量子计算

毛昕渝 2021/11/29

进入量子世界

不从“薛定谔的猫”讲起

概率：量子世界的入口

- 如果有N种可能的结果，我们可以把这些事件的概率写成一个N维实向量：
$$p = (p_1, p_2, \dots, p_N) \in \mathbb{R}^N.$$
- 显然，我们要求$p_i \geq 0, \forall i$, 并且 $\sum_{i\in[N]} p_i = 1$.
  - 从向量的角度，后一个要求等价于 $\|p\|_1 = 1$.
- 如果换成2-范数呢？
  - 考虑一个比特的情况：

1-范数

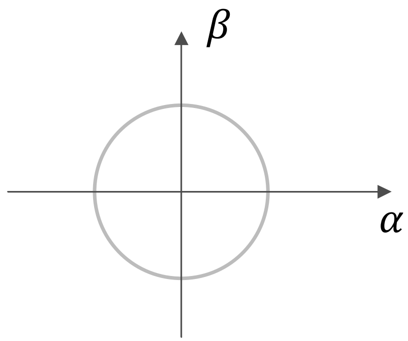
以a的概率等于1，
以b的概率等于0。

$$a + b = 1$$

2-范数

以α^2的概率等于1，
以β^2的概率等于0。

$$\alpha^2 + \beta^2 = 1$$



如何改变世界?
如何操作一个比特?

- 一个操作可以看成给概率向量左乘一个矩阵。
- 不管如何操作，所有可能情况的概率之和始终等于1.
  - 我们的操作必须保持范数不变!
  - 保持1范数不变→随机矩阵 (每列和为1的矩阵)
    - 例如: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1-p \\ p \end{pmatrix} = \begin{pmatrix} p \\ 1-p \end{pmatrix}$
  - 保持2范数不变→标准正交矩阵
    - 如果我们更大胆一些，允许α,β取复数值的话…→酉矩阵

2-范数

以α^2的概率等于1，
以β^2的概率等于0。

$$\alpha^2 + \beta^2 = 1$$

Dirac记号

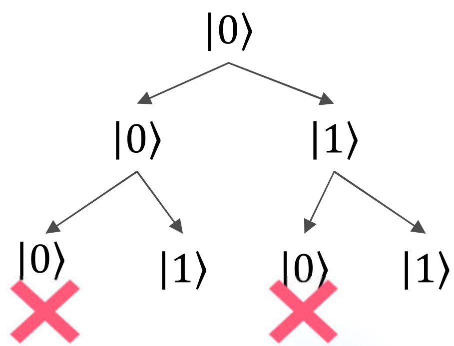
记$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$,

则$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$记为 $\alpha|0\rangle + \beta|1\rangle$.

量子干涉

- 考虑（对单比特的）如下操作：$U=\begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix}$.
- $U|0\rangle=\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ “抛一枚硬币”
- 神奇的事情：$\begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}=|1\rangle$.
  - 随机+随机 = 确定结果?
  - 有一些可能性互相抵消了！（相消干涉）

> “A good quantum computer algorithm ensures that computational paths leading to a wrong answer cancel out and that paths leading to a correct answer reinforce.”
>
> Scott Aaronson



还有其他世界吗?

- 考虑1范数，我们解释了经典世界
- 考虑2范数，我们进入了量子世界
- 3范数？4范数？p-范数?
- 限制：操作必须要保持范数不变
  - 平凡的变换：改变正负号，重新排列（基向量的）顺序
  - 定理：对于$p \geq 3$, 保持p-范数不变的线性变换只有平凡的变换。

虚与实
线性与非线性

- 为什么要考虑复数?
  - 复数域$\mathbb{C}$ 有何特别之处?
  - 复数域$\mathbb{C}$是代数封闭的。
- 为什么只考虑线性变换?
  - 如果允许非线性变换，量子计算将可以:
    - 高效解决NP问题
    - 超光速的信息传输

一半的操作

“连续性假设”

对于每一个合法的线性变换U，都存在一个合法的线性变换 V 满足$U = V^2$.

量子计算

BPP与BQP

带有一条“随机纸带”的图灵机

BPP的定义

设有判定问题 $f:\{0,1\}^* \to \{0,1\}$. $f \in$ **BPP** 当且仅当存在满足下列条件的概率多项式时间算法$\mathcal{A}$:

$$\forall x \in \{0,1\}^*,\ \Pr_{coin}[\mathcal{A}(x;coin) = f(x)] \geq \frac{2}{3}.$$

量子电路

一个量子电路C由一系列量子操作组成。如果电路C_n输入长度为n，则称$\{C_n\}_{n\in\mathbb{N}}$为一族量子电路。

BQP的定义

设有判定问题 $f:\{0,1\}^* \to \{0,1\}$. $f \in$ **BQP** 当且仅当存在满足下列条件的一族量子电路 $\{C_n\}_{n\in\mathbb{N}}$：

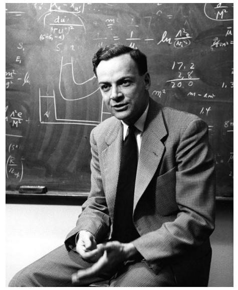
- $\forall n \in \mathbb{N}, \forall x \in \{0,1\}^n$, $\Pr[C_n(x) = f(x)] \geq \frac{2}{3}$.
- 存在一个多项式时间算法$\mathcal{A}$，当输入1^n时$\mathcal{A}$恰好输出C_n（的描述）。

BQP, BPP, P, 与 NP

指数时间内能解决的问题

- 定理. $\mathbf{BQP} \subseteq \mathbf{EXP}$.
- 定理. $\mathbf{BPP} \subseteq \mathbf{BQP}$.
- 猜想. $\mathbf{BPP} \neq \mathbf{BQP}$.
- 猜想. $\mathbf{BPP} = \mathbf{P}$.
- 量子计算机能解决更多问题!
  - Shor算法说明：$\text{FACTOR} \in \mathbf{BQP}$.
  - $\text{FACTOR} \in \mathbf{BPP}$? 大数分解问题是否存在多项式算法?
- 猜想. $\mathbf{NP}$ 不是 $\mathbf{BQP}$ 的子集.
  - 我们甚至不知道在$\mathbf{P} \neq \mathbf{NP}$ 的假设下如何证明这一猜想。

发展历程



- 1984年，费曼指出：很难通过经典计算机模拟量子力学；要做这样的模拟，我们需要建造量子计算机。
- 1985年，David Deutsch 给出了量子图灵机的定义。
- 1994年，Shor提出了大数分解的量子多项式时间算法。
- 1996年，Lov Grover 提出了Grover算法（量子搜索算法）。
- ……
- 2012年，法国科学家 Serge Haroche 与美国科学家 David Wineland 获诺贝尔物理学奖。
  - 获奖理由是“发现测量和操控单个量子系统的突破性实验方法”。

量子计算的物理实现（实验）

- 2019年10月：Google: 53个量子比特的量子计算处理器“悬铃木”
- 2020年9月：IBM公布其量子计算规划
  - 预计在2021年实现127量子比特，2023年实现1121量子比特。
  - 当地时间11月16日，IBM表示其“Eagle”（鹰）量子处理器已达到127量子比特，成为目前世界上操控量子比特数量最多的超导量子计算机。
- 2021年5月：中科大研究团队成功研制了62量子比特的原型机“祖冲之号”

“量子霸权和国际政治没有关系……”

量子优越性（“量子霸权”）：量子计算机在某个问题上超过现有最强的经典计算机。

Thanks for listening☺