量子计算和量子信息

引言

- 量子信息涉及的领域：
  量子力学（或者量子场论），计算机科学，信息论，密码系统

- **研究的动机：**

1. 器件越小，越会受到量子效应干扰
2. 强Church-Turing问题在量子层面上是否成立？
   注：
   1 . 强Church-Turing问题：任何算法过程都可以用Turing机进行有效模拟。
   2 .“有效”和“非有效”：有效模拟指解决问题的时间是问题规模的多项式，非有效模拟需要的时间是超多项式时间。
   3 .Turing机：Turing机是一个7元组：$M = \langle Q, \Gamma, b, \Sigma, \delta, q_0, F \rangle$
   其中：

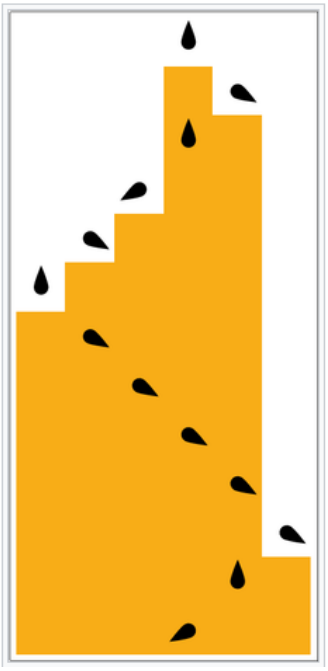
- Q是一个有限的非空集合，代表状态寄存器允许的状态
- Γ也是一个有限的集合，代表磁带字母表集合（整个运算过程中允许出现的字母集合）
- b是空格，唯一一个允许在磁带上有无限多个的符号
- Σ为最初允许在磁带上写入的字母集合，$\Sigma \subseteq \Gamma \backslash \{b\}$，不一定等于$\Gamma \backslash \{b\}$
- $q_0 \in Q$是寄存器初态
- $F \subseteq Q$是寄存器末态，为这个态时停止计算
- $\delta : (Q \backslash F) \times \Gamma \to Q \times \Gamma \times \{L, R\}$为映射，指出每一步寄存器动向，$L$向左，$R$向右，这里$Q$表示寄存器状态空间，而$\Gamma$表示当前寄存器所指磁带位置的状态空间，即磁带字母表集合

Turing机例子：

- $Q = \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{HALT}\}$寄存器态集合
- $\Gamma = \{0, 1\}$磁带字母表集合
- $b = 0$空格元素
- $\Sigma = \{1\}$初始允许写入字母表集合
- $q_0 = \mathbf{A}$寄存器初始状态
- $F = \{\mathrm{HALT}\}$寄存器末态
- δ函数如下：

Tape symbol	Current state A			Current state B			Current state C		
	Write symbol	Move tape	Next state	Write symbol	Move tape	Next state	Write symbol	Move tape	Next state
0	1	R	**B**	1	L	**A**	1	L	**B**
1	1	L	**C**	1	R	**B**	1	R	**HALT**

磁带状态和运算过程：



黑点代表指针位置，向上代表状态A，向右代表状态B，向左代表状态C，白色代表0，橙色代表1，时间方向从上到下。

对计算的一些思考：

（来自与天津大学杨润秋教授的一些讨论，部分观点出于自身思考，没有论证）
第一个问题，什么是最快的计算机？其实现实生活的世界也许就是最快的计算机，（当然不同物质结构的计算速度不一样），为什么这样说？ 因为我们可以问一个稍显哲学的问题，我们能否100%预言未来？（可以考虑量子效应，原则上我们只要知道了整个宇宙的态函数，加上计算速度无穷快的计算机我们就可以预言未来，量子力学固有的概率问题是在于我们没有完全考虑整个体系，原则上测量器也是量子态构成的）假如我们能够100%预言未来，那当我们计算出预言的结果的时候未来是不是已经到来？（这里预言是需要时间的）所以我们可以如下的观点看待世界：世界其实是一个很大的计算机，不断的在计算未来，当某一个未来点的结果计算完成的时候，未来即在此时间点到来。
所以对计算问题的考虑并不只是为了完成建设更快计算机的任务，其中还蕴藏了丰富的物理原理有待发掘。

