结绳与量子计算

王正汉

（美国微软研究院　2010 年 4 月）

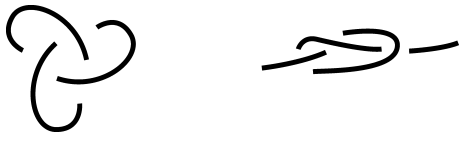
古人结绳记事. 延续祖先的思维，我们用绳圈来描述粒子的轨迹；记录它们的运动；进而探讨绳圈数学的应用——拓扑量子计算.

绳圈的数学叫纽结论，是一门趣味盎然的学科. 在此我们仅介绍新的纽结不变量——琼斯多项式（Jones polynomial）及其在量子计算中的应用. 如果读者有兴趣，我们推荐姜伯驹教授的书：绳圈的数学. 纽结论不仅是一门高深的数学理论，也在物理，生物和量子计算机学科中有许多的应用. 从上世纪八十年代，量子力学的思想深刻地影响着拓扑学的发展，形成量子拓扑学. 留美数学家林晓松教授(1957—2007)对量子纽结论的发展作出了很多开创性的贡献. 谨以此文纪念这位重要的拓扑学家. 他所钟爱的量子纽结论正走出数学，成为现代科技的一个有机部分.

上半部

无论是系领带，还是系鞋带，我们都是在用绳子打结. 但日常生活中的结和数学家们研究的结有所不同. 首先数学家用来打结的不是绳子，而是理想化的绳子——曲线；其次数学家的结是一个绳圈的模型——闭路线圈，也就是说绳子要首尾相连. 如果不是首尾相连，那么不管多么复杂的结都能解开，也就是说变成直线段.

纽结论是研究理想化的结的一门数学学科，它是拓扑学的一个重要分支. 平面上的圆代表数学家最简单的纽结，叫做平凡结. 一个不能变成圆的纽结叫做非平凡结. 是否存在非平凡结呢？只要我们用绳子做一些实验，就不难相信存在非平凡结，也就是死结. 下面的结是最简单的非平凡结(左图)，叫三叶结. 许多水手爱打这个结(右图)：



（三叶结）

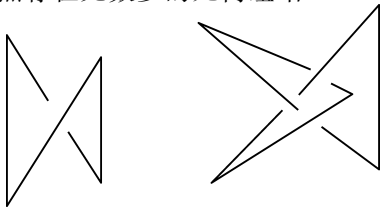
如果把右边的结头尾连在一起，但不可以从任何地方剪断绳子，不管我们怎样做，我们都不能把它变成平面上的圆. 尽管很直观，但要证明存在非平凡结却非易事，因为我们需要排除任何可能的解法，但可能的解法多得无法想像. 我们怎样才能肯定所有的解法都试过了呢？下面我们看看拓扑学家怎样解决这个问题的.

1　纽结论

1.1　纽结

拓扑学家用曲线打结. 曲线的严格数学理论要用到微积分. 为了避免这些知识，我们将用直线段打结. 因为光滑曲线可以看成由很短的直线段构成的，所以这样得到的理论跟用曲线得到的理论是等价的. 但这个理论只用到非常初等的知识.

现在我们严格定义我们的研究对象. 如果有一些直线段，它们可以长短不一，然后一段接一段地把它们在空间连在一起形成一个闭线圈. 如果构成闭线圈的任何两条直线段或者不相交或者只交于一个端点，我们就把这个闭线圈叫做一个几何纽结. 比如下面的几何纽结分别代表平凡结和三叶结. 平面上的任何一个多边形都是一个几何纽结. 显然存在无数多的几何纽结.



（平凡结和三叶结）

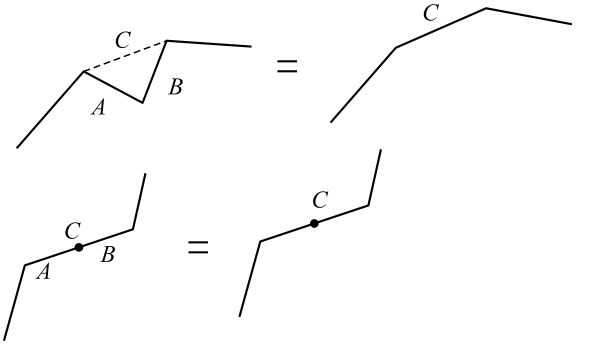
拓扑学的一个基本特征是不关心物体的长短,厚薄,粗细. 对拓扑学家来说,所有大大小小不同形状的三角形都代表同一个的纽结——平凡结. 不仅如此,所有平面上的多边形都代表同一个纽结. 如果我们是用绳子打结,这很容易理解. 由绳子做成的三角形是很容易变成四边形,五边形. 反过来也一样,四边形和五边形也可以变成三角形. 尽管我们的理论将会是基于由直线段打成的结,但我们可以用绳子打成的结来思考.

为了交流方便,我们引进一些名词. 一个几何纽结上的任何一条直线段,我们都叫它是这个几何纽结的一条边. 拓扑学家只关心纽结的所谓拓扑性质. 像一条边有多长是不重要的. 为了研究几何纽结的拓扑性质,我们会引进一个拓扑等价关系. 两个拓扑等价的几何纽结将会被看成是同一个拓扑纽结,简称纽结. 从概念上来讲,纽结和几何纽结是完全不同的. 几何纽结是具体的,纽结是抽象的.

严格的讲,一个纽结是由所有拓扑等价的几何纽结所形成的等价类. 所以,一个纽结代表一个由那些拓扑等价的几何纽结形成的集合. 和数类比,一个几何纽结像一个箱子里的苹果,而一个纽结是箱子里苹果的数目. 我们指出一个可能引起的混淆:拓扑学家经常不分纽结和纽结类,提到纽结而实际是指纽结类. 我们说的纽结严格地讲对应于拓扑学家的纽结类,而几何纽结对应于拓扑学家的纽结.

几何纽结间的拓扑等价关系定义很复杂,这也是我们需要考虑直线段的原因.

