

$$\begin{array}{r} 0111 (7) \\ + 1110 (-2) \\ \hline 10101 (5) \end{array} \quad \text{补码} \quad \begin{array}{r} 0011 (3) \\ + 1000 (-8) \\ \hline 1011 (-5) \end{array}$$

No.

Date

模拟信号随时间连续变换 数字信号随时间断续变化

* 二进 Binary 八进 Octonary 十进 Decimal 十六进 Hexadecimal 制 system

二进制换十进制: $\sum K_i 2^i$

十进制换二进制: 整数除2取余由低向高, 小数乘2取整由高向低

反码(补数) 符号位不变, 数值位逐位求反

补码(补数) 反码数值部分加1

十进制数=二进制编码

有权码: 8421码, 2421码, 5211码

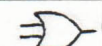
无权码: 余3码, 格雷码(循环码)

八位二进制	数	原码	反码	补码
0000 0000	0	+0	+0	+0
0000 0001	1	+1	+1	+1
0111 1110	126	+126	+126	+126
0111 1111	127	+127	+127	+127
1000 0000	128	-0	-127	-128
1000 0001	129	-1	-126	-127
1111 1110	254	-126	-1	-2
1111 1111	255	-127	-0	-1

或运算(逻辑加)

$$P = A + B$$

输入系数



$$1 + A = 1 \quad 0 + A = A$$

与运算(逻辑乘)

$$P = A \cdot B = AB$$



$$1 \cdot A = A \quad 0 \cdot A = 0$$

非运算

$$P = \bar{A}$$



与非

$$P = \overline{A \cdot B}$$



或非

$$P = \overline{A + B}$$



异或非

$$P = \overline{AB + \bar{A}\bar{B}}$$



异或 相异为真

$$P = A \oplus B = \bar{A}B + A\bar{B}$$



$$A \oplus 1 = \bar{A} \quad A \oplus 0 = A$$

同或 相同为真

$$P = A \odot B = \bar{A}\bar{B} + AB$$



<变换集合>

互补律 $A \cdot \bar{A} = 0 \quad A + \bar{A} = 1$ 交换律 结合律 分配律 $A \cdot (B + C) = A \cdot B + A \cdot C \quad A + B \cdot C = (A + B) \cdot (A + C)$

吸收律 $A + \bar{A}B = A + B \quad A \cdot (\bar{A} + B) = A \cdot B \quad A + A \cdot B = A \quad A(A + B) = A$

重叠律 $A + A = A \quad A \cdot A = A$ 包含律 $AB + \bar{A}C + BC(D) = AB + \bar{A}C$

代入规则 在含变量A等式中, 用另一逻辑(布尔)函数F代替所有变量A, 布尔逻辑等式仍成立

对偶规则 在逻辑函数式P中, 实行加乘互换, 0,1互换, 得对偶式P'; 等号两边对偶变换仍成立; $(P')' = P$

反演规则 加乘互换, 0,1互换, 原反互换(只变最底层变量, 大非号不变), 得反函数(反式) \bar{P} , 与德摩根结果相等
与或型逻辑式化简 ①与项最少 ②每一与项变量最少 ③最简式不唯一, 但简化程度一样 或与作对偶

最小项 ①全部n个变量, 各出现一次, 逻辑乘 ②原变量视1, 反变量视0, 按高低位排列, 换成十进制作下标 m_i ③一个为1, 其余全0

最大项 ①同上, 逻辑和 ②原变量视1, 反变量视0, 按高低位排列, 换成十进制作下标 M_i ③一个为0, 其余全1 * ① $M_i = \bar{m}_i$ ② $\sum m_i$ 与 $\prod M_i$ 互为对偶式

