

计算科学评论

环球科学

WWW.COMPUTER.ORG

2016年第4期

计算新概念

活的计算机博物馆 P6

DNA 电路 P50

SMP 2016 P79

定价：25元

合作机构



IEEE
computer society



ISSN 1673-5153



9 771673 515122

云计算

人工智能

工控机

制造业

电子

嵌入计算

传感器

互联网

3D 打印

绿色计算

图形图像

虚拟现实

职场
市场
行业分析
创业
学习 科技新闻
竞赛

找工作
教育

互联网金融

芯片

大数据

软件架构

纳米架构

人机交互

多媒体

普适计算 MEMS



微信名：计算机人 微信号：jisuanren



Copyright

版权

主管单位 Authorities in Charge

中华人民共和国教育部 Ministry of Education of the People's Republic of China

主办单位 Sponsor

中国大学出版社协会 China University Presses Association

出版单位 Publisher

《环球科学》杂志社有限公司 GLOBAL SCIENCE MAGAZINES Co. Ltd

社址 Address: 北京市朝阳区秀水街1号建外交公寓4-1-21 Office 4-1-21, Jianguomen Diplomatic Residence Compound, No. 1, Xiu Shui Street, Chaoyang District, Beijing, China. 邮编 100600

联系电话: 010-85325810 / 85325871

社长 / 总编辑 Editor-in-chief

陈宗周 ChenZongzhou

副校长 / 副总编辑 Deputy Editor-in-chief

刘芳 LiuFang

执行出版人 Publisher

管心宇 Xinyu Guan

资深编辑 Senior Editor

马法达 Falda Ma

刘妍 Yan Liu

特约编辑 Contributing Editor

史彦诚 Yancheng Shi

刘大明 Daming Liu

高天羽 Tianyu Gao

费楠 Yong Fei

王璇 Xuan Wang

运营中心 OPERATING DEPARTMENT

运营机构 Publisher

上海灵宸文化传媒有限公司

发行部 Circulation Department

发行总监 Circulation Director

谢磊 XieLei 010 - 57439192

市场部 Marketing Department

市场总监 Marketing Director

孔祥彬 KongXiangbin 010 - 85325810 - 807

广告部 Advertising Department

销售总监 sales Director

范欢 FanHuan 010-85325871-802 010-85325981

读者服务部 Reader Service

杜珺 Du Jun 010 - 57458982

印刷: 北京博海升彩色印刷有限公司

如发现本刊缺页、装订错误和损坏等质量问题, 请在当月与本刊读者服务部联系调换 (请将坏书寄回)。

国际标准刊号: ISSN 1673-5163

国内统一刊号: CN11-5480/N

广告经营许可证号: 京朝工商广字第8144号

知识产权声明:

IEEE, IEEE Computer, IEEE中文网站的名称和标识, 属于位于美国纽约的电气电子工程师学会有限责任公司所有的商标, 仅通过授权使用。这些材料的一部分由IEEE Computer英文版翻译而来, 版权归IEEE所有, 并经IEEE授权翻译复制。

IEEE Computer杂志的中文版权, 由美国电气电子工程师学会有限责任公司授予上海灵宸文化传媒有限公司, 并由本刊独家使用。

本刊发表的所有文章内容由作者负责, 并不代表上海灵宸文化传媒有限公司、美国电气电子工程师学会有限责任公司的立场。

本刊内容未经书面许可, 不得以任何形式转载或使用。

编辑团队

执行编辑 Carrie Clark

cclark@computer.org

高级编辑 Chris Nelson

编辑 Lee Garber, Meghan O'Dell

特约编辑 Christine Anthony, Rebecca Torres

多媒体编辑 Brian Brannon

设计和产品

Monette Velasco, Lead

Jennie Zhu-Mai, Lead

Mark Bartosik

Larry Bauer

Erica Hardison

封面设计 Andrew Baker

平面设计 Hector Torres

高级商务拓展经理 Sandy Brown

高级广告经理

Marian Anderson Debbie Sir

产品和服务总监 Evan Buttereld

会员总监 Eric Berkowitz

编辑服务高级经理 Robin Baldwin Manager

编辑服务内容开发 Richard Park

主编

Sumi Helal

University of Florida

helal@cise.u.edu

副主编

Ying Dar Lin

National Chiao Tung University

ydlin@cs.nctu.edu.tw

副主编, COMPUTING PRACTICES

Rohit Kapur Synopsis

rohit.kapur@synopsys.com

副主编, PERSPECTIVES

Bob Colwell

bob.colwell@comcast.net

副主编, SPECIAL ISSUES

George K. Thiruvathukal

gkt@cs.luc.edu

副主编, MULTIMEDIA EDITOR

Charles R. Severance

University of Michigan

csev@umich.edu

2016年IEEE计算机协会主席

Roger U. Fujii

Fujii Systems

r.fujii@computer.org

行业编辑

大数据和数据分析

Naren Ramakrishnan

Virginia Tech Ravi Kumar Google

云计算

Schahram Dustdar

TU Wien

计算机架构

David H. Albonesi

Cornell University

Greg Byrd North

Carolina State University

Erik DeBenedictis

Sandia National Laboratories

绿色和可持续计算

Kirk Cameron

Virginia Tech

健康信息学

Upkar Varshney

Georgia State University, Atlanta

高性能计算

Vladimir Getov

University of Westminster

识别科学和生物识别技术

Karl Ricanek

University of North Carolina

Wilmington

物联网

Roy Want

Google

安全和隐私

Rolf Oppliger

eSECURITY Technologies

软件

Renée Bryce

University of North Texas

Jean-Marc Jéz é quel University of Rennes

视觉、可可视化和增强技术

Mike J. Daily

HRL Laboratories

顾问委员会

Doris L. Carver

Louisiana State University (EIC Emeritus)

Carl K. Chang

Iowa State University (EIC Emeritus)

Theresa-Marie Ryne

Consultant

Bill Schilit

Google

Savitha Srinivasan

IBM Almaden Research Center

Ron Vetter

University of North Carolina

Wilmington (EIC Emeritus)

Alf Weaver

University of Virginia



中国计算机学会(CCF) 会员专属权益

▽ 项目

▽ 会员

▽ 非会员

▽ 说明

CCF通讯 (CCCF)	免费	480元/年	全年12期，纸质版，每月邮寄；另有PDF版及IPAD版
中国计算机科学技术年度发展报告	免费	96元/册	权威报告，每年一册，电子版
特价加入ACM	100元/年	240元/年	CCF会员特价加入ACM会员，享受ACM会议优惠、ACM电子版通讯、电子刊等
YOCSEF	免费	付费	除北京总部外，CCF已在24个城市建立了分论坛，每年活动逾百次
会员活动中心活动 (CCF城市分部)	免费	付费	CCF已在24个城市建立会员活动中心，每年活动逾百次
计算机职业资格认证 (CSP)	优惠	付费	一年3次，每年近万人参加，认证结果受到知名高校及企业认可
CCF电子刊	免费	无	每月6期
数字图书馆	免费	无	期刊、培训视频等资料
CCF网站信息发布	免费	无	会员登陆会员系统后在CCF官网发布会员成就、推荐会议、求职、招聘等信息
选举权、被选举权、参与学会治理	专有	无	
中国计算机大会 (CNCC)	优惠	全价	每年一次，每次参会人数逾3000人
学科前沿讲习班 (ADL)	优惠	全价	每年10期，每期邀请该领域国内外顶级专家作为讲者
IEEE CS准会员资格	65元/年	+240元/年	享受IEEE CS会议优惠、每月3期电子刊等
专业委员会议	8折	全价	CCF拥有35个专业委员会，每年活动近百次
CCF13种会刊论文版面优惠	8.5折	全价	限第一作者

获得以上CCF会员专属服务，只需支付**200**元/年会费！

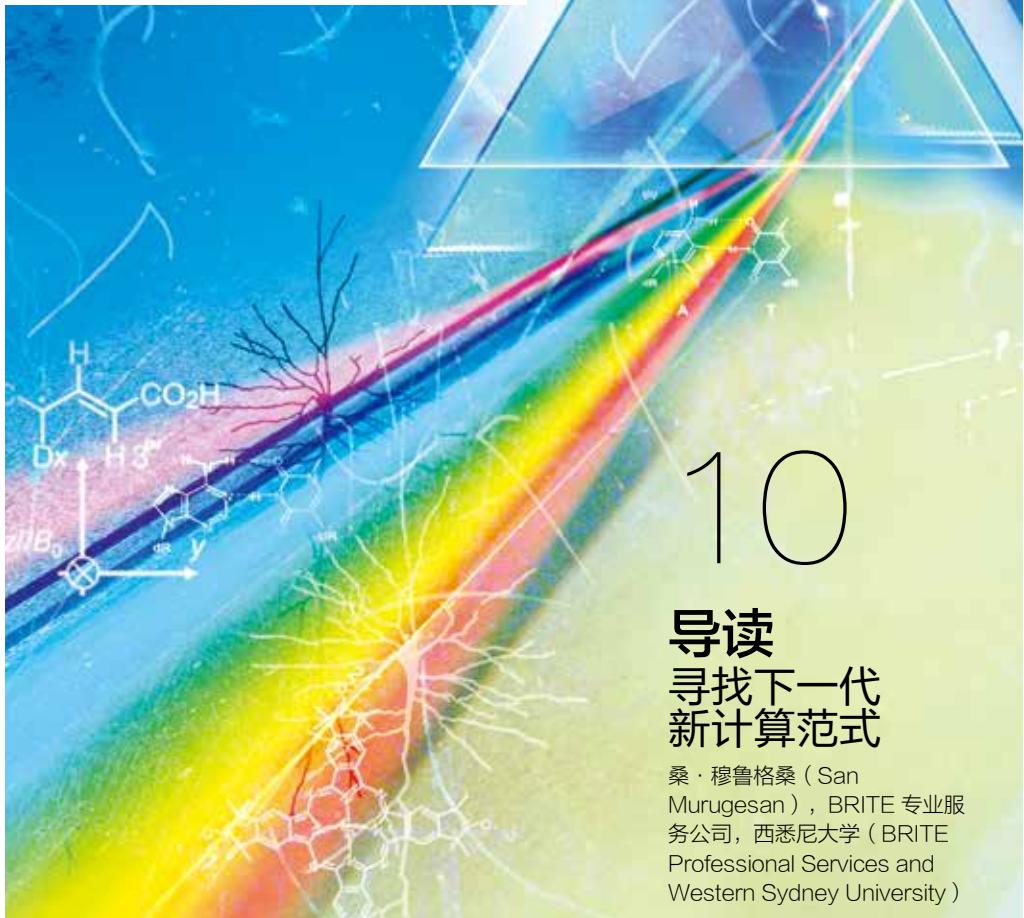
地址：北京科学院南路6号
电话：(86-10) 62648654
网址：www.ccf.org.cn

通信：北京2704信箱，100190
邮箱：membership@ccf.org.cn



扫码成为CCF会员

计算科学评论



10

导读 寻找下一代 新计算范式

桑·穆鲁格桑 (San Murugesan), BRITE 专业服务公司, 西悉尼大学 (BRITE Professional Services and Western Sydney University)

2016年11月刊

封面报道

17

29

41

计算的量子未来

克里斯塔·M·斯沃
特罗耶·马赛厄斯

通往可扩展的分布 式量子计算之路

罗德尼·范米特

实体分子计算: 机遇 与挑战

维多利亚·科尔曼

2016年11月刊

目录



52

从群体智能到元启发：自然启发式优化算法

杨新社
方正天
贺兴时
赵玉新

62

与大脑皮层互联的计算：协同式脑机接口新范式

萨米尔·萨普罗
约瑟夫·福勒
维克多·辛
保罗·赛达
尼古拉斯·维托维奇等

计算访谈

06 活的计算机博物馆

查尔斯·赛佛伦斯（Charles Severance），密歇根大学（University of Michigan）

本文作者参观了华盛顿州西雅图市的活计算机博物馆，想要找回从前

科幻小说原型

76 工作中的原型科幻

伊万·艾瑟顿（Evan Atherton）

尽管欧特克以设计类软件而闻名，但其实这家公司已开始利用原型科幻来探讨设计、技术及人类的未来。

会议

79 2016年全国社会媒体处理大会介绍

中国中文信息学会社会媒体处理专业委员会

图片新闻

08 可折叠的轻薄显示屏

26 史上最小晶体管诞生

50 DNA 电路

72 能扎针的机器人

74 互相帮助的机器人



活的计算机博物馆

文 | 查尔斯·赛佛伦斯 (Charles Severance)，密歇根大学 (University of Michigan)

译 | 刘大明

本文作者参观了华盛顿州西雅图市的活计算机博物馆，想要找回从前

活

计算机博物馆 (Living Computer Museum) 位

于华盛顿州西雅图市，它设立的目标别具一格：让计算机的旧技术保持生机，并随时供老人体验使用。博物馆没有将这些老旧的艺术品放入温控玻璃柜，馆内的大多数计算机都处于开机状态，并配有操作指南供阅读，还有一把椅子和一个键盘，在这里你可以真正体验一下使用过去的计算机是什么感受。你来到这家博物馆，就准备坐下来好好玩吧。这里有一段我去博物馆时拍的视频，其中有一段幕后之旅，看看他们如何维护这些几十岁的老设备的日常运转。

让旧技术维持运转

这座博物馆由微软共同创始人保罗·艾伦 (Paul Allen) 等人出资支持，目标是要保证参观者可以在这里体验到计算机技术过去50年来的兴起和发展历程。尽管该馆也会对历史上重要的计算机技术进行收集、分类、解释和展览，但大多数时间都是在对展出的计算机进行保养和维修，以确保其正常运行。该馆的馆员兼案卷保管员辛德·莫亚 (Cynde Moya) 表示：

在许多计算机博物馆里，艺术品是一种“特殊而神圣的东

西”。你会把它小心地收好，一般情况下从来不使用。而我们这座博物馆是零件实验室与博物馆的一个真正的交汇。我们的藏品就是一种资源，可以作为计算机使用，也可以当作零件来修复另一台计算机。这就是说，我们不但要对藏品进行跟踪监测，还要监测藏品内部的零件，这些零件可能会被拿去修理别的计算机。

如果找不到替换零件，或是原来的零件太贵或存在可靠性问题，有时就需要对计算机做一点点调整。比如，馆内藏有许多由数字化设备公司 (DEC)



出品的系统，它们都使用相同的电源。原来设计的电源效率太低，需要定期修理，而且维修费用很高。博物馆的高级系统工程师基斯·佩雷斯（Keith Perez）表示：

馆内的多种DEC机共有56部电源。我们需要每隔13年将电源上的又大又贵的电容更换一次，因为它们会坏掉。所以我们决定改用一种现代设计方案来维护。我们使用的新电源比原来的DEC电源更好，电源内部不使用焊接，可靠性更高。它使用军用级供电模块，保修40年。我们采购了不少，每台350美元，现在都装在DEC机上。

解决电源不稳定这类问题是一种有趣的挑战。你必须要搞清部件的工作原理，利用现代科技找到一种更好的替代方案。基斯表示，DEC机的新电源比原来的电源在能耗上要省电得多。

原来的电源是线性供电，能效只有15%。而新电源的能效高达90%。这使我们节约了大量的散热费用，因为新电源的发热要低得多。机器的运行温度更低、故障更少，我们的维修频率也越来越低。

一堂重要的历史课

该馆的目标是让这些老计算机能够实现24/7的连续可靠的运行，辛德表示：

让这些计算机恢复使用是我们博物馆的特别之处。来展厅参观的人可以使用这些机器，还能上网。用户可以获得账号、登录，再尝试一下真实计算机上运行的不同操作系统。

博物馆的目标是 让参观者体验计算机技术过去 50 年来 兴起和发展的历程。

来馆参观之前，最好重温一下 BASIC 编程基础，要想使用早期的许多迷你机和微型机，你需要了解 BASIC 语言。我个人最喜欢使用 TTY-33 终端设备在 RPD-8 型迷你机上写 BASIC 程序。我还在 Heathkit H-19 迷你机上写过一些 BASIC 程序，此外还在早期的太阳公司的工作站上写过一个“Hello world” C 语言程序。

在馆内可以使用这么多老计算机，但最有趣的展品还是一台 IBM-029 型键控打孔机。插入空白卡片，输入七个空格（Fortran 语言要求），然后开始打字，字符串由机器打出的孔表示。这一过程仿佛让我回到了上世纪 70 年代刚开始学习编程的日子。IBM-029 打孔机当时非常好用，我也乐于重温那段早年的经历。

辛德还说到程序员来馆参观时都有哪些反应。

老人来参观时常常会有怀旧感。他们会高兴地说：“快看啊，

这机器原来我也有，真令人激动。啊！我想起来了！”他们会想起曾经的日子，那时计算是很困难的事情，载入程序需要使用盒式磁带，或者使用电传打字机与程序进行交互。

如果来参观的是精通技术的年轻人，那么这些老计算机就是一堂重要的历史课：从一些机器身上可以看到我们在这么短的时间内取得了多么大的进步，从这些巨型超级计算机发展到了今天的电话，计算力超过了整个博物馆的展品。

如果你住在西雅图，就应该打算来这里看看，在这里你可以近距离接触这些精美的艺术品。但一定要小心：一旦你坐下来，开始使用这些精美的老计算机，你可能会在这里呆上一整天而流连忘返。C

查尔斯·塞弗伦斯（Charles Severance）是密歇根大学信息学院临床副教授，也是《计算机》杂志多媒体编辑。联系方式：csev@umich.edu，Twitter:@drchuck



图片新闻

可折叠的轻薄显示屏

瑞典查尔莫斯理工学院的研究人员利用等离子聚合物材料制成的电子纸的发光原理与 Kindle 类似，但耗能还不到 Kindle 屏幕的十分之一。这块屏幕还不到一毫米厚，但却可以显示五彩斑斓的几乎整个色域。

论 文：*Plasmonic Metasurfaces with Conjugated Polymers for Flexible Electronic Paper in Color*

寻找下一代新计算范式

文 | 桑·穆鲁格桑（San Murugesan），BRITE 专业服务公司，西悉尼大学（BRITE Professional Services and Western Sydney University）

鲍勃·科尔威尔（Bob Colwell），R&E Colwell & Associates

译 | 刘大明

为了解决新计算应用的问题，我们必须寻求激进的新计算范式。通过量子计算、生物启发式计算和纳米计算，我们可以探索能够改变生活、造福社会的新方式。

在过去50年中，计算机技术的发展已经重新定义并改变了我们生活中的每个领域，但其基本计算概念一直没有改变，依然遵循着阿兰·图灵和冯·诺依曼最初提出的设想。随着对计算、存储和通信需求的逐步扩大，基于硅和传统架构的数字计算机已经达到了物理极限，并面临相关的经济性和可靠性问题。因此，在天气预报、生物信息学、机器人和自动化系统等领域出现了一些与传统计算范式有关的局限性问题。

我们是否需要对现代传统计算机的这些基本原则和假设

进行革命性的再思考？是否需要探索和利用新的计算范式来解决尚未解决的、不可预知的挑战？答案当然是肯定的。在这个过程中，我们将重新定义计算，并努力寻找下一代计算的新范式。

下一代计算范式

研究人员和业界已经在探索新的计算范式，如量子计算、生物启发计算、纳米计算和光学计算等，这些新范式都有

重新定义计算和寻找下一代计算
范式的旅程已经开始

可能带来一系列颇具挑战性的新应用。对这些新兴的创新方法的理解、掌握和应用能让我们更有力地描绘计算学科的未来。本期封面文章对一些新计算范式的原则和潜力进行了探索，研究了其现有状态和未来前景。我们希望借此启发对这一方向的进一步研究和实践。

本期内容

本期封面报道的文章探索了量子计算、分子计算、自然启发式算法以及通过大脑皮层互联计算的协同人机交互。这些方法有助于我们通过创新来解决现在及未来面对的计算挑战。有两位专家发表了对于下一代计算的观点，提出了量子计算将给信息安全带来哪些影响（具体见本文插文中的两篇文章）。此外，为了帮助读者理解这些新的计算范式，我们推出了一个视频合辑。请访问www.computer.org/web/computer-multimedia观看。

量子计算的进展

在某些情况下，现有经典计算机无法完成的计算问题可以用使用量子力学叠加和纠缠性质的设备来解决。这种方法让我们能够设计出具有超过所有经典计算机性能的设备。近来，量子器件和量子技术已经引起了研究人员和工业界的广泛关注。其实，在市场上已经可以买到用于生成随机数和安全加密通信的量子技术了。

在《计算的量子未来》一文中，克里斯塔·M·斯沃 (Krysta M. Svore) 和特罗耶·马赛厄斯 (Matthias Troyer) 描述了量子比特、量子门和量子算法的原理。作者还概述了使用量子计算机作为专用协处理器；强调了量子算法在一系列应用中的运用，例如加密，(保护)隐私和搜索；并提出了用于量子计算的软件堆栈。

在《通往可扩展的分布式量子计算之路》一文中，罗德尼·范米特 (Rodney Van Meter) 和西蒙·德维特 (Simon J. Devitt) 提出了用于大规模量子计算的结构模型。他们描述了操作大型量子计算机所需的经典资源，并探讨了支持可扩展

视角：下一代计算范式与信息革命

文 | 埃里克·本尼迪克蒂斯（Erik DeBenedictis），桑迪亚国家实验室（Sandia National Laboratories）

新的计算范式能够推动信息革命的完成。当今社会对计算的定义基于阿兰·图灵和冯·诺依曼以及戈登·摩尔的贡献。图灵描述了如何基本使用C语言来描述一个可计算问题的解。冯·诺依曼建立了运行程序的计算机架构，而摩尔描述了半导体规模的扩展会使计算机的性能随时间呈指数级增长。

对摩尔定律的信心压制了其他计算范式的成果。如果只需发展半导体，就能让我们解决可计算问题的能力实现指数级增长，还研究其他东西干什么？我回想起几年前有个新计算机架构的研究寻求资助，该项目声称能让微处理器的能效提高10倍，当时的一个反对意见就是，“我们现在什么都不做等上四年，然后买一台普通计算机，按照摩尔定律，它的性能就是现在的10倍了。”

然而，传统的计算范式存在几个重大局限，甚至连摩尔定律都无法解决。

» 计算机解决一些问题需要无限大的内存，但实际计算机的内存有限。

- » 除非人类对计算机编程，否则它们什么都不会做。
- » 一台计算机可以永远运行下去，但仍解决不了某些问题，比如分解质因数。
- » 戈登·摩尔的预测仅仅始于1975年。

所以，现在应该转移注意力，通过其他途径解决这些局限性。比如生物计算、人机合作和量子计算等。

生物计算

一些仿生学的计算方法能补救计算机内存不足的问题。一些算法需要大量的内存，但是冯·诺依曼架构的计算机因为不具备制造内存的能力，所以自己无法增加内存。然而，生物细胞可以在保留复制能力的基础上被修饰用于计算。这样一来，细胞既可以作为电脑，也可以作为内存组装设备。即使没有人类的帮助，执行特定计算任务的一小簇细胞也能发育成越来越大的规模。

人机合作

今天的计算是程序员和硬件实现合作的结果，但我们可以改

量子计算机构造的各种不同系统的实
验进展。

这篇文章不仅描述了实体分子计算的原
理和潜能，而且也指出了建立、使用通
用分子计算机所面临的挑战。

呼吁在某些领域实现进一步发展，以解
决现实世界中各类应用问题。

分子计算

寻找更好、更快，更加经济的革命性的新算法解决传统计算机瓶颈问题的需求，引发了分子计算的研究。这种方法有可能从信息密度、平行性和能量效率方面大幅改善传统计算方法。

在《实体分子计算：机遇和挑战》一文中，维多利亚·科尔曼（Victoria Coleman）描述了一种通过生物修饰用“被编程”的活细胞来完成计算任务的方法。在实体分子计算中，生物系统，包括DNA等细胞材料被用来执行计算。

源于自然的计算灵感

自然启发人们提出各式各样巧妙的问题解决办法与最优化策略。确切地说，自然启发算法尤其适合解决最优化问题、机器学习以及多目标和高度复杂的设计问题。

在《从群体智能到元启发：自然启发式优化算法》一文中，杨新社、苏阿什·戴布、方正天、贺兴时和赵玉新描述了自然衍生算法的近期发展，对这些来源于生物行为的算法进行了概括。他们

协同式人机交互与团队合作

人与机器的交互和合作方式很可能出现巨大进步。在《与大脑皮层互联的计算：协同式脑机接口新范式》一文中，萨米尔·萨普罗（Sameer Saproo）、约瑟夫·福勒（Josef Faller）、维克多·辛（Victor Shih）、保罗·赛达（Paul Sajda）、尼古拉斯·维托维奇（Nicholas R. Waytowich）、艾迪森·伯翰农（Addison Bohannon）、维农·劳伦（Vernon J. Lawhern）、布伦特·兰斯（Brent J. Lance）、大卫·江劳（David

变这种合作的性质。在最近的机器学习的突破中，由人类构建一个程序结构，计算机在该结构下做了大量的简单编程工作。此外，人机界面为这种合作提供了新的运行界面。这可能在未来产生新的人机合作模式，即具备计算机的高计算能力，又具备人的问题解决能力、动机与直觉。

量子计算

有些问题在传统计算机上解决需要非常长的运行时间。根据传统计算机复杂度理论，解决规模为N的问题，比如输入数据为N个比特，该问题只有在多项式次数小于等于N的情况下才“容易解决”，如果次数过大，比如N的指数级，那么即使有摩尔定律的指数级增长也不足以解决。

量子计算能够打破这个局限。比如，对数N进行分解质因数。非量子最优算法是数域筛选法(*number field sieve*)，步骤数约为 $\exp(1.52(\log N)^{1/3}(\log \log N)^{2/3})$ ，这个表达式比较复杂，但是是个关于e的指数函数，表明步骤数要高于多项式函数。因此这个问题就是“难于解决”的。但如果使用量子计算，运行时间约为 $(\log$

$N)^2 (\log \log N) (\log \log \log N)$ 次量子操作，这个值在多项式法步骤数范围之内。由于N值一般在密码分析中使用，所以按第一个式子得到的运行时间超过了宇宙的年龄，而第二个式子则可以接受。

未来展望

很明显，人们有兴趣继续进行信息革命，并在经济方面加以扩展。这场信息革命最初的动力是摩尔定律的预测在10年后到更长的时间内可能不再适用。尽管最初的项目已经达到了极限，但计算机和计算技术的新模式将会变得越来越现实和实用，成为推动这场信息革命的新动力。

参考文献

1. E.P. DeBenedictis, "Rebooting Computers as Learning Machines," Computer, vol. 49, no. 6, 2016, pp. 84–87.

埃里克·本尼迪克蒂斯(Erik DeBenedictis)是桑迪亚国家实验室非传统计算技术部门的技术人员。联系方式: epdeben@sandia.gov。

Jangraw)假定机器智能基本可以达到人类智能的效率，人类可能不一定需要对机器进行明确编程。作者通过几个真实系统的实例解释了与大脑皮层互联计算的概念，即人和机器都活跃参与到计算任务中，人机通信通过脑机接口(BCIs)进行。这类系统将人脑发出的信息教授给未经事先编程的机器，为我们展望了一个可能的美好未来。即掌握先进人工智能的计算机和人一起合作，共同执行任务，增强了人机之间的协同。实现人机协同交互的大脑皮层互联计算，其性能可能超过人机的计算力之和。

计算范式还将继续发展和演化，使

计算获得新的能力，扩大其应用范围，并提升实用性。为了成功获得新计算范式带来的潜力，研究人员、开发者和业界必须要解决几个问题：我们如何有效解决这些新计算范式带来的挑战？这些新范式能否在下一代计算机上演化并实现？它们能否转换为其他形式？



过本期的几篇封面文章，我们向读者简要介绍了新兴计算技术的发展，我们鼓励来自多个领域的研究和开发人员互相学习和合作，进一步推进计算技术的进步。■

参考文献

1. "Rebooting Computing," special issue, Computer, vol. 48, no. 12, 2015; www.computer.org/csdl/mags/co/2015/12/index.html.
2. "Rebooting Computing Initiative," website, IEEE; <http://rebootingcomputing.ieee.org>.
3. S. Murugesan, "Radical Next-Gen Computing," Computing Now, vol. 8, no. 6, June 2015; www.computer.org/web/computingnow/archive/radical-next-gen-computing-june-2015.

