

专题研讨

专题 1：机器学习与类脑智能

王立威：深度学习的表示与泛化理论



王立威，1999 年获清华大学学士学位，2002 年获清华大学硕士学位，2005 年获北京大学博士学位。现为北京大学信息科学技术学院教授。长期从事机器学习相关研究，目前主要致力于机器学习基础理论，即泛化理论的研究，差分隐私算法的设计与分析以及医疗影像诊断算法与系统的开发。自 2002 年以来，在 PAMI、CVPR、ICML 等国际顶级期刊和会议上发表论文 60 余篇，并参与编写《机器学习及其应用》2009 版“关于 Boosting 算法的 Margin 解释”及 2015 版“差分隐私保护的机器学习”相关章节。曾获得第 11 届 Meeting on Image Recognition and Understanding 会议最佳论文奖，2010 年获得《Pattern Recognition Letters》期刊最高引用论文奖（2005-2010），2010 年入选 AI' s 10 to Watch，2012 年获得国家自然科学基金优秀青年基金并入选“新世纪优秀人才支持计划”。

龙子超、董彬：PDE-Net: Learning PDEs from Data

龙子超，北京大学数学科学学院 15 级博士，主要研究兴趣包括深度学习、数值偏微分方程。

马贤忠，北京大学数学科学学院 14 级博士，研究方向有深度学习、数值偏微分方程、分数阶微分方程数值解。



董彬，北京大学北京国际数学研究中心研究员，北京大数据研究院深度学习实验室研究员、生物医学影像分析实验室副主任。2009 年在美国加州大学洛杉矶分校（UCLA）数学系获得博士学位。博士毕业后曾在美国加州大学圣迭戈分校（UCSD）数学系任访问助理教授、2011—2014 年在美国亚利桑那大学（University of Arizona）数学系任（Tenure-Track）助理教授，2014 年底入职北京大学。主要研究领域为应用调和分析、优化方法、机器学习、深度学习及其在图像和数据科学中的应用。应用包括图像重建及修复、生物与医学成像、生物医学影像分析、疾病量化、治疗方案优化等问题，在包括《Journal of the American Mathematical Society》、《Applied and Computational Harmonic Analysis》、《SIAM 系列期刊》、《Inverse Problems》、《Mathematics of Computation》、《Journal of the Royal Statistical Society Series B》在内的国际重要学术期刊和会议上发表论文 40 余篇，拥有 2 项美国专利。于 2014 年获得求是基金会的求是杰出青年学者奖，2015 年入选中组部第十一批“千人计划”青年人才。

摘要： Partial differential equations (PDEs) play a prominent role in many disciplines such as applied mathematics, physics, chemistry, material science, computer science, etc. PDEs are commonly derived based on physical laws or empirical observations. However, the governing equations for many complex systems in modern applications are still not fully known. With the rapid development of sensors, computational power, and data storage in the past decade, huge quantities of data can be easily collected

and efficiently stored. Such vast quantity of data offers new opportunities for data-driven discovery of hidden physical laws. Inspired by the latest development of neural network designs in deep learning, we propose a new feed-forward deep network, called PDE-Net, to fulfill two objectives at the same time: to accurately predict dynamics of complex systems and to uncover the underlying hidden PDE models. The basic idea of the proposed PDE-Net is to learn differential operators by learning convolution kernels (filters), and apply neural networks or other machine learning methods to approximate the unknown nonlinear responses. Comparing with existing approaches, which either assume the form of the nonlinear response is known or fix certain finite difference approximations of differential operators, our approach has the most flexibility by learning both differential operators and the nonlinear responses. A special feature of the proposed PDE-Net is that all filters are properly constrained, which enables us to easily identify the governing PDE models while still maintaining the expressive and predictive power of the network. These constraints are carefully designed by fully exploiting the relation between the orders of differential operators and the orders of sum rules of filters (an important concept originated from wavelet theory). We also discuss relations of the PDE-Net with some existing networks in computer vision such as Network-In-Network (NIN) and Residual Neural Network (ResNet). Numerical experiments show that the PDE-Net has the potential to uncover the hidden PDE of the observed dynamics, and predict the dynamical behavior for a relatively long time, even in a noisy environment

