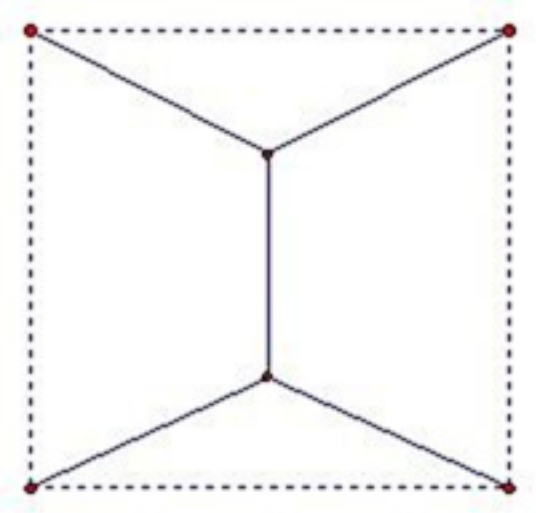
IBM七月份的Ponder this

©Zhang-Zi, July 12, 2007 @ 3:39 pm

今年IBM七月份的Ponder This问题（原题在这里，英文）：

> 一个单位正方形的土地，其内（包括边界）建一些篱笆，使得任何与正方形相交的线段都被篱笆阻断（即与篱笆相交），问所建篱笆的总长度最少要多长？

有趣的是提出问题者自己虽然有一个构建方法，但还不知道怎么证明为什么是最短的。他的方法十有八九就是下面（实线部分）：



当然我现在也还不会证明。

PS：不知道Ponder This的官方译文是啥？

本文还有**19**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/622.html#comments**

策略游戏：医生和病人（I）

©Zhang-Zi, July 10, 2007 @ 3:56 pm

我很早之前就想过这个问题，但一直只知道一个trivial的答案。前两天无意中发现网上已经有高手给出了更好的方案，故记录在此。有兴趣的可以自己想一想。

岛国上流行一种极易接触传染的病
一旦染上该病1月后病发身亡
但该病可通外科手术治愈

岛上每个人都有已被传染的可能
国王怀疑自己得了该病
在该岛上找到了医术最高名的3个医生
并要求这3个医生在当天轮流给自己动手术
然而已消毒过的手术手套只有2双
怎样最安全

现在把问题一般化，假设岛上有n个医生，还有m个（非医生）居民。现在岛上流行一种极易接触传染的病。每个居民要想治愈传染病，必须得到这n个医生的治疗，治疗的顺序无所谓（先别管这种假设的由来）。怎么安排它们手术的次序和带手套的方案，使得所用的手术手套最少。

注一：医生也有可能已被传染，故他们之间也要防止相互感染。
注二：手套可以套着用...还可以反着用...

下面的解答作者是JtR，来自水母IQDoor版。

用{m/2}+{n/2}+{n/4}(m<=n)双手套即可。{}表示向上取整。

为了叙述方便，假设m是2的倍数，n是4的倍数，不是4的倍数时类似，只是手套的“ 利用

率”没有那么高。可能可以通过优化减少一副到两副。

1.将医生平均分为两组，分别为A，B。各m/2人；
将病人分为三组，人数分别为a＝n/2，b=n/4，c=n/4

2.将m/2副手套分配给A，n/2副手套分配给a，A中的每一个医生检查a中的每一个病人；
检查前均在自己的手套外套上指定给该病人的手套；
注意所有的手套均只有一面污染。（假设医生之间也要防止相互感染）

3.将分配给a的n/2副手套中的一半翻转，两两一组套在一起，污染面互相接触，此时每一组手套内外均无污染；将这n/4组手套分配给b(n/4人）；
将剩下的未使用过的n/4只手套分配给c(n/4人）；

4.A中的每一位医生分别检查b，c中的病人，检查前均在自己的手套外套上指定给该病人的手套（或两只套在一起的手套）；
这样A中的医生完成对所有病人的检查，而且医生的手套外侧和指定给病人的手套内侧(注意有n/4是翻转过的)均无污染。

5.A中所有的医生将各自的手套翻转后给B中的医生戴上；
b中的病人把套在一起的手套里面的那只抽出来翻转后套入c组病人的手套中。此时c组的手套每一组相互接触的面都是干净的；

6.B中所有的医生按前述方法给b，c两组病人检查；

7.将c组的手套两两分开，把套在外面的手套翻转，这样得到n/2只外侧干净的手套重新分配给a组的病人。

8.B中的所有医生检查a组的病人。

这样就完成了所有医生对病人的检查。

如果医生的数量比病人多只要把医生和病人交换即可。在该问题中二者是对称的。

本文还有1条留言，察看留言和讨论请到http://zhiqiang.org/blog/617.html#comments

帽子游戏二

©Zhang-Zi, June 25, 2007 @ 3:52 pm

这个题目听说是MSRA的面试题。

在这个游戏的开头，我们设想自己要参加一个电视游戏大奖赛。规则呢，是这样。我们有 n 个人，作为一个小组来参加游戏。游戏中，主持人会给我们每人头上戴一顶帽子。帽子有黑白两种颜色，可以认为它们在我们各自头上的分布是临时随机决定的。小组中的每一个人，可以看到其他人的帽子颜色，但不知道自己的帽子颜色。每个游戏成员都被要求回答自己帽子的颜色（且必须回答，而且是独立回答的）。只有当所有人都回答正确（注意这里与帽子游戏一的区别），他们才能获胜，一起获得最后的大奖。

这个游戏还有最关键的一点：在游戏开始前(帽子戴上之前)，有一个“协商时间”，小组成员可以聚在一起，讨论决定小组应采取什么样的策略。但这个交流过程在游戏开始时自然终止。

现在的问题是：小组选择什么样的策略，才有最大的机会获胜呢？

因为任何一个人没有关于自己的帽子的任何信息，所以正确率不可能超过1/2。关键是怎么让所有人要么同时正确，以达到这个1/2的正确率。

所以，正确的策略应该是每个观众回答其余所有观众的帽子的异或（0表示白帽子，1表示黑帽子，则第i个人回答$\oplus_{j\neq i}^{n} x_j$。

OK，现在这个问题到这里已经完整了。但令人惊奇的是，在两个星期前，来自伦敦大学的Taoyang Wu给了一个非常有趣的讲座，上面这个游戏恰是这个讲座的一个特例。

上面的问题其实是说有一个完全的有向图，每个顶点上有一个随机的变量。每一个点都知道它的邻居（连向它的点）的变量，需要猜测自己的信息。问以怎么样的策略能够使得所

有点同时正确的概率最大？

显然，这个概率（记作$p(G)$）与这个图G的结构密切相关，这样，$p(G)$某种意义上是这个图的结构的一个度量，称为Guessing Number，等于$g(G)=n+\log p(G)$。根据前面所说，完全图的Guessing Number为n-1。另易知一个单环的Guessing Number等于1。而对一般图Guessing Number问题，无论是从直接求解（猜测是NP-hard），还是其性质分析，都还留下很多未解决的问题。

本文还有**2**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/608.html#comments**

帽子游戏一

©Zhang-Zi, June 19, 2007 @ 11:01 pm

在这个游戏的开头，我们设想自己要参加一个电视游戏大奖赛。规则呢，是这样。我们有 n 个人，作为一个小组来参加游戏。游戏中，主持人会给我们每人头上戴一顶帽子。帽子有黑白两种颜色，可以认为它们在我们各自头上的分布是临时随机决定的。小组中的每一个人，可以看到其他人的帽子颜色，但不知道自己的帽子颜色。每个游戏成员都被要求回答自己帽子的颜色。我们各人面前有三个按钮，可以选择“黑色”“白色”或“弃权”(也就是 pass，不作猜测的意思)。小组成员彼此之间没有任何信息交流，他们必须各自独立地作出自己的选择，并且谁也不知道其他人的选择。如果小组成员全部选择了pass，也就是每个人都弃权，则他们输了；如果有小组成员作出了明确的猜测，但某个人猜错了，则结果也是输。只有当小组中有人做出猜测，并且每个做出猜测的人都猜对了，他们才能获胜，一起获得最后的大奖。

这个游戏还有最关键的一点：在游戏开始前(帽子戴上之前)，有一个“协商时间”，小组成员可以聚在一起，讨论决定小组应采取什么样的策略。但这个交流过程在游戏开始时自然终止。

现在的问题是：小组选择什么样的策略，才有最大的机会获胜呢？

在这里用Hamming码给出了问题在$n=2^k-1$时候的一种解释和策略，成功概率为$1-1/2^k$。但这个问题为什么最后归结于Hamming码，这种方法为什么是最优的呢？这里再讨论一下。

模型：帽子的黑白状态为一个n长的串，可以用一个n维的超立方体G的顶点坐标$(x_1, x_2, \cdots, x_n)$来表示，坐标为0表示白帽子，1表示黑帽子。G上两顶点相邻当且仅当它们之间仅相差一位，这样每个顶点恰与n个点相邻。

目标：主持人在G上随机选取一个顶点P，第i个观众知道这个顶点除第i个之外的n-1个坐标值，给出一种回答策略，使得所有问答的观众都答对了正确的P。

这个问题的关键是怎么把“策略”模型化。

注意到在游戏中，每个人他能观测n-1个坐标值，也就是他能够确定P为G上某条边(u,v)的两个顶点之一。他在游戏中的策略具体表现为，当他观测到这条边时，他选择这条边的哪个顶点，或者不做选择。

如果观测到(u,v)，策略选择了u，则在G上连一条有向边$u \to v$。

策略：一个策略C可以表示为G的某些边的有向化。

引理：如果P点处出度（即P连出的边数）等于0——没有人回答错误，且入度（连向P的边数）大于0——至少有一人回答，则当主持人选择P点，观众获胜。否则观众失败。

在策略C下，错误点构成的集合记作R_C。此时，观众成功的概率为$1-|R_C|/2^n$.

定义：图G(V,E)上，V的子集D称为G的Dominating Set当且仅当G的任何顶点要么在D中，要么与D的某个顶点相邻。

定理：G的顶点集R为某个策略C的错误点集R_C当且仅当R为G（无向图下）的Dominating Set。其中$C=\{u \to v: u \in R, (u,v) \in E(G)\}$。

对于一般图，求Dominating Set是NP完全问题。对于这个超立方体而言，一方面有下界：

定理：$R_C \geq 2^n/(n+1)$. 相应的，观众成功的概率不可能大于 $n/(n+1)$.

而在$n=2^k-1$时，上面的等号可以取到，构造2^{2^k-k-1}个2^k-1长度的01串，任何两个之间的距离大于2（即为纠错度为1的纠错码）。

讨论：如果帽子颜色有三种，又该如何？

本文还有3条留言，察看留言和讨论请到http://zhiqiang.org/blog/607.html#comments

概率论中几个有趣的例子

注：各大高校BBS上经常有些好文章，但BBS上洪水滔天，而且拒绝搜索引擎的抓取（通过robots.txt禁止），好些好文章就此湮没。我决定借助阅微堂这个平台，援引一些BBS上的文章，原则是：作者原创，内容有价值，未在其它地方转载过，主题与Science相关。所有转载都是经过作者授权，会标明作者，发信站和版面，以后不再说明。

作者：ni1985（妮子||从东方席地卷来一团野火），原发新水木Mathematics

已经酝酿很长时间的本文终于出场了。

写本文的主要目的：1 很多人看了我前面大量的历史日志后，对我的数学水平产生了怀疑；2 有高中的校友师妹咨询关于大学数学学习的问题；3 概率论是数学中一个重要而美的分支，可惜多数同学尚没有机会看到其冰山一角。

本文的读者适用范围：最低标准是学过工科专业的高等数学和概率论，最高标准不清楚（也许水平比我高的人就不屑于读了）

当我跟皇上提到要写这篇文章的想法时，我提到：试图用比较短的篇幅让只要有初等概率论基础的人，也能看懂，从而对较深的概率论的研究对象和有趣的结论有一个初步的了解，激发其进一步深入学习概率论的兴趣。皇上说：那可不容易，相当于一个毕业设计了。我觉得，确实如此，本文是基本失败还是基本成功，还要看读者的评价。

要想引入本文的内容，首先从数学美的定义说起。关于数学美，我比较欣赏的有两种观点，一是Birkhoff的观点，数学美=逻辑的复杂程度/表述的复杂程度；二是Von Neumann的观点，数学的活力依赖于与它有联系的科学分支的多寡与分支的活力。也许做应用的人更喜欢后者，但我是比较喜欢前者的。因此，我下面的主要内容就是介绍一些概率论中的基本例子，这些例子的表述是相当简单的，但得到这些例子的手段却比较复杂。我将试图把每个例子表述清楚，让只要有初等概率论基础的读者就知道在说什么，但对得到这些结

果的证明过程则一律省略，只简要提出涉及的基本工具，但其中有些比较简单的细节会给大家留为习题。这些例子一律来自伟大的Durrett的著作：Probability theory and examples——我认为最优秀的概率论教材。

例1. Coupon collector问题：X1,X2,…是独立同分布，均匀的取自集合{1, …, n}的随机变量序列。大家把集合{1, …, n}想象为若干张扑克牌，每次我们等概率的取一张扑克牌，取完放回。$t(n,k)=\inf_m\{m:|\{X_1,\cdots,X_m\}|=k\}$，意思就是手中取过k种不同的扑克牌所需的次数。T(n)=t(n,n)表示取过所有扑克牌所需的次数。X(n,k)=t(n,k)-t(n,k-1)，则X(n,k)服从参数是1-(k-1)/n的几何分布（思考题！），它的期望和方差可求，且容易发现X(n,1),…,X(n,n)相互独立，从而可以求出ET(n),Var T(n)（习题！）。且去证明$(T(n)-ET(n))/n\log n$ 依概率趋近于0.（数学基础稍微深一些的同学都知道，L2收敛蕴含依概率收敛）最终得到一个漂亮的结论：

$T(n)/n\log n$ 依概率收敛于1.

数学基础比较少的同学可以直接看这一行，我把这一行的实际意义说清楚：就是假设我们要收集的邮票有n张，而每次别人给我们提供的邮票恰恰是等概率的，那么要想把n张收集全，需要的时间依概率趋近于 nlogn。 所以大家就可以发现，为什么我们想集齐比较少的邮票要比集齐多的邮票容易的多。

作为更为深层次的读者，我要说的是，在随机变量收敛性问题的研究中，独立性和矩总是常见的关注对象。为什么我们非常喜欢方差这个概念呢？我想一个重要的性质就是：对于独立的随机变量，方差对和有分配律。于是二阶中心矩才会成为最重要的矩。通过对矩的估计把随机变量的收敛性问题，转化为实数序列的收敛性问题，最后完全是数学分析的东西，这种手段是屡屡使用的。

例2 非对称的简单随机游动问题：$X_1,X_2,\cdots$独立同分布，$P(X_i=1)=p$，$P(X_i=-1)=1-p=q$，$S_n=X_1+\cdots+X_n$.

对于数学基础不太好的同学，我简单介绍一下这个问题的背景，其实很好理解。设有一个点在0时刻位于实轴的原点0处，它在每个时刻以概率p向右跳跃一个单位长度，以概率q向

左跳跃一个单位长度，且跳跃的方向与以前每次跳跃的情况是独立的。S_n表示的是：n时刻这个点所在的位置。

我们有如下非常精彩的结论：

1 $T_x=\inf\{n:S_n=x\}$，T_x的直观意思就是，这个点首次跳到x的位置的时刻。那么对于任意的$a<0<b$，$P(T_a<T_b)=\frac{f(b)-f(0)}{f(b)-f(a)}$这里函数$f(x)=(\frac{1-p}{p})^x$。

上面的这个等式的直观意义：a是负半轴上一点，b是正半轴上一点，点没到b之前先到a的概率被计算了出来。

得到这个结论最快的方法就是用鞅论。鞅实在是一个漂亮的东西，而它的漂亮之处就在于它与停时结合在一起后的巨大威力。用N表示T_a和T_b中的较小值，则N是停时。首先要说明的是N小于无穷大。要得到这个结论，我掌握的有三种方法：

（1）通过EN小于无穷大，得到这个结论，这事实上是通过一个强的多的结论说明的，具体见Durrett书181页。

（2）通过鞅收敛定理，见Durrett书275页。其中用了一个重要结论：一致有界的鞅序列必然一致可积（应该是很显然的吧，呵呵）。

（3）通过马氏链的性质：对于一个有可列状态，不可约的马氏链，用F表示状态空间的一个有限子集，设初始状态属于F,用T表示链首次离开F的时间，则一定有T小于无穷大。（可以作为本科生三年级应用随机过程的习题，证之！）

2 $ET_b=b/(2p-1)$ 即首次到达b点的平均时间是$b/(2p-1)$。

处理方法还是用鞅论，这里不再多说。

关于用鞅论解决马氏链问题的例子，我还推荐数学基础比较高的同学阅读Durrett书上的

（1）M/G/1排队（282页，298页，309页）　（2）生灭过程（295页，301页）

本来我认为这两个例子是更加漂亮的，但考虑到数学基础一般的同学的阅读水平，就不写了。

例3 遍历定理的一个应用（Benford定律）

首先提一个问题：随机选取一个正整数，它的第一位数字是1 的概率是多少？

很多同学会武断的回答：1/9.

可是你忘记了问我一个问题：你是如何随机选取的？

也许你会说：这还用问？就是等概率的选取呗。

可是不要忘记，对于可列状态的状态空间，不存在一个概率测度，使得它在任意两个单点集上的概率相同！（思考题！）

其实一个直观的想法是：我们考虑前n个正整数中（均匀分布是可能的），首位数字是1的概率记为f(n),然后把f(n)的极限作为我上面所提问题的答案。

可是随后会不幸的发现，极限是不存在的！

于是作为习题，设前ｎ个正整数中，首位数字是１的概率记为$f_1(n)$,则$f_1(n)$的上极限是5/9,下极限是1/9，且对于任意属于区间[1/9,5/9]的实数a，都存在$f_1(n)$的子序列，它的极限就是a。类似的，记前n个正整数中，首位数字是2的概率是$f_2(n)$,其上极限是10/27,下极限是1/18.（作为数学分析的习题！）

但是，当我们转而思考这样的等比序列，1，2，4，8，16，…记这个序列的前n项中首位数字是1的概率为$f_1(n)$,则$f_1(n)$是有极限的，且极限是$\lg 2$.一般地，对于任意一个非10的整数次幂的正整数q，考虑以1为首项，以q为公比的等比数列，它的前n项中首位数

字是k的概率为$f_k(n)$,则$f_k(n)$的极限是$\lg(k+1)-\lg k$. （证明不可能在这里给出了，大家只管从结论中去欣赏概率论之美吧！）

这个结论是非常漂亮的！叙述是非常简单的，意义是非常直观的，但并不是容易猜到的，证明所需的背景——遍历定理又是极其深刻的。读来畅快淋漓！

今年春天，陈大岳教授对我说，在现代概率论的研究中，遍历定理显现的越发重要。当看到上面这个结论后，我初步认识到遍历定理内涵的深刻和丰富。

以上仅选取三个概率论的基本例子，它们的结论的直观易懂与其所需理论背景的负责程度形成了鲜明的对比，体现了概率论作为一个数学分支的美妙。管中窥豹，可见一斑，希望能以此激发大家深入学习概率论的兴趣，使不同数学基础的同学都能有所收获。

--
你的安拉管不着我.

本文还有1条留言，察看留言和讨论请到http://zhiqiang.org/blog/601.html#comments

TCS课堂笔记：数据背后的真实

©Zhang-Zi, May 12, 2007 @ 12:34 pm

假设某一天，某媒体发布一条消息，说清华大学研究生新生录取的面试过程中，每个系的女性报考者的通过率都要比男性报考者的通过率要低，然后攻击清华大学的新生录取歧视女性。你对这件事情有何看法？

魔鬼经济学中教育我们要对数据进行分析，揭露隐藏在表象世界下的真实世界。但是，对于数据的不同分析方式，会得出截然不同的结果，至少表面上看起来截然不同。

比如在上面的例子，表面上看起来女性报考者在每个系都受到了歧视，但真实情况如何呢？

为了简单起见，不妨将各系分为两大类，文科系和理工科系，

	文科	理工科	全校
男	4/10=40%	20/100=20%	24/110=22%
女	30/100=30%	1/10=10%	31/110=28%

表格里面的 a/b=c%的含义为b人报考，a人通过，通过率为c%。

这个例子便显示即使数据表明在每个系，女性通过率要低于男性，在全校范围看来，女性的通过率也可能比男性高，这样看来，歧视女性报考者的说法就无法成立了。

上面是一个例子，显示出数据必须从整体来看。下面是一个例子，单从整体来看数据也是不够的。

某气象台号称它的天气预报整体准确率高达80%。你对这个数据有何看法？

似乎80%是足够高了。但其实不然。大多数人关注的天气也就是下雨和不下雨之分。任何

一个人都能预测天气，达到90%以上的准确率，只需要总是预测不下雨即可（显然，在北京，雨天的概率要<10%）。

想想看，你是否被人用上面的两种方法忽悠过？

注：上面的例子和数据均为作者伪造，清华大学也从没有歧视女性之说，请勿用作其它论据。

本文还有**13**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/588.html#comments**

TCS课堂笔记：数据库存储问题

©Zhang-Zi, May 8, 2007 @ 6:04 pm

理论计算机(I)课上讲的一个问题，很有意思。

已经一个n，m和$\{1,2,\cdots,m\}$里n个数，设计一种保存这n个元素的表的数据结构形式，使得对$\{1,2,\cdots,m\}$中任何一个数，可以最少的查询次数（每次查询，可以选择一个位置，然后你能知道表中这个位置的数据），获知这个数是否在表中。

如果设计这个表为有序表，用二分法需要$\log n$次查询。

有序表是最优的么？

举一个例子，一个保存1，2，3里面的两个数的有序表，要想知道2是否在这个表里面，至少需要两次查询。可不可以用一种特定的数据结构，使得一次查询就能判定任何一个数是不是在数据库里面？

结论是可能的，见下图：

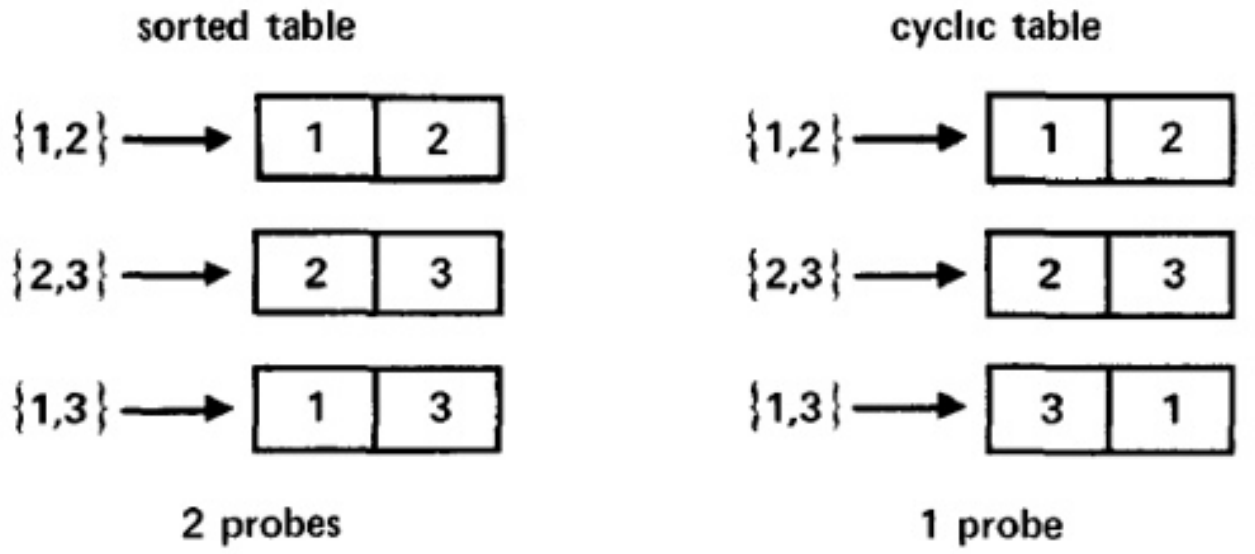


FIG 1 The sorted table is not optimal for $n = 2, m = 3$

一般的，假如表里的n个数的范围是1，2，...，2n-2，即$m = 2n-2$，可以设计一种方法，使得，对于任何一个数，只需要查询一次，便能知道这个数是否在这个表里面。

课堂上有同学当场就想出设计方法，向他致敬！

另外，利用广义的Ramsey定理，对于固定的n，能够证明当m足够大时，无论你怎么设计那个表的结构，也至少需要$\log n$的查询次数。

一个很神奇的问题。相关论文Should Table be Sorted?, 上面的图片也来自这篇文章。

本文还有**4**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/587.html#comments**

圆周率π的计算及纪录

©Zhang-Zi, May 6, 2007 @ 5:22 pm

今天gezhi上有一篇关于π的八卦文章，里面讲到了π的计算问题。但我对其中的一些数据起了疑心，并不是说数据错了，而是作者所用的数据实在是太老了。

作者提到的π的最高纪录才八百多万位，但就我以前就见过清华某FTP上，提供π的120亿位的下载，总文件大小超过5G。可惜忘了在哪个服务器上看到的了。

Google找到一个纪录，圆周率206,158,430,000位，也就是2060多亿位吧。用的是Gauss-Legendre算法(Brent-Salamin)，占用内存865G，计算时间消耗37个小时（不要以为这个时间没有多长，看看占用的内存量便知，计算在大型机或者计算集群上进行的）。

补充：计算在日本东京大学的Information Technology Center, Computer Centre Division进行的。所用机器有128个CPU，运算能力大约1万亿次浮点运算每秒。

这个纪录很难说是最新的，因为它是1999年的，有兴趣的可以去查一查最新的纪录是多少。

补充：查到一个纪录，2002年有一个12411亿位的纪录，似乎又是日本人做的。在这里有2002年之前的纪录列表。到这里，π本身的计算已经不重要了，重要的是比拼谁家的计算机NB。日本在这一方面的实力确实有目共睹。

π的计算是一个非常有趣的话题，一般来说，都是利用级数来计算的，所以，级数的收敛速度越快，计算复杂度越低，比如Gregory-Leibniz series

$$\pi = 4\left(1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots\right)$$

就是一个收敛性能非常糟糕的级数，但下面这个

$$\pi = 3\sum_{n=0}^{\infty}\frac{(2n)!}{n!^2(2n+1)16^n} = 3+\frac{1}{8}+\frac{9}{640}+\frac{15}{7168}+\cdots$$

收敛地快多了。

另外贴一个 π 的算法，我一直没看懂过，算法高手出来解释一下？

```
#include <stdio.h>
long a=10000,b,c=2800,d,e,f[2801],g;
void main(){
  for(;b-c;)f[b++] =a/5;
  for(;d=0,g=c*2;c-=14,printf("%.4d",e+d/a),e=d%a)
  for(b=c;d+=f[b]*a,f[b]=d%--g,d/=g--,--b;d*=b);
}
```

本文还有**4**条留言，察看留言和讨论请到的计算及纪录**">http://zhiqiang.org/blog/586.html#comments**

一个算法面试题 & 面试题库

©Zhang-Zi, April 27, 2007 @ 10:34 pm

一个面试题，号称是微软的

> 输入$a_1,a_2,...,a_n,b_1,b_2,...,b_n$，如何在O(n)的时间，用O(1)的空间，将这个序列顺序改为$a_1,b_1,...,a_n,b_n$。

刚一眼看上去觉得很容易，做了一回儿才发现深不可测。题目大致是要求在线性时间，常数空间实现下面的置换

> x -> 2x mod 2n+1

我做了两小时没做出来，上网一搜，最近这个题目很热，已经有人在讨论这个题目，还翻出了问题的发源地http://www.cs.uvic.ca/~jellis/perfect.html，一个完美洗牌的构造问题。此网页上一篇长达12页的论文Computing the Cycles in the Perfect Shuffle Permutation给出了完整的算法和证明。

不知道有没有人给出直接而简便的方法？

在搜索过程中发现两个很好的程序设计类面试题库（英文），共享一下，如果你想面试Microsoft，Google或者Goldman Sachs，看看这两个网站上的题目就可以了。

- techInterview Discussion
- CareerCup：网站似乎被G-F-W了，幸好RSS还能用。

本文还有**10**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/579.html#comments**

PKC'07 会议结束

©Zhang-Zi, April 19, 2007 @ 9:19 pm

The International Conference on Theory and Practice of Public-Key Cryptography

公钥密码学理论和实践会议

公钥密码是一个非常好玩的东西，记得高中时张筑生老师讲到数学的应用时，举得就是这玩意儿。

本文还有**1**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/567.html#comments**

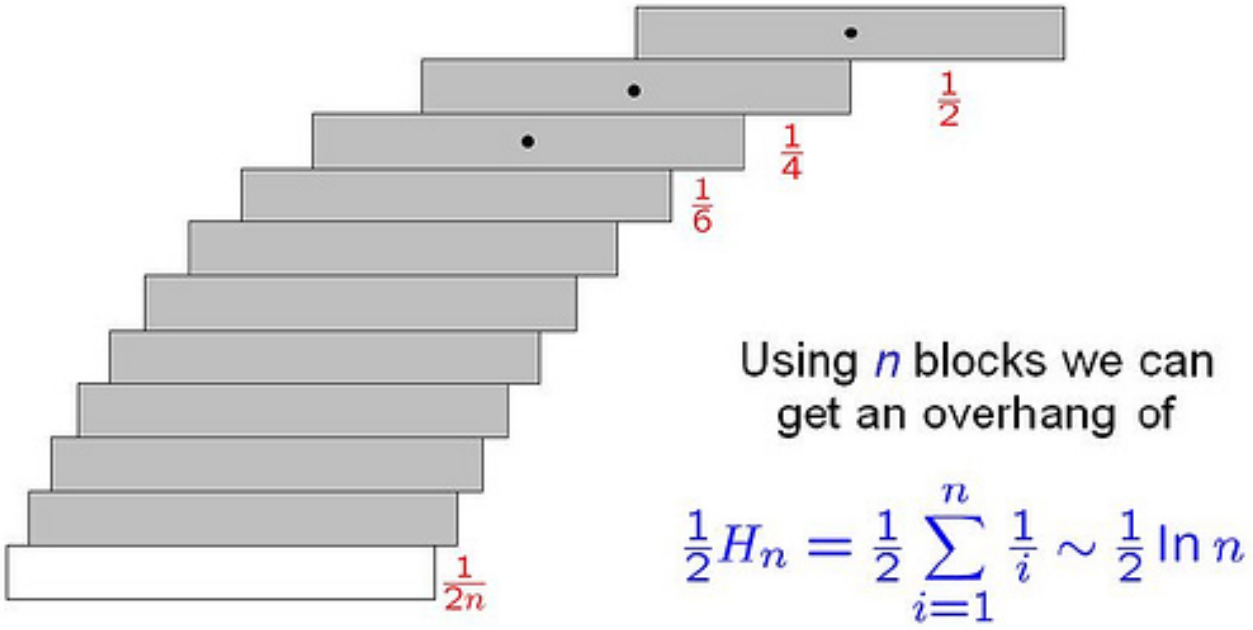
overhang 堆积木 - 能伸出桌面多远？

©Zhang-Zi, April 13, 2007 @ 12:49 pm

来自University of Warwick的Mike Paterson星期二在Yao的理论计算机课堂上给了一个非常有趣的小讲座。

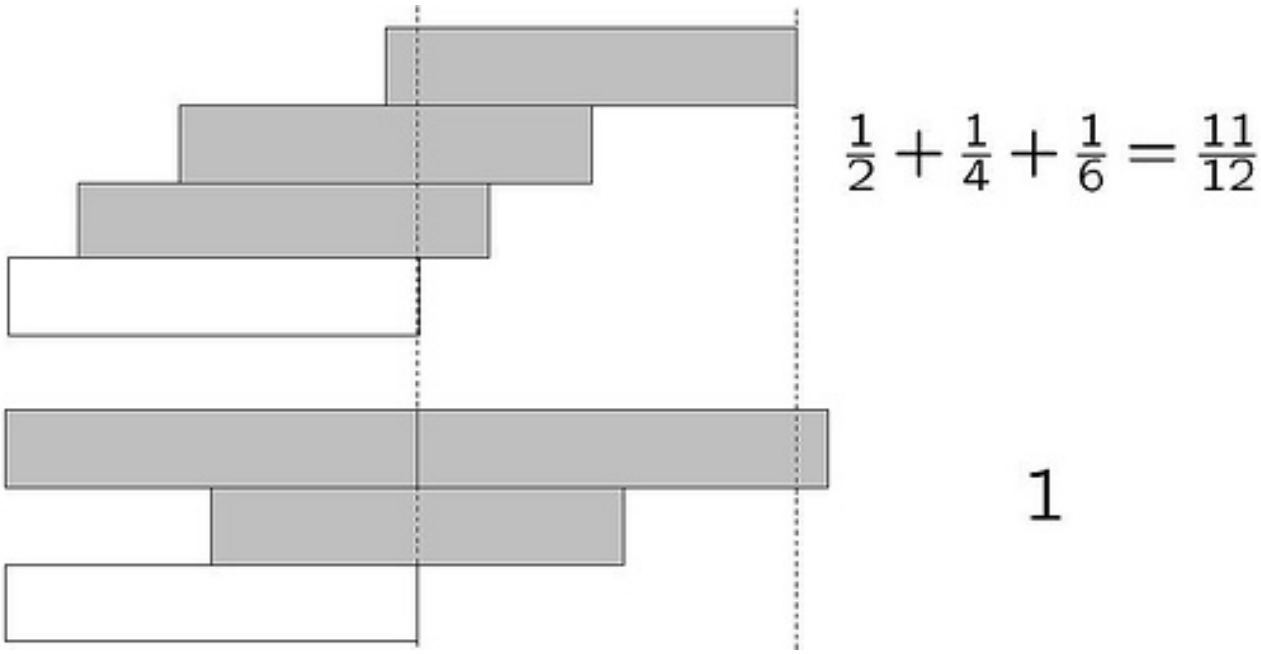
n个长度为1的砖块，叠起来能伸出桌面多远？（只考虑方块各平面都与桌面平行的情况）。