视角：量子技术对信息安全的影响

文 | 简·梅里亚 (Jane Melia), Quintessence实验室 (QuintessenceLabs)

对量子技术的讨论逐步将重点转移到了量子计算机及其性能上，同时受到关注的还有该技术会给当前的网络安全基础设施构成哪些威胁。但很多人并不知道，量子技术也可以作为增强安全的解决方案，在保护最敏感的数据方面，量子技术前途光明。

威胁：量子计算机面临的安全挑战

量子计算机一向被奉为下一代计算机革命的标志。通过叠加和纠缠等纯量子力学现象，量子计算机可以解决以前不能解决的问题。现在，量子计算机已经解决了某些类别的问题，如因数分解问题。随着研究的继续，人们还将发现更多的量子算法，这会产生一些研究分支，如医学研究。

但是，量子计算机也给当前的安全基础设施造成了挑战。现有的加密密钥分享策略要部分依赖于对一个大合数进行分解质因数的高难度，传统计算机无法在合理的时间内解决这个问题。而一旦量子计算机走向成熟，就会迅速攻破这个数学上的挑战。这样，通过公用密钥基础设施进行密钥共享就将不再安全。

对称加密本身还是安全的，条件是密钥长度足够长（加倍），并且完全随机。因为使用Grover算法的量子搜索预计只能让搜索速度呈平方级增长，现已证明不可能出现速度呈指数级增长的搜索算法。遗憾的是，在后量子世界，公用密钥共享已经不再安全，对称加密的安全性已经无关紧要，除非我们找到一个安全传输的方法。

美国国家标准技术研究所（NIST）估计，成熟的量子计算机可以在15年内攻破我们的公用密钥基础设施。这听起来好像很遥远，但我们已经在与时间赛跑了：更新基础设施需要数年时间，而且许多敏感数据需要安全地保存很长一段时间，随着量子计算机的成熟，它们很容易被以后的解密技术获取并保存。任何打算长期保存个人或财务信息的组织都需要尽早做好准备。

正面影响

量子技术也可以用来增强数据安全，既能用来防御现在的进攻，也能防御未来的量子计算机的进攻。一般将这一领域称为量子网络安全。

除了与量子计算机相关的威胁之外，随机数的质量太低或数

量不足也会带来安全风险。如何高速生成高质量的随机数已经成为一个非常难解决的问题。幸运的是，量子技术能够为这个问题提供简练而强大的解决方案。

量子物理中的很多过程是随机的，这种内在随机性已被用于商用量子随机数生成器上，它能以低成本的方式高速生成完全随机数，彻底解决了这个问题。这些设备已经在金融等领域开始与云安全基础设施整合，这一趋势预计在未来几年内将越发明显。美国国家安全局（NSA）也确认并推荐使用质量更高、长度更长的密钥，作为保护数据免遭量子计算机侵入的策略。所以，使用高质量的量子随机数生成器，可以让安全意识强的公司朝这个方向先行一步。真随机数也是使用单本加密（one-time pad encryption）的先决条件。在这种加密方式中，加密文本不提供关于明文文本的任何信息，所以是安全的，与攻击者的处理能力无关，包括量子计算机攻击。

在更高的层面上看，量子密钥分发（QKD）利用量子力学定律来实现双方的私密信息共享，即使双方并不能控制通信链接。因此也就解决了前文提到了那个棘手的问题。它的安全性基于量子力学的基本性质：对量子系统的测量过程会对系统造成扰动。如果攻击者试图拦截密钥传输，就会不可避免地留下可监测的踪迹，使得相应的密钥信息被废置不用。现已证明，量子密钥分发在信息上是安全的，也就是说这种安全和攻击者的数据处理能力无关，也无惧量子计算机的攻击。但这种开发技术仍存在一些需要克服的挑战，不过很多企业已经开始推出商业化的实现方案，现在已经有团队在进一步开发，突破其点对点传输能力，将该技术从光纤网络移至自由空间，最终目标是应用在移动设备上。这绝对是值得关注的方向。

未来前景

除了这些技术驱动型解决方案之外，人们也在寻找能够同时防范传统攻击和量子计算机攻击的算法。这些能够抵御量子攻击的算法将会面临挑战：它们不能作为现行方法的普适性替代方案，因此需要修改现有的协议。而且，它们可能无法抵御新攻击。新算法可能要用几年时间才能实现标准化。但这些算法的灵活性是量子安全总体方法的一个重要要素。

为了保护我们的数据免遭强大的量子计算机的侵入，很可能会出现混合式解决方案。我们会利用完全随机性，让密钥强度变

得更高，并使用灵活的量子密钥分发全球网络保护关键的通信连接，抵御量子计算机的入侵。最后，更高级的算法可以更好地保护更短、暴露更少的连接，并根据威胁的增长定时更新。

然而量子计算机仍然是网络安全的主要威胁。量子随机数生成器、量子密钥分发和抵御量子攻击的算法正在努力应对这一挑战，使我们在利用量子计算获益的同时保证信息安全。

发现更多的内容

现在围绕着量子安全的开发和活动有很多，越来越多的企业和政府机构在寻求保护机密信息，标准化组织也在寻求构建新的安全通信方式，许多公司和研究机构正在开发应对这一挑战的解决方案。如果读者有兴趣了解更多的信息，可以与量子安全工作小组（QSS-WG）联系，该组织于2014年底在云安全联盟内部成立。这个组织的论坛上活跃着多个企业、组织和个人，其目标是增进对量子安全加密技术应用的理解、接受、使用和传播，促进这些技术向商业机构、决策者和其他相关政府部门的推广。

参考文献

1. D. Moody, "Post-Quantum Cryptography: NIST's Plan for the Future," Nat'l Inst. Standards and Technology; <http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf>
2. K. Kennedy, "NSA Recommendations Include High Entropy and Longer Keys to Protect Against Quantum Computer Developments," CTOVision.com, 12 Oct. 2015; <https://ctovision.com/2015/10/nsa-recommendations-include-high-entropy-longer-keys-protect-against-quantum-computer-developments>.
3. C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proc. IEEE Int'l Conf. Computers, Systems, and Signal Processing, 1984, pp. 175–179; [www.cs.usb.edu/~chong/290N-W06/BB84.pdf](http://cs.usb.edu/~chong/290N-W06/BB84.pdf).

简·梅里亚（Jane Melia）是Quintessence实验室战略商业开发副总裁，云安全联盟（CSA）量子安全工作小组共同主席。联系方式：jm@quintessencelabs.com。

关于作者

桑·穆鲁格桑（SAN MURUGESAN） BRITE

专业服务机构主任，西悉尼大学兼职教授。他是《IT：专业技术》杂志主编、《计算机》和《IEEE云计算处理》编委会成员，《绿色IT：原理与实践》及云计算百科全书的编者之一，《计算机》云技术专栏编辑。穆鲁格桑是澳大利亚计算机学会资深会员、电子与电信通讯研究所（IETE）会员。

联系方式：san@computer.org 或 <http://bitly.com/sanprofile>。

鲍勃·科尔威尔（BOB COLWELL） R&E

Colwell & Associates 机构独立顾问，曾于2012–2014年任国防部高级研究计划局微系统技术办公室主任。1992–2000年间任英特尔公司IA32（奔腾）微处理器首席架构师。他于2002–2005年任《计算机》杂志观点栏目编辑，专栏作者。《奔腾编年史》作者之一。现任IEEE资深会员。联系方式：bob.colwell@gmail.com

微信名：计算人

微信号：jisuanren



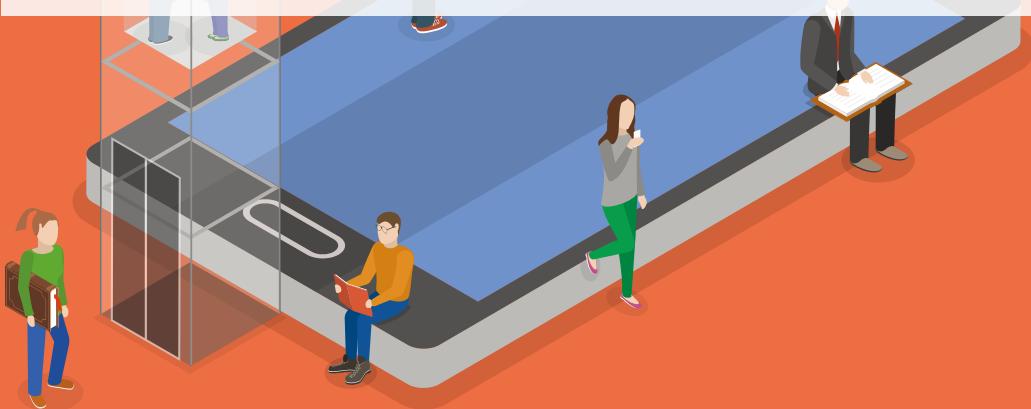
IEEE 计算机学会数字图书馆： IEEE 的首个电子图书馆



作

为全球领先的计算机科学及相关技术的信息出版商, IEEE计算机学会通过旗下的计算机学会数字图书馆(CSDL)通过在线和移动端提供学会的30多种期刊和5500多篇会议出版物。CSDL拥有流畅的用户界面、支持全文内容搜索和多项浏览功能选择, 能够保证快速返回搜索结果。CSDL内容包括60多万篇权威论文, 其作者人数超过25万, 可以为各个阶段的学生和专业人士提供最前沿的、经同行评议的内容以及历史上的过刊内容。

CSDL建立于1995年, 是技术内容数据库的早期成功案例之一, 并于5年后催生出了IEEE Xplore, CSDL是一个具有革命性意义的计算机出版物资源库, 其影响力涵盖了诸多应用领域, 包括太空探索、医疗、商务处理、网络安全、软件工程和全球人道主义救济活动等。CSDL以报道计算机相关的广泛领域的专家成果为特色, 不仅可以作为一个关键参考点, 也是许多新开发、技术进步和创新思想的助推器。大学、企业和订阅用户可以很方便地在第一时间获得首先在学会杂志、通讯和会议论文集上发表的最新信息。■





文 | 克里斯塔·M·斯沃 (Krysta M. Svore), 微软研究院 (Microsoft Research)

特罗耶·马赛厄斯 (Matthias Troyer), 苏黎世联邦理工学院和微软研究院 (ETH Zurich and Microsoft Research)

译 | 贺冉

尽管还处于发展初期，量子计算却已在颠覆我们当前关于计算方法和设备的观念。了解量子计算所带来的应用以及如何驾驭它们，将改变经济、产业、学术和社会格局。

在

量子力学诞生一个世纪之后，我们正站在一个新时代的门槛上，量子特性不仅让我们制造出经典设备，如晶体管，也将让这些设备进化至

超越它们现有的能力。不同于经典计算机，量子器件可以同时处于多个不同状态的“叠加”上，并在空间上分离的实体之间有着深刻的联系（“纠缠”）。这些特性使得我们有可能设计出功能上超过任何可以想象的经典计算机的设备。实际上，能够生成量子随机数和为通信加密的设备在市场上已经可以买到了。

可以说最简单的量子器件就是量子随机数发生器，它使用的是叠加态的性质：一个量子比特（在量子计算机中信息的基本单元，也称量子位，qubit）可以被制备成处于状态 $|1\rangle/2$ ($|0\rangle+|1\rangle$)，这是经典比特0和1的叠加态（见侧栏《量子比特和量子门》）。一旦测量该量子比特的值，叠加态就会坍缩成

两种经典状态之一，测量结果为0或1中的一个值，概率各占二分之一。这个过程实现了真正的随机数生成器，而由于传统物理的确定性性质，这有经典方法是不可能实现的。

把两个量子比特 A 和 B 纠缠到叠加态 $|1\rangle/2$ ($|0\rangle A |0\rangle B + |1\rangle |1\rangle$) 中，使得它们要么都为0要么都为1，这个态可用在密码技术中。考虑有两个参与者 Alice 和 Bob，他们想交换秘密消息。给 Alice 分配一个量子比特（标 A 的量子比特），另一个给 Bob（标 B 的量子比特）。不管 Alice 和 Bob（及其各自的量子比特）分离多远的距离，这两个量子比特都可以一直保持纠缠。当 Alice 和 Bob 测量他们各自的量子比特时，他们将分别读取到一个随机的测量结果。但是，他们都将获得相同的随机数。此过程可用于量子隐形传态（传输量子信息）或建立一个共享密钥进行安全的通信，这又一次超越了经典的技术。

面对在经典计算机上模拟量子系统的困难，理查德·费曼

(Richard Feynman) 在1982年建议，构建利用量子效应进行计算的计算机，将经典计算机的比特和门操作推广为量子比特和量子门¹。事实证明，所谓的量子计算机的用途远远不止解决物理问题，而且我们已经有了各种各样优于其经典对应算法的量子算法（见侧栏《量子算法》）。

量子计算机最广为人知的特点是它能够解决整数分解问题²，即给出整数 $N = P \times Q$ ，任务是确定质数 p 和 q 。这个问题构成了今天电子商务的支柱，因为它是RSA的基础。RSA是使用最广泛的公钥密码体制。由大约十亿个物理量子比特³的量子计算机就可以在很短的时间里破解2000位的RSA密钥。尽管破解加密方法的量子算法的确体现了量子计算的优势，但是随着旨在抵抗量子攻击的“后量子”经典密码系统的开发，其重要性一定是会降低的⁴。世界各地的公司和政府都已经开始积极从RSA等公钥方案过渡到后量子的密码系统，因为实现量子安全的方法所必需的软件升级将至少需要十年才能完成。

在对物理系统的模拟中，涌现除了越来越多影响力巨大，且有经济价值的应用，这是费曼的开创性论文背后的原始动机。在超级计算机目前的使用中，分子和材料的量子模拟占主要部分。用量子计算机进行几天到几个月规模的分子和材料的精确的模拟，就将相比于采

取最先进的超级计算机进行数十亿年的计算还要可靠。这些模拟可用于帮助解决严峻的实际问题，如阐明生物固氮的机制，这可以用于化肥生产⁵，或设计用于碳捕集和封存的催化剂，以应对全球变暖。改进这些方法，可以帮助材料建模找到解决方案，包括找到高温超导材料，用于低损耗电力传输和磁悬浮列车（使用磁悬浮的超高速列车，列车运行甚至可以不接触地面）。

利用经典机器学习法来进行预测，并获得基于数据的分析，过去的十年取得了爆炸式的进展。机器学习已经彻底改变诸如语音识别、计算机视觉和网络搜索等领域。凭借在计算统计方面的基础，机器学习领域已经做好被量子计算改进的准备。最近的结果表明，量子算法可以实现分类和聚类等方法，例如 k 均值和最近邻方法，这要比经典方法更高效。Boltzmann机器训练、深度学习和神经网络也被证明可从量子计算中受益。

总的来说，量子算法的运行时间复杂性相对于经典算法来说是不是的确有所改进，还需要严格的证明。不过，在实际数据中表现最好的算法实际上往往都是启发式的算法。因此，我们可以期待拥有一台用于测试和掌握量子编程和算法设计艺术的中等规模的量子计算机。这个努力的成果将导致许多具有现实应用的量子算法出现，我们这一代程序员期待着在速度和准确性上

有新颖改进的量子硬件。

量子计算机作为专用加速器

量子计算机不像它们的经典堂兄弟。虽然在原则上它们可以执行任何经典计算机能够执行的计算，但我们不该期望用量子计算机来驱动未来的个人电脑或手机。在这些任务中，经典计算机将一直比量子计算机更便宜，更小，更轻便。通过操作处于叠加态的数值，量子计算机在运行特殊量子算法解决特定计算任务的时候，其运行速度比任何经典计算机都要快（在某些问题中会有指数级的加速能力），展现了其强大之处。因此，一个量子计算机将作为协处理器，接收经典处理器堆栈的说明和提示。为了抑制噪声和错误，从而让量子比特保持在叠加态，量子计算机的大多数设计都需要用稀释制冷机将量子比特冷却到非常低的近乎绝对零度的温度。我们设想，大规模量子计算机将在数据中心里运行，可以作为云服务远程访问。在本地，人们可能只拥有有限数目的量子比特，以此来建立安全通信，或使用安全的“量子钱”，这种钱是不可伪造的。

单纯只有低温并不足以让量子比特在一个不平凡的量子算法的运行时间里一直处于叠加态，还需要量子纠错

最优化问题的要素

当一个经典比特x只可以取两个值x=0或者x=1的时候，一个量子比特q却可以处于一个叠加态

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (1)$$

其中 α 和 β 是两个复数，满足归一化条件 $|\alpha|^2 + |\beta|^2 = 1$ 。将两个经典比特0和1作为二维的复矢量的基矢

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ 和 } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (2)$$

那么量子比特的状态可以用下面的矢量描述

$$|q\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad (3)$$

这也叫做量子比特的波函数。

推广到一个由N个量子比特组成的量子寄存器 $|x\rangle = |x_0x_1\dots x_{N-1}\rangle$ 时，就需要一个由系数 c_i 构成的 $2N$ 维的复矢量来描述所有可能的叠加态

$$|x\rangle = \sum_{i=0}^{2^N-1} c_i |i\rangle \quad (4)$$

其中整数*i*的第*k*个比特对应第*k*个量子比特的数值。

仅仅N个量子比特的状态就需要指数级的经典内存，这暗示了量子计算机很有可能相对于经典计算机具有指级别加速能力。目前高端的超级计算机几乎无法表示N≈50个量子比特的状态。在一些特定的应用上，大约有100个量子比特的小规模量子计算机就已经能够提供超越任何经典计算机的计算能力。

尽管在经典计算机上需要2N个复数来表示一个量子态，但当读取量子寄存器时，我们只能获取N比特的信息。测量时，在叠加态的所有 $2N$ 个经典值中，只有一个值被随机地选择出来，其概率分布由波函数中的系数的平方 $|c_i|^2$ 给出。

量子门，类似于经典门，通常只作用于几个量子比特。它们的作用可以被描述为在由波函数的系数构成的矢量x上的么正矩阵操作。表A列出了一些常用的门操作。这些矩阵的么正性意味着所有量子门都是可逆的。与经典逻辑门类似，电路线表示量子比特，

表 A. 标准量子门

符号	名称	矩阵
	非门	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
	泡利Y门	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
	泡利Z门	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
	阿达马门	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
	$\pi/8$ 门	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
	Z旋转门	$\begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$
	受控非门	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

方框表示作用于量子比特的门操作。作用在n个量子比特上的量子门可通过 $2^n \times 2^n$ 维的么正矩阵来表示。

对于单个量子比特的两个状态，我们使用一组基 $\{|0\rangle, |1\rangle\}$ ，对于两个量子比特的四个状态，我们使用 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ 为基。作用在n个量子比特寄存器上的这些门操作，可以通过作用在一个或者两个量子比特上面的门操作矩阵的张量积得出，对剩余量子比特的操作是与它们完全相同的。

(QEC) 来延长量子信息的寿命。只要在物理量子比特中的错误率低于一个给定阈值，那QEC就显然允许一个任

意大的量子计算高效执行。量子信息的不可克隆定理使得量子通信非常安全的，但很遗憾，这也使得QEC比要比经

典容错难得多。QEC会导致很大的开销，需要数千或更多的“物理”量子比特才能够实现一个对错误有保护能力的

量子算法

量子计算机优于经典计算机是因为使用的是量子算法, 它能够比最有名的经典算法 (<http://math.nist.gov/quantum/zoo>) 更好地解决一系列问题。我们在此列举出了一些例子。图A概括了许多量子算法的设计图。

- » **Grover 搜索算法。**搜索非结构化项目的数据库是计算机科学的一个关键问题。给定对函数 $f: \{0,1\}^n \rightarrow \{0,1\}$ 的估值能力, 任务是找到 x 满足 $F(x) = 1$, 如果这样的一个 x 不存在, 则返回无此项目存在。最坏的情况下, 在量子计算机上 Grover 算法只需要 $O(\sqrt{N})$ 次估值就可以解决非结构化的搜索问题, 而经典计算机则需要 $O(N)$ 次。
- » **周期查找。**给定一个周期函数 $f(x) = f(x+r)$, 找到周期 r 。经典上, 这需要 $O(r)$ 次函数计算。而在量子上, 使用 Shor 周期查找算法(这也是其大数分解算法基础), 同样的问题可在(相对比特数)多项式的时间内解决, 给出函数值和

参数, 所用时间可以指数地小于 r 。

- » **线性系统。**给定一个 $N \times N$ 的矩阵 A 和一个 N 维矢量 b , 求 x 使得 $Ax = b$ 。经典上, 使用像高斯消元或迭代求解这些方法需要 N 的多项式的时间可以解决。但在量子上, 对于条件数 K 最多以 N 的多重对数增长的良态的矩阵, 只要求 $\log N$ 的多项式长的时间就可以求出解。
- » **分布中抽样。**经典上, 为了估计一个误差为 ϵ 的随机变量的平均数, 需要的采样数 N 就会按照 $N \propto \epsilon^{-2}$ 的规模来增加。量子上, 如果制备出的波函数可以表示这个分布, 则大概只需 ϵ^{-1} 次就可以测定期望值, 这要比经典少了一个平方。
- » **量子游走。**(随机)游走是指在一个给定的图形上一连串的随机轨迹。经典随机游走的量子推广就是量子游走, 它能够产生一个量子叠加态, 其概率分布与一个经典的随机游走的概率分布一致。它们比经典随机游走传播得要快很多, 这减少了基于游走算法的到达时间和混合时间。

“逻辑”量子比特。

拓扑量子比特将信息编码到量子态的非局域性质上, 利用对本地噪声源保持鲁棒性, 这是减少QEC开销的一个有希望的方法。虽然QEC工作在软件层面, 拓扑量子比特也有内在的, 硬件水平上的保护, 这使量子比特能有更长的寿命和较低的错误率。有了较低的错误率, QEC的开销可以被显著地降低好几个数量级。

鉴于量子容错的成本, 量子比特在量子计算机中是一种稀缺资源, 因此量子计算机与经典计算机相比在设计上有一个根本性的转变, 因为经典的内存很便宜。早期量子计算机并非将数据移动到计算单元, 而是将操作移动到数据上, 直接在寄存器量子比特上施加门操

作。在许多电子系统中, 其控制和操作计算机或设备的固件很少更新。然而在量子计算机的计算过程中, 固件天生就要不断被优化和更新, 从而重新配置设备, 用于下一步骤。

量子算法本身的设计中还存在着一个更大的差异。要利用量子叠加态固有的指数并行能力, 计算需要是可逆的, 类似于单指令多数据(SIMD)类技术, 并遵循一定的设计模式。侧栏《从经典角度看量子算法》对这些模式进行了讨论。

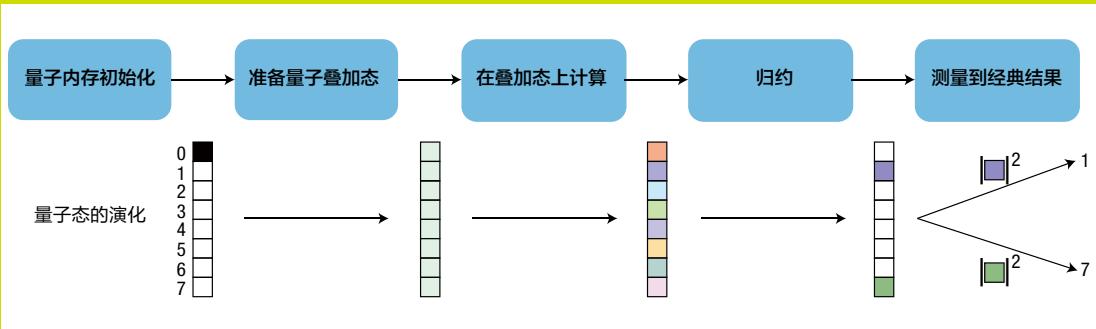
原生应用: 量子化学和材料科学

模拟量子模型可以被认为是量子

计算机的原生应用。什么能比本质上以量子力学方式运作的设备更好地理解一个量子力学系统呢?

小型量子计算机的第一个应用是简单的量子模型, 100个格点或者轨道模型的精确动力学模拟对于经典计算机来说就已经很困难了。这种模型系统的精确解可以用于开发和验证新的经典模拟方法, 然后可以反过来模拟比一个小型量子计算机所能处理的还要更加复杂的系统。

最近算法的进步已经大大提高了用于分子或复杂材料算法的规模。一个实际的例子是如何利用量子计算机来了解生物固氮, 了解这个过程可能会提高人造肥料的生产效率⁵。固氮酶的铁钼辅基(FeMoco)可以分解一个氮分



图A.很多量子算法的设计模式。从单一的经典初始状态开始，准备出许多输入状态的量子叠加态。然后，量子算法就在这个叠加态上执行。因为读取叠加态时，只会给出一个随机输入对应的结果，所以在这个叠加态随着测量过程坍缩到一个单一的经典结果之前，要对其实施一个集体归约操作。如果最终的波函数不集中在单个经典状态，则最终的测量结果将是概率的，由波函数中对应项系数的平方确定。图的下半部分表示大小为 $2N$ ($N = 3$ 量子比特) 的波函数，描绘了用单指令多数据 (SIMD) 类比量子并行。

- » **量子隧穿。**避免局部极小解是启发式优化算法的一个重要问题。如果障碍物又高又窄的话，量子系统可以在局部最小值之间“隧穿”，这比能攀爬隔在极小值之间的屏障的经典局部搜索算法要快。但是目前尚不清楚的是，这能否给有实用价值的优化难题带来更快的解决方案。
- » **量子模拟。**作为本身就分立的量子器件，量子计算机在结

构上就适合于模拟离散的量子系统，如在分子轨道中的电子。量子计算机可以用于计算电子基态和激发态。它们可以通过模拟干涉来测量这些状态的能量，也可以通过模拟实验测量过程来测量其他性能。

子，在常温常压环境下就能形成两个氨分子，而目前在工业生产过程中使用的Haber-Bosch工艺，是一种耗能多，需要高温高压的方法。

为了弄清FeMoco如何实现这一壮举，需要沿着备选的反应途径精确计算分子的各种构型的能量。虽然大多数的蛋白可用经典超级计算机的近似方法来模拟，但对FeMoco活性中心（含有铁和钼的原子）的精确计算经典计算机还无能为力，不过如果使用一台量子计算机作为协处理器，那就可行了。考虑到催化过程在化学工业中的相关性，量子计算机在这方面可以找到许多商业上的应用。

研究人员已经开发了类似的算法用于晶体材料，其中近似的经典方法可

以通过量子计算来增强，以理解和设计具有独特属性的新材料。其中可能包括高温超导体、性质可切换的新功能材料和无毒的染料。

量子加速的经典应用

利用量子叠加性和纠缠性质，量子力学的能力也可以被用于纯粹的经典计算问题。这里，基于侧栏文章《量子算法》中所述的量子算法，我们列举出一些可能的和潜在的应用。

加密

用于整数分解的Shor算法²是用量子计算机解决量子物理学领域之外计算难题的第一个范例，并促使人们对

这个当时只有少数人了解的计算方法产生了兴趣。整数分解在隐含子群这类问题(HSPs)中很广泛。不仅有破解RSA的多项式时间的量子算法，有能力破解Diffie-Hellman加密算法、数字签名算法(DSA)、Buchman-William算法和其他协议的量子算法，从而给许多常见的公钥加密方案带来威胁。

搜索

量子算法超越经典的另一个著名例子是Grover算法，可用于在无序集合中搜索某个项目的索引⁹。经典方法需要 $O(N)$ 次查询，但量子计算机仅仅需要 $O(\sqrt{N})$ 次就可以解决这个问题。在寻找最小(最优)值，确定图的连通度，以及模式匹配中都有应用。

从经典角度看量子算法

量子计算机相对于经典计算机的优点有时可以简单地说成量子计算机能够对所有可能的输入值同时进行计算。准确地说，许多量子算法都可以被看作“量子算法”栏中图A所示的实例。在很大程度上，这种量子程序可以被视为与映射归约(MapReduce)类似，不过它是在单个量子CPU里对所有可能的值进行作用。在制备出一个包含所有输入值的量子叠加态之后，对所有的值同时执行一个计算，然后在归约和读取操作时就可以得到概要信息了。

虽然量子程序在概念上类似于映射归约(MapReduce)，但在体现能力和量子计算限制的很多方面二者都存在着差异。量子计算机可对包含指数级多输入值的叠加态进行操作，这能被看作是SIMD处理器的一个极端形式。虽然量子计算机相比经典计算机有指数级的计算能力，但用SIMD进行类比也暴露除了它的一些问题：实施条件指令还需要使用屏蔽寄存器(称为控制量子比特)，if-else语句的两个分支都必须执行，在最坏的情况下任何循环都必须进行迭代。

由于量子门是幺正操作，根据定义它们应是可逆的。这需要量子计算机所执行的任何经典功能都要首先被转换为一个可逆的经典功能，这可能会导致存储器(附属寄存器)和运行时间的大量开支。

人们可能会天真地认为，下一步就是结果读取。不过，要记得每当读取一个N位量子比特的量子寄存器的时候，人们只能随机获得N个经典比特的信息，而且反过来，在所获得的叠加态中，人们也只能得到一个计算出的态(见“量子比特和量子门”边栏)。如果在计算时对一个输入的叠加值使用了一个经典函数，这就相当于给这个函数一个随机的输入，并读取所给出的结果，这将导致使用叠加态来计算的目的以失败告终。

想要利用量子并行，量子算法必须在某次测量读出量子寄存器之前对所有的量子比特执行全局归约函数。这种归约操作包括在Shor的周期查找算法中使用的量子傅里叶变换，或在Grover的搜索算法使用的振幅放大。发展目前还选择有限的这类操作，是设计新量子算法面临的一大挑战。

然而，单独考虑查询复杂度可能会产生误导。的确，对于简单的数据库查找，每个量子查询必须访问整个数据库，复杂度为O(N)，从而将整个成本提升到O(N^{3/2})，这超越经典的复杂度O(N)。因此，若一个给定索引处的值可以高效算出，使用Grover算法就是在盲目搜索¹⁰。

线性系统

类似的考虑也适用于线性系统算法¹¹。只要e^{-iAt}运算可以用量子门高效地实现，这个算法就允许从一个满足方程Ax = b的良态线性系统的解X中进行取样，并且相对经典算法具有指数加速能力。对于任意的N×N的矩阵，这需

要至少O(N²)次计算，这使得量子算法不具任何优势。因此在该算法的实际应用中，矩阵A需要可以通过算法来描述。这些问题包含了对偏微分方程的有限差分法求解和有限元离散化，其中我们可以确定例如指数密集网格的电磁散射等问题的解决方案。

采样

使用蒙特卡洛方法进行统计抽样在诸多应用领域，包括机器学习的广泛领域中都起着重要作用。量子计算机能为这些应用提供两种二次加速的可能方法。

为了加速采样，量子比特可以根据所需分布来制备到叠加态。从叠加

态中简单地读取采样量子比特时，随着采样数M的增加，采样均值的误差将以1/M的形式减少。通过使用Fourier 抽样定理的量子类比，量子计算机可以令误差以二次加速地减少，达到1/M。

当用于实现量子游走时(见侧栏《量子算法》)，在马尔可夫链的混合时间上，量子计算机也能获得二次加速。这可应用于随机优化方法，如模拟退火之类的优化难题，人们一直期待出现二次加速。

隐私

随着人们越来越关注隐私，量子器件对计算的最广泛的影响甚至可能不在于超越经典计算机的量子算法，而是

在秘密计算上。确实，盲量子计算允许用户在运行量子算法的时候，量子计算机操作员不能检测出计算的是什么。例如，一位医生可能想要计算患者得病的可能性，但或许不希望保险公司了解计算内容，因为这可能提高患者的保险费用。对于许多用户来说，可靠的隐私性和云计算的安全性可能会比量子加速计算更为重要。相反，在很多情况下，人们甚至可能愿意牺牲性能来换取更好的安全性。这最终可能成为量子计算机的最大应用之一。

软件架构

近来，量子算法的理论和实验之间出现了分歧，理论专注于算法改进的数学证明而实验专注于控制量子比特的寿命。迄今为止，量子计算主要是在数学和逻辑门操作的层面进行描述（见侧栏《量子比特和量子门》），而仅在小型量子设备或模拟器上对此进行了编译和手动优化。虽然已有一些量子编程语言和编译器，完整的软件架构仍然有待开发。随着硬件从只有单个量子比特的装置稳步走向有100个甚至更多量子比特的装置，计算机科学家、工程师以及开发人员都面临着设计并构建一个编程软件框架和控制一台可扩展容错量子计算机的挑战。

人们正在设计高级编程语言和优化编译器来为计算提供抽象层，以此创

建一个简单的、模块化的编程环境。在完全可扩展的硬件架构之前就进行软件开发，可实现软件组件的验证和分析以及在算法设计上的快速创新。这种想法可以追溯到Fortran（公式翻译程式语言）上，研究者就为了将用户从数学公式和机器代码转移到算法设计和规范上来才被发明这种语言。Fortran的简单语言允许更快速的编程和执行，提高编程速度500%，并减少了程序的长度。

量子计算需要一个类似的软件革命，因为它的算法和硬件都是复杂系统。为了充分利用和操纵量子态来获得算法优势，用于编程、优化和控制量子硬件的新颖结构是很有必要的。因量子比特的纠缠和不可克隆的性质，调试工具也需要革新方法。在这方面，模拟器和仿真器将对于量子算法和电路的设计以及测试至关重要。早期的设计决策可导致在端到端系统最终化的道路上节约可观的成本，并允许对系统关键部件进行验证、分析和重新设计。