给定一个几何纽结,叫它 K,和它的两条相联的边,叫它们 A 和 B. 假设 A 的末端连在 B 的首端. 用一条新线段连接 A 的首端和 B 的末端,我们叫这一条新的线段 C.(见下图) 如果 C 和 K 别的边都不相交(但可以和 A, B 重和),我们可以从 K 的边中拿掉边 A 和 边 B,然后加入 C 得到一个新的几何纽结,叫它 K'. 我们把从边 A, B 到边 C 或者反过来从边 C 到边 A, B 的变换叫做一个三角形变换. 注意三角形变换的一种特殊情况,在一条边的内部加一个点变成两条边,或者反过来. 如果由 A, B, C 所形成的三角形的内部和 K 的除 A, B 以外的任何边都不相交,我们称这样的三角形变换为 Δ-变换. 两个几何纽结 K 和 K' 是拓扑等价的如果 K 能通过有限次的 Δ-变换变成 K'. 我们以后将拓扑等价简称为等价.



(Δ-变换)

如果 K 是由 K' 通过一个三角形变换得到的,那么 K 和 K' 有时是等价的,有时是不等价. 本节开始的平凡结可以从它右边的三叶结通过一个三角形变换得到,但它们是不等价的.

最简单的纽结是平凡结,它是包括所有三角形在内的几何纽结的等价类. 实际上,平面上所有多边形都代表平凡结. 给一个纽结,我们叫它的任何一个几何纽结为它的一个代表.

思考题:

1. 证明平面上所有多边形都可以通过有限次 Δ-变换变成一个三角形.
2. 证明所有四边形,不限于平面上,都等价于三角形.

1.2 纽结不变量

我们都相信存在非平凡结,但怎样证明呢?也就是说,存在一个几何纽结,无论一个人多么聪明,花多长时间,做多少 Δ-变换,都不可能把这个几何纽结变成一个三角形? 拓扑学家的想法很简单,引进所谓的不变量. 我们给每一个几何纽结一个我们熟悉的量,像一个数,或者一个多项式. 这个量叫做不变量,如果这个量在任何 Δ-变换下不变. 即两个等价的几何纽结所得到的量是一样的. 但不等价的纽结也有可能得到同样的量.

定义不变量是一件很容易的事. 譬如,我们可以给所有平凡几何结 1,给所有别的几何纽结 0. 但这个不变量对于研究纽结来说,毫无用处. 考虑所有纽结形成的集合,从这个集合到实数的

任何一个映射都是一个纽结不变量.用这个想法,我们可以定义一个有用,但很难计算的纽结不变量:离散长度. 给定一个纽结,把这个集合里的所有几何纽结的边数的最小值取出来,这是一个正整数. 我们把这个正整数叫做这个纽结的离散长度. 它反映出如果真的用绳子打这个结,我们至少需要一定长度的绳子. 不难证明,平凡结的离散长度是 3,而三叶结的离散长度是 6.本节开始的五边三叶结实际上需要六条边.

纽结论的重要问题是如何分类纽结. 即给出一个几何纽结的集合使得在这个集合里每一个纽结都有而且只有一个几何纽结代表. 拓扑学家希望能找到一个完备的纽结不变量,即一个不变量使得不同的纽结会有不同的不变量. 如果我们有这样一个不变量,纽结的分类就简化成这个不变量的计算.存在不少的完备纽结不变量,但我们还没有发现完备而容易计算的不变量,或许这样的不变量是不存在的.

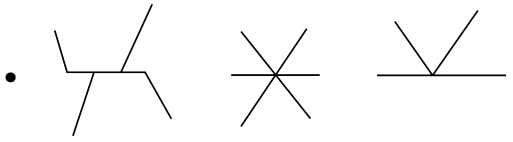
思考题:

1. 当离散长度足够大时,我们可以得到不同的纽结. 最小的离散长度使我们可以得到不同的纽结是多少? 我不知道答案.
2. 在纽结上取个方向,我们就可以定义两条相邻边的角度. 用这些角度定义一个纽结不变量.

1.3　纽结投影

想研究纽结,我们就要有办法把所有纽结都画出来. 拓扑学家的办法是利用纽结在平面上的投影. 前面我们已经看到,在平面上是画不出非平凡结的. 纽结是我们所生存的空间的一个现象. 如果你听说过四维或更高维空间,在那里面同样画不出非平凡结. 为了能在平面上表示出非平凡结,我们就必须记住纽结的一些空间性质.

给一个几何纽结,想像在它的后面远处有一个屏幕.如果我们把这个几何纽结投影到这个屏幕上会是什么样子? 一条线段的投影是一条线段或是一个点,所以纽结的投影是一个由线段组成的闭路,但可能有很多交点:双重点,三重点等等. 如果我们稍微移动一下后面的屏幕,我们可以做到这样:没有任何一条直线段被投影成一个点,而且只有直交的双重交点;任何其它类型的交点都叫奇点. 没有奇点的纽结投影叫正则投影. 这又是这样一个事实,虽然不难相信,但严格证明并不显然. 有兴趣的同学可以自己试试.

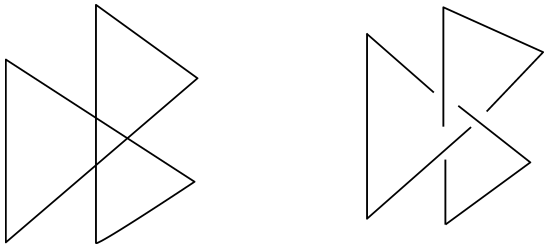


(奇点)

一个正则投影的每一个双重点都是两条边投影的交点. 这两条边一上一下(每一个双重点都是两个点的投影,我们把离屏幕近的那一点所在的那条边叫下.)如果我们在一个几何纽结的一个正则投影的每一个双重点处都记下那两条边的上下关系,我们就得到了一个纽结图. 我们把带有上下信息的双重点称做交叉点. 交叉点分为上交叉点和下交叉点:

(交叉点)

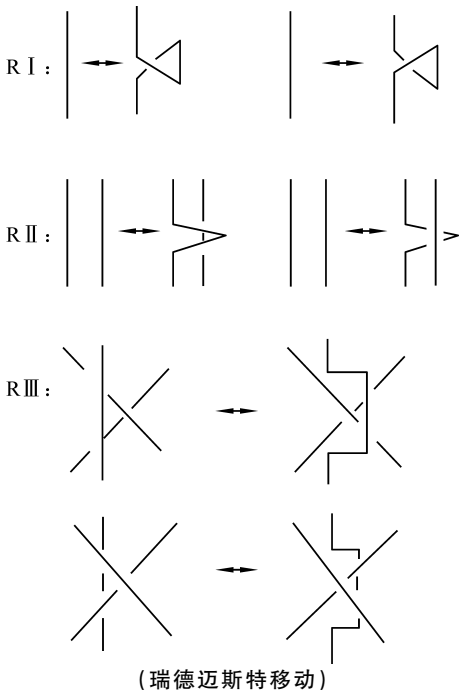
如果可以用曲线,通常我们会把下面那条边画在平面上,而上面的那条边在双重点附近画在平面上面. 但如果只能用直线段,我们可以把上面那条直线段变成两条线段稍微高于平面,使得原来的端点的投影都在平面上. 我们把这样由正则投影图得到的图叫纽结图. 一个几何纽结和它的任何一个纽结图是拓扑等价的,所以在很多情况下,我们只需要考虑纽结图.



