量子计算，人工智能与区块链

2018年8月

张首晟

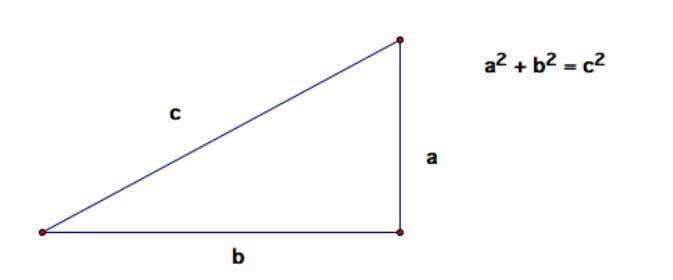
正反对立的世界观

我们似乎生活在一个充满正反对立的世界：有正数必有负数，有存款必有负债，有阴必有阳，有善必有恶，有天使必有恶魔。

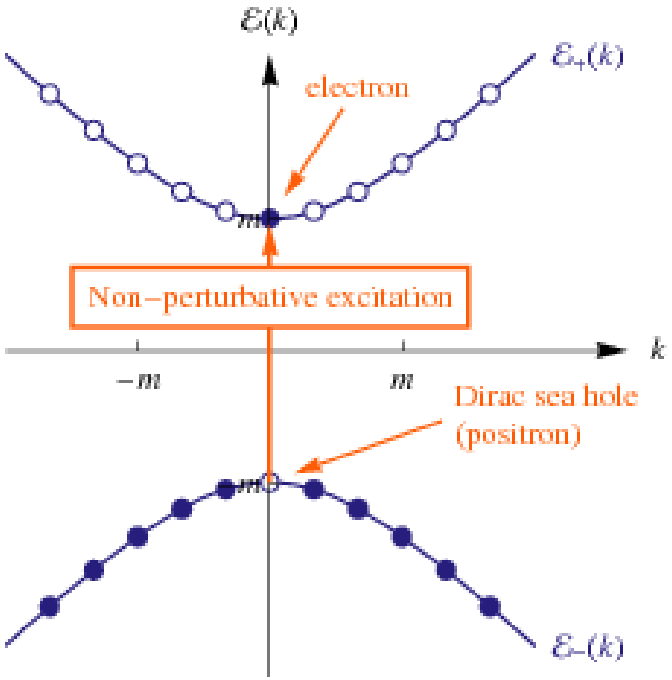
狄拉克方程

1928年，伟大的理论物理学家狄拉克(Dirac) 作出惊人的预言：宇宙中每一个基本粒子必然有其相对应的反粒子。

$$E(p) = \pm\sqrt{(pc)^2 + (mc^2)^2}$$

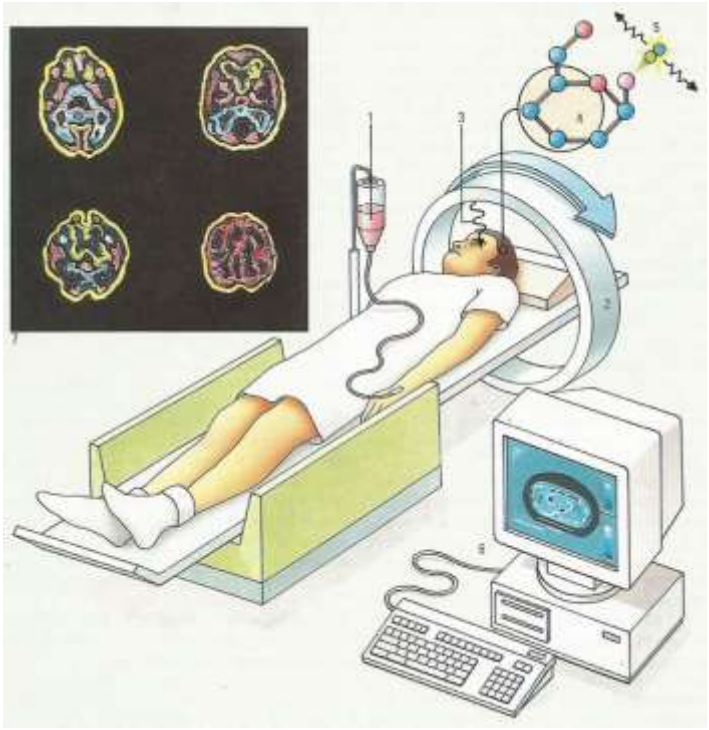


狄拉克海和反粒子



几年之后，正电子果然在宇宙射线中被发现，验证了有史以来最伟大的理论预言之一。

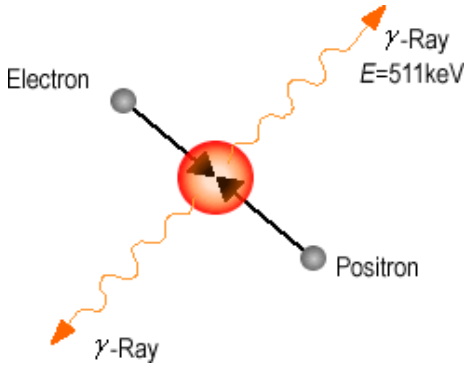
生活应用：正电子发射断层扫描



目前，正电子被广泛应用到人类生活之中，医学影像
技术PET (Positron Emission Tomography, 正电子发射断层扫描) 就是其中之一。

天使与魔鬼

当一个粒子遇上它的反粒子时，根据爱因斯坦$E = mc^2$的质能公式，它们会相互湮灭从而将所有质量释放出成能量。Dan Brown的小说及其电影《天使与魔鬼》就描述过这样的正反粒子湮灭爆炸的场景。



