0111 (7)
+ 1110 (-2)
10101 (5)

补码

0011 (3)
+ 1000 (-8)
1011 (-5)

0101

数电 3

No.　逻辑

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(一补数) 符号位不变,数值位逐位求反

补码(二补数) 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)　$P = A+B$　扇入系数　$1+A=1$　$0+A=A$

与运算(逻辑乘)　$P = A\cdot B = AB$　$1\cdot A=A$　$0\cdot A=0$

非运算　$P = \bar{A}$

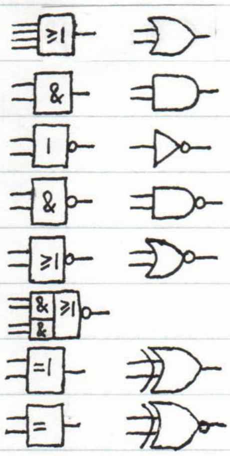
与非　$P = \overline{A\cdot B}$

或非　$P = \overline{A+B}$

与或非　$P = \overline{AB+CD}$

异或 相异为真　$P = A\oplus B = \bar{A}B + A\bar{B}$　$A\oplus 1=\bar{A}$　$A\oplus 0=A$

同或 相同为真　$P = A\odot B = \bar{A}\bar{B}+AB$



〈实变集合〉

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

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

重叠律 $A+A=A$　$A\cdot A=A$　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

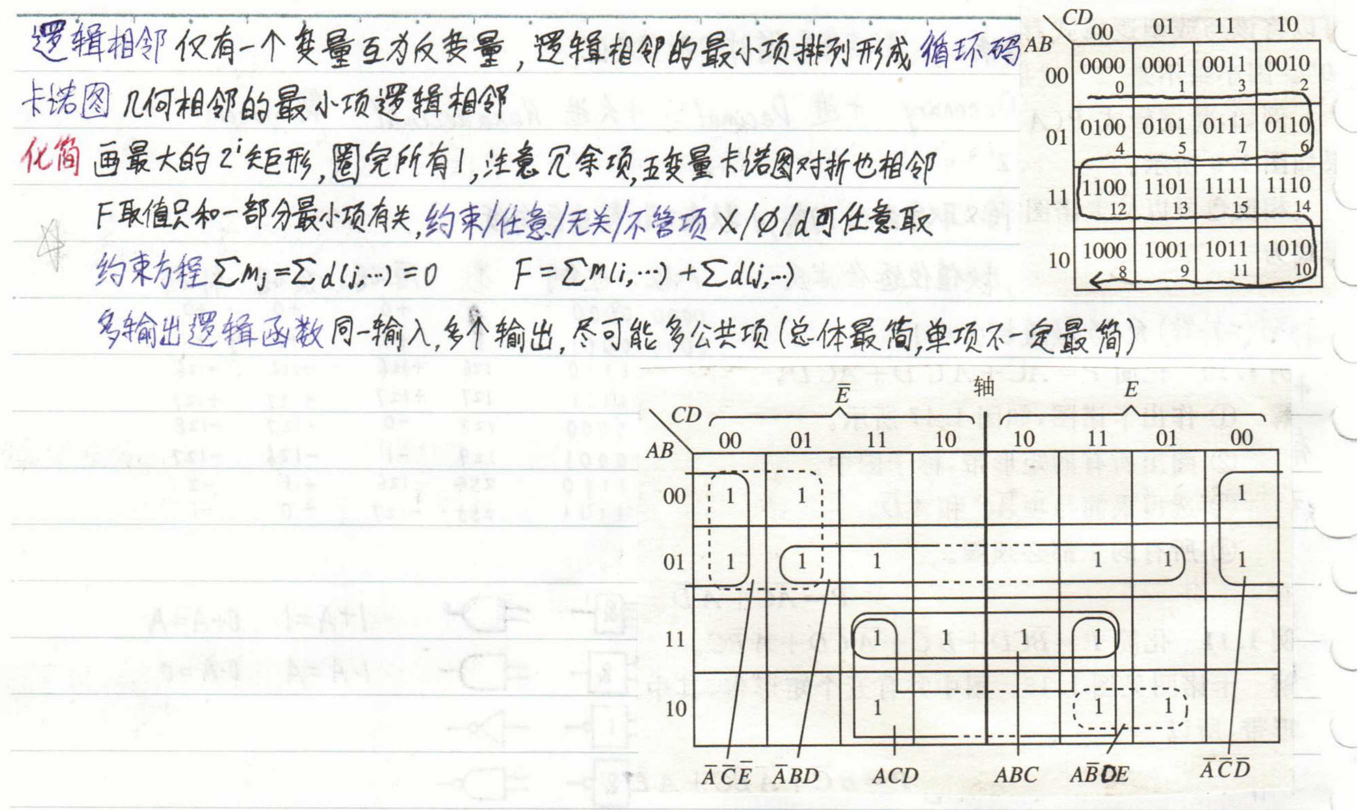
最小项 ①全部n个变量,各出现一次,逻辑乘 ②原变量视1,反视0,按高低位排列,换成十进制作下标 m_i ③一个为1,其它全0

