太原理工大学
TAIYUAN UNIVERSITY OF TECHNOLOGY

数学学院
College of Mathematics

量子计算与量子信息 /Quantum 创新实践小队

Quantum Computing and Quantum Information

Social Practice

李岳昆
realyurk@gmail.com

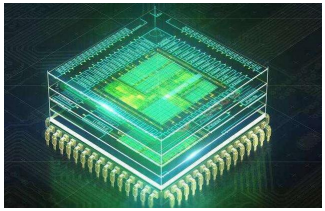
2021 年 7 月 12 日

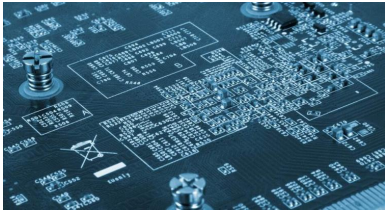
第 I 部分

量子计算

历史

量子计算 (Quantum Computation) 的概念最早由阿岗国家实验室的 P. Benioff 于 80 年代初期提出，但真正引起关注的是 20 世纪 90 年代中期。这期间人们发现了 $Shor$ 量子因子分解算法和 $Grover$ 量子搜索算法，这两类算法展示了量子计算从根本上超越经典计算机计算能力和在信息处理方面的巨大潜力。与此同时，量子计算机和量子物信息处理装置在物理实现的研究，成为继并行计算机、生物计算机等之后的非串行计算体系的又一热点。





量子计算介绍

内容介绍

量子计算是一种遵循量子力学规律调控量子信息单元进行计算的新型计算模式。对照于传统的通用计算机，其理论模型是通用图灵机；通用的量子计算机理论模型是量子力学规律重新诠释的通用图灵机。从可计算的问题来看，量子计算机智能解决传统计算机所能解决的问题，但是从计算的效率上，由于量子力学叠加性的存在，某些已知的量子算法在处理问题时速度要远快于传统的通用计算机。

量子比特 $qubit$

- $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$，$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ 对应量子的两种自旋状态
- $qubit$ 的一般形式可以写作 $|\psi\rangle = a|0\rangle + b|1\rangle$，其中 $a, b \in \mathbb{C}$，且 $|a|^2 + |b|^2 = 1$

测量

我们通过一个被称为是“测量”的过程，可以将一个 $qubit$ 的状态以概率幅的形式转化为 bit 信息。转化过程大致如下：

1. 概率为 $|\langle 0|\varphi\rangle|^2$ 变化为：bit 0.
2. 概率为 $|\langle 1|\varphi\rangle|^2$ 变化为：bit 1.

这里需要我们先求出量子比特 $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ 的两个内积结果：

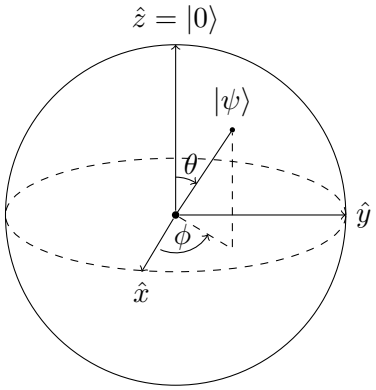
$$\langle 0|\varphi\rangle = \alpha\langle 0|0\rangle + \beta\langle 0|1\rangle = \alpha$$

$$\langle 1|\varphi\rangle = \alpha\langle 1|0\rangle + \beta\langle 1|1\rangle = \beta$$

总结来说：$|\varphi\rangle$ 以概率为 $|\alpha|^2$ 取值 bit 0，$|\beta|^2$ 取值 bit 1，特别的，当 $\alpha = 1$ 的时候，$|\varphi\rangle$ 取 0 的概率为 1；当 $\beta = 1$ 的时候，$|\varphi\rangle$ 取 1 的概率为 1；这样，理论上我们就完成了将 $qubit$ 与经典的 bit 对应的任务.