下面这种放法，很多人高中学物理的时候都见过吧？它用N个砖块伸出了大约1/2ln(N)。

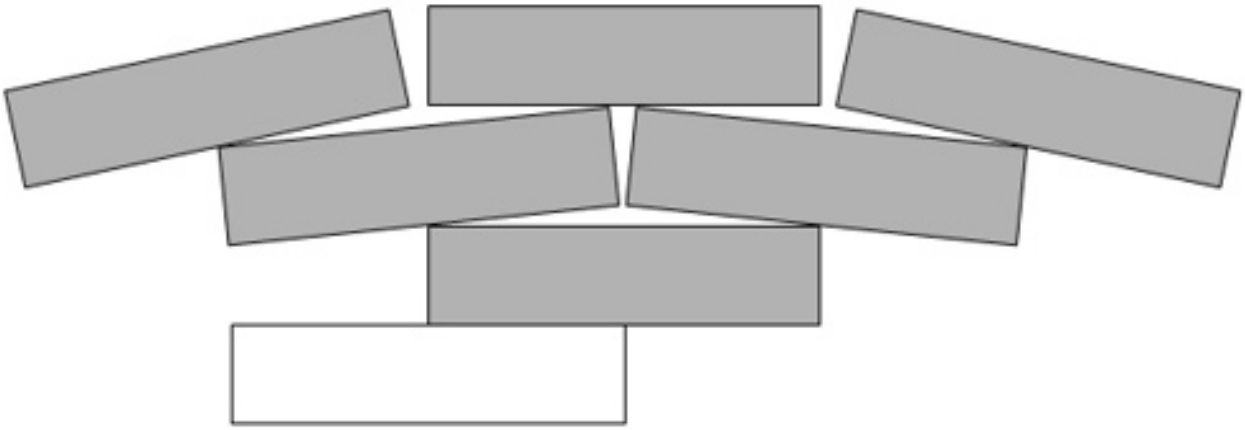


Harmonic Stacks

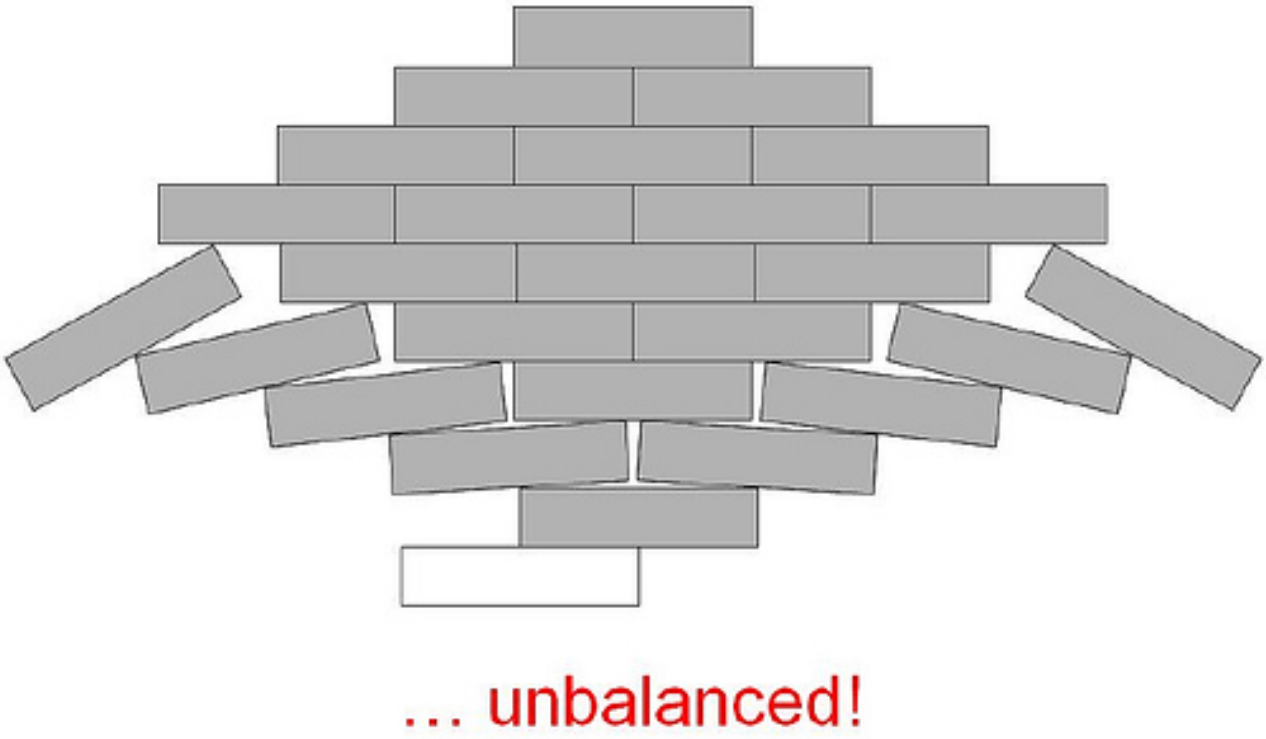
上面这种叠放方法称为Harmonic Stacks，但它是最优的吗？下面这个例子可以看出，在3个砖块，我们就已经能做的更好了。



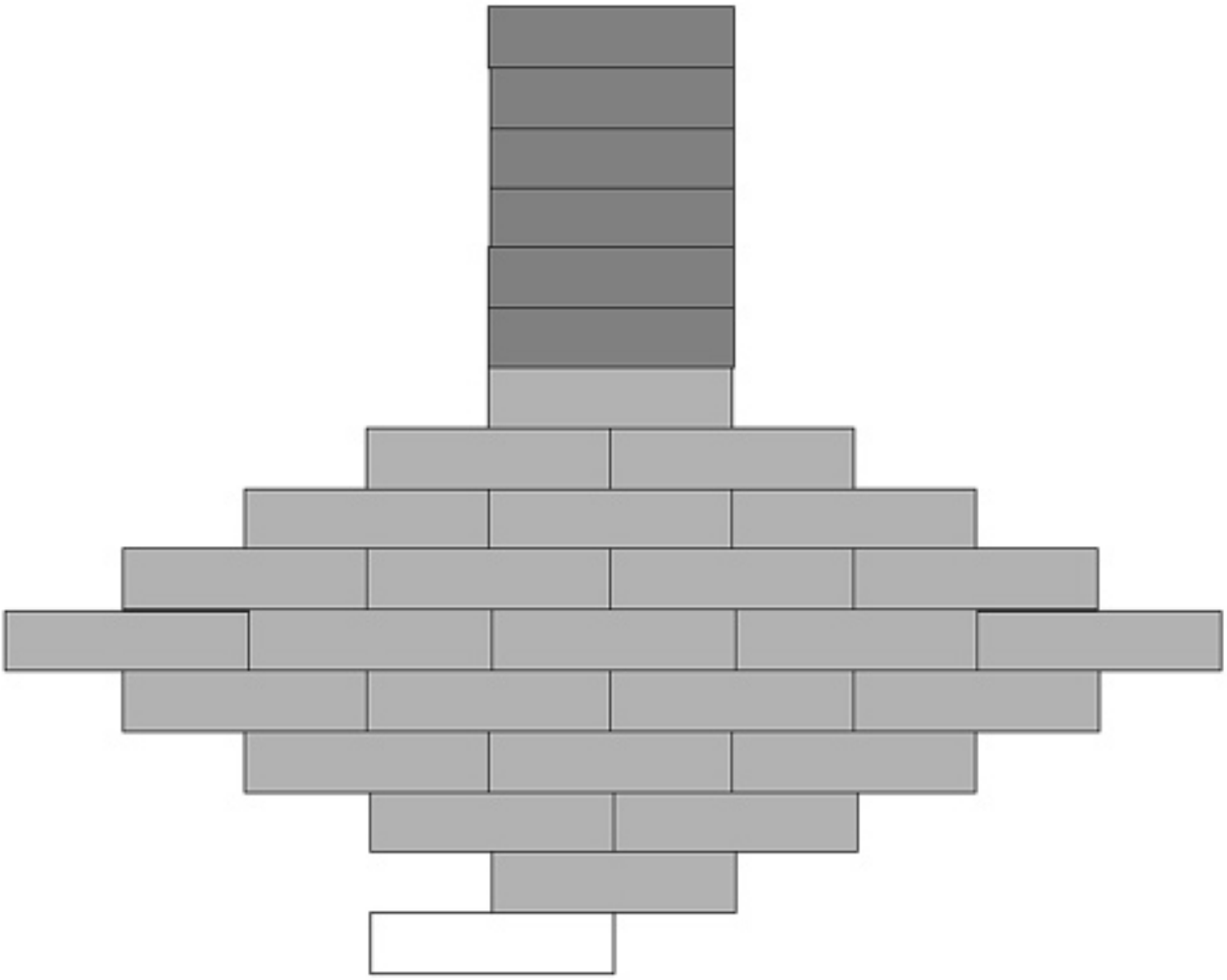
上面这个能继续往上堆么？很不幸



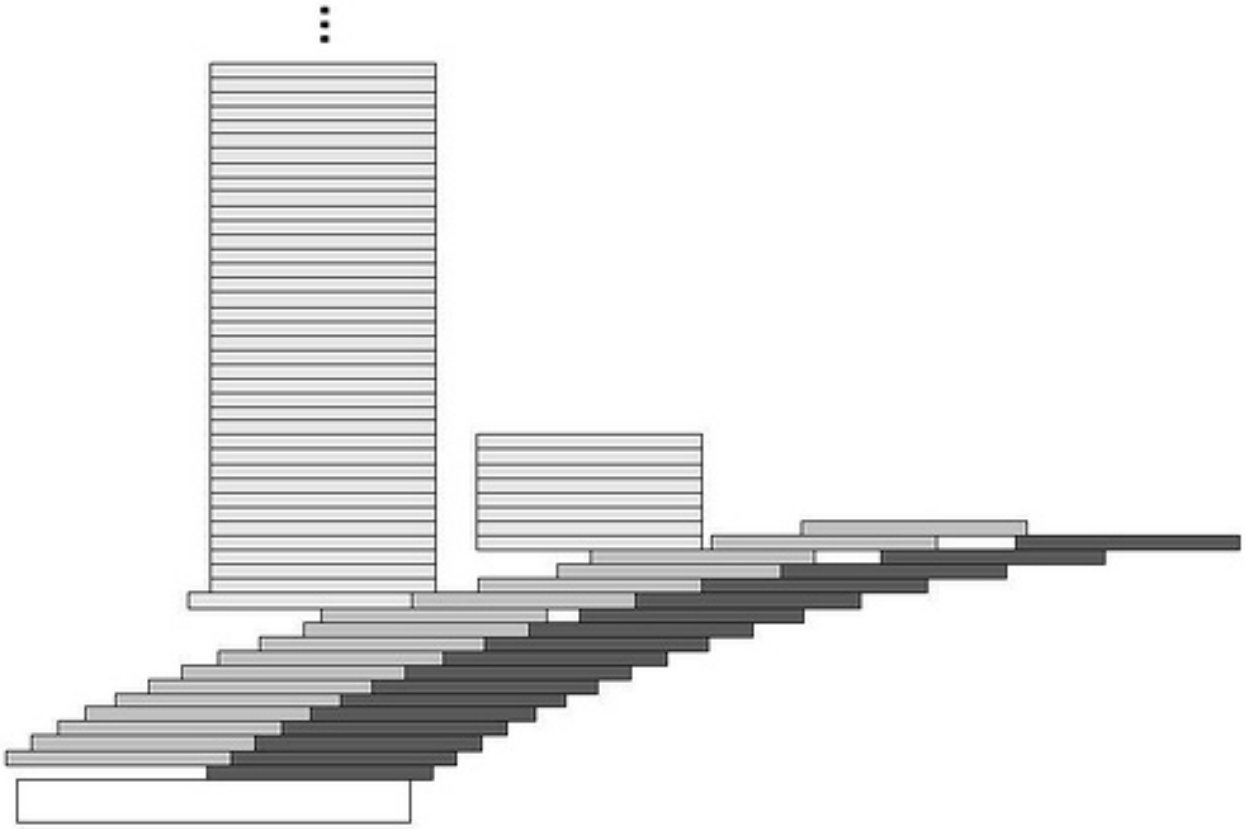
下面这个也不行



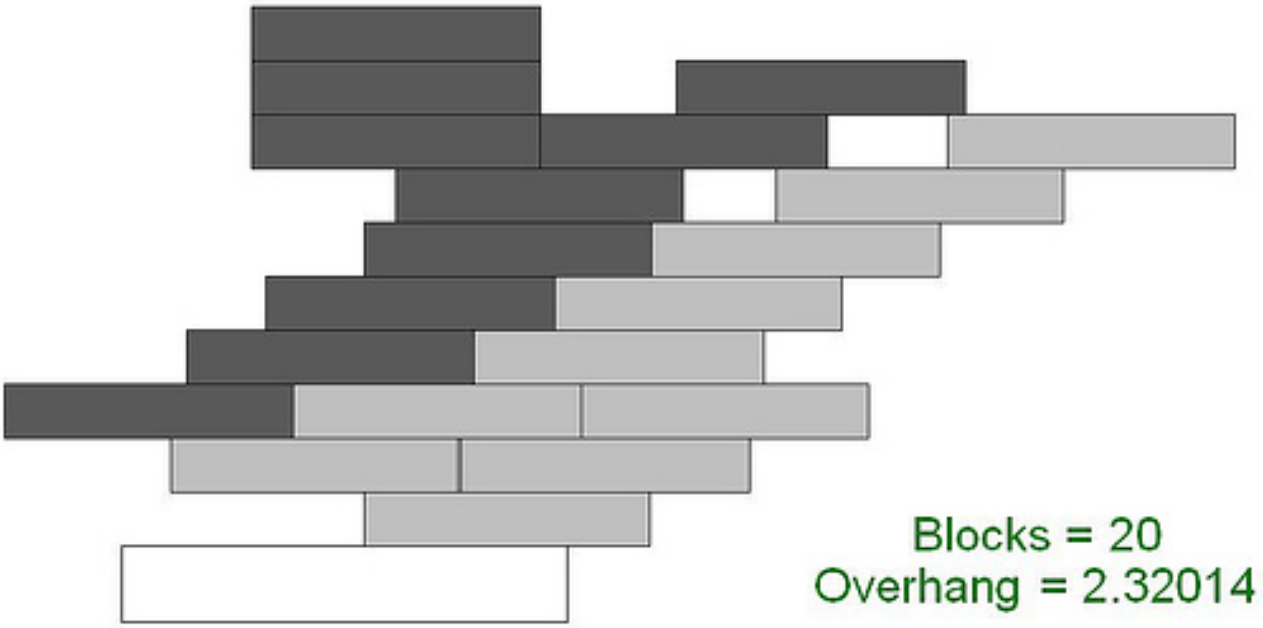
如果在上面再压很多砖块就可以了

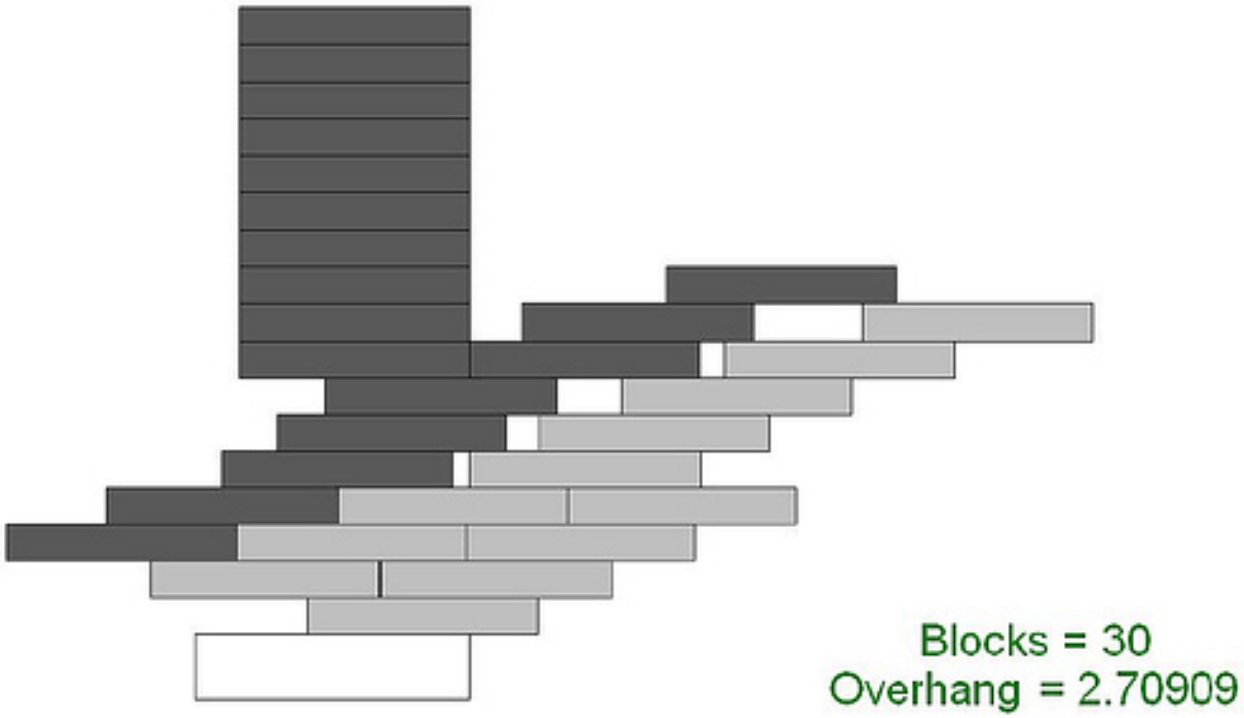


下面是一种叠放方法，可以做到大约O(lnN).

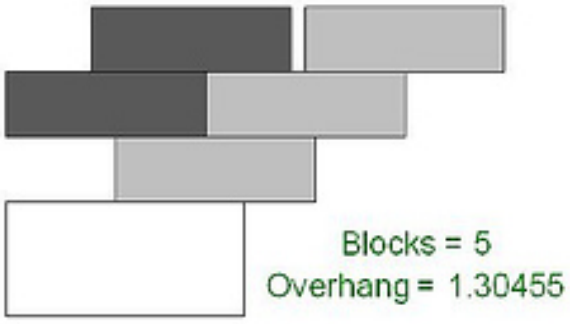


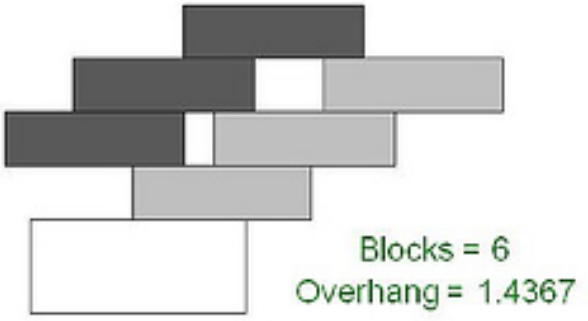
但它也不是最优的，下面是20个和30个方块的最优叠放方法，它比上面的要好

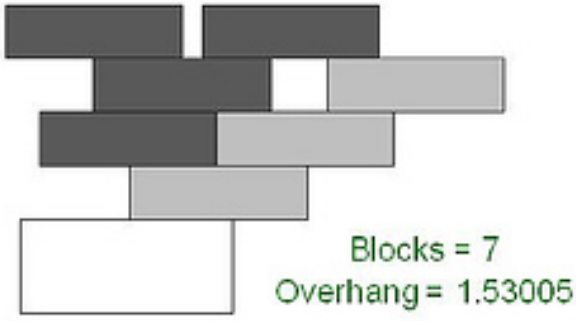


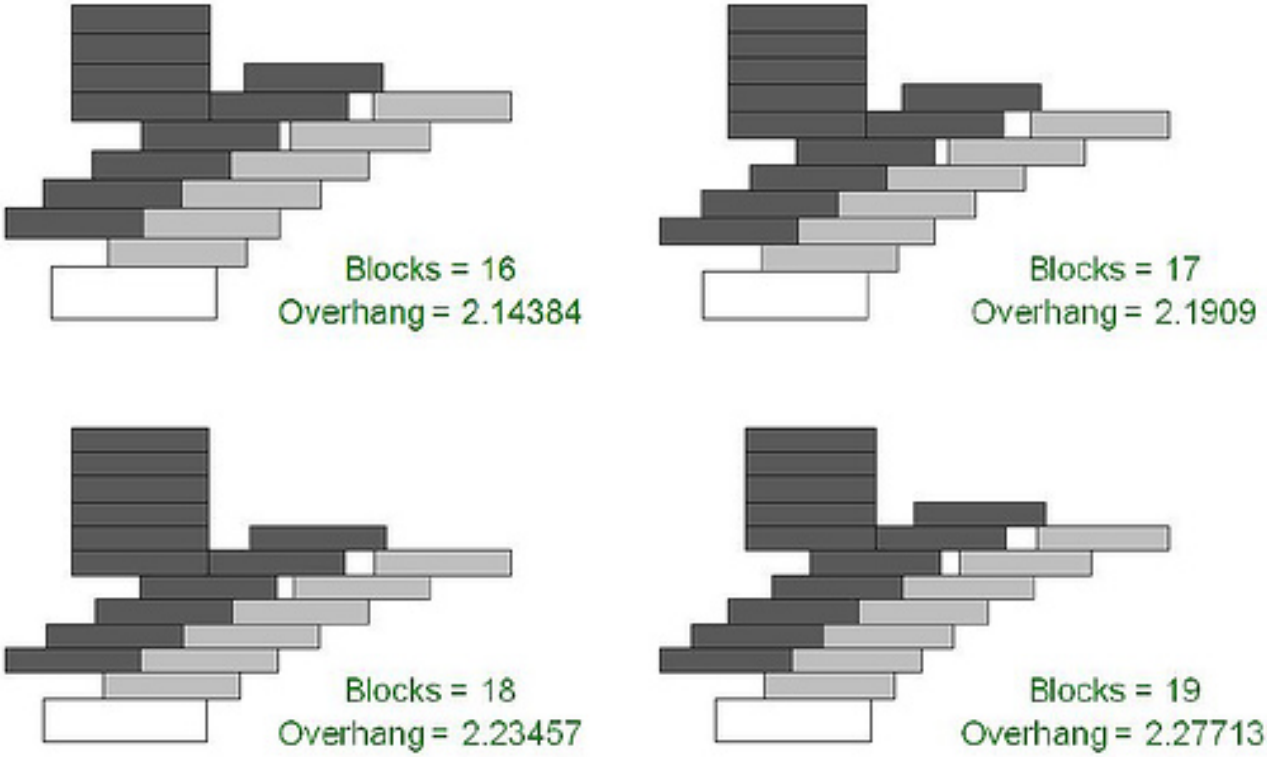


下面是砖块数目比较少的时候的最优叠放方法。

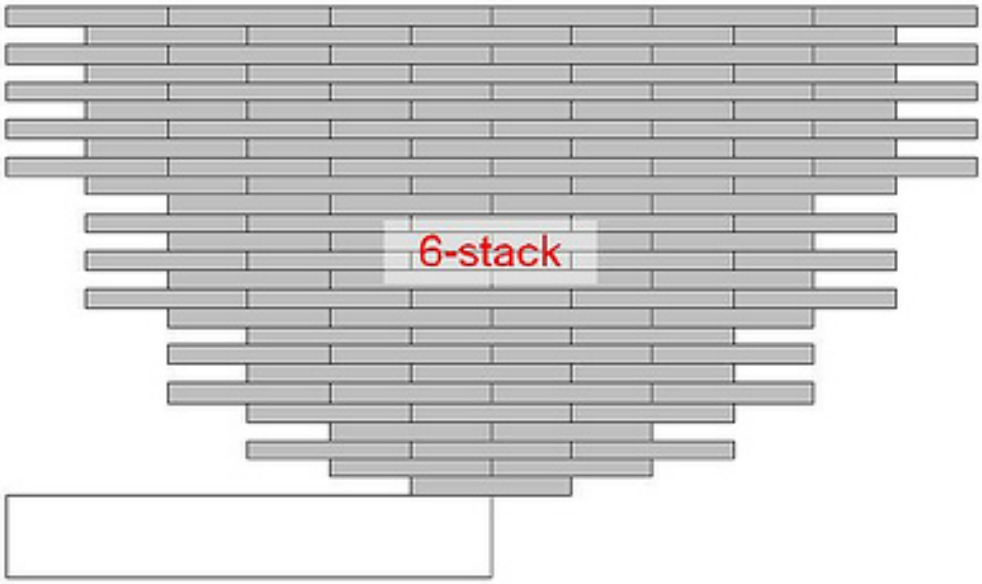








不过说了这么多，上面的方法都只能做到ln(N)的量级，而下面这个方法可以用N个砖块，往前伸出 N^(1/3)的长度。



Balanced!

Number of blocks:

$$\frac{(d-1)d(2d-1)}{3}+1$$

Overhang:

$$\frac{d}{2}$$

而且，Mike Paterson及其合作者证明了，这种方法在量级上已经是最优的了！

本文还有**15**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/564.html#comments**

China Theory Day

©Zhang-Zi, April 12, 2007 @ 6:04 pm

Tsinghua ITCS Theory Day (I)

time: Apr. 11, 2:00-5:00pm

The Institute for Theoretical Computer Science in Tsinghua University has initiated a Theory Day program, a one-day public workshop to be held each semester. This program is intended to communicate some of the exciting latest research results in theoretical computer science, especially those carried out in China. The talks are designed to convey the essence of the work, not only to the experts but also to the computer science community at large. Whether you are a specialist in this area, you will find the program stimulating.

The Theory Day inaugural program will be this Wednesday. Three brilliant young scientists of our institute will share their research results and insights with you. They are Dr. Xiaoming Sun (who graduated from our Institute in 2006), Xi Chen (fourth-year graduate student), and Pinyan Lu (second-year graduate student). Xiaoming's research interests include quantum computing, quantum information and classical complexity. Xi's interests lie in characterizing the computational complexity of natural problems in Algorithmic Game Theory and Computational Biology. And Pinyan's interests are in complexity theory, algorithms design and algorithmic game theory.

Tsinghua ITCS Theory Day (II)

time: Apr. 12, 2:00-5:00pm

The Institute for Theoretical Computer Science in Tsinghua University has initiated a Theory Day program, a one-day public workshop to be held each semester. This program is intended to communicate some of the exciting latest research results in theoretical computer science,

especially those carried out in China. The talks are designed to convey the essence of the work, not only to the experts but also to the computer science community at large. Whether you are a specialist in this area, you will find the program stimulating.

The Theory Day program II will be this Thursday. Three scientists will share their research results and insights with you. They are Professor Mike Paterson (who is a Professor of Department of Computer Science, University of Warwick, Coventry, CV4 7AL, United Kingdom), Professor Mario Szegedy (Rutgers University) and Professor Ran Raz (faculty of mathematics and computer science at the Weizmann Institute). Prof. Mike Paterson's research interests include graph theory. Prof. Mario Szegedy's interests are in complexity theory, combinatorics, combinatorial geometry and quantum computing. And Prof. Ran Raz's interests lie in Boolean circuit complexity, Arithmetic circuit complexity, Communication complexity, Propositional proof theory, Probabilistic checkable proofs, Quantum computation and communication and Randomness and derandomization.

本文还有**1**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/562.html#comments**

Why Quantum Computation? - 为什么要研究量子计算？

©Zhang-Zi, March 28, 2007 @ 11:40 am

最近被要求学习量子，所用教材是Berkeley的Vazirani在2004年所开的Intro, Qubits, Measurements, Entanglement的notes。下面是这套讲义的第一章的开头部分：

There are several reasons why we might wish to study quantum computation. Here are a few:

- Moore’s Law
  Moore’s Law states that the density of transistors on a chip roughly doubles every eighteen months. Current estimates say that in about a decade this should be down to single electron transistors. This is the end of the road for further miniaturization of classical computers based on electronics. Long before that chip designers will have to contend with quantum phenomena. Quantum computation provides a method of bypassing the end of Moore’s Law, and also provides a way of utilizing the inevitable appearance of quantum phenomena.
- Factoring, Discrete log, Pell’s equations, etc..
  There are certain problems that quantum computation allows us to solve more efficiently that any classical computational method. A few examples are listed above. We may wish to exploit this feature of quantum computation.
- Cryptography
  Quantum computation allows us to do cryptography in a way that doesn’t require assumptions about factoring primes, etc.. It also allows us to break classical cryptography schemas. Obviously, if we are interested in cryptography, we’ll also have to be interested in quantum computation.
  Above are the three standard reasons for studying quantum computation. There are other reasons as well that are perhaps just as compelling.
- Quantum Mechanics is a model of computation
  We can study quantum mechanics as a model of computation.
- Quantum Entanglement

In particular, the detailed study of entanglement is the most important point of departure from more traditional approaches to the subject. For example, quantum computation derives its power from the fact that the description of the state of an n-particle quantum system grows exponentially in n. This enormous information capacity is not easy to access, since any

measurement of the system only yields n pieces of classical information. Thus the main challenge in the field of quantum algorithms is to manipulate the exponential amount of information in the quantum state of the system, and then extract some crucial pieces via a final measurement.

Quantum cryptography relies on a fundamental property of quantum measurements: that they inevitably disturb the state of the measured system. Thus if Alice and Bob wish to communicate secretly, they can detect the presence of an eavesdropper Eve by using cleverly chosen quantum states and testing them to check whether they were disturbed during transmission.

本文还有**2**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/550.html#comments**

What if P = NP?

©Zhang-Zi, March 23, 2007 @ 9:44 pm

Princeton的Sanjeev Arora和Boaz Barak最近写了一本计算复杂性方面的书：Complexity Theory: A Modern Approach，其初稿提供下载，并承诺出版后也会继续保留——要是所有作者都这么好心就好了。

下面这段摘自于第二章NP and NP completeness，写得很有趣。为什么多数人不同意P=NP呢？因为

> “if (3SAT has a O(n^2) algorithm), then this would have consequences of the greatest magnitude. That is to say, it would clearly indicate that, despite the unsolvability of the (Hilbert) Entscheidungsproblem, the mental effort of the mathematician in the case of the yes-or-no questions would be completely replaced by machines.... (this) seems to me, however, within the realm of possibility.”
>
> Kurt Godel in a letter to John von Neumann, 1956

If P = NP — specifically, if an NP-complete problem like 3SAT had a very efficient algorithm running in say O(n^2) time — then the world would be mostly a Utopia. **Mathematicians could be replaced by efficient theorem-discovering programs** (a fact pointed out in Kurt Godel’s 1956 letter and discovered three decades later). In general for every search problem whose answer can be efficiently verified (or has a short certificate of correctness), we will be able to find the correct answer or the short certificate in polynomial time. AI software would be perfect since we could easily do exhaustive searches in a large tree of possibilities. Inventors and engineers would be greatly aided by software packages that can design the perfect part or gizmo for the job at hand. VLSI designers will be able to whip up optimum circuits, with minimum power requirements. Whenever a scientist has some experimental data, she would be able to

automatically obtain the simplest theory (under any reasonable measure of simplicity we choose) that best explains these measurements; by the principle of Occam's Razor the simplest explanation is likely to be the right one. Of course, in some cases it took scientists centuries to come up with the simplest theories explaining the known data. This approach can be used to solve also non-scientific problems: one could find the simplest theory that explains, say, the list of books from the New York Times' bestseller list. (NB: All these applications will be a consequence of our study of the Polynomial Hierarchy in Chapter 5.)

Somewhat intriguingly, this Utopia would have **no need for randomness**. As we will later see, if P = NP then randomized algorithms would buy essentially no efficiency gains over deterministic algorithms; see Chapter 7. (Philosophers should ponder this one.)

This Utopia would also come at one price: there would be **no privacy in the digital domain**. Any encryption scheme would have a trivial decoding algorithm. There would be no digital cash, no SSL, RSA or PGP (see Chapter 10). We would just have to learn to get along better without these, folks.

This utopian world may seem ridiculous, but the fact that we can't rule it out shows how little we know about computation. Taking the half-full cup point of view, it shows how many wonderful things are still waiting to be discovered.