陆一平、董彬：Beyond Finite Layer Neural Networks

陆一平，北京大学数学科学学院 15 级本科生，研究方向有机器学习、低级计算视觉。

钟傲啸，哈佛大学博士生。

李全政，北京大学医疗健康大数据中心主任、生物医学影像分析实验室主任、哈佛大学医学院副教授、麻省总医院 Gordon 医学影像中心人工智能研究室主任、麻省总医院临床大数据研究中心研究员。美国国立卫生研究院(NIH) NIBIB 项目评审委员会委员，新加坡 A*STAR Program 基金评审委员会委员。核医学与分子成像协会 Society of Nuclear Medicine and Molecular Imaging、IEEE Computer Society、IEEE Nuclear & Plasma Sciences Society、IEEE Signal Processing Society 会士，IEEE Transaction on Imaging Processing 副主编。IEEE Nucl. and Plasma Sci. Society 早期成就奖。发表逾 110 篇 SCI 期刊和会议论文，拥有 8 项美国专利。李全政教授领导的北京大数据研究院医学影像分析实验室团队，在医学图像重建、分割、配准以及融合方法上形成了系统的研究方法及成果，同时对人工智能、深度学习算法在医疗健康方向上有着国际领先的理论研究和实际应用。



董彬，北京大学，北京国际数学研究中心研究员，北京大数据研究院深度学习实验室研究员、生物医学影像分析实验室副主任。2009 年在美国加州大学洛杉矶分校（UCLA）数学系获得博士学位。博士毕业后曾在美国加州大学圣迭戈分校（UCSD）数学系任访问助理教授、2011—2014 年在美国亚利桑那大学（University of Arizona）数学系任（Tenure-Track）助理教授，2014 年底入职北京大学。主要研究领域为应用调和分析、优化方法、机器学习、深度学习及其在图像和数据科学中的应用。应用包括图像重建及修复、生物与医学成像、生物医学影像分析、疾病量化、治疗方案优化等问题，在包括《Journal of the American Mathematical Society》、《Applied and

Computational Harmonic Analysis》、《SIAM 系列期刊》、《Inverse Problems》、《Mathematics of Computation》、《Journal of the Royal Statistical Society Series B》在内的国际重要学术期刊和会议上发表论文 40 余篇，拥有 2 项美国专利。于 2014 年获得求是基金会的求是杰出青年学者奖，2015 年入选中组部第十一批“千人计划”青年人才。

摘要： Deep neural networks have become the state-of-the-art models in numerous machine learning tasks. However, general guidance to network architecture design is still missing. In our work, we bridge deep neural network design with numerical differential equations. We show that many effective networks, such as ResNet, PolyNet, FractalNet and RevNet, can be interpreted as different numerical discretizations of differential equations. This finding brings us a brand new perspective on the design of effective deep architectures. We can take advantage of the rich knowledge in numerical analysis to guide us in designing new and potentially more effective deep networks. As an example, we propose a linear multi-step architecture (LM-architecture) which is inspired by the linear multi-step method solving ordinary differential equations. The LM-architecture is an effective structure that can be used on any ResNet-like networks. In particular, we demonstrate that LM-ResNet and LM-ResNeXt (i.e. the networks obtained by applying the LM-architecture on ResNet and ResNeXt respectively) can achieve noticeably higher accuracy than ResNet and ResNeXt on both CIFAR and ImageNet with comparable numbers of trainable parameters. In particular, on both CIFAR and ImageNet, LM-ResNet/LM-ResNeXt can significantly compress ($>50\%$) the original networks while maintaining a similar performance. This can be explained mathematically using the concept of modified equation from numerical analysis. Last but not least, we also establish a connection between stochastic control and noise injection in the training process which helps to improve generalization of the networks. Furthermore, by relating stochastic training strategy with stochastic dynamic system, we can easily apply stochastic training to the networks with the LM-architecture. As an example, we introduced stochastic depth to LM-ResNet and achieve significant improvement over the original LM-ResNet on CIFAR10.

邹磊：面向知识图谱的自然语言问答研究



邹磊，北京大学计算机科学技术研究所教授，国家自然科学基金委优秀青年基金项目获得者，北京大学大数据科学研究中心主任助理。目前的主要研究领域包括图数据库，RDF 知识图谱，尤其是基于图的 RDF 数据管理。邹磊及其团队构建了面向海量 RDF 知识图谱数据（超过 100 亿三元组规模）的开源图数据库系统。邹磊已经发表了 30 余篇国内外学术论文，包括数据库领域国际顶级期刊/会议论文（SIGMOD, VLDB 等）近 20 余篇；其论文被引用超过 1200 多次（根据 Google Scholar 的统计），单篇最高被引用 298 余次。邹磊获得 2009 年中国计算机学会优秀博士学位论文提名奖和 2014 年中国计算机学会自然科学二等奖（排名第一）。

