街道、社区只进不出	大数据分析，手机连接基站数据分析，app数据	粒度较粗，各方数据难以协调融合，经济损失较大
楼宇 楼层级别	封楼 分楼层人流控制	???	需要更合理的技术，以及更精细化的管控措施
家庭 个人级别	追溯个人轨迹	新加坡TraceTogether、Apple暴露日志、德国Corona Warn	商业公司做公共卫生监测比较尴尬

图 5：管控措施粒度分级

针对疫情爆发后的管控措施粒度，边凯归将整体分成了四个级别：城市级别、街道社区级别、楼宇级别、家庭个人级别。前两个级别所带来的经济损失都非常大，但由于在疫情爆发的初期，这种方式是最为简单有效的。**楼宇级别的管控，则需要更合理的技术、更精细化的管控措施，边凯归和北京智源联合团队便是基于这个层级来完成追踪的功能（详见后续介绍）。**最后就是家庭和个人级别的追溯个人的轨迹，新加坡、Apple 与 Google 都完成了个人 APP 产品的开发，但是其必须由政府发布。新加坡可以说做的十分成功，因为新加坡是由政府发布，但如果是由商业公司完成必然会引发一些社会问题，因为以商业公司的角色来完成公共卫生监测显得比较尴尬。那么有些同学会问支付宝和微信是否能够完成类似的任务？答案也是可以的。但是这类软件属于社交软件，不能直接抓取数据拿来防疫使用，用户条款中仅仅表述了是一个社交用途，并没有说明能拿来用作防疫使用，所以这类软件在接触者追踪的过程中显得同样尴尬。

如上所述，接触者追踪系统需要满足街道社区级别、楼宇级别、个人级别，不管哪个级别的管控粒度，需要解决三个问题：第一是追溯，第二是发现，第三是决策。最难做的也就是“追溯”，这一步的核心就是采集位置信息（绝对位置与相对位置），通过位置信息即可判断感染者和接触者之间的距离，从而得出最后的决策是否需要为密切接触者采取相应的措施。

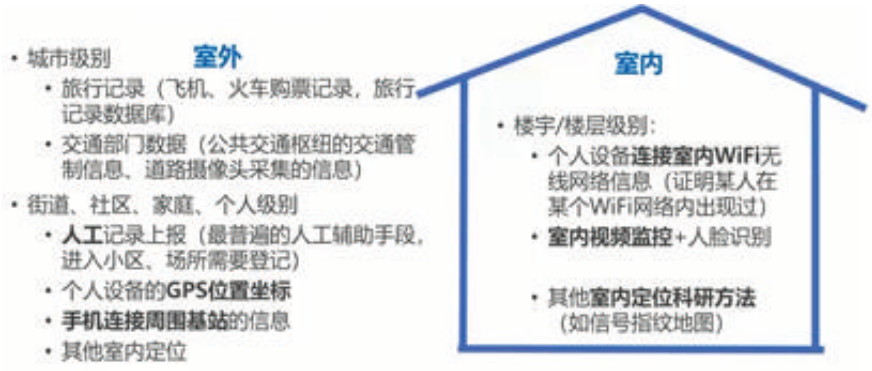


图 6：追踪绝对位置信息的常用手段（室内与室外）

边凯归列举了追踪绝对位置信息的常用手段，如图 6 所示。对于室外级别的，在之前的论述中已经略有谈及，包括：旅行记录、交通数据、个人设备的 GPS 坐标等。而对于室内级别的定位，现用最多的是基于科研的方法，大规模的工业界的室内定位产品暂时还没有。以往会做一些基于 WIFI、监控视频的绝对位置的采集，这些有利于疫情爆发初期的信息采集，快速锁定感染者和近距离接触者。**而对于常态化防控方式，通过汲取国内外的方法，边凯归团队建议采集相对位置信息，可以理解为一种间接证明感染者和接触者距离的信息。**最终，团队决定选择蓝牙 4.0 技术来实现，其优点就是可近距离判断与功耗低。**值得注意的是，由于所采集到的是相对位置信息，避免了绝对位置信息暴露用户隐私的痛处，而相对位置只是判断你是否近距离接触，可以最大化的保护用户的隐私。**

图 7：集合所有技术的接触者追踪系统

那么假设我们可以设计一个“All in One”的系统，即将所有的国内外的方法都集成为一体，我们就可以实现出一个非常完美的接触者追踪系统。这种系统的优点肯定是大而全且实用，但是里面有很多的技术因为各种担心却不太推荐去使用，例如：中国还有很大一部分的人没有智能手机，即根本没有从传感器获取来的数据是无法完成上述大系统中的某一些分支功能的。

