量子计算与量子信息心得

16337341 朱志儒

很荣幸能够听邱道文教授为我们讲解新型的计算--量子计算与量子信息。

从 Church-Turing 命题看计算机科学的发展：一个问题若能被计算机解决的当且仅当它能被 Turing 机解决；概率 Turing 机能有效地模拟任意现实的计算模型（平方根模素数）；量子 Turing 机能有效地模拟任意现实的计算模型（大数分解）。

量子计算机——以量子力学原理进行计算的计算机；量子信息与量子计算是信息论和计算机科学与量子物理交叉的学科。研究量子计算的基本动机：计算速度：大数分解、数据搜索；安全性：量子密码；物理实现性：离子阱、光学、超导、腔量子电动力学、核磁共振、半导体等十余种。

在 1994 年 Shor 证明了大数分解问题可以被量子图灵机在多项式时间内解决，该问题在经典计算机下的难解性是 RSA 公钥密码系统之所以存在的理论依据。

安全通信：利用 BB84 协议安全生成秘钥；基于 Heisenberg 测不准原理和量子非克隆定理，任何窃听将被发现；已得到商业应用。

数据搜索：假设你把东西遗失在已知的 N 个可能地点，经典计算大致需要搜索 N/2 个地点才能找到，Grover 的量子搜索算法可在 O($\sqrt{N}$)内完成，在大数据等问题中有重要应用。

国际上的重视：美国国家安全局：对于量子计算，布防刻不容缓；2015 年 Google、NASA 和宇宙空间研究协会合办著名的量子人工智能实验室；Google 量子计算梦：10 年后机器学习全部量子化；IBM 向公众开放量子计算平台 Quantum Experience；加拿大 D-Wave 于 2011 年 5 月 11 日正式发布了全球第一款商用型量子计算机“D-Wave One”；2017 年 1 月，D-Wave 公司推出 D-Wave 2000Q，2000 个 qubit 构成，可以用于求解最优化、网络安全、机器学习、和采样等问题；2017 年 5 月，10 比特光量子计算机即将到 20 比特；中国科学院-阿里巴巴量子计算实验室于 2015 年 7 月 30 日在上海成立。实验室将结合阿里云在经典计算算法、架构和云计算方面的技术优势，以及中科院在量子计算和模拟、量子人工智能等方面的优势，颠覆摩尔定律，探索超越经典计算机的下一代超快计算技术；2016 年 8 月 16 日，中国造量子卫星“墨子号”发射成功。