摘要：自然语言问答(QA)是指利用各种技术和数据对用户提出的自然语言问题直接给出问题答案。QA 任务根据所依赖的数据形态可以分成三类，分别是基于知识库的问答(KB-QA)、基于文档的问答(DB-QA)和社区问答(C-QA)。本次报告主要关注面向知识图谱的问答系统。知识图谱是目前知识库的一种常见的表达形式，是以图形(Graph)的方式来展现“实体”、实体“属性”，以及实体之间的“关系”。近年来随着大数据，人工智能等概念与技术的兴起，知识图谱和 KB-QA 相关的研究工作和工业应用逐渐引起重视。本次报告主要介绍目前学术界和工业界面向知识图谱问答的主要关键技术和我们组在面向知识图谱的自然语言问答系统方面的工作 gAnswer。

朱占星：在深度学习中如何增强对抗样本的迁移能力

Enhancing the transferability of adversarial examples in deep neural networks

朱占星，北京大学大数据科学研究中心，助理研究员。2016年在英国爱丁堡大学获得人工智能博士学位。2016年5月加入北京大学大数据科学研究中心下的深度学习实验室和北京大数据研究院。主要研究领域为机器学习、深度学习、强化学习以及大规模优化和贝叶斯方法，同时将机器学习技术应用在交通大数据中的各种预测问题、医学影像、网络安全及计算机图形学当中。在包括人工智能领域国际顶级期刊及会议 NIPS、ICML、ACL、AAAI、ECML、ISBI 发表论文近 20 篇。

摘要： Deep neural networks provide state-of-the-art performance for many applications of interest. Unfortunately, they are known to be vulnerable to adversarial examples, formed by applying small but malicious perturbations to the original inputs. Moreover, the perturbations can ****transfer across models****: adversarial examples generated for a specific model will often mislead the other unseen models. Consequently, the adversary can leverage it to attack against the deployed black-box systems.

In this talk, I will present a plausible understanding on the phenomenon of adversarial transfer. Based on this understanding, we propose a simple and effective strategy to craft adversarial examples using noise reduced gradient. This new approach can enhance the transferability dramatically, and its effectiveness is justified on various classification models over ImageNet.

孙 栩：面向自然语言的机器学习技术



孙栩，34岁，北京大学信息学院研究员，博士生导师。日本东京大学博士。先后在日本东京大学、美国康奈尔大学、香港理工大学担任研究职位。曾在微软公司美国雷蒙德研究院实习。研究方向为自然语言处理、机器学习、人工智能，目前关注自然语言的结构表示与学习、自然语言的自动生成。先后在国际高水平会议和期刊 ACL, ICML, NIPS, AAI, IJCAI, EMNLP, TKDE, CL 等发表 30 余篇论文。担任 EMNLP、IJCNLP 等国际学术会议的领域主席；ACL, IJCAI, AAI, COLING, EMNLP, NAACL 等国际学术会议的程序委员会成员；IEEE TPAMI, Comput. Linguist. 等期刊的审稿人。2014 年入选中组部第十批“千人计划”青年人才。2015 年获得求是杰出青年学者奖（香港求是科技基金会）。2016 年获得大川研究助成奖（日本大川情报通讯基金会）。

摘要：将简要介绍我们在“面向自然语言的机器学习技术”中的具体研究，包括以下几个方面：

1，自然语言的结构表示与学习：研究自然语言的内部结构以及如何去建模学习，包括自动分词、句法分析、篇章分析等（如 NIPS 2014, ACL 2016）；

2，自然语言的自动生成：研究自然语言是怎么产生的，包括 paraphrasing, 自动文本摘要，神经机器翻译等（如 ACL 2017, AAI 2018）；

3，面向自然语言的深度学习模型的创新：深度学习方法、模型方面的创新研究（如 ICML 2017, AAI 2017）；

王 阳：受生物学启示的非典型数字电路神经形态芯片系统研究

王阳，1992 博士（清华微电子），1986 硕士（哈工大半导体），1982 学士（哈工大物理）。1992-1993 北京大学微电子所博士后，1993-今北大微电子所教师。长期研究借助生物学启示，从整体出发、充分利用器件特性设计高效率芯片系统问题。

摘要：芯片不仅仅是实现算法的一种物理方法，也是以实验方法研究大规模系统的一种手段。在大规模复杂非线性系统理论仍处于发展的今天，传统的实验方法可以推动对于芯片级系统的认识，并可能以经验和直觉的方法指导芯片级系统设计。晶体管密度迅速提高的同时，芯片的其它资源难以同步增加，芯片资源已逐渐成为芯片发展的重要限制因素，作为解决当今智能问题物质基础—相关芯片表现的更为严重。为解决芯片性能提高与芯片系统资源限制之间的矛盾，人们不断探求各种有效方法，包括从制造技术方面和芯片系统设计两个方面。尽管人们采用许多措施，但是与生物系统（人脑）比较，人造系统（CPU，GPU，FPGA 等）的计算效率（单位能量消耗完成的计算数）还是比较低，因此在利用有限资源提高芯片信息处理能力方面，人们还有许多东西可以向生物系统学习。虽然对这个问题早有认识，但由于人们至今没有弄清生物系统处理信息的机制，所以这方面工作进展速度较慢，思维方式上进展有限，最终的进展落后于期望。尽管无法一下达到生物系统的资源利用效率，但可以在生物系统的启发下，解决一些传统计算方式较难解决的问题。特别是从提高现有芯片系统的资源利用率角度，借助生物学启示，以合理的资源消耗解决一些传统计算方式较难解决的问题。