(正则投影)

一个纽结会有很多纽结图,但它们全都等价. 给定两个纽结图,怎样决定它们是否代表同一个纽结呢? 原则上我们已经知道答案:只要考虑所有 Δ-变换的正则投影. 实际上这个办法却很难应用,因为 Δ-变换中的三角形可以很大. 纽结论里的一个著名定理把 Δ-变换简化到下面三组变换,

叫瑞德迈斯特(Reidemeister)移动 RI, RII, RIII, 反之亦然.

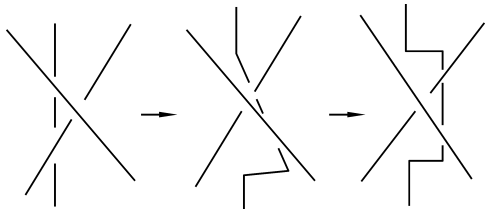


(瑞德迈斯特移动)

我们可以证明:

瑞德迈斯特定理 两个纽结图 D 和 D' 所代表的纽结是等价的当且仅当 D 能通过有限次的瑞德迈斯特移动变成 D'.

由于这个定理, 纽结论也可以只研究纽结图和它们在瑞德迈斯特移动下的等价类. 以下一组图证明 RIII 移动可以用 Δ-变换实现.



(RIII 与 Δ-变换)

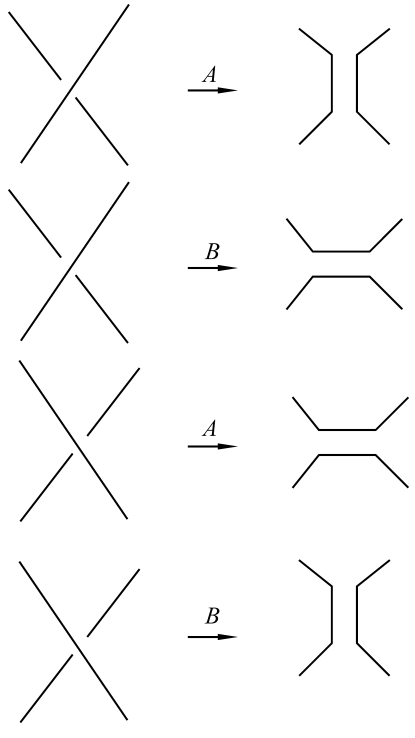
思考题:

1. 证明只有一个或两个交叉点的纽结图总表示平凡结.
2. 证明所有纽结的集合是可数的, 即我们可以把它们和正整数一一对应.

2 琼斯多项式

1984 年, 新西兰数学家琼斯(V. Jones)发现了一个全新的纽结不变量, 叫做琼斯多项式. 琼斯多项式的发现引起了纽结论里的一场革命, 进而推动了一个新的拓扑方向——量子拓扑的产生. 琼斯多项式其实不是严格意义下的多项式, 因为它的变量的次方可以是负整数和分数.

我们首先引进一些定义和记号. 假设 D 是一个有 n 个交叉点的纽结图. 如果给每个交叉点一个标号 A 或 B, 我们就叫 D 的一个态, 记作 s. 给定 D 上一个交叉点和一个标号 A 或 B, 我们可以在这个交叉点的附近做一个手术 (surgery):



(手术)

上图里的手术的规则是这样的: 在交叉点的附近, 从上面的边逆时针旋转到下面的边, 上面的边会扫过两个区域(一个交叉点把平面分成四个区域)叫 A 区, 另外两个叫 B 区. A 手术就是打通 A 区, 而 B 手术就是打通 B 区.

假设 t 是一个参数变量. 给定 D 的一个态 s, 那么每一个交叉点都有一个 A 或 B. 如果是 A, 我们就做 A 手术, 如果是 B, 我们就做 B 手术. 每一个手术都从纽结图中去掉一个交叉点, 当所有手术完后, 我们得到平面上的一些闭线路, 这些闭线路的个数记作 $d(s)$. 我们用 $s(A)$ 记态 s 上 A 型交叉点的个数, 同样用 $s(B)$ 记态 s 上 B 型交叉点的个数.

让$<s>=t^{\frac{s(B)-s(A)}{4}}\cdot(-t^{\frac{1}{2}}-t^{-\frac{1}{2}})^{d(s)}$.

定义$<D>=\sum<s>$,这个和一共有 2^n 项. 我们叫$<D>$为 D 的考夫曼（L. Kauffman）括号.

每个纽结图有两个方向:从图上的某点出发,沿纽结图朝前或后走一圈. 取定纽结图 D 的一个定向,每条边都有一个方向. 我们给每个交叉点一个符号:正负 1 如下:

（符号）

改任何一个箭头,符号正负 1 互换. 注意到如果我们取得是另一个方向，因为每个交叉点的两条边方向同时改变，所以这个符号是不依赖于纽结的方向的.

把 D 的所有交叉点的符号的和记作 $w(D)$.

最后定义纽结图 D 的琼斯多项式

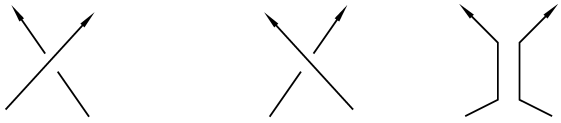
$$J(D;t)=(-1)^{w(D)}\cdot t^{\frac{3w(D)}{4}}\cdot<D>.$$

可以证明 $J(D;t)$ 在瑞德迈斯特移动下不变，所以确实是一个纽结不变量. 这就是著名的琼斯多项式. 给一个纽结 K，它的琼斯多项式 $J(K;t)$定义为 K 的任何纽结图的琼斯多项式.