完全定义的逻辑函数 各最小项不在F中就在F中

标准与或表达式/最小项表达式/与或标准型 全部由最小项构成的与或型逻辑式, 唯一

卡诺图

逻辑相邻 仅有一个变量互为反变量, 逻辑相邻的最小项排列形成循环码

卡诺图 几何相邻的最小项逻辑相邻

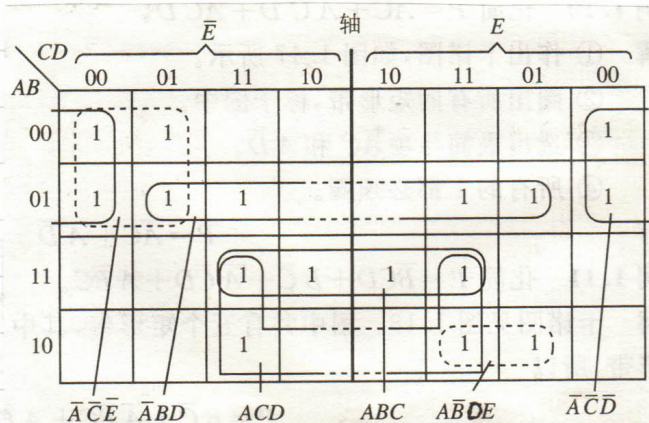
化简 画最大的2ⁱ矩形, 圈完所有1, 注意冗余项, 五变量卡诺图对折也相邻

F取值只和一部分最小项有关, 约束/任意/无关/不管项 X/0/d可任意取

约束方程 $\sum m_j = \sum d(i, \dots) = 0$ $F = \sum m(i, \dots) + \sum d(i, \dots)$

多输出逻辑函数 同一输入, 多个输出, 尽可能多公共项 (总体最简, 单项不一定最简)

CD \ AB	00	01	11	10
00	0000 0	0001 1	0011 3	0010 2
01	0100 4	0101 5	0111 7	0110 6
11	1100 12	1101 13	1111 15	1110 14
10	1000 8	1001 9	1011 11	1010 10



逻辑门

通用门 任意布尔函数可以用与非门的复合来实现

异或门不改变奇偶性 异或门即使加上非门也不是通用门

数字电路

触发器

时序电路

信息学

Turing machine

1936 图灵证明存在 通用图灵机, 标志现代计算机科学形成

Church-Turing thesis

邱奇-图灵论题

Moore's law

摩尔定律 计算机硬件能力约 18 个月增长一倍

efficient

有效算法 解决问题所需时间是问题规模的多项式

经典机可以模拟量子机, 但似乎无有效方式去模拟

strong Church-Turing thesis

强邱奇-图灵论题 任何算法过程都可以用图灵机(后改为概率图灵机) 进行有效模拟

(经典通讯概述在书 1.6.1)

information source

Shannon entropy

信源 随机变量 X , 发出状态 j 的概率是 p_j 香农熵 $H(X) = -\sum_j p_j \lg(p_j)$

Shannon's noiseless channel coding theorem

香农无噪声编码定理 定量给出用于存储从信源发出信息所需物理资源, 比特数少于香农熵将导致高误

码率

纠错码 给信息引入足够多的冗余, 以便被部分污染后仍能恢复信息

Shannon's noisy channel coding theorem

香农有噪声编码定理 定量给出有噪声信道能可靠传送信息的量, 纠错码可保护信息, 有上限
channel capacity

信道 容量

对称密码 AES, Grover 算法可加速, 换用更长的密钥可解决

非对称密码, RSA, 密钥分发, 使用广泛, Shor 算法构成威胁

Rivest Shamir Adleman

RSA 公钥系统

public key

private key

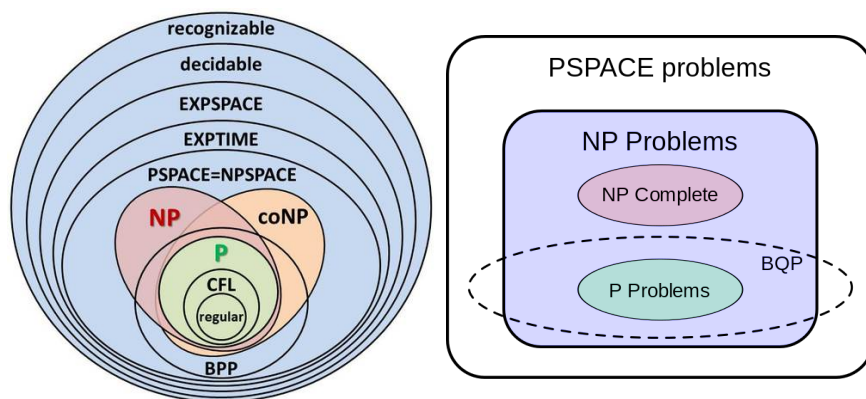
公钥 所有人都可用它加密 **私钥** 有私钥才可解密, 安全性建立在分解质因数困难上