图1展示了用于量子计算的软件堆栈。它可在软件和硬件系统之间提供明确定义的接口，并应能实现对任意大小任意目标架构的任意量子算法的编程。

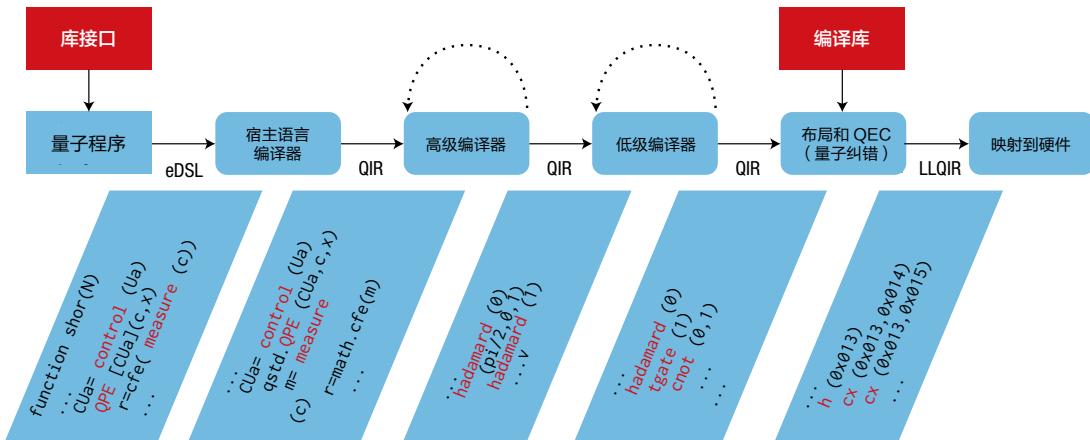
该图的顶部是一个高级语言，其中人们可以写量子程序。由于量子程序是由经典和量子指令均匀混合而成

的，这类语言应该是类似Quipper¹⁵或LIQUI|>16的嵌入式特定领域语言，它们能最大限度地利用经典的语言和编译功能。

为了确保灵活性和模块化，高级编译器应是硬件无关的，并能结合像条件指令和用户注解这类的量子元函数，实现一个非常高水平的量子代码优化。堆栈的低级编译器将允许特定的后端量子器件自动转换为硬件指令。

量子子程序，包括那些算术运算和复杂的量子子程序的标准库的发展，将加速新的量子程序的发展。这些量子库的自动调优能让待定的给定目标后端实现最佳表示，并且反过来还可使得在任何硬件上最终执行的量子算法节省大量成本。在函数库中建立高水平的量子应用程序将让开发者能够利用这些组件上的算法改进，就像经典应用程序那样。最近有几个在量子领域实现这种优化的例子，包括在量子化学系统的模拟中大幅度的降低复杂性以及在量子门合成上节约了几个数量级的成本。

栈底支持多种后端设备，包括模拟器、仿真器、资源分析仪，或者任何已提出的量子硬件等。而栈顶不知道硬件后端具体是什么系统，无论是离子阱、超导系统、量子点，还是拓扑量子计算机都一样，下层允许对特定器件设计的调优和控制优化，包括布局和时序安排。



eDSL (an embedded domain specific language) : 嵌入式特定领域语言
 QIR (quantum intermediate representations) : 量子中间表示
 LLQIR (low-level quantum intermediate representation) : 低级量子中间表示

图3. 人类自动图像标记器 (HAIL) 的并行图像分配模式。HAIL 利用广义指派问题的方法 (GAP) 实现了从数据库向计算机视觉主体、以系统设定步调以及自定步调的人类主体分配图片的优化。主体负责对所分配的图片进行分类, HAIL 则应用 Spectral Meta-Learner (SML), 在混合节点为每张图片分配一个总体置信度。基于已经得出的图片置信度及对主体分类准确性的推断, 系统将认定图片已被分类, 或将其送回图像分配节点进行进一步的分类。

展望

量子比特的实验方面的进展已经到了拥有可扩展的量子技术的水平, 在未来的几年中, 我们期望可以看到发展出超过100个物理量子比特的小型量子计算机。这将能创造出一些短于量子比特寿命的量子算法的早期应用, 并提供量子计算机在某些问题上超越经典计算机的第一个示范。

更重要的是, 这些量子计算机将加快用QEC建立逻辑量子比特并在工程上努力扩展出更大的鲁棒量子计算机的进程。量子软件的工作需匹配硬件的发展, 并包含从量子比特的低级控制到高级应用的整个堆栈。量子模拟和质因子分解的量子算法已经被优化一定程度了, 可以被看作是中小规模量子计算机的现实应用。对于其他应用, 包括线性系统、取样和机器学习, 我们仍然需要

优化算法和深入地估计所需资源。



管人们对量子算法的认识还远不如对其经典堂兄弟那样深入, 但人们一直在寻找哪些重要问题可以用量子计算机更快地得到解决, 而哪些又是不能的。回答这个问题已变得日益重要, 工业上也开始将努力重点放在即将到来的量子革命上。找到最终能实现可扩展性的量子硬件架构, 这需要当今的计算机科学、物理学家、数学家和工程师的共同努力, 一起克服在实现普适量子计算的道路上遇到的激动人心的挑战。■

致谢

感谢Doug Carmean, Thomas Häner 和Damian Steiger与我们的讨论, 也感谢Thomas Häner提供本文所用图片。

参考文献

- R. Feynman, "Simulating Physics with Computers," Int'l J. Theoretical Physics, vol. 21, nos. 6–7, 1982, pp. 467–488.
- P. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proc. 35th Ann. Symp. Foundations of Computer Science (FOCS 94), 1994, pp. 124–134.
- R. Van Meter and S.J. Devitt, "Systems for Local and Distributed Quantum Computation," Computer, vol. 49, no. 9, 2015, pp. 31–42.
- D. Augot et al., Initial Recommendations of Long-Term Secure Post-Quantum Systems, tech. report, Eindhoven Univ.

关于作者

克里斯塔·M·斯沃是位于华盛顿州雷德蒙德的微软研究院的高级研究员，也是量子架构和计算小组的负责人。她的研究兴趣包括量子计算机的应用及容错编程，还有应用于网络的机器学习方法。斯沃以最高荣誉获得哥伦比亚大学计算机科学专业的博士学位。她是ACM（美国计算机协会）的高级成员，而且是2010年的雅虎机器学习排名挑战赛冠军队的成员。联系方式为ksvore@microsoft.com。

of Technology, 2015; <https://pqcrypto.eu.org/docs/initial-recommendations.pdf>.

5. M. Reiher et al., “Elucidating Reaction Mechanisms on Quantum Computers,” 2016; <https://arxiv.org/abs/1605.03590>.

6. P. Wittek, *Quantum Machine Learning*, Academic Press, 2014.

7. J. Adcock et al., “Advances in Quantum Machine Learning,” 2015; <http://arxiv.org/abs/1512.02900>.

8. D. Lidar and T. Brun, *Quantum Error Correction*, Cambridge Univ. Press, 2013.

9. L.K. Grover, “A Fast Quantum Mechanical Algorithm for Database Search,” Proc. 28th Ann. ACM Symp. Theory of Computing (STOC 96), 1996, pp. 212–219.

10. G.F. Viamontes, I.L. Markov, and J.P. Hayes, “Is Quantum Search Practical?,” Computing in Science and Eng., vol. 7, no. 3, 2005, pp. 62–70.

11. A.W. Harrow, A. Hassidim, and S. Lloyd, “Quantum Algorithm for Linear Systems of Equations,” Physical Rev. Letters, vol. 103, no. 15, 2009; <http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.103.150502>.

特罗耶·马赛厄斯是苏黎世联邦理工学院计算物理系的教授，也是微软研究院量子架构和计算小组的顾问。他的研究兴趣包括量子材料的模拟、量子计算，以及生态系统建模仿真。马赛厄斯在苏黎世联邦理工学院获得物理学博士学位。他是美国物理学会会员，曾获Annesuhr Rahman计算物理奖，也是Aspen物理中心的受托人。联系方式为troyer@phys.ethz.ch。

/10.1103/PhysRevLett.103.150502.

333–342.

12. R.D. Somma et al., “Quantum Simulations of Classical Annealing Processes,” Phys. Rev. Letters, vol. 101, 2008; <http://arxiv.org/abs/0804.1571>.

16. D. Wecker and K.M. Svore, “LIQUi| : A Software Design Architecture and Domain-Specific Language for Quantum Computing,” 2014; <https://arxiv.org/abs/1402.4467>.

13. A. Broadbent, J. Fitzsimons, and E. Kashefi, “Universal Blind Quantum Computation,” 50th Ann. Symp. Foundations of Computer Science (FOCS 09), 2009, pp. 517–526.

14. T. Häner et al., “A Software Methodology for Compiling Quantum Programs,” 2016; <http://arxiv.org/abs/1604.01401>.

15. A.S. Green et al., “Quipper: A Scalable Quantum Programming Language,” ACM SIGPLAN Notices, vol. 48, no. 6, 2013, pp.

微信名：计算人

微信号：jisuanren



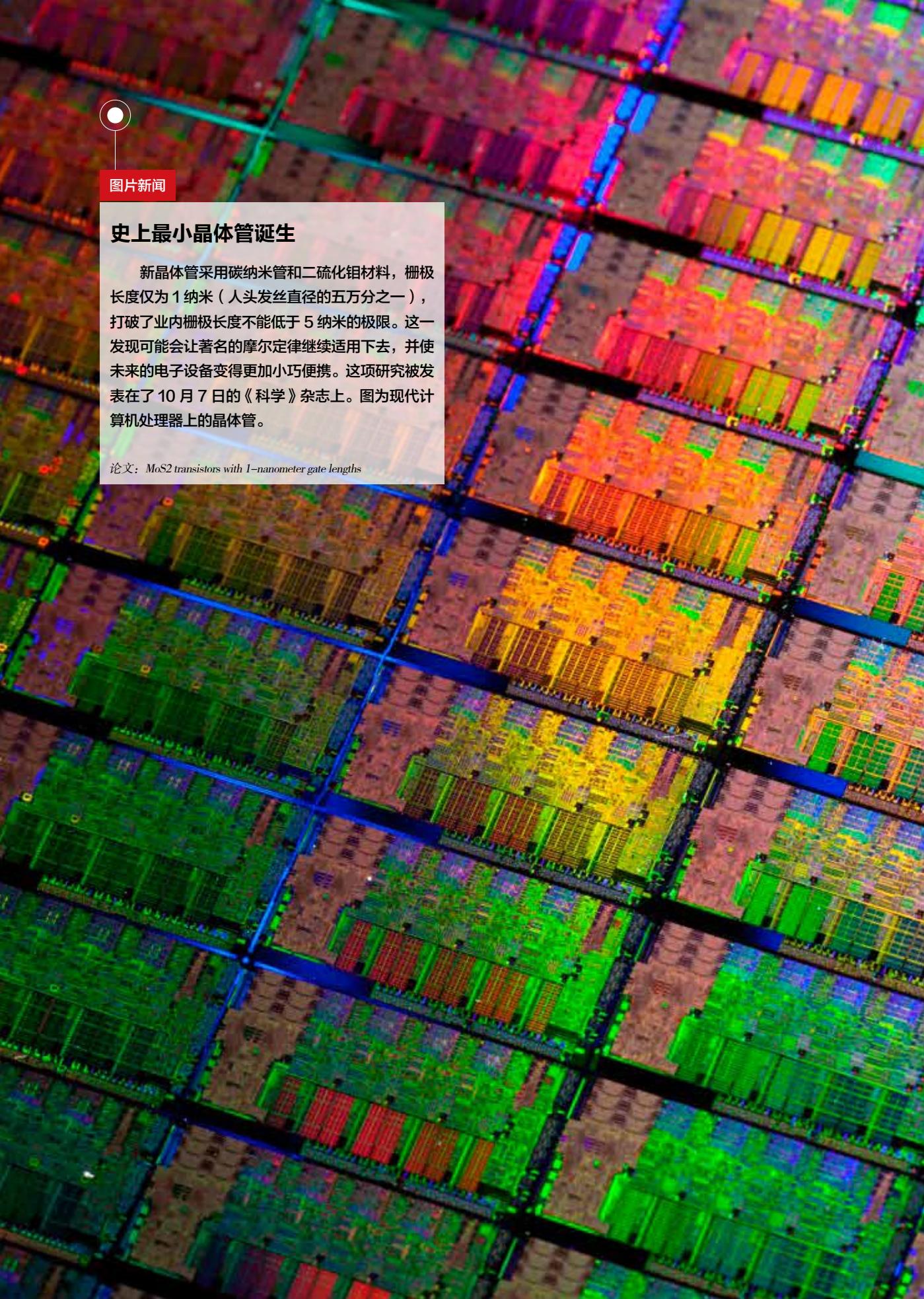


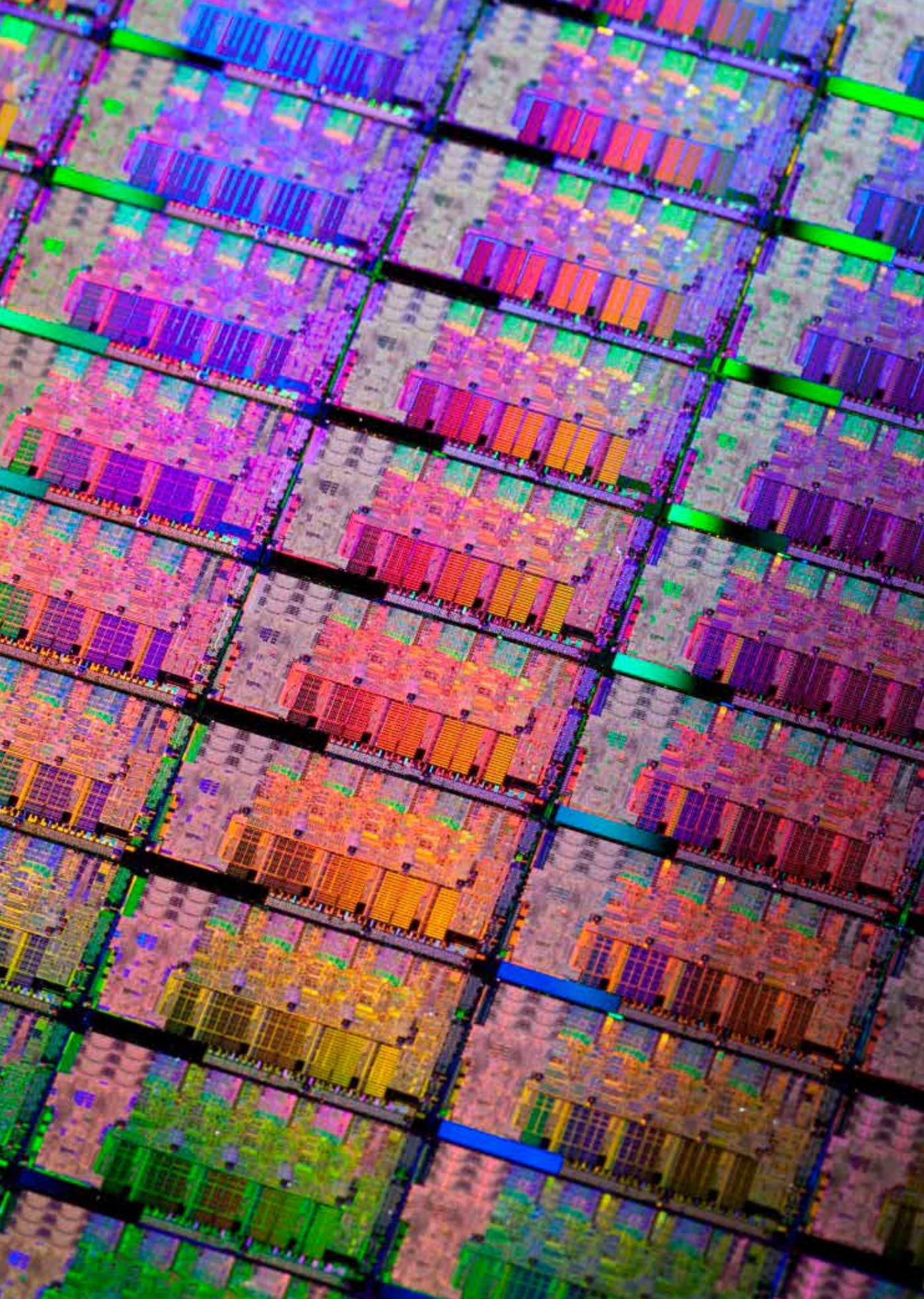
图片新闻

史上最小晶体管诞生

新晶体管采用碳纳米管和二硫化钼材料，栅极长度仅为1纳米（人头发丝直径的五万分之一），打破了业内栅极长度不能低于5纳米的极限。这一发现可能会让著名的摩尔定律继续适用下去，并使未来的电子设备变得更加小巧便携。这项研究被发表在了10月7日的《科学》杂志上。图为现代计算机处理器上的晶体管。

论文：*MoS₂ transistors with 1-nanometer gate lengths*







会议就在你的手中

IEEE计算机协会的会议发布服务（CPS）现在可以提供组织会议的移动应用了！让会议的日程、会议信息和论文列表在你的与会者手中的设备上显示。

会议的移动应用可在[安卓](#)设备、[iPhone](#)、[iPad](#)和[Kindle Fire](#)上运行。



欲知更多信息，请联系cps@computer.org





通往可扩展的 分布式量子计算之路

文 | 罗德尼·范米特 (Rodney Van Meter)，庆应义塾大学藤泽校区 (Keio University Shonan Fujisawa Campus)

西蒙·J·德维特 (Simon J. Devitt)，日本紧急物质科学中心 (RIKEN Center for Emergent Matter Science)

译 | 贺冉

研究者们正在制造的量子处理器，已强大到能够执行量子算法的小型实例了。可扩展性问题一直在激励着分布式存储的多机结构的发展，实验工作已证实一些构造模块可用于这种设计。为了实现局域和分布式量子计算，已涌现出来许多新系统。

量

子计算机和量子网络已经逐渐扩展到足以令经典的计算和通信能力震惊的水平了^{1,2}。就如侧栏《量子计算的关键概念》所述，量子计算有六个基本概念。每一个概念都很简单，但是它们放在一起的话，就显示出经典计算是不完备的，而量子效应可以用来高效地解决一些之前棘手的问题。

在上个世纪八九十年代，研究人员构造了几个量子算法，奠定了量子计算复杂度的基础，但是他们并没有完全理解构建新的量子算法的过程。自本世纪初以来，研究人员开始对这个过程有了更为深入的了解，这导致了在诸多领域中新构建的量子算法出现了爆发式增长(<http://math.nist.gov/quantum/zoo>)，从量子化学到天体物理，再到与机器学习相关的矩阵操

作等³。与经典算法相比，一些量子算法只能提供多项式加速；其他的算法能提供在渐进复杂度上的超多项式的加速。然而，在很多情况下，这些研究并没有考虑算法与量子计算机结构之间的相互作用，并以此来确定不变因子和保真度要求以及资源需求。简单地说，就是具有商业价值的量子计算机所需要的规模、速度和保真度等问题都有待解决。

各实验组正在制造的量子处理器，已强大到能够执行量子算法中的小实例，并且能演示延长量子数据寿命的量子纠错算法了，这增加了结构研究的紧迫性。尽管人们还在探索其他的一些方法，但主要的努力还是紧紧围绕在拓扑编码模型上，它被认为是在可行的微型结构上最为实用的量子纠错实施方案。可扩展性问题也一直在推动着具有分布式存储的多机结构的发

量子计算机的关键概念

很多量子现象都展现出一组离散的状态，比如原子能级，磁场中的电子自旋方向，或者光的水平和竖直偏振。每个量子比特，或者叫做 qubit，都具有两个分立的，正交的状态：0态和1态。

叠加态

在量子力学中，叠加态的行为有些类似经典的波。45度角偏振的光是水平和竖直偏振光的平衡叠加态。同样，也可以制备两个电子自旋或者两个原子能级的叠加态。最终得到某个确定结果的概率与叠加态中0态和1态的相对比例有关。

纠缠

当一个量子系统具有不止一个粒子或者量子比特的时候，想要分别描述各自的状态基本上是不可能的，因为这些量子比特可以被纠缠起来，此时各自的状态变得相互依赖。这种关联要比独立的经典概率关联要强，并构成了量子通信的基础。尽管在使用得当的时候，分开的很远的纠缠粒子会展现出经典理论解释不了的关联性，但是纠缠却不能被用于超光速通信。

振幅和相位

当量子系统增大的时候， n 个量子比特具有 2^n 个可能的状态，0...0到1...1，这与经典比特类似。这组量子比特就是寄存器。因为整体状态需要用所有可能状态的波幅和相位来描述，一个完备的经典状态描述需要 $O(2^n)$ 个寄存单元。量子算法设计者的工作

就是调节振幅的值，操控相位产生干涉，来改变叠加态：当相位相同的时候，相干相长，就会增加某个特定结果出现的概率。当相位不同的时候，相干相消，这就会减少该结果出现的概率。

可逆性

在一个基于线路的量子计算机中，算法设计者通过定义一系列的门操作来构建算法，这些门操作可以同时改变一个或者两个量子比特，大概类似于经典指令中或者 Boolean 体系中的逻辑门。但是与经典逻辑门不同的是，这些量子门必须要是可逆的，或者在数学上说，是幺正的。受控非门（CNOT）就是这样的一种通用构建模块。

测量

可逆性要求的一个主要例外就是测量，这涉及到从量子系统的寄存器中读取一个数值。读取的过程导致了叠加态塌缩到一个单态上。坍缩到哪个态是随机的，其概率取决于这些态的相对振幅，同时也要考虑相干的影响。测量会破坏纠缠。

退相干

量子态非常脆弱，必须要与环境很好的隔离。但是，时间一长，错误不可避免地会混进系统——这个过程叫做退相干。经典解决办法是给脆弱的数据保持冗余备份，但是量子力学的一个基本原则——不可克隆原理表明，对一个未知量子状态不可能复制一个独立的拷贝。

展，相关实验工作已经表明，一些构造模块可以实现这种设计变为。为了衡量可扩展量子计算机的进展，我们重点关注那些强调用量子网络来实现可扩展性的各种系统，研究它们的最新结果。

超越经典计算机

图1展示了量子计算机与经典信息

处理系统交互的基本原理。这个交互作用类似于从一个经典的外部程序查询一台经典的协同处理器。除了这个交互作用，在量子计算机内部还有第二个经典系统，用于控制这个交互作用与硬件本身。在研究者们开始探索量子计算机概念的时候，因在量子计算发展初期的工作而被广泛认可的戴维·迪文森佐（David DiVincenzo）提出，如果一个

技术可以被设计者用于建造基本的量子计算机，那么这个技术必须要满足五个标准：

- › 该技术必须具有一个可扩展的二级结构寄存器，用来充当量子比特（qubit）；
- › 该寄存器必须能够初始化到一个已知状态；

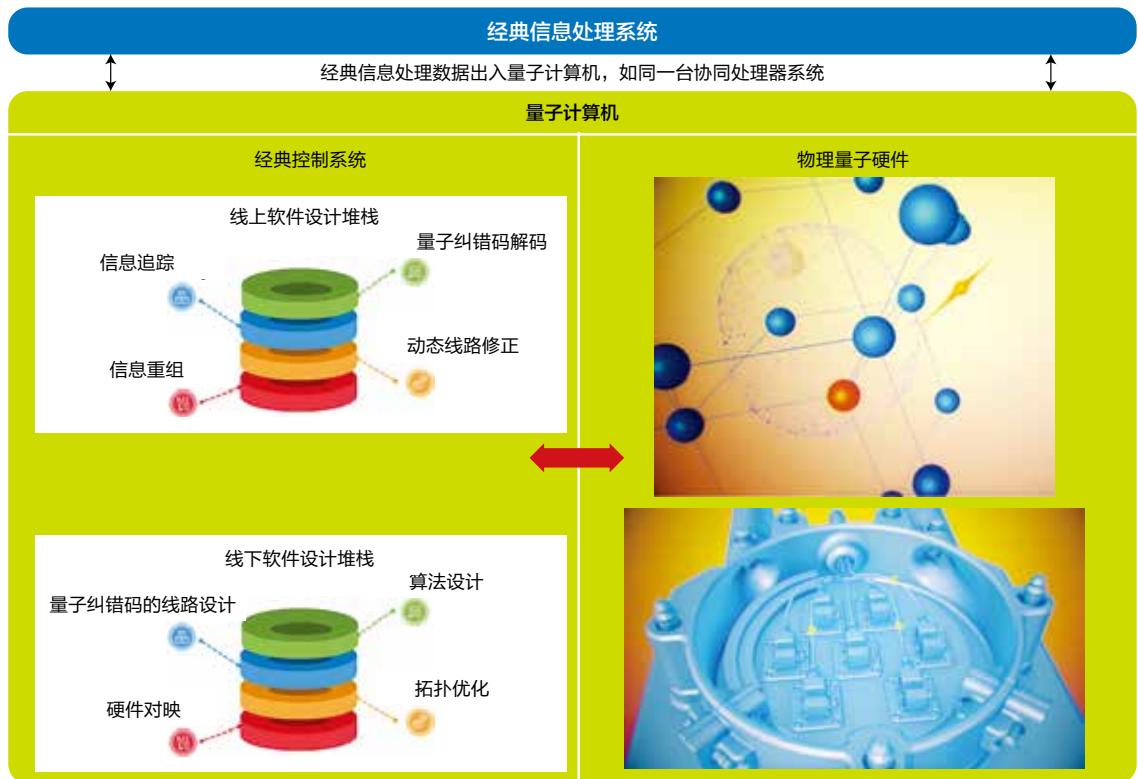


图 1. 量子计算机如何与经典信息处理系统交互。可以类比于经典的协同处理器的工作方式，一个量子计算机能够接受合适的外界查询和将问题规范化。除了这个交互作用，还要有一个完全分立的经典系统来控制量子硬件本身。QEC：量子纠错码

- › 该技术必须有一组普适门操作；
- › 寄存器中的量子比特和操作必须展现出足够的相干时间和保真度，用于长时间的量子计算；
- › 必须可以对数据进行单次测量。

关于这几个标准，有几个值得一提的要点。在第一个标准里，“可扩展性”隐藏了大量的工程复杂度。第三个标准意味着，能够实现所提出的任何算法的能力包含在量子计算机的基本框架内。第四条标准在量子计算机早期的标准中处于中心地位，而且导致了量子纠错码和容错性的发展。最后，第五条标准保证了数值数据可以被读取，这是一台实用计算机的必要功能。

迪文森佐随后增加了两个标准来保证可以利用光子互连来实现可扩展性，或者来建立可以将纠缠态投入使用量子网络：这个技术必须能够可以在固定量子比特和光子（飞行量子比特）之间的转换，也要能够捕获并控制光子路径。对于迪文森佐的标准，我们提议增加实用的工程上的限制：系统一定要足够小，足够便宜，还要足够可靠，足够快，才能够有用武之地。实施上的限制因素使得局域分布计算是必然趋势，这要求系统局域网络要快速，高保真度，并且要可扩展。通过将小的量子计算机紧密地耦合，构成大的多机系统，以便实现大规模纯数值的单体算法，这有助于分布式量子算法和传感的发展。在这

些应用中，分布式量子态的使用将提高科学设备的灵敏度和精确度，增加经典加密功能。

量子计算架构

如今，大规模量子计算的理论架构几乎完全依赖于拓扑量子纠错码模型。在近年来的架构设计中占统治地位的两类拓扑编码是在二维格子上运行的表面码，和在三维格子上运行的 Raussendorf 码⁴。每个系统使用的都是不同的物理技术来定义量子比特。纠错模型与量子硬件的物理限制之间的适应问题导致了设计上会采用多重架构。由于完整的系统的规模会很大，而

且量子比特也要比晶体管大上很多，所以整个系统的宏观结构最有可能会是多计算机的设计。

拓扑编码的优势

拓扑编码之所以这样命名，是因为它们的结构可以通过少数紧密联系的量子比特上的一组重复的算符来定义，同时其编码信息的特征是通过在整个二维（或者三维）阵列上的操作来定义的。这些编码之所以被广泛采用，有如下三个原因：

- › 对实验人员来说，存储寿命和门操作出错率仍是一个有待解决的问题，而根据所用的物理模型，表面码具有接近于百分之1的阈值；
- › 固有的最近邻结构保证了物理硬件不需要长程的相互作用；

操作逻辑量子比特的软件驱动编程模型使得运行时间资源配置适合于任意的应用算法，包括（在一定范围内）调整纠错强度。

拓扑编码一个已知的缺点是高的资源消耗，每个逻辑量子比特都需要使用很多物理量子比特。但是分析显示，只有物理错误率要比其他编码的操作阈值高的情况下，才会消耗大量资源。

拓扑编码模型允许架构在设计上

具有高度的模块化。用小的重复单元连通起来可以构成一个具有任意规模的计算机；我们把用于运行纠错的基本单元的架构称为微架构。这相对简单的硬件结构使得它能够更容易地被建造出来，所以现今最大的挑战就是设计量子比特元件，并使其具备能够让拓扑纠错有效的保真度。

拓扑编码模型

拓扑编码模型的几篇详细的综述介绍了纠错和逻辑计算的原理。尽管模型很复杂，但是基本硬件配置却十分简单。图2展示了这个模型的四个主要元素。

数据编码

正如图2a所示，二维表面码的一半量子比特作为数据量子比特，剩下的另一半作为校验子量子比特。图2b表示在整个表面码上平行地连续运行两个线路，读取校验子信息用于防御物理系统错误。计算是通过临时断开一些这样的线路，产生缺陷（孔）来实现的。如果在每一个绿色或者黄色方形上的线路都开启的话，那么整个量子态将会严格受限以至于不能在上面编码任何一个逻辑量子比特。将这些线路中的一个（或者一个连通的块）关闭时，将会在这个系统中引入一个自由度，可以用作一个逻辑量子比特。随着缺陷的大小和分离

程度线性增加，信息的逻辑错误率会指数地减少。因此， d 就是码距。在每一个循环里改变关闭哪些区域本质上是操控了被编码的缺陷，这使得编译的容错量子线路转变为计算机的物理控制信号。

管件

图2c表示一个管件。它将量子线路的几何结构和二维表面码和三维Raussendorf码中所需要的总的量子比特数目联系起来。我们使用一个负空间来形象地表示缺陷，其中缺陷用红色区域来表示，有效格子部分没有显示。对于表面码来说，该图的三个维度由图2a中格子的两个物理维度加上时间维度组成，时间方向为从图像的前面指向后面。

图2d表示由管件组成的几何结构。它规定了计算机的各区域必须要如何安排，才能够制定出量子态蒸馏程序。这个结构的三维物理体积决定了一个纠错程序必须要用多少时间和多少量子比特。一个大型程序，比如Shor质因数分解算法，可能需要重复这个结构几百万次。

早期的编码模型

在拓扑编码模型发展起来之前，大规模量子计算机的设计主要依赖于多层（串联）使用从经典理论推出的量子纠

错模型，至今仍有一些研究人员继续从事这种方法的研究。这些早期的编码在运行时更容易解码，而且，如果底层技术支持量子比特之间的长程相互作用，那么最主要的技术挑战就是在物理操作时需要让拓扑编码模型具有更高的保真度。

量子计算技术

自从2010年里程碑式的综述¹以来，以大规模量子计算为目标的实验研究已经在可扩展系统的方向上有了进展。图3展示了七个主要的技术的定性总结，这些技术得到学术和工业的重点关注。在正在发展的十几个技术中，我们选择重点突出前六个——不仅因为它们的实验进展，还因为相对于其他方案来说，它们在实现完整的、可扩展的结构上有更为具体的建议。我们将任意子也包含进来，因为它是正在发展的技术中唯一一个可能会将量子纠错码（QEC）淘汰的技术。

我们相信，这些技术是互补的，而且在一个新兴的技术领域中具有一个明确的位置。开发时间，成本，运行速度和物理体积都是衡量标准，在不同的系统中，这些标准将会相差几个数量级。而且，总的来说，这些具有更高性能的潜力的系统现在处于更为初级的发展阶段。