最大项 ①同上,逻辑和 ②原0反1, M_i ③一个为0,其它全1　* ① $M_i=\overline{m_i}$ 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$\bar{F}$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

Karnaugh map
卡诺图



逻辑门

circuit wire gate
线路 连线加门
Boolean function
布尔函数
decision problem
判定问题
「使用连线，辅助比特，扇出，与非门可模拟与，异或，非门」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
half-adder
半加器

数字电路

触发器

时序电路

信息学

Turning machine tape
图灵机 ⓪ 带子：一维无限长方格，每个方格上有符号，符号来自一个有限的字母表，例如 $\{0, 1, -$ (空白) $\}$

halting state
① 处理器：有限状态控制器，状态记为 $q_{1\sim m}$，另有 q_s 表示开始，q_h 表示停机状态
off-tape
② 内存：提供离带暂存，足够大 ③ 读写头：每次只能看到并修改一格
④ 程序：有限多个具有 $(q, x; q', x'; s)$ 形式的程序行 (一种程序对应一种图灵机)

图灵机从 q_s 开始, 读带子的初始格子 x_0, 在程序中找 $(q_s, x_0; \dots)$, 然后机器内部状态变 q', 修改带子为 x', 读写头按 $s=\pm1,0$ 左右移或不动, 以后每个机器周期重复此事, 直到找不到程序行, 状态变 q_h

例 TODO 需图灵机例子

Church-Turing thesis
邱奇－图灵论题 能由自然算法计算的函数都可由图灵机计算

(意义: 将模糊的直观概念和精确数学定义相联系) (量子机也服从, 区别是效率可能比经典高)

图灵数 每个单带图灵机 M 可唯一分配一对应的数 T_M「每个正整数有唯一素因子分解」

Universal Turing Machine
通用图灵机 输入 T_M 加空格加 x, 输出 M 对 x 的结果 $\to$ 能模拟任何其它图灵机 M

1936 图灵证明存在通用图灵机, 标志现代计算机科学形成

undecidability
不可判定性 不存在能判定一切数学问题的算法 (例如两拓扑空间是否同胚是不可判定问题)

halting problem
停机问题 具有图灵数 $T_M=x$ 的图灵机对输入 x 能否停机? 假设存在算法 $h(x)=1$ 停 $=0$ 不停, 则存在算法 $t(x):=$ if $h(x)=0$ then 停机 else 死循环, 记 $t(x)$ 这个程序的图灵数是 T, 则当且仅当 $h(T)=0$ 时 $h(T)=1$, 矛盾

Moore's law
摩尔定律 计算机硬件能力约 18 个月增长一倍

efficient / tractable / feasible
有效 / 可解 / 可行 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** $H(X)=-\sum_j p_j \,\mathrm{lb}\,(p_j)$

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

channelcapacity
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 **S**hamir **A**dleman
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

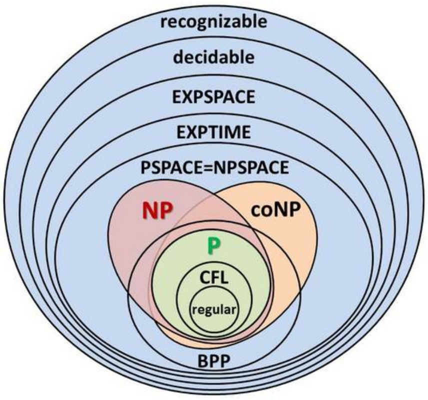
计算复杂度

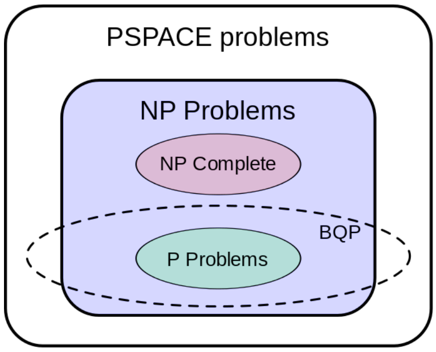
PSPACE
P 空间 使用有限的空间资源可以求解 (时间资源不限) (PSPACE 包含 P 和 NP 也是未被证明的)