Bloch 球面

Bloch 球面是 $qubit$ 的一种表现形式



$qubits$ 在 Bloch 球面上的表示：
每一种线性组合

$$|\psi\rangle = a|0\rangle + b|1\rangle \in \mathbb{C}^2$$

对应于 Bloch 单位球面上的一个点 (θ, ϕ)，其中 $a = \mathbf{cos}(\frac{\theta}{2}), b = e^{i\phi}\mathbf{sin}\frac{\theta}{2}$

$$\begin{aligned}|\varphi\rangle &= a|0\rangle + b|1\rangle \\ &= \mathbf{cos}(\frac{\theta}{2})|0\rangle + e^{i\phi}\mathbf{sin}(\frac{\theta}{2})|1\rangle \\ &= \mathbf{cos}(\frac{\theta}{2})|0\rangle + (\mathbf{cos}(\phi) + i\mathbf{sin}(\phi))\mathbf{sin}(\frac{\theta}{2})|1\rangle\end{aligned}$$

Bell 态（或 EPR 对）

Bell 态或 EPR 对是一个重要的双量子态：

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

它是量子隐传态和超密编码的关键要素。Bell 态指出：

- 双量子比特系统中，第一个量子比特的状态观测值与第二个完全相同，即测量结果是相关的.
- 双量子比特系统中的相关性比经典世界中任何存在性的相关性都要强.

Example：量子隐形传态

- Bell 态是否意味借助量子纠缠，我们可以超过光速传输信息？
- 量子隐形传态并没有带来超光速通信，因为完成隐形传态，Alice 必须通过经典信道把她的测量结果传给 Bob，如果没有经典信道，隐形传态根本传送不了任何信息。
- 经典信道受到光速限制，因此量子隐形传态不能超过光速.

两个量子比特的张量积 (tensor product)

假设我们有两个独立的状态空间，它们都有正交积 $\{|u\rangle\}$和$\{|v\rangle\}$

- 这个复合系统的基可以定义为 $|w\rangle = |u\rangle \otimes |v\rangle$（张量积）
- 也可写为 $|u\rangle|v\rangle$，或 $|u, v\rangle$，或 $|uv\rangle$
- 若 $|u\rangle = \begin{bmatrix} u_1 \\ u_2 \end{bmatrix}$，$|v\rangle = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$，那么 $|u\rangle \otimes |v\rangle = \begin{bmatrix} u_1 v_1 \\ u_1 v_2 \\ u_2 v_1 \\ u_2 v_2 \end{bmatrix}$

例子：
考虑两量子比特的系统，正交基为 $|0\rangle$ 和 $|1\rangle$，那么复合系统的正交基为：

$$|0\rangle \otimes |0\rangle \equiv |00\rangle, |0\rangle \otimes |1\rangle \equiv |01\rangle$$

$$|1\rangle \otimes |0\rangle \equiv |10\rangle, |1\rangle \otimes |1\rangle \equiv |11\rangle$$

我们可以用 $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ 来描述，α_{00}^2 是测量时落在 $|00\rangle$ 的概率。同样，它们的平方和恒为 1. 对于一个双量子比特系统，如果我们测量第一个粒子，得到 $|0\rangle$，那么第二个粒子的状态则为：

$$\frac{\alpha_{00}|0\rangle + \alpha_{01}|1\rangle}{\sqrt{\alpha_{00}^2 + \alpha_{01}^2}}$$

（第一个粒子为 $|1\rangle$ 的可能被消除，下面的分母是为了保证概率的归一性）

Example：

考虑两个独立的量子态：

$$|\psi_1\rangle = \frac{1}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle, |\psi_2\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$$

- 复合系统的基为 $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$
- 两个量子比特的联合状态为

$$\begin{aligned}|\psi\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle \\ &= \frac{1}{\sqrt{15}}|00\rangle + \frac{2}{\sqrt{15}}|01\rangle + \sqrt{\frac{2}{15}}|10\rangle + \frac{2\sqrt{2}}{\sqrt{15}}|11\rangle\end{aligned}$$

酉矩阵（Unitary Matrix）

- 若一 n 行 n 列的复数矩阵 U 满足

$$U^\dagger U = UU^\dagger = I_n$$

其中，I_n 为 n 阶单位矩阵，$U^\dagger$ 为 U 的共轭转置，则 U 称为酉矩阵（Unitary Matrix，其中 Unitary 为归一或单位的意思）。即：矩阵 U 为酉矩阵，当且仅当其共轭转置 $U^\dagger$ 为其逆矩阵：

$$U^{-1} = U^\dagger$$

- 每一个量子逻辑门（Quantum Logic Gate）都对应了一个数学上面的一个酉矩阵，所有的量子操作都是可逆的。

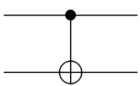
受控非门

令 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ 为两个量子比特系统的基，受控非门的操作为

$$U_{CNOT} : |00\rangle \to |00\rangle, |01\rangle \to |01\rangle, |10\rangle \to |11\rangle, |11\rangle \to |10\rangle$$