P vs NP问题的介绍见以前的文章问题概述和历史，现状和未来。

本文还有**3**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/545.html#comments**

TCS课堂笔记：最佳约会策略

©Zhang-Zi, March 10, 2007 @ 8:00 pm

题外话：最近阅微堂发的都是网友转发的政治方面的文章，不爱看的人会比较痛苦。现在讨论一个轻松一点的话题。其问题，已经被研究了很多年，有许多不同形式的阐述方式和变种，应用范围也很广。下面应该是比较吸引人和简单的那种，来自姚期智教授的理论计算机（I）的授课内容——我是其助教之一。

现假设你在PIE上征友，或者以其它方式，选定了某些约会对象，比如n=20个。约会当然得一个一个来，那么假设

1. 可以将所有已约会的对象按优劣排序，但无法得知他们在所有的人里面的排名。在约会过程中，你知道某人是你目前已见到的最好的，但当时还不能确定是不是所有人里面最好的。
2. 如果你在约会当时决定放弃某人，后面再没有机会和此人和好——好马不吃回头草。
3. 选定意中人后，约会结束——骑驴找马是不道德的。

OK，现在目标当然是找到你心目中最喜欢的人。关系定得太早，会因为第2条假设——精彩的还在后头，定得太晚，会因为第3条——而后悔莫及。所以，什么策略才能让你以最大概率找到你最满意的那个人呢？

一个简单而且自然的方法是，待定k，与前k个人约会，不做任何选择。继续约会直到遇到比这前k个人还好的那个人为止。

通过概率计算得出，这个方法比我们想象中要好得多。通过选取合适的k=n/2.8=0.37n=7，有接近40%的机会选中最好的那位，有几乎70%的机会选中最好或者次好的那位。

可以证明，上面的策略已经是最优的了。

这个问题在日常生活中有更多应用。比如你打算在30岁前结婚，现在20岁。那么在24岁前

先别确定目标，24岁以后遇到比之前都好的就可以定下来。这几乎就是你能达到最好的结果了——假设你的候选人在这十年是均匀或者随机出现的。

这种策略也许能说明为何初恋成功率低？

以上所用都是爱情和婚姻的简化模型，没有考虑爱情中的主观因素。所以，请只把它当作一个脑力游戏。

本文还有**18**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/534.html#comments**

人有人的用处

©sog white, December 20, 2006 @ 10:24 pm

第一次听到“控制论”这个名词大概是上初中的时候，有一次在家里和哥哥聊天，说起了某个话题；哥哥突然冒出来一句：“你有时间看看《控制论》吧？”。当时觉得这是一个很奇怪的名词，便一直记在了心里。事后想一下也觉得很诧异，哥哥虽然比我大不少，但是学英语的，应当也没有系统看过控制论方面的东西，最多可能是道听途说的看过一点简介，何以会在当时那个场景之下提示我？因此便慢慢的觉得控制论对我而言有某种暗示。

后来，有机会接触60年代左右的科学哲学思潮，当时对系统论较为深入的看过两本书，信息论也看过一点，控制论方面的东西就只有皮毛了。作为一个心结，经常想到要解开；曾经硬着头皮啃维纳的经典之作，味同嚼蜡、不知所云，就放弃了。到前两天重新找出来其《人有人的用处——控制论和社会》，到昨天晚上终于看完；而且，许多地方看的很有心得，让人油然而生欣喜之意，得到不少收获。

控制论，被维纳称之为一个偶然性的宇宙观；把一种方法论提高到宇宙观的高度来看待，其意义在我理解来是说——按照控制、反馈模式这个框架来套万事万物，所有的现象（从自然到社会）都可以纳入这个模式框架之内。所谓一锤在手，天下皆钉；作者的意思似乎是说，如果运用好控制论，就可以控制世界；反正我觉得管理学和控制论是有些关系的。维纳是个数学家，从数学物理方法的角度来讲，一个人就是自然数1，一台机器也是自然数1，抽象的失去了个体差异。所谓带甲三万，屠城五座，杀敌六万形式的描述，更是一种数字化的白描的战功，而失去了血肉形象和人性化的道德感。遑不论其中人的个体差异，和牵涉其中的复杂的事件。以致我有时候觉得数学和计算机是残酷的，让人容易陷入救一人、杀一人的逻辑。是不是理性的人容易悲观？

作者是从控制论的直观意义和哲学层面来写本书的，而不是从数学角度，中间只有很少的一小段提到偏微分方程和参与的火炮自动控制工作方面的内容。作者强调控制论的意义：当整个宇宙（如果真的有整个宇宙的话）趋于衰退时，其中就有一些局部区域，其发展方向看来是和整个宇宙的发展方向相反，同时它们内部的组织程度有着暂时的和有限的增加

趋势。生命就在这些局部区域的几个地方找到了它的寄居地。控制论这门新兴科学就是从这个观点为核心而开始其发展的。有点整体悲观，局部乐观的意味；就像人生一场空，但生活依然有其意义一样。

控制论是建立在信息论的基础之上的，从信息的通信开始说起，信息的作用就是控制，通信的有效性体现为控制的反馈；根据反馈进行调节和二次控制。从控制的角度讲，信息和力并没有本质上的差异，其实这是一个意义非常重大的观念。例如：我可以自己动手把一本书从一楼拿到五楼，也可以给另一个人说话（控制命令信息），让其把书替我从一楼拿到五楼；对我而言，动口相当于动手，信息相当于力。通过信息可以传输物质，也许可以变为现实。让我们举两个科幻的例子：（1）、在某科环童话中，通过传真机可以传送人；（2）、在电影《Martix》（黑客帝国）中，大家可以自由的通过固定电话跑来跑去；呵呵，可以理解为灵魂出窍，而灵魂的道路是电话线。让我们设想一下，如果人包含的生物信息可以全部被破译，类似于DNA编码的数据当然可以被传送，然后通过通信线路传送到 另外一个物理位置，然后通过生物合成技术被还原制造（克隆）；如果这一切在很短的时间之内发生，难道不是信息通信传送物质吗？

从通信的信码讲到语言，语义损耗等问题。许多大牛讲到哲学问题，最后总是会把其中一些哲学问题，归结为语言问题；因为语义分歧等问题，相同的概念，难以得到一致的认同，于是思辨产生了，带来了所谓的哲学问题。维特根斯坦认识到了这个问题；禅宗大师更是说：言语道尽，不立文字，以便不让惶惑的误解起不好的指引。举例说，把一种语音译成另一种语言时，字义之间的不完全等当就限制着这一语言的信息向另一语言流动，其中的种种困难是显而易见的。

由语言也讲到了法律问题，作者先肯定世界上是没有公平的（人生来是平等的，作为法律的基本信条是一种理想），法律是追求公平的一种努力。作者指出：噪声可以看作人类通讯中的一个混乱因素，它是一种破坏力量，但不是有意作恶。这对科学的通讯来说，是对的；对于二人之间的一般谈话来说，在很大程度上也是对的。但是，当它用在法庭上时，就完全不对了。当事人力图用法律条文所规定的种种方法使审判官和陪审员成为自己方面的合作者。在这种博奕中，对方的律师，不同于自然界自身，能够设法把混乱引进他所反对的那一方的消息中去，而且他是有意识地这样做的。他设法把对方的陈述变成没有意义的东西，并且有意识地把对方和审判官与陪审员之间的消息堵塞起来。在这种堵塞的过程

中，欺骗手段有时不免非常需要。由此分歧而造成了两种法律体系：（1）、罗马法系，以抽象的正义原则为基础。（2）、英国法系，以公开宣称判例作为法学思想的主要基础。中国似乎属于罗马法系阿，加之中文自然语言的不严密性和法官的模棱两可，效果很不好。

其中也提到了知识分子和科学家的作用：自然界的被动抗拒和一位敌手的主动抗拒，达二者之间的差别使人联想到了科学研究工作者和军人或赌#徒之间的差别。科学研究工作者随便在什么时候和什么地方都可以从事他的种种实验而不用担心自然界会在什么时候发现他所使用的手段和方法，从而改变其策略。所以，他的工作是由他的最好时机支配着；反之，一位棋手就不能走错一着棋而不会碰上一位机敏的敌手打算利用这个机会而打败他的。因此，棋手之受他的最坏时机的支配要多干受他的最好时机的支配。我对这个论点也许有偏见，因为我觉得我自己能在科学上作出有效的工作，但在下棋的时候，却经常由于自己在紧要关头的轻率大意而遭到失败。所以，科学家是倾向于把自己的敌手看作一位作风正派的敌手。这个态度对于他之作为科学家的有效性讲来，是必要的，但这会使他在战争中和政治上容易受到无耻之徒的欺骗。这个态度的另一个结果，就是一般公众对他难于理解，因为一般公众关心一己之敌远甚于关心象自然界这样的敌手。这段论述非常精辟，以至于我感到自己无从插嘴。所以，要想作为一个成就卓著的科学家，那他就必须纯朴，甚至是有意识地纯朴，假定自己是跟诚实的上帝打交道，所以他就得象个诚实的人那样地对世界提出自己的问题的。因此，科学家的纯朴虽然是顺应职业而形成的特点，但不是职业上的缺点。这个态度对于他之作为科学家的有效性讲来，是必要的，但这会使他在战争中和政治上容易受到无耻之徒的欺骗。

在文中，作者多次提到了爱因斯坦的科学方法论名言：上帝精明 ，但无恶意。科学家总是力图发现宇宙的秩序和组织性的，但是总是有一种奥古斯汀式的恶魔妨碍我们去发现自然界的规律。自然界抗拒解密，但它不见得有能力找出新的和不可译解的方法来堵塞我们和外界之间的通讯的；这个恶魔其实就是我们自身弱点的量度。这方面的含义，作者举了一个例子：二战时期同盟国和轴心国竞赛赶造原子弹，作者认为其中最大的机密是，明确了可以通过某种方法造出原子弹；然后双方分别集中自己最优秀的科学家、工程师和组织力量来攻破这个目标。事实上，德国在这方面的进度也就落后一点而已。从这句名言引申出去，我想到了：凡事都有好方法这一越来越被我理解的更深的做事原则。许多事情，多动一下脑筋，都是游刃有余的。

维纳还谈到了许多对科技史的理解：第一次工业革命的蒸汽机和第二次的电动机，最大的不同是能量可以自由的传输：蒸汽机传动需要复杂的机械，但是电能通过电缆就可以流动；所产生的自动机都是对人的肌力的替代物和解放。在他那个时代（1950年前后），第三次工业革命的计算机刚刚起步，作者预估了计算机在自动控制中的核心地位；我们站在总结一下，不难得出计算机是对人脑力的补充和解放这一结论，但是反观今天的许多困境，需要思考：我们使用计算机的方式得当吗这个问题？

也许有一天会出现人的心力替代物的自动机，真正具有自我学习改善功能；如果计算机不具有感性，计算机自身是不能造出比自己更强大的智能自动机的。

本文还有3条留言，察看留言和讨论请到http://zhiqiang.org/blog/501.html#comments

"完美"的洗牌次数 - 7次

©Zhang-Zi, December 15, 2006 @ 12:23 pm

在大家玩牌的时候，每一局之前都需要重新洗牌——一次洗牌指将牌分为左右两垛然后穿插放牌，但多少次洗牌才是正当的呢？就我多次打牌的观察，多数人都不超过4次。

但就D. Aldous和P. Diaconis在1992的一个结果，要想达到“比较完美”的洗牌效果——洗完牌后牌局基本上随机分布，至少需要5次，要达到“完美”洗牌，则需要7次。但更多次数不会有太多改进。这还是对于一副牌而言的。对于两副牌则需要9次，6副牌需要洗12次。

所用方法是计算图上随机游走达到稳定分布的速度。而这个方法就应用于上面这个结果之后，对于理论计算机的概率算法产生了深远的影响，这也使得P.Diaconis的这篇论文超出了它本身看似玩物的领域。

再谈一下P. Diaconis，此君14岁离家，去做职业魔术师，没上高中，后来用白天魔术表演挣来的钱晚上念大学课程，最后获得哈佛的博士和斯坦福的教职。另传说中，此人赌技惊人，是赌场不受欢迎之人物。

本文还有**4**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/498.html#comments**

TCS：One-Time Password 一次性密码及其应用

©Zhang-Zi, November 1, 2006 @ 7:19 pm

题外话：此篇隶属于理论计算机(TCS)系列。

昨天，RSA实验室的首席科学家Burt Kaliski（同时也是副总裁）给我们做了一个讲座，关于最新的One-Time Password的一些应用。开始讲的时候还不觉得有啥，后来想了一下，这玩艺儿还是挺有用的，怪不得RSA Lab对之这么看重。

One-Time Password，就是给用户端一个Token（可以是一个小电子设备的形式），与服务器段共享了一个seed，利用这个seed，双方在相同时间能产生一个相同的password（比如使用hash函数处理seed + time——hash函数介绍见从hash函数到王小云的MD5破解），用户利用Token生成的密码登录服务器，服务器进行对比验证。

目前密码体系的不安全之处在于数据传输可能被监听，用户客户端可能存在木马，用户可能随手写下密码造成密码泄露等等。而利用上面的One-Time Password，即使这个密码被人非法获取，也不会造成损失。所以，这玩艺儿在银行的密码管理中是非常有用的，听说有银行已经开始使用此类技术。

Burt Kaliski此次讲座讲了One-Time Password的四个应用：

- How to authenticate to a laptop computer with an OTP token --- without storing long-term secrets on the computer
- How to use the same token to authenticate to multiple servers --- without sharing secrets among the servers or relying on a third party
- How to set up a strong, shared key between parties that only share a short OTP value
- How to protect OTPs against malware and MITM attacks

这些比较技术化，不详述。

关于RSA实验室：RSA即鼎鼎有名的RSA公钥密码体系，在密码界举足轻重。讲座完毕之后，有人问起RSA的前途，Burt说RSA公钥密码体系已经发明30年了，估计还能用30年，

因为估计30年后量子计算机已经有所突破（量子计算机下，RSA公钥密码体系所依赖的大数分解已经被证明是不安全的）。

记得Yao以前也多次提到，在未来15到20年，量子计算机必有所突破，是将来的大热门啊。也许我也应该去玩这个。

参考：

- RSA Lab上的One-Time Password主页
- 2nd Trustworthy Interfaces for Passwords and Personal Information Workshop

本文还有**3**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/474.html#comments**

“21世纪的计算”大会

©Zhang-Zi, October 26, 2006 @ 9:50 pm

前天（24日），21世纪的计算大会在清华举行，今年的主题演讲嘉宾包括微软全球高级副总裁、美国国家工程院院士里克·雷斯特（Rick Rashid）博士、清华大学高等研究中心教授，2000年图灵奖获得者姚期智（Andrew Yao）博士、微软硅谷研究院院士，1998年图灵奖获得者Jim Gray博士、前瑞士联邦技术学院计算机系教授，1984年图领奖得主Niklaus Wirth博士等八位在全球久负盛名的大师。上午老板姚先生讲的PCP定理，我由于有课没能一睹姚的风采，但估计现场能听懂的人不会超过1%。

我去听了下午的四场演讲。微软亚洲研究院院长沈向洋的Research 2.0比较有趣。其间展示了MSRA的两项新成果。第一个是对联生成器：给出上联，软件生成下联和横批。现场演示的效果非常出色，几个对子都对得很不错，连拆字联都能识别出来。不过我觉得有作弊嫌疑，因为给出的上联都是他们自己输入的，这些可能是他们事先就挑选好了的，如果真正让观众出上联的话，难不成下联会对成什么样子。不过，昨天同学发现了MSRA专为此建了一个网站http://duilian.msra.cn，上面已经给出了这个软件的演示和下载，不过功能比现场展示的功能要弱一些：

点击试用
清晰版(1282K)
压缩版(351K)

沈还展示了一个视频软件，这个软件可以跟踪人脸，替换背景。类似的技术已经发展好多年了，以前在MSRA实习的时候旁边的同事就做的这玩意儿，后来还发了一篇SIGGRAPH。我怀疑这个软件就是那个同事后来的改进版本。现在这个东西不但可以跟踪人脸，而且可以具体到人脸上的具体的器官，比如眼睛，鼻子，嘴巴等。现场就演示了直接修改脸部形象，比如把眼睛加大，鼻子垫高，嘴唇变厚等，还可以加个面具，加幅墨镜啥的。表演者很恶搞，场面十分有趣。个人感觉，这个软件已经很成功了。不过想到，这种软件一出，以后视频聊天谁也不能保证屏幕上一定是对方的庐山真面目了，比如我，就想着把眼睛弄大一点要帅一些 。

本文还有**8**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/468.html#comments**

TCS: 拜占庭将军问题 (The Byzantine Generals Problem)

©Zhang-Zi, September 22, 2006 @ 1:08 pm

这个问题在Yao的理论计算机课上整整讨论了2节课。它是一个算法设计问题，也极具趣味性。下面是它的一些介绍和解决方案([1])。

拜占庭帝国就是5～15世纪的东罗马帝国，拜占庭即现在土耳其的伊斯坦布尔。我们可以想象，拜占庭军队有许多分支，驻扎在敌人城外，每一分支由各自的将军指挥。将军们只能靠通讯员进行通讯。在观察了敌人以后，忠诚的将军们必须制订一个统一的行动计划——进攻或者撤退。然而，这些将军中有叛徒，他们不希望忠诚的将军们能达成一致，因而影响统一行动计划的制订与传播。问题是：将军们必须有一个协议，使所有忠诚的将军们能够达成一致，而且少数几个叛徒不能使忠诚的将军们做出错误的计划——使有些将军进攻而另一些将军撤退了。

抽象出来，可以表述成：

> 拜占庭将军问题：设计一个协议，一个司令要送一个命令给他的n-1个副官，使得
> IC1. 所有忠诚的副官遵守同一个命令。
> IC2. 假如司令是忠诚的，则每一个忠诚的副官遵守他送出的该命令。
>
> 约定：忠诚的将军将遵守协议，而叛徒则可能破坏协议，尽可能的干绕其它人的判断。叛徒是匿名的。而且最后不需要确定谁是叛徒。

注意司令也有可能是叛徒，所以IC2与IC1是不同的。

递归设计协议OM(n, m)为

OM(n, 0):

1. 司令发送命令给所有副官。
2. 副官按照接收到的命令行事。

OM(n, m):

1. 司令发送命令给所有副官，设副官i收到命令vi。
2. 分为独立的n-1轮：对每个副官i，将其视为司令，使用协议A(n-1, m-1)将vi发送到所有其它副官。
3. 这样每个副官都收到n-1条信息，每个副官都按照出现次数更多的命令行事（如果进攻和撤退的命令一样多，则默认取撤退）。

递归证明

引理：当n>2m+k，n个将军中至多k个叛徒，协议A(n, m)满足IC2，即司令是忠诚的，每个忠诚的副官将会执行司令的命令。

进而说明：

当n>3m时，n个将军，且至多m个叛徒，协议A(n, m)可以同时满足IC1和IC2。

更深刻的结论：

当n<=3m时，n个将军中的m个叛徒可以让将军们无法达成一致，也就是满足IC1和IC2的协议不可能存在。

参考：

1. The Byzantine Generals Problem, the first paper involved
2. 可信计算VII:拜占庭将军问题
3. Byzantine failure - Wikipedia, the free encyclopedia

PS: 标题里TCS是Theoretical Computer Science(理论计算机科学)的缩写，这篇文章同属于理论计算机介绍系列文章，算作理论计算机初步系列文章的补充吧。

本文还有**0**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/449.html#comments**

理论计算机初步：从**hash**函数到王小云的**MD5**破解

©Zhang-Zi, September 18, 2006 @ 8:51 pm

密码学是理论计算机的一个很大的方向。之前准备先写密码学概论再提在hash函数破解上做出重大贡献的王小云教授的工作，不过前两天王小云获得求是杰出科学家奖以及100万奖金，在媒体上又掀起了一轮宣传狂潮，但是有些报道极端弱智，错误百出，所以我趁机纠正一下，并介绍密码学的一个组成部分——hash函数，以及王小云在这上面的工作。

王小云的主要工作是关于hash函数的破解工作。她在2005一个密码学会议上宣布破解了SHA-1，震惊了全世界。所以要介绍和理解她的工作，先看一下hash函数具体是怎么回事。

简单的说，**hash**函数就是把任意长的输入字符串变化成固定长的输出字符串的一种函数。通俗得说，hash函数用来生成信息的摘要。输出字符串的长度称为hash函数的位数。

目前应用最为广泛的hash函数是**SHA-1**和**MD5**，大多是128位和更长。

hash函数在现实生活中应用十分广泛。很多下载网站都提供下载文件的MD5码校验，可以用来判别文件是否完整。另外，比如在WordPress的数据库，所有密码都是保存的MD5码，这样即使数据库的管理员也无法知道用户的原始密码，避免隐私泄露（很多人在不同地方都是用的同一个密码）。

如果两个输入串的hash函数的值一样，则称这两个串是一个碰撞(**Collision**)。既然是把任意长度的字符串变成固定长度的字符串，所以，必有一个输出串对应无穷多个输入串，碰撞是必然存在的。

一个“优良”的hash函数 f 应当满足以下三个条件：

- 任意y，找x，使得f(x)=y，非常困难。
- 给定x1，找x2，使得f(x1)=f(x2)，非常困难。
- 找x1，x2，使得f(x1)=f(x2)，非常困难。

上面的“非常困难”的意思是除了枚举外不可能有别的更快的方法。比如第3条，根据生日定理，要想找到这样的x1，x2，理论上需要大约2^(n/2)的枚举次数。

几乎所有的hash函数的破解，都是指的破坏上面的第三条性质，即找到一个碰撞（前两条都能被破坏的hash函数也太弱了点，早就被人抛弃了）。在密码学上还有一个概念是理论破解，指的是提出一个算法，使得可以用低于理论值得枚举次数找到碰撞。

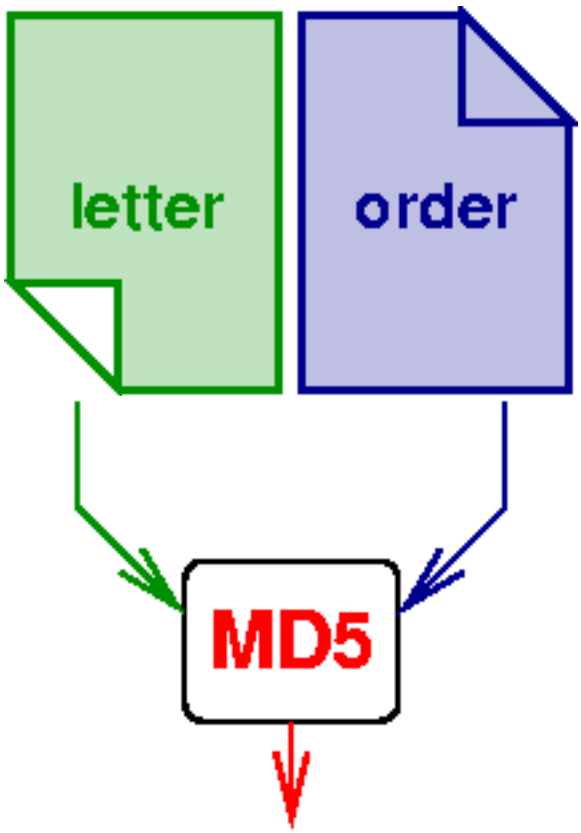
王小云的主要工作是给出了MD5，SHA-0的碰撞，以及SHA-1的理论破解，她证明了160位SHA-1，只需要大约2^69次计算就能找出来，而理论值是2^80次。她的寻找MD5碰撞的方法是极端高效的。传说王小云当时在会议上把碰撞写出来，结果被下面的人验证发现不对，原来她把MD5算法的一个步骤弄错了。但是她立马联系她的当时留在中国的学生，修正算法，并找到一个新的碰撞。这一个是对的。

看到这里，那些认为中国国安局应该将这些结果封存作为秘密武器甚至幻想用这些成果来袭击美国之徒可以停住你们的YY了。这种形式上的破解，在大多数情况下没有实际性的作用。更别提MD5早就被美国人抛弃了。

但是，说这种破解一点实际意义都没有，那就侮辱了广大密码学家的智商，密码学家不会无缘无故的弄出碰撞这么一个概念来。下面简单的介绍一下在特定情况下，怎么利用给定的碰撞来做坏事(翻译自Attacking Hash Functions)：

Caesar给实习生Alice叫写了一封推荐信(letter)。同一天，Alice叫Caesar在推荐信上数字签名，并提供了一份推荐信的电子板。Caesar打开文件，发现和原件一模一样。所以他在文件上签了名。

几个月后，Caesar发现他的秘密文件被非法察看。这到底是怎么回事呢？



a25f7f0b 29ee0b39 68c86073 8533a4b9

事实上，Alice要求Caesar签名的文件letter已经被Alice做了手脚，准确地说，Alice还准备了另外一个文件order，它们的MD5码完全一致。而Caesar的数字签名还依赖于MD5算法，所以Alice用order文件替换Letter文件之后，Caesar的数字签名依然有效。那封order给Alice提供了察看秘密文件的权限。

具体的实现方法可见Hash Functions and the Blind Passenger Attack。我在这里简单的解释一下(只是大致思路，具体实现方式，需要对文件结构信息有所了解)：

letter文件的内容是：

```
if(x1==x1) show "letter" else show "order"
```

order文件的内容是：

```
if(x2==x1) show "letter" else show "order"
```

其中字符串"letter"和"order"代表两封信实际显示的内容。x1，x2是一个MD5的碰撞。

上面的方法，只供参考和学术用途，实际使用所引起的后果概不负责。

参考：

- Attacking Hash Functions by Poisoned Messages "The Story of Alice and her Boss"
- Hash function, wikipedia
- SHA, wikipedia
- Interview with Yiqun Lisa Yin concerning the attack on SHA-1

PS：我跟王小云老师的接触很少，上过俩次她的讨论班而已，亦感觉到王小云老师的严谨和耐心。在去年一个Turing奖获得者的演讲上，王小云提问的时候竟口而出“I ask who”的中式英语，在引起哄笑的同时，我也极端佩服她的勇气。也许只有这样才能做出非常好的工作吧。

PS2: wikipedia在国内可以通过free_door浏览。

本文还有**18**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/446.html#comments**

理论计算机初步：概率算法和近似算法

©Zhang-Zi, September 14, 2006 @ 9:32 am

前面已经提到了显示中大多数难解问题问题最后都被证明是NP-完全问题。这意味着，除非NP=P，它们是不可能有多项式时间算法的（而且，在这篇文章提到即使NP=P，人们也可能找不到一个NP完全问题的“有效”算法）。

所以人们发展了各种工具来避开它们，最常用的两种方法是使用概率算法和近似算法，这两种方法也符合实际需要：在解决实际问题中，我们不需要结果绝对正确，也不需要结果绝对精确。

所谓概率算法，就是在算法的过程中引入随机数，使得算法在执行的过程中随机选择下一个计算步骤。它最后可能导致结果也是不确定的。一个结果不确定的概率算法叫做Monte Carlo算法，而总是得到准确解的概率算法叫做Sherwood算法（一个例子是引进随机因子的快速排序算法）。

为何引入随机数能够提升计算性能（事实上，理论计算机学家还没能证实随机因子本质上更有效率——指具有指数级别的效率提升），主要有下面两个原因：

首先，通常一个算法，它对于很多种情况是比较快的，但对于某些“特别差”的输入，它要找到一个解则特别困难。引入随机数之后，使得算法的时间复杂度平均化了，然后算得更快（评价一个随机算法的复杂性通常是考虑其平均复杂性）。

其次，对于Monte Carlo算法，它的输出是不精确的，这种牺牲使得算法能够在较短时间内完成。

需要指出的是，下面这个定理，使得一个不那么精确的Monte Carlo算法亦有实际的效用的：

如果一个判定问题的某个Monte Carlo算法有2/3的正确几率(这个2/3可以

> 替换成任何一个大于1/2的数，当然小于等于1/2的随机算法一点意义都没有，因为还不如抛硬币），重复这个算法k次，取出现次数更多的结果作为问题的答案，则这个答案的正确率大于1-1/2(8/9)^k。

上面的结果由于k出现在指数上，所以只需要将一个Monte Carle算法重复很少的次数，便能得到很高的准确率。

近似算法从字面的意思来看似乎和上面的Monte Carle算法差不多，其实它们的考虑对象是不一样的，而且通常所指的近似算法是确定型算法。近似算法多用在组合优化的问题，而不是判定性问题上。组合优化问题，指的是那些需要求最优解的问题，比如下面这个

> 旅行商问题
>
> 有n个城市，一个推销员要从其中某一个城市出发，不重复地走遍所有的城市，再回到他出发的城市。问这个推销员的最短路程。

对于这种问题，如果最短路径是1000，而且我们能很快找到一个1000.1的路径，在实际运用中，我们还需要浪费巨大的计算资源去找那个1000的路径吗？近似算法便基于此思想而来。

近似算法指在解决优化问题中，最后得到的结果能保证在一定的误差之内的算法。

从近似算法的角度来说，同为NP完全问题，它们也有不同的可近似度。在多项式时间内，有些问题可以无穷小误差的逼近，但有些问题却连常数倍数之内的结果都没法得到。

本文还有2条留言，察看留言和讨论请到http://zhiqiang.org/blog/442.html#comments

杨振宁讲坛系列讲座：Richard M. Karp

©Zhang-Zi, September 12, 2006 @ 9:21 am

昨天Karp在理学院报告厅进行了一次讲座，主题是Theory of Computation as a Lens on the Sciences: The Example of Computational Molecular Biology。

之前，Karp跟我们进行了小组讨论，回答了我们的一些问题。Karp认为，博士生的方向，有发展潜力的目前有两个。如果有足够雄心的话，可以去试图P vs NP问题——我想不太可能真有人把这个当成博士生的方向吧。另外一个方向是网络计算，一种不同于传统turing机的计算模型。

有意思的是，Yao接着Karp的话说，他认为目前有潜力的还是量子计算和量子信息这一块，无论从计算机，物理，工程上来看。我们组目前还没有做量子这个方向的学生，不知道Yao是不是觉得很郁闷。

有同学问到（在以前对Karp的一个采访报告A Day in the Life of Richard Karp中也提到），Karp的两个大学同学，后来一个拿了Nobel奖，一个拿了Fields奖，Karp觉得很有压力，于是决定不搞数学，避开他们，最后拿了Turing奖。这个事实充分说明，牛人都是一蜂窝一蜂窝的。不过Karp也提到，当时还有一个更聪明的同学，不过"not heard of him again" :).

Karp早年在NP完全问题上做了很多工作，所以我当时想问的问题是：为何你觉得P vs NP这么重要，你却转去做biology了呢？不过时间有限，最后也没问成。

本文还有**1**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/441.html#comments**

从Poincare猜想到Poincare定理——一个馒头引发的血案

©Zhang-Zi, August 25, 2006 @ 9:04 am

作者：独钓寒江雪

盛传Poincaré猜想终于被证明了，从此演变为Poincaré定理。据说Poincaré定理的伟大意义在于，如果亲爱的天文学家能够证明宇宙是单连通的、封闭的、三维的流形，那么我们就可以把宇宙想象成一个馒头。所以那些企图把宇宙当作面包圈吃掉的同学们恐怕要失望了。

当然从现实的角度来看，Poincaré的馒头倒是真正养活了一批数学家。可惜这些被称为数学家的小朋友耍起了脾气，听说有个叫Hamilton的小朋友当年提供了一个秘方，有个叫Yau的小朋友看了一眼说，哦，原来是蒸馒头用的，就是还差点。本来很有希望，结果大家蒸了好多年愣是蒸不出来。这个时候有个叫Perelman的俄国小朋友自己在家里偷偷蒸了一锅馒头，把照片给大家一看，嗬，这不就是传说中的馒头么？但是Perelman小朋友从此不来幼儿园了，这可怎么办？其他小朋友只能按照Perelman小朋友的方法接着蒸馒头，终于一蒸蒸到了2006年。蒸完馒头争馒头。Yau小朋友替Cao小朋友和Zhu小朋友出头，说这个馒头是他们最后蒸出来的，却见Tian小朋友和Morgan小朋友也没闲着，人家正在写蒸馒头手册。结果最后向日葵小班的Ball班长说，这个馒头啊，还是人家小P的，要奖励小P小红花一朵。没成想Ball班长到小P家里去的时候，人家小P说，馒头我都蒸出来了，要你这小红花干啥？

蒸馒头是苦差事，全世界会蒸的多说也就十来个人。不过这争馒头可就热闹了，大字报小字报满天飞，从不学无术到抄袭拼凑，从兼职骗钱到勾结官府，猛料迭出，估计写部《四刻拍案惊奇》早就绰绰有余了，其间众生嘴脸，直堪比镜花缘。只见那边厢Yau与无名小报《北京科技报》谈笑风生，这边厢某大便就风声鹤唳。从去年夏天不点名批评某弟子，到指责某大本科教育水平低下；从指名道姓说Tian抄袭，到炮轰某大学阀；从批评院士制度，到质疑长江教授；从蒸馒头，到争馒头，Yau终于在中文媒体和网络中掀起了一

场批判大潮，同志们！运动啦！七八周就来一次！

终于不幸的时刻在2006年8月23日降临，《纽约客》上竟然不识相地把馒头给了Perelman，而且将Yau描写成了一个争名夺利的市侩。据分析家指出，这篇文章的出现，标志着Yau-Tian-某大之间的恩怨已经进入了英文世界的主流媒体，实质上伤害了整个华人数学圈，甚至整个华人学术圈。抛开民族感情不谈，此言不谬。不论事态如何发展，不论Yau所说的抄袭、兼职和学阀等等是否属实，整个华人数学界声誉扫地恐怕都是无可改变的事实了。

然而这个世界只会缺少荒谬的事实，却永远不会缺少可笑的逻辑。因为英文媒体说了Yau坏话，所以一定是Yau的敌人捣蛋，画个圈子左右一框，那就必然是Tian通风报信了！永远站在道德制高点的网络暴民，关心的从来不是事实真相，而是任何可以表现自己卓尔不群的机会。在这个坐在屏幕背后就可以指点江山的年代，人人都是最伟大的思想家。

抄袭门、兼职门的真相如何，恐怕也不是一两天就能水落石出的。而在Yau不断的指责中，Tian迄今只说了一句话：我尊师重道。于是Yau的面对空气挥拳，终于一时失手栽入了馒头门的是非官司中，但愿在今后不太好过的岁月中，Yau能够不蒸馒头争口气……

这就是，一个馒头引发的血案。

本文还有10条留言，察看留言和讨论请到http://zhiqiang.org/blog/414.html#comments

理论计算机初步：P vs NP - 历史，现状和未来

©Zhang-Zi, August 24, 2006 @ 8:08 am

上篇文章已经提到，P vs NP是理论计算机科学的核心问题。从数学的角度来说，它和其他历史上有名的数学问题一样，给与人们一个智力上重大的挑战。而更为重要的是，在无数与计算有关的的学术领域中，NP-完全问题以各种不同形式层出不穷。因此，这并不是一个纯粹的与世独立的智力游戏，而是对计算机科学有全面影响力的问题。

历史上的进展

从上个世界70年代初这个问题被Cook提出以来，人们发展了各种工具来试图解决它，下面引自堵丁柱&葛可一的《计算复杂性导论》前言：

> 人们在七十年代开始对NP-完全问题的研究主要是横向发展，也就是以许多不同的计算模型来分析难解问题的本质。这些新的计算模型包括了平行计算模型、概率计算模型、布尔线路、判断树、平均复杂性、交互证明系统以及程式长度复杂性等等。对这些新的计算模型的研究一方面使我们对难解问题有了更深一层的认识，一方面也产生了一些预想不到的应用。最显著的一个例子就是计算密码学的革命性突破：基于NP问题的公钥密码体系。另一个有名的例子是线性规划的多项式时间解的发现。
>
> 到了八十年代中，对NP-完全问题的研究有了纵向的突破，在许多表面看来并不相关的计算模型之间发现了深刻的刻划关系。这些刻划关系不但解决了几个令人困扰多年的未解问题，同时也刺激了其它相关领域的发展。其中之一是对线路复杂性的研究发现了一些问题在某种有限制的线路模型中必有指数下界。这些结果使用了组合数学与概率方法等新的数学工具，并且解决了一个有名的有关多项式分层的未解问题。另一个更重大的结果是以概率可验证明对NP类的刻划。由此得出了许多组合优化问题近似解的NP-完全性，从而刺激了算法界对近似算法研究的新热潮。这个结果来自于对交互证明系统这个概念的扩展，并且使用了线性代数与编码理论等数

学证明技巧。

但是，明显的，目前还没有一个看上去有希望的方向。相反的，1993年Razborov和Rudich证明的一个结果表明，给定一个特定的可信的假设，在某种意义下“自然”的证明不能解决**P** vs **NP**问题。这表明一些现在似乎最有希望的方法不太可能成功。随着更多这类的定理得到证明，该定理的可能证明有越来越多的陷阱要规避。

数学里最伟大的定理之一——费马大定理，用了数学家300多年时光。P vs NP问题，作为理论计算机领域最困难的问题，40年时间似乎太短了。

不过我还是相信，这个问题被拖这么长时间，是因为没有足够伟大的数学家来做这个问题。

大牛们怎么看？

对于NP是否等于P，大家看法不一。在2002年对于100个研究者的调查中，61人相信答案是否定的，9个相信答案是肯定的，22个不确定，而8个相信该问题可能和现在所接受的公理独立，所以不可能证明或证否。同时，在被询问到这个问题可能在何时被解决时，79个人给出了确切的数字，统计结果如下：

1. P=NP will be resolved between 2002-2009: 5
2. P=NP will be resolved between 2010-2019: 12
3. P=NP will be resolved between 2020-2029: 13
4. P=NP will be resolved between 2030-2039: 10
5. P=NP will be resolved between 2040-2049: 5
6. P=NP will be resolved between 2050-2059: 12
7. P=NP will be resolved between 2060-2069: 4
8. P=NP will be resolved between 2070-2079: 0
9. P=NP will be resolved between 2080-2089: 1
10. P=NP will be resolved between 2090-2099: 0
11. P=NP will be resolved between 2100-2110: 7

12. P=NP will be resolved between 2100-2199: 0
13. P=NP will be resolved between 2200-3000: 5
14. P=NP will never be resolved : 5.