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 **P**olynomial
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?)

推论 P⊆NP (P 是否等于 NP 是世纪难题)





coNP 给一个候选非答案, 验证之, NP 的语言 (Language) 的补集

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)

Hamilton cycle
哈密顿圈问题 遍历一次所有顶点, 图是否含 HC 是 NPC (欧拉圈问题 (遍历一次所有边) 却很简单)

Traveling **S**alesman **P**roblem
旅行商问题 是否存在经过所有城市距离小于给定数的旅行路线

reduction
HC 到 TSP 的 归约 相连城市距离定 1, 不连为 2, 则距离小于 $n+1$ 就是 HC **性质** 归约有传递性

Circuit **SAT**isfiability
线路满足性 给定与或非门组成的布尔线路, 是否存在一组输入使输出为 1

Cook-Levin
库克定理 CSAT 是 NPC

用途: 证明一个问题是 NPC, 可证明问题 NP, 然后 CSAT 可归约到它

例 SAT 问题(CSAT 的布尔函数版) 是 NPC * 3SAT 问题 NPC, 2SAT 问题居然是 P

EXP 指数时间 L 对数空间

time hierarchy theorem
时间层次定理 $P \subset EXP$

space hierarchy theorem
空间层次定理 $L \subset PSPACE$

$L \subseteq P \subseteq NP \subseteq PSPACE \subseteq EXP$ (至少有一个应是严格的, 但还不知道是哪个)

Merlin-Athur
MA

Bound-error **P**robabilistic **P**olynomial time
BPP 类 允许有限的误差概率后, 可以在多项式时间内求解

Chernoff bound
界

TODO: 见选课笔记

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 $P \leqslant BQP \leqslant PSPACE$, 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

Einstein–Podolsky–Rosen paradox
EPR 佯谬 即使在空间上分离得很远的纠缠对, 测量其中一个也会立即导致另一个坍缩

① 量子力学认为未被观察的粒子尚不具有物理性质的测量值 → 导致存在超距的扰动作用

hidden variable
② 本来是有确定值的, 量子力学理论不完备, 存在某个隐藏物理量 (隐变量), 引入它就可以在测量前准确预测物理性质的值

贝尔不等式不成立, 定域性和实在性必须放弃至少一个

locality
定域性 物体只能被其紧接的周围所直接影响

realism
实在性 物理性质独立于观测值而存在

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

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 $|\langle\vec{a},\vec{b}\rangle-\langle\vec{a},\vec{c}\rangle|-\langle\vec{b},\vec{c}\rangle\leqslant 1$, 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 $|\langle\vec{a},\vec{b}\rangle+\langle\vec{a},\vec{c}\rangle+\langle\vec{a}',\vec{b}\rangle-\langle\vec{a}',\vec{c}\rangle|\leqslant 2$, 可以画 $|3\cos\theta-\cos 3\theta|$ 图像

GHZ 定理 对于 3 粒子纠缠态, 存在一组对易可观测量, 直接确定地(而不是统计地) 给出与经典不相容的结果

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
任何双态量子体系都可称为一个 量子比特, 状态 $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \xlongequal[\text{取}\alpha\text{为实}]{\text{归一}} \cos\frac{\theta}{2}|0\rangle+\mathrm{e}^{\mathrm{i}\varphi}\sin\frac{\theta}{2}|1\rangle$

二维复向量空间中单位向量 → 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 $S(\hat{\rho})=\mathrm{tr}(\hat{\rho}\,\mathrm{lb}\,\hat{\rho})=-\sum_j\lambda_j\,\mathrm{lb}(\lambda_j)$

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 ⩽ 香农熵, 仅当 $|\psi_j\rangle$ 正交时取等

