面向计算机爱好者的量子信息

吕铭

2016 年 6 月 11 日金枪鱼之夜

物理系毕业狗

量子态是什么

量子态（量子比特）是什么

- 经典的比特: “0” 或者 “1”
  - 以概率 p 为 “0”, $1-p$ 为 “1”
- 量子的比特: $|\psi\rangle = c_0\,|0\rangle + c_1 e^{i\varphi}\,|1\rangle$
  - 相位 φ 和波
  - $|0\rangle$ 的概率 c_0^2, $|1\rangle$ 的概率 c_1^2
    - 归一化 $c_0^2 + c_1^2 = 1$
    - $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
  - $(|0\rangle + |1\rangle)/\sqrt{2}$ 的概率? —— 线性代数
  - $\langle\psi| = (|\psi\rangle)^\dagger$, $p = |\langle\psi|\psi'\rangle|^2$

$$|\psi\rangle \equiv \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

一些概念

- 纯态 $|\psi\rangle$: 包含全部信息 (Bell 不等式)
- 混合态: 经典概率与量子态合在一起的描述.. 通常 “退相干” 到 (完全) 混合态
- 直积态: 两个或多个比特简单放在一起的状态

$$|\psi\rangle = |0\rangle\,|0\rangle \equiv |0\rangle \otimes |0\rangle$$

- Bell 态与最大纠缠态

$$|\Psi^{\pm}\rangle = |0\rangle\,|0\rangle \pm |1\rangle\,|1\rangle\,; \quad |\Phi^{\pm}\rangle = |0\rangle\,|1\rangle \pm |1\rangle\,|0\rangle$$

- 测量与态的坍缩

所以具体一点是什么

- $|0\rangle$ 和 $|1\rangle$ 具体是什么?
  其实大家还在探索中, 可能的答案包括:
  1. 超导电路 (现在最火的)
  2. 晶体缺陷 (NV-色芯)
  3. 离子阱 (存储)
  4. 光子 (偏振) 与非线性光学
  5. 核磁共振 (NMR)
  6. 拓扑序
  7. .....

- 骗! 经! 费!
- 夸大宣传
- 困难
  1. 相干时间
  2. 可操作性
  3. 可拓展性
- 大体上说我们还在做二极管的阶段

量子通信与量子密钥分发

量子纠缠 (Entanglement)

- 超出经典相关性的量子关联 (Bell 不等式)
- Bell 态是最大纠缠态:
  合在一起是纯态, 分开看是完全混合态
- 没有相互作用, 不能超光速通信!!!
- 对于量子传态 (teleportation) 和量子中继有重要作用
- 涉及基础物理的解释 (神棍...)
- 潜在的保密计算

对于测量的限制

- 测量一定伴随干扰
  如果某一次测量的结果与态有关, 那么测量后态一定发生改变
- 不可克隆原理
  没有办法从 $|\psi\rangle$ 得到 $|\psi\rangle\,|\psi\rangle$
- 不可分辨原理
  如果 $|\psi_1\rangle$ 和 $|\psi_2\rangle$ 不正交, 那么对于单个比特没有办法完美地区分二者
- 密钥分发: BB84 协议 (Bennett and Brassard, 1984)

量子通信/量子密钥分发

- 经典信道与量子信道共同使用
- 主要（唯一）优势是物理规律保护的安全性
- 最常见的是借助光纤/自由空间光子
- 主要困难在于空间衰减和单光子源效率
- 已经有产品了！（潘建伟，济南试验网）
- 卫星试验中… 光纤量子通信 50km 中继

量子计算

量子门 (Quantum gate)

- 描述量子比特的演化: 幺正算符 ($UU^\dagger = I$)
- 通用量子门集合:
  - 对于单量子比特, 任意量子门可以用 2 个基本门的组合来近似, 门序列长度 $\mathcal{O}(-\log^c \epsilon)$ (ϵ 是近似误差)
  - 对于 N 量子比特, 只需要增加对于两两产生纠缠的量子门 W_{ij}

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \quad T = \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\pi/2} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/8} \end{pmatrix}$$

$$\mathtt{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \mathtt{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

量子算法

- Grover 搜索算法: 已知函数 $f : \{1, \cdots, N\} \mapsto \{0, 1\}$, 假定 $f(n) = 1$ 数量 S 极少, 寻找这样的 n.
  - 时间复杂度: $\mathcal{O}(\sqrt{N})$ (经典算法 $\mathcal{O}(N)$)
  - 从 $|\psi\rangle = (\sum_n |n\rangle)/\sqrt{N}$ 出发, 经过 $\mathcal{O}(\sqrt{N/S})$ 个门, 以几率 $p \geq 1 - S/N$ 成功

  已经证明, $\mathcal{O}(\sqrt{N})$ 是量子力学范围内能做到的最好 (意味着无法解决 NP 问题)
- Shor 质数分解算法: 来源于数论中质因数和取余函数的周期性的关系,
  - 时间复杂度: $\mathcal{O}(L^3)$ (经典算法 $\mathcal{O}(\mathrm{e}^{L^{1/3}\log^{2/3} L})$)
- BQP (bounded error quantum polynomial) 问题

其他

- “异端”
  - 系综量子计算
  - D-Wave: 量子退火机, 复杂度用 $\mathcal{O}(f(\Delta E))$ 描述
  - 拓扑量子计算: ???
- 量子纠错
- 如果量子计算机做不出来怎么办?
- 如果量子计算机做出来怎么办?
  - 脆弱的存储, 复杂的控制
  - 潜在稍强的计算能力, 潜在更好的功耗控制

The End...

Thank you for listening!

Q & A?