就是把 $\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle$ 映射成 $\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_3|10\rangle + \alpha_2|11\rangle$，
也就是把 α_2 和 α_3 顺序交换。
它的矩阵形式为

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



Hadamard 门

- Hadamard 门定义为：

$$U_H : |0\rangle \to |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle \to |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- $U_H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
- 那么对于 n 个 $|0\rangle$ 呢？则是变成了 $\frac{1}{2^{\frac{n}{2}}} \sum_{x \in \{0,1\}^n} |x\rangle$，$x$ 是由 0、1 组成的所有长度为 n 的数字串
- 更进一步，如果 n 比特不是 $|0\rangle$，而是 $|0\rangle, |1\rangle$ 随意切换呢？例如数字串 $|u\rangle = |u_1 u_2 \cdots u_n\rangle$ 如果输入的是 $|u\rangle$，那么经过 H 门变换，输出会是什么？答案是：

$$\sum_x \frac{-1^{ux}}{2^{\frac{n}{2}}} |x\rangle$$，这里的$u \cdot x = u_1 x_1 + u_2 x_2 + \cdots + u_n x_n$

Bloch 球面上的 Hadamard 门变换

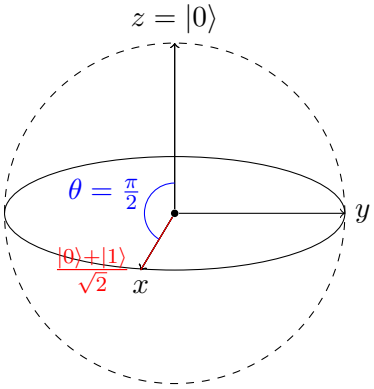


图: Basis state$|0\rangle$

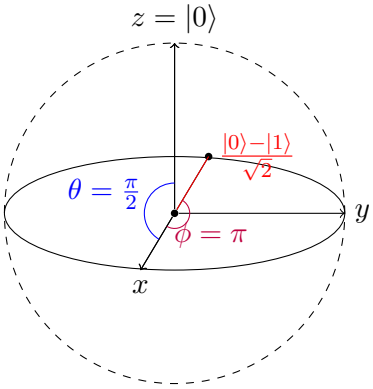


图: Basis state$|1\rangle$

Pauli 门

三种 Pauli 门（Pauli-X，-Y，-Z 门）对应在 Bloch 球面上 x，y 和 z 轴的三个旋转操作，转动弧度都为 π.

- Pauli-X 门交换了 $|0\rangle$ 和 $|1\rangle$ 的概率幅（量子非门）
- Pauli-Y 门交换了 $|0\rangle$ 和 $|1\rangle$ 的概率幅，把每个概率幅乘以 i，并将 $|1\rangle$ 的概率幅变为相反数
- Pauli-Z 门将 $|1\rangle$ 的概率幅变为相反数，令 $|0\rangle$ 的概率幅保持不变

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

交换门（SWAP 门）

双量子比特系统的交换门为：

$$U_{SWAP}|\psi_1,\psi_2\rangle = |\psi_2,\psi_1\rangle$$

举例来说：

$$U_{SWAP}: |00\rangle \to |00\rangle, |01\rangle \to |10\rangle, |10\rangle \to |01\rangle, |11\rangle \to |11\rangle$$

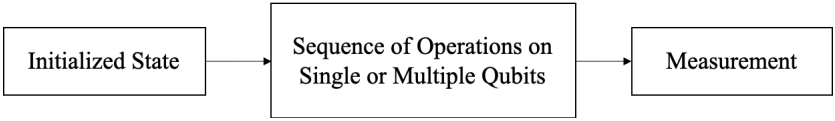
矩阵形式为：

$$U_{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

量子计算

量子计算是下列三个元素的组合：

- 一个初始状态 $|\psi\rangle$（Initial State）
- 执行某个给定量子算法的酉矩阵 U
- 测量（Measurement）



Example

数据库文件名	key	value
电话薄	姓名	电话号码
英汉词典	英文单词	汉语注释

- 假设有 $N = 2^n$ 条记录
- 如果是字典序，最多经过 $n = \log_2 N$ 步
- 如果是未整理？

分析

- 设第 i 个记录被查询的概率为 P_i，查到第 i 个记录需要 i 次，考虑查询每个记录的平均查找次数
- $\overline{N}_s = \sum_{i=1}^{N} P_i i$
- 每个记录被查询的几率相等 $P_i = \frac{1}{N}$，平均查找次数为
- $\overline{N}_s = \sum_{i=1}^{N} \frac{1}{N} i = \frac{1}{N} \sum_{i=1}^{N} i = \frac{N+1}{2} \approx \frac{N}{2} = O(N)$
- 然而 $Grover$ 发现量子的搜索算法的复杂度为 $O(\sqrt{N})$，只需要查询 $\sqrt{N}$ 次，就可以以非常接近 1 的概率找到所需要的结果