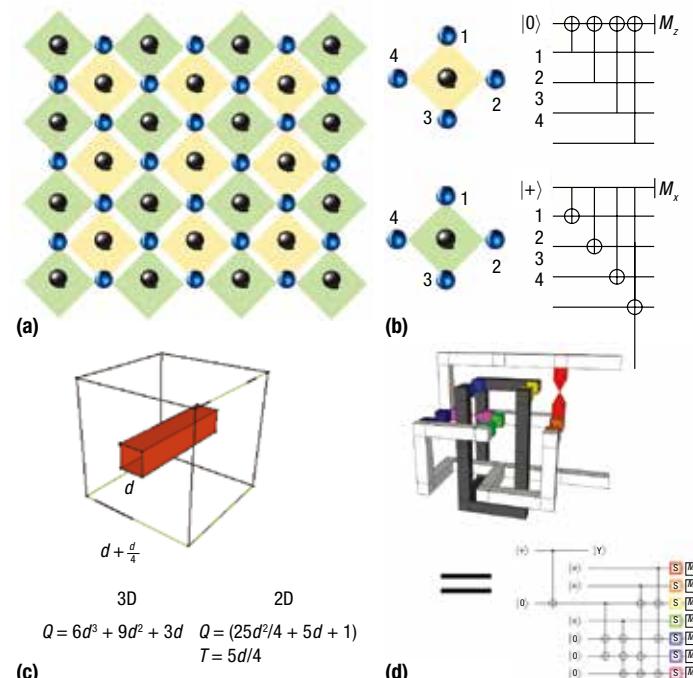


图2. 拓扑编码模型的原理。(a)二维结构，包含数据量子比特（蓝色）和用于提取纠错信息的校验量子比特（黑色）。(b)两个线路连续不断地在格子上运行，以此探测错误。利用两种方法中的一种（如图中黄色或者绿色方形所示），中心的黑色量子比特会积累围绕着它的四个蓝色量子比特的奇偶性。在线路图（右侧）中，从左到右为时间方向；竖直的符号代表所使用的量子操作（门），在每条时间轴上的，都以一个测量（要么是 M_x ，要么是 M_z ）结束，并用一个经典比特来表示奇偶性校验结果。(c)缺陷（红色）的负空间表示。缺陷是一个编码了信息的周长为 d 的方形区域（以带颜色的方块为单位）。管件的大小决定了在 Raussendorf 格子上实施一次编码所需要的量子比特的数目，或者表面码（底部的等式）所需要的量子比特数目 Q ，和时间步骤数目 T 。所获得的一个逻辑量子比特就是一个管件，它是拓扑量子线路的基础。

(d)由管件组成的几何结构。它规定了计算机的各区域要如何安排，才能够制定出量子态蒸馏程序（右下角）。时间从左向右。

离子阱

基于离子阱的量子计算是量子信息技术发展早期的一个成功范例⁵，因为研究人员本来是想要将之应用到原子钟上，才使得离子阱得以发展起来。精确控制的电场和激光让原子电离，并将离子束缚住，操作单个离子的状态，同时让它们保持在超高真空环境中。1995年研究者首次提出利用离子阱来进行量子计算，之后不久就在实验上演示了基本的门操作。

但是，在同一个阱中放入所有的量子比特来实现大规模量子计算是不切实际的，原因有如下几个，比如门操作

的时间会更长，量子门操作时会造成串扰，受限的操作并行度和增加的退相干速率。为了克服这些困难，研究人员想到了使用分段的离子阱⁵。在这个方法中，微型结构模型使用一系列的DC电极，可以顺着势阱的路线改变静电势，这实际上就可以拖着离子移动。单个离子可以被移动到储藏区，然后移动到相互作用区与多个离子之间实现门操作。这个分段的设计需要精细的控制才可以保证离子在具有复杂几何结构的势阱中移动时不会丢失。

可扩展化设计

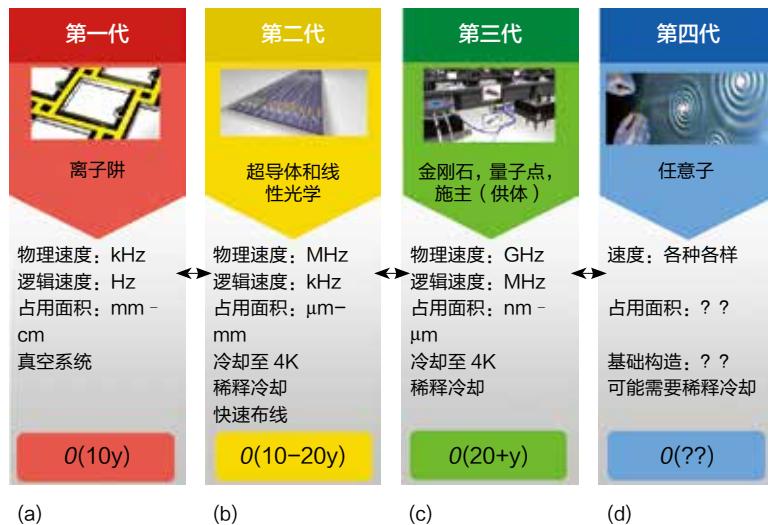


图 3. 一代代的量子计算机。这是对几个主流量子计算技术的定性评估——离子阱，超导体，线性光学，金刚石，量子点，施主（供体），和任意子。尽管每个技术都可以划分为一代，但在一两个指标上，具体的实现上可能会跨代。物理速度是指在制定拓扑编码所需要的物理操作的时候，所需要的最慢的门或者一组物理门的速度。逻辑速度是指在一组普通的门操作中，最慢的编码门操作速度。占用面积是指量子比特及其相应的控制系统和基础构造的预期大小。

基于分段阱来实现大系统的一个简单的办法是单体集成设计，先组装单个阱，在把它们对齐并相互连接，以此组成一个完整的计算机。这个设计的优势是表面码的物理操作可以尽可能地简单。缺点是整个计算机周围都需要有真空设备，还有包含高达330亿个量子比特的机器本身的巨大体积。

第二个方法是把计算机更进一步地分解为小的基本逻辑单元 (elementary logic units, ELUs)。其中ELUs可以是含有几十到几千个量子比特的分段阱。用概率光学连接可以把ELUs连接起来，这是通过光学手段激发两个远离的离子，并利用它们所发出的光子实现的。这个通信信道允许将独立的ELUs连接成一个更大的多计算机系统。

尽管这个方法缓解了可能会困扰单体型的离子阱计算机的基础构造问题，在离子之间建立纠缠的光子连接在

本质上说却是概率性的。考虑到对发出光子的捕捉，探测的效率低下，以及光开关中的损耗问题，想要在这个系统中得到一次成功的连接，必须要尝试很多次的纠缠。一开始的实验需要几十分钟才能够在离子间建立起纠缠，尽管现在已经提高到每秒钟成功五次。

总结

基于离子阱的系统正在迅速地发展，也许它会是第一个超越经典计算机的系统。但是，规模，速度和潜在的成本最终都将限制其可扩展性。

超导体

应用在离子阱系统中的原理都可以用到其他五个系统中，包括超导系统。在过去五年里，超导量子计算机取得了爆炸式的成功，并且是在量子领域首批的两个产业界的参与者，google和IBM首选的技术，它们都使用超导量子

比特和表面码技术来推进大规模系统的建设。

超导量子比特有几种类型，其中最成功的是使用在一个超导环中量子化的电流。超导量子比特可以被认为是超越离子阱的新一代系统，因为它固有的门操作时间为几百纳秒，而且一个量子比特的占地面积只有几百个平方微米 (μm^2)。该技术在实验中已经展示了单量子比特和双量子比特门的运行，并且在单个设备中，其初始化和测量的错误率小于容错计算的阈值。

可扩展化设计

现已有好几个大规模量子计算结构的方案。单片集成的方法已经展示了使用表面码来进行容错量子计算所必需的构建模块，但是一个主要的问题是，向二维最近邻量子比特阵列扩展的同时，还必须不影响单个量子比特的错误率。IBM公司演示了 2×2 的超导量子比特阵列，但是我们需要更大的阵列，而且如何制造和布置每一个量子比特所必需的控制线还是一个有待解决的工程问题。就像离子阱那样，分布式的设计可能会缓解大规模机器的基础设施和控制的问题，但是它们会引入更复杂的协议来实现基本门库。这个库对于实现表面码抑或其他用更慢，更容易出错的连接方式所需的纠错技术来说都是必须的。

总结

最近的飞速发展使得超导量子计算，而非离子阱，很可能将成为第一个在相关问题上超越经典计算机的数字量子计算机的基础。除了IBM和Google，诸如Rigetti和量子线路公司(Quantum circuits)这些刚成立的公司都专门把这个平台作为目标。

线性光学

线性光学是展示量子计算构建模块的第一个平台⁷。毫无疑问的，用线性光学做量子计算的理论基础是2001年Nature的一篇文章，它描述了通过测量引入非线性，因此实现普适量子计算的可能性⁸。

在演示了在体光学中进行线性光学量子计算的构建模块之后，人们又开始把开发的精力投入到集成光学之中，其中单个光子顺着在集成材料(硅表面)上面刻蚀出的波导传播。早期的工作极其成功，可以用高保真度的线路执行小的量子程序。最近的探索工作主要集中于将一个普适量子计算系统的各个方面都集成在芯片上，包括光子源，探测器和波导。

高保真度，高效率，按需产生的单光子源仍然是线性光学技术的阿喀琉斯之踵。一般有两种方法产生单光子源：使用基于原子的光子发射体来制备按需产生的光子，或者使用一个自发参

量下转换(SPDC)源和一个光学开关的组合来制备多路复用的光子源。使用多路复用的源将源的问题转移到构建极低损耗的单光子开关上面，这个是现在的研究重点。

可扩展化设计

线性光学的量子计算架构也发展出了两个一般的实现拓扑保护机的方法。第一个方法涉及到通过概率性地熔接越来越大的组件，来构建一个三维的Raussendorf网格。缺点是随着团簇的增长，需要对其进行光学存储，还要将计算机中相距较远的地方所成功制备的亚团通过簇路由链接到一起。这种结构花费较高，而且并不简单的路由问题需要非常低损耗的单光子开关。

第二个一般的方法是弹道模型，其中光子被发射到一个由熔接门构成的固定网络中，产生了一个不完备的图态(蜂窝奶酪)。这个模型依赖于加压熔接——使用纠缠来增加门的成功概率的技术——来获得比单个熔接门63%还要高的熔接概率。这个概率水平保证了所制备的网格能够渗透(制备出在所有的空间维度上边与边都互相连接的一条完整的连接)。弹道模型放松了对路由和存储的要求，但是增加了实时地将一个不完整的网格转化为一个完美的Raussendorf网格的计算消耗。

总结

线性光学量子计算机仍然具有巨大潜力，但是理论研究和实验结果都还尚显不足。相对来说，较少的基础设施投资是这项技术的一个重要卖点。

金刚石

长期以来，金刚石中的缺陷因有潜力应用于大规模量子计算和信息技术而备受关注⁹。氮空穴(NV)中心创建的电势可以捕获单个电子，因为它在量子技术中的潜在应用而成为迄今为止人们研究最深入的一类缺陷。人们对金刚石感兴趣在于它能够被用来将NV色心和一个处于光学频段的光子耦合起来，从而自然地将作为固定量子比特的量子寄存器，与在通信链路中作为飞行量子比特的光子相互连接起来。

可扩展化设计

研究者已经提出了两种基于金刚石的量子计算结构，利用单片晶体和分布式金刚石阵列。在第一种方法中，要在单晶内制造出大量的NV色心；在第二种方法里，要把金刚石阵列通过光学系统连接起来。与所有流行的量子计算架构一样，这两种方法都以表面码(二维)或Raussendorf模型(三维)的使用为基础。在2011年，一个NV中心的综综阵列被成功地耦合到一个超导磁通量子位上。在这个系统中，金刚石层被

设想为通过光学光子耦合超导量子位（其本身通过微波光子互相耦合）的一种方法。2015年，研究人员在第一次关闭了所有漏洞的纠缠演示实验中使用了基于金刚石的量子比特。

总结

虽然基于金刚石的量子计算机不如其他系统发展得成熟，还是有几个研究小组正专注于这项技术。人们的努力已确定了大规模计算所需的要素，但研究人员还没有展示出足够高的保真操作或在单个装置内的通用门组。但是，金刚石具有引人注目的优势。相对于离子阱和超导体，它的基础设施成本不高。真空也是不必要的，并只需要冷却到4开尔文，而不是毫开尔文的温度。较低的潜在基础设施成本和快速的运行时间使金刚石成为在第二代和第三代量子技术之间的理想桥梁⁹。

量子点

量子点能在不同的半导体材料之间的边界上束缚单个电子，并且可以用光、电或磁来控制。它们不像超导或离子阱那样在实验上有了巨大进展，在很大程度上是因为它们对噪声很敏感，但最近的工作正在努力克服这一障碍。量子点在更密集的集成和快速操作上都有潜力，但这种概念上的优势却明显需要更多的研发时间才可能体现出来。它

们除了量子计算之外还有很多其他用处，包括传感、通信和经典计算等。即便如此，全世界的研究小组都在朝着基于量子点的计算机而努力着。

可扩展化设计

从1998年原始的设备架构之后，基于量子点的可扩展化取得了十足的进步。一些量子点研究团队并不在学术领域，从而限制了他们公开信息，所以难以评估准确的进展。正如本文所述的各种技术那样，研究人员应该也是采用了一个基于表面码的大型量子点结构。

在量子点中对构造单元协议的实验演示也值得关注。有研究者已经展示了，控制保真度达到容错水平的可寻址量子点量子比特，连带着一个完整的双量子比特逻辑门。不像基于线性光学、离子阱和超导量子比特的系统，量子点中，可靠制造单个量子比特仍然是最重要的问题。材料的原子结构，包括惰性衬底的同位素，都会影响量子点中保持的量子态，特别是它的存储寿命。

已经有人提出了用于光控制量子点的大规模架构，但目前的趋势是朝向电控量子点努力，在这种系统中，芯片上的经典控制迹线使得在可扩展的布置中难以把量子点布置得更接近。

总结

世界范围内的多个研究小组，尤其

是在美国、澳大利亚和日本，正在完善基于量子点的量子比特的制造，并开始展示集成到大型的计算阵列所需要的控制和保真度。然而，想要拿出可扩展机器所需要的构件，这还需要进一步的实验研究。

施主(供体)

基于施主的量子计算系统使用半导体掺杂提供额外的，未成对的电子。在室温半导体的操作中，额外的电子能够穿过材料移动。但是在量子计算系统中，材料将会被冷却至毫开尔文温度，电子保持与其掺杂原子相结合。我们的目的就是使用这些单个的电子作为自旋量子比特，有时会与附近原子的核自旋结合起来使用。这些系统的一个例子是在硅中加入磷(Si:P)，针对这种系统的实验在过去五年中有了长足的进展。1998年原来的结构方案没有考虑到纠错或算法执行带来的问题。从那时起，研究者已经提出了好几代基于Si:P的量子计算架构。

可扩展化的设计

实际上，简单地使用磷供体生成的功能性量子比特会遇到重大问题，这是因为必须把磷供体原子级别精确的阵列嵌入原本是同位素纯的硅²⁸的晶体中。在晶体内，磷供体的实际位置可以是自顶向下或自底向上的。自上而下的

方法涉及到直接通过聚焦离子束注入磷。直接注入达不到原子级别的精确，这可能会显著损坏硅衬底，所以需要该材料经过退火处理来修复结构，而这又可能会导致供体移动。在自下而上的方法中，工程师一层层地生长硅衬底，在从上面生长硅层前，先以原子级别的精度放置每个磷供体。这种更为精确的方法是当今可扩展设计的首选。

2010年以来，Si:P技术已经从对小型磷供体簇的读取和寻址的能力发展到可以演示同位素纯硅中的单一供体的可预期长相干时间，高保真度读取和单量子比特的控制，以及使用单个磷供体的电子和核自旋来违背贝尔不等式。在传统硅工业中利用供体技术的原始动机依然很强劲。虽然其他的技术有可能会早些实现大规模的机器，基于供体的量子计算机仍是一个很有吸引力的选择，因为它们有更小更便宜的潜力。

任意子

在量子力学中，单个粒子的许多特性只能取特定的值：要么是整数（称为玻色子，如光子）或半整数（称作费米子，如电子）。值得注意的是，在某些情况下，某些材料是二分之一的倍数。第一类拓扑编码的原始描述表明这个数字量子纠错码机制和描述任意子的物理方程之间有一个直接对应。我们使用“任意子量子计算机”这个术语来区分

这个模型和前面已经描述的拓扑编码模型。

任意子量子计算已成为量子计算的一个非常复杂的模型，因此在一般的计算杂志上综述其进展。现在关于技术的理论基础和可能的实施手段也都已经有了出色的总结工作。在这里，我们

机各个部分接通和断开的一个功能，而纠错就是提取校验子信息并对其进行解码，以确定物理错误发生在哪里的一个连续的过程。一个大型量子计算机将需要大量的经典资源来操作（相对于可能使用量子计算机的任何经典系统来说）。这些资源可分为离线控制和在线

**超导量子计算机
可能会在相关量子问题上
首次超越传统计算机。**

把任意子量子计算分到第四代的原因有两个。第一，它试图使用该系统本身的基本物理性质来抑制错误。因此，一个任意子量子计算机并非在标准的两级量子系统（量子比特）上嵌入复杂的纠错码，而是能够展现出对退相干具有天然防御能力的量子激发。结果可能就是在工程系统内存在的任意子，不过还没有人将之可靠地展现出来。

软件控制

纠错计算的拓扑编码模型是基于软件的。软件控制的研究正成为量子技术发展的一个专门的分领域¹⁴。量子算法的制定就是按照上述算法控制计算

控制两种，其原理如图4和图5所示。

离线控制

离线控制是在计算机开启之前对容错量子线路的编译和优化。需要这些软件元件来将抽象算法翻译成与容错的纠错码相兼容的门序列，并将门列表转换成拓扑码中适当的控制结构。在离线编译的各个阶段，都必须对线路和拓扑结构的物理量子比特和计算时间进行优化，并且优化后的结构必须用所需的计算规范进行验证。

在线控制

在线控制是一组与量子计算机串联运行的经典软件包。它们主要处理动



图4. 离线设计堆栈。编译和优化拓扑量子线路需要多个步骤。



图5. 在线设计堆栈。与离线计算一样，大型量子计算机的在线处理也是很多层的。而不同于离线控制的是，这些要素必须跟量子计算机的物理时钟同步。还必须要附有经典在线处理，这样依赖于概率门的结构，比如线性光学，才可以寻址到被告知操作失败的门，并重整网格。

态误差解码和将编译线路映射到硬件上的物理控制和信号。在线控制软件需要在一个巨大的数据集上进行超快操作。其算法必须能够保持与量子硬件的物理时钟同步，而对于第三代计算机来说，这将处于GHz的范围。它们还要在可能包含数十亿量子比特的量子比特阵列上进行操作。因此，这些算法的尺度性能是一个严重的问题，需要进一步发展。

量子计算机不能没有这些程序包，而且若没有一个完全成熟的编译器和软件栈的话，也不可能恰当地对量子算法进行基准问题测试。虽然有一些人专注于对拓扑量子线路进行编译和基准问题测试，还有更多的人专注于更高级别的软件语言和线路编译器上，但相当多

的工作依然想要将功能性的拓扑线路优化到理论可达到的水平，并能够准确得出有用的量子算法所需要的量子比特数和计算时间。

网络和分布式应用程序

对于上述所有的7种技术，能够在一个芯片或设备上建立的量子比特的数目都存在技术限制，而这个数目远低于诸如Shor的分解算法所需量子比特的数量。在高容量可扩展系统的需求下，大部分从事大型系统研究的小组被迫采取一个包括多计算机系统的路线图，即通过某种形式的系统区域网络(SAN)将一组小型计算机连接起来。人们已经

提出了建立在离子阱、量子点或金刚石系统上特定的硬件平台，能提供良好的光学连接。想要让这些系统实用化，一个普通的单片计算必须被分裂成碎片式的分布式计算。

对量子多机系统的编程将需要使用量子隐形传态和纠缠。在远程数据编程方式下，数据可以在节点间传输，或者在远程门操作方式下，纠缠可以用来远程执行一个双量子比特门¹⁵。主要的限制就是要能够高效地使用节点间的纠缠，因为它是在每一个这样的过程中都要消耗的稀缺资源。

城市群和广域网也正在发展，这使分布式量子信息有三类应用：分布式数值计算，加密功能，以及传感器或控制类的服务。盲量子计算允许不可见的客

客户端-服务器计算，其中服务器无法确定输入的数据，使用的算法，或者输出的数据。加密功能包括密钥生成，拜占庭通讯协议和密钥共享。传感器的用途包括高精度干涉度量和时钟同步。

在过去的十年中，研究人员探索的多种QEC实现技术都已经达到了迪文森佐标准，包括达到了运用纠错除去的错误多于纠错本身引入的错误的阈值。与此同时，理论家们也分析出了多机结构和深入开发的拓扑纠错方法。这些概念与实验工作的结合才刚刚起步。

现在的问题是：要按需求建造一个足够大的量子计算系统到底有何限制？想要得到答案，需要理解什么是可扩展性。一个广泛的，非正式的定义是15：

首先，系统的扩大在物理上和经济上必须是可行的。物理资源的增加必须使系统的性能得到有价值的提升（性能上所有重要的指标，如计算速度或存储容量），而在负面特征上没有出现过度增加（例如，失败概率）。

这个定义意味着可扩展性在现实世界中从来都不是无限制的。成本超过十亿美元，或氦气或其他资源的需求量过大，根本无法获得的系统，在理论上

关于作者

罗德尼·范米特（Rodney Van Meter）是庆应义塾大学藤泽校区环境与信息研究副教授。他的研究领域包括存储系统、网络和后摩尔定律计算机架构。他在庆应义塾大学获计算机科学博士学位。他是 ACM 和 IEEE 会员，日本信息处理学会和美国科学促进会（AAAS）会员。联系方式：rdv@sfc.wide.ad.jp。

西蒙·J·德维特（Simon J. Devitt）是日本紧急物质科学中心高级研究员。他的研究领域包括量子计算机和通信系统大规模架构设计和拓扑量子计算软件的编译与优化。他在墨尔本大学获物理学博士学位。联系方式：simon.devitt@riken.jp。

虽然是可扩展的，但并没有实用意义。因此，追求最小经济可行的量子计算机正在进入一个新的阶段：它正从理论的可扩展性转向实际应用。在什么时候，*Science*或者*Nature*上能出现一篇新文章，描述的不是最新的量子计算机的设计，而是量子计算结果的话，那它就提供了证据，表明量子计算机已经不再是纯科学研究，而开始走向应用了。

虽然很多重要问题亟待解决，但如何建立一个量子计算机的基本问题，现在已经有了积极的答案。很显然，量子计算现在已经从理论研究转向工程，并有望重新定义现实世界的各种应用。■

致谢

这项工作受到日本学术振兴会（JSPS）通过KAKENHI（科学研究资金）Kiban B 16H02812的支持，日本学术振兴会资助具有挑战性的探索性研究。另外100多篇参考文献见本文初稿<http://arxiv.org/abs/1605.06951>。

参考文献

1. T.D. Ladd et al., “Quantum Computers,” *Nature*, vol. 464, 2010, pp. 45–53.
2. R. Van Meter, *Quantum Networking*, Wiley-ISTE, 2014.
3. A. Montanaro, “Quantum Algorithms: An Overview,” *npj Quantum Information*, vol. 2, 2016, article no. 15023.
4. A.G. Fowler et al., “Surface Codes: Towards Practical Large-Scale Quantum Computation,” *Physics Rev. A*, vol. 86, 2012, article no. 032324.
5. K.R. Brown, J. Kim, and C. Monroe, “Codesigning a Scalable Quantum Computer with Trapped Atomic Ions,” *arXiv preprint*, 2016; arXiv:1602.02840.
6. J.M. Martinis, “Qubit Metrology for Building a Fault-Tolerant

- Quantum Computer,” npj Quantum Information, vol. 1, 2015, article no. 15005.
7. D. Bonneau, J.W. Silverstone, and M.G. Thompson, “Silicon Photonics III: Systems and Applications,” Silicon Quantum Photonics, L. Pavesi and D.J. Lockwood, eds., Springer, 2016, pp. 41–82.
8. E. Knill, R. LaFlamme, and G.J. Milburn, “A Scheme for Efficient Quantum Computation with Linear Optics,” Nature, vol. 409, 2001, pp. 46–52.
9. A.D. Greentree, “Nanodiamonds in Fabry-Perot Cavities: A Route to Scalable Quantum Computing,” New J. Physics, vol. 18, no. 2, 2016, article no. 021002.
10. F.A. Zwanenburg et al., “Silicon Quantum Electronics,” Modern Physics Rev., vol. 85, 2013, pp. 961–1019.
11. C.D. Hill et al., “A Surface Code Quantum Computer in Silicon,” Science Advances, vol. 1, no. 9, 2015, article no. e1500707.
12. B.E. Kane, “A Silicon-Based Nuclear Spin Quantum Computer,” Nature, vol. 393, 1998, pp. 133–137.
13. S. Das Sarma, M. Freedman, and C. Nayak, “Majorana Zero Modes and Topological Quantum Computation,” npj Quantum Information, vol. 1, 2015, article no. 15001.
14. S.J. Devitt, “Classical Control of Large-Scale Quantum Computers,” Reversible Computation, LCNS, vol. 8507, Springer, 2014, pp. 26–39.
15. R.D. Van Meter III, “Architecture of a Quantum Multicomputer Optimized for Shor’s Factoring Algorithm,” PhD dissertation, Dept. of Computer Science, Keio Univ., 2006; <http://arxiv.org/abs/quant-ph/0607065>.





实体分子计算： 机遇与挑战

文 | 维多利亚·科尔曼 (Victoria Coleman)，波托马克政策研究所 (Potomac Institute for Policy Studies)

译 | 徐付琪

分子计算是一种颠覆性的计算方式，利用了物理、化学、生物系统的信息处理方法。随着对计算范式和计算机器要求的提高，美国国防部高级研究计划局 (DARPA) 开始深入研究分子计算。

1968 年，DARPA 成立了国防科学研究理事会 (DSRC)。理事会募集了全国顶尖的科学家。DSRC四处寻找有潜力的项目，邀请各地的专家进行长达一年的研究。通常研究包括两到三个研讨会。研讨结论在DSRC的年会上汇报给DARPA。在2015年DSRC解散之前，它在DARPA面向未来的研究中起到重要作用。

传统计算方法中存在瓶颈，有些问题不能通过调整节点大小、运行速度、核心处理器个数、存储空间大小等方式解决。2010年，DSRC开始试图解决这些“不可能”解决的问题。研究小组试图用非传统计算方式，如气候模式更好、更快、更低成本地解决这些问题。在这个过程中，我们发现，实体计算利用运算结构的物理性质，可以简明高效地解决大规模并行搜索等重要问题。已经有越来越多的成果证明了这一点。更有趣的是，我们意识到非传统计算大大拓宽了计算可以

解决的问题的范围。例如可以用有限个电脑程序构造，计算出病毒的复制或者药物抑制病毒复制的模型。这就是分子实体计算。它不仅可以解决传统计算无法解决的问题，同时可能解决目前传统计算机面临的基础问题比如信息密度、平行性、能源利用效率等，为传统计算方式带来重要变革。

方法

2008年春天，DSRC在参观科罗拉多州博尔德国家大气研究中心后受到启发，展开了一系列研讨会。在国家大气研究中心，科学家们努力搭建更好的预测模型，在占地几亩巨大的高性能计算机上，使用纳维叶-斯托克斯方程计算，这些方程已经几代时间没有变化。这些使用传统数值模型，用传统的计算软件硬件计算的结果，在效率和准确性上都不尽人意。

直觉告诉我们，重新思考计算的基础模型和过程可以更

好、更快、成本更低地解决这些困难的计算问题。因此我们召开了一系列会议探索这个问题，并接触了许多各个领域的杰出研究人员和科学家，包括逻辑哲学家、理论计算机科学家、复杂论理论家、数学家、物理学家、生物学家和计算机工程师。

我们讨论的方法涵盖了“超计算”（超级图灵机）、量子和细胞计算、神经、分子和化学计算等。尽管“超计算”的讨论很有趣，（我们聊到大批拥有自我复制能力的机器人以近乎光速冲向黑洞，解决了哥德巴赫猜想等与无限有关的问题）是原创的计算方面理论，我们最终把焦点集中在一种尤其吸引人的（而且很有实用潜力的）实体计算形式----分子计算上。我们认为目前系统生物学的研究，结合计算机科学的试验和理论，使这项艺术呼之欲出。

分子计算是体现在生物系统内，并在生物系统内（如DNA分子）进行的计算。DNA和可计算性中存在有趣的相似，提供了将生物过程用于计算的可能性，以及把生物过程理解为计算的思路。如果这种说法成立，它将影响深远。

实体计算原理

在定义实体分子计算时注意，使用DNA及其他有机材料作为运算结构，与将这些结构刻在现有的硅计算结构

上是不一样的。自1975年开始，阿里耶·艾维瑞姆（Arieh Aviram）在对后一种方式的研究上处于领先地位，他当时提出用单个有机分子代替硅晶体管。在随后的40年里，类似的方法不断进步，这些进步的最终目的都是要用单个有机分子晶体管取代硅计算的基本单位——晶体管。这一系列研究的最新成果忆阻器于2008年问世，惠普实验室仍积极开发这种工具。通过凯文·凯利（Kevin Kelly）和塞勒斯·穆迪（Cyrus Mody）的研究，我们可以追溯取代硅晶体管的研究过程。这种实验的思路是构建一种计算元件，从一个分子开始逐渐添加更多分子，逐渐形成一个更为复杂精确的结构。而非像现在制造硅晶体管一样，直接在一大块材料上进行雕刻。我们的出发点不同，我们希望探索发掘DNA和其他生物大分子的物理和生化性质，使计算“自发”进行，而非区别于人工一次制作一个晶体管。换句话说，我们关注点是实体分子计算。

布鲁斯·麦克伦南（Bruce MacLennan）表示实体分子计算有以下特征：

- › 直接用物理过程进行计算。
- › 信息和程序暗含在系统和其他环境的物理和其他性质中。
- › 通过物理过程的生长，组装，发展，变换，重构和拆解影响实体计算。

在这种方法中，物理基底允许多种运算“自发”进行。实体计算是通过和其他物理过程相互作用进行的一种物理或者生物过程。它的一个模型是扩散，扩散在很多液体中都可以自动发生，被用于广播信息、大规模并行搜索等计算任务。两种任务在硅芯片上运行时都需要大量的计算，但是换到液体体系中就可以自发进行。实体计算的另一个例子是拉杰什·吉甘纳巴迪（Rajesh Ganapathy）及其团队的工作，他们演示了如何用胶状晶体精确模拟晶体向外生长。

艾维瑞姆的工作和他的继承者的麦克伦南和吉甘纳巴迪的工作有很大不同，差异程度甚至与数字计算和模拟计算的差异相当。在讨论物理实体在非传统计算的巨大挑战中所起的作用时，苏珊·斯蒂芬尼（Susan Stepney）和她的同事写道：