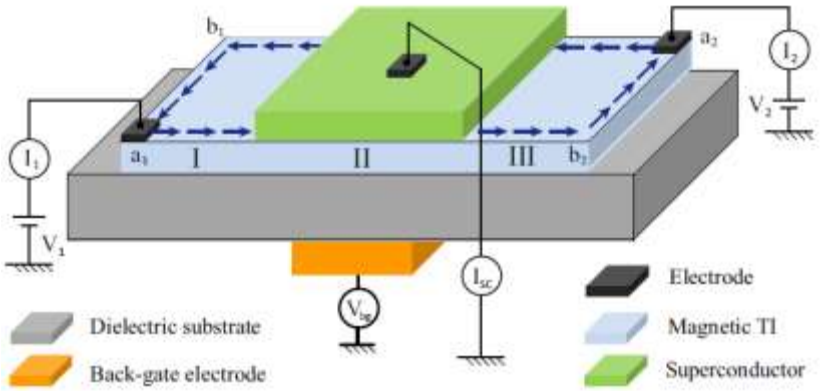
Majorana和他的费米子

从此以后，宇宙中有粒子必有其反粒子被认为是永恒不变的真理，但是会不会有这样一类没有反粒子的粒子，或者说它们自身就是自己的反粒子？1937年，也就是整整八十年前，伟大而神秘的意大利理论物理学家Ettore Majorana 猜测有这样神奇粒子的存在，这也就是我们今天所称的Majorana费米子。从那开始，寻找这一神奇粒子也就成了物理学中许多领域研究工作的崇高目标。

一份梦寐以求的表单

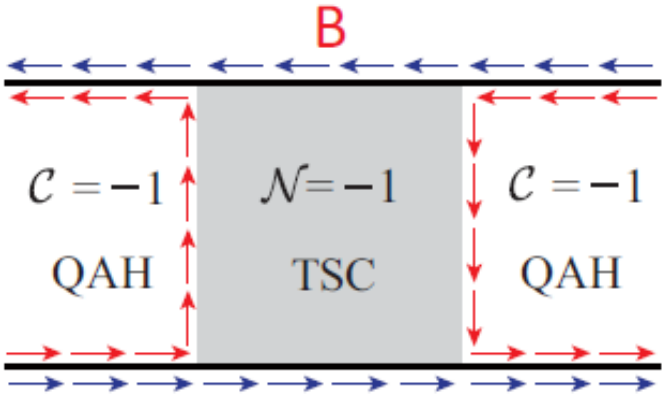
物理学中有一份表单, 囊括了那些人类梦寐以求的神秘粒子，其中就有希格斯波色子（也被称为上帝粒子，最近在欧洲粒子加速器中被发现）、引力子、磁单极、暗物质和Majorana费米子。相较其他粒子而言，Majorana费米子或许更加神秘，因为Majorana本人在文章泄露天机之后不久就失踪而从此销声匿迹了。

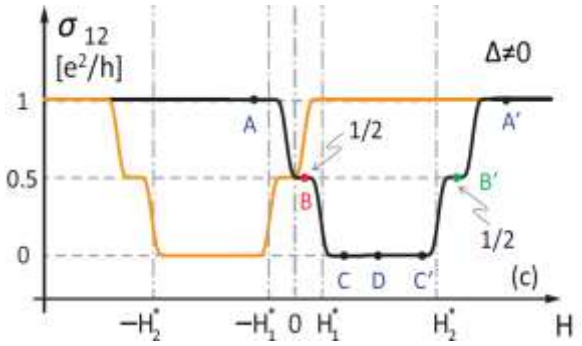
张首晟研究组预测：Where?



2010到2015年期间，张首晟与其团队连续发表三篇论文，精准预言了在哪里能够找到Majorana费米子，继而指出哪些实验信号能够作为铁证如山的证据。他们预言手性Majorana费米子存在于一种由量子反常霍尔效应薄膜和普通超导体薄膜组成的混合器件中。

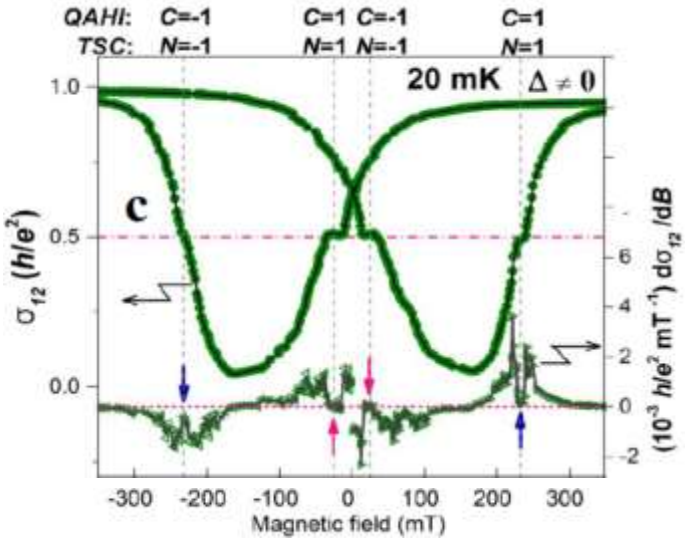
张首晟研究组预测：What?