布尔函数

计算模型

计算复杂度

PSPACE 使用有限的空间资源可以求解 (时间资源不限) (PSPACE 包含 P 和 NP 也是未被证明的)



complexity class P

P 类 问题可以在经典机上在多项式时间内求解 (目前还不知道求质因子的经典有效算法)

Non-deterministic Polynomial

NP 类 给一个候选答案, 可以在经典机上在多项式时间内验证它是不是解 (例: 某数的质因子是多少?)

(P 是否等于 NP 是世纪难题)

NP-hard

NP 困难 复杂度至少是 NP, 只要有一个 NPH 找到 P 解, 则将推出所有 NP 都是 P

NP-complete

NP 完全 既是 NPH 又是 NP 问题 (NP 中最难的问题) (若 $P \neq NP$, 则所有 NPC 都不是 P)

(目前也不知道质因子分解是不是 NPC, 如果是的话就说明量子机可以解决所有 NP 了)

Merlin-Athur

MA

Bound-error Probabilistic Polynomial

BPP 类 允许有限的误差概率后, 可以在多项式时间内求解

Bounded error Quantum Polynomial

BQP 允许有限的误差概率后, 量子机可以在多项式时间内求解

(已知 $P \leq BQP \leq PSPACE$, 然而并未证明 $P < PSPACE$, 如果不等, 才能说明量子机比经典机强)

QMA

QMA

基本实验

施特恩—格拉赫实验 (— 量子 —)

which way

哪条路实验

延迟选择实验 延迟和非延迟的实验结果相同

多粒子干涉

standard quantum limit

标准量子极限

BAE

回避反作用实验

QND

量子非破坏性实验

quantum eraser

量子擦除器

贝尔定理

如果贝尔不等式不成立, 要么放弃

locality

定域性 物体只能被其紧接的周围所直接影响

要么放弃

realism

实在性 世界和人的意识无关 mind-independent

Locality is one of the axioms of relativistic quantum field theory, as required for causality

Q bit

任何两态量子体系都可称为一个 量子比特, 如

贝尔基 取 $(\sigma_{1z}\sigma_{2z}, \sigma_{1x}\sigma_{2x})$ 表象, 4 个贝尔基分别为 $\chi_{++} = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$, $\chi_{+-} = \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle)$, $\chi_{-+} = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle)$, $\chi_{--} = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)$

记 $\langle \vec{a}, \vec{b} \rangle = \langle 0, 0 | \hat{\sigma}_a \hat{\sigma}_b | 0, 0 \rangle \xrightarrow{\text{根据量子力学}} -\cos(\vec{a} \wedge \vec{b})$

贝尔不等式 2 个处于自旋单态的粒子, 在 3 个方向测自旋关联 $|\langle \vec{a}, \vec{b} \rangle - \langle \vec{a}, \vec{c} \rangle| - \langle \vec{b}, \vec{c} \rangle \leq 1$, 可以画 $|- \cos \theta + \cos \theta| + \cos \theta$ 图像, 在两端会超过 1 (图见程檀生 P123)

CHSH 不等式 2 个处于自旋单态的粒子, 在 4 个方向测自旋关联 $|\langle \vec{a}, \vec{b} \rangle + \langle \vec{a}, \vec{c} \rangle + \langle \vec{a}', \vec{b} \rangle - \langle \vec{a}', \vec{c} \rangle| \leq 2$, 可以画 $|3 \cos \theta - \cos 3\theta|$ 图像

量子信息

在原子阱技术前, 人类尚无法单独访问单个量子系统 (此前都是对批量样本总体控制, 加速器中的单量子没操作性)

qubit

量子比特 状态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{\text{归一}} \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$