平凡结的琼斯不变量是$-t^{\frac{1}{2}}-t^{-\frac{1}{2}}$,因为圆只有一个态:无交叉点,但有一个闭线路. 而三叶结的琼斯多项式是 $J(t)=(t+t^3-t^4)(-t^{\frac{1}{2}}-t^{-\frac{1}{2}})$. 所以三叶结一定是非平凡的.

由多个不相交的纽结组成的多条曲线叫链环. 拓扑学家除研究纽结外，也对链环感兴趣. 琼斯多项式可以定义在链环上，但链环必须有定向. 如果处理好定向，我们前面的所有讨论都对链环适用. 我们把细节留给读者. 给一个定向链环 L，它的琼斯多项式 也记作 $J(L;t)$.

有了链环的琼斯多项式，我们可以有一个计算琼斯多项式的线团（skein）关系式. 假设 L_+ 是一个链环图(带定向)，而 p 是 L_+ 上的一个交叉点. 如果我们把交叉点 p 的两条边上下换了，我们就有一个新的链环图，记作 L_-；我们也可以顺方向光滑 L_+，得到另一个链环图 L_0(见下图). 我们可以证明，这三个链环的琼斯多项式满足以下恒等式：



L_+　　L_-　　L_0

$$t^{-1}\cdot J(L_+;t)-t\cdot J(L_-;t)=(t^{\frac{1}{2}}-t^{-\frac{1}{2}})\cdot J(L_0;t)$$

（线团关系式）

用线团关系式，我们可以递推得计算琼斯多项式. 因为每一个定向链环的琼斯多项式 $J(L;t)$ 除以 $-t^{\frac{1}{2}}-t^{-\frac{1}{2}}$还是一个链环不变量，我们定义 $V(L;t)=\frac{J(L;t)}{-t^{\frac{1}{2}}-t^{-\frac{1}{2}}}$. 这样平凡结的不变量就变成 1. $V(L;t)$也叫琼斯多项式，也满足线团关系式.

琼斯多项式是一个非常重要的链环不变量. 然而从定义或线团关系式进行计算，非常复杂. 如果一个链环有个 n 交叉点，那么计算它的琼斯多项式就需要做 2^n 个和. 学过幂指数的都知道指数增长的速度:据估计整个可见宇宙里的基本粒子数不会超过 2^{200}. 所以计算 200 个交叉点的链环的琼斯多项式，要加的和数已经不可思议. 但有没有别的聪明办法高效地计算链环的琼斯多项式呢? 数学家们相信高效的算法是不存在的. 但是如果我们有量子计算机，我们就可以高效的逼近琼斯多项式的值. 下半部我们看看量子计算机是怎样做到的.

思考题:

1. 把每一个交叉点的上下互换,琼斯多项式怎样变化?
2. 改变链环的方向，琼斯多项式怎样变化?
3. 是否存在非平凡结而它的琼斯多项式和平凡结是一样的? 这个问题极难，我们还不知道答案.

下半部

大卫·希尔伯特(1862—1943)是伟大的德国数学家. 1900 年他在巴黎国际数学家大会上提出了 23 个当时未解决的数学问题. 这 23 个问题对上个世纪前半叶的数学发展产生了深远的影响.

其中的第十个问题是：给定一个多元整系数多项式 $f(x,y,\cdots,w)$，给出一个算法来决定 $f(x,y,\cdots,w)$是否有整数解. 希尔伯特并没有定义什么是算法，而且他下意识的相信算法是存在的. 1970 年数学家证明不存在算法可以解决这个问题. 但早在 1936 年，英国数学家阿兰·图灵(A. Turing，1912—1954)就发表了题为“可计算数及在决断问题中的应用”的文章. 在这篇文章中图灵严格定义了算法，并证明存在数学问题是没有算法来求解的. 图灵定义的算法被称作图灵机. 是计算机理论奠基性的工作之一. 图灵对逻辑学，密码学和现代计算机理论都有巨大的贡献. 在二次世界大战中，他帮助盟军解密了德国的著名 Enigma 密码机器，加快了盟军的胜利.

学过数学的人都有算法的经验. 即使一个问题有算法可解，也不意味着这个算法是可行的. 理论计算机的一个重要方向就是研究高效（efficient）的算法. 比如著名的求两个正整数最大公因子的欧几里德算法. 欧几里德算法不但简单，而且高效. 然而另一个问题：给定一个正整数，找出它的素因子分解. 不但至今没人能找到高效的算法，数学家相信高效的算法根本就不存在. 所以很多秘密都是基于这个假设. 如果某一天有人发现了一个高效的素因子分解办法，很多国家，银行和个人的秘密，包括因特网上的很多交易，就会被泄漏. 令人惊奇的是，1994 年美国数学家肖尔（P. Shor）发现量子计算模型可以高效地进行素因子分解. 量子计算模型是基于量子力学理论的计算模型. 它的实现非常困难. 实现量子计算的一种办法是基于纽结论——拓扑量子计算. 怎样用纽结计算呢？

3 计算模型

每一种物理理论，都伴随着一种计算模型. 经典物理的计算模型就是我们现在的计算机. 每一种计算模型都可以高效的解决一类问题. 因为量子物理包含经典物理，所以任何高效的经典算法都可以看成高效的量子算法. 我们希望量子计算可以解决一些经典计算不能高效解决的问题，像素因子分解. 虽然我们有高效的量子素因子分解算法，且没有高效的经典素因子分解算法，但我们并不能证明高效的经典素因子分解算法是不存在的. 所以我们也就不知道量子计算是否真的比经典计算更高效.