在以往的量子反常霍尔效应实验中，随着调节外磁场，反常量子霍尔效应薄膜呈现出量子平台，对应着1、0、-1倍基本电阻单位e^2/h。当把普通超导体置于反常量子霍尔效应薄膜之上时，临近效应使之能够实现手性Majorana 费米子，相应的实验中会多出全新的量子平台，对应 1/2 倍基本电阻单位e^2/h。这半个基本电阻来源于Majorana费米子没有反粒子，所以某种意义上它可以视为半个传统粒子。所以，这多出来的半整数量子平台就提供了有力的证据，证明在时空中传播的手性Majorana费米子的存在。

实验观察

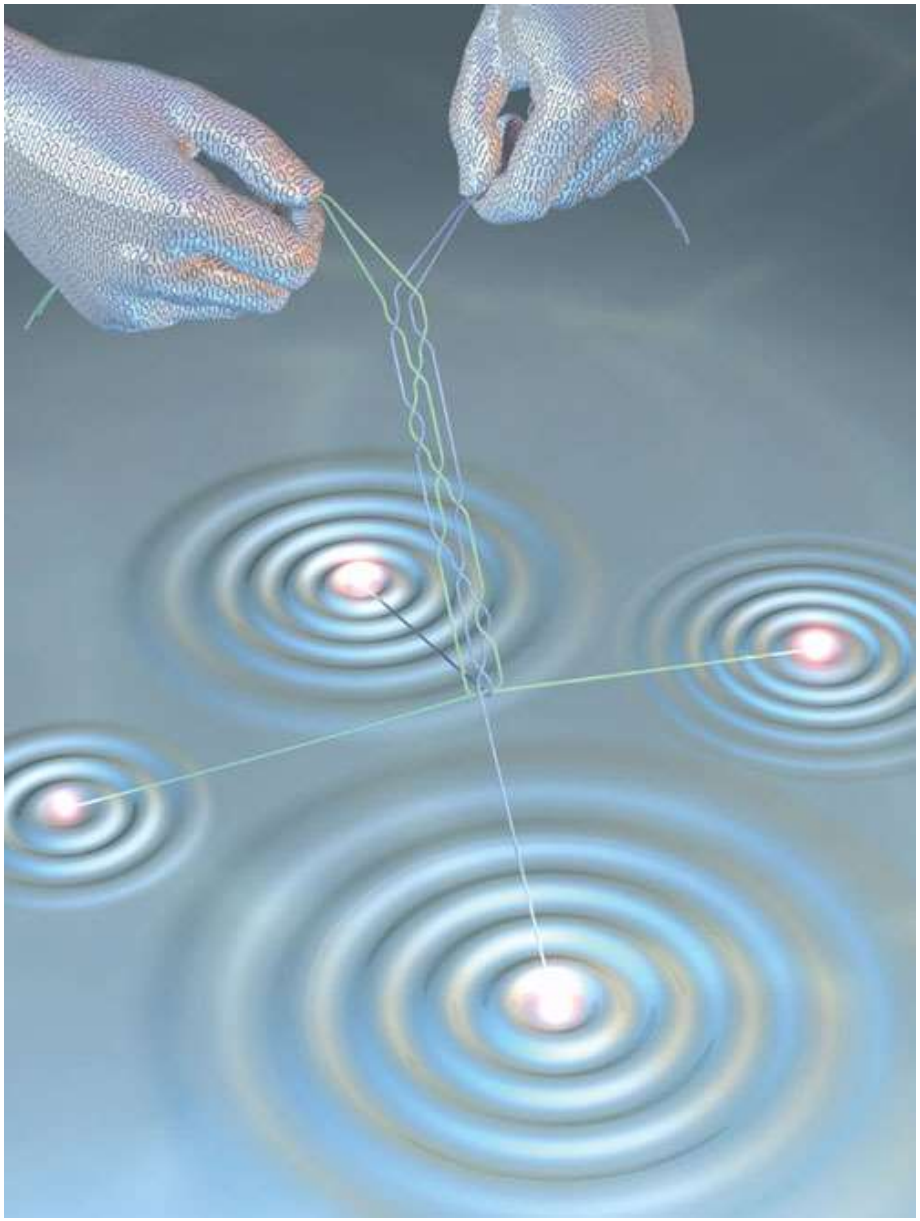


根据这一理论预言，来自UCLA, UC Davis, UC Irvine的实验团队与斯坦福大学张首晟教授的理论团队紧密合作，最终在所提出的器件中实验上发现了手性Majorana费米子。这一重大发现已发表在这一期的科学杂志上。