二维复向量空间中单位向量 \rightarrow 布洛赫球面

不进行测量, 则隐含大量信息, 且随比特数指数上升, n 量子比特的状态需 2^n 个复数

(通讯概述在书 1.6.1.2)

information source

von Neumann entropy

信源 发出状态 $|\psi_j\rangle$ 的概率是 p_j 冯诺伊曼熵 $S(\hat{\rho}) = -\text{tr}(\hat{\rho} \log \hat{\rho}) = -\sum_j \lambda_j \log(\lambda_j)$

fidelity

保真度

Schumacher's noiseless channel coding theorem

舒马赫无噪声编码定理 定量给出能以接近 1 保真度恢复在信源约束下量子数据压缩所需物理资源

冯纽曼熵 \leq 香农熵, 仅当 $|\psi_j\rangle$ 正交时取等

(证明见书 2.2.4 P81) 非正交的量子态不能可靠区分 (否则就可以利用纠缠对超光速通讯了)

(POVM 测量举例见 2.2.6)

quantum money

量子钞 银行在发行的钞票上印上经典序列号和非正交量子比特序列, 只有银行保存这两者匹配的列表, (可信赖的) 商家想验证真伪时, 把经典序列号告诉银行, 银行指示商家按哪种基来测量量子比特

量子门

quantum gate

量子门 么正性是唯一的要求, 故总可逆 (任意 2×2 么正矩阵可分解为 $\langle - \text{线路} \rangle$)

单量子比特门:

Pauli gate

泡利门 $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (量子非门, 交换幅度), $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Hadamard gate

哈达玛门 $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, 即 $\begin{matrix} |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{matrix}$, $H^2 = I$, (图像: 先绕 y 轴转 90° , 再绕 x 轴转 180°)

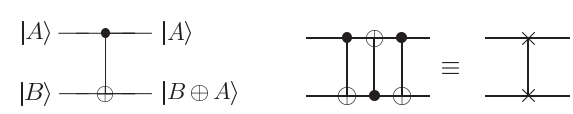
相位门 $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ (Z 门的根号) **$\pi/8$ 门** $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ (S 门的根号)

多量子比特门:

Controlled NOT

受控非门 控制比特, 目标比特 $|c, t\rangle \rightarrow |c, t \oplus c\rangle$ (控制比特为 0 则目标比特不变, 为 1 则翻转)

任意多量子比特门都可用受控非和单量子比特门复合而成 \rightarrow 通用门 (经典的与非门不可逆)

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad U_{SW} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad H^{\otimes 2} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$


swap

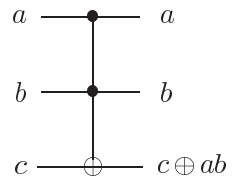
对换 3 个 CNOT, 中间的反放 $|a, b\rangle \rightarrow |a, a \oplus b\rangle \rightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \rightarrow |b, a\rangle$

n 量子比特上的 H 变换: $H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{a,b} (-1)^{ab} |a\rangle \langle b|$

Toffoli / CCNOT

控控非门 $C^2(X)$, 可逆, 逆是自身, 可实现与 $c=0$, 非 $a=b=1$, 与非 $c=1$

\rightarrow 故量子机可以做经典计算



量子线路

initialization operation

① 初始化 ② 操作 (经典: 单:NOT, 双:NAND, 量子: 单:旋转 \rightarrow 叠加, 双:CNOT \rightarrow 纠缠) ③ 探测

acyclic

无环 量子线路不允许回路, 即无反馈 线路不允许汇合, 扇入扇出禁止 (因为操作不可逆)

measurement

测量 把单量子比特状态变成(依概率的) 经典比特状态, 经典线路用双线表示

no-cloning theorem

不可克隆定理 不可能制作未知量子态的拷贝 源于量子理论是线性的 (可以有以概率成功克隆的方法)

若 $\exists U$ 能 $|00\rangle \xrightarrow{U} |00\rangle$, $|10\rangle \xrightarrow{U} |11\rangle$, 则对于叠加态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 有 $|\psi0\rangle \xrightarrow{U} (\alpha|00\rangle + \beta|11\rangle) \neq |\psi\rangle \otimes |\psi\rangle$

(U_{CN} 可以拷贝经典态)