3.1 公开的秘密

研究算法效率的理论叫计算复杂性. 计算复杂性考虑我们是否能够高效地利用我们的资源来解决一类问题 . 资源可以是很多东西，比如时间，记忆，也可以是精确度，但我们不考虑财富. 我们用一个例子来说明它的用处. 假设两个离得很远的网友在网上下一盘重要的围棋，很久他们还没有下完，所以决定停下来以后再下，但谁都不想下最后一招棋，给对手时间仔细研究对策. 假设他们不想任何别人参与，怎么办呢？利用计算复杂性，我们可以有这样一个可行的办法：把围棋盘想像成平面坐标系，那么它的每个位置都可以记成一对数 (m,n)，m 和 n 在 1 和 19 之间. 如果 m 和 n 是单位数，在前面加个零，这样它们就都是两位数. 让下最后一招的那个人先想好他最后一招棋的位置，约定首先他自己私下找一对很大的素数 p 和 q ，而且 p 小于 q. p 的个位和十位数是 m，而 q 的个位和十位数是 n. 然后他把 p 和 q 乘起来，记作 r. 最后他只把答案 r 告诉他的对手. 如果想知道他的最后一步棋，就得知道 p 和 q. 如果选定 p 和 q 在两百位数左右，那么用现在最好的算法和最快的超级计算机，大概需要几十亿年才能算出 p 和 q. 如果我们有量子计算机，几天就可以做到. 美国 NSA 网站上就有一些数字让大家去分解，每分解上面的一个数，都有一笔不菲的奖金. 宇宙现在的寿命估计也只有 140 亿年，所以在有限的时间内，知道 p 和 q 的机率几乎为 0. 当他们准备再战的时候，走最后一步的那个人只要告诉对手 p 和 q，就可以知道他的最后一步棋的位置. 由于有高效的算法验证一个数是否是素数，而乘法更是高效的，很容易就知道有没有做弊. 这样最后一步棋就成为公开的秘密.

什么样的算法是高效的呢？考虑欧几里德算法. 给定两个正整数 m 和 n，我们要找出它们的最大公因子. 假设 m 大于 n，并且 n 大于 1. 欧几里德算法如下：

第一步：

用 m 除以 n，假设商为 q，而余数为 r，即 $m=qn+r$，那么 $0\leqslant r<n$.

如果 $r=0$，停止计算，最大公因子是 n.

如果 $r=1$，停止计算，最大公因子是 1，即 m 与 n 互素.

如果 r 大于 1，进行下一步：

第二步：

分别用 n 和 r 代替第一步中的 m 和 n，重复上一步.

现在我们来分析这个优美的算法. 首先，这个算法在有限步之后一定会停止. 这是因为 $m>n>r>\cdots$；第二，我们一定能得到解. 因为 $r=m-qn$，m 和 n 的最大公因子也是 n 和 r 的最大公因子. 所以每一步两个数的最大公因子就是 m 和 n 的最大公因子；第三，也是最重要的，这个算法是高效的. 我们仔细地估计一下需要重复的步数 t. 每一步都有一个余数 $r=r_1, r_2, \cdots, r_t$：$(m, n) \to (n, r_1) \to \cdots \to (r_{t-1}, r_t)$. 注意到 $r_{t-1} \leqslant r_{t-2}/2 \leqslant \cdots \leqslant m/2^t$，因此 $t+1 \leqslant \log_2 m$，所以至多 $\log_2 m-1$ 步以后，我们就成功地得到了答案. 因为每步只做一次除法，m 和 n 的最大公因子在大约 $\log_2 m$ 步除法之后一定会得到.

给定一个关于所有正整数 N 的算法，如果存在一个固定的正整数 c，问题的答案能在大约 $(\log_2 N)^c$ 步加减乘除之后一定得到，我们就说这个算法是高效的.

计算复杂性考虑的问题和平时的数学问题有点不同. 计算复杂性的问题是一类问题，所以有些参数. 比如在希尔伯特第十个问题里，不变量的个数可以任意大，任何项的系数也可以是任何整数. 而数学问题，像费马大定理，我们只关心一个或一些特殊的方程. 计算复杂性是想知道当参数趋于无穷时，我们的算法多有效.

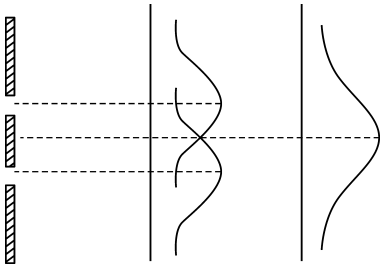
回到素因子分解，最直接的算法就是用 2，3，…，$N-1$ 去除 N，就可以找到 N 的所有素因子. 但这个算法用到大约 N 次除法，所以没有效率. 现在最好的算法大约需要 $10^{\sqrt[3]{N}}$ 多次计算，还不是高效的. 量子计算机怎么做到的呢？

3.2　奇妙的量子世界

量子力学和相对论是现代物理的两大支柱. 量子力学主要描述微观世界，所以当我们试图理解量子力学的现象时很多时候就变得不可思议. 量子力学最为奇妙的是线性叠加原理（superposition），测不准原理和纠缠（entanglement）. 线性叠加原理是最根本的. 测不准原理保护线性叠加原理，所以像它的保镖，而纠缠像线性叠加原理的影子. 下面我们通过电子的双狭缝（double－slit）实验看看线性叠加原理.

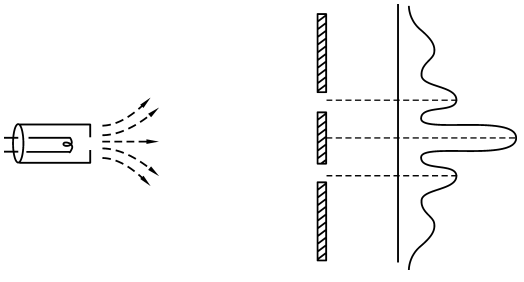
在大家的日常生活中，用到很多电器. 这些电器工作原理大多和电子有关. 电子恐怕是大家最为熟悉的基本粒子. 电子在 1897 年由英国物理学家汤姆森（J. J. Thomson）发现，从而推翻了原子不可再分. 因为电子是个基本粒子，我们把它想像成一个无限小的点，运动起来像台球一样. 然而双狭缝实验证明，这个模型很不完备：电子有时像粒子，有时又像水波，可以越过障碍产生干涉. 电子的双狭缝干涉实验在 2002 年被物理世界网站评为有史以来最漂亮的物理实验. 连伽里略开创近代实验科学方法的比萨斜塔实验也只能排在第二位.