本专题报告借助生物学启示，探讨充分器件特性构建高效率智能芯片系统的相关问题，包括非典型数字电路的语音信号特征提取，便于芯片实现的非线性电阻网络视频特征提取，充分利用器件特性构成的神经网络以及学习等问题。

任全胜：神经形态深度网络 FPGA 实现与光子神经形态系统



报告人简历：2013/08-至今，北京大学，信息科学技术学院，副教授；2010/09-2013/07，北京大学，信息科学技术学院，讲师；2008/08-2010/08，德国马普学会，自然科学数学研究所，博士后；2003/09-2008/07，北京大学，信息科学技术学院，博士；1999/09-2003/07，北京大学，信息科学技术学院，学士。主要学术任职：

Frontiers in Neuromorphic Engineering, Review Editor。

摘要：基于脉冲事件型传感器的仿生视觉信息处理被誉为自动驾驶等领域的搅局者和颠覆性创新。研究组致力于针对事件型仿生视觉数据进行 FPGA 深度学习及加速技术，已经在 FPGA 上实现了脉冲事件化卷积神经网络，并用于对仿视网膜摄像头芯片的输出数据进行智能识别，MNIST 数据集的准确率在 95% 以上。目前正在研究自动驾驶背景下的仿生视觉识别任务，以解决高速动态环境下行人、汽车、障碍物等目标快速检测与识别问题。

另一方面，随着超快光子学、光子集成技术的发展，基于飞秒激光脉冲的光子神经计算系统已显现出挑战现有电子器件与芯片的趋势。以深度学习为例，最新的光子神经计算方案能够比最新的电子芯片快两个数量级以上，功耗则低四个数量级，接近“零功耗”；在类脑计算方面，能比生物大脑快几百万至十亿倍的运行速度模拟神经拟态算法；且由于光子的量子属性，具有实现光子神经计算与量子计算融合潜力。研究组已在光子 STDP 突触学习、基于神经工程框架的光子神经拟态系统、光脉冲序列模式识别等方面取得了一定的研究成果，文章发表于 Optics Express、Applied Optics 等期刊，得到了国际同行的关注与认可。目前正在前期分立器件、算法方案的研究基础上，转向可集成光子神经元激光器制备、芯片级光子神经拟态系统的研制。

事件型仿生传感器数据驱动，及发挥光子的超快超低功耗，是目前类脑计算领域离产业应用距离最近、短时期最有可能超越传统深度学习范式的两个技术路线。报告将分别介绍研究组在前述两方面的已有成果和在研项目。

韦 骏：机器学习在地球科学的应用



韦骏,男,北京大学物理学院大气与海洋科学系,百人计划研究员。2006 年在美国纽约州立大学取得物理海洋学博士学位,2006-2011 年在美国麻省理工学院历任博士后、研究员。2011 年回国入职北京大学,一直从事台风海气相互作用、机器学习在地球科学应用方面的研究。与中国气象科学研究院合作,为我国台风预报业务化模式建立了一套基于大数据机器学习的台风预报模式参数化方案,提高了台风精细化模拟和预报技巧。

摘要: 机器学习的概念和算法逐渐进入自然科学的各个领域,我的报告将介绍一种基于大数据机器学习算法在台风预报方面的应用。近年来,台风路径的模拟和预报取得了较大进步,而台风强度预报精度的提高却相对较慢,与国家防灾减灾的迫切需求还不相适应。究其原因,对台风海气界面过程的复杂性认识不足,以及台风模式本身缺乏解析海洋反馈机制的模块是重要的原因之一。台风海气界面过程牵涉到大气与海洋之间的动量和能量交换,目前的物理方程并不能完全解析这样一个复杂的多变量耦合和反馈过程。因此,我们基于大数据机器学习的神经网络算法,利用台风大数据诊断海气界面多变量之间的相关关系及优化相关系数,从而通过在台风模式中建立一套基于机器学习的海气变量参数化方案,实现台风与海洋的反馈机制,进而提高台风强度的预报精度。目前,机器学习在地球科学领域的应用正处于起步阶段,我们相信它在这一领域将具有广阔的应用前景。