计算过程是物理的。我们需要把计算植入一台设备。这个设备按照物理法则运行，不能被一个封闭数学模型模拟。当我们一步步扩大物理规律的边界，实体计算的这种性质就越来越明显。

然而实体计算，这种非经典的计算方法和数学模型，需要系统的可预测的利用被微妙的平衡。我将在下文中讨

论这种平衡，先从计算的最基本的概念——图灵机开始。

图灵机和分子计算

1936年，阿兰·图灵开始深入研究计算的概念。这一纯理论工作在计算机真正出现10多年前就已经开始，并引领了20世纪的多项数学成就。图灵发明的计算机即图灵机，最初是解决数学问题的概念性工具，而后来被普遍应用于各个领域。它可以用来自计算任何可计算的事物。换句话说，如果一个问题不能用图灵机编程解决，那它就不可能被我们可能建造的任何机器解决。不论这个机器多复杂、性能多强大。图灵机是现代计算的核心概念。如图1所示的，它是一台由一条无限长的纸带，一个读写头，控制规则和状态寄存器组成的简单计算设备。（需要注意的是图灵机并非用来进行实际解决问题，必须通过有限的图灵机，即有限的纸带来解决问题。）

现在让我们梳理分子计算和图灵机的相似点。分子计算是一类实体计算。很多研究人员已经通过DNA替换或者酶门搭建基础的计算元件、逻辑门和环路。尽管这看起来很有趣，但关键在于这些思路可否用来解决实际问题，还是说他们仅仅是人们好奇心的产物。从计算的角度考虑，我们要问

的第一个问题是，分子计算是否是一个完整的图灵机。换句话说，分子计算机是否可以完成所有图灵机可以实现的工作。假设可以，那么第二个问题就是如何确定正确的计算初值。他们是逻辑门、1和0、还是其他完全不同的事物？由简单的DNA门搭建的简单分子计算回路可以解决一些模型问题，如井字棋游戏（见图2）。但是真正的问题是我们是否可以建造一个通用的分子图灵机。如果这种机器可能实现，我们要怎样实现呢？1994年，伦恩·阿德尔曼（Len Adleman）建造了DNA计算机是解决这些问题的重要尝试。

DNA 的实体计算

阿德尔曼的先驱性工作不仅精妙地解决了不确定性多项式哈密顿路径问题（在不定项图中，确定是否存在连接指定起点和终点，途中经过所有其他节点且只经过一次的路径是否存在），同时提供了DNA实体计算的关键思路。阿德尔曼运用图论中一个有若干个顶点的图的简单算法解决了这一问题：

1. 通过图生成一系列随机路径
2. 对于集合中的每种路径：
 - a. 检查这条路径的起点和终点是否与题设一致；不是的话排除。
 - b. 检查这条路径是否刚好通过n个

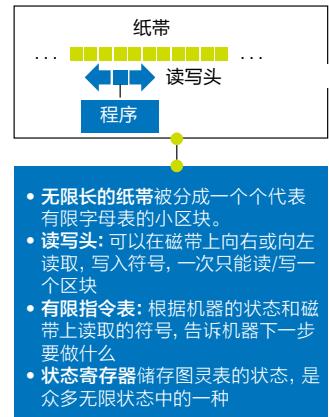


图1. 图灵机。

顶点；如果不是排除。

- c. 对于每种路径，检查是否这条路通过这个点；如果不是排除。
3. 如果排除后集合非空，汇报路径存在；如果是空集，路径不存在。

DNA用4种遗传字母编码信息

(A腺嘌呤, T胸腺嘧啶, G鸟嘌呤, C胞嘧啶)，而非传统计算机的二元字母表(1,0)。(www.britannica.com/technology/DNA-computing)。阿德尔曼用随机的一段DNA序列表示每个城市，用前半段表示每段路径的起点城市，后半段表示每段路径的重点城市，两段连接表示路径。随后分析了DNA城市的名称和路线数目，交给其他实验室合成DNA序列。收到序列后，向每个试管中加入少量DNA(约1014个分子)，加入水，连接酶和盐，反应1秒。

用多聚酶链式反应(PCR)来筛选起点和终点错误的序列(步骤2a)

用凝胶电泳删除长度不正确的DNA链。(步骤2b)

最终通过亲和分离剔出未经过所

(原理证明)
用DNA玩井字棋

尽管在简化编程方面存在局限，第一代自动机玛雅一号通过玩成井字棋游戏证明了DNA逻辑门的潜力。玛雅先开局，选择了中间方格（），而人类玩家第一步一定是选择左上角（方格1）或左侧的方格（方格4）。

尽管在简化编程方面存在局限，第一代自动机玛雅一号通过玩成井字棋游戏证明了DNA逻辑门的潜力。玛雅先开局，选择了中间方格（），而人类玩家第一步一定是选择左上角（方格1）或左侧的方格（方格4）。

人类“哈利”向九个井中加入了镁离子以启动玛雅。在5号井中酶切割底物，发出荧光，表明玛雅开始工作（ λ ）。

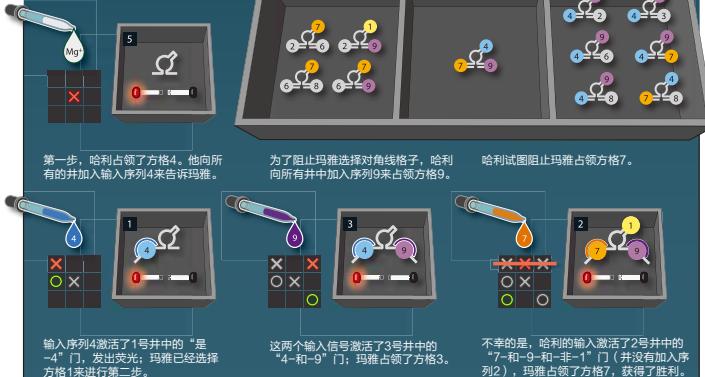


图 2. DNA 计算机玛雅一号。

有城市的路径。(步骤2c)

剩下的就是我们寻找的解。(步骤3)

这种结果令人激动。更重要的是，阿德尔曼观察到这种计算和普通计算有明显的相关性。给出一个DNA链，DNA聚合酶(一种负责从由脱氧核糖核苷酸合成DNA链的酶)，产生了对应的互补链(其中互补的碱基为C→G, G→C, A→T, 和T→A)。聚合酶附着在DNA链上并随复制在DNA链上滑动。这和图灵机的读写头相似，读写头沿着磁带移动读入数据，同时沿着输出磁带滑动写入数据。DNA聚合酶和图灵机有限控制元件之间有明显的相似性。

不幸的是，正如阿德尔曼观察到的，尽管DNA聚合酶可以按照碱基互

补配对法则进行匹配，自然界中不可

能进化出可以执行比如因式分解分解等等功能的酶。我们现在已经快速廉价的合成定制分子，因此我们的问题变成了：我们是否可以设计一个酶或者其他生物过程用来解决这些问题。换句话说我们可否用酶而非一系列0和1来解决这些问题。安德鲁·菲利普(Andrew Phillips)和鲁卡·卡尔代利(Luca Cardelli)提出了一种有力的解决方案：通过编程语言来设计和模拟DNA环路。在这套环路里，链的替代是最基本的算法。这种语言可以被核苷酸序列编译，模拟不同的环路，最近，亚力克·尼尔森(Alec Nielsen)和他的同

事提出了一种基于verilog的编程语言Cello。用真值表描述的环路，把它编译

成为质粒DNA序列，从基因层面上完成预期逻辑功能。DNA序列被注入活细胞，环路开始工作。这是DNA计算新方式的重要一步。

阿德尔曼简单有效的DNA计算工具箱告诉我们，尽管由一系列晶体管构成的逻辑门是硅基计算的雏形，它可能不适合被用于DNA底物。聚合酶在引物后边根据模板合成DNA链(复制)，连接酶负责把DNA链连接在一起(连接)，核酸酶切断核酸链(分割)。凝胶电泳负责依据长度分离DNA链(分离)。如果底物已经为我们提供了这一功能，为什么我们还要重新设计实现一种新筛选算法？

在他系统生物学机器方面影响深远的工作中，卡尔代利提供了分子计算工具盒更深刻的见解。他展示了四种大分子怎样整洁的组装成为一种通用的数据结构，为形成其他生化工具箱提供可能。

- RNA和单链数据相似，DNA和双链数据相似。
- 作为记录或者对象的蛋白质活跃并稳定。
- 脂质对应不同界面的容器(参数不同的模块)。
- 糖对应树。

实体计算的挑战机遇在于如何

利用自然计算材料，颠覆我们现在 的计算材料。用赫里斯多夫·托伊舍 (Christof Teuscher) 和皮特·迪特里希 (Peter Dittrich) 的话来说，颠覆而非遵照传统介质。在这种情况下，利用 DNA本身提供的计算元件，而不是制造简单的逻辑门等硅基计算元件，无疑是人类已知的最复杂的信息量最丰富的材料。

如何重复阿德尔曼在解决哈密尔顿途径的成功，把DNA分子用凝胶计算器，实用的、系统的、可预测的、可依赖的方式，同时尊重介质本身性质进行处理，是目前在分子计算的理论和实验中最有趣的问题。阿德尔曼的计算器很迷人，但是我们可以搭建一个模型，分析它计算的复杂程度，边界和收敛性吗？卡尔代利的工作使我们从抽象系统生物学机器的角度思考这个问题。

系统生物的抽象机器

虽然这种计算不断地接近基础的构造很有用，但是并不能解决我们对分析实体计算性质的要求。最近几年，系统生物学加深了我们对生物的理解。研究细胞如何工作不仅需要理解生物系统的结构，同时还有它所依赖和参与的生物过程。其中很重要的是，从信息处理的角度以而非化学角度理解细胞功能。卡尔代利展示了如何用抽象的机器

代表生物大分子类群。每个机器由离散的状态组成，存储了不同状态之间的不连续状态转换的批量指令。我们观察到很重要一点：理解复杂机器间的相互作用就是理解细胞是怎样工作的。程序起到了联系硬件的作用，允许用可预料的，高度限制性的操作进行治疗。这些相互作用可以被理解成为一种抽象计算的结果，这意味着，研发阻断病毒复制的药物和写程序相似。

卡尔代利的模型有三个基本的原件：

1. 基因机器负责处理细胞内信息处理工作，调节其他活动，包括组装，其他机器的维护和自身的复制。
2. 蛋白质负责处理所有的力学和代谢方面的工作和信号传导。
3. 细胞膜隔出不同的生化环境，通过复杂的多步反应动态操纵底物的运输。

理解细胞工作的实质上是理解这些机器是怎样在不同的时间和尺度上相互作用。

机器都自己的操纵指令。拿蛋白质机器作为描述基因和膜机器指令来讲，卡尔代利是这样描述他的工作的（图4）。

每个蛋白都以一系列位点和开关

进行控制。这些开关和位点在特定时间 内有“开”或“关”的状态。两个蛋白质可以在合适的位点结合成为更大的分子。复合物上的位点和开关决定了复合物的状态，系统的状态是这些特定状态独立复合物的集合。蛋白质机器有两种操作：复合物上的开关可以开启或者闭合，使蛋白质处在一个新的状态，在新状态中产生了一系列新开关和位点；两个蛋白质的复合物可以在合适的位点组装，或一分为二，每个新状态里都有一系列的新开关和新的调控位点。

蛋白质在细胞中如何找到它的结合对象呢？这计算起来很困难，但是细胞可以轻松解决。我们如何掌握蛋白质系统的指令呢？开关和结合受其它蛋白质调控。细胞内有数以万计的蛋白质，因此蛋白质的机器有上万个初始指令。每个蛋白都有和其他蛋白质作用的特殊方式。对于每个细胞层面的被模拟的亚系统，我们需要列出参与的所有蛋白，同时在开关和结合中与它相互作用的蛋白。

这三种机器频繁相互作用，却又高度独立。基因指导了蛋白质和膜的合成，并且引导蛋白质嵌入细胞膜。一些蛋白质作为基因之间的“信使”，另一些膜蛋白承担了不同的门控和信号传导工作。表面含有蛋白质的细胞膜限制了细胞的物质进出。

这些过程的执行可以模拟为每个

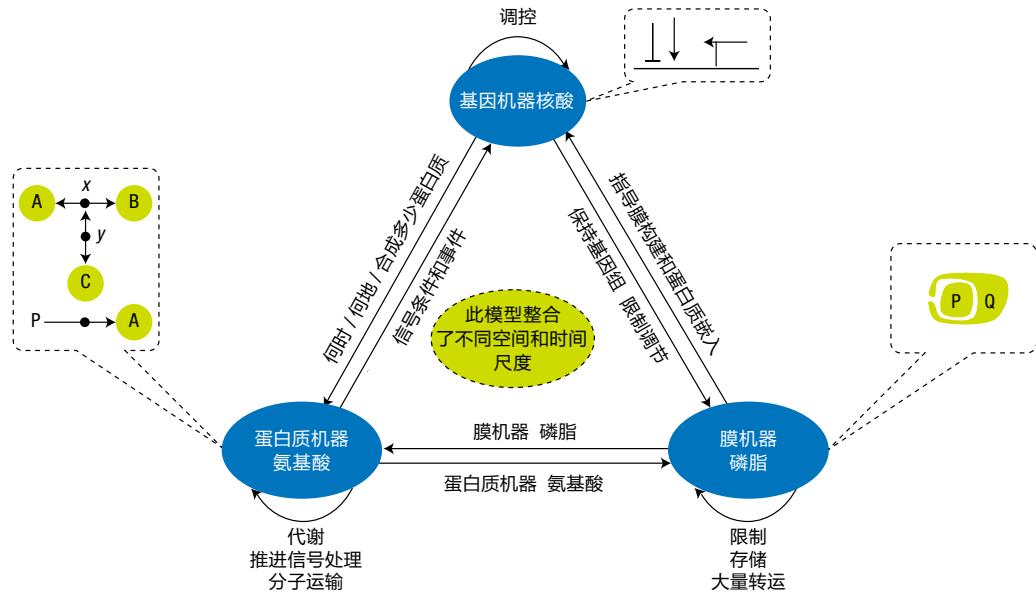


图 3. 卡尔代利的生物学机器抽象。

机器的指令程序来起作用。同时机器之间的相互作用在模型中相互独立，同时发生。在经典的计算中，尤其是在平行或同时计算中，理解这些相互作用的复杂性，促使了很多专有模型的出现，包括代数问题的解决。解决代数问题是一系列过程中高层次的相互作用、交流、同步。代数的公式定理来规范自发的有条理的，在相等或者其他关系和过程中的相互作用的，逻辑推论。代数处理中最著名的例子要数 π 值的计算，通过随机的语义和周围计算把 π 值限制在不同的区间，同时Brane的计算方法根植于生物中的不变量（矢量？）这些代数可以巧妙用于对基因，蛋白质和膜机器的分析和建模。这产生了一个强有力的理念框架，通过拓展，分子计算的语义执行，利用阿尔德曼的凝胶计算机可以理解和限制框架。这用来预测计算性质的模型铺

平了道路，可以系统的评价机器形式，讨论它的正确性等等。

如果生物是计算的话，那么生物过程就是程序。

卡尔代利的机器允许我们从信息处理的角度，而非生化的角度理解细胞的功能。换句话说，它允许我们寻找生物的算法。事实上它使我们进一步探究、设计生物算法。卡尔代利用semliki森林病毒复制做了精妙的解释。图5中病毒用基因，蛋白质，和膜的不同指令完成复制过程。

卡尔代利用Brane微积分模拟了病毒感染，复制和传播的每个阶段。这个理论模型有夯实的数学分析和预测基础，意味着我们不仅可以预测并且可以评价预测。如果我们反过来用分子

编程语言来解释这一模型的话，我们就可以同样写出病毒复制的代码，模拟它的算法和行为，这可能是用符号计算描述病毒复制的方法。

这种关联十分基础。阻止复制的药物仅仅是一个程序，治疗和药物开发从完全的实验科学变成用符号表示的科学。实体分子计算的方法不仅可以帮助我们解决阿尔德曼的哈密尔顿途径问题，也可以帮助我们通过符号化的计算解决生物化学问题。我之所以强调符号化是因为对病毒物理行为的准确模拟是高度复杂，绝大部分情况下不可操作。通过符号模拟和抽象，分析复杂的生物化学过程变得可行。

因此我们可以通过实体计算，扩充计算可以解决问题的领域。我们不仅可以更有效的解决已知的基础问题，同样可以解决当下只能凭借实验解决的问题。为了实现这一期待，我们需要一个

通用分子计算机。

通用分子计算机是天方夜谭吗？

DNA之所以被用于实体计算是因为它可以储存信息（尽管是以A, T, G, C的方式，而非1和0），其次它提供了有力的实体计算的初始模型：

- › DNA聚合酶附着在DNA单链上，根据碱基互补配对原理产生对应的DNA链，是自发的复制过程。
- › 脂质分子聚集在一起，是自发的连接过程。
- › 核酸酶切开核酸链，实现了分割操作。

这些满足建造通用分子计算机的要求吗？正如图灵用他的机器模型阐释的，制作计算机只需要两个必备工具：信息存储装置(DNA是绝佳的信息储存器)和一些简单的数据操作（如多聚酶就可以对操作DNA信息）。因此在理论上这种设想可行。

除此之外，分子组装的语言已经被设计运用，把DNA的操作翻译成为化学反应。正常的DNA合成中从DNA序列制造一系列分子。细胞成分图谱反映了树，列表等重要成分。处理代数问题反映了分子计算的可操作性语义，分子计

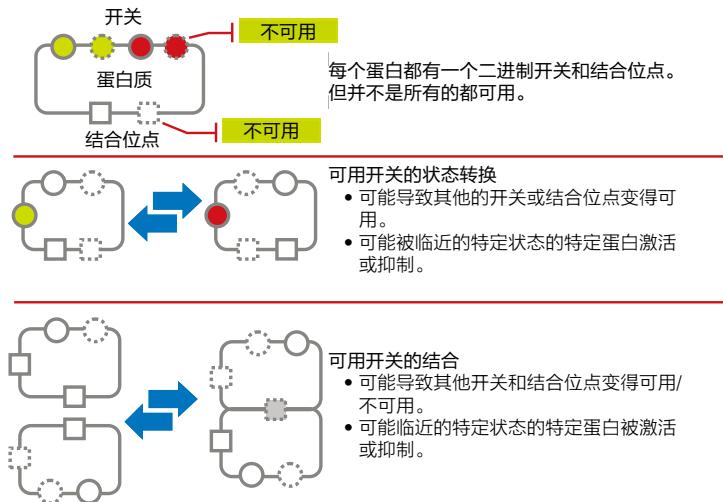


图4. 卡尔代利的蛋白质机器指令集。

算逻辑理论允许建造可预测的程序。凝胶为基础的DNA计算器已经被用来解决哈密尔顿问题和可满足性问题（如六个变量，11个条件）。

这种类比给我们展现了乐观的前景。但是在我们建造和使用分子计算器之前，必须解决一些技术挑战。

- › 首先也是最重要的是，我们必须确定我们期待用分子计算机解决哪些问题。一些可能是经典的计算问题比如哈密尔顿和布尔可满足性问题，另一些可能更加迫切，包括机器学习和深度学习。同样现在还有很多我们现在认为不可以通过计算解决的问题，比如药物设计，药物投递和纳米医疗。

- › 图灵机的重要性在于它定义了可计算性，而非实体的计算器。分子程序必须被编译来影响计算，高层次的分子编程语言会是什么样子呢？
- › 我们怎样在不同速率的计算程序

之间建立联系呢？换句话说，我们可否“校准”反应中相互联系的分子的时钟？

- › 转换成可编程的，可以控制的可以预测的生化反应的分子组装语言该怎样被定义？
- › 我们不能把鳄鱼夹放入试管读取计算结果，那么怎样实现信息的输入和输出呢？
- › 该用怎样的理论框架来描述分子计算的模型，我们可以解决的问题的复杂程度如何？
- › 要怎样相信分子计算和分子软件呢？怎样验证我们的代码有效？怎么实现系统的鲁棒性和容错性机制？

潜在的回报

如果我们成功地搭建了通用分子计算机，我们将可以采用液体计算机和编码药物，高度专一性的，无副作用的，靶向的解决患者所有疾病。我们可以用

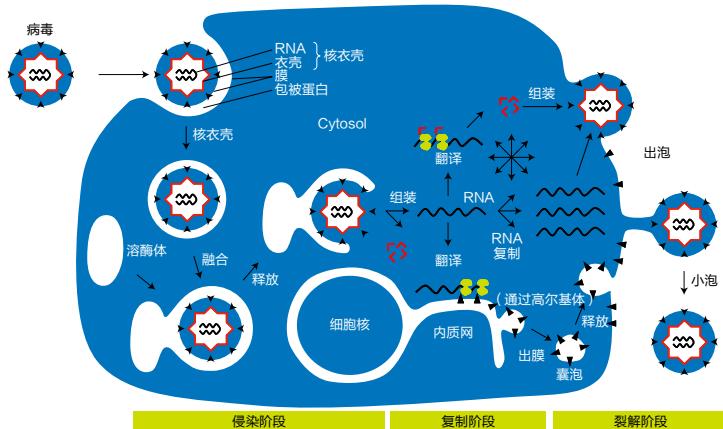


图 5. 森林脑炎病毒的复制原理。

分子机器人运输药物工作或修建记忆。同时，我们可以解决目前计算中的基本瓶颈问题。

- › 不可估量的信息密度和持久度。一个立方毫米的DNA可以储存艾字节信息，而半衰期长达500年。目前世界的数据预期可以在2017年增长至超过16泽字节。即便按照预期的存储技术发展速度，指数型增长的数据也远远超过我们存储能力。
- › 高度平行性。在阿德尔曼的实验中，一勺DNA溶液可以同时进行 10^{14} 项计算。而目前我们计算的复杂性通过多核计算机实现，受到编码的复杂程度的限制。
- › 能量高效。1焦耳的能量可以足够维持 2×10^{19} 反应，这逼近理论最大值 34×10^{49} 。反观目前最高效的超级计算机，日本名列2015年环保500强的RIKEN公司超级计算机Shoubu，每瓦的能量只能供其进行7.03G运算。分子计算机在

信息存储、信心处理，和能量高效方面，拥有大幅超过传统计算机的潜能。更重要的是，他把很多只能用实验进行的基本问题，如药物开发，带入了符号计算领域。阿德尔曼，卡尔代利，艾瑞克·温弗里(Erik Winfree)，保尔·罗彻姆得(Paul Rothemund)等等众多前人的工作让我们对这项技术充满信心。但是仍存在一些可怕的障碍，我们系统和预测性的利用分子计算的能力目前看来还只是停留在纸面上。除了国家科学基金会现在支持的分子计算项目外，我们必须加快节奏，联合计算机科学家，数学家，生物化学家，生物学家，化学家，物理学家等等，实现分子语言和分子编译的关键技术，随后解决由理论和分子计算介质决定的其他挑战。催化这个研究群体需要赞助机构和科学家的合作，研究团队也要尽快拿出研究议程，选择最有前景的方式，关注于一系列挑战性问题的解决方法。

忽 略分子计算潜力后果严重。随着近些年来分子计算和合成生物学理论的发展，我们的前景十分光明。C

致谢

作者在此衷心感谢参与该项研究的DSRC的同事们，没有他们的热心参与和协助，这篇文章不可能诞生。国防部高级研究计划局的很多同事也参与了这项研究，在此一并致谢。当然，作者还要特别感谢特邀发言人和为本文提出改进意见和建议的编辑和匿名评审人员，他们的评论让这篇文章中的观点更加明确。

参考文献

1. B.J. MacLennan, "Aspects of Embodied Computing: Toward a Reunification of the Physical and the Formal," tech. report UT-CS-08-610, Dept. of Electrical Eng. and Computer Science, Univ. of Tennessee, 2008.
2. H. Andre ka, I. Ne meti, and P. Ne meti, "General Relativistic Hypercomputing and Foundation of Mathematics," Natural Computing, vol. 8, no. 3, 2009, pp. 499–516.
3. K.F. Kelly and C.C.M. Mody, "Whatever Happened to the

关于作者

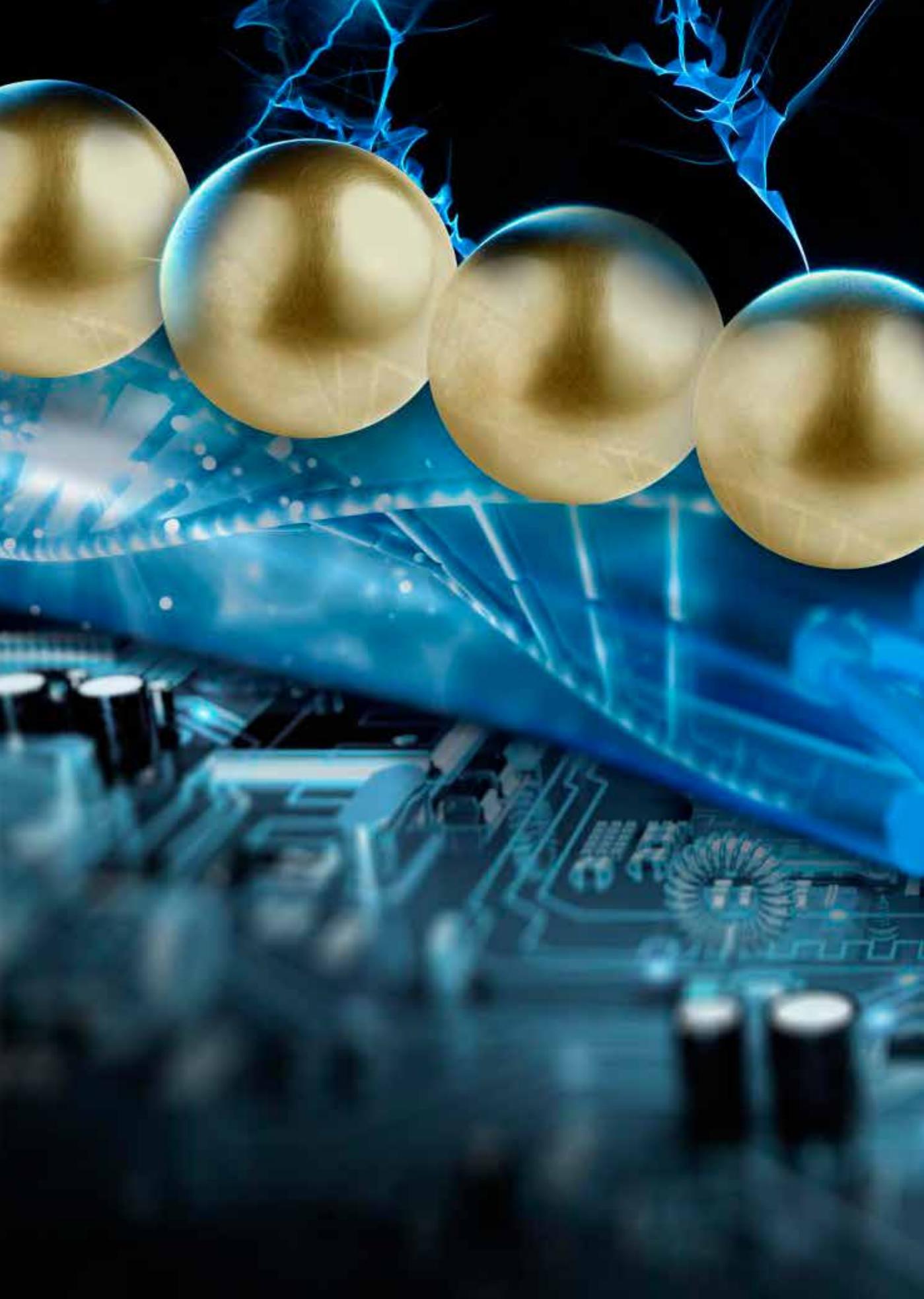
维多利亚·科尔曼 (Victoria Coleman) 是波托马克政策研究所高级研究员。她是国防部科学委员会成员、洛克希德马丁公司技术顾问团成员、圣克拉拉大学计算机工程系顾问委员会成员。科尔曼曾任 DARPA 信息科学与技术顾问团队成员，国防部科学研究委员会委员。她在索尔福德大学获电子计算机系统学士学位和计算机辅助逻辑设计硕士学位，在曼彻斯特大学获计算机科学博士学位。科尔曼持有四项专利，已发表论文和专著 60 余篇 / 部。联系方式：vcoleman@potomacinstitute.org。

Molecular Computer?,” IEEE Spectrum, 25 Sept. 2015;
<http://spectrum.ieee.org/biomedical/devices/whatever-happened-to-the-molecular-computer>.

4. R. Ganapathy et al., “Direct Measurements of Island Growth and Step-Edge Barriers in Colloidal Epitaxy,” Science, vol. 327, no. 5964, 2010, pp. 445–448.
5. S. Stepney, “Journeys in Non-classical Computation,” Grand Challenges in Computing Research, T. Hoare and R. Milner, eds., British Computer Society, 2004, pp. 29–32.
6. A.M. Turing, “On Computable Numbers, with an Application to the Entscheidungsproblem,” Proc. London Mathematical Society, series 2, no. 42, 1936, 230–236; correction no. 43, 1937, pp. 544–546.
7. L. Qian and E. Winfree, “Scaling Up Digital Circuit Computation with DNA Strand Displacement Cascades,” Science, vol. 332, no. 6034, 2011, pp. 1196–1201.
8. J. Zhou et al., “Enzyme-Based NAND and NOR Logic Gates with Modular Design,” J. Physical Chemistry, vol. 113, no. 49, 2009, pp. 16065–16070.
9. J. Macdonald, D. Stefanovic, and M.N. Stojanovic, “DNA Computers for Work and Play,” Scientific American, vol. 299, 2008, pp. 84–91.
10. L. Adleman, “Molecular Computation of Solutions To Combinatorial Problems,” Science, vol. 266, no. 5187, 1994, pp. 1021–1024.
11. A. Phillips and L. Cardelli, “A Programming Language for Composable DNA Circuits,” J. Royal Society Interface, 2009; doi:10.1098/rsif.2009.0072.focus.
12. A.K. Nielsen et al., “Genetic Circuit Design Automation,” Science, vol. 352, no. 6281, 2016; doi:10.1126/science.aac7341.
13. L. Cardelli, “Abstract Machines of Systems Biology,” Trans. Computational Systems Biology III, LNCS 3737, C. Priami et al., eds., Springer, 2005, pp. 145–168.
14. A. Adamatzky et al., eds., Unconventional Computing 2007, Luniver Press, 2007.
15. J. Bornholt et al., “DNA-Based Archival Storage System,” Proc. 21st Int'l Conf. Architectural Support for Programming Languages and Operating Systems (ASPLOS 16), 2016, pp. 637–649.