关于Turing机

其实Turing是模拟人对计算的做法，我们通常用草稿纸进行计算也是一样的，将一些中间的结果写在草稿纸上然后计算到某一步后参考前面的结果然后进行计算。

对Church-Turing问题的挑战

1. 随机性Solovay-Strassen测试算法：该算法不确定一个整数是素数或是合数。而是给出一种可能性，但是重复几次就几乎可以确定一个整数是素数或是合数，需要注意的是这个算法需要引入一个随机数。
2. 好像此算法在经典的确定型的Turing机上无法有效的进行。
3. 修改Church-Turing论题：任何算法过程都可以用概率Turing机进行有效模拟
4. 可以理解为我们通常在解决问题的时候先猜几个答案，然后进行验证。有趣的是穷举或某种确定的方法不能有效的模拟猜测然后验证的方法（所以不难理解现代理论物理都是猜个答案然后验证--大胆猜测，小心求证）
5. 所以如果我们大脑能产生随机数，那我们能有效的理解这个宇宙这件事应该是能够办到的（雾）
6. 上述对Turing问题的修改令人不安，如果又发现另外一个随机Turing机不能有效求解的计算问题，那Turing论题就又要修改。所以是否能找到能有效模拟任何物理系统的计算装置？这仍然是一个开放性的问题。但我们很自然的要问在量子领域，量子计算机是否比经典计算机或随机经典计算机更为强大的计算能力。换句话说量子算法能达到的结果能否通过经典算法或随机经典算法有效解决。

7. 进而我们还要在弦论，量子引力理论里面问同样的问题。
8. 目前为止还未发现可以有效模拟特定量子算法的经典计算机，此外，另一方面我们也不知道量子计算机是否可以有效解决所有的经典算法能解决的问题。现在只是用来解决一些特定问题。

信息论

量子理论的另一个比较有趣的方面是在信息论中的应用
现代信息论的奠基人是Shannon，他给出了两个关键的问题：

1. 通过信道传输信息需要哪些资源
2. 可以保护信息避免噪声的干扰吗?

Shannon通过两个定理给出了这两个问题的解决方案，分别为：无噪声信道编码定理和有噪声信道编码定理。

1. 无噪声编码定理例子
   具体定理留在后面讨论，这里只举一个例子说明：
   考虑一个理想模型，一个只输出0和1的独立同分布信源，输出0的概率是p，输出1的概率是$1-p$，它输出了一个序列$X_1, X_2, X_3, \cdots$，简单起见我们考虑有限的情况$X_1, \cdots, X_n$。很显然根据二项分布，当n非常大时，存在一系列典型序列我们记为$x_1, \cdots, x_n$，他们出现的概率最大，其中0出现p次，1出现$1-p$次。
   我们抽取这一系列典型序列中的一个，它出现的概率为：

$$p\left(x_1, \cdots, x_n\right)=p\left(x_1\right) p\left(x_2\right) \cdots p\left(x_n\right)=p^{np}(1-p)^{(1-p)n}$$

   两边取对数有：

$$\begin{aligned}-\log p\left(x_1, \cdots, x_n\right) &= -np \log p-n(1-p) \log (1-p) \\ &= nH(X)\end{aligned}$$

   其中$H(X)=-p \log (p)-(1-p) \log (1-p)$称之为源分布的熵，也可写为$H(p)$，log的基底取2。则每一个典型序列的概率为：$p\left(x_1, \cdots, x_n\right)=2^{-nH(X)}$。由于典型序列远远大于非典型序列，所以可以认为此概率为：

$$p\left(x_1, \cdots, x_n\right)=\frac{\text{一个典型序列}}{\text{所有序列}} \approx \frac{\text{一个典型序列}}{\text{所有典型序列}}$$

   所以我们可以得到所有典型序列的个数为$2^{nH(X)}$，注意$H(X)$是小于1的。对比，正常全记录下来所有序列有2^n个。所以我们我们只需要$nH(X)$个比特就可以标识一个典型序列，即压缩。若不是典型序列则压缩失败，但当n趋于无穷大时，失败概率趋于无穷小。于是用$nR > nH(X)$个比特来压缩是可靠的R称之为压缩比率。反之$R < H(X)$则压缩不可靠。
2. 有噪声编码定理例子