在这份调查报告中，还有国际上著名的计算机学家对这个问题的看法，比如：

> **Avi Wigderson**: (Institute of Advanced Study) I think this project is a bit premature. I think we know too little of what is relevant to even guess answers to your questions, certainly if "we" s replaced by "I"
>
> The only thing I can definitely say, is that it is one of the most important and interesting questions ever asked by humans, and more people and resources should participate in filling up the holes that would allow better guesses of answers to your questions.
>
> 姚期智: (Princeton) It's hard to say when the question will be resolved. I don't have even an educated guess. Probably the resolution is that P is not equal to NP. I think the mathematical techniques used will be beautiful.

可能的极为诡异的结果

从实际应用来说，人们都希望NP=P，因为这意味着很多问题都能有有效的算法，但有些极为诡异的结果也是可能的，人们从这个结果中什么都得不到。

比如某一天人们最终使用某种数学上的技巧证明了NP问题的多项式时间算法的存在性，但并不知道如何找到它——这在数学上是极为可能的，那最终会怎么样呢？

这种情况不会发生，事实上，在NP=P的假设下，人们已经找到了NP完全问题的多项法解法，但这并没有好太多，因为这个算法是这样的：

```
// 接受NP完全语言的一个算法。
//
```

```
// 这是一个多项式时间算法当且仅当P=NP。
//
// “多项式时间”表示它在多项式时间内返回“是”，若
// 结果是“是”，否则永远运行。
//
// 输入：S = 一个自然数的有限集
// 输出：是 如果某个S的子集加起来等于0。
// 否则，它永远运行没有输出。
// 注：上面这是一个NP完全问题
//
// 程序数P 是你将一个整数P写为二进制，然后
// 将位串考虑为一个程序。
// 每个可能的程序都可以这样产生，
// 虽然多数什么也不做因为有语法错误。

FOR N = 1...infinity
FOR P = 1...N
以S为输入运行程序数P N步
IF 程序输出一个完整的数学证明
AND 证明的每一步合法
AND 结论是S确实有（或者没有）一个和为0的子集
THEN
OUTPUT 是（或者不是）并停机
```

如果NP=P，上面这个算法便是一个NP完全问题的多项式时间算法。可是它一点价值都没有，更不用说来解决实际问题了。

另一种可能性：独立问题？

自从Godel的开创性结果以来，我们知道某些问题，比如连续统假设，是不可能从目前的条件（公理系统）推导出来的。有人怀疑P vs NP问题也是这样。这样的话，如果不存在

NP完全问题的有效算法，我们不可能证明这一点。同样，如果存在一个有效的算法，我们也不可能找到它。

花絮

中国民科一向喜欢做大问题，不知为何很少向P vs NP问题下手，但他们的外国同行可不会客气，这里就有一大帮，而且这些国外的前辈们专业多了，好多解答还提供pdf文档下载呢。

参考文献：

1. P verse NP problem
2. The history and status of P verse NP question
3. 千禧年大奖难题（一）
4. 堵丁柱, 葛可一, *计算复杂性导论*, 高等教育出版社, 2002

本文还有**14**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/413.html#comments**

理论计算机初步：P vs NP - 问题概述

©Zhang-Zi, August 23, 2006 @ 10:40 pm

P = NP?

这个问题，作为理论计算机科学的核心问题，其声名早已经超越了这个领域。它是Clay研究所的七个百万美元大奖问题之一，在2006国际数学家大会上，它是某个1小时讲座的主题。

要说起P和NP是什么东西，得先从算法的多项式时间复杂度谈起，注意，这里面的两个P都是指Polynomial。

一个问题的规模指的是输入的总位数，比如一个n个数的排序问题，输入规模就是n。注意，在某些时候，输入规模是要值得注意的，比如判定一个数n是否是一个质数这个问题，它的输入规模并不是n，而是log(n)，因为一个数n用大约log(n)位就能表示出来了，这也是为何枚举因子判定素数的算法并不是多项式时间算法的原因。

如果一个算法，它能在以输入规模为参变量的某个多项式的时间内给出答案，则称它为多项式时间算法。注意：这里的多项式时间是指算法运行的步数。一个算法是否是多项式算法，与计算模型的具体的物理实现没有关系，虽然大多数假想的计算模型不可能有任何物理的实现。

P指确定型图灵机上的具有多项式算法的问题集合，**NP**指非确定型图灵机上具有多项式算法的问题集合，这里N是Non-Deterministic的意思（图灵机的概念见理论计算机初步：算法和计算模型）。

脱离图灵机的概念，就在普通的计算机上看，P问题是指能够在多项式时间求解的判定问题（判定问题指只需要回答是和不是的问题），而NP问题则是指那些其肯定解能够在给定正确信息下在多项式时间内验证的判定问题。比如，要判定一个数是合数，如果给我一个约数，我们就很快判定它就是合数。所以判定一个数是合数的问题属于NP。 下面是一

些NP问题的例子：

零子集和问题

给n个整数，判断是否可以从中找到若干个数，其和为0。

旅行商问题

有n个城市，一个推销员要从其中某一个城市出发，不重复地走遍所有的城市，再回到他出发的城市。问这个推销员的最短路程(是否小于指定的K)。

从上面的定义知道，NP包含P。P vs NP问题指P是否完全等于NP，即确定型图灵机和非确定图灵机的性能是否一样。

人们为何要提出NP问题？因为，大多数遇到的自然的难解问题，最后都发现它们是NP问题。如果我们能证明NP跟P的关系，则解决了无数问题的算法复杂度问题。

NP里面有无数个不同的问题，我们是否要一个一个地判定它们是否属于P呢？P vs NP问题的美妙和简洁之处便在于在NP中，有一个子类，**NP**完全(NP Complete，简记为**NPC**)问题，指的是那些NP中最难的那些问题：所有其它的NP问题都可以归约到这些NP完全问题。也就是说，只要这些NP完全问题的某一个得到解决，无论是证明其存在多项式算法，还是不存在，都意味着P vs NP问题的解决。

而几乎所有NP里面无法确定是否属于P的问题最后都被证明为NP完全。正因为如此，多数理论计算机学家都猜测P≠NP。目前已知的NP完全问题数以千计，上面引用中的例子都是完全问题，更多NP完全问题见NP完全问题的不完全列表。

一个很自然的想法是如果NP≠P，则NP-P里面的问题都是完全问题。至少有两个自然的问题，一个是大数分解（给出一个数的质因数分解式），另一个是图同构问题（给出两个图，它们是否同构），它们既没有被证明是P的，也没有被证明是NP-完全。但是更惊人的是还有这个定理：

如果NP≠P，那么NP-P中存在非NP完全问题。

当然，这种问题具体是什么样子，是无法用直观的语言表示出来，它纯粹是一个数学上的构造性证明。

参阅：

- Complexity classes P and NP - Wikipedia, the free encyclopedia, P/NP问题- Wikipedia
- Turing machine - Wikipedia, the free encyclopedia, 图灵机- Wikipedia
- NP-hard - Wikipedia, the free encyclopedia,

备注：中国大陆可以通过http://browseatwork1.com 访问wikipedia.

本文还有**5**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/412.html#comments**

Fields奖得主：Okounkov, Perelman, Tao and Werner

©Zhang-Zi, August 22, 2006 @ 7:01 pm

8月22号，在Madrid举行的国际数学家大会的开幕式上，公布了此届的Fields奖得主，他们是：

美国普林斯顿大学数学家安德烈·欧克恩科夫（Andrei Okounkov）
俄罗斯数学家格里高利·佩雷尔曼（Grigori Perelman）
美国加州大学洛杉矶分校数学家陶哲轩（Terence Tao）
法国巴黎第十一大学数学家温德林·沃纳（Wendelin Werner）

奈望林纳奖获得者：

美国康奈尔大学计算机科学教授乔恩·克莱伯格（Jon Kleinberg）

高斯奖获得者：

日本数学家伊藤清（Ito Kiyoshi）

获奖者介绍可见ICM的官方文件。

在开幕式之前，科学网就公布了获奖人选，但很快新闻就被撤下，不过在baidu快照里还能看得到。按照Fields推选章程，除非获奖者本人透露，外界是不可能得知获奖人选的，而且获奖者本人也不知道其它的获奖者。所以，这次肯定在某个地方出了漏子。

另一个震惊的消息是：**Perelman**未到现场，并且已经声明拒绝领奖:

"The reasons center around his feeling of isolation from the mathematical

> community," Sir John, president of IMU, said, "and in consequence his not wanting to be a figurehead for it or wanting to represent it."

相关报道和文章：

- Highest Honor in Mathematics Is Refused
- Prestigious Award, 'Nobel' of Mathematics, Fails to Lure Reclusive Russian Problem Solver
- Perelman's Song

PS: 我这边ICM的网络直播不怎么畅通，就刚开始听了一会音乐会，后面就一直没连上去了。看来对于它的网络直播不能抱太大希望。幸好它还提供视频下载，后面的Lectures都看下载的视频好了。

本文还有**17**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/406.html#comments**

Ready for ICM 2006

©Zhang-Zi, August 21, 2006 @ 7:58 pm

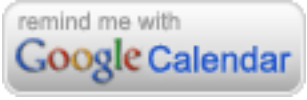
明天，2006国际数学家大会将在西班牙的Madrid正式开幕。四年一度的国际数学家大会千万不能错过，不过这种话我也只能说说而已:)。今天在其官方主页溜达了一下，发现它的1小时讲座在网络上同布播出，具体时间和题目见这里，这里还有主题摘要看。稍微看了一下，大部分都是我辈听不懂的，下面是我比较感兴趣的几个：

- Tuesday, 22 August, 17:15
  Richard Hamilton, Columbia University, New York, USA
  The Poincaré conjecture
  很可能在此讲座上宣布庞加莱猜想的解决，与咱们中国数学家也有莫大的关系（在Hamilton给的摘要中提到曹和朱）。
- Wednesday, 23 August, 10:15
  Avi Wigderson, Institute for Advanced Study, Princeton,USA
  P, NP and mathematics: a computational complexity perspective
  俺的本行，而且最近在写的系列文章他的这个报告一定得参考参考
- Thursday, 24 August, 14.00
  Special Lecture on the Poincaré Conjecture, by John Morgan
  A report on the Poincaré Conjecture
  跟田刚一个Group。也得听听
- Tuesday, 29 August, 11.45
  Ronald DeVore, University of South Carolina, Columbia, USA
  Optimal computation
  本行

以上时间都是GTM+2的本地时间，到时候直接到http://www.icm2006.org/onlineevents观看。

btw，谁能告诉我Fields奖名单的具体公布时间？

Google Calendar用户可以直接点击下面的图标添加ICM 2006日程安排:



本文还有**7**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/404.html#comments**

理论计算机初步：算法和计算模型

©Zhang-Zi, August 16, 2006 @ 9:27 am

下面是wikipedia上算法的定义：

> 算法是指完成一个任务所需要的具体步骤和方法。也就是说给定初始状态或输入数据，经过计算机程序的有限次运算，能够得出所要求或期望的终止状态或输出数据。
>
> 算法常常含有重复的步骤和一些比较或逻辑判断。如果一个算法有缺陷，或不适合于某个问题，执行这个算法将不会解决这个问题。不同的算法可能用不同的时间、空间或效率来完成同样的任务。一个算法的优劣可以用空间复杂度与时间复杂度来衡量。

一个简单而且耳熟能详的算法的例子是求最大公约数的辗转相除法：给出两个数，要求出他们俩的最大公约数。在小学的时候，我们就知道这样做就行了：将大数除以小数，用所得余数替换大数，继续用这两个数中大者除以小者，用所得余数替换较大者，继续下去，直到所得余数为0，此时除数即为所求的最大公约数。下面是一个实例：(15，21) = (15，6) = (3，6) = (3，0) = 3。又如，要判断某个数是否为质数，只需枚举所有比它小的数，检验是否其约数即可。

算法是理论计算机的灵魂。几乎所有问题都围绕它而来。为了讨论算法的性质，在理论计算机中，算法已不限于只是上面定义中的计算机程序。或者说，这里计算机的含义被大大扩广了。

我们平时所说和所使用的计算机，基于图灵提出的确定型图灵机模型。它是最好理解的：给出固定的程式，模型按照程式和输入完全确定性地运行。

但为了理解算法和这种确定型图灵机的能力，人们又发展了许多其它各式各样的图灵机模型。其中最为有名的是非确定型图灵机。这种计算模型，它在进行计算的时候，会自动选

择最优路径进行计算。通俗地说，它有预测能力。比如说，为了说明某个数是合数，非确定型图灵机会猜测一个数，恰好是其因子，从而证明了它不是质数。

确定型和非确定型图灵机的计算性能所引起的P vs NP问题，一直是理论计算机科学的核心问题，这点下面专文论述。

另一个引起广泛关注的计算机模型是量子计算机模型。与上面的非确定型图灵机只存在于人们的想象中不同，量子计算机在物理上是可以实现的。关于量子计算理论，以后也有单独的介绍性文章。

虽然上面的各种计算模型的效率可能不同，比如非确定性图灵机判定一个数是合数便要快得多，但是它们的计算能力是完全一样的。也就是在某个计算模型上面运行的算法，可以被其余模型模拟实现。

这些计算模型的计算能力是一样的，那是不是世界上所有问题都有算法呢？看上去这似乎是一个哲学问题，但答案早就有了，有些问题是不可能能通过算法求解的，连下面这个看上去很简单的问题都不行：给出一些分数（指12/23，18/9这样的），问是否可以从中选出若干个分数数（可以重复选取），使得按一定顺序排起来，其分母连起来和分子连起来恰好一样？

本文还有14条留言，察看留言和讨论请到http://zhiqiang.org/blog/390.html#comments

理论计算机初步：前言

©Zhang-Zi, August 15, 2006 @ 4:26 pm

这段时间Blog的更新频率大大降低，因为发现没啥好写的，也没有写文章的欲望。前段时间提到了我加入中国赛客联盟，而且给的说明语是"算机|数学|算法|复杂理论"，翻了一下我这个blog，觉得有些名不副实。所以决定写一些我的专业的介绍性文章，顺便充实一下本blog的内容。

我所学的专业英文名是Theoretical Computer Science，理论计算机科学，在这里我就简化成理论计算机了。具体研究些什么呢，下面是Andrew Yao的研究方向

- Analysis of Algorithms - 算法
- Computational Complexity - 计算复杂性
- Communication Complexity - 通讯复杂性
- Cryptographic Protocols - 密码
- Quantum Computing - 量子计算

这些概括了理论计算机的大部分内容。

在后面的系列文章中，我会对其中一些方面写一些具体的东西。因为我也才刚入门，而且这样的类科普性的东西，无论怎么写，在专业人士看来，总有不够严密的地方。所以，我只写一些最简单的东西，让大家都能看得懂为止，但又能对于这一领域能有一些最基本的了解。如果还能引发一些人的兴趣，更为妙哉。

顺便做一下广告：我所在的理论计算机研究小组，隶属于清华高等研究中心，目前有姚期智和王小云两位老师坐镇，其中姚期智是2000年计算机界最高奖Turing奖获得者，而王小云教授在密码学界享有盛名，另外还有大帮讲席教授，师资力量世界上都排得上号。如果有对理论计算机感兴趣的同学，这个小组将是你的不贰选择哈。目前，此小组只接受保送直博生，而且需要你在大三下学期就提出申请。欢迎加入。

本文还有**6**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/389.html#comments**

系列故事 —— 数学家和哲学家

©Zhang-Zi, August 1, 2006 @ 8:14 am
数学家系列故事，以前有一个很经典的系列：Heroes in My Heart，作者是ukim@BDWM，下面是它的前言部分：

> 给那些喜欢数学和不喜欢数学的人们
> 给那些了解数学家和不了解数学家的人们
>
> ---
>
> 在北大混了四年，一事无成；在未名上bbs也呆了快一年了，制造了几千篇的垃圾。要毕业的人想法总是奇怪的，譬如说竟然真的要正经的写几篇文章了。最初写成这些东西的时候，我发给了几个朋友，一个学数学的师弟说他很感动，一个非数学系的mm说她后悔当初没有选数学系，无论怎样，他们能这样子讲，我很感动，这是发自内心的那种。现在的打算是每天贴2-3个故事，一直到欧毕业那天。很多事情难免有些too old,这个我也没有办法，激动人心的事情毕竟只有那么多。不多说了，真心的希望大家会喜欢，哪怕只有一点点的喜欢。这些文字偶给了一个名字，叫做 我心目中的英雄 --- Heroes in My Heart
>
> --
> 美丽有两种
> 一是深刻又动人的方程
> 一是你泛着倦意淡淡的笑容

最近又有一个系列：数学捌，写一些数学家的简介和小故事。下面是引自原作者：

> 说出你所知道的，作你该做的，然后一切顺乎自然。
> —— 桑雅•卡巴列夫斯基（Sonya Kovalevsky，1850~1891）
>
> 我刚参加工作的时候，数学组开会，当时一个老师就笑言不管在什么学校数学老师的地位是最低的。因为数学难懂，大部分学生都学不好，家长们也不喜欢。

我无法认同这样的观点，在我记忆中数学老师往往是最高大的，数学的确很难，但正因为如此，陪伴身边帮助你我的数学老师才更加的重要。虽然我大学的时候不属于那种刻苦上进的学生，但是我对数学的热爱还是促使我选择数学教师作为终身的职业。在我眼里，数学是宇宙间最美丽的理论。可每每我在讲台上表达如上的情感，台下就笑翻大片。

学生不相信数学美，他们说听到“ 数学 ”两个字就头昏眼花的，他们形容它是最枯燥最无趣的学科。事实果真如此？我想说你们都错了，都误解了真实的数学。学习数学实则就像追求女孩子，好的女孩子并不是靠第一眼的感觉来判断，而要靠一生去沟通与了解。数学是一位好姑娘，相伴的时间越长，你越能感受到幸福。

这么说或者太抽象了，于是我建立网志：数学捌，讲数学与数学家的故事给你们听，就像暗火卷轴所制作的《Heros in my heart》一样，都是些有关数学的八卦故事。你们会发现其实数学、数学家跟所有有血有肉的生物一样，都是富有感情和理想的。我希望你们从这些侧面了解数学之后，可以正面的、勇敢的去挑战数学。

还有前两天看到的哲学水浒一百单八将，介绍了历史上一些有名哲学家和哲学思想，共108个。下面引自原作者的前言：

我想我还是得再次感谢一下伟大的爱尔兰哲学家巴克莱，是他的学说，从观念上消解了我原先那种与神较劲的怒气，使我得以启动介于艺术与生活之间的那种叫作喜剧的资源，为我们这个本来就是如此的生活世界，做些我力所能及的事情。

也许这种从瓦格纳向罗西尼的转变，本身就充满了啼笑皆非的因果关系，而满身兽皮总在扮酷的齐格弗里德，似乎也很不乐意屈尊到塞尔维亚的理发店里，但这都无所谓，费里尼就无所谓，在《8-1/2》里，两者相处得荒诞无间。

不知从什么时候起，哲学就成了必须把脸板起后才能有所言说的学问，似乎人类

的语言一到了哲学这地头，就得峨冠博带紫绶绯袍一番，否则，就对不起满天排列着的那一张张哲学家们的灵牌，和他们一副副搜肠刮肚的面容。——什么时候我开始写哲学恐怖小说，我就会拿以上场景当素材。

我想我们得承认，人思索的时候是不笑的，所以想再进一步地把哲学的严肃脸谱给弄花，很有可能是个相当愚蠢的念头，但我们学会了适可而止，于是我们在严肃脸谱前止步，转弯，再来到另一个地头，然后尝试怎样用打哈欠伸懒腰等各种世俗姿态，把哲学当相声一般，一个包袱又一个包袱给抖出来，如果我们恰好抖出了一百单八个包袱，那么，下面这些文字就成了。

要在维护知识正确性的同时将叙述风格进行夸张变形，这工作还真不好做，一不留神，拓扑关系就保不住了，幸好，放到网上的资源都是公共的，任何人都可以指出这其中的学理谬误，或来段更搞笑的叙述段子。——用这种类Linux的方式来升级一套系统，真的是多快好省。

要声明一下的是，水浒诨名和哲学家的配对，并非个个都能水乳交融，圆凿方枘的情况还是有的，没办法，什么中箭虎跳涧虎病花项虎插翅虎锦毛虎之类好大喜功的诨名实在太多，而鼓上蚤金毛犬这类很性格的诨名又太少，幸好，这只是玩儿，不必作了真就是。

本文还有2条留言，察看留言和讨论请到http://zhiqiang.org/blog/383.html#comments

中国赛客联盟

©Zhang-Zi, July 9, 2006 @ 3:19 pm

今天打开Google Reader，发现有一篇标题是赛克的文章引用了我的Blog地址，进去一看，原来说的是他的Blog被选入了中国赛客联盟的赛客名录，名录最后一个就是我这个Blog。

赛客就是sciblog，也就是科学博客的简称。我这里除了几篇关于庞加莱猜想的文章以及几篇转载的八卦，关于科学的文章不多。sog white曾建议我写一些有关于数学课程的直观意义和对思维的影响，不过我写作水平不高，有什么也表达不出来，另者我对于数学课程的理解也很少，现在更是丢的差不多了。所以，这个赛客的名号对我来说真是名不副实啊。不过，以后我会考虑写一些有关于计算机理论特别是算法方面的文章。

赛客名录里面有些还是比较纯粹的科学Blog，各种专业的都有，感兴趣的可以去瞧一瞧。而在我这个blog里面，跟科学有点关系的分类只有Science和Research，也许IQDoor也算？不过IQDoor这个分类我一直想把它并到别的分类里面去。目前名录正在增加中，名副其实的赛客们可以把自己添加到名录里面去。

本文还有**2**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/368.html#comments**

ICM 2006和Fields奖

©Zhang-Zi, June 27, 2006 @ 9:37 am

ICM（国际数学家大会）每四年举行一次，是数学界最重要的会议，2006 ICM将在今年八月22号到30号在西班牙的Madrid举行。每届数学家大会上最重要的莫过于宣布每次的Fields(菲尔兹)奖得主了。菲尔兹奖是数学界最具盛名的奖项，被成为数学界的诺贝尔奖，虽然几年前新颁发的Abel奖由于奖金额巨大，抢走了不少风头。菲尔兹奖4年评审一次，每次颁发给2到4位数学家，并且获奖的数学家在当年的1月1号未满40岁。

我对于数学牛人所知甚少，不过谣传此次的热门是Grigori Perelman和Terence Tao.

Perelman（佩雷尔曼）的主要工作是声称解决了庞加莱猜想。通常的说法是，Perelman至少解决了庞加莱猜想，但对于完整的Geometrization Conjecture（几何化猜想）还需要更详细的论述（中国两位数学家主要补充的也是这个东西的证明）。不过，这个成就已经足以让他取得Fields奖了。另外，还有两个问题。其中之一，Perelman是个独行侠，在2002发布惊世声明之前曾在数学界销声匿迹8年（比Wiles解决Fermat大定理还NB），传闻这次ICM给他也发了邀请函，甚至“没有收到回复”。有人担心到时Perelman到时候不来领奖，那就成了一个大笑柄了。另外一个问题是Perelman的年龄问题，Wikipedia上面的资料说他出生于1966年，今年恰好40岁，加上Perelman的第一篇论文发表于1985年（19岁？），至少这次是他最后的机会拿取Fields奖了。

Terence Tao的工作要杂一些，他证明了好些猜想，其中之一是证明了存在任意长度的等差质数序列。Tao出生于1975年，现在31岁，即使这次没评上也还有两次机会。Tao又叫陶哲轩, 其父母都是中国人，所以他算正宗的华人，只是很可惜，他“consider myself primarily an Australian”。

另外早就听说Tao是澳大利亚三届IMO-国际数学奥林匹克(86, 87, 88年)国家队成员，分别获得铜牌，银牌，金牌。可没想到Perelman也是俄罗斯的82年国家队成员，并以满分夺取金牌。算算时间，中国早几届的IMO奖牌得主也差不多30多岁了，不知有哪些人现在做的

比较好？

写到这里，突然想起为何Yau急于发布曹和朱的结果了。很显然，这次ICM很可能发布关于庞加莱猜想的结果，这次曹和朱还可以当一当配角，否则这届Perelman拿到菲尔兹奖之后，等到下届再来宣布Yau他们的结果，就没多少人感兴趣了。

本文还有**2**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/354.html#comments**

丘成桐和庞加莱猜想

©Zhang-Zi, June 21, 2006 @ 12:20 am

昨天，丘成桐在友谊宾馆举办了一个讲座，提到了庞加莱猜想证明的更多细节，听说还请到了霍金到场。今天在同一地方，曹怀东和朱熹平每人又给了1个小时的讲座。我也跟同学一起，去感受了一下气氛，不过一点都听不懂，最后还提前退场了。

根据同学对于昨天现场的描述，Yau应该是想把这次讲座办成新闻发布会的形式，现场有很多记者。显然Yau认为上次晨兴数学中心发布会还不够正式，从以往情况来看，Yau对于媒体的作用一向特别重视。比如，今天的讲座曹怀东讲完后的提问时间里，主持人就说：“欢迎提问，特别是记者朋友们”。

其实我一直就认为Yau挺小气的。以前看到他的一个讲座的PPT，讲到很多结果都是"我很是第一个想这个问题的"，"经过我的提议，某某有了重大的进展"等。翻看他昨天讲座的PPT，发现又是这种情况，连Hamilton研究Ricci流都是他建议的，以前Hamliton的办公室在Yau的隔壁。虽然我们都知道Yau您老NB，未卜先知，可是您老也不用老挂在嘴上啊。所以，我有时候也很理解田刚。

丘是一个战术家，懂得什么时候为自己造势，加上他自己的名气，所向披靡，以前的田刚事件就是如此。显然，这次丘又把自己给赌上了，因为这个结果其实没有接受多少人的检验，弄来弄去还是那么几个人看了整个证明过程，然后以最快的速度发表在一个二流的杂志上面，到现在也没听说有谁看到了证明的全文，不得不说这里面有争夺优先权的因素。

一篇报道：庞加莱猜想：华人数学家的临门一脚，我觉得这篇比大多数报道都要客观得多。

本文还有**20**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/349.html#comments**

topowu与Perelman的搞笑对话（仿鹿鼎记）

©Zhang-Zi, June 18, 2006 @ 12:02 am

转载一篇老文章。

发信人: topowu 信区: Mathematics
标　题: 在北大数学院读研(4)

前日在群与图讨论班徐老谈到自己一个弟子已博士毕业却想着出家当和尚。我听说此事之后，顿觉数学和佛学倒是有共同之处，于是模拟《鹿鼎记》中韦小宝和澄观的对话写些无聊的文字。请看：topowu与Perelman对话（Perelman号称解决三维Poincare猜想）。

topowu说道：“ 你刚才随便写写，Poincare猜想就顺利解决，这是什么功夫？ ”

Perelman道：“ 这是‘ Ricci 流 ’功夫，你不会吗？ ”

topowu道：“ 我不会。不如你教了我罢。 ”

Perelman道：“ 师叔有命，自当遵从。这‘ Ricci 流 ’功夫，也不难学，只要问题看得准，用点时间仔细算算，也就成了。 ”

topowu大喜，忙道：“ 那好极了，你快快教我。 ”心想学会了这门功夫，就随便算算，那难题便轻松搞定，那时要得Fields奖，还不容易？而“ 也不难学 ”四字，更是关键所在。天下功夫之妙，无过于此，霎时间眉花眼笑，心痒难搔。

Perelman道：“ 师叔的偏微分内功，不知练到了第几层，请你解这个椭圆方程试试。 ”topowu道：“ 怎样解法？ ”Perelman屈指一算，大吼一声，拿起粉笔就写，瞬间题目搞定。

topowu笑道：“ 那倒好玩。 ”学着他样，也是大吼一声，拿起粉笔就写，但半天也未见动静。

Perelman道：“原来师叔没练过偏微分内功，要练这门内劲，须得先练调和分析。待我跟你聊聊调和分析，看了师叔功力深浅，再传授偏微分。”topowu道：“调和分析我也不会。”Perelman道：“那也不妨，咱们来拆复分析。”topowu道：“什么复分析，可没听见过。”

Perelman脸上微有难色，道：“那么咱们试拆再浅一些的，试同调论好了。这个也不会？就从抽象代数II试起好了。也不会？那要试线性偏微分方程。是了，师叔年纪小，还没学到这路功夫，抽象代数I？微分几何？？点集拓扑？”他说一路功夫，topowu便摇一摇头。

Perelman见topowu什么科目都不会，也不生气，说道：“咱们低维拓扑武功循序渐进，入门之后先学点集拓扑，熟习之后，再学微分几何，然后学抽象代数I，内功外功有相当根柢了，可以学线性偏微分方程。如果不学线性偏微分方程，那么学现代分析基础也可以……”topowu口唇一动，便想说：“这现代分析基础我倒会。”随即忍住，知道XXX所教的这些什么现代分析基础，十条定理中只怕有九条半没说清楚，这个“会”字，无论如何说不上。只听Perelman续道：“不论学线性偏微分方程或现代分析基础，聪明勤力的，学三四年也差不多了。如果悟性高，可以跟着学复分析。学到复分析，别的大学的一般弟子，就不大能比你强了。是否能学调和分析，要看各人性子是否适合学数学。”

topowu倒抽了口凉气，说道：“你说那Ricci流并不难学，可是从点集拓扑练起，一门门科目学将下来，练成这Ricci流内功，要几年功夫？”

Perelman微笑道：“师侄从大二开始学点集拓扑，总算运气极好，能入名校学习，学得比一般人扎实，到40岁，于这内功已略窥门径。”

topowu道：“你从大二练起，到了40岁时略跪什么门闩，那么总共练了二十二年才练成？”Perelman甚是得意，道：“以二十二年而练成Ricci流内功，近一个世纪，我名列第三。”顿了一顿，又道：“不过老衲的内力修为平平，若以功力而论，恐怕排名在七十名以下。”说到这里，又不禁沮丧。

topowu心想：“管你排第三也好，第七十三也好，老子前世不修，似乎没从娘胎里带来什么武功，要花二十二年时光来练这指法，我都四五十岁老头子啦。老子还得个屁的Fields！”说道：“人家伽罗华年纪轻轻，你要练二三十年才比得过他，实在差劲之至。”