微信名：计算人
 微信号：jisuanren







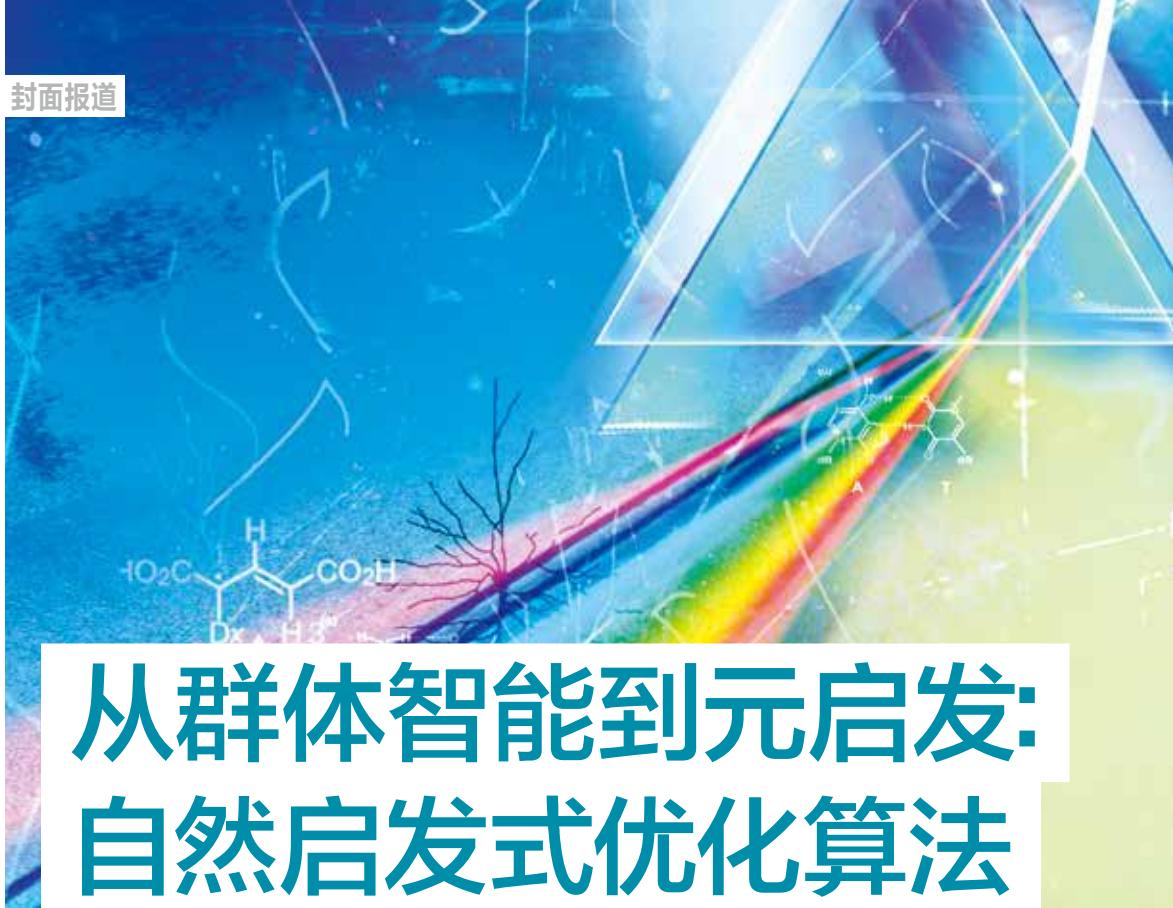
图片新闻

DNA 电路

德国亥姆霍兹联合会（Helmholtz-Zentrum Dresden-Rossendorf）的科学家把DNA制成长纳米线，然后将之与镀金的纳米颗粒结合，这样DNA纳米线就可以导电了。研究人员也许可以借此开发出一个基于遗传物质的电路来。

图片来源：亥姆霍兹联合会

论 文：*Temperature-Dependent Charge Transport through Individually Contacted DNA Origami-Based Au Nanowires.*



从群体智能到元启发： 自然启发式优化算法

文 | 杨新社 (Xin-She Yang), 苏阿什·戴布 (Suash Deb), 密德萨斯大学 (Middlesex University)

方正天 (Simon Fong,) 澳门大学 (University of Macau)

贺兴时 (Xingshi He), 西安工程大学 (Xi'an Polytechnic University)

赵玉新 (Yu-Xin Zhao), 哈尔滨工程大学 (Harbin Engineering University)

译 | 杨晨

自然界为我们解决计算问题 (*computational problem*) 提供了丰富的模型, 比如以萤火虫、蝙蝠、蚂蚁等生物的群体智能为基础的最优化算法。这些模型启发计算机科学家从传统之外的角度进行思考, 并创造新的工具来解决应用程序设计 (*application design*) 上的挑战。

大

部分 (甚至全部) 的工程任务都需要作出产品、服务和系统设计方面的决定, 这在某种程度上就涉及时间与资源的最优化处理, 达到性能、

利润、持续性、质量、安全和效率的最大化与成本、能耗、缺陷和环境影响最低之间的平衡。如同本文插文 “最优化问题的要素” 中描述的那样, 在这类设计问题中, 很多都包含多个目标, 这些目标之间具有高度复杂的约束关系。传统的方法是按问题的类型设计专门的方案, 这种方式已无法适应复杂

的非线性问题, 比如大数据下多判据工程设计 (*multicriteria engineering designs*) 和多重复杂特征提取 (*multiple complex feature extraction*) 等。

传统方法适应性差的问题引起人们研究新型最优化方法的兴趣。一条新兴的方向是, 将启发式搜索 (*heuristic search*) 与多主体系统 (*multiagent systems*) 结合起来, 解决实际商业和工程问题。¹这种结合在精准度、效率和性能上, 都优于传统方法。例如, 在人工神经网络 (它是许多人

最优化问题的要素

典型的最优化问题具有一个主要的设计目标，如花费、能效等。但这个目标往往受到许多设计条件约束，需要通过两个阶段完成最优化：一是问题构建（problem formulation），确定约束条件并确认其优先顺序；二是解法搜索（solution search），用最优方法解决这个问题。

问题构建

为说明在最优化问题中如何构建问题，可以考虑如下场景：寻找某条跨大西洋航线上丢失的黑匣子。搜索设计的约束条件有预算、洋流、天气和搜索时间等，它们处于对立关系。天气不好会延误搜索，从而增大开支和工作量，这些都会阻碍在一定时间内找到黑匣子的目标。同时，问题还有严峻的时间约束，因为黑匣子电池的寿命比较短。因此，构建问题时必须在开支、时间和找到黑匣子的概率之间进行一定的权衡，而权衡的结果则受其它因素影响，如可获得的资源或可以接近的地区等等。

解法搜索

构建好合适的最优化问题后，主要任务就是找到问题的最

优解。飞机最后的失踪地点或许可以提供黑匣子的位置信息，可以从那个区域开始搜索。但是，洋流可能会将黑匣子带到其它区域，如此，起始的搜索位置就带有准随机的性质。让一个搜救员（searcher）检查整片海域的每一寸地点，可以做到彻底搜索，但太不现实。另一种方法是让一群搜救员分区搜索，并分享各自的信息。信息分享产生群体智慧（collective intelligence），可以缩小搜索范围（search space）。

在实际情形中，大部分搜索过程都介于随机搜索与锁定目标之间；即使没有任何目标线索，搜索也不是完全随机的。在黑匣子的例子中，最可能的方案是以准随机搜索寻找线索。从某个可能的区域开始，搜索到临近的可能区域，如此持续搜索。搜救队成员之间相互交换线索，努力搜索并将经验运用到搜索更多可能区域（解）的成员将得到奖励或其它形式的鼓励；而懒惰或消极的成员可能会被开除（取消）。经过这样的挑选，找到黑匣子的概率便会逐渐提高。这个通过提炼群体智慧获得解法的过程，是当前元启发最优化算法（基于集群智能）的核心。

人工智能任务的核心）的优化或参数调节当中，新方法具有更高的效率和精准度。

在新型最优化算法中，有一类算法的基础是群体智能（swarm intelligence, SI）。SI的设计思想是：群体（蚂蚁和蜜蜂等）中的有机个体，根据区域信息、行为主体（agent）之间的交流及其自身环境做出的决定，是群体智慧（collective intelligence）或社会智慧（social intelligence）的起源。有一个假说认为，高度发达的物种成员之间直接或间接的交流，是其智力的来源，理由是，生物上的变化来自于有机体对其所在团体和环境的反应与适应。

同一种群通过群体智慧可以成功执行某些特定的任务。²⁻⁴如果生存资源非常匮乏，不同物种也会进行合作，甚至共同演化。

SI启发研究者根据昆虫和鸟类行为提出一系列巧妙的最优化方法。这类算法也叫做元启发式算法（metaheuristic），已被用来解决机器学习和工程问题。这类SI算法之所以有效，是因为在很多情况下，算法的迭代过程与自组织体系的演化非常相似。^{5,6}此外，算法中的噪音和随机性可以提高得到不同解的概率，避免程序只得出局部优化解（local optimal solution）。其结果是，选择机制能够更快地收敛

到一个全局优化解（global optimal solution）上。就像自然界里，体系通过迭代重组（iterative reorganization）达到新的状态结构，这类状态可以作为解决当前问题的方法。

为更好地理解SI和元启发式算法，我们查阅文献确认了它们的根本概念。以下描述的算法代表了140多种自然启发（nature-inspired）算法和它们的变种。⁷然而，这个数字现在可能已经低于实际情况了，因为在这个领域，几乎每星期都会出现一些新的算法。因此，我们在这里描述这些算法只是略作示意，以说明自然带来的启发可以转化为解决问题的有效方法。我们希望这份调研，

```

    初始化种群和迭代计数
    评估初始种群并找到最优解
    while(未满足停止条件)
        修改局部或全局现有的种群，生成新解
        评估新解
        if 新解更好, then 接纳新解, 更新种群
        if 新解不好, then 依照某些概率性准则接纳新解
        更新迭代计数
    结束
    输出过程结果

```

图 1. 典型自然启发算法的伪代码。

因为元启发式算法能够进行更广泛的搜索，并记录最优解，所以这种方法有超过简单启发法的趋势。^{7,10}我们可以从无限和有限猴子定理 (Infinite and Finite Monkey Theorems) 中看清这类算法的工作原理。

能成为用新方法和工具解决计算难题的出发点。

基本概念

SI是自然启发算法的核心，它又构成元启发式算法的基础。

群体智能

SI是一个复杂的过程，我们还不清楚哪些机制能够保证出现群体智慧。不过，最近大量研究表明，蚂蚁或蜜蜂等单个主体的行为都遵循着简单的规则，能对局部信息作出反应，而整体则没有中心指挥。⁸这类一定规则下的互动 (rule-based interaction) 可以产生自组织现象，带来更高层次的结构和特征。系统中的个体不具备智能，但系统整体却表现出群体智慧。这样的自组织可以解释重要的群体行为（不论这个群体是蚂蚁还是人）。

系统发生自组织需要特定的条件：反馈、共识主动性 (stigmergy)，系统单独部分间通过修改局部环境的方

式进行间接交流）、多重互动 (multiple interaction)、记忆和环境设置。^{2,8}不过，我们还不清楚这些条件发挥的作用，以及自组织结构从中出现的原由。不同研究通常关注于其中的一个或少数几个因素。

元启发式算法与猴子

大部分元启发式算法都源于自然案例。尽管在解决最优化难题时，可以用启发法 (heuristic) 得到一个很好的解，但我们不能保证得到最优解。启发法也许在大多数情况下都有效，但无法保证总是有效。相比之下，元启发式算法可以在很大的设计空间 (design space) 中进行更高级的搜索，通常需要记录历史最优解和解的选择形式。在最早的元启发式算法中，有一个种模拟金属退火的准随机方法。⁹它的方法是为系统的能耗指定一些概率，如果温度高，概率就趋于1；如果温度低（接近绝对零度），概率就趋于0。因此，当系统降温时，算法就不太可能得到较差的解，而只会得出较好的解。

无限猴子定理

这个定理假设，猴群中的每只猴子都有一台打字机。如果猴子的数量无限，而且每只猴子都在无限长的时间里随机打字，那么它们打出给定文本（比如莎士比亚全集）的概率几乎一定是1。^{11,12}现在缩小规模，将任务条件换成猴子们使用一台101键的键盘，随机打出一条包含n个字母的序列，而将目标变更为打出组成“computer”的八个字母。那么，随机序列中出现连续八个字母组成“computer”的概率，就是 $p=(1/101)^8 \approx 9.23 \times 10^{-17}$ ，这个数虽然很小，但不是零。

其实，这个定理的中心思想是，无限多只猴子打出任意给定文本的概率不是零。实际上，我们可以用概率论证明，在一条无限长的序列中，出现任意文本（包括这篇文章）的概率几乎一定是1。¹³

有限猴子定理

假设资源无限太过不切实际，有限猴子定理是一个更合理的设定：如果一

表 1. 不同算法的优缺点

算法类型	优点	缺点
基于梯度 确定性	更高的收敛速度 局域搜索更有效	梯度不易估算 无法保证全局最优
自然启发 元启发式算法 随机性 群体智能	全局最优 简单灵活 可以解决困难问题 处理问题的范围广 易于并行	计算成本更高 无法重复相同结果 处理局域搜索和简单问题时效率更低

定数量的猴子在一定时间内随机打字，那么它们打出特定文本的概率大于零。将这个结论套用在人类身上就是，几十亿人每天都在用键盘打字，虽然现在没有打出一部莎士比亚全集，但这件事终有一天会发生的概率大于零。

明显的差异

元启发式算法和两个猴子定理有三点重大差异。第一，猴子打字是随机的，不会学习或记住之前的行动；而元启发式算法则会学习历史，从中找到更好的解。第二，猴子不会选择要打哪些字母；而元启发式算法倾向于选择那些最好或最合适的解。它们大多会用某种随机的方式增强搜索的能力，从而增大找到真正最优解的概率。理论上，如果这类算法在多重运行(multiple run)下运行足够长的时间，就很有可能找到最佳的设计解(design solutions)。不过，我们不可能有无限长的搜索时间，所以大部分方法会使用数千甚至数百万个/次设计估值(design evaluation)或迭代。第三，猴子打字至多等效于在一片目标解空间(landscape)上进行随机搜索，而元启发式算法则利用解空间信息来引导搜索过程，产生新的解。算法会不断发现更好的解，这个过程和登

山非常相似。

算法的一般特征

尽管各类算法的灵感来源和使用的数学公式都各不相同，但它们仍具有一些共同的特征。比如，它们都会用到解种群(solution population)，如果其中某个解的成功率变低，它就会被淘新解。新解一般通过修改局部或全局的解种群产生。如果新解的适应性比已有的更高，就会被解种群吸纳，而这又会引起解种群的更新。

因此，宽泛地说，所有自然启发算法都可以用图1的标准伪代码表示。

如图1所示，所有自然启发算法都包括探索(exploration)和利用(exploitation)两种功能。为有效地检索设计空间，备选解种群(population of candidate solutions)必须具有一定的差异性。另一方面，为使算法以最少的迭代快速收敛，必须使用解空间信息(梯度、模型形状等)引导程序在可能性最高的区域进行搜索。利用这类信息可以加快收敛的速度。但是，这样也会导致解种群差异性增长过快，引起所有解都具备相近的概率，致使程序崩溃。

和其它算法的比较

如表1所示，相比基于梯度的算法，自然启发式元启发式算法简单灵活、可以解决困难的问题，具有明显的优势。而它们的缺点是计算成本更高，因为元启发式算法在设计选项上需要多重估值(multiple evaluation)，它们随机的性质也使其很难得到可重复的解。

算法类型

我们下面列出七种自然启发算法。其它这类算法还有很多很多，如引力(gravitational)、和声(harmony)、狼群(wolf)搜索算法，以及以生物地理学和免疫系统为基础的最优化算法。¹⁴

蚁群优化算法(Ant colony optimization)

蚂蚁是一种社会性昆虫，生活在有组织的社群当中，单个社群的蚂蚁数量可以达到2,500万之多。蚂蚁通过一种可以指示自身存在的化学物质进行交流，这种物质称为信息素。任何蚂蚁都能跟随其它蚂蚁的信息素踪迹并留下自己的气味信息素，完成相互之间的交流。在踪迹选择中，信息素沉积

(deposition) 相当于正反馈机制; 信息素消散 (evaporation) 相当于回避机制 (escape mechanism)。

蚁群最优算法的提出是在1992年, 它利用局域互动与信息素变化, 从本质上模拟了蚂蚁的主要行为和社

蜂, 其它都是雌性工蜂。工蜂会进行侦查、观望、守卫和采集花蜜等活动。侦查的工蜂发现新的花蜜源后, 会用一种上下飞舞的舞蹈通知其它工蜂。2005年提出的人工蜂群优化算法, 就模拟了蜜蜂搜索行为的主要特征。¹⁵这个算法将

分贝 (相当于大型喷气式客机起飞时的噪音强度)。蝙蝠发现昆虫后, 在定向捕猎飞行中, 超声波脉冲的发射频率上升到每秒200次, 声波频率也更高。此时蝙蝠可以更准确地判断飞虫的大小、位置、飞行范围、速度和方向。

蝙蝠算法提出于2010年, 利用了蝙蝠发射超声波脉冲和频率调节的特点, 将蝙蝠的位置作为搜索空间 (search space) 中的解矢量。蝙蝠通过调节超声波频率, 可以搜索范围更大的空间; 而提高脉冲发射频率, 则可以锁定附近区域中可能出现的局部解。在整个蝙蝠群中, 有一个全局最优解, 其它蝙蝠都趋向于飞向这个位置。因此, 算法的收敛速度相对较快。这个算法由声波频率、脉冲发射频率及音强三个因素控制, 可以应用于许多实际应用当中, 如解决工业最优化问题、训练神经网络、图像处理以及解决TSP问题。

自然启发式元启发的相对优势 包括其简易性、灵活性和 处理困难问题的能力。

会特征。⁸它在处理最优化问题方面出乎意料地有效, 不论是车辆路径问题 (vehicle routing) 还是著名的旅行推销员问题 (traveling-salesman Problem, TSP) 都可以解决。算法将蚂蚁行走的路径编码为实际路径 (actual path)。蚂蚁在多条实际路径的交汇点做出的选择, 取决于路径上信息素的浓度。路径上有信息素沉积说明这条路比较好; 而信息素消散则确保早期搜索阶段中, 那些不太好的路径不会很快地收敛。

蜂群优化算法 (Bee colony optimization)

单个蜜蜂社群一般由2万到8万只蜜蜂组成, 其中有一只蜂王和几百只雄

蜜蜂按状态分为雇佣 (employed)、侦查和观望 (onlooker) 三种, 以花蜜源为解矢量 (solution vector), 并将其与目标解空间联系起来。虽然这个设定有些简单, 但它抓住了蜜蜂搜索行为的主要特征。这个算法被用于训练神经网络, 以及解决无约束数值优化问题和约束优化问题。

蝙蝠算法 (Bat algorithm)

小型蝙蝠共有八百多种, 其中大部分都用回声定位进行导航, 为此蝙蝠需要每秒发出10到20次超声波脉冲, 每个脉冲的持续时间只有几千分之一秒, 频率在20到200千赫兹之间 (人耳最高只能听到20千赫兹), 音强可以达到120

布谷鸟搜索算法 (Cuckoo search)

一些布谷鸟很擅长巢寄生, 它们将蛋生在其它鸟 (比如林莺) 的巢里, 然后由宿主孵化喂养。这是因为布谷鸟的蛋可以模仿宿主鸟蛋的质感、颜色和大小, 效果十分接近。即便如此, 有些宿主还是可以认出布谷鸟的蛋, 然后将它们踢出巢外或抛弃自己的鸟巢。这就在两个物种之间形成一种进化上的军备竞赛。

布谷鸟搜索算法提出于2009年，它将布谷鸟的蛋作为解矢量，筑巢区作为搜索空间。¹⁷证据表明，布谷鸟和宿主鸟的飞行路线都遵循列维飞行(Lévy flight)模式，即偶尔的长距离飞行伴随着局部的随机行走，这使得大范围的搜索更加有效。鸟蛋相似可以转化为解相似，有助于迭代搜索过程达成收敛，而发现概率(discovery probability)则有利于全局探索。布谷鸟算法在工程最优化问题和图像处理问题中都有成功应用。

粒子群优化算法 (Particle swarm optimization)

鸟和鱼类在移动时往往聚成一群，数量带来安全是其原因之一。每只鸟都遵循简单的飞行规则，只会追踪临近七只鸟的飞行状态。虽然飞行运动受牛顿力学支配，但奇怪的是，鸟群中的鸟却几乎完全不会相撞。从这类群体中，可以看出一些组织结构。

粒子群优化算法提出于1995年，它的基础就是上面提到的简单规则以及群体运动的特征。¹⁸它以粒子的位置为解矢量，因此每个粒子都有历史最优位置，而当前的最优解由整个粒子群产生。粒子在上述简单规则下更新它们的位置和速度，而全体粒子都倾向于向质心(centroid)移动，那里是全局最优解。这个体系能在很多情形下迅速收敛。一方面，快速收敛使这个方法

成为有效的优化控制器(optimizer)；另一方面，收敛的时机可能会太早，从而导致早熟收敛(premature convergence)。因为我们有许多解决早熟收敛问题的方法，所以这个算法有不少变种。粒子群优化算法几乎在科学和工程的每个领域都有应用，包括设计最优化问题、图像处理和调度问题(scheduling)等。

萤火虫算法 (Firefly algorithm)

热带地区的萤火虫以生物发光的方式进行交流，每类萤火虫都有特定的闪光模式，作为各自的信号系统。萤火虫会被同类的闪光吸引，并向发光方向飞去。因为光强会随距离增加和空气污染而减弱，所以萤火虫只能看见几百米之内的闪光。

萤火虫算法提出于2008年，它的基础是上述闪光特征。萤火虫的位置对应于解矢量，目标解空间决定发光的亮度或吸引力。因为短距离的光比长距离的光更有吸引力，所以整个萤火虫算法可以自动分割为许多子群体(subgroups或subswarms)，每个子群体在解空间的局部模型附近运动，形成峰(最大值)和谷(最小值)。因此，这个算法能同时找到多个最优解。在一定条件下(如正确的吸引范围及随机性单调递减)，它的收敛速度可能比遗传

算法(genetic algorithm)和粒子群算法都更快。萤火虫算法也和粒子群算法一样，从调度与分类问题，到图像处理、工业设计最优化问题等领域，都拥有广泛的应用。

花朵授粉算法 (Flower pollination algorithm)

显然，不是所有算法都以群体行为作为基础。植物同样提供了许多巧妙的模型，比如授粉过程。在25万种开花植物中，有九成是生物授粉，靠蝙蝠、鸟类、蚂蚁和蜜蜂之类的动物传递花粉。某些传粉生物(如蜂鸟)只会接近特定种类的植物，它们具有访花恒定性(flower constancy)。剩下一成开花植物靠非生物授粉，花粉由风或水传播，局限在一定范围内。相比之下，生物授粉是全局性的，因为传粉生物可以移动很长的距离。

花朵授粉算法提出于2012年，以花粉配子作为问题的解矢量，用生物传粉来模拟全局搜索，而用非生物传粉模拟局部搜索。¹⁹全局与局部的转换由一个概率控制，这个概率表示生物传粉与非生物传粉比例。这个算法被用于解决多目标最优化问题。

应用领域

自然启发算法的应用范围很广，

以这类算法探索和解决现实不同领域应用问题的论文，每年都有几百（根据Web of Science）甚至几千（根据Google）篇。

困难问题

TSP是典型的困难问题，它已经用蚁群最优化算法等元启发式算法得到了解决。⁸困难问题无法用现有方法在现实时间尺度内解决，而自然启发方法可以是很有用的选择，TSP就是一个代表。尽管自然启发算法不能保证总能得到最优解，但次优解（suboptimal）也非常有用，至少比没有任何解要好。

电信

自然启发算法可以用于解决局域接入网络（local access network）最优化问题，使服务质量最优，而整体能耗最低。²⁰由这类算法得出的设计，比用传统方法得到的更好；新的设计方案普遍效率更高、能耗更低、同信道干扰更少。

图像处理

图像处理通常是耗时很长的计算任务。将传统技术与自然启发算法结合之后，在图像分割、分类和深度信念网络（deep-belief network）²¹等许多应用中，程序可以更准确地提取图像特征。

工程设计

许多工程设计问题都是高度非线性问题，比如结构设计、无线传感器网络（wireless sensor network）等。传统方法处理这类非线性问题的效果很不好。最近的研究显示，自然启发算法通常可以更有效地得到更好的设计选项，因为它们使用解空间信息来搜索设计空间区域，不同主体（或解集，solution sets）之间也能分享信息。^{14,17,22}

车辆路径问题

车辆路径问题是一个很有挑战性的问题，在物流和组合最优化问题中有许多应用。许多车辆路径问题（比如在不同约束条件下调度车辆）都使用自然启发算法来增强性能。在一项研究中，元启发式算法解决车辆路径问题比传统算法更有效，运费也更低。²³而飞机调度、起飞时隙分配（departure slot allocation）和空域管理也可以用自然启发元启发式算法得到圆满解决，所得的解既有更低的运营成本，也可以更有效地利用起飞时隙。²⁴

现

在应用问题变得越来越复杂，还需要处理容量大、速度快、类型多的大数据。因此，研究者需进一步观察自然如何处理类似的问题，并在重要的新

方向展开研究。理论分析是其中一个方向，研究自然启发算法的工作原理。任何理论发现都有巨大作用，能够引导我们合理运用当前算法，并设计出更有效的新算法。最优化问题依旧存在于科学、工程、工业和商业应用的所有领域之中，我们毫不怀疑接下来会出现一场应用程序爆发（application explosion）。

从模仿自然的算法之外，发现解决问题的新视角也很重要。达尔文方式（Darwinian manner）下的生物系统演化没有高层次的目标，它们只是响应和适应环境的变化。因此，如果活下来的最适者能维持一定数量或形成一个物种，那么它们就不必是全局最优的结果。既然自然不总是最优解，研究者就必须找到令算法更稳健的方法，使其能适应变化。

杂合（Hybrid）算法或许是个有趣的选择，因为它融合了多种算法的优点。如何设计一个更好的杂合算法本身就是一个更高层次的最优化问题——最优化算法的最优化问题。发展杂合算法不能只让它比非杂合算法的效率和稳健性更高，研究者必须跳出这种潮流。杂合算法的比较研究应该只涉及杂合之后的算法。

在物联网时代，算法必须具备自适应能力和智能。为一个特定问题找到最佳算法的应用程序太多了。相比之

关于作者

下，自适应方法能够自动选择适合给定任务集的算法，在没有或极少的用户干预下执行任务。自适应也意味着可以控制自身性能并自动调节参数，保证程序高效运行。最终目标是开发出一个智能工具箱（intelligent toolbox），只要用户按下开始按钮，就能解决所有给它的问题。

显然，我们只有少数几个可能的方向。结合新算法与传统技术应该会很有用，值得一试。毕竟，传统技术有稳固的基础，经受过大量测试，也是针对特定类型问题最有用的方法。在传统方法效果不好的领域才最需要新方法。不过，在给定的应用需求下，我们希望能看到更多对自然启发算法的研究，用它们发展出更有效的工具，解决现实世界中各式各样的应用问题。■

参考文献

1. X.S. Yang, *Engineering Optimization: An Introduction with Metaheuristic Applications*, John Wiley and Sons, 2010.
2. L. Fisher, *The Perfect Swarm: The Science of Complexity in Everyday Life*, Basic Books, 2009.
3. P. Miller, “Swarm Theory,” *Nat'l Geographic*, July 2007; ngm.nationalgeographic.com/2007/07/swarms/miller-text.
4. J. Surowiecki, *The Wisdom of Crowds*, Anchor Books, 2004.
5. W.R. Ashby, “Principles of the Self-Organizing System,” *Trans. Symp. Univ. of Illinois: Principles of Self-Organization*, H. Von Foerster and G.W. Zopf, Jr., eds., Pergamon Press, 1962, pp. 255–278.
6. E.F. Keller, “Organisms, Machines, and Thunderstorms: A History of Self-Organization, Part Two: Complexity, Emergence, and Stable Attractors,” *Historical Studies in the Natural Sciences*, vol. 39, no. 1, 2009, pp. 1–31.
7. X.S. Yang, *Nature-Inspired Optimization Algorithms*, Elsevier, 2014.

杨新社是密德萨斯大学建模与最优化高级讲师，剑桥大学唐宁学院研究员。他的研究方向是自然启发计算、群体智能、建模和最优化问题。杨新社拥有牛津大学应用数学博士学位。他是IEEE计算智能学会商业智能和知识管理小组主席。联系邮箱: x.yang@mdx.ac.uk。

苏阿什·戴布 (Suash Deb)是信息技术与教育顾问。他的研究方向是元启发式算法和群体智能。Deb拥有加尔各答大学计算机科学技术硕士学位，并获得斯坦福大学计算机科学的United Nations Fellowship。他是IEEE高级会员，国际神经网络协会印度分会创建人兼主席。联系邮箱: suashdeb@gmail.com。

方正天是澳门大学计算机与信息科学系副教授。他的研究方向是数据挖掘、元启发式算法和大数据分析。方天正拥有拉筹伯大学计算机科学博士学位。他是IEEE和ACM会员。联系邮箱: ccfong@umac.mo。

贺兴时是西安工程大学理学院教授兼副院长。他的研究方向是数学建模、算法、统计学和计算智能。贺兴时拥有陕西师范大学数学硕士学位。他在2016年获得陕西省优秀教学成果奖。联系邮箱: xsh1002@126.com。

赵玉新是哈尔滨工程大学控制与导航教授。他的研究方向是自然启发计算、智能运输系统和航海导航系统。赵玉新拥有哈尔滨工程大学控制科学与工程博士学位。他是英国皇家导航学会会员。联系邮箱: zhaoyuxin@hrbeu.edu.cn。

8. E. Bonabeau, M. Dorigo, and G. Theraulaz, *Swarm Intelligence: From Natural to Artificial Systems*, Oxford Univ. Press, 1999.
9. S. Kirkpatrick, C.D. Gelatt, and M.P. Vecchi, "Optimization by Simulated Annealing," *Science*, vol. 220, no. 4598, 1983, pp. 671–680.
10. C. Blum and A. Roli, *Metaheuristics in Combinatorial Optimization: Overview and Conceptual Comparison*, ACM Computing Surveys, vol. 35, no. 2, 2003, pp. 268–308.
11. A. Gut, *Probability: A Graduate Course*, Springer, 2005.
12. G. Marsaglia and A. Zaman, "Monkey Tests for Random Number Generators," *Computers & Mathematics with Applications*, vol. 26, no. 9, 1993, pp. 1–10.
13. G. Lorge, "The Best Thought Experiments: Schrödinger's Cat, Borel's Monkeys," *Wired*, 22 May 2007; www.wired.com/2007/05/st-best-4.
14. X.S. Yang et al., *Swarm Intelligence and Bio-inspired Computation: Theory and Applications*, Elsevier, 2013.
15. D. Karaboga, *An Idea Based on Honey Bee Swarm for Numerical Optimization*, tech report TR06, Computer Eng. Dept., Erciyes Univ., 2005.
16. X.S. Yang, "A New Metaheuristic Bat-Inspired Algorithm," Proc. Conf. Nature-Inspired Cooperative Strategies for Optimization (NICSO 10), J.R. Gonzales, ed., *Studies in Computational Intelligence*, vol. 284, 2010, pp. 65–74.
17. X.S. Yang and S. Deb, "Multi-objective Cuckoo Search for Design Optimization," *Computers and Operations Research*, vol. 40, no. 6, 2013, pp. 1616–1624.
18. J. Kennedy and R.C. Eberhart, "Particle Swarm Optimization," Proc. IEEE Int'l Conf. Neural Networks (ICNN 95), 1995, pp. 1942–1948.
19. X.S. Yang, M. Karamanoglu, and X.S. He, "Flower Pollination Algorithm: A Novel Approach for Multiobjective Optimization," *Eng. Optimization*, vol. 46, no. 9, 2014, pp. 1222–1237.
20. X.S. Yang, S.F. Chien, and T.O. Ting, *Bio-inspired Computation in Telecommunications*, Elsevier, 2015.
21. X.S. Yang and J.P. Papa, *Bio-inspired Computation and Applications in Image Processing*, Elsevier, 2016.
22. H.E.P. Espinosa, *Nature-Inspired Computing for Control Systems*, Springer, 2016.
23. N. Labadie, C. Prins, and C. Prodhon, *Metaheuristics for Vehicle Routing Problems*, John Wiley and Sons, 2016.
24. N. Durand et al., *Metaheuristics for Air Traffic Management*, John Wiley and Sons, 2016.