- Hamming距离：两串序列$A=\{x_1, x_2, x_3, \ldots\}$,$B=\{y_1, y_2, y_3, \ldots\}$，他们之间的距离定义为他们对应元素取值不同的个数，例如$A=\{1,0,1,0,1\}$，$B=\{1,0,0,1,1\}$他们的距离为2。可以明显看出此定义满足距离定义：
  1 . 非负性：$d(x, y)>0$
  2 . $d(x, y)=d(y, x)$
  3 . 三角不等式$d(x, z) \leqslant d(x, y)+d(y, z)$：由于$AB$中的元素只有0和1，故按照定义$d(A, B)=\Sigma_i\left|x_i-y_i\right|$，明显绝对值满足三角不等式。（如不满足三角不等式会违反两点之间线段最短公理）
- 现在考虑一个二元对称信道：

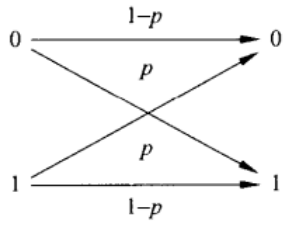


图 12.4　二元对称信道

我们希望通过信道的n次使用来传输nR比特的信息，设我们要传输的信息有$(q, 1-q)$的到$(0,1)$的概率分布，我们称之为码的先验分布。此时在这样一个先验分布下产生一个序列$x=\left(x_1, \cdots, x_n\right)$，很明显我们预期大概有$np$

个比特被翻转，于是所有的被翻转后的序列在一个半径为np的Hamming球内：

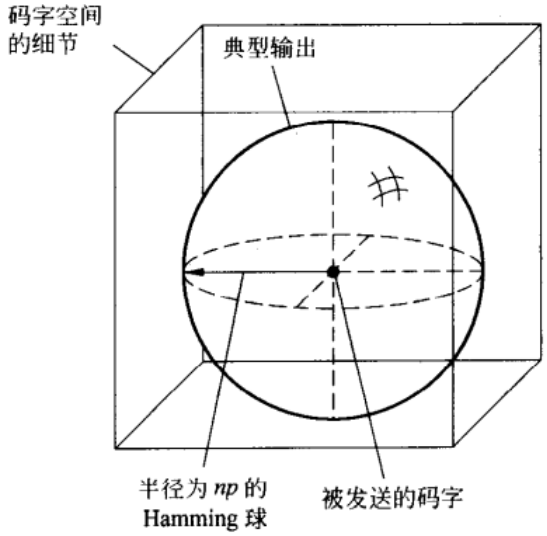


图 12.5　设码字 x^1 被二元对称信道的 n 次使用所传送. 那么信道的一个典型输出就是围绕被发送序列的半径为 np 的 Hamming 球(本图是图 12.6 的局部放大).

在这样一个Hamming球内大概有多少个元素？参考上面无噪声信道编码的例子，我们一个序列有$(p, 1-p)$的概率到$(翻转, 不翻转)$，那么它的典型翻转（对应典型序列）数目为$2^{nH(p)}$

- 现在我们考虑信源的独立同分布序列$(X_1, \cdots, X_n)$通过二元对称信道传递后为$(Y_1, \cdots, Y_n)$，它的典型值有$2^{nH(Y)}$（这里只考虑典型值，发送的序列也是考虑典型值，就是说两个信道编码定理考虑的所有序列都是典型值，因为，非典型值在n比较大的时候比较少）个。
- 现在考虑如何才算是能准确的传输信息，很明显我发送的一个序列，发送后会很大概率随机的在一个Hamming球中，于是我只要将整个Hamming球中的所有序列都认为是原来的序列即可准确的通过发送后的序列还原出原来的序列。即一个球代表原来的一个序列：