想像有一支电子枪，向一个屏幕一个一个发射电子. 屏幕上有两个狭缝. 在屏幕的后面有个电子感应屏. 当电子穿过狭缝，到达感应屏时，感应屏会记下电子到达的位置，并发出响声. 响声的高低和电子的电荷成正比. 而且每次发射电子，都是在已经听到前一个电子已经到达之后. 如果电子是像个小台球，那么电子就应该都落在狭缝附近. 如果只开一个狭缝，电子到达感应屏的分布是中间图的两个分布. 这和电子是粒子相符合：大多数电子落在狭缝后面. 如果没有干涉，两个狭缝都开时，电子的分布应该是最右边的图.



（单狭缝）

然而看到的却是下面的分布：



（干涉分布）

这个分布和光的干涉实验是一模一样的. 大多数电子落在两个狭缝中间墙的后面. 难道电子到达感应屏时变成波了吗? 实验证明并非如此. 电子到达感应屏时总是落在一个点上, 而且响声都是一样大. 所以电子是做为一个整粒子到达感应屏的. 对这个实验的许许多多的解释最终都没站住脚. 最为合理的解释来自量子力学.

量子力学的解释是基于线性叠加原理. 电子可以从狭缝 1 穿过到达感应屏, 也可以从狭缝 2 穿过到达感应屏. 但电子的实际运动即非单从狭缝 1 过, 也非单从狭缝 2 过, 而是这两种可能的线性叠加. 假设我们把电子从狭缝 1 过叫做状态 $|1\rangle$, 而把电子从狭缝 2 过叫做状态 $|2\rangle$, 那么每个电子的状态就被由 $\alpha|1\rangle+\beta|2\rangle$ 来描述, 这里 α 和 β 是两个不同时为 0 的复数. $\alpha|1\rangle+\beta|2\rangle$ 叫做状态 $|1\rangle$ 和状态 $|2\rangle$ 的线性叠加. 描述状态 $|1\rangle$ 和 $|2\rangle$ 是波函数. 它们绝对值的平方给出上面的单狭缝的分布.

如果在狭缝 1 或狭缝 2 的地方放上一个仪器来测量电子是否从这个狭缝穿过, 干涉就被破坏, 而出现上面的单狭缝粒子分布. 也就是说测量破坏了叠加.

把叠加原理用到微观世界之外产生很多不可思议的现象, 是非常有争议的. 比如著名薛定谔猫状态: 猫的生与死的叠加. 但在微观世界里, 无数的实验证明了线性叠加原理的正确性.

3.3 肖尔算法

肖尔是怎样用量子力学的原理高效地分解素因子呢? 我们先在量子世界里做一个在经典世界里不可能的简单事情. 假如我们想在四样东西里找一样我们知道的东西. 在经典世界里, 如果没有任何别的信息, 要保证每次去找总能 100% 成功, 这样得看三样东西才行. 在量子世界里, 我们可以一次找到.

首先我们可以准备四样东西的线性叠加 $|1\rangle+|2\rangle+|3\rangle+|4\rangle$. 虽然我们不知道要找的东西是哪个, 但如果我们见到它, 我们是认识的. 用量子世界的语言, 如果我们要找的东西是第 a 个, $a=1,2,3,4$, 那么一个叫 O_a 的变换可以作用到状态 $|1\rangle+|2\rangle+|3\rangle+|4\rangle$ 上; O_a 作用在状态 $|1\rangle+|2\rangle+|3\rangle+|4\rangle$ 上, 就会在 $|a\rangle$ 前面加一个负号. 比如 $O_1(|1\rangle+|2\rangle+|3\rangle+|4\rangle)=-|1\rangle+|2\rangle+|3\rangle+|4\rangle$. 在量子世界里, 看一次就是用一次 O_a.

从量子世界的状态 $|\psi\rangle$ 到我们经典世界的状态, 我们需要测量在量子态 $|\psi\rangle$ 时的某个物理量. 量子力学是这样描述测量的: 每一个可测的物理量 M, 像能量, 位置, 都有一组完备的状态 $|e_i\rangle$. $|e_i\rangle$ 完备的意思是每一个状态 $|\psi\rangle$ 都可以写成 $|e_i\rangle$ 的线性叠加, 即 $|\psi\rangle=\sum_i \alpha_i|e_i\rangle$, 而且 $\sum_i |\alpha_i|^2=1$. 测量之后, 我们并不知道从 $|\psi\rangle$ 会到那个态, 但一定是 $|e_i\rangle$ 里面的一个, 而它发生的概率是在 $|\psi\rangle$ 展开里, 它前面那个系数 α_i 绝对值的平方, 即 $|\alpha_i|^2$. 因为需要测量, 量子算法都是概率算法.

现在我们可以一次找到我们想找的东西. 找一个完备状态是 $\{-|1\rangle+|2\rangle+|3\rangle+|4\rangle, |1\rangle-|2\rangle+|3\rangle+|4\rangle, |1\rangle+|2\rangle-|3\rangle+|4\rangle, |1\rangle+|2\rangle+|3\rangle-|4\rangle\}$ 的可测物理量 M. 先把四样东西放在线性叠加态里 $|1\rangle+|2\rangle+|3\rangle+|4\rangle$; 然后看一次 $|1\rangle+|2\rangle+|3\rangle+|4\rangle$, 即用 O_a 作用在 $|1\rangle+|2\rangle+|3\rangle+|4\rangle$ 上; 看完后, 东西的状态是 $O_a(|1\rangle+|2\rangle+|3\rangle+|4\rangle)$. 随后我们测量 M, 因为 $O_a(|1\rangle+|2\rangle+|3\rangle+|4\rangle)$ 就是 $\{-|1\rangle+|2\rangle+|3\rangle+|4\rangle, |1\rangle-|2\rangle+|3\rangle+|4\rangle, |1\rangle+|2\rangle-|3\rangle+|4\rangle, |1\rangle+|2\rangle+|3\rangle-|4\rangle\}$ 中的一个, $O_a(|1\rangle+|2\rangle+|3\rangle+|4\rangle)$ 写成它们线性叠加时, 三个系数是 0, 一个系数为 1. 所以测量时看到它的概率是 100%, 而我们只用了一次 O_a.