Perelman早想到了此节，一直在心下盘算，说道：“是，是！咱们武功如此给人家比了下去，实在……实在不……不大好。”

topowu道：“什么不大好，简直糟糕之极。咱们低维拓扑这一下子，可就抓不到武林中的牛耳朵，马耳朵了。你是牛校教授，不想个法子，怎对得起一个世纪来这个方向的高人？你死了以后，见到庞什么莱、布什么尔，大家责问你，说你只是吃饭拉屎，却不管事，不想法子保全低维拓扑的威名，岂不羞也羞死了？”

Perelman老脸通红，十分惶恐，连连点头，道：“师叔指点得是，待师侄回去，翻查图书馆中的Paper，看有什么妙法，可以速成。”topowu喜道：“是啊，你倘若查不出来，咱们也不用再在数学界中混了。不如让他们搞代数的来当我们的老板。”

Perelman一怔，问道：“他们搞代数的，怎么能做我们搞低维拓扑的老板？”

topowu道：“谁教你想不出速成的法子？你自己丢脸，那也不用说了，低维拓扑从此在数学圈中没了立足之地，本方向几千名教授，都要去改拜他们搞代数的为师了。大家都说，花了几十年时光来学低维拓扑，又有什么用？人家伽罗华脑袋灵光一闪就解决几百年的难题。不如大家都搞代数去算了。”

这番言语只把Perelman听得额头汗水涔涔而下，双手不住发抖，颤声道：“是，是！那……那太丢人了。”topowu道：“可不是吗？那时候咱们也不叫低维拓扑了。”Perelman问道：“那……那叫什么？”topowu道：“不如干脆叫低维代数好啦，低维拓扑改成低维代数。只消将山门上的牌匾取下来，刮掉那个‘拓扑’字，换上一个‘代数’字，那也容易得紧。”Perelman脸如土色，忙道：“不成，不成！我……我这就去想法子。师叔，恕师侄不陪了。”合十行礼，转身便走。

topowu道：“且慢！这件事须得严守秘密。倘若有人知道了，可大大的不妥。”Perelman问道：“为什么？”topowu道：“大家信不过你，也不知你想不想得出法子。而大家都想一举成名，在现实考虑之下，都去改学代数，咱们偌大低维拓扑，岂不就此散了？”

Perelman道：“师叔指点的是。此事有关本派兴衰存亡，那是万万说不得的。”心中好生感激，心想这位师叔年纪虽小，却眼光远大，前辈师尊，果然了得，若非他灵台明澈，具卓识高见，低维拓扑不免变了低维代数，百年主流，万劫不复。

topowu见他匆匆而去，袍袖颤动，显是十分惊惧，心想：“他拚了老命去想法子，总会有些门道想出来。我这番话人人都知破绽百出，但只要他不和旁人商量，谅这他也不知我在骗他。”想起得了Fields后的荣誉，一阵心猿意马，拿起本书看了看，却发现身边没了Perelman指导，单身一人，什么也学不动，只得叹了口气，回到自己宿舍休息。

本文还有3条留言，察看留言和讨论请到http://zhiqiang.org/blog/343.html#comments

庞加莱猜想被证明？

©Zhang-Zi, June 6, 2006 @ 9:57 am

Stephen SMALE 解决4维以上广义庞加莱猜想获1966菲尔兹奖

Michael H. FREEDMAN 解决4维广义庞加莱猜想获1986菲尔兹奖

但本来的庞加莱猜想未解决。 Clay 数学所将其列为7个百万美元大奖问题之一。

“七大世纪数学难题”之一的庞加莱猜想，近日被科学家完全破解，而且是中国科学家完成“最后封顶”工作——中山大学朱熹平教授和旅美数学家、清华大学讲席教授曹怀东以一篇长达300多页的论文，给出了庞加莱猜想的完全证明。

中国科学家究竟做出了多大贡献？

丘成桐多次用“封顶”一词来形容中国科学家的作用。他反复强调，在这个过程，美国科学家和俄罗斯科学家都做出了重大贡献，尤其是美国数学家汉密尔顿。“他是我的朋友，他的贡献是开创性的。”

记者就此问题请教数学家杨乐。这位数学家说，如果按百分之百划分，那么美国数学家汉密尔顿的贡献在５０％以上，提出解决这一猜想要领的俄罗斯数学家佩雷尔曼的贡献在２５％左右。“中国科学家的贡献，包括丘成桐、朱熹平、曹怀东等，在３０％左右。”

但也有人多人认为曹和朱的贡献顶多算得上有10%。关于这一点，实在难以判定到底怎么有多少。我更感兴趣的是Clay数学所的百万美元奖金将会怎么分？

附录：下面是Dionysus写的关于庞加莱猜想的来龙去脉的一个非常精彩的报道，当然他写的时候朱熹平和曹怀东的工作还没有出来。

- 庞加莱猜想-前言

- 庞加莱猜想-问题的由来
- 庞加莱猜想-维数的玩笑
- 庞加莱猜想-与风车搏斗的人们（此篇写得最有意思，强烈推荐之）
- 庞加莱猜想-造化爱几何
- 庞加莱猜想-Free at last?
- 庞加莱猜想-附录一：拓扑的初步概念
- 庞加莱猜想-附录二：几何的基本观点
- 庞加莱猜想-附录三：低维拓扑

证明庞加莱猜想是数学史上的又一个突破。但是一个重大问题的解决，有时候很难说是好是坏，比如说庞加莱猜想被解决掉，很可能导致某个数学分支的衰落，更直接一点就是以前做这个的人就没东西可以做了。

本文还有**11**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/323.html#comments**

囚徒的困境

©Zhang-Zi, May 26, 2006 @ 12:05 am

译者：吴鹤龄
作者：（美）庞德斯通 / 吴鹤龄
副标题：冯·诺伊曼、博弈论，和原子弹之谜
isbn：7564005726
页数：358
出版社：北京理工大学出版社
装帧：平装
出版年：2005-9-1

这是一本关于博弈论及其在冷战和核军备竞赛中的作用的出色的社会历史教科书。不过我感兴趣的是博弈论本身。

博弈论中最有名的问题即本书的标题——囚徒的困境，这个问题太经典，也太常见了。此书花了很大一部分篇幅详细分析和应用这个问题。后面也给出了在多次博弈中的最优策略——一报还一报。不过呢，这些以前都在别的地方见过，倒是另外一个变种——胆小鬼博弈，让我有些新鲜感。这个博弈，就像很多蹩脚的电影一样，两个大佬都想向对方展现自己无比的勇气，所以他们决定各自开着豪华汽车对撞，那个先打方向盘的就输了（当然一般电影里面主角总能坚持到最后）。

上面胆小鬼博弈的多人游戏版本叫做志愿者的困境，可以引申出有趣的跟直观相悖的结论。这点待我有空再来整理。另外一个更有趣的问题是：

苏比克的美元拍卖：一个极为简单，非常有娱乐性和启发性的客厅游戏。

游戏中一张一美金纸币被当众拍卖，规则有两条：

1. 同任何拍卖一样，钞票归价格最高者所有，新的报价必须高于上一次报价，直

到规定时间内没有新的报价结束。
2. (不同于索斯比拍卖行的规则！)报出第二高价这也要付出他最后一次报价的款项，但什么都得不到。你当然不想成为这样的竞拍人。

这个游戏最后会演变成什么样子呢？如果是你，你会怎么做？想一想这些问题是很好的思维训练。

博弈论的优美之处在于它不但有深刻的数学背景，又有强大的现实中的应用。比如，上面这个美元拍卖问题，看上去只是一个游戏，可是在现实中不难找到类似的困境——在等公共汽车时总想再等几分钟，最后才决定放弃而招呼一辆出租车。

另，前一篇文章钱应该怎么分？中提到的财产分配问题被公认为有史记载的最早的博弈论的应用，大约在公元前500年左右。

本文还有0条留言，察看留言和讨论请到http://zhiqiang.org/blog/315.html#comments

钱应该怎么分？

©Zhang-Zi, May 24, 2006 @ 11:05 pm

今天上课的时候老师讲的，我觉得很有意思。

在犹太教法典《塔木德》里讲述了这么一个案例：一名富翁向他的三位妻子许诺他死后将给大老婆300金币，二老婆200金币，小老婆100金币。可是等他死后人们清算遗产的时候，发现这名富翁撒谎了，他只有300金币的财产，问这时候他的三名妻子各应该分多少金币？

《塔木德》给的答案是150，100，50，看上去似乎没什么惊奇的，不就是按照比例分配么？可是同时给出的另外情况，如果富翁只有200的遗产或者100的遗产，此时又该如何呢？最后答案分别是75, 75, 50和100/3, 100/3, 100/3。这就很难从直观上解释了。

不过牛人就是不一样，2005年的诺贝尔经济学奖得主罗伯特-奥曼，在他1984年的一篇文章中给出了这种分配方案的理论依据，严格证明了在“假设的模型”下，上述分配方案是最优的。严格的理论推导无法在这里推出，在这篇文章犹太法典中的三妾争产与2005年的诺贝尔经济学奖金中有对上面的特殊案例的直观解释。

上面事例也告诉我们，研究问题要多看看古籍，外国人读圣经等，咱们也可多念念《庄子》啥的，说不定就从哪段话里得到了宇宙大一统的真理呢。

本文还有**2**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/314.html#comments**

Research犹如登山

©Zhang-Zi, May 13, 2006 @ 7:52 pm

基于同Prof. Ker-I Ko的关于理论计算机研究的讨论。

在学术领域里面，有很多座高山，每个研究工作者就是希望能够早日登顶。可是，很多高山，你都只知道顶峰，你不知道它有多高，甚至找不到任何可行的路径。在理论计算机方向，P vs NP就是这样最高的一座山，无数人在此前仆后继，可是无人能得其要领。

有时候一座山，找不到路径，就去爬它旁边的山，虽然高度不及，可也比直接爬原来那座山要爬得高，这样就能从远处窥视一下山顶，期望找到一条路径。为了解决P vs NP，人们在它旁边爬了无数的高山，可离P vs NP还是太远，要想突破还是需要寻找新的路径。

做研究是阶段性的。有时候，突然发现一座新的高峰，大家都争先恐后的往上爬，形成一个热门领域，等此山爬得差不多了或者找不到往上爬的路径，此领域就慢慢沉寂了，只有几个大牛，没有学术压力的人去继续爬啊爬。可一旦发现新的可行的路径，又会吸引一大批人来做这个问题，重新成为一个热点。

做理论计算机和做数学不同。数学发展到现在，群峰耸立，每座山都已经被爬得很高了，宽度也很窄，不像山脚下，随便找条路都能往上爬。每个想做数学的人，必须得先费力的爬到已知的高度，然后在现有基础上试图能再往上爬一点。所以学数学更要求勤奋，得先苦读若干年才能做些比较大的问题。伽罗瓦这样的天才后无来者。而理论计算机领域就不一样了，现在很多山峰还没有被完全开发，随便找座山，都能往上爬一爬，当然别人对你是否感兴趣，是否愿意跟着你爬就不一定了。所以，做理论计算机方面的东西，入手比较快。碰到一个问题，完全可以直接从山脚开始爬，因为大家都爬得不够高，一条新的路径说不定更有效。所以，不提倡拿到一个问题，就先去寻找和阅读文献，而应该先自己多想想。

每一个领域，都有圈内人(指那些审稿人或者已经很有名气的教授等)，边缘人(认识一些圈内人)和圈外人(一般教授或者我们这些研究生学生)。同样质量的文章，圈内人80%的机

会被接受，边缘人能到40%，圈子外面的就只有20%的机会了。这也是有些人能在顶尖杂志灌水，而大多数人只能望文叹气的原因。所以做学术也讲究关系，学者都喜欢到处访问交流就是这个道理。而学术界也分为若干个圈子，不同圈子里的人互不往来。特别提到数学界。

对于一个研究生，进入一个领域，开始做第一个问题和发第一篇文章是最难的。一个比较好的方法是：跟着导师直接从一个问题的中途入手。

本文还有7条留言，察看留言和讨论请到http://zhiqiang.org/blog/303.html#comments

How to do research?

©Zhang-Zi, May 5, 2006 @ 7:30 pm

今天同Prof. Shao就research和phd life聊了一下，下面写一些摘要

对于每一个方向和问题和别人的工作，你应该不断追问：你为什么要做这个？这个问题有什么价值？同样，对于自己的工作，也必须能够回答这个问题。即使对于导师布置的问题，这个为什么也要弄得明明白白。因为以后是你去找工作，不是你的导师，而你的导师很可能根本不需要回答这个问题。

不要为了论文而论文。找工作的时候你的publication list长度不起作用，重要的是你能说明你的结果的重要性。不要短视，做你该做的事清。

不要被问题和别人的方法牵着鼻子走。研究一个问题的时候，应该先try to solve it alone，找出问题的难点所在，再去找相关文献，这样读起来容易把握问题的整体结构，不会陷入paper海的困挠。不提倡遇到一个问题，马上去查找和阅读相关文献。

推荐阅读: You and Your Research，中文译文见做大事，成大业。

顺便贴出以前看到过的一篇文章，是跟Andrew Yao的圆桌讨论的摘要。

> Round Table Meeting with Andrew Yao
>
> 1、与人交流脸皮厚。
>
> 2、做研究要学会自己找资料，然后与导师讨论，而不是倒是告诉你研究方向。
>
> 3、对学生的要求：
> 很聪明，要有主动性。学会发现自己的研究兴趣，主动去发掘问题，然后

去解决。

4、CS研究：
学生越早接触研究越好，要学会创新的精神。
你的研究并不重要，重要的是要有天不怕，地不怕的创新精神。
不能等读完天下所有的书才开始做研究，那时候已经晚了。
不能好高骛远。

5、对博士的期望：
一个博士生读完后，就应该具备独立工作的能力。即使把他扔到一个荒岛，他也能够自己展开研究。
不但能够解决technical的问题，而且能够开创一个领域让别人来follow。

6、研究选择
对自己的能力有个公正的衡量，然后去做稍高于自己能力的问题。

7、不断push yourself
搞研究就是要一天工作十三四个小时，不许balance！
年轻时就是要好勇斗狠，要揪着人家脑袋往墙上撞（Harry 语）

8、要知道怎样去close a work， 而不是give up it.
结束了现在的工作可能有更多有意思的task。
一个问题想了几个星期，可以停下来，过一段时间再想。

9、Decision with experience
Be brave to try!

10、最好的物理学家不是因为数学，而是因为能够推理预测出一个结果。

11、科学就是用最好的方法去解决一个问题。

12、如何评判自己：

过二十年回头看看自己的成就是不是很骄傲？

13、Accept failures! learn from error

14、不要isolate。

15、TCS是最有活力的数学分支，要建立一个conceptual framework to solve problems

TSC应该open to all areas, 与实际相结合。

本文还有**6**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/292.html#comments**

以华人数学家命名的研究成果

©Zhang-Zi, April 5, 2006 @ 7:30 pm

[据少年数学网消息]中华民族是一个具有灿烂文化和悠久历史的民族，在灿烂的文化瑰宝中数学在世界也同样具有许多耀眼的光环，我国古代算术的许多研究成果里面就早已孕育了后来西方数学才涉及的思想方法，这不仅反映了中华民族文化的博大精深，也说明了我们的民族是一个聪明智慧的民族，有不少数学人才和在世界领先的数学研究成果，我们应该引以为荣，更应该发扬和光大数学前辈的治学精神，爱好数学，学好数学，用好数学。我们希望能看到更多的华人数学家诞生！希望有更多的以华人数学家命名的研究成果载入世界数学史册，扬我中华民族之威！下面就是收集到的以华人数学家命名的研究成果。

「李氏恒等式」数学家李善兰在级数求和方面的研究成果，在国际上被命名为“ 李氏恒等式 ”。

「华氏定理」数学家华罗庚关于完整三角和的研究成果被国际数学界称为“ 华氏定理 ”；另外他与数学家王元提出多重积分近似计算的方法被国际上誉为“ 华—王方法 ”。

「苏氏锥面」数学家苏步青在仿射微分几何学方面的研究成果在国际上被命名为“ 苏氏锥面 ”。

「熊氏无穷级」数学家熊庆来关于整函数与无穷级的亚纯函数的研究成果被国际数学界誉为“ 熊氏无穷级 ”。

「陈示性类」数学家陈省身关于示性类的研究成果被国际上称为“ 陈示性类 ”。

「周氏坐标」数学家周炜良在代数几何学方面的研究成果被国际数学界称为“ 周氏坐标；另外还有以他命名的 ” 周氏定理 “ 和 ” 周氏环 “ 。

「吴氏方法」数学家吴文俊关于几何定理机器证明的方法被国际上誉为“ 吴氏方法 ”；另外还有以他命名的“ 吴氏公式 ”。

「王氏悖论」数学家王浩关于数理逻辑的一个命题被国际上定为“ 王氏悖论 ”。

「柯氏定理」数学家柯召关于卡特兰问题的研究成果被国际数学界称为“ 柯氏定理 ”；另外他与数学家孙琦在数论方面的研究成果被国际上称为“ 柯—孙猜测 ”。

「陈氏定理」数学家陈景润在哥德巴赫猜想研究中提出的命题被国际数学界誉为“ 陈氏定理 ”。

「杨—张定理」数学家杨乐和张广厚在函数论方面的研究成果被国际上称为“ 杨—张定理 ”。

「陆氏猜想」数学家陆启铿关于常曲率流形的研究成果被国际上称为“ 陆氏猜想 ”。

「夏氏不等式」数学家夏道行在泛函积分和不变测度论方面的研究成果被国际数学界称为“ 夏氏不等式 ”。

「姜氏空间」数学家姜伯驹关于尼尔森数计算的研究成果被国际上命名为“ 姜氏空间 ”；另外还有以他命名的“ 姜氏子群 ”。

「侯氏定理」数学家侯振挺关于马尔可夫过程的研究成果被国际上命名为“ 侯氏定理 ”。

「周氏猜测」数学家周海中关于梅森素数分布的研究成果被国际上命名为“ 周氏猜测 ”。

「王氏定理」数学家王戍堂关于点集拓扑学的研究成果被国际数学界誉为“ 王氏定理 ”。

「袁氏引理」数学家袁亚湘在非线性规划方面的研究成果被国际上命名为“ 袁氏引理 ”。

「景氏算子」数学家景乃桓在对称函数方面的研究成果被国际上命名为“ 景氏算子 ”。

「陈氏文法」数学家陈永川在组合数学方面的研究成果被国际上命名为“ 陈氏文法 ”。

本文还有2条留言，察看留言和讨论请到http://zhiqiang.org/blog/264.html#comments

How to be a Terrible Graduate Student

©Zhang-Zi, March 14, 2006 @ 4:00 pm

How to be a Terrible Graduate Student

gh@cs.toronto.edu (Graeme Hirst)
21 May 94 19:26:43 GMT

---

1. Come to graduate school only because it allows you to postpone your entry to the real world.
2. Assume that your advisor acts solely in their own best interests, and never in yours.
3. Assume that your advisor (being more than 34 years old) doesn't understand current research, and is not (and never was) as smart as you are.
4. Never come to a meeting with your advisor prepared with an agenda of things you want to talk about, and never take notes during the discussion. (After all, little that your advisor says matters, and anyway, if it were important you'd remember it.)
5. Never take notes when you read a paper or book, or record any of your ideas in a research diary. (After all, if it were important, you'd remember it.) Corollary: It is not necessary to keep complete bibliographic citations for anything that you read.
6. Expect your advisor to give you a thesis topic and tell you exactly how to carry out the work, step by step. Corollary: If your thesis is not going well, it's your advisor's fault, not yours.
7. Regard any ideas that your advisor gives you for your thesis as your own exclusive property, and present them to the world as if you alone thought of them.
8. Frequently cancel meetings with your advisor, giving little notice (or none at all), whenever there is the slightest excuse to do so.
9. Assume that you can write up the final thesis in a month or two.
10. Don't bother checking any of your results or proofreading anything you write; that's your advisor's job.
11. Regard your graduate education as a 9-to-5 Monday-to-Friday job.
12. Give the draft of your thesis to your advisor on a Friday, so that they can read it over the weekend and give you feedback on Monday.

Maybe I am.

本文还有**0**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/20.html#comments**

来活跃活跃大脑

©Zhang-Zi, February 23, 2006 @ 4:00 pm
多做思维游戏有助于保持和提高智商

- 大 老板上课讲的：现在有两个人，"酷毙"与"帅呆"，正在花园里一边喝着酒，一边讨论关于精灵的神话。正好有个精灵从此经过，被他们的对话吸引，精灵认为在 这个时代，还有人这样仰慕和了解他们值得鼓励，于是便决定给这两个人一点奖赏。于是，他把一笔钱放入两个信封，将信封分给"酷毙"与"帅呆"，出于喜欢恶 作剧的个性，精灵透露，这两个信封里金额不同，其中一个是另一个的两倍，但他没有说哪个多哪个少。然后精灵随着一缕轻烟消失无踪。在精灵消失后，两个人拆开信封，偷看自己拿到的那笔钱，同时心里忖度着，自己到底拿到多的那份？还是少的？" 酷毙"心想：这是笔意外之财，我拿到的数额已经很不错了，如果这是多的那份，"帅呆"就只有我的一半；不过，他也可能很走运，拿到我的两倍。再回顾整个过 程，精灵是先把钱装好，密封之后才随机发给我们，因此这是一个对等赌局，两人拿到大份的几率是一半一半。所以也许我应该跟"帅呆"谈个交易，互相交换。既 然我赢得一倍金额和损失一半金额的几率都是50%，则仍有期待净利：我的交换期望收入将是现在所有的 1/2*2+1/2*1/2=5/4倍。根据决策原则，"酷毙"认为这对他相当有利，便决定和"帅呆"交换。即使"酷毙"没有拆开信封也可以作出相同决 定，因为支票的面额并不影响整个思考逻辑。

  "帅呆"以同样的方式思考后，也认为与"酷毙"进行交易对自己较有利，于是当"酷毙"一提 出交换的建议，"帅呆 "马上欣然允诺。两人的情况完全一样，都认为自己能遵从一定的逻辑推理规范。那么，有没有可能两人同时都是对的呢？毕竟这是个零和游戏，"酷毙"赢就等于 "帅呆"输，反之亦然，既然不能双赢，就一定有人是错的。但这两人不都是经过缜密逻辑思考了吗？

  & nbsp;
- 一个类似的问题[钱包悖论]：史密斯教授和两个数学学生一起吃午饭。教授：我来告诉你们一个新游戏，把你们的钱包放在桌子上，我来数里面的钱，钱包里的钱最少的那个人可以赢掉另一个人钱包里的所有钱。

  乔：哟……，如果我的钱比吉尔的多，她就会赢掉我的钱，可是，如果她的多，我就会赢多于我的钱，所以我赢的要比输的多。因此这个游戏对我有利。吉尔：如果我的钱比乔多，他就会赢掉我的钱。可是，如果他的钱比我的多，我就可以赢，而我赢的比输的多，所以游戏对我有利。

问题：一个游戏怎么会对双方都有利呢？注意我们可以假设不但不知道对方的钱的数量，连自己的钱的数量也忘了。

- 一个老问题：你上台参加一个节目：有三个箱子，其中一个装着宝贝，主持人知道宝贝藏在哪个箱子里。让你猜宝贝藏在哪个箱子里，如果能猜中宝贝就是你的。你只好随机选了一个。然后主持人先打开了另一个箱子，里面是空着的，这时候主持人问你：现在你可以选择另一个箱子，你换不换选择？笼统而言，简单的概率知识可以算出你应该选择另外一个箱子：这将使你得到宝物的概率从1/3增加到2/3。但问题就此结束了么？仔细分析就会发现，上面的概率分析基于主持人事先知道她打开的箱子会是空的。事实上，如果主持人打开的箱子里面是空的只是一个偶然的话，你换箱子是没有任何作用的。

看了这些，脑袋糊涂了吧，这时候来做个测试是再好不过的了：http://zhiqiang.org/IQ200602.htm ，你答对了几个？

本文还有2条留言，察看留言和讨论请到http://zhiqiang.org/blog/24.html#comments

牛人故事：唐翔（zz）

©Zhang-Zi, December 18, 2005 @ 4:00 pm

唐翔是我认识的最牛的人。

这句话得好好解释一下：首先，什么叫做认识？认识当然指的是相互关系。比如说，我的老板姜伯驹和王诗宬，一个是两院院士，一个是长江学者，都曾获得过陈省身数学奖。我当然跟他们彼此认识，甚至可以说熟悉。那他们有没有唐翔牛呢？窃以为没有。又比如说，我还是见过几位当代一流数学家的：陈省身、丘成桐、Smale、Atiyah，但他们根本不知道我是何许人，所以他们不能算我认识的人。那他们有没有唐翔牛呢？我觉得不好比较。

不光是我觉得不好比较，很多人都有类似的感觉。有一次老谢(这是一个精通数学物理和数论的家伙)说："二十世纪中国最伟大的三位数学家是陈省身、华罗庚、唐翔。"

"不对！"何旭反驳道。这位几个月后将坐在MIT里研究李群的表示论的好吃懒做的不敢吃辣的重庆人意味深长地说道："应该是唐翔、陈省身、华罗庚。"

另外一个需要澄清的概念是"牛"。很多认识唐翔的人都认为，唐翔除了数学牛以外，再没什么长处了。但我这里说的"牛"是把各个方面：数学、物理、化学、语文、外语、泡mm、灌水、切星际……都加到一起。在每个领域中定义一个牛指标，然后把它们生加到一起。我将之称为"综合牛指标"。所谓某甲比某乙牛，就是说某甲的综合牛指标大于某乙的综合牛指标。容易证明，我认识的其他人的综合牛指标都是有限数，但唐翔在数学领域的牛指标是趋于+∞的，而他在别的领域的牛指标至少是非负数，所以唐翔的综合牛指标大于我认识的其他人的综合牛指标，也就是说唐翔是我认识的最牛的人。证毕。

--

对于一个学数学的人来说，认识唐翔是他的不幸。这个不幸很不幸地降临在了96级数学系除了唐翔以外的师兄师姐们身上，也降临在了97级数学系大部分同仁的身上。我的不幸始

于大二下学期。那时我们年级好多人都一窝蜂地去选大三的拓扑课，我也跟着去选，然后就认识了唐翔。唐翔身材魁梧，膀大腰圆，戴眼镜，坐前排，听讲非常认真。看不出来是一个牛人，因为通常牛人都是不大听课的，比如我的偶像Smale，据说大学期间常翘课，而且经常坐在台阶上很深沉地望着夕阳。

我们年级有一位mm也选了拓扑课，也总坐在前排，于是乎就经常向唐翔请教问题，没想到两年后这位mm会成为唐翔的gf……当然这位mm跟唐翔大概并不是在拓扑课上认识的，因为他们都担任一定职务，平时可能经常一起开会什么的。至于其中细节我并不大清楚，所以还是不说的好。但可以肯定的是，唐翔泡mm的牛指标是一个充分大的正数。

一学期转眼就过去，期末考试的时候，尤承业出题照例很简单，但对于我这种头脑不灵活的人来说做起来就很是费劲了。考完后出考场，我跟唐翔聊起试题，说有一小题没做出来。唐翔说："很简单呀，这是书上一道习题，你把……"三言两语就把做法讲清楚，顿时让我感觉一学期的拓扑课算是白上了。

那时候才发现原来唐翔是个牛人，后来又陆续听到各种有关他的传说。一个流传很广的说法称，唐翔是一个绝对的完美主义者。有一次他考泛函，一个地方可能被扣1分，于是痛苦了一下午；还有一次他考测度论，一个地方可能被扣2分，于是别扭了一整天。通常来说，如果有一次数学考试连唐翔都没有得满分，那这次考试最后的成绩一定要经过若干次开方乘10的处理。也有人说唐翔的长处是记忆力好，所以他即使政治考试分数也很高。最后算平均分的时候，唐翔的各科成绩(包括政治)平均起来超过了95分。

我以前上高中的时候，老师经常跟我们说他以前的某个学生在北大数学系期间有七门功课是满分，创了北大的纪录。到了北大后，才觉得他十有八九是在吹牛，因为七门满分不大可能是北大数学系的纪录。不过我相信唐翔的13门功课满分一定是纪录。有一次我曾很不幸地看到了唐翔的成绩单的一页，在一堆100分中很刺眼地夹杂着一个90分，仔细一看，那门课是"ProbabilityTheory"，主讲教师为"QianMinping".

其实13门专业课满分并不能说明一个人的数学有多牛，充其量只能说明他很会考试。比如说99级一个师弟现在的专业平均分是99.x，还有一个师妹的专业平均分是98.x，虽然这样高的分数我考不出来，但光凭这个也不能让我佩服。因为大一大二的基础课还比较简单，

数分高代解几等课程要拿满分也不算太困难，另外陆果的物理课又纯属是考背书，所以分数高一点儿并不奇怪。而唐翔的长处就是大一的时候还不很突出，大二起就习惯于考满分了。

另外，考试考得好跟研究作得好是两回事，这一放之四海而皆准的真理早已为无数事实所证明。像Smale从小数学成绩就不突出，上大学时系主任追着要他退学。还有JohnF. Nash，自小就被目为天才，但他参加两次普遍特别难的数学竞赛，都没进前五名，备受打击，连Harvard的offer都不敢要。到如今，谁还记得当年的前五名呢？

所以说虽然唐翔成绩好，但还不能成为让人佩服的理由。打个不太恰当的比方，就像是中国足球队友谊赛灭了无数强队，但也没人因此把你当根葱。

大二下学期末的时候，听说周民强金盆洗手，下学期的实变课改由一位年轻老师教。无庸隐讳，这位年轻老师科研虽然不错，但讲课肯定比不上有三十多年实变教学经验的强强。那会儿我正感觉前两年虚度时光，所以决心暑假待在学校，疯狂自学实变，下学期就找老师要求免修。

没日没夜地读书、做题，最后书上的习题大概还剩下不到十题没做出来，自我感觉非常之好，巨有成就感。那些没做出来的题，每道想的时间都超过了十个小时，最后不得不放弃。一日从图书馆出来时遇见了唐翔，谈起自己近日来的活动，不免吹起了牛："大概还剩不到十道题没做出来吧！"唐翔说："很不错啊！那本书上的习题，我至今还没听说有谁能全部做完的。"

我听后十分得意，顺势拿一道不会做的题，"虚心"向他请教。唐翔听后，不假思索地说道："我现在记不太清楚了。这种题就用那个什么定理，Egorov定理吧，找一个函数逼近一下就行了。"我说："Egorov定理是有条件的，得是有限测度的集合。"唐翔说："你可以取一个□□□(以下略去若干字)"

锵哉锵哉锵锵哉，一句话惊醒我梦中人！再回到图书馆一做，果然立刻就搞定了，而且用同样办法又解决了两三道题，另外以前有些我做得很麻烦的题，现在很简单就能做出来了。真是听唐翔一席话，胜读半月书啊！

后来有什么问题做不出来，要是能碰见唐翔的话，就直接问他了。不过没敢跟他一起自习，因为怕得神经衰弱。而且好象跟牛人一起自习是mm的习惯……

按lonekite的说法，96、97级不少人都养成了问唐翔问题的习惯。老谢曾跟唐翔一起上过黎曼几何，他说唐翔脑子很活，做题时很不少想法。这大概确是真的吧。一般来说，一道题如果连唐翔都做不出来，那就是真做不出来了，当然偶尔也有例外，这是后话。

--

唐翔最让人佩服的是他的刻苦。每天早上六点他就起床，到图书馆自习，晚上11点从三教回来。四年如一日，从不间断。后来图书馆的门卫都认得他了，所以他不用证件也能进去。他曾告诉flying说自己每天工作的时间是16小时。

当代数学家里最刻苦的是Erdos，每天工作19个小时，其次就得数丘成桐这样的人了，但他们年轻时平均每天工作也达不到16个小时。这样算来，唐翔之刻苦实在是让人瞠目结舌。有一次，我们年级一个到MIT的家伙突出豪言："我要是有唐翔那么刻苦，早就是博士了！"此言一出，众人均ft，然后无数臭鸡蛋烂土豆都向那人扔过去了。

flying声称唐翔到图书馆最晚的一次是他离开北大的前一天，那天早上7:20时flying看见他进入图书馆。不过我怀疑flying弄错了，因为那段时间我天天早上都在学五看见唐翔，我估计flying看见唐翔是他从学五吃完早饭后进入图书馆。

让人奇怪的是，尽管唐翔这样没日没夜地学习，但身体还那么好。中午不睡觉也照样精神奕奕，晚上头一沾枕就能入睡，然后鼾声如雷。我们这些人要是不午睡，自习或上课的时候必定犯困，看看唐翔，实在让人既羡且妒。有时跟唐翔比较起自习时间，发现差得实在太远，只好乘上一个午睡系数什么的，因为要是不午睡的话，学习效率会低得多。

唐翔在国内的时候就决定出去学非交换几何。NoncommutativeGeometry这门学科是近一二十年兴起的，发展得非常热闹，跟弦理论有密切联系。这东西到底讲什么的我也不清楚，只知道国内搞的人非常少，而Atiyah将它称为二十一世纪最有前途的两个数学分支之一。

大概算子代数在非交换几何中起到了重要的作用，正如交换代数是代数几何的基本语言一样。非交换几何领域里的头号牛人AlainConnes当初就因为算子代数方面的工作获得的Fields奖。唐翔嫌自己的算子代数水平不高，就找了一本这方面的专著来读。那可是真正的学术专著，而非一般的入门教材。书名就特别长，又是"representations"，又是"*-Algebra"，又是"locallycompactgroups"的，总之都是正常人没法学懂的东西。

其实如果光是题目吓人倒也没什么，看看那本书吧：共两卷，加起来一千四百八十余页。这个数字是什么概念呢？G.W.Whitehead写过一本臭名昭著的"ElementsofHomotopyTheory"，厚七百四十多页，重一公斤。这书已经被圈内人士认为过于厚重，不适合当教材，只能作为工具书查一查。而唐翔看的那书，每一卷的厚度都和Whitehead的书相当！

据说唐翔把那本两卷的书分成了四个部分，每两个月看一部分，用了将近一年的时间全部看完。老谢说，每当他在图书馆看见唐翔啃那本书时，他就流汗。

现在的人过于浮躁，一个个都恨不得两年就把本科课程学完，再用一年就写出博士论文，很少有人肯下苦功夫练一练基本功的。谁还会花上一年的时间，啃一本一千四百八十多页的书呢？

唐翔深受钱敏的赏识，后者把唐推荐给了丘成桐。据说发offer的那段日子，丘成桐不在学校，所以唐翔只被列入了Harvard的waitinglist，尽管是第一位。后来唐翔waiting不下去了，就去了Berkeley，然后Harvard的offer就来了……

个人认为，丘成桐没有招到唐翔，是丘的不幸而非唐翔的不幸。唐翔和丘成桐其实有很多相似之处：两人都有做数学的硬功夫，天资都不能算是太高，但都以刻苦而闻名。不同的是唐翔比丘成桐更刻苦，但丘比唐更有名，至少现在是这样。

顺带说一下，在Fields奖得主中，丘成桐的天资不算高，但刻苦程度绝对没几个人能比得上他。有人曾请陈省身评论几位当代数学家，问到某人时，陈说："他很用功。"问到另外一人时，陈也说："他很用功。"但问到丘成桐时陈不说话了，因为丘成桐的用功是出了名的。据说丘吃饭的时候也要想数学问题，想着想着连饭都吐出来了。丘如今五十多岁，早

已功成名就，但每天仍工作八小时以上，系里所有的数学会议都参加。另外他对自己的学生也极严格，要求每四天读一篇高质量的论文。可以想象，要是丘成桐得到了像唐翔这样刻苦的学生，一定会喜极而泣。

唐翔到了Berkeley，导师是Weinstein，——也是陈省身的学生和钱敏的朋友。Weinstein是搞Poisson几何的，对非交换几何估计肯定不懂，所以在那里是他教唐翔Poisson几何，而唐翔教他非交换几何。自然唐翔的非交换几何是自学的，以他的算子代数功底和刻苦程度，要自学这种东西肯定是小菜一碟。

唐翔写信回来说，在Berkeley几乎人人看过的书都比他多。那是自然，想来也没有谁会花一年的时间看一本一千多页的书。有那一年的时间，牛人们肯定至少看完了几十本书了。不过一年看几十本书的只是小牛，唐翔才是真的大牛。

(完)

本文还有4条留言，察看留言和讨论请到http://zhiqiang.org/blog/52.html#comments

一个小游戏 --- 直觉和理论的悖论？

©Zhang-Zi, November 11, 2005 @ 4:00 pm

一个游戏：持续的抛一个均匀硬币，直到抛到出现反面为止，假设在之前你抛除了k次正面，你将得到2的k+1次方这么多钱。

问题：你愿意花多少钱来玩这个游戏？

直觉上而言，一个人不可能愿意花1000块钱来玩这个游戏。但从概率上分析，将有1/2^(k+1)的概率得到2^(k+1)的钱，也就是你每次得到的钱的期望是无穷大(k=0,1,2,...有无穷大取值)。也就是说从数学上而言，你值得为这个游戏花上任意多的本钱，比如说1000块钱。

两点可能的原因：

- 金钱的效应原因：在钱多到一定数量的时候，钱数本身已经失去了意义，比如说赢了2^100和2^101的钱对于个人而言产生的效应是一样的，但是在期望计算中，后者的分量还是前者的两倍。比如说人能够承受的钱的最高数量是2^40(已经世界首富了)，也就是说此时游戏的实际期望只有42块钱，也就是说这个游戏只值得用42块钱来玩。
- 无穷现金的庄家：在这个游戏里面，假设了庄家有足够的现金。是不是也就意味着你有足够乃至无穷的现金，才能跟庄家对抗？

以上两点是我想到的可能原因，也许不一定对，希望有兴趣的朋友继续讨论。

本文还有**2**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/78.html#comments**

学数甘苦谈（zz）

©Zhang-Zi, August 17, 2005 @ 4:00 pm

http://www.rainbowplan.org/bbs/topic.php?topic=1189&select=&forum=1

送交者: 元江 于 2005-08-18 12:50:29

送交者: 摘星子 2005年8月17日19:10:05 于 [教育与学术]http://www.bbsland.com

学数甘苦谈

摘星子

俺懂的这点数学,都是俺师傅教的.俺师傅是谁?你大哥这辈子只有一个师傅,所以一说师傅,只能是他老人家. 就象一说主席,只能是指毛主席,一说总理,只能是指周总理一样.所谓生我者父母,教我者师傅也.