简化版的搜索问题

假设有一个映射 $0, 1, 2, \cdots, N \longmapsto \{0, 1\}$，即为函数 $f(x) \longmapsto \{0, 1\}$.

$$f(x) = \begin{cases} 0, & (x \neq x_0) \\ 1, & (x = x_0) \end{cases}$$

例如 $N = 4$

$$f(1) = 0$$

$$f(2) = 1$$

$$f(3) = 0$$

$$f(4) = 1$$

题目要求找到 $f(x) = 1$ 的解。答案显然易见，是 2,4。我们的搜索算法只需要找到其中一个即可。

Oracle

- 假设有一个量子 Oracle 可以识别搜索问题的解，识别结果可以通过 Oracle 的一个量子比特给出。于是可以 Oracle 定义为：
- $|x\rangle|q\rangle \xrightarrow{Oracle} |x\rangle q \oplus f(x)\rangle$
- 其中 $|q\rangle$ 是一个结果寄存器，$\oplus$ 是二进制加法。Oracle 实现了当索引为目标结果时，寄存器翻转；反之，寄存器结果不变。从而我们可以通过判断结果寄存器中的值是否为我们需要的答案来实现搜索。

Oracle 过程阐述

- 若 $f(x)=0$

$$\frac{1}{\sqrt{2}}(|f(x)\rangle-|1\oplus f(x)\rangle)=(-1)^0\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

- 若 $f(x)=1$

$$\begin{aligned}\frac{1}{\sqrt{2}}(|f(x)\rangle-|1\oplus f(x)\rangle)&=\frac{1}{\sqrt{2}}(|1\rangle-|0\rangle)\\&=(-1)^1\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\end{aligned}$$

- 借助 Hadamard 门令量子处于激发态，若初始化不是 $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$，则不改变状态；反之，令两量子位交换，于是我们可以概括此过程中酉算子 Oracle 的作用：

$$|x\rangle(\frac{|0\rangle-|1\rangle}{\sqrt{2}})\xrightarrow{Oracle}(-1)^{f(x)}|x\rangle(\frac{|0\rangle-|1\rangle}{\sqrt{2}}),\text{简记为：}\ |x\rangle\xrightarrow{Oracle}(-1)^{f(x)}|x\rangle$$

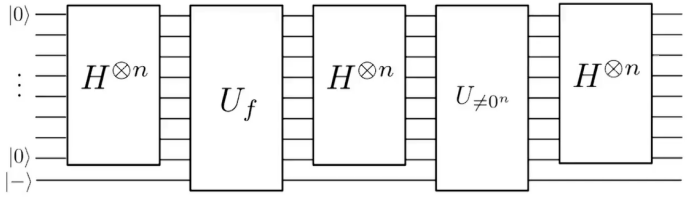
Oracle 过程阐述

- 我们说 Oracle 改变了解的相位，对于有 M 个解的 N 元搜索问题，时间复杂度开销仅为 $O(\sqrt{\frac{N}{M}})$.
- 量子搜索中“知道解”与“找到解”的区别：我们不需要让算法去识别哪个答案才是解，只需要让其能够识别解即可。

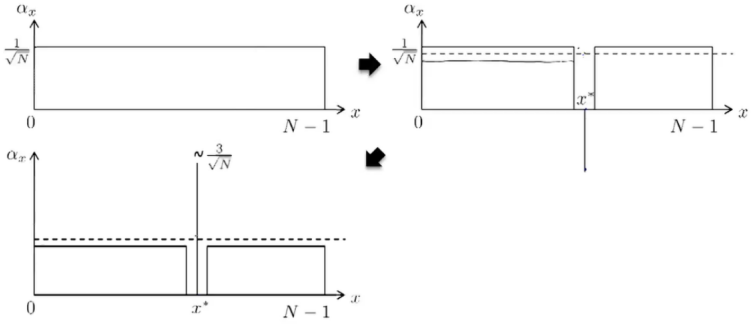
算法流程

Algorithm

- (Phase Inversion) 应用 oracle O
- (Inversion about the Mean I) 应用 Hadamard 变换 $H^{\otimes n}$
- (Inversion about the Mean II) 在计算机上执行条件相移，使 $|0\rangle$ 以外的每个计算基态获得-1 的相位移动
- (Inversion about the Mean III) 应用 Hadamard 变换 $H^{\otimes n}$