微信名：计算人
微信号：jisuanren





搜索你的工作机会

IEEE Computer Society 招聘可以帮你轻松找到IT、软件开发、计算机工程、研发、编程、架构、云计算、咨询、数据库很多其他计算机相关领域的的新工作。



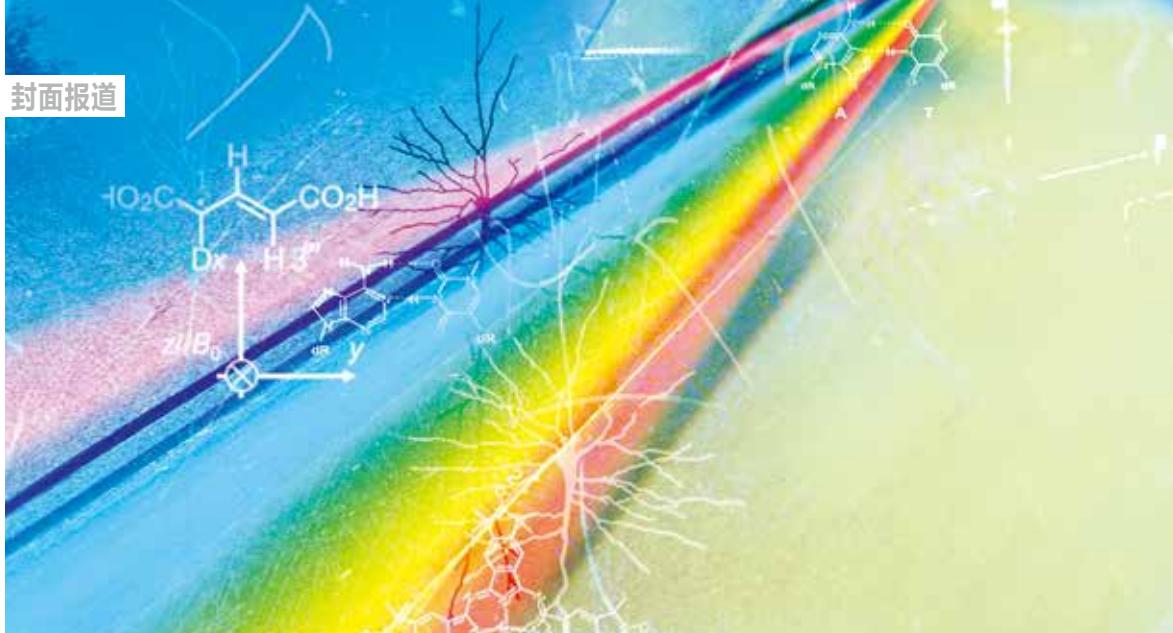
新功能：找出那些建议或要求拥有IEEE CS CSDA或CSDP认证的工作！

点击www.computer.org/jobs，
从全世界的雇主那里搜索技术工作岗位和实习机会。

<http://www.computer.org/jobs>

IEEE  computer society | JOBS

IEEE计算机协会是AIP Career Network的合作伙伴。其他合作伙伴包括《今日物理》杂志（Physics Today），美国医学物理协会（American Association of Physicists in Medicine），美国物理教师协会（American Association of Physics Teachers），美国物理学会（American Physical Society），AVS科学和技术学会（AVS Science and Technology），物理学生协会（Society of Physics Students）和Sigma Pi Sigma。



与大脑皮层互联的计算： 协同式脑机接口新范式

文 | 萨米尔·萨普罗 (Sameer Saproo)，约瑟夫·福勒 (Josef Faller)，维克多·辛 (Victor Shih)，保罗·赛达 (Paul Sajda)，哥伦比亚大学 (Columbia University)

尼古拉斯·维托维奇 (Nicholas R. Waytowich)，艾迪森·伯翰农 (Addison Bohannon)，维农·劳伦 (Vernon J. Lawhern)，布伦特·兰斯 (Brent J. Lance)，美国陆军研究实验室 (US Army Research Laboratory)

大卫·江劳 (David Jangraw)，美国国家精神卫生研究院 (National Institute of Mental Health)

译 | 洪琳碧

与传统意义上应用大脑信号对计算机和机器人进行直接控制的脑机接口不同，与大脑皮层互联的计算系统能够投机性地检测出当前的脑状态，从而捕捉用户直接或间接的脑计算，而后再将这个信息通过脑机接口传递给传统计算机系统。

绝

大多数现代计算机采用的都是基于冯·诺依曼架构的一个变种，这一架构的核心思想是储存程序或指令集的概念。而开发合适的指令集（即编程）则是训练有素的操作人员的专门领域。简而言之，编程是这样一门艺术：人类在其基础上运用键盘和鼠标等机电接口，向电脑传递有关这个世界的知识、以及一套能够达成某些预期结果的可执行命令。在改进机器的计算能力上，人类用户

时常会成为这个过程中的瓶颈。这是因为人机间的信息传递既受我们将脑中知识转化为逻辑命令的能力所限，亦受接口比特率的影响。然而，随着机器智能在一般效力上日趋媲美人类智能，我们与机器交互或协作的方式，将很可能会影响到如今人类对机器进行明确编程的需求。

作为计算机科学界发展最为迅猛的领域之一，机器学习对于数据标签有着严重的依赖性。举例而言，在有关现实生活

IEEE 大脑倡议

2015

年末，IEEE 提出了 IEEE 大脑行动 (<http://brain.ieee.org>)，旨在通过促进跨学科间的协调与合作，增进神经科学领域的研究、标准化进程及技术开发，并由此帮助改善人类当前的状况。IEEE 处在一个独一无二的位置可以充分利用自己在电气、通信、传感器、能源管理及其他技术领域的广泛专业知识，在工程学和系统方面为理解大脑并与其交互的世界性活动提供新的观点。例如，IEEE 大脑行动目前正在和多个组织一起协调标准化和技术开发进程。这些组织包括以美国领导的创新神经技术大脑研究 (BRAIN) 提议 (www.braininitiative.nih.gov)，欧盟领导的人类大脑计划 (www.humanbrainproject.eu)，以及数个正在开展或将于日本、澳大利亚和中国开展的相关倡议。

的照片中，目标上的标签使得机器可以学习这组数据中不同对象间的联系。这些标签中许多都带有主观色彩 -- 毕竟这是人类用自己掌握的关于世界的知识所创建的 -- 因此也就无法通过纯粹的自动化方法生成，所以很有价值。实际上，用户 -- 点击流量分析已被证实是谷歌、亚马逊、Facebook 等商业公司所不可或缺的一部分，这些公司可通过数据为用户提供更加个性化的服务。尽管通过人类活动（例如在网页上点击并选择）而产生的明确标签数量颇为可观，它与人在间接处理感官数据时产生的标签量仍然无法相提并论。即使没有产生明显的行为，人类的知觉仍然处在活跃的处理过程中。如果有可能获取当人们在街上闲逛，或安静地看着电视节目时其脑内认知过程的内容，那么机器学习系统能够使用的信息量将极可能将会是革命性的。

人脑-计算机接口（BCI），又名人脑-机器接口（BMI），能够对人脑中的内容进行解译，并基于此内容指示计算机系统重建人脑与外部的沟通和/或对外部的控制。人脑当前的内容可借由非侵入式脑机接口，通过颅外电极所采集的脑电图（EEG）获得；也可以由侵入式脑机接口，通过大脑皮层上植入电极所采集的皮层脑电图（ECoG）获得。最为常见的脑机接口应用，是让瘫痪病人通过想象移动电脑屏幕上的鼠标，实现现

实中屏幕上鼠标的真实移动。不过，尽管旨在实现主观控制的脑机接口对于特定人群有着重要意义，对于一般人群而言，所测脑电波不甚理想的低信噪比（SNR），是目前这一应用针对一般大众的适用性仍然极其有限的主要原因。然而，如能长时间监测，即便信号受低信噪比影响，也仍能为我们提供有用的信息。这样的信息可以被用来增强其他计算系统的能力，尤其是学习能力。

由此，我们提出一个新的模式：与大脑皮层互联的计算技术。在这种计算技术中，人类和机器均需要完成计算任务，而二者间的之间的通信由脑机接口实现。这个技术最简单的版本，是试图运用大脑生成的关于这个世界的信息，将某些专门的知识教给一台并无先验知识的机器。如果这一技术能够完全实现，它为我们勾画出的即是这样一个未来：高度先进的人工智能和人类用户可以协同、无缝地完成任务，而下一代脑机接口则促进了这种人机协同。接下

来，我们将以几个能够从不同角度实现这个创新模式的真实系统为例，来进一步说明与大脑皮层互联的计算技术的概念。

与大脑皮层互联的计算机视觉系统

尽管计算机视觉领域（CV）如今已经有了长足的发展，特别是深度学习领域在近期取得的进展，但如何让机器在嘈杂和背景复杂的环境中全面“理解”图像，仍然是一个挑战。试想，一名图像分析员正在通过空中侦察数据评估该地区的潜在危险。与针对每张图片需要进行的详细评估相比，图片的总数量之多显然是首要问题。因此，分析员必须通过自己对图片的重要性，即图片“概要”的主观判断来先行分拣。在这里，完成图像理解不需要通过图像本身推断出的目标信息，同时也需要通过背景信息来评估其重要性。为完成这个

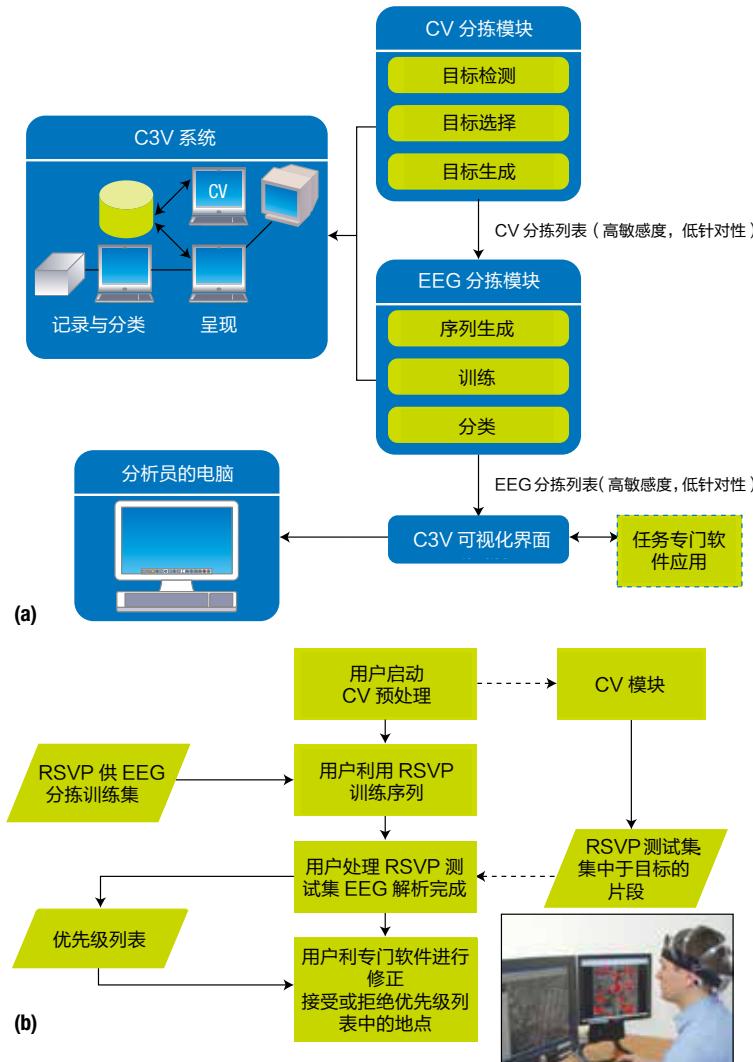


图 1. 与大脑皮层互联的计算机视觉系统的示例：(a) 系统组成部分以及 (b) 系统流程。CV: 计算机视觉; EEG: 脑电图; RSVP: 快速系列视觉呈现。本图改编自 P. Sajda et al., “In a Blink of an Eye and a Switch of a Transistor: Cortically Coupled Computer Vision,” Proc. IEEE, vol. 98, no. 3, 2010, pp. 462–478。

目标, 计算机视觉系统必须利用受训图像分析员的专业技能。

与大脑皮层互联的计算机视觉系统 (C3V) 结合了人类视觉系统的一般用途及其背景能力, 以及计算机视觉系统不知疲倦的数字计算能力。^{1,2}这个系统最关键的思想, 是通过对图像分析员脑电波信号的分析, 用脑机接口收集

更多的信息, 评估其对瞬时图像的兴趣度, 从而提高自动图片检索与分拣系统的数据量。简而言之, C3V 系统为数据库中的每张图片都创建了一个由人生成的认知标签, 然后进行机器学习。

为了生成这些认知标签, C3V 系统会通过快速系列视觉呈现技术 (RSVP), 向图像分析员展现与当前任

务有关的图片。RSVP 技术即按顺序向用户呈现几百张图片, 每张图片呈现时间仅 100–200 毫秒。因为每张图片在屏幕上停留的时间极短, 图像分析员只能获得图片内容的概要。在此如此之短的时间内, 人类分析员只能获取对这张图片的概念性理解, 这是个非常适合由人类完成的任务。³如果对这张图片的大致理解恰与分析员的意图或特定关注点相吻合, 那么他或她将能够快速地把注意力导向这张图片, 产生一个可通过 C3V 系统解译的神经生理学信号。^{1,4,5}由于注意力的导向并不是非有即无的二元状态, 而是对兴趣度的平滑函数。因此, 如同谷歌利用网页排名分数来为搜索结果进行优先级排序一样, 这个被解译的标识也可以被当作一个能够为所有图片进行优先级排序的兴趣度分数。有趣的是, 这个标志注意力导向的脑信号, 在用户观看静止图片中的物体, 以及捕捉动态视频中特定的时空事件时均可被脑电图检测到。⁶尽管这个实现注意力导向的模式利用了人类视觉系统, 能够快速标记某张含有感兴趣物体的静止图片, 或一段视频中包含的兴趣物体的片段, 但系统的吞吐量仍然受到限制, 因为人类每秒只能处理约 5–10 张图片。而 C3V 系统可通过充分利用计算机视觉技术, 在前期为图像分析员先行过滤出可能包含所找寻信息的图片, 或者在后期处理完毕有限图片集的关注



(a)



(b)

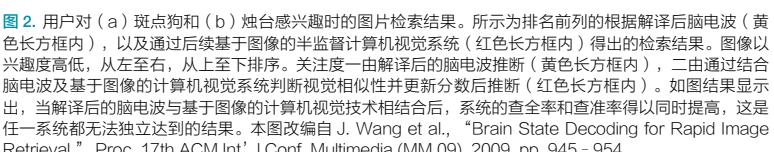


图2. 用户对(a)斑点狗和(b)烛台感兴趣时的图片检索结果。所示为排名前列的根据解译后脑电波(黄色长方框内),以及通过后续基于图像的半监督计算机视觉系统(红色长方框内)得出的检索结果。图像以关注度高低,从左至右,从上至下排序。关注度一由解译后的脑电波推断(黄色长方框内),二由通过结合脑电波及基于图像的计算机视觉系统判断视觉相似性并更新分数后推断(红色长方框内)。如图结果显示,当解译后的脑电波与基于图像的计算机视觉技术相结合后,系统的查全率和查准率得以同时提高,这是任一系统都无法独立达到的结果。本图改编自J. Wang et al., “Brain State Decoding for Rapid Image Retrieval,” Proc. 17th ACM Int'l Conf. Multimedia (MM 09), 2009, pp. 945–954。

度分数后,以更高效的方式在更大的图片数据库中进行检索。在下面的章节中,我们将详细描述上面这两种情形。

先计算机视觉, 后人类视觉处理

图1所示为一个用来分析卫星图片的C3V系统原型。²这个系统包含三部分:一个基于计算机视觉的分拣模块,一个基于脑电波的分拣模块,以及一个能够为用户呈现综合分拣结果的显示界面。首先,用户可启动用来分析整张图片的计算机视觉分拣模块——在这个案例中是一张大型卫星图片。计算机视觉处理将通过一些普适标准或用户设定的限制(如搜索人造物体或目标),来检测图片中可能存在的关注点。系统利用检测结果来构筑图像“碎片”,即子图像,并通过快速系列视觉呈现技术将其呈现给用户。用户头戴脑电图帽(如图1b所示),而脑电波先行分拣模块则运行一个基于机器学习的分类器,该分类器事先已经训练完成,旨在用户脑电波信号中识别注意力导向事件。接下来,系统将计算机视觉模块生成的一系列图像碎片传给用户,对用户的脑电波信号进行实时解码,为每张图像碎片创建关注度分数,以这些分数标记这些图像碎片,并据此生成基于用户关注区域的优先级列表。接下来,显示界面将把这个优先级列表与卫星图像相结合,

使得图像分析员能够在屏幕上对目标进行移动、缩放和标记,并可以切换至高分数的不同地图区域。该系统已在真实图像搜索环境中接受过测试,将图像搜索数据量提高了300%。

先人类视觉, 后计算机视觉处理

在C3V系统中,计算机视觉模块不仅可被用作环路中人类用户的预处理器,也可在人类用户处理之后使用。在后一种情形中,通过利用图像碎片上的认知标签,计算机视觉模块可以在一个

大型数据库中识别视觉或语义上类似的图片。举例而言,C3V系统能够利用半监督式的图形推演模块将关注度分数扩散至尚未被标记的图片上,并以此评估那些用户仍未看到的图片的关注程度。⁷如图2所示,在大型数据库中,采用这种处理方式能够同时提高某个被搜索图像类别的查全率和查准率。当使用人类注意力分数来为计算机视觉模块创建标签时,模块本身便能够依据人类用户的认知关注度为新图片排序,使得系统表现进一步提高。在闭环模式下运行时,C3V系统的准确率最初即大

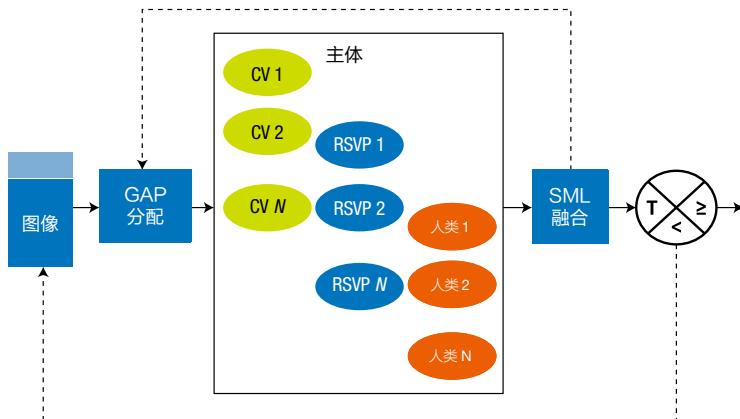


图3. 人类自动图像标记器（HAIL）的并行图像分配模式。HAIL利用广义指派问题的方法（GAP）实现了从数据库向计算机视觉主体、以系统设定步调以及自定步调的人类主体分配图片的优化。主体负责对所分配的图片进行分类，HAIL则应用Spectral Meta-Learner（SML），在混合节点为每张图片分配一个总体置信度。基于已经得出的图片置信度及对主体分类准确性的推断，系统将认定图片已被分类，或将其送回图像分配节点进行进一步的分类。

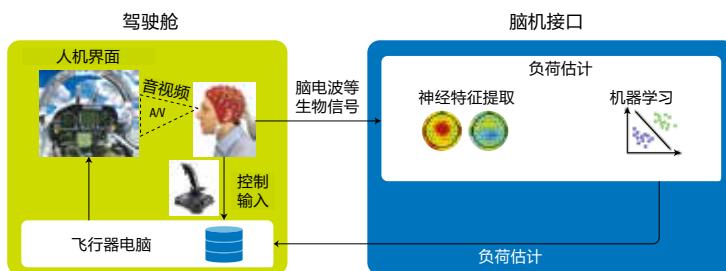


图4. 能够持续监测飞行员认知负载并将此信息告知飞行器电脑的脑机接口。飞行器电脑可根据此信息为飞行员提供直接反馈或改变驾驶舱内界面，缓和飞行员负荷。该系统可应用预估的认知负载来为驾驶舱内的每一类人行为进行标记。通过评估哪些因素增大了认知负荷，改善人机间的交互。

幅提高，并在脑电波解码和计算机视觉搜索迭代2.5次之后逐渐平缓。

将C3V系统延伸至多主体环境

应用不同的计算机视觉模块、可用度更高、更符合人体工学的脑机接口、以及不同种类的通信拓扑结构，C3V模式可以拓展为更多的平台。由美国陆军研究实验室研发的人类自动图像标记器（HAIL）即是一个可扩展的闭环图像标记系统，为同一网络下不同的人及计

算机视觉图像标记主体的相互合作提供了支持。利用基于机器学习的分配策略，HAIL凭借所有主体而非一部分主体的共同努力，来实现更好的系统性能。⁹ 在为主体分配图像信息时，HAIL既可以串行模式为高流量的主体事先分配图像，也可以按并行模式分配，即每个主体同时分析图像数据库中的一部分数据。

串行图像分配模式

在串行图像分配模式下，HAIL首先会将图像分配给一个基于深度学习

的计算机视觉模块，并基于搜索模板进行识别。在计算机视觉算法对图像进行优先级排序后，HAIL会将排序后的图像通过RSVP传递给一个“遵循系统步调”的人类主体，以供其观察。在人类主体观看稳定图像流时，HAIL会对其脑电波信号进行实时解码，并依此来再次评估计算机视觉模块的决策。最后，HAIL会把剩余的图像展示给一个自定步调的人类主体，这个人会通过触屏在一个直观的平铺图像的显示屏上提供人工决策。尽管目前的系统在计算机视觉模块和脑电波解码器上使用的都是静态统计模型，如今的研究正着力于将自适应分类器及反馈模式引入当前系统。这个改变将使得人类和计算机视觉主体能够更好地适应彼此，并从中互相学习。

并行图像分配模式

HAIL的并行图像分配模式的诞生受到了众包模式优化研究的启发。¹⁰如图3所示，系统按广义指派问题方法（GAP）创建了一个最优化的并行图像分配模式，将图像分配给计算机视觉主体、遵循系统步调及自定步调的人类主体。HAIL将不同主体的图像分类决策与SML相结合，并根据综合起来的结果以及对主体可靠性的推断来确定后续图像的分配。这里，SML是一种非监督式整体混合分类器。接下来，系统将

对图像分配以及综合起来的图像分类决策进行迭代，直到所有图像的分类决策都达到预期的置信度。与单人或多个人主体的模式相比，这种由不同主体（人类和计算机）联合协作的图像处理方式，能够在显著缩短的时间内达到与人类处理的表现相当。更值得一提的是，HAIL的多主体自适应模式可以最大化地结合先验效率未知、或效率随时间改变的主体的综合表现。这样一来，系统的计算特征能够随着各节点及网络拓扑结构的实时变化而变化。

复杂人机交互下的动态认知负载推断

协同式的人机系统可以智能地适应动态认知负载这个想法，可以扩展到非视觉导向的人机交互中。如图4所示为一个闭环脑机接口，它能够持续监测飞行员在压力下的导航任务：即在边界大小动态变化的情况下，避免与边界相撞。在这样的任务中，飞行员的承受的负载由多种动作决定，比如对操纵杆及油门杆的控制，以及与驾驶舱内各类界面的交互（例如对声音和显示屏上出现的事件作出反应）——同时也与对仪表盘和数字显示器上的连续监测息息相关。

在有关这个项目的初步研究结果中，我们发现了与飞行员高负荷相对应

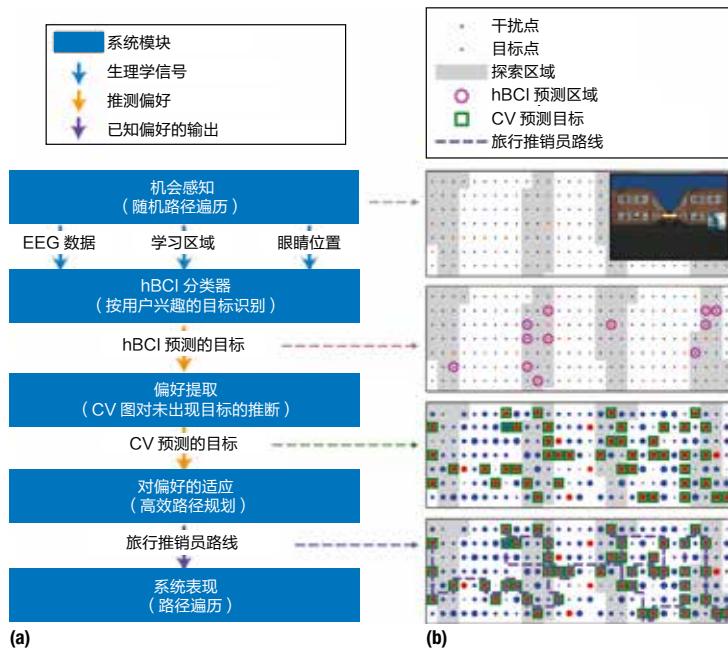


图5. 将机会感知与自动导航系统相结合的脑机接口实例。(a) 系统设计, (b) 导航环境的俯瞰及用户视图。图中点的大小表示计算机视觉得分的高低: 分数更高的对象被认为更有可能是目标物体。混合脑机接口(hBCI)用生理学信号来标记那些看上去吸引了用户注意力的物体。然后, 计算机视觉技术将标签推广至环境中尚未出现的物体。最后, 路径规划器将依据预期会引起用户注意力的物体分布, 来创建能够遍历这些物体的最有效的路径。如此, 该导航系统便创造出一条既不超越当前环境所限, 又能适应用户特定需求的路径。本图改编自 D.C. Jangraw et al., “Neurally and Ocularly Informed Graph-Based Models for Searching 3D Environments,” J. Neural Eng., vol. 11, no. 4, 2014; doi:10.1088/1741-2560/11/4/046003.