没错,最近师傅又和俺的田师弟掐起来了,嘿嘿,这几年田师弟也是猖了些.不过这事得怪张恭庆.谁都知道, 田师弟是个孝顺孩子,和蒙师感情深.丫张恭庆就不能劝劝田师弟,到师傅面前陪个理道个歉,实在不行就下个跪哭一场?师傅他老人家嘴头上硬,其实心肠最软,这样不就什么都了结了?这个老不死的,七十多了还没过去更年期,仗着是北大的,硬是不低头.田师弟夹在中间,左右不是人,有苦说不出.到了今天这烂样子,全是丫张恭庆一手制造的.

不过师傅这回也是气糊涂了,颠来倒去说什么几年前就发现Ricci流大有前途,而张恭庆等人抗旨不遵, 误了国家前途. 师傅说过Ricci流大有前途是不假,可他老人家忘了,他同时还说过其它几十个方向,东南西北都说遍了, 全是大有前途.做出来是我老人家高瞻远嘱,做不出来是你们自个傻逼.哈哈,这才叫领袖风度.那天和一个华尔街的哥们打电话,这老哥笑着说,这是我们华尔街的做事风格嘛,我们向客户推荐股票都这么干, 怎么也传到你们学术界去了?丫那里知道,师傅下海做生意也不是一年两年了.

老萧掐田师弟是好多年前的事了,那时候田师弟还是个毛头孩子,老萧跟丫过不去干什么?谁都知道,这是冲着俺师傅去的,师傅能不跟丫翻脸么?嘿嘿,三十年河东,三十年河西,毛主席说过么,矛盾是在运动中变化的,现在是轮到师傅和老萧联手了.

不过自古以来,师傅说徒弟剽窃是天经地义,要是徒弟说师傅剽窃,那就是大逆不道了.哥大马生明的事听说过么?马生明的博士题目快做完的时候,丫老板对他说,这题目你不用做了,我给你换个题目做. 马越想越不对劲,跑出去一打听,才知道丫老板已经把他做的拿出去发表了.可惜呀可惜,马生明这个土鳖,头脑僵化分不清敌我形势,仗着自个是北大出身,要硬碰硬,四处写信告状.师傅还收到过丫的信,看完之后师傅二话不说扔进废纸篓.结果怎么样,以卵击石,自然不得好死.马当场就被哥大开了,直到现在还在街头打工.

闲话说了那么多,现在该给你们讲讲你大哥学数学的经验了.咳,这东西说起来也简单,该你顺的时候, 就会顺得不得了,不该你顺的时候,你丫就是使出吃奶的劲也没用,除非丫是天才.任何一个领域,刚开始的时候,可做的问题多得不得了,任何一个鸟人都能出好多文章.等过了几年,可做的都做光了, 只剩下一堆不可做的,这领域就做死了,那时候要出一篇象样点的文章,比登天还难.八十年代初,Ricci流这块刚刚开张,你大哥博士论文就做的这个,呵呵,乘着东风,也风光了好几年.可惜好景不长,这东西很快就做死了,剩下的问题谁也搞不动.你大哥也跟着倒运,哪也待不住,最后漂到德州农大去了.

那时候你大哥的心情可是糟透了.回国去都觉得抬不起头来.别人问您在哪工作,俺说是德州农大的, 就跟说是在咱们吉林农专一样.瞧别人那目光,俺都觉得身上有股牲口味,恨不得找个地洞钻进去. 你大哥是做梦都想跳出农大啊.可惜不管费多大的劲,就是写不出好文章来.

过了两年周铁找不到工作,也漂到农大来了.丫见我这样,跑过来说,星哥,跟我一块干吧,我这块好出文章.俺想闲着也是闲着,就干干吧.嘿嘿,丫这块文章是好出,一搞就是十几篇.拿去给别人一看,别人都是哈哈哈一阵大笑就没了下文.俺越想越不对,回过头再看俺那十几篇文章,就觉得什么都不是,全是一堆狗屎.俺是被周铁这小子给坑了.当时你大哥是两眼一黑,心想这辈子是在农大死定了.

不过周铁也没好结果,他连农大都待不下去了,只好去投奔俺田师弟.田师弟正被逼着往国

内推荐人呢，顺手一套组合拳把丫打回了国内.后来丫又跟着俺那刘师弟算了一通积分,又打又闹,哭哭笑笑,出了名了.咳,丫也算是熬出头了.

周铁能时来运转,你大哥也不能落后不是.正当俺心如死灰呢,天上掉下来这个西伯利亚的老毛子,扬言解决了Ricci流里的所有问题,而且只给了大概,没有细节.妙就妙在这儿,丫要是说全了,俺除了鼓鼓掌,还能干什么?这么一来,整个领域全活了,大会小会不断.这种机会你大哥能错过么?呵呵,乘着春风俺也是东奔西跑,开会做报告.这两年,俺是又象回到了二十多岁,青春焕发了.

连师傅他老人家也想起俺来了,一天把俺叫到跟前说,星子,这些年为师没好好照顾你,让你流到了农大那么多年,整日与牲口为伍,受了不少委曲,为师的很对不住你.这些年来为师为了坚持真理,很得罪了一些人,很多杂志的编辑都越来越不听话了.唯有这微分几何杂志,是咱们的老根据地,怎么也不能丢啊.现在为师把它交给你,你可要好好给我看住了.

俺的眼泪当场就下来了.师傅他老人家把这千钧重担交给俺,是知道俺老实,勤快,立场坚定啊.俺能不肝脑涂地么?你们看俺每天兢兢业业,刻苦攻关,为了什么?就是为了俺师傅!士为知己者死!俺这下半辈子，就跟着师傅战斗下去了.

本文还有0条留言，察看留言和讨论请到http://zhiqiang.org/blog/110.html#comments

费尔马大定理阅读手记（zz）

©Zhang-Zi, August 17, 2005 @ 4:00 pm

发信人: bmn (mn), 信区: reading
标　题: 费尔马大定理阅读手记
发信站: 一见如故 (Tue Aug 16 12:53:08 2005), 本站(yjrg.net)

（一）

从昨天夜里开始，除了实在支持不住而睡去外，我置各种迫在眉睫的任务于不顾，一直在看《费马大定理》。

关于这本书，一定要好好说说。

几年前，缪哲对我说，有本书叫《费尔玛大定理》，好看，实在好看。

老缪是做学问的人，喜欢向我兜售他看过的英文原版书，那未尝不是一种得意，但这种得意对我来说，则有许多难堪，因为他说过的书，大多不可能翻译出版，而这么偏门的海市蜃楼都能让他把持着，也更增其得意。我的英语水平，是永远不可能读原版的，双重压迫之下，对"老缪的书"基本抱持可有可无的空灵态度。

但说来奇怪，书与人之间也是有某种缘分的。老缪向我推荐过的书不少，大多被我边应承边从记忆中抹去，却留下了《费尔玛大定理》这一本。

从那天起，我就利用本来就为数不多的进书店的机会，一直寻找这本书的中译本。几年下来，遍寻不着，看来这样的书是不会被国内出版商看中了，但我并不绝望，这根弦不时绷紧一两次，撩拨一下我已经所剩无及的阅读欲望。

几个月前，在一次集会中见到黄集伟老师，我问他，《费尔玛大定理》出过吗？

我给你找一本。黄老师用确定的口吻说。

现在想起来，黄老师是将信息优势转化为了心理优势。他那时大概已经知道该书即将被上海译文出版社推出的消息，于是昭显了一次他双馨的德艺。天可怜见，我兴奋不已，已经开始憧憬黄老师将一本发黄磨损的老书递过来时，我应该咂多少下嘴巴了。

几天前，在黄老师的博客上看到他参加天津书市后开列的书单，里面赫然有一本《费马大定理——一个困惑了世间智者358年的谜》。原来是一本新书，那就不用劳黄老师之手了。

我上得当当网，找到这本书，迅速填好购书单。

昨天，2005年6月4日，当当的送货员按响了我家的门铃。

拆开包装，这本定价33元、不到300页厚的书呈现在我的面前。每次初见一个美女，我都要一脸媚态地说一句"我在梦中见过你的"，没有任何人当真。但这次——书与人之间真的是有一种缘分的——《费马大定理》的封面，让我恍惚间确有一种似曾相识的感觉，却记不起在哪里见过。

从昨天夜里到现在，除了睡觉，我就全是在捧读这本书。

刚刚从梦中醒来，见窗外下起了应该在昨天下的雨，我吐出一口气，再度打开这本书。

（二）

"那完全就是一部惊险小说。"

当年缪哲这样评价这本书。

不是这本书像一本惊险小说，而是费马大定理本身从提出到证明的过程，就是一部不折不扣的惊险小说——

一个读者，在自己读过的书的空白处留下附注。除了他自己之外，还有谁会关注呢？

但是，法国人费马死后，他在一本《算术》书上所写的注记并没有随之湮没。其长子意识到那些草草的字迹也许有其价值，就用五年时间整理，然后印出一个特殊的《算术》版本，载有他父亲所做的边注，那里面包含了一系列的定理。

在靠近问题8的页边处，费马写着这么几句话：

"不可能将一个立方数写成两个立方数之和；或者将一个4次幂写成两个4次幂之和；或者，总的来说，不可能将一个高于2次的幂写成两个同样次幂的和。"

这个喜欢恶作剧的天才，又在后面写下一个附加的评注：

"我有一个对这个命题的十分美妙的证明，这里空白太小，写不下。"

费马写下这几行字大约是在1637年，这些被侥幸发现的蛛丝马迹成了其后所有数学家的不幸。一个高中生就可以理解的定理，成了数学界最大的悬案，从此将那些世界上最聪明的头脑整整折磨了358年。一代又一代的数学天才前赴后继，向这一猜想发起挑战。

欧拉，18世纪最伟大的数学家之一，在那本特殊版本的《算术》中别的地方，发现费马隐蔽地描述了对4次幂的一个证明。欧拉将这个含糊不清的证明从细节上加以完善，并证明了3次幂的无解。但在他的突破之后，仍然有无数多次幂需要证明。

等到索非?热尔曼、勒让德、狄利克雷、加布里尔?拉梅等几个法国人再次取得突破时，距离费马写下那个定理已经过去了将近200年，而他们才仅仅又证明了5次幂和7次幂。

事实上拉梅已经宣布他差不多就要证明费马大定理了，另一位数学家柯西也紧随其后说，要发表一个完整的证明。然而，一封来信粉碎了他们的信心：德国数学家库默尔看出这两个法国人正在走向同一条逻辑的死胡同。

在让两位数学家感到羞耻的同时，库默尔也证明了费马大定理的完整证明是当时的数学方法不可能实现的。这是数学逻辑的光辉一页，也是对整整一代数学家的巨大打击。

20世纪，数学开始转向各种不同的研究领域并取得非凡进步。1908年，德国实业家沃尔夫斯凯尔为未来可能攻克费马大定理的人设立了奖金，但是，一位不出名的数学家却似乎毁灭了大家的希望：库特?哥德尔提出不可判定性定理，对费马大定理进行了残酷的表达－－这个命题没有任何证明。

尽管有哥德尔致命的警告，尽管经受了三个世纪壮烈的失败，但一些数学家仍然冒着白白浪费生命的风险，继续投身于这个问题。二战后随着计算机的出现，大量的计算已不再成为问题。借助计算机的帮助，数学家们对500以内，然后在1000以内，再是10000以内的值证明了费马大定理，到80年代，这个范围提高到25000，然后是400万以内。

但是，这种成功仅仅是表面的，即使那个范围再提高，也永远不能证明到无穷，不能宣称证明了整个定理。破案似乎遥遥无期。

最后的英雄已经出现。1963年，年仅十岁的安德鲁?怀尔斯在一本名叫《大问题》的书中邂逅费马大定理，便知道自己永远不会放弃它，必须解决它。70年代，他正在剑桥大学研究椭圆方程，看来与费马大定理没什么关系。

此时，两位日本数学家已经提出谷山－志村猜想，将怀尔斯正在研究的椭圆方程与模形式统一在一起。看来也与费马大定理没什么关系。

80年代，几位数学家将17世纪最重要的问题与20世纪最有意义的问题结合在一起，找出了证明费马大定理的钥匙：只要能证明谷山－志村猜想，就自动证明了费马大定理。

曙光在前，但并没有人对黎明的到来抱有信心，谷山－志村猜想已经被研究了30年，都以失败告终，如今与费马大定理联系在一起，更是连最后的希望都没有了，因为，任何可能导致解决费马大定理的事情根据定义是根本不可能实现的－－这几乎已成定论。

就连发现钥匙的关键人物肯?里贝特也很悲观："我没有真的费神去试图证明它，甚至

没有想到过要去试一下。"大多数其他数学家，包括安德鲁?怀尔斯的导师，都相信做这个证明会劳而无功。

除了安德鲁?怀尔斯。

曾经有人问伟大的逻辑学家大卫?希尔伯特为什么不去尝试证明费马大定理，他回答说："我没有那么多时间去浪费在一件可能会失败的事情上。"

但安德鲁?怀尔斯会。他意识到自己的机会不大，但即使最终没能证明费马大定理，他也觉得自己的努力不会白费。他花了18个月的时间为将来的战斗收集必要的武器，然后得出全面估计：任何对这个证明的认真尝试，很可能需要10年的专心致志的努力。

怀尔斯放弃了所有与证明费马大定理无直接关系的工作，在完全保密的状态下，展开了一个人对一个困扰世间智者三百多年的谜团的挑战，妻子是唯一知道他在从事费马问题研究的人。

1993年，经过七年专心努力的安德鲁?怀尔斯完成了谷山－志村猜想的证明。6月23日，剑桥牛顿研究所，他开始了本世纪最重要的一次数学讲座，每一个对促成费马大定理证明做出过贡献的人实际上都在现场的房间里，两百名数学家被惊呆了，他们看到的是，三百多年来第一次，费马的挑战被征服。

怀尔斯写上费马大定理的结论，然后转向听众，平和地说："我想我就在这里结束。"会场上爆发出一阵持久的掌声，第二天，数学家第一次占据了报纸的头版头条。《人物》杂志将他与黛安娜王妃、奥普拉一起列为"本年度25位最具魅力者"之一，一家时装公司则请这位温文尔雅的天才为他们的新系列男装做了广告。

但事情并没有在这里结束，接下来的发展依然像惊险小说一样，悬案得破，但案犯并不轻易束手就擒。怀尔斯长达200页的手稿投交到《数学发明》杂志，开始了庞杂的审稿过程。这是一个特大型的论证，由数以百计的数学计算通过数以千计的逻辑链环错综复杂地构造而成。只要有一个计算出差错或一个链环没衔接好，整个证明将可能失去其价值。

在苛刻的审稿过程中，审稿人碰到了一个似乎是小问题的问题。而这个问题的实质是，无法使怀尔斯像原来设想的那样保证某个方法行得通。他必须加强他的证明。

时间越耗越长，问题依然解决不了，全世界开始对怀尔斯产生怀疑。14个月的时间过去了，他准备公开承认失败并发表一个证明有缺陷的声明。

在山穷水尽的最后时刻，9月19日，一个星期一的早晨，他决定最后检视一次，试图确切地判断出那个方法不能奏效的原因。一个突然迸发的灵感使他的苦难走到了尽头：虽然那个方法不能完全行得通，但只需要可以使另一个他曾经放弃的理论奏效，正确答案就可以出现在废墟之中——两个分别不足以解决问题的方法结合在一起，就可以完美地互相补足。

足足有20分钟，怀尔斯呆望着那个结果不敢相信，然后，是一种再也无事可做的巨大失落感。

一百年前，专为费马大定理而设的沃尔夫斯凯尔奖将截止日期定为2007年9月13日。就像所有的惊险片一样，炸弹在起爆的最后一刻，被拆除了。

（三）

《费马大定理》既是一部惊险小说，也是一部武侠小说，激荡着绝顶高手传诵千古的传奇故事。

那个数学世界里的江湖是属于年轻人的。少年英雄在这里尽情挥洒他们的天纵其才，库特?哥德尔提出他的不可判定性定理时，年仅25岁；挪威的阿贝尔在19岁时做出了他对数学的最伟大的贡献，8年后在贫困交加中去世，法国数学家埃米尔特评价"他留下的思想可供数学家们工作500年"；相较而言，安德鲁?怀尔斯40岁开始研究费马大定理，别人认为他应该是才思枯竭的岁数了。

"年轻人应该证明定理，而老年人则应该写书。"英国数学家哈代说，"数学较之别的艺术或科学，更是年轻人的游戏。"还有哪片领土更适合年轻人来谱写传奇？在英国皇家学会会员中，数学家的平均当选年龄是最低的。

围绕着费马大定理发生的故事，更是超出了最优秀编剧的想像。寻求费马大定理的证明牵动了这个星球上最有才智的人们，巨额的赏格，自杀性的绝望，黎明前的决斗。

1954年1月，东京大学的年轻数学家志村五郎去系图书馆借一本书，令他吃惊的是，那本书被一个叫谷山丰的人借走了。志村给这位并不熟悉的校友写了封信，几天后，他收到对方的明信片，谷山告诉他，他是在进行同一个计算，并在同一处被卡住了。

一种惊喜的默契顿时产生，两人开始了惺惺相惜的合作。"他天生就有一种犯许多错误，尤其是朝正确的方向犯错误的特殊本领。"志村评价他的拍档。1958年11月17日，这个心不在焉的天才人物、刚刚订婚的谷山选择了自杀。几个星期后，他的未婚妻也结束了自己的生命，遗书中写道："既然他去了，我也必须和他在一起。"

谷山在遗书中为他的自杀行为引起的种种麻烦向他的同事们表示歉意，而他遗留下的对数学的许多根本性想法，成为解开费马大定理的唯一一把钥匙：谷山－志村猜想。30年后，他的伙伴志村目睹了他们的猜想被证实，用克制和自尊的平静对记者说："我对你们说过这是对的。"　　他依然保存着谷山第一次寄给他的那张明信片。

德国实业家沃尔夫斯凯尔并不是一个有天赋的数学家，但一桩最不可思议的事件将他与费马大定理永远联系在一起。

对一位漂亮女性的迷恋及被拒绝，令沃尔夫斯凯尔备感绝望。他决定自杀，并定下了自杀的日子，准备在午夜钟声响起时开枪射击自己的头部。沃尔夫斯凯尔认真地做着每一个细节：处理好商业事务、写下遗嘱，并给所有的亲朋好友写了信。

他的高效率使得所有的事情略早于午夜的时限就办完了。为了消磨最后的几个小时，他到图书室翻阅数学书籍：一篇关于费马大定理证明的论文……他不知不觉拿起了笔，一行一行进行计算……

然后，天亮了。

沃尔夫斯凯尔为自己发现并改正了论文中的一个漏洞感到无比骄傲，原来的绝望和悲

伤消失了，数学将他从死神身边唤回。

1908年，得享天年的沃尔夫斯凯尔写下了他新的遗嘱：他财产中的一大部分作为一个奖，规定奖给任何能证明费马大定理的人，奖金是10万马克，按现在的币值超过100万英镑。

这是他对那个挽救过其生命的盖世难题的报恩方式。

1832年，法国数学家伽罗瓦陷入一桩风流韵事中。与他相好的一个女人事实上已经订婚，那名绅士发现了未婚妻的不忠，非常愤怒地向伽罗瓦提出决斗。

对方是法国一名最好的枪手，而伽罗瓦非常清楚自己的实力：遑论开枪，就连数学演算他都是只在头脑里进行，而不屑于在纸上把论证写清楚，为此他的许多数学成果都得不到法国科学院的重视与承认。决斗的前一晚，他相信这是自己的最后一晚，也是把他的思想写在纸上的最后机会。

他通宵达旦，写出了存在自己头脑里的所有定理，在复杂的代数式中，那个女人的名字不时隐藏其间，还有绝望的感叹——"我没有时间了，我没有时间了！"

第二天，1832年5月30日，伽罗瓦死于决斗。

等他潦草的手稿被递至欧洲一些接触的数学家手里，那些演算中迸发出的天才思想使专家们发现：一位世界上最杰出的数学家在他20岁时被杀死了，他研究数学只有5年。

伽罗瓦在手稿中对五次方程的解法进行了完整透彻的叙述，而他演算的核心部分则是称为"群论"的思想，他将这种思想发展成一种能攻克以前无法解决的问题的有力工具。

伽罗瓦生命中最后一夜的工作，一个半世纪后成为安德鲁?怀尔斯证明谷山－志村猜想的基础。

1997年6月27日，符合沃尔夫斯凯尔委员会的规定战胜费马挑战的安德鲁?怀尔斯收到了价值5万美元的沃尔夫斯凯尔奖金。

是的，费马大定理被正式解决了。怀尔斯汇集了20世纪数论中所有的突破性工作，并把它们融合成一个万能的证明。

人们又重新掂量起费马写下的那一行附加评注："我有一个对这个命题的十分美妙的证明，这里空白太小，写不下。"可以确定的是，几个世纪以前，费马没有发明出安德鲁?怀尔斯证明大定理所用的模形式、谷山－志村猜想、伽罗瓦群论和科利瓦金－弗莱切方法。

那么，费马本人是用什么方法证明他所提出的猜想的呢？只是一个有缺陷的证明，还是他以17世纪的技巧为基础，涉及到的却是其后几百年所有数学家都没有发现的另一种方法？我们永远也没机会知道了。

"那段特殊的漫长的探索现在结束了，我的心灵归于平静。"安德鲁?怀尔斯说。

传奇似乎已经落幕，而事实上更大的传奇却被永远隐藏在358年以前。

（四）

公元前212年，罗马军队入侵叙拉古，将近80岁的阿基米德正在全神贯注地研究沙堆中的一个几何图形，疏忽了回答一个罗马士兵的问话，结果被长矛戳死。

18世纪的巴黎女孩索非?热尔曼在一本叫《数学的历史》的书中看到这一章，便得出这样的结论：如果一个人会如此痴迷于一个导致他死亡的几何问题，那么数学必定是世界上最迷人的学科了。

她马上对这最迷人的学科着了迷，经常工作到深夜，研究欧拉和牛顿的著作。父母没收了她的蜡烛和衣服，搬走所有可以取暖的东西，以阻止她继续学习。她用偷藏的蜡烛并用床单包裹着自己继续学习，即使墨水已经在墨瓶中冻僵。最后她的父母妥协。

在那个充满偏见和大男子主义的时代，她冒名"勒布朗先生"，通过书信在只接受男性

的巴黎综合工科学院学院学习，并以这个身份与"数学家之王"高斯通信探讨费马大定理。1806年，拿破仑入侵普鲁士，热尔曼拜托一位法国将军保证高斯的安全。得到特殊照顾的高斯这才知道她的真实身份，否则，她对费马大定理的杰出贡献恐怕就被永远记在那个"勒布朗先生"的头上了。

高斯在致谢信中谈到数学的魔力："还没有任何东西能以如此令人喜欢和毫不含糊的方式向我证明，这门为我的生活增添了无比欢乐的科学所具有的吸引力决不是虚构的。"

他的表述太过冗长了。还是让热尔曼的同类来回答这个问题吧——当有人问公元4世纪时的女性数学家希帕蒂娅为什么一直不结婚时，她说，她已经和真理结了婚。

就像两千年间涌现出的大多数女数学家一样，索非?热尔曼终生未婚。

凡物皆数，这就是数学的魔力。

数字会奇妙地出现在各种各样的自然现象中。综观世界上所有曲曲弯弯的河流，剑桥大学的地球科学家汉斯?亨利克发现，从河源头到河入海口之间，实际长度与直线距离之比，基本接近于圆周率的值。爱因斯坦提出，这个数字的出现是有序与紊乱相争的结果。

事实上早在公元前6世纪，毕达哥拉斯就发现了数与自然之间的关系。他认识到自然现象是由规律支配的，这些规律可以用数学方程来描述。比如，他在铁匠铺里发现了音乐和声与数的调和之间的关系：那些彼此间音调和谐的锤子有一种简单的数学关系，它们的质量彼此之间成简单比，或者说简分数，像二分之一、三分之一、四分之一。

在昆虫中，蝉的生命周期是最长的，17年。这个素数年数有没有特殊的意义？按照生物学家的解释，这个为素数的生命周期保护了它。只有两种寄生物可以威胁到它：1年期或17年期。而寄生物不可能活着接连出现17年，因为在前16次出现时没有蝉供它们寄生。于是，生命周期为素数有着某种进化论意义上的优势。事实也证明了这一点：蝉的寄生物从未被发现。

数字本身的神秘，更是扣人心弦。完满数意即一个数的因数之和恰好等于其本身的数，比如6的因数为1、2、3，后者相加正好是6，所以是完满数。这个概念已经提出将近

三千年了，而数学家们发现的完满数才30个，而可爱的老6，就是最小的那个。圣奥古斯丁说："6是一个数，因其自身而完满，并非因上帝在6天中创造了万物；倒过来说才是真实的：上帝在6天中创造万物是因为这个数是完满的。"

再比如26，费马注意到它被夹在一个平方数（25是5的平方）和一个立方数（27是3的立方）之间。他寻求其他这样的数都没有成功，那么26是不是唯一的？迄今没有人能够拿出证明。

说一不二，是数学的另一个魔力。

在数学王国，不存在公说公有理，婆说婆有理，不存在正方反方的辩论赛，参赛者抓阄决定自己的立场，最后获胜的居然是口才好的人。

在数学词典中，数学证明是一个有力而严格的概念，它高于物理学家或化学学家所理解的科学证明。科学证明靠的是观察和理解力，按照评判系统来运转，如果有足够多的证据证明一个理论"摆脱了一切合理的怀疑"，那么这个理论就被认为是对的。而数学并不依赖于容易出错的实验的证据，它立足于不会出错的逻辑，推导出无可怀疑的正确并且永远不会引起争议的结论。

科学仅仅提供近似于真理的概念，而数学，本身就是真理。数学赋予科学一个严密的开端，在这个绝对不会出错的基础上，科学家再添加上不精确的测量和有缺陷的观察。

于是我们就能理解数学家们的残酷，依靠计算机的帮助，有人能断定费马大定理对直到400万为止的幂都是对的，但该命题依然不算被证明。

在这方面不是没有反例。31、331、3331、33331、333331、3333331、33333331，经过仔细的探究，数学家们证明了这些数都是素数，那么是不是这种形式的数都是素数呢？下一个数333333331就不是，它可以被分解为17乘以19607843。

费马大定理之后，欧拉也提出过一个猜想，即不可能将一个高于2次的幂写成三个同样次幂的和。二百多年来没有人能证明这一猜想，后来用计算机细查，仍未找到解，没有

反例是这个猜想成立的有力证据，但谨慎的数学家是不会因此而承认欧拉猜想的。果然，1988年，哈佛大学的内奥姆发现了一个解：2682440的4次幂加15365639的4次幂加18796760的4次幂，等于20615673的4次幂。

依靠一块块绝对可靠的公理定理，数学家构筑出坚固的数学大厦，每一块基石都是可靠的，整栋大厦是人类智慧家园里最可信任的一幢。

这是数学的荣耀。

数学的魅力，在乎对人类智力和好奇心的挑战。

面对费马大定理，数学家们经受了三个多世纪的壮烈失败，任何卷入其中的数学家都冒着白白浪费生命的风险。他们为什么还要这样前赴后继？

如果能够证明大定理，那么就是解决了其他同行几百年来都深受困扰的难题，在其他人失败过的地方取得了成功。除了这种胜人一筹的成就感，就是人类与生俱来的难以克制的好奇心。解答某个数学问题的欲望多半是出于好奇，而回报则是因解决难题而获得的单纯而巨大的满足感。数学家蒂奇马什说过："弄清楚圆周率是无理数这件事可能是根本没有实际用处的，但是如果我们能够弄清楚，那么肯定就不能容忍自己不去设法把它弄清楚。"

数学在科学技术中有它的应用，但这不是驱使数学家们的动力。有个学生问欧几里得他正在学习的数学有什么用处，欧几里得转身让奴仆将其逐走："给这个孩子一个硬币，因为他想在学习中获得实利。"哈代在《一个数学家的自白》中坦言："从实用的观点来判断，我的数学生涯的价值等于零。"

当安德鲁?怀尔斯知道自己将要付出十年心血并且破解费马大定理的机会并不大时，他依然开始了孜孜演算："即使它们并未解决整个问题，它们也会是有价值的数学。我不认为我在浪费自己的时间。"

数学是最大的浪漫。

发展到现在，数学已经成为世界上最孤独的科学。致力于尖端问题研究的数学家，如果试图找到与其对话的人，遍寻全世界，都可能仅以个位数计。

需要解决的数学问题离普通人越来越远，而数学作为智慧体操，也在我们的头脑中越来越疏于练习。

让我们来操练一下，体验那种久违的解题的快感吧。

将国际象棋棋盘两个对角的白格方块拿掉，只剩下62个黑白相间的方块。现在我们取31张多米诺骨牌，每张骨牌正好可以覆盖2个方块。能否用这31张骨牌摆放得覆盖住棋盘上的62个方块？