算法图解


α_x
$\frac{1}{\sqrt{N}}$
0
$N-1$
x
α_x
$\frac{1}{\sqrt{N}}$
x^*
0
$N-1$
x
α_x
$\sim \frac{3}{\sqrt{N}}$
0
x^*
$N-1$
x

Procedure

$$H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$$

其中 $|\psi\rangle$ 是指均衡叠加态

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=1}^{2^n}|i\rangle$$

$$|00...0\rangle \xrightarrow{H^{\otimes n}} |\psi\rangle$$

于是，$Grover$ 迭代 G 可以写成 $G = (2|\psi\rangle\langle\psi| - I)O$

为了不失一般性，假设 $f(i)=1$ 的所有 i 组成的量子态为

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x}^{I} |x\rangle$$

那么 $f(i)=0$ 所组成的量子态为

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x}^{II} |x\rangle$$

其中 $N=2^n$，最终 $|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$

$Grover$ 算法总结

运行时间：$O(\sqrt{2^n})$，成功的概率为 $O(1)$
流程：

- 初始状态：$|0\rangle^{\otimes n}$
- 对所有 $qubit$ 进行 Hadamard 变换：

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle = |\psi\rangle$$

- 执行 $Grover$ 迭代 $R \approx \frac{\pi\sqrt{2^n}}{4}$ times：

$$[(2|\psi\rangle\langle\psi| - I)|O\rangle]^R|\psi\rangle \approx |z\rangle$$

- 测量结果：z

第 II 部分

量子信息

经典信息论

- 1938 年发表论文《A Symbolic Analysis of Relay and Switching Circuits》，提出用布尔代数来分析开关电路.
- 1941 年以数学研究员的身份进入新泽西州的 ATT 贝尔电话公司.
- 二战期间发表论文：《Communication Theory of Secrecy Systems》，使保密通信由艺术变成科学.
- 1948 年在 Bell System Technical Journal 上发表了《A Mathematical Theory of Communication 》.

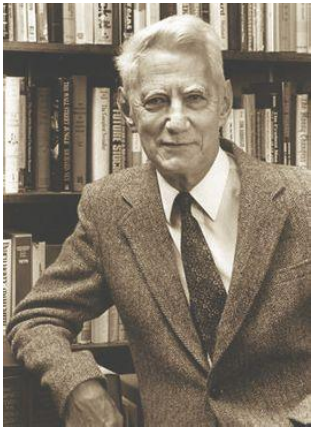


图: Claude Elwood Shannon

Shannon 熵

得到 x 值前关于 x 的不确定性的测度即为 x 的 Shannon 熵，因此熵函数为：

$$H(x) = -\sum_{x} p_x log p_x$$

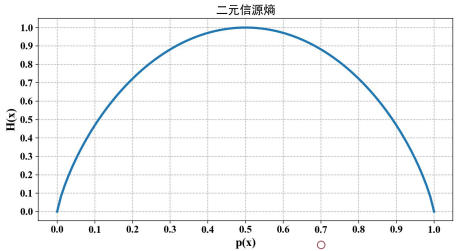
- 熵可以用来量化信息，我们可以用熵来确定“重构该信息源产生的信息需要的最少物理资源”.
- 例如：一个信号源能够产生四种信号：1，2，3，4. 若不对信息进行压缩，存储这四个信号需要用 2 比特的空间.
- 此时 $P(X=1)=P(X=2)=P(X=3)=P(X=4)=\frac{1}{4}, H(x)=2.$
- 若 $P(X=1)=\frac{1}{2}, P(X=2)=\frac{1}{4}, P(X=3)=P(X=4)=\frac{1}{8}$，则我们可以通过 Shannon 熵公式直接确定存储这些信息需要的最小物理单元：$H(x)=\frac{7}{4}$.