的明确神经学内容。事实上，飞行员的高认知负荷可能会导致飞行员与飞行器间的互联无法达到最佳状态，并因此导致一种名为“飞行员诱发震荡”的危险情形。然而，通过实时解译与任务相关的认知负荷，并以反馈形式为人类或机器提供必要干涉，可以给人机间的交互带来正面影响。除此之外，这个系统还能够以预估的认知负荷来标记人驾驶舱中的活动。在事后分析中，机器学习技术可以依此判定是哪些动作或动作组合增大了飞行员的认知负荷。这样的信息有助于构建更加高效的驾驶舱界面。这个概念性的模式可以被推广到其他与导航有关的任务中，比如驾驶汽车。通过优化与汽车控制和信息呈现的

界面，司机在驾驶时能够更加专注，因此减少事故的发生。

通过投机感知使人工智能适应人类取向

随着人工智能系统性能的提高，它们已被越来越多地用来为人类用户提供协助，或与用户进行交互。从选择娱乐项目到驾驶汽车，类似的例子不胜枚举。能够感知用户的偏好，很多面向用户的人工智能系统就可以对AI输出进行个性化，在人类和机器间建立信任，从而使系统从中受益。然而诸如深度学习等现代人工智能体系大多依赖于大量的训练数据，将这些偏好与机器通信

需要用户付出难以承担的巨大努力。让人庆幸的是，近期在机会感知领域所取得的进展，可能会让用户在无需特定训练环节甚或无需明确指示的情况下，即能完成对用户偏好的评估，实际上，系统可以利用与日常事件中用户产生的主

够引起受试产生注意力反应。这个反应会影响到受试的脑电波信号、瞳孔大小以及驻留时间（即目光在目标上停留的时间）。系统采集这些生理学信号，运用bHBI分类器确定一小组看上去成功吸引受试注意力的“hBCI预测目标物

度或转弯准确度进行调整。系统可以透过与不适或惊讶相关联的生理学内容，来推断是否没有满足用户偏好。这类对动作的标签可以进一步推广到一个模拟训练环境中。在这个环境下，深度学习系统可以在无需额外等待用户输入的情况下，根据大量已推演出的标签调整其驾驶方式。接下来，新训练过的系统将能够更好地依照用户的喜好来刹车和转弯。这样一来，系统可以避免明确评估用户取向而产生的高成本，并仍然能够为现代人工智能系统提供所需的大量训练标签。

与大脑皮层互联的计算技术可适用于现实世界中的多种应用。

观兴趣或预期相关的生理学内容。12这些几乎毫不费力就能生成的认知标签，可被用来定制一个能够满足个人用户特定取向需求的人工智能系统，因此提高了人机间的协同性。

图5所示为使用混合脑机接口（hBCI）的导航系统，可以推断用户偏好的目标类型，并生成一条访问所有目标的高效路径。实验对象经过一个包括各类目标的大型3D虚拟环境的一小部分，并被要求对一个“目标”类别内的物体进行计数，并忽略其他三个“干扰”类别内的目标。目标类别即代表用户偏好访问的目标，而整个系统的目的即是找到一条高效的路径，以访问尽可能多的用户偏好目标。

在实验最初的探索阶段，目标能

体”。然后，系统再通过计算机视觉技术将这些目标物体的标签推给其他还未出现的目标，和“旅行商人问题”的求解器，来求出“通过计算机视觉预测的目标”的最有效路径。遵从此路径，受试能够在只通过看到全部目标所需路径距离的40%的情况下，就看到84%的目标。因此，在用户无需大费周章的前提下，该系统便能够找到一条既不超越当前环境所限，又能适应用户特定偏好的路径。

新型的人工智能应用可以将机会感知用于其他领域，通过生理学信号对不同种类的偏好进行推断，或用人工智能完成其他不同的目标。举例而言，要实现自动驾驶的深度学习系统的开发者，可能会希望根据用户偏好对刹车速

度或转弯准确度进行调整。系统可以透过与不适或惊讶相关联的生理学内容，来推断是否没有满足用户偏好。这类对动作的标签可以进一步推广到一个模拟训练环境中。在这个环境下，深度学习系统可以在无需额外等待用户输入的情况下，根据大量已推演出的标签调整其驾驶方式。接下来，新训练过的系统将能够更好地依照用户的喜好来刹车和转弯。这样一来，系统可以避免明确评估用户取向而产生的高成本，并仍然能够为现代人工智能系统提供所需的大量训练标签。

在现实世界中能够稳定感知生理学信号的硬件和软件，将有助于类似应用的发展。值得庆幸的是，这类软件和硬件都在迅速发展，从消费级脑电波头戴设备到基于视频的眼球监测系统都在面向移动应用。除此之外，虚拟现实系统越来越受欢迎，这可能为虚拟环境或游戏中评估用户偏好提供了机会。在这类环境下，对用户进行监测更方便，而环境本身的可控性也更高。



大脑皮层互联的计算技术适用于现实世界中的多种应用。这既包括大型快速图像检索及标记、自动驾驶，也包括飞行器导航等高精度任务中的控制。这一技术利用了对大脑状态进行机会感知

关于作者

萨米尔·萨普罗 (SAMEER SAPROO) 是哥伦比亚大学生物医药工程系博士后。他的研究方向包括神经计算、神经成像、人工智能以及脑机接口。Saproo在加州大学尔湾分校获计算机科学硕士学位，在加州大学圣迭戈分校获心理学博士学位。联系方式: ssaproo.ucsd@gmail.com。

约瑟夫·福勒 (JOSEF FALLER) 是哥伦比亚大学智能成像及神经计算实验室的博士后。他的研究方向包括脑机接口和神经成像。Faller在奥地利格拉茨技术大学获计算机博士学位。联系方式: josef.faller@columbia.edu。

VICTOR SHIH 是哥伦比亚大学生物医药工程系博士生。他的研究方向包括机器学习、计算神经模型、人工智能以及脑机接口。Shih在哥伦比亚大学获得了生物医药工程硕士学位。联系方式: vs2481@columbia.edu。

保罗·赛达 (PAUL SAJDA) 是哥伦比亚大学生物医药工程系、电气工程系以及放射科学系的教授，哥伦比亚大学智能成像及神经计算实验室主任。目前他的大部分研究是利用多模态神经成像和行为方式，监测快速决策任务中的选择性注意力。同时，他也运用这些基础科学的发现来构建能够改善人机交互的神经科技系统。他在宾夕法尼亚大学获得了生物工程博士学位。他是IEEE会员、IEEE神经系统及修复会刊的主编，及IEEE大脑计划的主席。联系方式: psajda@columbia.edu。

尼古拉斯·维托维奇 (NICHOLAS R. WAYTOWICH) 是哥伦比亚大学智能成像及神经计算实验室和美国陆军研究实验室人类研究与工程办公室的联合博士后。他的研究方向包括机器学习、脑机接口，人机自治整合以及自适应系统。他在欧道明大学获生物医药工程博士学位。他是IEEE和IEEE SMC的会员。联系方式: nick.waytowich@gmail.com。

艾迪森·伯翰农 (ADDISON BOHANNON) 是美国陆军研究实验室的一名研究科学家。他是马里兰大学学院市分校应用数学、统计及科学计算系的在读博士生。他的研究方向是人机系统，智能系统以及科学计算。Bahannon在马里兰大学学院市分校获得了应用数学、统计及科学计算硕士学位。他是IEEE以及IEEE SMC的会员。联系方式: addisonb@math.umd.edu。

弗农·劳伦 (VERNON J. LAWHERN) 是美国陆军研究实验室人类研究与工程办公室的统计师。他的研究方向包括机器学习，统计信号处理以及应用于脑机接口的神经生理学数据挖掘。Lawhern在佛罗里达州立大学获得了统计学博士学位。他是IEEE的会员。联系方式: vernon.j.lawhern.civ@mail.mil。

布伦特·兰斯 (BRENT J. LANCE) 美国陆军研究实验室人类研究与工程办公室的一名计算机科学家。他的研究方向包括人机交互，人机自治整合以及机器学习。Lance在南加州大学获得了计算机科学博士学位。他是IEEE的高级会员。联系方式: brent.j.lance.civ@mail.mil。

大卫·江劳 (DAVID JANGRAW) 是美国国家精神卫生研究院功能性成像方法分部的博士后。他的研究方向是通过机器学习和创新的手段来分析自然实验条件下的生理学数据，目前他正着力于研究持续注意力与视觉决策。他在哥伦比亚大学获得了生物医药工程博士学位。联系方式: david.jangraw@nih.gov。

的概念，系统捕捉到用户直接或间接的计算结果，这个信息通过诸如非侵入式头皮脑电图采集等脑机接口，与传统计算机系统进行通信。这和传统意义上的脑机接口有着本质不同，后者用大脑信号对计算机和机器人进行直接控制。

在不远的未来，我们预计上述技术会产生大量的扩展。举例而言，HAIL和C3V系统均可扩展为更广义的与大脑皮层互联的数据分析系统，解决分析和计算都颇为棘手的复杂问题。通过脑机接口将不同的计算机视觉分析主体及人类分析员连结到一起后，系统可以运用视觉分析技术将复杂问题重新投射入人类的视域，通过多主体系统将分解后的任务在网络内传递，将返回的结果聚合为高置信度的解决方案。这种分析引擎会推动复杂数据分析的进步，能够为诸多领域提供新的想法和能力。

另一方面，与大脑皮层互联的计算技术也可用于整合人类用户和物理机器人的不同感知及行动能力。比如，急救人员正试图利用一组小型无人机，快速对一个受灾区域进行评估。如果无人机能通过机会感知了解用户搜索时最看重哪些要素，它们就能够在动态地图上识别类似区域或目标，加速救援行动。最终，通过类似的系统，与大脑皮层互联的计算技术将被证明是可以令人机交互实现协同合作的一项技术，其计算力要强于人机的简单结合。■

致谢

本文由美国国防高级研究计划局，美国陆军研究办公室项目W911NF-11-1-0219，美国陆军研究实验室协议W911NF-10-2-0022，美国国防部长办公室飞行员自主研究倡议项目MIPR DWAM31168，以及英国经济与社会研究协会项目ES/L012995/1共同协助。

参考文献

1. A.D. Gerson, L.C. Parra, and P. Sajda, "Cortically Coupled Computer Vision for Rapid Image Search," *IEEE Trans. Neural Systems and Rehabilitation Eng.*, vol. 14, no. 2, 2006, pp. 174–179.
2. P. Sajda et al., "In a Blink of an Eye and a Switch of a Transistor: Cortically Coupled Computer Vision," *Proc. IEEE*, vol. 98, no. 3, 2010, pp. 462–478.
3. A. Oliva and A. Torralba, "Building the Gist of a Scene: The Role of Global Image Features in Recognition," *Progress in Brain Research*, vol. 155, 2006, pp. 23–36.
4. P. Sajda, M.G. Philiastides, and L.C. Parra, "Single-Trial Analysis of Neuroimaging Data: Inferring Neural Networks Underlying Perceptual Decision-Making in the Human Brain," *IEEE Reviews in Biomedical Eng.*, vol. 2, 2009, pp. 97–109.
5. L. Parra et al., "Spatiotemporal Linear Decoding of Brain State," *IEEE Signal Processing Mag.*, vol. 25, no. 1, 2008, pp. 107–115.
6. D. Rosenthal et al., "Evoked Neural Responses to Events in Video," *IEEE J. Selected Topics in Signal Processing*, vol. 8, no. 3, 2014, pp. 358–365.
7. J. Wang et al., "Brain State Decoding for Rapid Image Retrieval," *Proc. 17th ACM Int'l Conf. Multimedia (MM 09)*, 2009, pp. 945–954.
8. E.A. Pohlmeyer et al., "Closing the Loop in Cortically-Coupled Computer Vision: A Brain-Computer Interface for Searching Image Databases," *J. Neural Eng.*, vol. 8, no. 3, 2011; doi:10.1088/1741-2560/8/3/036025.
9. A.R. Marathe et al., "Confidence Metrics Improve Human-Autonomy Integration," *Proc. ACM/IEEE Int'l Conf. Human-Robot Interaction (HRI 14)*, 2014, pp. 240–241.
10. C.-J. Ho, S. Jabbari, and J.W.

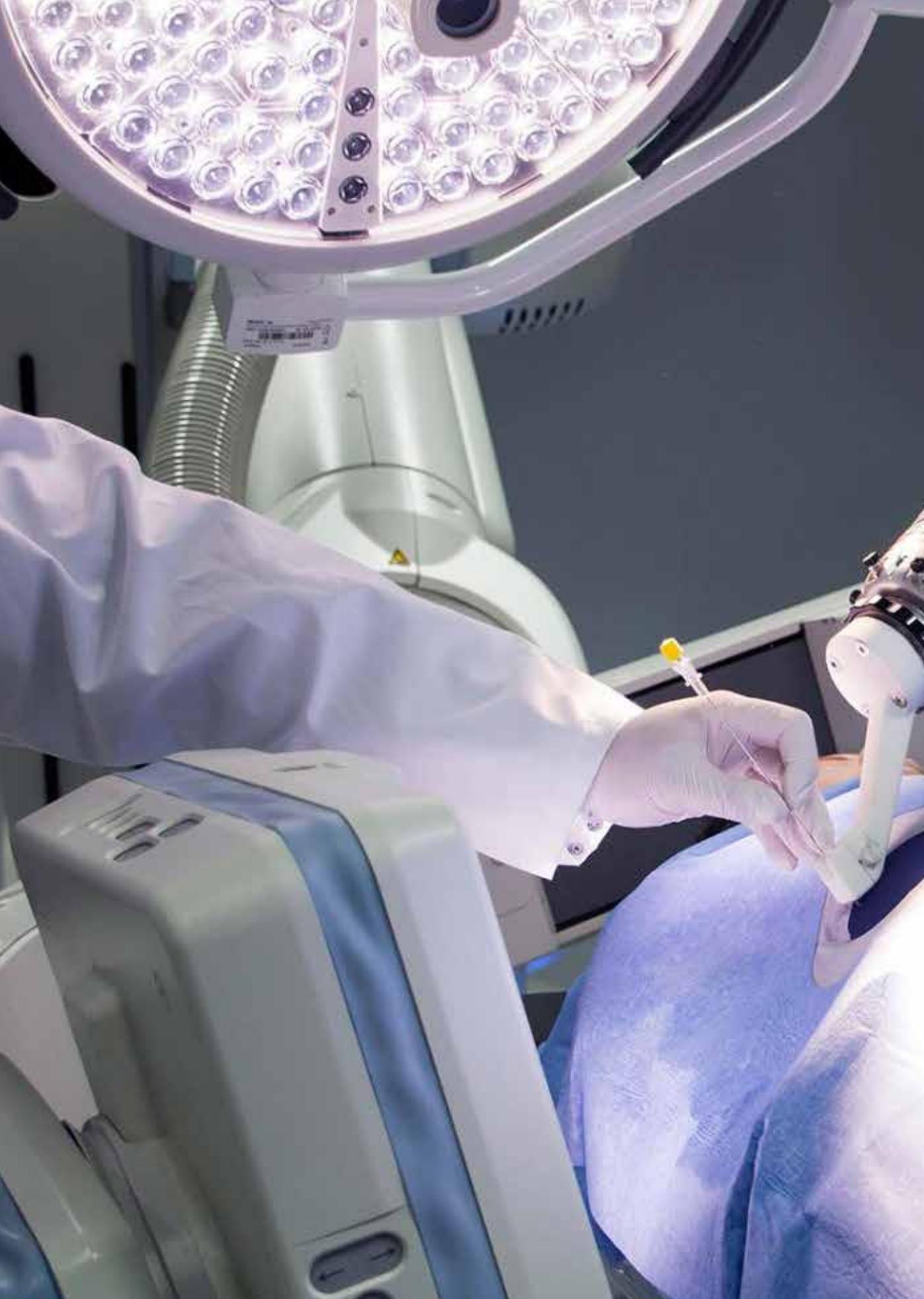
- Vaughan, "Adaptive Task Assignment for Crowdsourced Classification," Proc. 30th Int'l Conf. Machine Learning (ICML 13), 2013, pp. 534–542.
11. F. Parisi et al., "Ranking and Combining Multiple Predictors without Labeled Data," Proc. PNAS, vol. 111, no. 4, 2014, pp. 1253–1258.
12. B. Lance et al., "Brain–Computer Interface Technologies in the Coming Decades," Proc. IEEE, vol. 100, 2012, pp. 1585–1589.
13. D.C. Jangraw et al., "Neurally and Ocularly Informed Graph-Based Models for Searching 3D Environments," J. Neural Eng., vol. 11, no. 4, 2014; doi:10.1088/1741-2560/11/4/046003.



《IEEE软件杂志》为软件从业者提供了前沿观点，专家分析和深刻的洞察，让他们跟上日新月异的技术变迁。这本杂志还为软件理论转化为应用提供了权威观点。

[www.computer.org/
software/subscribe](http://www.computer.org/software/subscribe)

SUBSCRIBE TODAY





图片新闻

能扎针的机器人

传统的活检扎针定位过程要花费医生 30 分钟时间，但在机器人的帮助下，医生只要 5 分钟就能找到扎针点。因为针点定位需要 X 光辅助，所以机器人可以减少医生和病人在放射性环境中的暴露时间。

图片来源：Photo Fraunhofer IPA

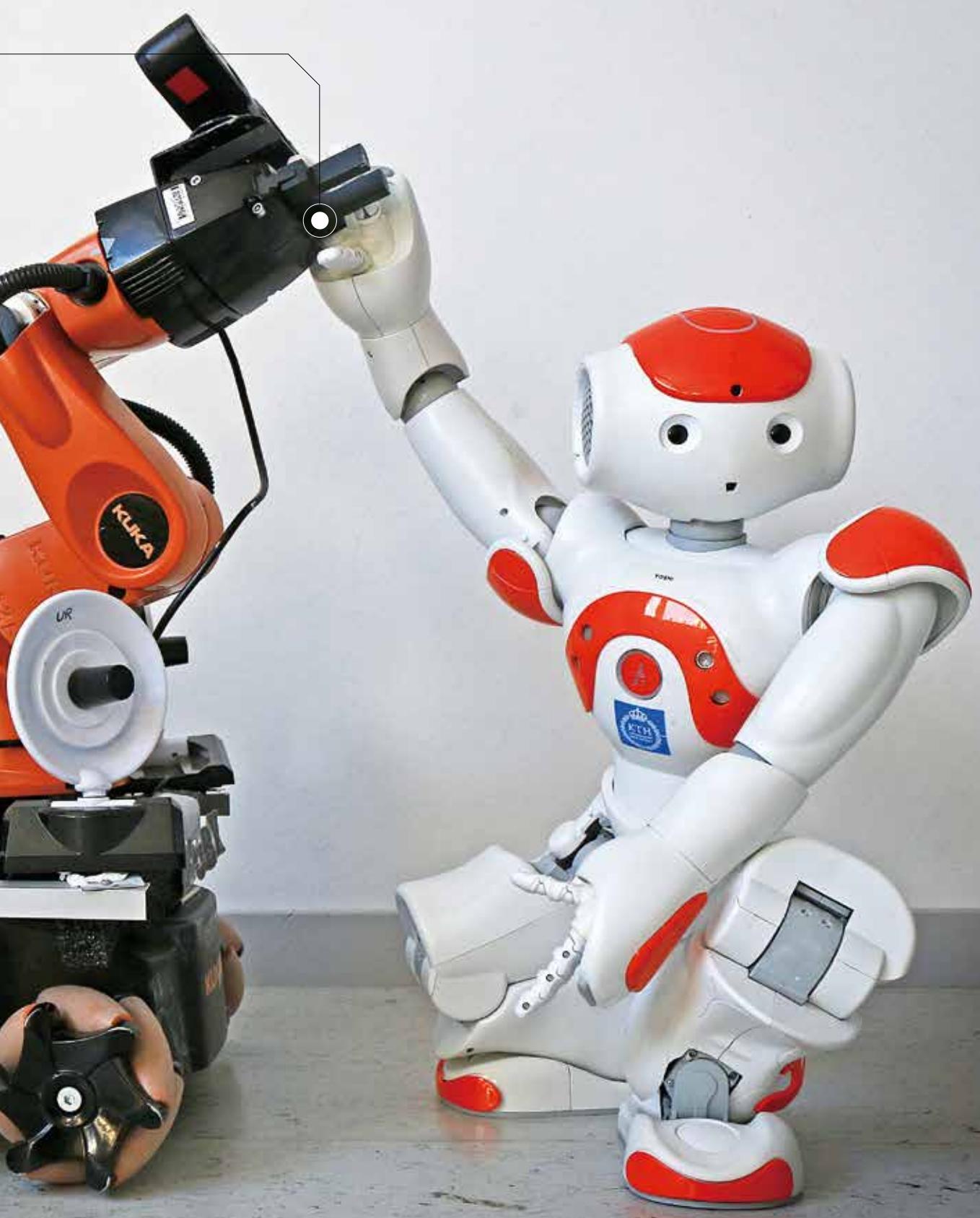
互相帮助的机器人

人和人之间可以通过肢体动作传达信号，在合作中进行交流。那么机器人呢？

瑞典皇家理工学院的研究人员在欧盟的RECONFIG项目中设置了一套协议，可以让机器人在遇到任务困难时，能够主动向其他机器人发出求助信息，并相应地做出任务调整。

图片来源：瑞典皇家理工学院







工作中的原型科幻

文 | 伊万·艾瑟顿 (Evan Atherton)，欧特克 (Autodesk)
译 | 汪梅子

尽管欧特克以设计类软件而闻名，但其实这家公司已开始利用原型科幻来探讨设计、技术及人类的未来。



编辑寄语

我们非常高兴看到有更多机构利用原型科幻流程来探讨可能的未来。每一个新项目都会带来一种全新的方法。我们在本月专栏中请来了欧特克的高级研究工程师伊万·艾瑟顿，他将向我们讲述率先开始使用原型科幻的欧特克公司是如何将实用主义与绝妙设计结合起来的。

——布莱恩·大卫·约翰逊

欧

特克最为知名的产品是 AutoCAD 等设计类软件。

所以，当人们发现我们在为分子设计和人机合作开发工具时，他们的第一反应是问为什么。我们的回答通常都会从科学角度来解释，我们正在学习如何操控脱氧核糖核酸 (DNA)，就像操控计算机一样，只不过利用的工具从 0 和 1 变成了 A、C、T、G，有时还会举个例子，就像是有人对一颗种子编程，

使它长成一幢房子。但这些回答都难以表达技术对社会的真正影响。

讲故事在人类文化发展中发挥了至关重要的作用，甚至在我们开始通过言语交流之前便已如此。但技术专家在表达新概念方面仍然没有充分利用讲故事的方式。

如果你是本专栏的忠实读者，我就不用多费口舌宣传原型科幻的种种优点了。我更希望讲讲欧特克是如何利用讲

故事等手段、以更易理解和更具影响的方式来回答有关未来技术的问题的。

在欧特克讲故事

尽管在布莱恩·大卫·约翰逊和亚历克斯·麦克唐威尔等先驱的带领下，欧特克利用原型科幻已有数年，但仅限于在讲习班和头脑风暴时少量使用。我们认识到了这些做法的价值，终于决定创建一个正式的讲故事项目。

2014年初，我和同事亚瑟·哈苏瓦纳齐推出了一个利用原型科幻探讨未来设计的暑期实习项目。我们建立了一支小团队，由四名背景各异的优秀学生组成，可以说，这是我们自己的迷你版早餐俱乐部。他们整个暑假都在调研、头脑风暴、设计和讲故事。项目成果比较粗糙，不过，对于如何将模糊的想法化



图1. 在《四》的第三个故事中，一个放牧者带着一群彼此联通的生物力学机器人在大平原上搜索，从“失败者”的废土中寻找资源，为他们的游牧社会建造新的家园。（插画作者：玛丽亚娜·卡利尔）。

为易于理解的叙述性文章，我们得到了很大收获。

我们通过那次暑期试验发展出了自己的声音和流程。次年夏天，我们更为深思熟虑，启动了一个短篇小说选集项目，最终出版了《四：探索设计、技术及我们的未来的短篇小说集》(<http://autode.sk/28SY4Yf>)。《四》由卡罗

琳·布鲁尔执笔，她和玛丽亚娜·卡利尔绘制了插图，两人都是罗德岛设计学校插画专业的在读学生。

《四》：探讨人机合作、气候变化等问题

正如标题所示，《四》收录了四篇

小说，分别设定在四个不同的未来时代，集中探讨了对欧特克尤为重要的四个主题——从合成生物学和气候变化到我们与机器人和人工智能的关系。

我们的目标并非一定要预言或预测未来，因为，说实话，我们很有可能是错的。我们希望尝试的是创造一些世界，在其中以一种吸引人的方式探讨一些宏大的概念。例如，第三篇故事的主角是一个女性放牧者，她带着一群彼此联通的生物力学机器人在大平原上搜索，从“失败者”的废土中寻找资源，用于为他们的游牧社会建造新的家园（见图1）。

放牧者不小心落入一个你我大概比较熟悉的旧时代工厂的废墟中。她将自己的机器人“骇飞（hepphae）”与固定在工厂地板上的工业机器臂相比较：

在她四周，一栋建筑从套索散发的幽幽紫光中浮现出来。她面前矗立着带立柱的内厅，柱子被水线环绕，浇筑混凝土地板表面覆盖着厚厚一层盐和尘土。大厅延伸至黑暗中，只听得到她马靴敲地的声音回响，四下散落着垃圾，还有一排排密布的巨人。

整整齐齐十五排陈旧机器静静地立在黑暗中。放牧者咽了口唾沫，在它们之间穿行，举起火炬照亮视野。这些老古董潜伏在早已腐朽的橡胶皮带上方，不像是什么实用的东西，倒像是文物。但她从中看出了与骇飞的相似之处。“机器人。”放牧者低声说出这

归

根结底，我们在欧特克将原型科幻视为一种工具，它帮助我们探讨我们当下正在搭建的技术会如何影响未来，以及科幻可能会对我们搭建的技术产生何种影响。凭借讲述故事的力量，我们正在创建一个足够逼真的空间，使技术专家和消费者都能参与进来，发动思考。C

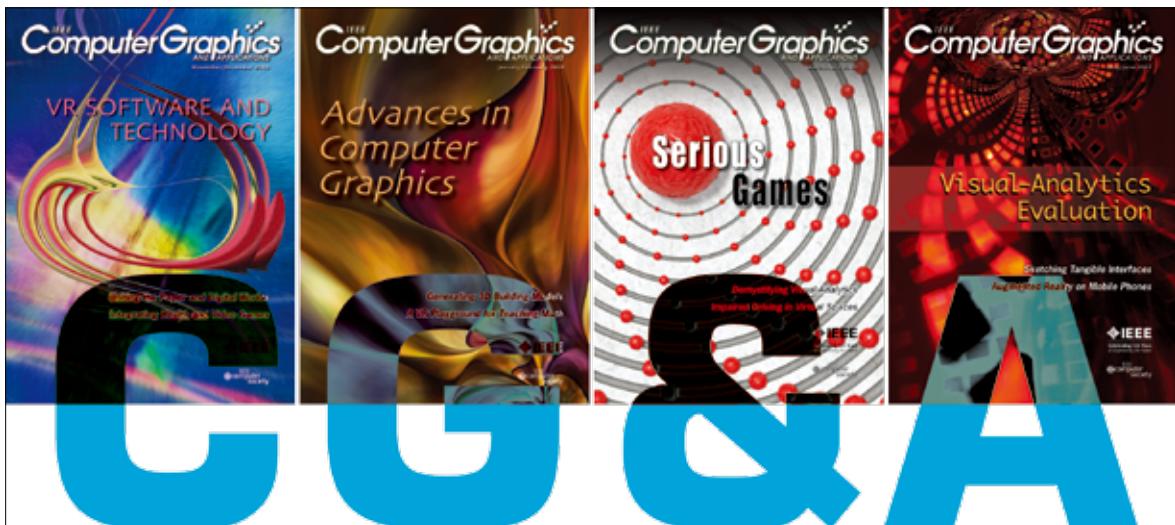
伊万·艾瑟顿是欧特克公司的高级研究工程师。他的联系方式：evan.atherton@autodesk.com。

个古老的词。大厅在黑暗中低声重复着她的话。机器人。放牧者认为，这是一个肯定的答复。

机器都架在倾斜的支架上，方向奇特。一只臂，一只手。没有眼睛。无法说话。最糟糕的是，它们都被固定在原地。她的骇飞灵活敏捷，充满好奇，在漫长的电子生涯中可以凭自己的意愿移动。它们生来就要跑跳，建造，注定要以合金和塑料为食，再将这些材料铸造成为它们共同构想出的事物。一言以蔽之，骇飞生来具有

思考能力。它们不仅拥有自己的思维，也拥有彼此的思维。它们是自由的，可以学习、分享和思考。

尽管放牧者的世界可能永远也不会成真，但探索她与骇飞的关系使我们能够以批判性的眼光看待我们迈向自动化的道路，考虑为了提高人机合作效率所需的工具，确保人类在未来所发挥的作用。正如亚历克斯·麦克唐威尔在该书前言中所说：“故事不是毫无意义的，它能够改变我们对工作方式的思考方式。”



《IEEE计算机图形及应用》(IEEE Computer Graphics and Applications, 简称CG&A)把计算机图形学领域的理论和实践联系在一起。《IEEE计算机图形及应用》提供了包括从某个特定算法到全系统实现在内的同行评议的深度报道。它为那些处于计算机图形技术前沿的人们提供了必不可少的资料。无论他们处于商界还是艺术界，这本杂志都能让他们受益。

请点击：www.computer.org/cga



2016 年全国社交媒体处理大会介绍

文 | 中国中文信息学会社会媒体处理专业委员会

2016 年10月29-30日,由中国中文信息学会社会媒体处理专委会主办,江西师范大学计算机信息工程学院承办的第五届全国社会媒体处理大会(SMP 2016)在南昌市江西师范大学成功召开。大会专注于以社会媒体处理为主题的科学研究,为传播社会媒体处理最新的学术研究与技术展示提供了一个广泛交流的平台,大会旨在构建社会媒体处理领域的产学研生态圈,成为中国乃至世界社会媒体处理的风向标。

本次大会得到了国内外研究人员和业界人员的广泛关注,共有来自全国各地的400多位学者,包括清华大学、北京大学、哈尔滨工业大学、复旦大学、中科院、社科院等等。同

时,本次会议也得到了国内外多家知名企业赞助,包括钻石赞助单位:腾讯科技(深圳)有限公司、仟传网络科技(上海)有限公司;金牌赞助单位:北京拓尔思信息技术股份有限公司、北京国双科技有限公司;银牌赞助单位:科大讯飞股份有限公司、北京微众文化传媒有限公司;铜牌赞助单位:上海小零网络科技有限公司、北京宏博知微科技有限公司等。

10月29日上午,第五届全国社会媒体处理大会开幕仪式在江西师范大学音乐艺术广场举行,由大会程序委员会主席、计算机信息工程学院院长王明文教授主持,江西师范大学副校长张艳国教授致大会开幕辞,中国中文信息学会副理事长、秘书长孙乐研究员致辞,他充分肯定了社会媒体处理专委会

的相关工作，并提出了许多建设性意见指导专委会的未来发展。同时，在开幕式上，社会媒体处理专委会主任刘挺教授介绍了社会媒体处理专委会一年来的各项工作，大会程序委员会主席林鸿飞教授介绍了SMP 2016的组织、宣传、论文出版等工作。

本次大会共举办6场特邀报告，邀请了汪小帆教授、马少平教授、黄萱菁教授、袁晓如教授以及沈华伟博士、刘知远博士等数位国内外知名的社会媒体处理领域专家，围绕社会物理学、社会化推荐、社会媒体可视化、深度学习与社会计算等主题，进行了精彩报告，为与会者开阔了研究视野、激发了科研灵感、拓宽了学术思路。会议PPT将陆续在网站上发布：
<http://www.cips-smp.org/smp2016>。

本次大会收到来自包括清华大学、哈尔滨工业大学、复旦大学、大连理工等数十所高校及研究机构的论文投稿，共计109篇，分四组进行报告。其中，英文论文由Springer出版，11月30日前可在大会网站上<http://www.cips-smp.org/smp2016/index.html>点击“英文论文集”即可下载。被录用的优秀英文文章将被推荐至SCI杂志《Science China》F版(SCI)、《Tsinghua Science and Technology》自然版(SCI)上。中文论文将被推荐至《中国科学》、《中文信息学报》。

本次大会设立多个专题论坛就社会媒体处理当下的研究热点展开讨论，分别为数据挖掘(SMP-KDD)论坛、情感分析论坛、计算社会科学论坛以及表示学习论坛等。包括秦兵教授、梁玉成教授、熊辉教授、谢幸研究员、邱锡鹏博士、杨洋博士等二十余位专家分享了近期科研成果。几个专题论坛吸引了大量学者，特别是年轻学者与在读博士参与讨论，观点交锋异彩纷呈，奇思妙想层出不穷，很多青年学者表示收获颇丰。

另外，本次大会举办了首届技术评测竞赛——“微众杯”技术评测，本次评测由蒋盛益教授、万怀宇博士组织，由北京微众文化传媒有限公司冠名赞助。本次技术评测的任务是利用给定的新浪微博数据来进行微博用户画像，吸引了超过100家参赛队伍报名参赛，最终来自哈尔滨工业大学深圳研究生院的HLT_HITSZ队斩获冠军，多支队伍在SMP2016大会上作技术评测报告。



10月30日下午，第五届全国社会媒体处理大会举行闭幕仪式，由程序委员会主席林鸿飞教授主持。闭幕式上，江西师范大学计算机信息工程学院院长王明文教授宣布了优秀论文的获奖名单，并为获得最佳论文的作者颁奖。

同时，数据分享工作组复旦大学的张奇博士在会上分享了由“知微公司”提供的微博事件数据库以及复旦大学的Twitter用户与关系数据库，包含400万用户信息、3.4亿条Twitter以及2263万用户关系，参会代表免费下载。这些数据为相关学者研究社会媒体处理相关问题提供了重要的研究资源。

最后，由社会媒体处理专委会秘书长唐杰老师为大会进行总结，“第六届全国社会媒体处理大会”将于2017年在北京举行，将由中科院计算所承办。

2016 BYTE CUP

International Machine Learning Competition

国际机器学习竞赛

今日头条与IEEE联手举办大数据竞赛

TOUTIAO AND IEEE JOINTLY ORGANIZE THE BIG DATA CONTEST.

为 **5.5** 亿头条用户寻找问答答案贡献者
LOOKING ANSWER CONTRIBUTORS FOR 550 MILLION TOUTIAO USERS.

总奖金金额

10,000 美元

40名IEEE会员资格、100名中国计算机学会会员资格

参赛网址 LAB.TOUTIAO.COM

8月15日: 比赛上线

11月11日: 发布测试数据

11月20日: 比赛截止, 计算排名

11月21-22日: 公布比赛排名

12月初: 颁奖活动

IEEE中国代表处



今日头条
toutiao.com



HOSTS: IEEE-CHINA TOUTIAO

CO-ORGANIZER: TSINGHUA UNIVERSITY KNOWLEDGE ENGINEERING GROUP





保持联系。

无论你在哪里，都能紧随IEEE计算机协会的脚步。

在Twitter、Facebook、Linkedin和YouTube上关注我们。



@ComputerSociety, @ComputingNow



facebook.com/IEEEComputerSociety
facebook.com/ComputingNow



IEEE Computer Society, Computing Now



youtube.com/ieeecomputersociety