有的人已经开始一次又一次的摆放了。让我们动用脑子，看看这个问题有没有答案——

一，棋盘上被去掉的方块都是白色的，那么剩下的方块是32个黑方块和30个白方块。

二，每个骨牌能够覆盖2个相邻的方块，而相邻方块的颜色总是一黑一白。

三，所以，无论如何摆放骨牌，都可以用30张骨牌覆盖住30个白方块和30个黑方块。

四，结果，总是留下1张骨牌和2个黑方块。

五，但是，每张骨牌所能覆盖的相邻方块必然是颜色不同的，而剩下的2个方块则是相同的，所以不可能被1张骨牌覆盖。

六，所以，用31张骨牌覆盖这个缺损的棋盘是不可能的。

再来思考一下"三人决斗"的问题。

黑先生、灰先生和白先生要用手枪进行决斗，每人只能开一枪，轮流射到只剩下一个人活着为止。黑先生枪法最差，三次才能击中一次，灰先生次之，三次中能击中两次，白

先生枪法最好，三发三中。为了公平起见，他们商定先由黑先生开枪，然后是灰先生（如果他还活着），再接着是白先生（如果他还或着）。问题是，黑先生应该先向什么目标开枪？

（五）

天文学家、物理学家和数学家坐着火车在苏格兰的大地上奔驰。他们往外眺望，看到田野里有一只黑色的羊。天文学家说："多么有趣，所有的苏格兰羊都是黑色的。"物理学家反驳道："不！某些苏格兰羊是黑色的。"数学家慢条斯理地说："在苏格兰至少存在着一块田地，至少有一只羊，这只羊至少有一侧是黑色的。"

伊恩?斯图尔特在《现代数学的观念》中通过这个笑话，揭示出数学家一丝不苟的严格态度：需要经过确实无疑的证明才能承认某个结论。

所以，一个真正的数学家从来不说过头话。有人问格丁根大学的埃德蒙?蓝道，他的同事埃米?诺特是否真是一个伟大的女数学家，他回答道："我可以作证她是一个伟大的数学家，但是对她是一个女人这点，我不能发誓。"

也只有数学家，才有资格说出那么不容置疑的话。1986年，两位数学家里贝特和梅休尔出席伯克利的国际数学家大会时，在一家咖啡馆巧遇。里贝特说起正在试图证明的椭圆方程，以及他一直在探索的实验性策略。梅休尔一边品着他的卡布其诺咖啡，一边听着里贝特的叙说。他突然停下咖啡，用确定无疑的口吻说："难道你还不明白？你已经完成了它！你还需要做的就是加上一些M－结构的γ－0，这就行了。"

确定无疑的，世界上只有极少数的人能在随便喝杯咖啡的时候想出这一步。

数学家在某方面表现得近乎迂直。费马在世时是一名文职官员，还在司法部门工作。为了避免这个职务上的人陷入人情腐败，政府要求法官不得参加社交活动，他于是得以潜心研究数学问题。但无论如何，数学都只能算是他的业余爱好，埃里克?贝尔就称他是"业余数学家之王"。但有人对这样的描述并不满意。朱利安?库利奇写《业余大数学家的数学》一书时，执意将费马排除在外："他那么杰出，他应该算作专业数学家。"

他们的脾气也同样火爆。索非?热尔曼对费马大定理的证明做出过杰出的贡献，她在物理学领域也颇有建树，并荣获法国科学院的金质奖章，成了第一位不是以某个成员夫人的身份出席科学院讲座的女性。在高斯的说服下，格丁根大学准备授予她名誉博士学位，遗憾的是，此时热尔曼已经死于乳腺癌。

当那些官员为热尔曼出具死亡证明时，竟将她的身份写成"无职业未婚妇女"，而不是女数学家。而对材料弹性理论做出极大贡献的她，也没有出现在埃菲尔铁塔上所铭刻的72名专家的名字中。莫赞斯为此大事鞭挞："对一位如此有功于科学并且由于她的成就而在名誉的殿堂中已经获得值得羡慕的地位的人做出这种忘恩负义的事情来，那些对此负有责任的人该是多么的羞耻。"

文学家永远成不了数学家，但数学家却可能写出非常动人而性情的文字。

因为说一不二，因为非此即彼，因为无可争议，所以数学家有着异于常人的愿赌服输的磊落和坦荡。《美丽心灵》中，一群数学家在大厅里向约翰?纳什纷纷献上钢笔，作为一种致敬的方式。这一幕体现出数学王国里特有的荣辱和伦理。

为鼓励证明费马大定理，法国科学院设立了一系列奖和巨额奖金。1847年，加布里尔?拉梅登上科学院的讲台，自信地预言几个星期后他会在科学院杂志上发表一个关于费马大定理的完整证明。

拉梅一离开讲台，另一位数学家柯西也要求发言。他宣布自己一直在用与拉梅类似的方法进行研究，并且也即将发表一个完整的证明。

三个星期后，两人各自声明已经在科学院存放了盖章密封的信封，里面是他们急于标明为自己所有的证明方法。数学界的许多人都暗暗希望是拉梅而不是柯西赢得这场竞赛，因为后者是一个自以为是的家伙，一个狂热的教徒，特别不受同事欢迎。

出乎意料的是，一个月后德国数学家库默尔致函法国科学院，根据拉梅和柯西透露出来的少量细节，他指出了两人共同犯下的逻辑错误。

库默尔的信使得拉梅一下子泄了气，但柯西却拒绝承认失败，几个星期内，他连续发表文章予以辩解，直到夏季结束才变得安静下来。

十年后，不招人待见的柯西、一贯自以为是的柯西，向法国科学院递交了关于费马大定理的最终报告："数学科学应该为几何学家，尤其是库默尔先生，出于他们解决该问题的愿望所做的工作而庆幸。委员们认为，如果撤消对这个问题的竞赛而将奖授予库默尔先生，以表彰他关于由单位根和整数组成的复数所做的美妙工作，那将是科学院作出的一项公正而有益的决定。"

（六?后记）

1986年，安德鲁?怀尔斯做出了那个改变其生命历程的决定：证明谷山－志村猜想，进而证明费马大定理。这一年，我也需要做出影响生命历程的选择：上文科，还是理科？

所有的路标都指向理科。不管是考试成绩，还是个人兴趣。张洁有篇小说叫《祖母绿》，曾令儿喜欢上一个绣花枕头的草包男人，她也不会向他撒娇卖嗲，只会不停地做数学题，比任何别人都快都好。这一幕烙在我心中，觉得那个黝黑的渔家女儿有着说不出的性感。当年，我最大的乐趣就是做数学辅导书上的题，专拣难度最高的C型题，每做出一个，都有莫大的快乐。

非常幸运的是，我所在的中学，是在高二年级中期分科，而不像大多学校那样一升入高二就把这事儿给办了。所谓幸运就是，我摊上了一个优秀的数学老师，他叫郜宝先，如果上文科，就不可能由他来教了－－好数学老师当然要用在理科班上。郜老师的课，永远是全校笑声最多最大的课堂，他的动作和表情都极为丰富，讲至兴处，能将板擦顺利完成左右手交接工作，兼以复杂的空中旋转，而他的粉笔头，也能准确地呼啸击中那些打瞌睡的同学。经常在晚自习的时候，他悄无声息地溜进教室，在黑板上写下几道题，然后扬长而去。第二天上课，再一脸坏笑地问我们做出来没有："一想到你们被难住，我就乐得不行"，然后将更漂亮的解法告诉我们。那一个学期，是我最轻松愉快的时光，解析几何不知不觉就学完了，从此再没有题能难得住我。

而另一方面，我们的语文课也由一位全国特级老师来教授，光一篇《白杨礼赞》，他

就上了有半个月。这样的语文，实在是味如嚼蜡。

但是，在天平的另一端，尽管只有一个砝码，却沉重无比：我是色盲，上理科，会有许多专业不能报考。

现在很难理解那种战战兢兢的心情，而在当年，高考之难，难于上蜀道，能考上个学就不错了，谁还考虑你的个人志趣和未来设计？

在一片懵懂中，我摸索着做过三次这样影响生命历程的选择：填报志愿时，有人撺掇在提前录取里填上北京广播学院，我老以为那所学校培养的是电器维修人员，就硬下心空着那一栏；报了人大后，负责招生的副校长盛情难却地鼓励我考人口学系，说是竞争又小，分配又好，我唯唯诺诺地应承下来，但还是咬着牙没报那个专业，那个后来被我们讥为"人口贩子"、人口稀薄整天被别系欺负的专业；而在最重要的文理分科时，我经过痛苦的犹豫挣扎，置物理课班主任的挽留于不顾，最终去了文科班……

二十年后，我看到了《费马大定理》这本书。唯一确定无疑的感觉就是，如果在1986年的那一天，我能看到这本书，肯定会学理科，考数学系。

人生若只如初见。我永远不能假设，行走在另一条轨迹上的我，会是什么样子。至少，我可以做一个像郜宝先老师那样的人，体验着数学的成就与快乐。

这本书的阅读，是一个惊心动魄欲罢不能的过程，中间搀杂着不得不睡的觉和不得不上的班。那天晚上参加一个活动，我却惦记着家里没看完的《费马大定理》，硬是没喝酒，早早就离开现场。关乎阅读，这样的事情已经很久没有发生了。

这是一本写得非常精彩的书，费马大定理的破解过程，与一部简明的数学史，被作者西蒙?辛格有机地糅合在一起。但我贱得嘀嘀叫的疯狗劲儿发作，以极大的兴趣和耐心将其拆散，以《读者文摘》的笔法重新归置梳理了一遍。一字一字敲在电脑中时，我的心中涌动着巨大的惆怅。但愿有一个少年，能够在如我那个决定命运的关键时刻，读到这个故事。

"牛顿研究所存在的唯一目的是将世界上一些最优秀的学者聚集在一起，呆上几个星期，举办由他们所选择的前沿性研究课题的研讨会。大楼位于（剑桥）大学的边缘，远离学生和其他分心的事，为了促进科学家们集中精力进行合作和献策攻关，大楼的建筑设计也是特殊的。大楼里没有可以藏身的有尽头的走廊，每个办公室都朝向一个位于中央的供讨论用的厅堂，数学家们可以在这个空间切磋研究，办公室的门是不允许一直关上的。在研究所内走动时的合作也受到鼓励——甚至电梯（它只上下三个楼层）中也有一块黑板。事实上，大楼的每个房间（包括浴室）都至少有一块黑板。"

请允许我抄下书中的这一段文字。我清楚的知道，那是我再也不可企及的精神故园。

《费马大定理——一个困惑了世间智者358年的谜》，（英）西蒙?辛格（Simon Singh） 著　薛密　译　上海译文出版社出版.

本文还有5条留言，察看留言和讨论请到http://zhiqiang.org/blog/112.html#comments

二十一世纪科学和数学的趋势

©Zhang-Zi, August 5, 2005 @ 4:00 pm

P. A. Griffiths

早晨好．我很高兴今天与诸位一起开始进入新的千年．我不能想出一个比谈科学和数学趋势更好的题目，因为在新千年中科学和技术可能比目前更为重要．我不是一个谈论大趋势的专家，在讨论未来时感到相当紧张．但是最近我在美国联邦政府的科学政策委员会里工作，为政府服务的一个职责是你要对于不甚了解的非常大的题目进行说教．所以大家会原谅我在今天就我们正在讨论的议题作某些猜测．如果我们同意这些大趋势确实是我们今天看到的样子，那么我们也会同意至少在不远的将来，这些趋势的动量将把它们运动到什么地方．

我要谈的最重要的论题是数学和科学正在如何相互联系．我们正在领会到所有科学和数学的知识是相互关联和相互依赖的．我们也开始看到这些知识作为原理和关系的集合体，已从不可见的原子扩展到地球上巨大的生物和社会系统．其结果使我们更加清晰地认识到，需要将理论研究和应用研究紧密地靠近，也需要多个领域的人员进行合作．

我是一个数学家，我的演讲主要从数学角度看问题，由此出发可知，目前的时代显然是一个黄金时代．其原因之一是数学开始与科学和工程非常密切地相互作用．这种相互作用促使科学得到新的视野，也促使数学得到根本性的进步，我下面打算描述在科学和数学中五个主要趋势，同时也谈到二十一世纪在等待我们的一些挑战．

趋势一：研究从直线模型到动态模型

第一个重要趋势应当是我们描述研究的方式．不少人在讨论科学政策时，都认为基础研究和应用研究不同．他们说基础研究是为了自身的缘故而探索知识的，用不着多想它将会有何用途．而应用研究不同，这种研究在思想上具有比较特定的目标．许多人谈论研究的"直线模型"，他们说知识只沿一个方向运动，从基础研究到应用研究再到开发，最后到应用．但是这种模型与现实世界的情况并不完全符合，即便是最简单的研究项目也都包含

思想和信息沿多个方向的动态流动.

研究者对这一点也不会感到惊奇，因为他们的研究一直如此．但是对于给研究者提供经费的机构来说，可能会感到意外．如果这些机构认识到研究的这个动态过程，他们可能会更有效地资助研究，从而把事情做得更好，例如，一个机构可能会明智地同时资助基础和应用研究，而不仅只资助一种研究，如果他们因为想要直接推进实际应用，而决定只资助应用研究，他们可能会严重地扭曲科学的进程.

我们可以想出许多个例子，表明最有创见的研究如何同时依赖于基础和应用的思考，伟大的法国生物学家路易·巴斯德(1)(Louis Pasteur)常常从医学、酿制啤酒、制造葡萄酒和农业方面的实际问题中得到研究的动力，促使他得到基础生物学和疾病方面的一些基础性发现．现代基因学之父孟德尔（Gregov Mendel）是在研究如何改进农作物这样很实际的问题时，发现基因基本定律的．举一个近一些的例子．物理中基础光学的研究具有传统的目标：为相机和望远镜生产更好的镜头，但现在给我们带来了现代电信业最重要的基础之一：纤维光学．我们需要设置不同类型研究人员的职位，并以多种方式使他们联合在一起，以使研究工作保持平衡和多样化.

趋势二：从理论＋实验，到理论＋实验＋计算

第二个趋势是研究过程自身的扩展．就在不久以前，我们把研究方式还归结为两种手段：理论与实验．现在由于计算机能力的开发，我们又加上了第三种重要的手段：计算，这第三种手段使我们可以对于直接测量或定量化太复杂的一些系统，来设计它的数学模型，从而回答几十年前不能理解的一些问题.

臭氧洞

需要大规模计算的一个人们熟知的例子是海洋与大气的混合体，我们试图把流体力学和非线性动力学组合起来去了解这个混合体，模拟它所基于的物理和化学过程，但是它比诸如墨水在水中运动这种快速扩散过程要复杂得多.

例如，仔细看一下，两种环境中均有非混合流体的"孤岛"，另一种介质无法从外部穿入进

来在海洋中这种现象对鱼的生死是至关重要的，因为鱼依赖于营养物、化学物质、浮游生物和其他鱼这种混合环境，在大气中，这些孤岛可决定污染和温室气体的传播．例如每年冬天在南极上空形成的臭氧洞就是这种孤岛之一．洞中的臭氧几乎完全被上层云的化学反应所破坏，洞由臭氧包围，大气被湍流搅动，但是周围的臭氧不能进到洞内，这是由于它在强大的涡流中心．而数学模型正确地预示出涡流的外沿是阻碍混合的壁垒．每年春天温度上升后涡流被破坏，阻碍消失，新的臭氧便回到洞内．

理解这个问题需要科学研究中的所有三种手段：流体力学的理论，对大气层条件进行实验，最后还需要计算，然后检查它与初始观察是否一致．在过去我们没有强有力的计算机，这种研究是不可能进行的．

KepIer球填装猜想

计算机的威力还可使我们解决数学的一个重大难题，这就是关于球填装（sphere packing）的开普勒（Kepler）猜想，它曾经难倒了将近四个世纪的数学家，这个问题始于十六世纪后半期,Walter Raleigh爵士写信给英国数学家Thomas Harrot，希望他给出一种快速方法来估计船甲板上堆积的炮弹个数．Harrot又写信给德国天文学家开普勒，后者对堆积问题颇有兴趣：如何在空间排放一种球，使球之间的空隙最少？开普勒找不到比船员堆放炮弹或者水果店老板堆放水果的最自然的方式更好的办法，这个最自然方式就是以正方体诸面的中心作为球心的安排方式，上述推断就成为著名的开普勒猜想．

这个问题之所以困难，是因为要排除巨大数量的可能性．在二十世纪中期，数学家们原则上知道如何把它归结于一个有限性问题，但即便如此，对当时可行的计算来说该问题仍是太大了．1953年取得重大进展，匈牙利数学家Laszlo Fejes-Tóth把问题简化成由许多特殊情形组成的一个巨大的计算，他还提出了用计算机解此问题的新途径．

Hales给出的证明非常复杂．他的方程有150个变量，每个变量都要变化，用于描述想象出来的各种堆放方式．证明中大量采用整体优化理论、线性规划和区间算术的方法．证明共有250（教科书）页和3个gigabytes（3×10^9个字节）的计算机程序和数据．只有到证明的末端才能知道Hales的将问题简化为一个有限问题是合理的．他本人也承认这个证明又长又复杂，要别人来确认所有细节还需要时间．

值得提及的是，这项工作照亮了其他相关领域．球填装问题属于数学的一个重要部分，可应用于差错检测码和纠错码的研究．这两种码被广泛应用于在压缩盘内存储信息，以及用于压缩信息以在世界范围内传送，在今天的信息社会中，很难再找到比这更重要的应用．

理论计算机科学

我要强调一下，计算属于计算机科学这个大领域，而它的理论方面已成为今天最重要和活跃的一个科学研究领域．它在半个世纪之前才真正开始，那时现代计算机还不存在，图灵(Alan Turing)和他的同代人用数学方法定义计算概念，并研究计算的威力与极限．这导致冯·诺依曼(von Neumann)建造了第一台电子计算机，再后来便是我们今天目睹的计算机革命．

计算机的实际使用和"计算"概念的出人意外的深度，使理论计算机科学得到更大的扩展．在最近25年里，理论计算机科学已成长为一个富饶而美妙的领域，并与其他科学建立了联系，同时吸引了一批一流的年轻科学家，其中一个重要的发展是把研究的焦点从"计算"转到更加难以捉摸的"有效计算"．其他重要问题有： NP—完备性，用随机性使算法理论革命化以及发展现代密码学和复杂性理论．

理论计算机科学除了这些内部发展之外，还有它与数学（诸如组合学、代数、拓扑和分析）之间重要的交叉成果．甚至理论计算机科学的基本问题异军突起，进入数学的中心问题之列．愈来愈多的数学家正在考虑他们研究领域的"计算"问题．换句话说，他们始于理论结果： "这个问题有解"，然后他们紧接着问："能以多快的速度和多大的近似程度找到解？"

理论计算机科学最后一个方面也是不少人特别感兴趣的，就是其他科学提出的一系列全新的算法问题．在这些问题中所需要的输出不能预先定义，并且它几乎可以始于任何类型的数据：一张图画，声波显示，从哈勃空间望远镜中读出的资料，股票行情，DNA序列，动物对刺激的神经反应的记录等，数学模型是试图使这些数据有意义，或者预测它们的未来值．

一般来说，"计算"一词本身和它周边一些主要问题，既具有实际的也具有深刻的哲学意义和推论．这个领域集中于几个明确而深刻的问题．例如：随机性是否能帮助计算？构成一个困难问题的证明的是哪些东西？能够做成量子或光子计算机吗？在这个新领域，取得令人惊奇的成长和加深新的基本性理解的时机已经成熟．

趋势三：从学科内研究到跨学科研究

目前第三个影响广泛的发展趋势是：从学科内研究转向跨学科研究．学院式的研究机构在传统上是按学科组织的，研究方案和成果由同领域的某些研究人员来鉴定．一个成功的学术生涯仍然主要依靠于学科内研究的成功程度，而这主要由发表的论文、学术职称的选举(这也按学科部门进行)和得到研究经费的能力来衡量．

总的说来，各学科在研究的深度和焦点问题上都取得了很大的成功：物理学探索了物质的构作部件，化学创造了具有特定性能的新的合成物质，生物学判定了控制和调节生命的许多基因和蛋白质，与此同时，一些现代问题要求新的更广阔的研究态度，新的跨学科研究小组正在探索更大的问题，其复杂程度远大于任何一个学科中的问题，

生命科学

在生命科学方面，这个趋势特别明显，在这里，新的技术和知识极大地改善了理解正常生物功能和疾病的能力．广阔的科学学科正在开始相互交织，成为生物、化学、物理和数学的新的聚合体．

比如，物理学为许多公共医疗的临床实践提供了基础性原理，有了诸如X光透视，CAT扫描，纤维光学视仪，激光外科手术，ECHO心动描记器和胎儿测音等．材料科学帮助制作新的人工关节，心脏阀门和其他人工组织．同样地，对核磁共振和正电子的理解有助于成像实验，使我们能跟踪大脑伴随思考、运动、情感、会话和药物使用而活动的位置和时间．基于三维蛋白体结构，将X射线晶体学、化学和计算机建模相结合，现在可以用来改进药物设计．

如果没有重组DNA的方法，人类基因组计划（目前，正在对从微生物到人的有机体的染色

体，进行作图和排出核苷酸序列）就不会存在．反过来，如果没有早期对合成、切断与重组DNA的各种酶的研究，也没有可能进行分子克隆．再进一步，今天打算到2005年完成人体DNA的3×10^9个基本序列的图谱，要依赖干机器人的加工采样和计算机对资料的存取比较能力．其他更专门的子领域的研究也不可缺少．目前正致力于以商业化的规模从事DNA的序列研究（如筛选出许多能导致某些癌症的突变的个体），使用的是毫微级技术和光化学，把接近于10^5个DNA的不同短链合成到一个小芯片上．

传染病

数学和生物学在研究人体传染病方面的结合呈现为一种新的发展很快的伙伴关系．这项工作的基础建于二十世纪二十年代，意大利数学家Vito Volterra发展了捕食与被捕食（predator-prey）关系的第一个模型．他发现鱼类中的捕食与被捕食种群的增减可以很好地用数学描述．二战以后，对动物群体变化建立的数学模型扩展到流行病学研究中．用类似于种群生物学的方法研究大的人群中的疾病变化状态．

更近一些时候，在分子基因方面的成果已启发和鼓舞科学家用同样的方法来研究传染病，此时的研究对象不是有机物或人的群体，而是细胞群体．例如，在细胞系统中，捕食者是病毒群体，而被捕食者为人体细胞群体．这两个群体在复杂的达尔文式的战斗中此起彼伏，而这种战斗正可以用数学进行描述．

生物数学家已经可以定量地预测细胞受病毒感染后的生命期望值．在研究艾滋病传染方面发现了一些奇妙的结果，这又反过来帮助我们理解艾滋病病毒在受感染病人体内变化情况．流行的观点是艾滋病病毒有10年左右的潜伏期，然后开始感染宿主细胞并引起疾病．但是数学模型表明引起主要疾病的艾滋病病毒没有潜伏期；它们不间断地快速增长，半生命周期只有两天左右．

那么，为什么要经过10年左右才开始感染？又是由数学模型表明，疾病的进展可能是由病毒的进化引起的，免疫系统可以长时间抑制病毒，但实际上病毒变异成若干新形式并且愈来愈多，最终压倒了免疫体系．

同样的数学模型已使我们理解为什么抗艾滋病病毒药物要组合服用并且在感染期间要尽早

服用．组合服用效果最好，是由于病毒每次极少产生多种变异．另一方面，应当在病毒还没进化得太远之前就要服用．

趋势四：简化主义伴之以复杂系统研究

第四个主要趋势是从传统的集中致力于简化方法转到更多地研究复杂系统．把一个系统简化成一些最小系统的简化主义一直到最近仍是主流．许多人把研究最小粒子的物理学作为科学的最真确部分．卢瑟福(Rutherford)爵士曾有句名言："所有的科学或者是物理学，或者是收集邮票．"卢瑟福爵士显然是简化主义信条和早期物理定律简明性的热情崇拜者．

但是，尽管有关世界的定律是简明和有序的，但世界本身并不如此．让我们看看任何一个地方，比如教室外面，到处都是复杂的现象：起伏山峰的排列，沙丘表面呈现的纷乱模式，金融市场的相互影响，生物学中种群的忽涨忽落．

因为世界是复杂的，就需要较为复杂的模型．复杂的模型不只是使问题本身更大和更烦琐，而且会有根本的差异．我们不能用研究具有良好行为的系统的工具来刻划复杂系统，只采用将基本定律用于大规模方程组的外推方法是不够的，对复杂系统的研究比

这要困难得多．

研究气候是一个好的例子．确定大气变化的基本方程——Navier-Stokes方程是非线性的．这意味着每个要预测的变量（如风速或风向）在方程中均有方幂．这些指数使系统对初值的微小变化或测量的误差均非常敏感：初值稍有改变就会有很不同的结果，这就是使天气预报有效期只有3－5天而更长期预报则不准的原因之一．

工程师们早就遇到过这种复杂性．例如每个奔腾芯片包含数百万个小元件：晶体管，连线和纵横交织的各种门元件阵列．每个元件的基本功能是清楚的，但集成之后这些元件相互影响的方式则不简单．设计师要精心制作模型程序来预测这些相互影响，以消除对错误（bugs）的敏感性．

生命科学已经在复杂系统的研究中得到了丰富的成果．经过几十年的努力，已成功地把关于生命的基本问题归结为个体基因和蛋白质的问题，现在生物学家的兴趣则是要用更系统的方法考察这些构成要素．基因排序和其他技术在不久的将来就会把细胞的各个部件分开，并读出它们的个体功能．现在研究者想要知道作为一个系统它们的功能是什么．

一个重要的挑战性问题是要了解控制细胞功能的化学网络，它是个高度复杂的系统．例如单个的基因表达(2)(expression of individual genes)通常不是由1个、2个或5个蛋白质来控制的，而需要许许多多的蛋白质．其中有些一直与DNA相连，有些只是暂时相连.细胞分子之间的相互作用有反馈效应，这会增加或减少其他分子的表达.

我们这里所说的是用计算机为细胞系统建模的初期尝试，可把它称作生理学研究的第三个方面．第一方面是 "in vivo"(活体内)，然后是"in vitro"(活体外，即试管内)，现在则是"in silico"（利用硅片，即用计算机）．这种基本的模拟就可以告知我们当营养和环境发生简单变化时细胞是如何反应的．目前正在进行的另一些跨学科研究方案，着力于了解病毒如何"决定"它是在载体中复制，还是潜伏以等待更好的机会．看起来，病毒好像有反馈控制机制，是它本身固有的"噪声"，从而在同样条件下并不全都做出同样的决定．这个聪明的适应性能保证在别的途径有危险时，总会有一些生存下来．

趋势五：全球化和知识的扩散

影响研究工作的第五个趋势是科学的全球化．我在前面说过，我们需要各种类型的研究，基础性的和应用性的．这个思想的引伸，就是在国际性竞争中每个国家都需要进行所有类型的研究，二十世纪七十和八十年代，曾经有人相信一个国家可以使用其他国家的研究成果，只要有好的制造业和市场运作技巧就可拿来受益．但是现在看来，这种"技术第一"的战略并不如我们预想的那么有效．近年来，曾经采用此战略的日本、韩国和其他一些国家均改变方针，建立自己的研究队伍．他们认识到，为了理解和扩展别人得到的发现，需要自己有高水平的队伍.

这个趋势的第二层含义是指知识在发达国家和发展中国家同时进行全球性交流．这个趋势对于发展中国家特别重要，这些国家迫切想要提高自身的科技实力．在一代人以前，这些国家的科学家只能去他国寻找最好的研究机会和设备．现在情况开始转变，这些国家最好的科学家逐渐地愿意留在家里为本国科学事业效力.

最近世界银行发起一项动议，在世界各地的一些国家建立小型示范性的研究所，称作"新千年科学启动项目"(The Millennium Science Initiative). 它从Packard基金会得到种子基金，再从世界银行贷款便开始运作. 第一批新千年科学研究所（The Millennium Science Institute，简称MSI）现已建在智利，以后还将陆续在拉丁美洲和世界各地的其他国家建立MSI.

这些MSI的目标是使科学家能在自己的祖国工作，他们在本土从事研究，并通过培养研究生和博士后来训练下一代科学家. 他们将与现有的研究单位建立联系，并能帮助促进经济发展. 这些研究所将形成一个全球网络，通过电子设备连在一起，并具有共同的目标. 我预言你们在将来会听到更多建立这种研究所的消息.

一些挑战

最后我想谈谈在新千年等待着我们的一些巨大困难和挑战，这些困难和挑战会阻碍跨学科合作研究的趋势. 我说过我们需要学科间高水平的相互交叉，但是有一些重大的障碍需要克服. 我在下面仍以数学为例，其他学科的情形是类似的.

影响相互交叉的一个障碍是我们自己的孤立传统，我们数学家过去总是与数学其他分支隔绝，与科学的其他领域隔绝，更是与非学术领域特别是与私人公司或单位隔绝. 重要的是应在研究所内和研究所之间建立更多的桥梁. 比如说，大学文化和私人工业的文化很不相同，几乎没有数学系大学生具有起码的工业知识，使他们将来在工业界能有满意的职业生涯. 在美国，新的数学博士中大约80%只考虑从事数学研究. 而我在前面提到过许多非常活跃的工业领域，例如生物信息和通信技术，在那里有许多前途广阔的发展机会.

"纯粹"数学的文化

使我们感到不适的更基本原因可能是在二十世纪我们所受的教育：最艰深的数学问题才是最重要的. 我们的文化也教导我们说：最有价值的是数学在心智上使人激动，数学结构的精巧和简单，以及探究有趣问题的自由性，不管这种探究将你带到何方.

在我当研究生的年代，为数学而研究数学的这个传统起着决定性的作用．比如说，哈代（Hardy）的书《数学家的自白》（A Mathematician's Apology）曾给我很大的影响．哈代讲数学的内在美．他认为我们作数学是由于它作为美学的和心智的活动的重要性．任何与实际应用或与物理世界的关联都是不恰当的甚至是我们所不希望的．没有老师教我们去研究像在工程、生物、化学或气象学等方面看上去乱糟糟或者没有精确解的那种问题．我们总喜欢"纯粹"的问题，而"纯粹"这个词给出了表明我们态度的一幅清晰的图画，仿佛所有其他类型的活动都不是那么纯粹．

但是，让我们再回到数学悠久的历史中看一看，这会有所帮助．在前面提到的巴斯德和孟德尔两个例子中，我们看到基础数学中的发现是由于实际问题的驱使．我们再想一想牛顿、欧拉、高斯、黎曼、庞加莱和其他一些数学家，他们的数学都跟对物理世界的研究相结合．从大部分历史中，我们都已分享到物理的数学方面，并且发现它们实际上很有趣．

不过在二十世纪，逐渐发展了为数学而做数学的传统．我们所设计的大学中，不再鼓励跨越学科边界的合作．我们人为地把"应用数学"系从"纯粹数学"系里分出去，这反映了对数学思维的一种狭隘的观点，

又比如，我在二十世纪的七十和八十年代教数学的时候，当时的数学系教员仅限于关注纯粹性研究，当然在这方面教授们干得很漂亮．但是我们人为地与应用数学家隔开，应用数学和计算机科学、控制论和其他工科一起，成为应用科学系的一部分．曾经有一次我打算聘一个优秀数学家同时在两个系任职，他研究流体力学，既从偏微分方程方面("应用"方面?)也从数值分析方面("纯粹"方面?)进行研究．不幸的是，系里其他人认为他的工作对我们来说不够"纯粹"，我认为聘任他是跨学科研究的绝好的机会，但其他人拒绝我的看法．

今天，这种事情很少再发生了，数学已经与科学与工程更加互动，这种互动已使科学和数学的基础性研究均受益匪浅．所以我们要更加关注我们自身研究以外的领域，包括数学以外的一些学科．

我认为在有效地组织研究工作方面，大学可以从私人机构那里学到很多东西．比如位于新泽西州的老贝尔实验室就是美国的一个很出色的研究单位．在那里，研究人员被组织成多

学科的小组．在贝尔实验室，不是由组织结构决定科学，而是由科学决定组织结构．在这里探索问题有更大的自由和灵活性，在创造杰出科学成果上取得了巨大的成功．

很幸运，风向似乎有些改变．比如在去年，美图国家卫生研究所（National Institute of Health）宣布要成立一个新的生物工程项目，资助多学科研究．而跨学科评估专门小组似乎也想跟着这样做，正在计划成立一些新的跨学科研究中心，其中一个建议设在斯坦福大学，集中研究生物物理．另一个是在普林斯顿，集中研究基因和蛋白体．美国Packard基金会近来投入一笔巨大经费支持跨学科研究项目，这类项目要想在现有联邦机构内得到资助是非常困难的．

结 论

在结论中我要强调，无论是观察我们的研究活动，还是我们彼此工作的方式，我们都正在看到全球性的相互交流与合作的大的发展趋势．研究工作正在变得更为复杂，因为我们要进行大量计算工作．研究也愈来愈要跨学科进行，因为这是理解复杂系统的最好方式/世界各国都开始认识到，如果要参加二十一世纪的知识和经济竞赛，一定要有自己的研究能力．

我在这里与中东科学家讨论一件令人振奋的事情，就是打算在贝鲁特建立一个小型和跨学科的国际性研究中心．这个中心将作为新千年科学启动工程的组成部分、它的一个目标是在阿拉伯国家和以色列科学家之间促进不同学科的合作研究与教育，我确信科学研究是一个很好的场地，不仅使科技知识更为先进，而且也有助于使人们学会进行跨越国界的合作．我确实相信，迎接二十一世纪挑战的最好方式是认识并适应这个强大的趋势，向老贝尔实验室这样的组织机构学习，它们在多年前就看出团队工作和跨学科研究的价值．今天我们面临的挑战是要把这种研究模式继续改进，把它们从工业界扩展到学术研究和教育中，训练明天的科学家和工程师，

非常感谢大家．

本文还有0条留言，察看留言和讨论请到http://zhiqiang.org/blog/122.html#comments

数学中的武林故事 作者：怪客

作者：怪客

1.黄教授.