- 有时未知的结果只有两种情况，例如：抛一枚硬币，得到的只能是正面或者反面，我们将这种输出结果的称之为二元熵，公式可化简为：

$$H_{bin}(p) = -plogp - (1-p)log(1-p)$$

- 直观来说，硬币正反两面概率相等时，二元熵最大.
- 若某人有两枚质量分布不均匀的硬币，假设我们已知各个面出现的概率，那么根据观测结果我们还会知道：抛出的可能是哪种硬币.

$$f(p(x) + (1-p)y) \geqslant pf(x) + (1-p)f(y)$$



条件熵

对于两种变量形成的系统，我们有

$$H(X,Y) \equiv -\sum_{x,y} p(x,y) log p(x,y)$$

假设我们已知 $H(Y)$，那么对于 $H(X,Y)$ 而言，剩余的不确定度完全由 X 自己提供. 例如：同时投掷两枚骰子，若我们知道其中一个的点数，则整个系统的不确定度则由此时另一个骰子完全提供，可整理成公式为：

$$H(X|Y) = H(X,Y) - H(Y)$$

互信息

若 X 给出了十条信息，Y 给出了十条信息，则 X 与 Y 提供的信息总量为

$$H(X:Y) \equiv H(X) + H(Y) - H(X,Y)$$

代入条件熵公式，有

$$H(X:Y) = H(X) - H(X|Y)$$

Shannon 熵性质

- $H(X,Y) = H(Y,X)$,$H(X:Y) = H(Y:X)$
- 由 $H(Y|X) > 0$，故 $H(X:Y) \leqslant H(Y)$，即：加入信息后熵变小（不确定度变小）.
- $H(X) \leqslant H(X,Y)$，即：单独一个骰子出现的不确定程度一定不超过两个骰子的不确定度.
- $H(X,Y) \leqslant H(X) + H(Y)$

信息学基本定律

信息一旦丢失，将永远丢失.

数据处理不等式

设 $X \to Y \to Z$ 是一个 Markov 链，则

$$H(X) \geqslant H(X:Y) \geqslant H(X:Z)$$

当且仅当在给定 Y 条件下可以重构 X，第一个不等式达到饱和.

量子信息论

- 20 世纪 30 年代撰写的《量子力学的数学基础》被证明对原子物理学的发展有极其重要的价值.
- 1942 年起，同莫根施特恩合作，写作《博弈论和经济行为》一书，成为数理经济学的奠基人之一.
- 1946 年，开始研究程序编制问题，是现代数值分析——计算数学的缔造者之一.
- 提出计算机的冯诺伊曼架构，主要著作收集在《冯 · 诺伊曼全集》(6 卷，1961) 中.

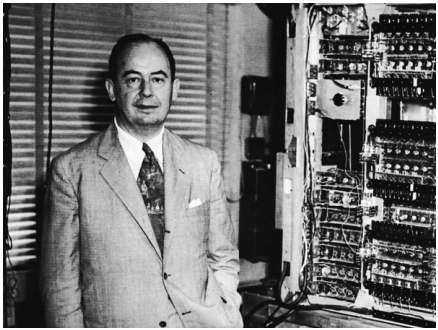


图: von Neumann

von Neumann 熵

von Neumann 定义：

$$S(\rho) \equiv -tr(\rho log \rho)$$

若 λ_x 是 ρ 的特征值，则 von Neumann 的定义可以写为：

$$S(\rho) = -\sum_x \lambda_x log \lambda_x$$

von Neumann 熵基本性质

- 熵是非负的，当且仅当状态为纯态时，熵为零.
- 在 d 维 Hilbert 空间中熵最多为 logd，当且仅当系统处于完全混合态 I/d，熵等于 logd.
- 设复合系统 AB 处于纯态，则 S(A)=S(B).
- 设 p_i 是概率，而状态 ρ_i 在正交子空间上支集，则

$$S(\sum_i p_i\rho_i) = H(p_i) + \sum_i p_i S(\rho_i)$$

联合熵定理

设 p_i 是概率，$|i\rangle$ 是子系统 A 的正交状态，ρ_i 是另一系统 B 的任一组密度算子，则

$$S(\sum_i p_i|i\rangle\langle i| \otimes \rho_i) = H(p_i) + \sum_i p_i S(\rho_i)$$

太原理工大學
TAIYUAN UNIVERSITY OF TECHNOLOGY

谢谢

李岳昆
realyurk@gmail.com · 量子计算与量子信息 /Quantum 创新实践小队