应用举例

Bell state / EPR pair

贝尔态 / EPR 对 关联 $\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, 反关联 $\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, 可由 H 门后 CNOT 制备, 相应列记为

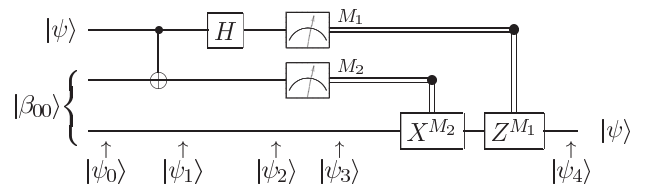
$$\begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{bmatrix} \xrightarrow{\frac{1}{\sqrt{2}}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{bmatrix}$$

quantum teleportation

量子传态 无需量子通信信道就可转移量子态 (必需经典通讯, 故非超光速)

以 EPR 对 $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 为例, 狸持有左边那个, 桃持右边那个, 狸想把 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 传给桃, 他把 $|\psi\rangle$ 和粒子放一起做贝尔基测量(上方 2 根线), 然后通过经典通讯告诉桃结果(双线), 桃根据结果做相应操作可恢复 $|\psi\rangle$: 若 $|00\rangle$ 不动, 若 $|01\rangle$ 做 X 门, 若 $|10\rangle$ 做 Z 门, 若 $|11\rangle$ 做 ZX

$|\psi_0\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle)$
 $|\psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle))$
 $|\psi_2\rangle = \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle))$
 → 测量导致坍缩, 按前 2 位重新分组 →



$|\psi_3\rangle = \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle))$
 意义: 纠缠对是一种静态资源, 消耗一个 EPR 对加 2 经典比特通讯可实现 1 量子比特的传送

GHZ 态 3 量子比特的纠缠态 $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = (|xxx\rangle + |x\bar{x}\bar{x}\rangle + |\bar{x}x\bar{x}\rangle + |\bar{x}\bar{x}x\rangle)$
 特点: 任意 2 者一对可确定第 3 者手中的态 → QSS

量子计算

quantum computation

量子计算

量子并行 以两个比特都做 H 变换为例 $H^{\otimes 2}$

(此段在书的 1 章 1.4.2 1.4.4, 先跳过)

目前只有 3 类已知优于经典算法的量子算法 ① 量子傅氏变换 (Deutsch 问题, 肖氏算法, 离散对数, 隐含子群问题): 指数加速 ② 量子搜索: 根号加速 ③ 量子模拟: 所需资源随问题规模线性增加

* 量子搜索可视为一种量子模拟问题的解

量子傅氏变换

离散傅氏变换是 $N=2^n$ 个复数集合 $\{x_j\}$ 到 $\{y_k\}$ 的变换 $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} x_j$

有么正变换 $|j\rangle \xrightarrow{U} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k / N} |k\rangle$, 则 $\sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{U} \sum_{k=0}^{N-1} y_k |k\rangle$

经典的 FFT 花 $N \log(N) = n 2^n$ 步, 量子傅氏变换用 $(\log N)^2 = n^2$ 步, 指数加速, 但计算结果不能直接利用

量子搜索

已证明, 不能通过"用量子并行搜索所有可能解"这种方法, 来有效求解所有 NP 问题

量子密码

quantum cryptography

量子密码学

量子纠错

threshold theorem

阈值定理 如果量子噪声可降到某阈值以下, 则量子纠错码可继续使它无限下降, 代价是仅增加一点计算复杂度

tomography

量子态层析 通过反复制备相同量子态, 以不同方式测量, 建立量子态的完整描述

entanglement distillation

纠缠纯化

(量子计算的实现概述在书 1.5.2)

用光子的优点是量子信息的承载高度稳定, 缺点是光子要相互作用必须借助其它物质, 从而增加噪声

ion trap

离子阱 用原子存储量子比特, 光子用来操作原子

参考文献

Nielsen & Chuang. Quantum Computation and Quantum Information. Cambridge

↳ 中译: 赵千川. 量子计算和量子信息 (一: 量子计算部分, 二: 量子信息部分). 清华大学出版社

离散数学及其应用作者: (美) 罗森著, 袁崇义等译出版社: 机械工业出版社