天使粒子

手性Majorana费米子的发现为持续了整整80年对这一神秘粒子的搜索画上了圆满的句号。类比Dan Brown描述正反粒子湮灭爆炸的小说《天使与魔鬼》，张首晟提出这一新发现的手性Majorana费米子应该称为天使粒子：我们发现了一个完美的世界，那里只有天使，没有魔鬼。

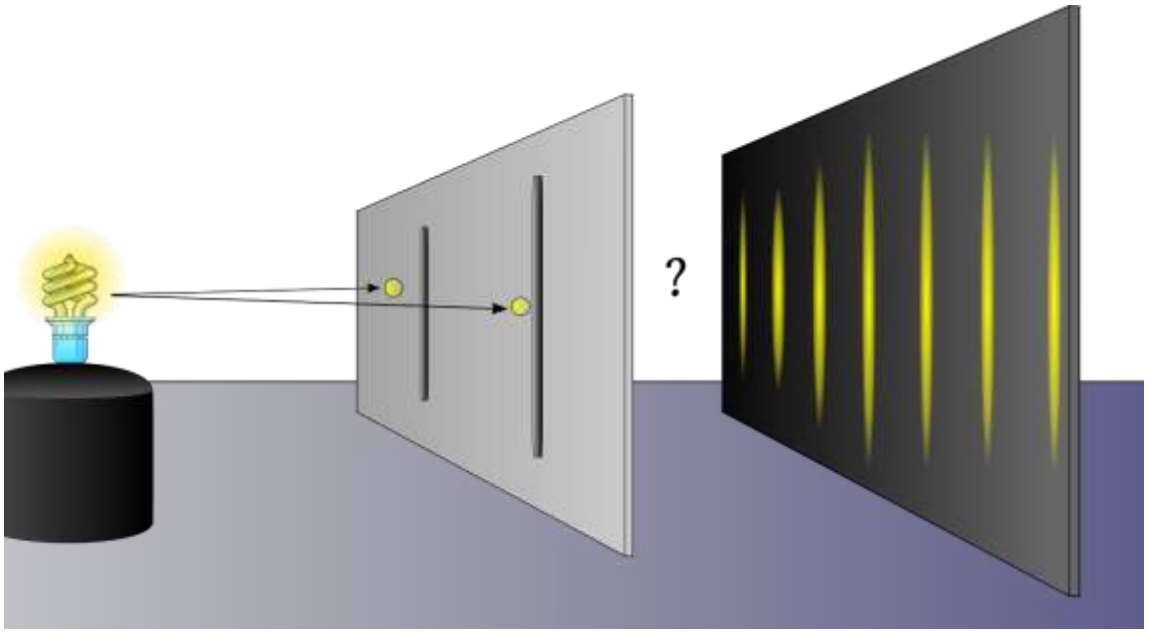
拓扑量子计算机



15 = 3 x 5

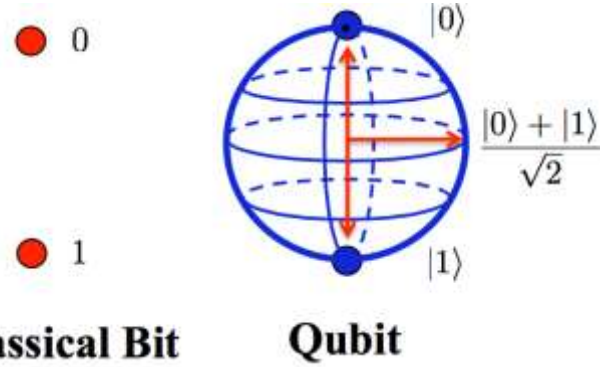
154750274720472640572930348473745639384723937392273646483629374393272932729272363292729282028273937 3 = ?