这些故事都是在一个饭馆里从黄教授那儿听来的.

黄教授是我几十年的老相识,也是我一直佩服的朋友,他早年从学解析数论起家,在国内时就小有名气,到美国后改练算术几何,虽然没做得特别大,也算是成就斐然,毕业后经过一番波折,几年前在此间的一所大学混到了tenure,所以现在是正儿八经的教授.也许是读书时专心过度,黄教授四十多岁了,依然是光棍一条,错过了婚姻大事.好在他生性豪爽豁达,也不以此为意,而且喜爱户外活动,除了打网球,一年四季海边钓鱼不说,每到秋冬季节还扛把猎枪到山里打猎,所以每天乐乐呵呵,倒也过得快活自在. 只是人到中年,诸事烦杂,岁月易得,我和他虽然同在一地,但见面的机会却是越来越少了.

长话短说,这次找到黄教授,是为了一个小朋友小胡.小胡两年前从国内顶尖大学数学系毕业后就来到美国的一所长青藤名校,师从一位几何大师读学位,最近刚刚过了资格考试,来我这儿玩几天散散心.我在国内时多蒙小胡的父母帮忙,知恩图报,很想有机会报答一下.和小胡深谈几次,我感觉到他是有些彷惶,好象是数学上不知道该干什么好."这样吧小伙子,"我说:"我带你去见黄教授,让他和你好好谈谈."

找到黄教授后我说明了来意,黄教授呲出黄牙一乐:"老怪,你这不是要我来毒害青少年么?"

我说:"这是哪儿的话!小胡兄弟这样优秀的青年人才,又是初涉人世,老兄你不好好给他讲讲这江湖上的急风险浪,我还要为他的前途担心呢.再说黄兄,我们兄弟好一段不见了,也该好好聚聚,今天由我来做东."

黄教授笑说:"我们是该好好喝一顿了,这样吧,十四街新开了一家川菜馆,我们去那儿边吃

边聊如何?"

2.武林.

我们一行三人在小饭馆里坐定,两杯啤酒下肚,黄教授当即直奔主题:"小胡兄弟,你看武侠小说吗?"

小胡有些迷惑:"当然,在大学看过."

黄教授说:"咱们中国人学数学的,没有不看武侠的.记得八几年的时候,那时国内管数学竞赛的老裘,是系统所的副研究员,有一天我们几个到他家里去玩,发现他家里满满的几书架书,没一本是数学书,全是武侠小说.看到我们吃惊的样子,老裘笑着告诉我们,数学界没有一个不是精通武侠的.老裘讲,八四年的时候中国数学会在上海开年会,会议结束后北京代表团一行一百多号人在机场等飞机,大家闲聊起来,隔行如隔山,本来没什么好说的,但最终发现了一个共同话题,武侠小说.这些教授研究员,居然个个都是武侠迷. 这帮老家伙还投票选了最喜爱的武侠,你猜结果是什么?居然一致通过是神雕侠侣. 金庸里我最讨厌的就是神雕侠侣,什么他妈古墓派,莫明其妙."

我笑着说:"记得华老曾经说过,武侠小说是成年人的童话."

黄教授说:"这都是表面上打哈哈,哪有成年人看童话的?那岂不是个神经病?这里面是有一个深层原因的,说起来简单,数学界实际上就是武林,就是江湖.我在国内国外数学界混了几十年,越来越感觉到这一点."

小胡不解地说:"我所见过的老师个个都是谦谦君子,儒雅长者,没有象绿林中人物的."

黄教授哈哈笑着说:"在学生面前装假正经,古今中外都一样.我问你,武林中最重要的是什么? 是武功,只要武功超群,其他什么都不重要. 数学界也是一样,最重要的是数学功夫,只要你解决了什么超级难题,不管怎么样别人也得服你.武侠里最看重的是座次排名,数学里也是一样,最重要的就是排名.老板给学生写推荐信,主要就是说这学生比谁谁强. Borel在回忆录里说,每年IAS的老家伙们最大的乐趣之一就是给申请Postdoc的人排名,看看谁比谁厉害,其实他没说的是这帮老家伙何止只给Postdoc们排名,他们是在给整个数学界排名,虽

然从不明说,可圈里的人谁的心里都有数,谁比谁强,谁比谁差,一清二楚."

小胡说:"IAS一共只有七个教授,怎么可能给整个数学界打分排名?"

黄教授摇头说:"你哪里知道这七个人的厉害,那可是真正的绝顶高手. 有一次有人给Weil看一篇paper,Weil看了作者就说,这个问题这小子做不出来,即使做出来也肯定是错的.果不其然,Weil老先生的眼光,可谓如电如炬.还有一次,十几年前我的老板曾尽几年之力写成一长篇paper,200多页,非常technical,复杂得要命,拿去给Deligne看,结果Deligne花几分钟看了前言就说有错,最终果然如此.就象是洪七公一看郭靖,就知道他有几分武功一样,呵呵,那七个人可都是人精哪."

我说:"早年在国内的时候就听人讲,数学会开会,华老的座位一定要在正中间,往后是他的大弟子,二弟子,三弟子,等等,要是谁把苏步青排到了前面,那就惹了大麻烦了."

黄教授笑着说:"华老那一茬人都是农村出身,所以难免把农村的陋习搬过来,但内涵是一样的.其实洋人这儿也不例外,记得Polya在回忆录里说,他和Hermann Weyl在ETH同事多年,但Weyl很少跟他说话,这个老家伙到老了也不明白,Weyl哪是不愿跟他说话,根本就是看不上他,想想看,西毒欧阳锋怎么会愿意和智灵上人说话?会几个大手印又能怎样?"

小胡也笑说:"我可就是做智灵上人的数学分析习题集过来的."

黄教授笑说:"看来你是练了一身藏传武功.说起来武林里面帮派芜杂,数学界也是一样,山头林立,互相之间互不买帐,尤其在一些公立大学的数学系,山头之间为了一些蝇头小利而往往斗得你死我活,乐此而不疲.每四年开一次的数学家大会,整个儿就是一华山论剑,英雄排座次的战场,所以每次都热闹得不得了."

我说:"上次的ICM在北京开,进了人民大会堂,还他妈开了国宴,够过瘾的."

小胡说:"现在咱们中国人也开数学家大会了,今年就在香港,还要发金牌银牌呢."

黄教授说:"你知道什么,中国人开数学家大会,这叫清理门户,把各种逆子叛徒给逐出门

墙．当然了,发发金牌银牌,除了奖掖后进,也有调济各个山头的意思."

我说:"黄兄,咱们身为海外游子,时刻也要关心祖国建设,是不是?你给我算算,中国的数学什么时候能赶上世界一流?"

黄教授长叹一声:"哪有那么容易,说到底数学这东西是一种文化传统,没有几代人的努力,根本一点希望都没有.你看看国内这些搞数学的,哪有一个象样的?整天吃喝玩乐,研究的好象都不是数学.我觉得恰当地说,中国数学的水平非常类似中国足球的水平,一路货色."

小胡笑说:"这不又输给日本队了么,球迷还闹了事."

黄教授也笑着说:"咱们中国不出球星,倒出不少足球流氓,数学界也是一样,老陈岁数大了,回国后经常信口开河,一帮人跟着瞎起哄,欺负老年人,说中国要成数学大国了,其实都在给自己捞好处,又碰上李铁映这个科盲,居然把这个叫成陈省身猜想.我觉得这个猜想要加上一个必要条件,当中国队拿了世界杯冠军的时候."

我们三个都哈哈大笑起来,引来不少临桌的侧目.

小胡止住笑说:"黄教授,我今天算是开了眼界,你能不能再给我多讲讲数学界里的人物?"

黄教授说:"我在这个行业里混了这么多年,各种各样的人物也都见过,见得多了之后,也不知怎么了,越来越觉得这些数学家们都在武侠小说里见过,搞到后来我自己也胡涂了,好象是生活在武侠里一样."

我说:"你到底见了些什么人?"

黄教授说:"比如说星宿老仙,东方不败,四大恶人,东邪西毒,南帝北丐,任我行,苗人凤,左冷禅,苏星河,带头大哥,韦小宝,岳不群等等,有华山派,衡山派,少林派,峨眉派,星宿派,有练九阴真经的,练葵花宝典的,逆行经脉的,走火入魔的,剽窃秘芨的,还有破腹自杀的,什么都有."

小胡摇头说:"这些到底是谁呀?"

黄教授说:"你先别忙对号入座,以后慢慢就明白了."

我问:"谁是丁春秋?"

黄教授瞪我一眼说:"老怪,你这是明知故问."然后黄教授轻轻说了个名字.

看着小胡目瞪口呆的样子,黄教授和我都笑了起来.

3.女人.

我说:"黄兄,你把数学界比做武侠世界,我多少同意.可是有一点数学界和武侠截然不同,在武侠小说里到处是美女缠在这些侠客身边,可你去看看,数学系有几个女的?这里面又有谁是漂亮的?"

黄教授说:"这也难怪,女人天生就不应该学数学,其实不只是数学,任何理论科学,到后来都是个体力活,需要长时间的concentration,而女人到了二三十岁,都要考虑嫁人生孩子的问题,哪还有可能长时间地集中精力做数学?Weyl曾经说过,There are only two women in mathematics, one is not mathematician, one is not woman.呵呵,他说的这两个女人,一个是Sofia Kovalevskaya,另一个是Emmy Noether,这两位的画像现在还在我们系里挂着呢. Kovalevskaya长得漂亮,可她的paper谁都知道是被她美色迷倒的老板Weierstrass代写的.至于Emmy Noether,无论从长相到言行举止,没有一点象个女人的,整个一男的."

小胡说:"Weierstrass还这么不老实,真想不到."

黄教授笑着说:"相比现代数学界的几个糟糕老头子,Weierstrass还算是有情有义的."

我说:"怪不得数学系的光棍特别多呢."

黄教授叹气说:"不单是数学系的女生少,一般象样点的女孩也不愿嫁给数学系的人.一来没钱,二来数学系的人一做起问题来,其它什么都忘了,没法过日子.一个数学问题,短则做几个月,长则几年,陷进去之后,每天走路想,吃饭想,连和老婆上床都在想,不象一般人还有个

上下班,这是他妈全天候24小时,每天都神神癫癫的,做不出问题还要拿老婆当出气筒.聪明点的女孩谁愿意过这种不人不鬼的日子."

"哈哈哈哈..."我们笑得前仰后合.

黄教授接着说:"我还读研究生的时候,老板跟我说过,两个数学家相遇,第一个话题肯定是数学,第二个话题肯定是Sex.我当时还半信半疑,后来才发现是千真万确.你想,一堆大男人,整日里切磋武功做问题,闲下来的时候还能谈什么其它的?外边的人来了,总觉得数学系里是成堆的色棍,每天不务正业谈论女人,不理解个中原因."

我说:"费曼在自传里讲,有一次他大着胆子到Las Vegas逛妓院,到那里才发现那儿的妓女认识他的大部分教授同事,费曼还纳闷,难道这里的婊子都是Caltech物理系毕业的不成?"

黄教授笑着说:"你这故事多半是费曼自己编造的,为了给他自己的不轨行为打圆场.数学系虽然色棍多,但多半是纸上谈兵,出一两个采花大盗不奇怪,但说人人如此就有悖常理. 原因很简单,每天都在想问题,实在不会有太多其它空闲时间.给你们讲个典型的小故事. 我在读书的时候有一个日本师兄,不但学问做得好,而且为人谦虚有礼,和我们关系都很好.有一段时间大概用功过度了些,师兄有些厌倦,就到学校的酒吧去消遣,居然真的勾上了个漂亮的白人女孩,有那么几天这两位手拉手在系里走来走去.过了几个星期我发现日本师兄又一个人鬼鬼祟祟地在系里东躲西藏,我问他怎么回事,师兄直跳脚说,老子还要回来读paper做问题呢,哪他妈有空整天陪她鬼混?呵呵,师兄本想逢场做戏,没想到撞上一个多情的,纠缠不休,害得我这师兄在系里躲了几个月,全系传为笑谈.这一晃多少年了,现在师兄在日本也当上教授了."

4.激情.

我说:"做问题到底有多大的吸引力,让你这师兄这么神魂颠倒,连女人都顾不上了?"

黄教授说:"罗素把这个叫the intoxicating feeling of sudden understanding,中文里应该叫顿悟吧,一个问题思考了很久,突然一瞬间明白了,这种感觉,绝对是一种生理快感.Weil老先生曾经比较过这种快感和性高潮时的快感,他的结论是两者各有千秋,但时间长短有所不同.性快感总是短时间的,哪怕你他妈是练了藏传密宗吃了大补丸,了不起也就能折

腾几十分钟,而顿悟的快感能持续好几天.我的老朋友田刚在国内电视上说什么会当凌绝顶,一览众山小,不懂的人只知道他在自吹自擂,其实他是在说这种快感,只不过不好明说罢了."

我笑说:"所以外人说数学系的人都是色迷迷的也是有道理的."

黄教授叹气说:"往深里讲这其实是一种激情,一种无法控制排山倒海的力量在推你前进,任何搞数学的都会有亲身体会,但人的一辈子这种激情最多只有几次,现在的数学体系浩大繁杂,要做出大的问题没有这种激情根本就没有可能.菲尔兹奖只给40岁以下的是有道理的,40岁以上的人步入了中年,还会有个什么激情?荷尔蒙分泌量已经不对了,该雄起时雄不了,还谈做什么数学."

我知道黄教授也40多了,而且和菲尔兹奖也只是擦身而过,就说:"黄兄,菲尔兹奖之外还有Cole奖,Wolf奖,再说40岁以上真的不灵了?总会有些例外吧."

黄教授说:"我只知道一个例外,是Grothendieck.在退隐多年之后,1982年时,Grothendieck老先生突然在5个月内一气写下1600页的paper,真正的激情迸发,那时他已是50出头的人了,了不起呀.你猜他的paper的标题是什么,The Long March Through Galois Theory,哈哈,Galois理论的长征,怎么样,够厉害的吧."

看小胡有些困惑的样子,我说:"长征对咱们中国人来说是一政治名词,历史名词,最多也就是宣传队播种机,可是对西方人来说长征是一个非常浪漫的故事,意谓着为了某种目标而历尽千辛万苦,最终取得胜利. 我记得美国老牌政治家布热津斯基有一次在电视上教训几个小瘪三,说小子们,你们知道长征是什么,长征是从纽约出发走到三藩,再从三藩走回来,然后再走两个来回!"

黄教授点头说:"是这样的,Grothendieck老先生对代数基本群的刚性有着超人的领悟,他认为这完全决定了双曲曲线的同构类,以及曲线模空间的同构类.通过对曲线以及模空间的胞腔分解和代数基本群的作用,老先生认为可以得到对Q上绝对Galois群的精确描述,这就是他心里的长征."

看我们有些发晕,黄教授笑说:"算了算了,不和你们谈细节了,再给你们说个Grothendieck的故事吧.你们知道Grothendieck老先生在盛年的时候就归隐田园,从数学界消声匿迹了,二十几年前我老板刚刚毕业,在Rutgers当助教,有一天在餐厅吃饭的时候,老板赫然看到Grothendieck,正抱着一个Rutgers的女生在亲热吃饭呢.老板大着胆子上去打招呼,Grothendieck斜着眼看他问:'你是干什么的?'老板说是做代数几何的,Grothendieck一乐说:'我对那东西已经不感兴趣了,现在我在干更重要的事.'老板琢磨着这更重要的事就是搂着女孩吃饭,就胡说几句走了."

"过了一阵老板听说那个女孩跟着Grothendieck去法国了,忽忽又过了一年多,这女的抱着一个刚出生的孩子又从法国跑回Rutgers来,举目无亲,只好找到我老板来哭述,Grothendieck已经把她给抛弃了,显然这女人和小孩已成了老先生新长征路上的绊脚石."

我笑说:"长征路上女人生了孩子,留在当地脱离大部队的不算太奇怪."

黄教授有些出神地说:"我最近听说这孩子已经长大,从哈佛毕业了. 二十多年一晃过去,Grothendieck再也没有了消息,他老人家的万里长征,也该走了一大半了吧."

时间不觉过去,夜已深了,饭馆里只剩了我们三个,掌柜的远远的在不耐烦地看我们,我看黄教授已有几分醉意,就说:"黄兄,今天就到这吧,我们改日再来."

外面夜澜风静,街上依然车水马龙,我们再没说话,走到路口黄教授向我们挥挥手,径自回去了.

本文还有0条留言, 察看留言和讨论请到http://zhiqiang.org/blog/126.html#comments

诺贝尔的遗嘱全文

©Zhang-Zi, May 31, 2005 @ 4:00 pm

我，签名人艾尔弗雷德-伯哈德-诺贝尔，经过郑重的考虑后特此宣布，下文是关于处理我死后所留下的财产的遗嘱：

在此我要求遗嘱执行人以如下方式处置我可以兑换的剩余财产：将上述财产兑换成现金，然后进行安全可靠的投资；以这份资金成立一个基金会，将基金所产生的利息每年奖给在前一年中为人类作出杰出贡献的人。将此利息划分为五等份，分配如下：

一份奖给在物理界有最重大的发现或发明的人；

一份奖给在化学上有最重大的发现或改进的人；

一份奖给在医学和生理学界有最重大的发现的人；

一份奖给在文学界创作出具有理想倾向的最佳作品的人；

最后一份奖给为促进民族团结友好、取消或裁减常备军队以及为和平会议的组织和宣传尽到最大努力或作出最大贡献的人。

物理奖和化学奖由斯德哥尔摩瑞典科学院颁发；医学和生理学奖由斯德哥尔摩卡罗琳医学院颁发；文学奖由斯德哥尔摩文学院颁发；和平奖由挪威议会选举产生的5人委员会颁发。

对于获奖候选人的国籍不予任何考虑，也就是说，不管他或她是不是斯堪的纳维亚人，谁最符合条件谁就应该获得奖金，我在此声明，这样授予奖金是我的迫切愿望……

这是我惟一存效的遗嘱。在我死后，若发现以前任何有关财产处置的遗嘱，一概作废。

ps: 没有数学，不爽。

本文还有**1**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/183.html#comments**

有奖征答

发信人: WhaleJean (~.~), 信区: Mathematics
标 题: 另一个有奖征答
发信站: 北大未名站 (2005年04月14日14:49:18 星期四) , 站内信件
规则：
两人轮流切蛋糕，甲为先手，甲先切一刀，接着乙再选其中的一块，切一刀成两块，甲再切其中一块，切成两块……如此轮流切蛋糕，直到两人总共切了游戏要求的刀数(设为n)为止。(允许不切，视为切成0及原本被切的那块本身，（也就是（1，0））但仍算一刀，这就是所谓的『虚切』)
最后会切成n+1块（虚切，质量为0的，也算一块）。由甲或乙开始轮流从这些蛋糕中挑选
直到拿完，最后计算两人各拿到的蛋糕总量。假设两人都想尽量得到多一点的蛋糕，故两人都会以能得到最多蛋糕的最佳策略进行游戏。
而要探讨的游戏方式分两种：
先切先选：甲先切，两人全部轮流切完后，甲先选。
先切后选：甲先切，两人全部轮流切完后，乙先选。

猜想一：两人轮流切，共切2n刀，先切者先选，则甲=(n+1) /(2n+1)。
Proof or disproof 悬赏迪比特手机一只。

二：两人轮流切，共切2n刀，先切者后选，则?

给出一般式及证明悬赏迪比特手机最高档手机一对。
(听说是J6, 我不是很懂手机)
请直接发信到ccmp@seed.net.tw孙先生

Heroes in My Heart By ukim@BDWM

一本写数学家的八卦的小册子，非常值得一看。

点击下载： PDF Version: Heroes in My Heart By ukim@BDWM。

这是我在北大未名bbs连载的66篇文章，讲的是数学家们的故事。从第一次发文到现在，已经将近三个月。在davibaby的帮助下，把这些东西编成这么一个小册子，和bbs上的版本相比，这里的错别字要明显的少了，很多数学家的名字后面还加了中文的译名，不过，我还是想尽量保留bbs上的风格，从一开始的发信日期到最后的签名档，都作了保留。希望大家喜欢。发信人: ukim (我没有理想),
信区: Mathematics
标 题: 从今天开始连载数学家们的故事
发信站: 北大未名站 (2002年04月06日14:20:15 星期六), 转信

给那些喜欢数学和不喜欢数学的人们
给那些了解数学家和不了解数学家的人们

在北大混了四年，一事无成；在未名上bbs也呆了快一年了，制造了几千篇的垃圾。要毕业的人想法总是奇怪的，譬如说竟然真的要正经的写几篇文章了。最初写成这些东西的时候，我发给了几个朋友，一个学数学的师弟说他很感动，一个非数学系的mm说她后悔当初没有选数学系，无论怎样，他们能这样子讲，我很感动，这是发自内心的那种。现在的打算是每天贴2-3个故事，一直到欧毕业那天。很多事情难免有些too old,这个我也没有办法，激动人心的事情毕竟只有那么多。不多说了，真心的希望大家会喜欢，哪怕只有一点点的喜欢。这些文字偶给了一个名字，叫做 我心目中的英雄 --- **Heroes in My Heart**--

美丽有两种

一是深刻又动人的方程

一是你泛着倦意淡淡的笑容

本文还有**0**条留言，察看留言和讨论请到**http://zhiqiang.org/blog/245.html#comments**

一页纸多一点的博士论文拿到诺奖

©Zhang-Zi, April 11, 2005 @ 4:00 pm

故事发生在二十世纪初的法国。

巴黎。一样的延续着千百年的灯红酒绿，香榭丽舍大道上散发着繁华和暧昧，红磨坊里弥漫着躁动与彷徨。而在此时的巴黎，有一个年轻人，名字叫做德布罗意（De Broglie），从他的名字当中可以看出这是一个贵族，事实上德布罗意的父亲正是法国的一个伯爵，并且是正是一位当权的内阁部长。这样一个不愁吃不愁穿只是成天愁着如何打发时光的花花公子自然要找一个能消耗精力的东西来磨蹭掉那些无聊的日子（其实象他这样的花花公子大约都会面临这样的问题）德布罗意则找到了一个很酷的“事业”——研究中世纪史。据说是因为中世纪史中有着很　多神秘的东西吸引着这位年轻人。

时间一转就到了1919，这是一个科学界急剧动荡动着的年代。就在这一年，德布罗意突然移情别恋对物理产生了兴趣，尤其是感兴趣于当时正流行的量子论。具体来说就是感兴趣于一个在当时很酷的观点：光具有粒子性。这一观点早在十几年前由普朗克提出，而后被爱因斯坦用来解释了光电效应，但即便如此，也非常不见容于物理学界各大门派。

德布罗意倒并不见得对这一观点的物理思想有多了解，也许他的理解也仅仅就是理解到这个观点是在说“波就是粒子”。或许是一时冲动，或许是因为年轻而摆酷，德布罗意来到了一派宗师朗之万门下读研究生。从此，德布罗意走出了一道足以让让任何传奇都黯然失色的人生轨迹。

二

历史上德布罗意到底花了多少精力去读他的研究生也许已经很难说清，事实上德布罗意在他的5年研究生生涯中几乎是一事无成。事实上也可以想象，一个此前对物理一窍不通的中世纪史爱好者很难真正的在物理上去做些什么。

白驹过隙般的五年转眼就过去了，德布罗意开始要为他的博士论文发愁了。其实德布罗意

大约只是明白普朗克爱因斯坦那帮家伙一直在说什么波就是粒子，（事实上对于普朗克大约不能用“一直”二字，此时的普朗克已经完全抛弃自己当初的量子假设，又回到了经典的就框架。）而真正其中包含的物理，他能理解多少大约只有上帝清楚。

五年的尽头，也就是在1924，德布罗意终于提交了自己的博士论文。 他的博士论文只有一页纸多一点，不过可以猜想这一页多一点的一份论文大约已经让德布罗意很头疼了，只可惜当时没有枪手可以雇来帮忙写博士论文。他的博士论文只是说了一个猜想，既然波可以是粒子，那么反过来粒子也可以 是波。

而进一步德布罗意提出波的波矢和角频率与粒子动量和能量的关系是：

动量＝普朗克常数／波矢

能量＝普朗克常数＊角频率

这就是他的论文里提出的两个公式而这两个公式的提出也完全是因为在爱因斯坦解释光电效应的时候提出光子的动量和能量与光的参数满足这一关系。

可以想象这样一个博士论文会得到怎样的回应。在对论文是否通过的投票之前，德布罗意的老板朗之万就事先得知论文评审委员会的六位教授中有三位已明确表态会投反对票。本来在欧洲，一个学生苦读数年都拿不到学位是件很正常的事情，时至今日的欧洲也依然如此。何况德布罗意本来就是这么一个来混日子的的花花公子。然而这次偏偏又有些不一样——德布罗意的父亲又是一位权高望众的内阁部长，而德布罗意在此厮混五年最后连一个Ph.D都没拿到，双方面子上自然也有些挂不住。情急之中，朗之万往他的一个好朋友那里寄了一封信。当初的朗之万是不是碍于情面想帮德布罗意混得一个PhD已不得而知，然而事实 上，这一封信却改变了科学发展的轨迹。

三

这封信的收信人是爱因斯坦。

信的内容大致如下：

尊敬的爱因斯坦阁下：在我这里有一位研究生，已经攻读了五年的博士学位，如今即将毕

业，在他提 交的毕业论文中有一些新的想法……请对他的论文作出您的评价。另外顺便向您提及，该研究生的父亲是弊国的一位伯爵，内阁的＊＊部长，若您……，将来您来法国定会受到隆重的接待

朗之万

在信中，大约朗之万的潜台词似乎就是如果您不肯给个面子，呵呵，以后就甭来法国了。

不知是出于知趣呢，还是出于当年自己的离经叛道而产生的惺惺相惜，爱因斯坦很客气回了一封信，大意是该论文里有一些很新很有趣的思想云云。

此时的爱因斯坦虽不属于任何名门望派，却已独步于江湖，颇有威望。有了爱因斯坦的这一封信，评审委员会的几位教授也不好再多说些什么了。

于是，皆大欢喜。浪荡子弟德布罗意就这样“ 攻读 ”下了他的PhD（博士）。而按照当时欧洲的学术传统，朗之万则将德布罗意的博士论文印成若干份分寄到了欧洲各大学的物理系。大约所有人都以为事情会就此了结，多少年以后德布罗意那篇“ 很新很有趣 ” 博士论文也就被埋藏到了档案堆里了。德布罗意大约也就从此以一个PhD的身份继续自己的浪荡生活。。

但历史总是喜欢用偶然来开一些玩笑，而这种玩笑中往往也就顺带着改变了许多人的命运。

在朗之万寄出的博士论文中，有一份来到了维也纳大学。

四

1926年初。维也纳。当时在维也纳大学主持物理学术活动的教授是德拜，他收到这份博士论文后，将它交给了他的组里面一位已经年届中年的讲师。这位讲师接到的任务是在两周后的seminar（学术例会）上将该博士论讲一下。这位“ 老 ”讲师大约早已适应了他现在这种不知算是平庸还是算是平静的生活，可以想象，一个已到不惑之年而仍然只在讲师的

位置上晃荡的人，其学术前途自然是朦胧而晦暗。而大约也正因为这位讲师的这种地位才使得它可以获得这个任务，因为德拜将任务交给这位讲师时的理由正是“ 你现在研究的问题不很重要，不如给我们讲讲德布罗意的论文吧 ” 。这位讲师的名字叫做——薛定谔（Schrodinger）

在接下来的两周里，薛定谔仔细的读了一下德布罗意的“ 博士论文 ”，其实从内容上来讲也许根本就用不上“ 仔细 ”二字，德布罗意的这篇论文只不过一页纸多一点，通篇提出的式子也不过就两个而已，并且其原型是已经在爱因斯坦发表的论文中出现过的。然而论文里说的话却让薛定谔一头雾水，薛定谔只知道德布罗意大讲了一通“ 波即粒子，粒子即波 ”，除此之外则是“ 两个黄鹂鸣翠柳 ”——不知所云。两周之后，薛定谔硬着头皮把这篇论文的内容在seminar上讲了一下，讲者不懂，听者自然也是云里雾里，而老板德拜则做了一个客气的评价：“ 这个年轻人的观点还是有些新颖的东西的，虽然显得很孩子气，当然也许他需要更深入一步，比如既然提到波的概念，那么总该有一个波动方程吧 ”多年以后有人问德拜是否后悔自己当初作出的这一个评论，德拜自我解嘲的说“ 你不觉得这是一个很好的评论吗？ ”并且，德拜建议薛定谔做一做这个工作，在两周以后的seminar上再讲一下。

两周以后。薛定谔再次在seminar上讲解德布罗意的论文，并且为德布罗意的“ 波 ”找了一个波动方程。这个方程就是“ 薛定谔方程 ”！当然，一开始德布罗意的那篇论文就已经认为是垃圾，而从垃圾产生出来的自然也不会离垃圾太远，于是没人真正把这个硬生生给德布罗意的“ 波 ”套上的方程当一回事，甚至还有人顺口编了一首打油诗讽刺薛定谔的方程：欧文用他的psi，计算起来真灵通：但psi真正代表什么，没人能够说得清。（欧文就是薛定谔，psi是薛定谔波动方程中的一个变量）

故事的情节好像又一次的要归于平庸了，然而平庸偏偏有时候就成了奇迹的理由。大约正是薛定谔的“ 平庸 ”使得它对自己的这个波动方程的平庸有些心有不甘，他决定再在这个方程中撞一撞运气。

五

上面讲到的情节放到当时的大环境中来看就好像是湖水下的一场大地震——从湖面上看来

却是风平浪静。下面请允许我暂时停止对“老”讲师薛定谔的追踪，而回过头来看一看这两年发生物理学界这个大湖表面的风浪。此前，玻尔由普朗克和爱因斯坦的理论的启发提出了著名的“三部曲”，解释了氢光谱，在这十几年的发展当中，由玻尔掌门的哥本哈根学派已然是量子理论界的“少林武当”。 1925，玻尔的得意弟子海森堡提出了著名的矩阵力学，进一步抛弃经典概念，揭示量子图像，精确的解释了许多现象，已经成为哥本哈根学派的镇门之宝——量子届的“屠龙宝刀”。不过在当时懂矩阵的物理学家没有几个，所以矩阵力学的影响力仍然有限。事实上就是海森堡本人也并不懂“矩阵”，而只是在他的理论出炉之后哥本哈根学派的另一位弟子玻恩告诉海森堡他用的东西在数学中就是矩阵。

再回过头来再关注一下我们那个生活风平浪静的老讲师薛定谔在干些什么—— 我指的是在薛定谔讲解他的波动方程之后的两个星期里。事实上此时的他正浸在温柔乡中——带着他的情妇在维也纳的某个滑雪场滑雪。不知道是宜人的风景还是身边的温香软玉，总之是冥冥之中有某种东西，给了薛定谔一个灵感，而就是这一个灵感，改变了物理学发展的轨迹。

薛定谔从他的方程中得出了玻尔的氢原子理论！

六

倚天一出，天下大惊。从此谁也不敢再把薛定谔的波动方程当成nonsense（扯淡）了。哥本哈根学派的掌门人玻尔更是大为惊诧，于是将薛定谔请到哥本哈根，详细切磋量子之精妙。然而让玻尔遗憾的是，在十天的漫长“切磋”中，两个人根本都不懂对方在说些什么。在一场让两个人都疲惫不堪却又毫无结果的“哥本哈根论剑”之后，薛定谔回到了维也纳，薛定谔回到了维也纳之后仍然继续做了一工作，他证明了海森堡的矩阵力学和他的波动方程表述的量子论其实只是不同的描述方式。从此“倚天”“屠龙”合而为一。此后，薛定谔虽也试图从更基本的假设出发导出更基本的方程，但终究没有成功，而不久，他也对这个失去了兴趣，转而去研究“生命是什么”。

历史则继续着演义他的历史喜剧。德布罗意，薛定谔都在这场喜剧中成为诺奖得主而名垂青史。

尾声

其实在这一段让人啼笑皆非的历史当中，上帝还是保留了某种公正的。薛定谔得出它的波动方程仅在海森堡的矩阵力学的的诞生一年之后，倘若上帝把这个玩笑开得更大一点，让薛定谔在1925年之前就导出薛定谔方程，那恐怕矩阵力学就根本不可能诞生了（波动方程也就是偏微分方程的理论是为大多数物理学家所熟悉的，而矩阵在当时则没有多少人懂）。如此则此前在量子领域已辛苦奋斗了十几年的哥本哈根学派就真要吐血了！薛定谔方程虽然搞出了这么一个波动方程，却并不能真正理解这个方程精髓之处，而对它的方程给出了一个错误的解释——也许命中注定不该属于他的东西终究就不会让他得到。对薛定谔方程的正确解释是有哥本哈根学派的玻恩作出的。（当然玻恩的解释也让物理界另一位大师——爱因斯坦极为震怒，至死也念念不忘“ 上帝不会用掷色子来决定这个世界的 ”，此为后话）。更基本的量子力学方程，也就是薛定谔试图获得但终究无力企及的的基本理论，则是由根本哈根学派的另一位少壮派弟子——狄拉克导出的，而狄拉克则最终领袖群伦，建起了了量子力学的神殿。

本贴由ZT于2004年5月12日11:36:06在乐趣园〖华夏知青论坛—广阔天地〗发表.

本文还有6条留言，察看留言和讨论请到http://zhiqiang.org/blog/246.html#comments