肖尔算法非常复杂, 我们只简单讲一下它的步骤. 假设 N 是个正整数, 我们想知道 N 的所有素因子. 首先我们用已知的高效经典算法判定 N 是否是个素数的幂次. 如果是, 停. 如果不是, 随便找一个与 N 互素但不太大的正整数 x. 因为判定 N 与 x 是否互素的欧几里德算法是高效的, x 是很容易找的. 然后找一个正整数 a 使得 $x^a=1 \bmod N$. 现在没有高效的经典算法找到这样的 a, 但肖尔找到了一个量子算法, 可以找到这样的 a. 如果有了这样的 a 而且又是偶数, 那么 $(x^{\frac{a}{2}}+1)(x^{\frac{a}{2}}-1)=0 \bmod N$. 如果 a 是奇数, 再找一个 x 重新来过. 所以 $(x^{\frac{a}{2}}+1)$ 或 $(x^{\frac{a}{2}}-1)$ 和 N 就有公因子. 用欧几里德算法找到它们的最大公

因子. 如果是 1，再找一个 x 重新来过. 如果大于 1，就找到了 N 的一个因子. 可以证明这样高效地找到 N 的所有素因子的概率可以任意接近 100%. 肖尔算法有时会失败，但我们不需要知道每一个秘密.

量子计算机不但可以高效地作素因子分解，更重要的应用在于模拟量子系统. 通过模拟，我们可以更深刻了解量子世界. 这样会给材料学、化学从而医学带来革命性的进步. 量子计算机这么有用，为什么我们到现在还没有呢？量子计算机的建造非常困难，因为线性叠加很脆弱. 对量子系统的任何操作都可能引起相退干 (decoherence).

4　拓扑量子计算

科学家最近想用一种奇异准粒子 (quasi-particle)——非交换任意子来建造拓扑量子计算机. 在拓扑量子计算中，任意子世界线形成的辫子就是计算过程. 我们还不知道是否存在非交换任意子，但如果存在，这样的量子计算机会非常稳定，那么量子计算的时代就会早日到来.

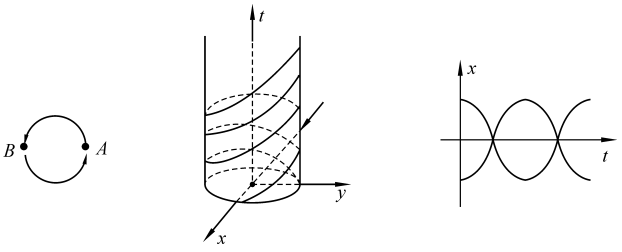
4.1　基本粒子和准粒子

在阿尔卑斯山脉以北法国和瑞士交界的地方，一百多米的地下埋着一个直径四米左右，周长二十七公里的大型强子对撞机 (LHC). 经过十几年的建造，上百亿美元的成本，一百多个国家上万名科学家的努力，大型强子对撞机终于开始运行. 两束质子流被加快到接近于光速的速度进行了对撞(光速约每秒三十万公里，质子的最高速度最终将会达到每秒仅低于光速约几分米.)如果粒子标准模型的预言准确，大型强子对撞机一切运转正常，在不久的将来，每过几个小时，一个希格斯玻色子 (Higgs boson) 会产生. 这种被称作上帝粒子 (God particle) 的发现，将为粒子标准模型划上完美的句号，也是还原论 (reduction) 的辉煌胜利.

希格斯玻色子是一种预言的基本粒子. 什么是基本粒子？即使希格斯玻色子被发现，这个问题的探索也不会终止. 我们把基本粒子看做是没有内部结构，不能再分的物理状态. 而所有别的状态都是由它们构成的. 基本粒子是真空的一种激发态. 什么是真空？什么是激发态 (excitation)？真空是我们想像的一种什么都没有的特殊物理系统. 物理系统的最低能量态叫基态. 不是基态的叫激发态. 激发态中最低的不可再分的态叫元激发态 (elementary excitation). 基本粒子是真空的元激发态. 然而，在真空中，并非什么都不发生. 和任何物理系统一样，真空也有量子涨落. 演生 (emergence) 论者认为真空并没有天生的特权. 很多别的物理系统也非常特殊，所以这些物理系统的元激发态同样有权利被叫做粒子. 为了和基本粒子区别，我们称它们为准粒子. 随着物理的发展，基本粒子和准粒子的区别也就越来越模糊. 所以演生论者认为准粒子和基本粒子同样重要，而且可能它们原理是一样的. 从现在起，我们提到的粒子时可能是基本粒子也可能是准粒子.

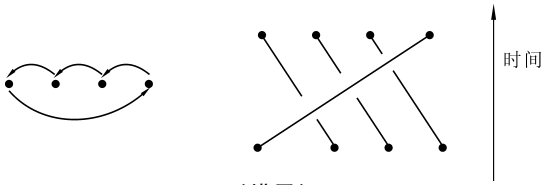
4.2　粒子的轨迹

考察平面上的两个粒子 A 和 B. 假设 A 和 B 都在实轴上，坐标分别为(1,0)和(−1,0)，并在单位圆上以单位弧速度逆时针方向转动. 经过时间 t 以后，A 和 B 的位置分别是：A：$(\cos 2\pi t, \sin 2\pi t)$，$B$：$(-\cos 2\pi t, -\sin 2\pi t)$. 粒子在时空的轨迹叫粒子的世界线 (worldline). 下面中间的图就是 A 和 B 的世界线 .最右边的是世界线在 (t,x)平面的投影.



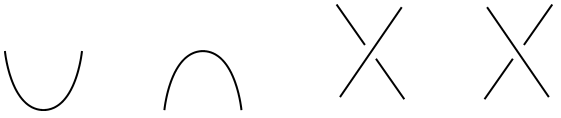
(世界线)

更一般考虑平面上的多个粒子. 为了方便，假设它们全在实轴上. 随着时间的流逝，这几个粒子在平面上运动，但互相不能碰撞. 经过一段时间后做为一个集合它们回到了原先的位置上去. 那么它们的世界线就形成了一个辫子. 当 1，2，3，4 按下面的左图的运动时，它们世界线形成右图的辫子.