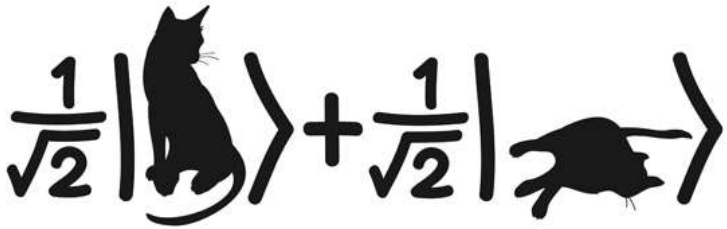
量子世界本质上是平行的



量子世界本质上是平行的，一个量子粒子能够同时穿过两个狭缝。所以量子计算机能够进行高度并行的量子计算，远比经典计算机有效。

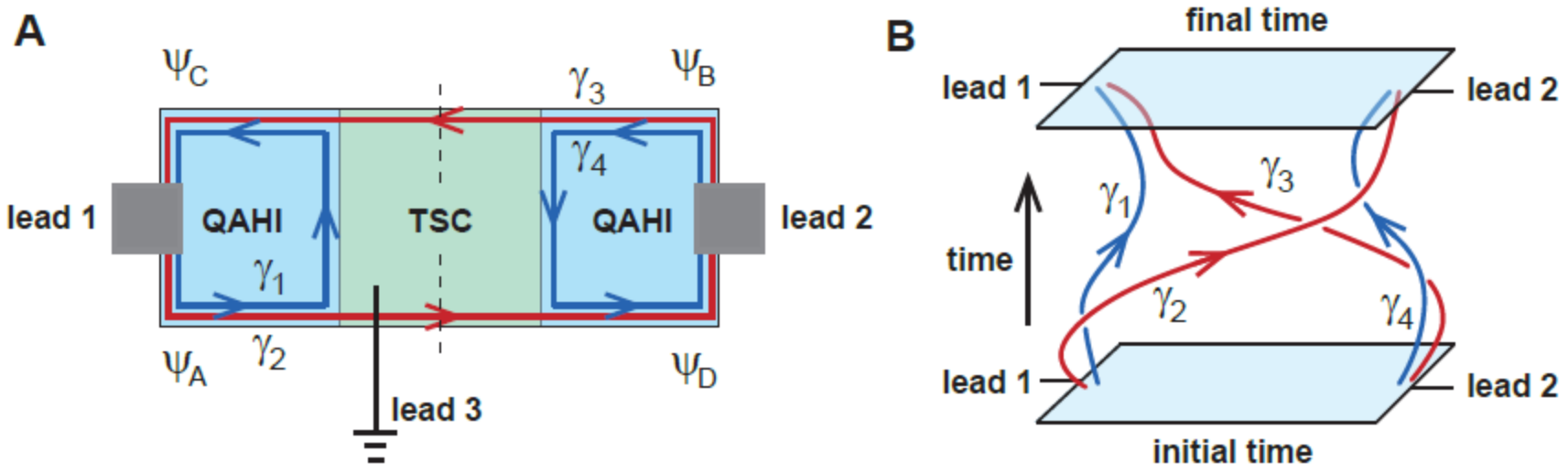
量子比特(qbit)





然而，一个量子比特的信息非常难以存储，微弱的环境噪声都能够引起退相干从而毁灭其量子特性。

基于"天使粒子"的拓扑量子计算机



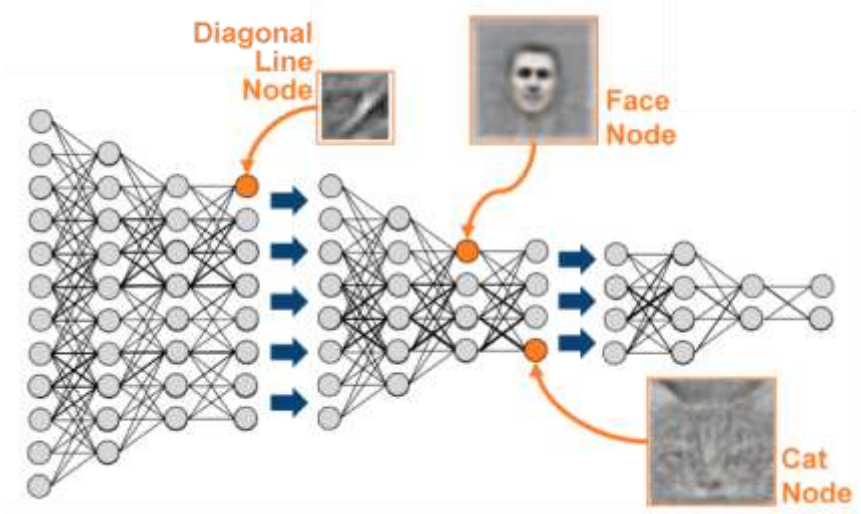
我们最近发现手性Majorana费米子，也称为天使粒子。粒子的自然传播导致非对易的编辫。这样信息就能够非局域的存储，因而不受局域的微扰影响！