三、三个约束：隐私、计算、成本

超越之前讨论的研究层面，在实际产品的落地应用中，还会面临着三个约束条件：

- 隐私：保护责任不够清晰、数据使用和存放不安全、绝对位置信息的滥用。
- 计算：多源数据的融合困难程度高、人工智能背景下视频监控跟踪计算成本巨大且延迟问题严重。所以推荐主要使用独立的系统采集的无线信号作为防疫数据，使用视频监控作为辅助数据加以支撑。
- 成本：普及安装 App 成本高、基于 WIFI 的室内定位算法开发成本高、视频监控系统造价高。

四、保护隐私的流行病接触者精准追踪系统

图 8：智源蓝保（Blue Bubble）

随着社会的需求和技术的发展，Blue Bubble 这一款最大化保护隐私的流行病接触者追踪系统应运而生，这是一款独立的、非商业的系统。这种基于蓝牙开发的系统支持人与人、楼宇之间互相发现，另外包含视频测温系统。该系统有如下特点： 用户数据分布式去中心化存储，从而可以有效地保护隐私； 独立采集相对位置信息，不牵涉多源数据的融合； 双工作模式，可不安装 App； 低功耗、低成本、快速部署； 可恢复待追踪者的行为轨迹。边凯归对两种工作模式进行了展开说明:

图 9：楼宇蓝牙发现模式

- 楼宇蓝牙发现模式： 楼宇蓝牙发现个人蓝牙，并存储于楼宇的边缘设备中，数据不上传中心，可基于蓝牙发现数据进行感染者轨迹生成。

图 10：个人蓝牙发现模式

- 个人蓝牙发现模式： 独立设计的一套不依赖于底层操作系统 API 的协议，包括 iOS 和 Android 系统的互相发现。可通过蓝牙互传、数据存储于个人设备。

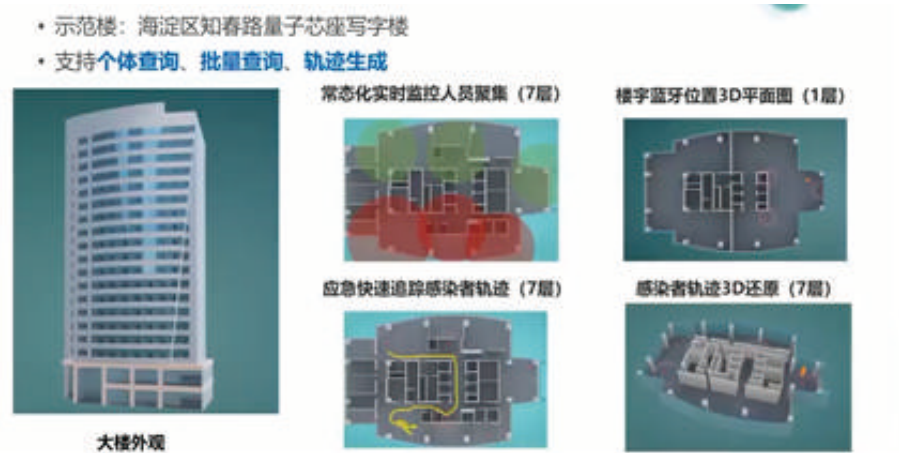


图 11：3D 可视化监控

另外，该系统提供的可视化监控可以整合到已有的视频监控系统中，支持个体查询、批量查询和特殊感染者的轨迹生成，常态化防控的时候生成一张热力图，可以看到室内的聚集度。

管控粒度	管控方法	借助技术手段	问题
城市级别	封城	无任何防备的情况下，难以提前进行技术部署	不得已而为之，经济损失巨大
街道 社区级别	街道、社区只进不出	大数据分析，手机连接基站数据分析，app数据	粒度较粗，各方数据难以协调融合，经济损失较大
楼宇 楼层级别	封楼 分楼层人流控制	智源蓝保楼宇模式	需要更合理的技术，以及更精细化的管控措施
家庭 个人级别	追溯个人轨迹	新加坡TraceTogether、Apple暴露日志、德国Corona Warn 智源蓝保个人app模式	商业公司做公共卫生监测比较尴尬

图 12：智源蓝保楼宇模式

该系统还可以用于补充楼宇级别的管控力度，最大化地保护数据不离开本人的手机，因为蓝牙的近距离关系判断可以达到米级。

五、总结

习近平说过，要把人民的生命健康放在第一位，其次还要同步加快经济恢复的速度，最终观察的结论就是各国都推出了具有本国特色的防疫追踪系统。**正因为这是涉及国家的数据安全，不能用别的国家的，并且还要独立于其他国家的技术框架，拥有独立采集技术系统，这样可以避免很多问题。**最后我们需要做分布式的数据存储，最大限度保护隐私，隐私数据不能离开楼宇或者用户手机，甚至在不安装 App 的情况下可以跨设备、跨操作系统地追踪楼层级别的接触者。

最后，边凯归还留下一个思考题： 如果没有智能手机怎么办？欢迎大家进入我们的讨论区展开讨论：hub.baai.ac.cn。