(辫子)

根据量子场论的观点，足够的能量可以产生粒子—反粒子对，而粒子的逆时间运动等价于反粒子的运动，那么粒子—反粒子对的产生和泯灭的世界线就是下面左边的两个图. 所以当一个粒子在运动中有粒子—反粒子对的产生和泯灭，他们的世界线就是一个纽结. 而多个粒子的世界线就是一个链环. 每一个链环都有以下这些基本的图形成，对应于物理的基本过程：



（世界线分解）

4.3 非交换任意子

假设有 N 个等同粒子，它们的状态是波函数$|1,2,\cdots,N\rangle$. 如果对换第一和第二个粒子，新的波函数$|2,1,\cdots,N\rangle$和 波函数$|1,2,\cdots,N\rangle$有什么关系呢？因为第一和第二两个粒子是一样的，所以两个波函数在描述同一个态. 那么它们之间只能差个复数 $e^{i\theta}$. 如果再把第一和二个粒子对换，那么就完全回到了以前. 所以 $e^{i\theta}\cdot e^{i\theta}=e^{2i\theta}=1$. 这样 $\theta=0$ 或 π . $\theta=0$ 的粒子叫玻色子，像光子；而 $\theta=\pi$ 的粒子叫费米子，像电子. 以前我们认为所有的粒子或是玻色子或是费米子. 然而现在科学家意识到，如果存在仅仅生活在平面上的准粒子，那么 θ 就不必总是 0 或 π. 平面上 θ 不是 0 或 π 的准粒子叫任意子，因为 θ 几乎可以是任意的. 我们有很多证据 $\theta=\frac{\pi}{3}$ 的粒子存在于平面上的电子系统中.

建造拓扑量子计算机，仅仅有任意子是不够的. 我们需要更奇特的非交换任意子. 理论上知道最多一种非交换任意子可能存在于 5/2 分数量子霍尔效应的平面电子系统中. 在这种系统中，有一种叫 σ 的准粒子. 我们已经知道它的电荷是电子的 1/4. 把球面看成是平面加上无穷远，假设在球面上有四个 σ 准粒子. 即使把这四个 σ 准粒子固定在一定的地方，理论预言这四个 σ 准粒子有两个不同的基态，记为$|1,2,3,4\rangle_1$，$|1,2,3,4\rangle_2$. 假设开始时这四个 σ 准粒子的状态是$|1,2,3,4\rangle_1$，那么我们把 2 和 3 交换后，它们是哪个态呢？理论表明即不是$|1,2,3,4\rangle_1$ 也不是$|1,2,3,4\rangle_2$，而是它们的线性叠加. 这样的线性叠加可以用一个矩阵来表达. 平面上粒子交换的世界线是辫子. 把第 i 个粒子和第 $i+1$ 个粒子对换的辫子记作 σ_i. 这个辫子给我们以下的矩阵：

$$\sigma_1\to e^{-\pi i/8}\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$$

$$\sigma_2\to e^{-\pi i/8}\begin{pmatrix}\frac{1-i}{2} & \frac{1+i}{2}\\ \frac{1+i}{2} & \frac{1-i}{2}\end{pmatrix}$$

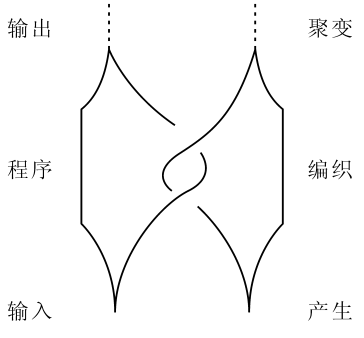
（矩阵）

所以每一个辫子就给出一个矩阵. 矩阵的第 i 行告诉我们从第 i 个态开始，这些粒子按这个辫子运动后，第 i 个态变到的线性叠加. 我们知道矩阵的乘法是非交换的，所以这样的任意子叫非交换任意子.

4.4 任意子量子计算机

本节里提到的任意子都指非交换任意子.

任何计算都有三步：输入，处理，和输出. 任意子量子计算机是这样计算的：



（任意子量子计算机）

在任意子量子计算模型中，输入等价于从“真空“产生一组任意子. 为了方便，我们假设它们全部在实轴上. 任意子只能成对产生，所以是偶数个. 随着任意子个数的增加，任意子的基态个数成指数增长. 如果我们要做 N 的素因子分解，取大约 $\log N$ 多的非交换任意子使它们基态的个数大于 N. 我们的计算就从第 N 个基态开始. 计算的过程就是任意子编制辫子的过程. 随着任意子的运动，任意子的状态也起着变化. 回到素因子分解，肖尔算法告诉我们怎样编织这些任意子. 当编织结束后，我们把任意子一对一对放到一起进行聚变(fusion)，观测什么样的新粒子出

现. 我们重复很多次，就可以知道不出现任何粒子的概率，即每一对都回到真空的概率. 聚变的结果就是任意子量子计算机的输出. 如果我们作 N 的素因子分解，那么通过这个概率，就可以找到 N 的所有素因子.

素因子分解不是任意子量子计算机解决的最自然的问题. 最自然的是琼斯多项式的在 $t=e^{2\pi i/r}$，$r=3,4,5,\cdots$ 值的高效逼近，因为聚变的结果的概率是由琼斯多项式的在 $t=e^{2\pi i/r}$，$r=3,4,5,\cdots$ 值决定的. 我和朋友证明拓扑量子计算机和别的量子计算模型是高效等价的，而且琼斯多项式在 $t=e^{2\pi i/r}$，$r=3,4,5,\cdots$ 值的高效逼近是一个量子计算模型的完备问题. 也就是说量子计算机能高效解决的任何问题都可以化成是琼斯多项式值的逼近.

微软研究院的 Q 部（Microsoft Station Q）主要研究拓扑量子计算. 我们和世界许多大学和公司的实验室合作，正在寻找非交换任意子. 在这些实验室里，分数量子霍尔效应电子系统正在接近绝对零度的超低温下和超强磁场里. 或许非交换任意子正在编织着我们所期望的纽结. 如果成为现实，这一切将给人类带来科技的革命. 一个丰富多彩，远比经典世界奇妙的的量子世界正等待着新一代去窥探她的奥妙！想更多了解拓扑量子计算，我们推荐“环球科学“2006 年 5 月号的文章：量子计算新突破.

后记

本文基于作者 2007 年夏天在扬州数学之星夏令营上的报告. 感谢田刚教授的邀请和苏维宜教授的盛情款待. 由中国天元基金支持的数学之星夏令营旨在提高高中学生对数学的兴趣和全面认识. 林晓松教授生前积极参与了夏令营的组建和活动，对她倾注了很多心血. 数学不但是一门学问，更是一种文化. 希望年轻一代数学家不但有解决难题的才华，更有发现新问题，发展新分支和新思想的能力. 重视和推动数学在各学科中的应用，为人类造福，让数学之树常青.