人工智能，为何是现在？

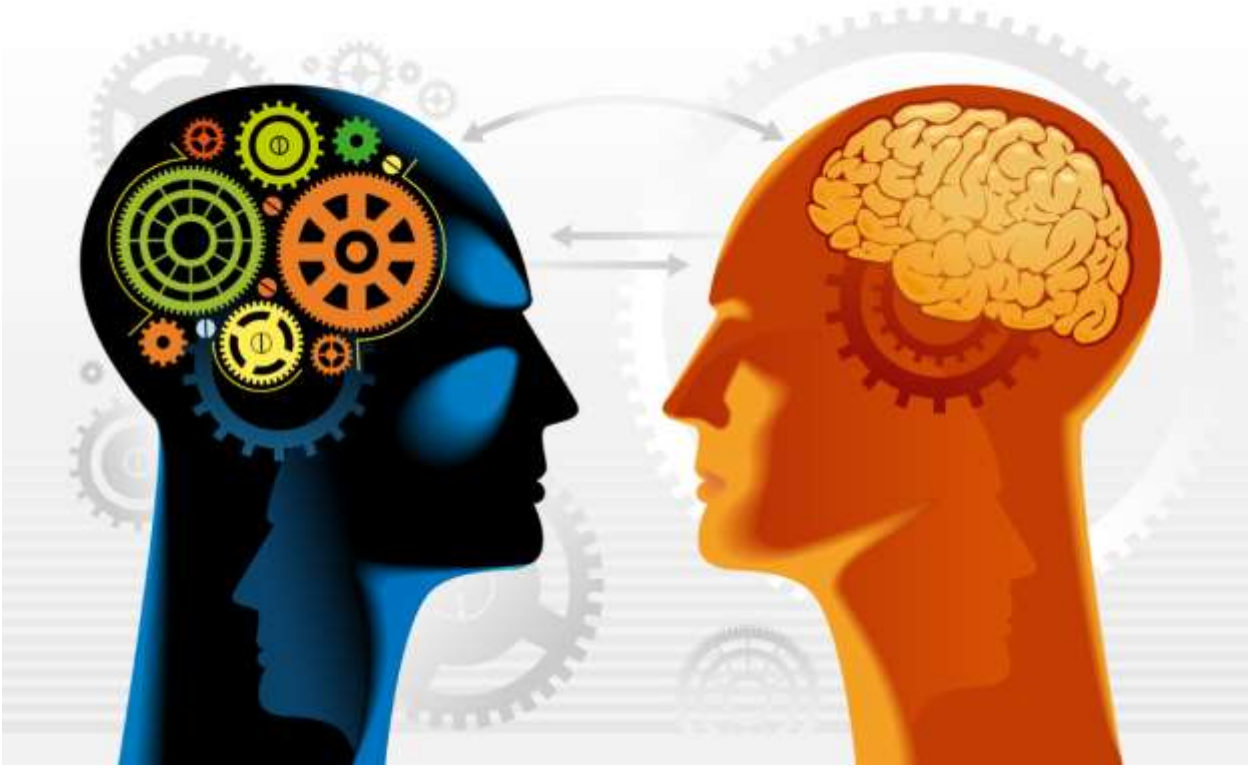
- 我们处在人类历史的特殊时代。作为地球上最智能的物种，人类在过去的十万年间不断进化，但我们正目睹着比人类更为智能的、新的人工智能物种的出现！
- 人工智能的基本概念早已有之，但为什么我们“现在”才看到如此快速的发展？
- 人工智能的爆发源于三个重要趋势的神奇汇聚：
  - 摩尔定律所描述的计算能力的指数增长
  - 互联网和物联网的爆发性增长所产生的海量数据
  - 智能算法的快速发展

神经网络对人脑的模仿

- 飞行的数学原理是流体动力学 ⬆
- 神经网络的数学原理是什么？ ⬇



机器智能何时超越人类？图灵测试的误导



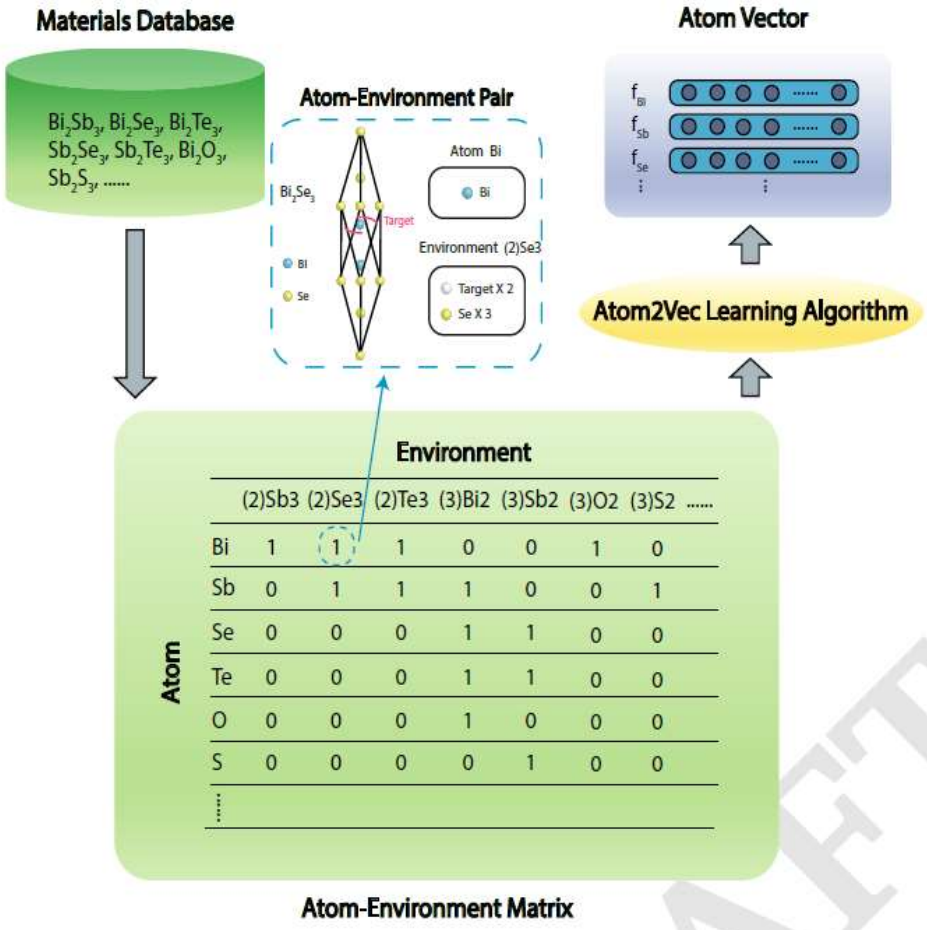
- 图灵测试的误导：机器无法也没有必要实现对人脑的完全模仿
- 更深入的疑问：机器能比人脑更好地发掘自然和数学规律吗？