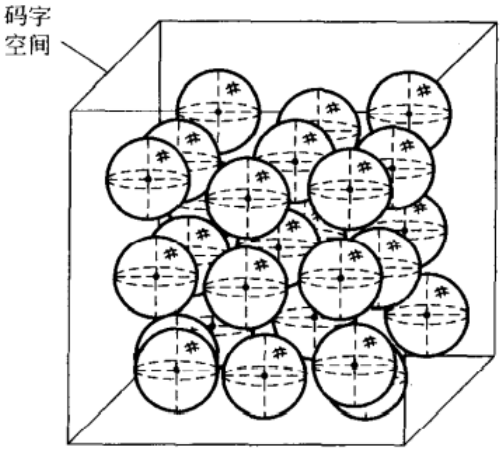


图 12.6　典型输出的 Hamming 球包围的为二元对称信道随机选取的码字. 图 12.5 给出一个单个码字的局部.

于是我们希望发送nR比特的信息，我们需要的空间的大小为$2^{nR} \times 2^{nH(p)}$，而通过二元对称信道发送后的空间大小为$2^{nH(Y)}$，很明显如果有：

$$2^{nR} \times 2^{nH(p)} < 2^{nH(Y)}$$

则Hamming球是可以几乎不重叠的，于是我们理论上可以精确的还原传输前的信息。其中空间$(Y_1, \cdots, Y_n)$受到空间$(X_1, \cdots, X_n)$的影响，所以可以通过调节$(X_1, \cdots, X_n)$的先验分布来使得$H(Y) = 1$（$H(Y)$是Shannon熵）。于是：

$$R < H(Y) - H(p) = 1 - H(p)$$

R称之为信道容量，描述了最多以R比率传输信息。

- 注意这里只是给了一个理论的上限，没有给具体的纠错码的构造，这个上限通常称为Shannon极限，Arikan在它的极化码中给出了达到Shannon极限的方法，一个比较吹牛的视频可以参考 https://www.bilibili.com/video/BV1fq4y1g7hq?from=search&seid=13632969387431513612&spm_id_from=333.337.0.0

当进入量子领域后以上的极限会有突破，如果可能的话以后会讲到：

- 超密编码：传送一个量子比特就可以传送两个景点信息
- 一个信道容量为零的拷贝与它自身相向发送信息可以产生非零信道

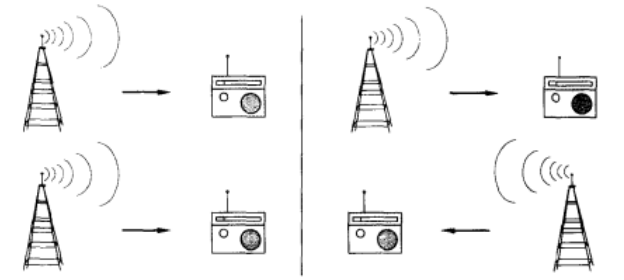


图 1.1 从经典角度看，两个噪声很大的零容量信道并排运转，联合的信道发送信息的容量为零，若一个信道反向，不奇怪，发送信息的容量仍为零，而从量子力学角度上，掉转一个零容量信道真的可以让我们发送信息！

在密码学中的应用

1. 私钥密码系统
   私钥密码系统的安全性在于只有参与者A和B知道秘钥，其他人截获了信息也不知道如何解密，比如方言。但是私钥密码系统的问题在于秘钥的分配，秘钥的分配过程中是可能存在泄露的。担当这个问题在量子中考虑的时候就可以有完全保密的私钥系统，在分配私钥的时候用量子线路传输，一旦A到B的私钥分配被C截获，B就不会收到正确的私钥（量子不可克隆原理），所以可以实现绝对安全的私钥系统。
2. 公钥密码系统
   公钥密码系统为：A用一个预先由B公布的公钥加密信息，要用此公钥逆向解出原来的信息是十分复杂的，一般是一些多项式时间无法解决的问题，但对于某些复杂的问题存在一些私钥，通过这些私钥可以很快的还原原来的信息，于是B可以通过掌握的私钥快速还原信息。
   公钥密码系统的安全性在于经典计算机无法快速有效的解决一类问题（多项式时间），一般为建立在计算机分解质因数是困难的观念下，联系Church-Turing问题，量子计算机其实可以快速的分解质因数（Shor算法），于是对于目前的某些密码系统，量子计算机是可以破解的。