定理 非正交的量子态不能可靠区分(以概率 1 得不同结果) (否则就可以利用纠缠对超光速通讯了)

「设存在测量 E_i, $i=1,2$ 使 $\langle\psi_i|E_i|\psi_i\rangle=1$, 由测量算符完备, 有 $\sum_i\langle\psi_1|E_i|\psi_1\rangle=1$, 从而 $\langle\psi_1|E_2|\psi_1\rangle=1-1=0$ 然而 $|\psi_1\rangle,|\psi_2\rangle$ 并非正交, 与 $\langle\psi_2|E_2|\psi_2\rangle=1$ 矛盾」

例 要区分 $|\psi_1\rangle=|0\rangle$, $|\psi_2\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, 靠投影测量有概率误判, 用 POVM 测量可不误判(代价是有概率不能区分):

$E_1=\frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1|$, $E_2=\frac{\sqrt{2}}{1+\sqrt{2}}\frac{1}{2}(|0\rangle-|1\rangle)(\langle 0|-\langle 1|)$, $E_3=I-E_1-E_2$

测得 1 必为 ψ_2, 测得 2 必为 ψ_1, 测得 3 无法判断 (Q: 实验如何实现?)

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子比特

superdense coding
超密编码 Alice 和 Bob 分别持 EPR 对中的一个,Alice 想把 2 比特信息传给 Bob, 若 $|00\rangle$ 不动, 若 $|01\rangle$

做 X 门, 若 $|10\rangle$ 做 Z 门, 若 $|11\rangle$ 做 $ZX=\mathrm{i}Y$, 然后把她手中的量子比特传给 Bob, Bob 做贝尔基测量即可

量子门

quantum gate
量子门 幺正性是唯一的要求, 故总可逆 (任意 2×2 幺正矩阵可分解为⟨ 线路 ⟩)

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) , $Y=\begin{bmatrix}0&-\mathrm{i}\\\mathrm{i}&0\end{bmatrix}$, $Z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$

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

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

[对于 $\hat{\sigma}_n^2=I$ 有 $\mathrm{e}^{\mathrm{i}\hat{\sigma}_n\theta}=I\cos\theta+\mathrm{i}\hat{\sigma}_n\sin\theta$], 例 $\hat{R}_z(\theta)=\begin{bmatrix}\mathrm{e}^{-\mathrm{i}\theta/2}&0\\0&\mathrm{e}^{\mathrm{i}\theta/2}\end{bmatrix}$

常用 线路恒等式 $XYX=-Y$, $X\hat{R}_y(\theta)X=\hat{R}_y(-\theta)$

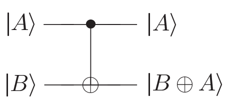
$HXH=Z$, $HYH=-Y$, $HZH=X$, $HTH=\hat{R}_x(\frac{\pi}{4})$

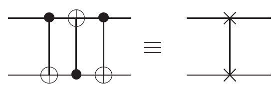
定理 任意单量子比特可分解为 $U=\mathrm{e}^{\mathrm{i}\alpha}\hat{R}_n(\theta)=\mathrm{e}^{\mathrm{i}\alpha}\hat{R}_z(\beta)\hat{R}_y(\gamma)\hat{R}_z(\delta)\to\mathrm{e}^{\mathrm{i}\alpha}AXBXC$

多量子比特门:

Controlled NOT
受控非门 $|$控制 c, 目标 $t\rangle\to|c,t\oplus c\rangle$ (控制比特为 0 则目标比特不变, 为 1 则翻转)

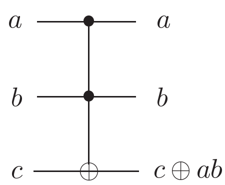
$U_{\mathrm{CN}}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$ $U_{\mathrm{SW}}=\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$ $H^{\otimes2}=\left[\begin{array}{cc|cc}1&1&1&1\\1&-1&1&-1\\\hline1&1&-1&-1\\1&-1&-1&1\end{array}\right]$





swap
对换 3 个 CNOT , 中间的反放 [$|a,b\rangle\to|a,a\oplus b\rangle\to|a\oplus(a\oplus b),a\oplus b\rangle=|b,a\oplus b\rangle\to|b,a\rangle$]