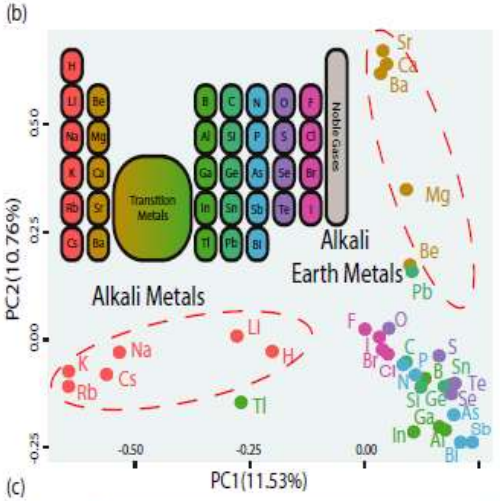
利用人工智能发现元素周期表

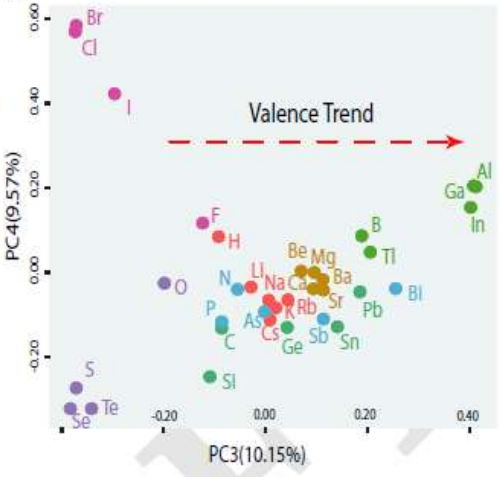
Atom2Vec: learning atoms for materials discovery

Quan Zhou[a], Peizhe Tang[a], Shenxiu Liu[a], Jinbo Pan[b], Qimin Yan[b], and Shou-Cheng Zhang[a,c,1]

[a]Department of Physics, McCullough Building, Stanford University, Stanford, California 94305-4045, USA; [b]Department of Physics, Temple University, Philadelphia, Pennsylvania 19122, USA; [c]Stanford Institute for Materials and Energy Sciences, SLAC National Accelerator Laboratory, Menlo Park, California 94025, USA





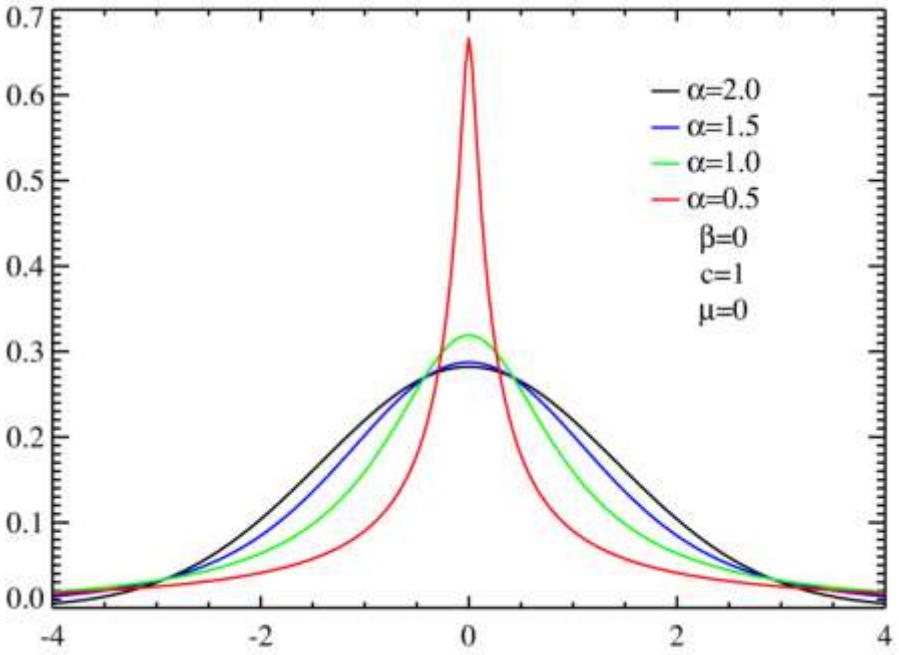


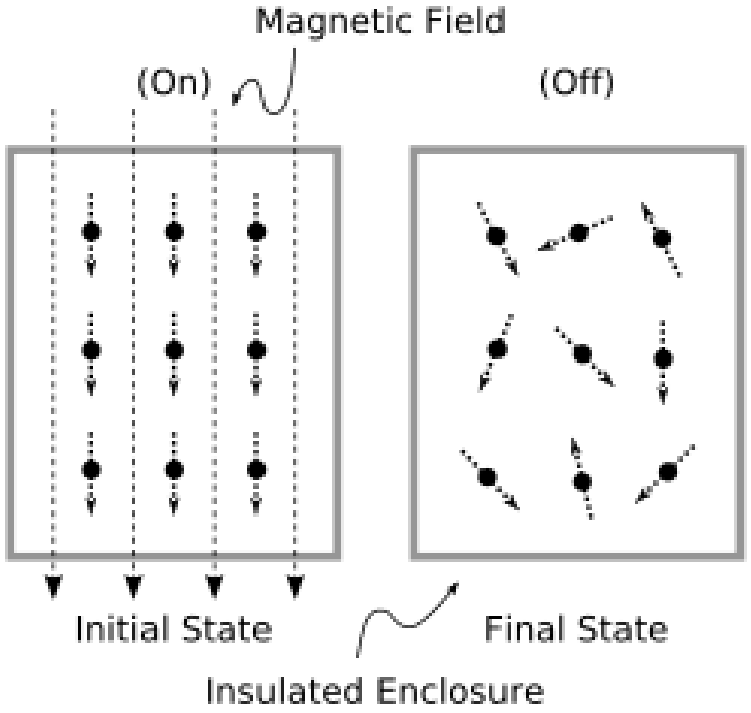
Centralization vs decentralization

分久必合，合久必分

- In the era of circuit switching, AT&T becomes the centralized monopoly of network resources.
- Packet switching based on TCP/IP leads to a decentralization network, breaking the monopoly of AT&T.
- Fragmentation of web content leads to the centralized content platforms like Google and Facebook.
- Blockchain technology leads to a new wave of decentralization with self-organized p2p trust and consensus based on math.

为何共识具有内在价值?





- 高度共识意味着低熵。然而，热力学第二定律告诉我们整个系统的熵必然趋于增加。人们可以通过把多余的熵排放到其他地方，从而减少子系统的熵。

自我组织的区块链共识

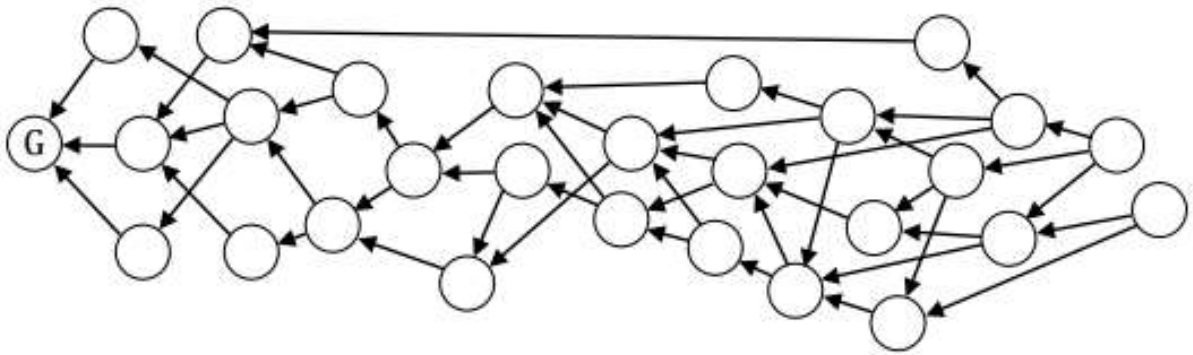
- 在分布式系统中，共识无法通过一个主决定性算法实现: Fisher-Lynch-Patterson 定理.
- 一个主决定性算法可以像麦克斯韦妖一样，不排出熵而实现共识。Fisher-Lynch-Patterson 不可能定理原则上等价于热力学第二定律。
- 区块链系统可以通过计算数学哈希函数来达成稳定的共识，它通过工作量证明排出额外的熵，从而实现低熵的共识状态。

区块链和人工智能的共生

- 人工智能需要数据，但是数据往往被中心化平台垄断，因而阻碍创新。从这种意义上人工智能有所欠缺。
- 加密经济学创造了一个对于数据提供者有正确激励机制的数据市场。人工智能能够依赖这个数据市场起飞。

我们信仰数学

- 基于椭圆曲线的公钥/私钥体系，代理再加密。
- 加密哈希函数。
- 零知识证明：**Zk-snark and Zk-stark**。
- 安全的多体系计算，微分隐私。
- 形式验证。
- 同态加密。
- **Dag,** 有向非循环图**:** 树结构上的货币 **“**摇钱树**”**



加密经济学实现社会福利

- 人工智能需要数据，极端情况在机器学习中最有价值。因此，在一个公平的数据市场中，数据的价值是通过互熵来衡量。
- 在我们的社会中，有些少数派会遭受歧视，然而在加密数据市场中，他们提供的数据会最受重视。因此，加密经济学能够抵消当前社会经济学中的各种偏见。
- 丑小鸭也能变成白天鹅！

区块链技术展望

区块链扩展：DAG

稳定货币

绿色环保区块链：Chia

网络基础设施的区块链化

区块链和人工智能的共生

区块链身份和信用管理：Ontology

基因组学和生物医疗的数据市场：Vivo

一带一路加一链

区块链资产证券化

用第一性原理做投资

丹华资本

科学的最高志向: 简单和普世

我们生存的周围世界复杂而多变，但若是能够对万物寻根溯源，我们就可以用简单对抗复杂，赢得效率的提高：**Google Page Rank, Deep Learning, Barefoot**

当理解并使用第一性原理时，我们就能够创新地进行新联通，成为中央路由器

丹华资本也期待我们的创业家从第一性原理出发思考问题

让我们重回信封背面的故事！