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



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 $c=1$
→ 故量子机可以做经典计算

用 Toffoli 门就可以构造出可逆的经典计算电路, 完成计算之后, 再把逻辑门按照逆序操作一次, 我们会发现整个计算过程并没有消耗能量。

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 → 通用门 (经典的与非门不可逆)

最早确认的一组是两比特的控制非门和两个正交的单比特逻辑门。

后来 Yaoyun Shi2002 证明只用 Toffoli 门加上单比特的 Hadamard 门就可以构造出任意的量子电路。

这个结论有可以用下面这句话概括: 量子计算超越经典计算的地方就在于多了单比特的 Hadamard 门, 或者说所有的量子计算算法不过就是经典计算机加上 Hadamard 门。

量子线路

initialization operation rotation superposition entanglement detection
① 初始化 ② 操作 (经典: 单:NOT, 双:NAND, 量子: 单:旋转 → 叠加, 双:CNOT → 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

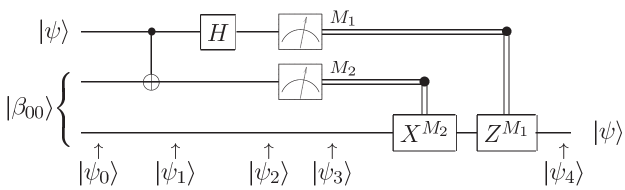
no-cloning theorem
$\boxed{\text{不可克隆定理}}$ 不可能制作未知量子态的拷贝「源于量子理论是线性的」(可以有以概率成功克隆的方法)
「若 $\exists U$ 能 $|00\rangle \xrightarrow{U} |00\rangle$, $|10\rangle \xrightarrow{U} |11\rangle$, 则对于叠加态 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 有 $|\psi 0\rangle \xrightarrow{U} (\alpha|00\rangle + \beta|11\rangle) \neq |\psi\rangle \otimes |\psi\rangle$ 」
(U_{CN} 可以拷贝经典态)

应用举例

Bell state / EPR pair
$\boxed{\text{贝尔态 / EPR 对}}$ 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 $|\beta_{ab}\rangle$

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

quantum teleportation
$\boxed{\text{量子传态}}$ 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, Alice 持有左边那个, Bob 持右边那个, Alice 想把 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 传给 Bob, 她把 $|\psi\rangle$ 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 Bob 结果(双线), Bob 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 」



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

$|\psi_3\rangle = \frac{1}{2}(|00\rangle\lceil(\alpha|0\rangle + \beta|1\rangle)\rfloor + |01\rangle\lceil(\alpha|1\rangle + \beta|0\rangle)\rfloor + |10\rangle\lceil(\alpha|0\rangle - \beta|1\rangle)\rfloor + |11\rangle\lceil(\alpha|1\rangle - \beta|0\rangle)\rfloor)$
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
当 Alice 测量后, 未传经典消息前,Bob 端是 4 种量子态经典叠加, 可算得其密度矩阵为 $\hat{\rho} = \frac{I}{2}$ 不含 $|\psi\rangle$ 的信息

Greenberger–Horne–Zeilinger state
$\boxed{\text{GHZ 态}}$ 3 量子比特的纠缠态 $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) = (|xxx\rangle + |x\overline{x}\overline{x}\rangle + |\overline{x}x\overline{x}\rangle + |\overline{x}\overline{x}x\rangle)$
特点: 任意 2 者一对可确定第 3 者手中的态 $\rightarrow$ QSS

量子计算

quantum computation
$\boxed{\text{量子计算}}$

$\boxed{\text{量子并行}}$ 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)

discrete logarithm factoring
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 (隐含子群问题,离散对数,求因子(肖氏算法),Deutsch 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
quadratic
* 量子搜索可视为一种量子模拟问题的解

quantum counting
$\boxed{\text{量子计数}}$ 结合了搜索和傅变两者

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 $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i} jk/N} x_j$

有幺正变换 $|j\rangle \xrightarrow{U} \frac{1}{N}\sum_{k=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i} jk/N}|k\rangle$, 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 $N\,\mathrm{lb}(N)=n2^n$ 步, 量子傅氏变换用 $(\mathrm{lb}\,N)^2=n^2$ 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

精

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

参

Preskill@Caltech 讲义

编者：LePtC　笔记项目主页：http://leptc.github.io/lenote

Last compiled on 2015/06/30 at 17:40:00