

应用数学教育

EDUCATION OF APPLIED MATHEMATICIANS

林家翘

提 要

本文从应用数学的性质以及怎样发展一个能够相互了解的应用数学家的集体出发, 讨论了应用数学教学计划的作用。文中还介绍了麻省理工学院所采用的应用数学教学计划。

原文是作者的一篇演讲, 发表于“SIAM review”, 20卷, 4期, 1978年10月。为了便于读者理解, 我们在翻译时作了一些文字上的调整。

什么是应用数学

对于应用数学的性质与作用有种种不同的见解。

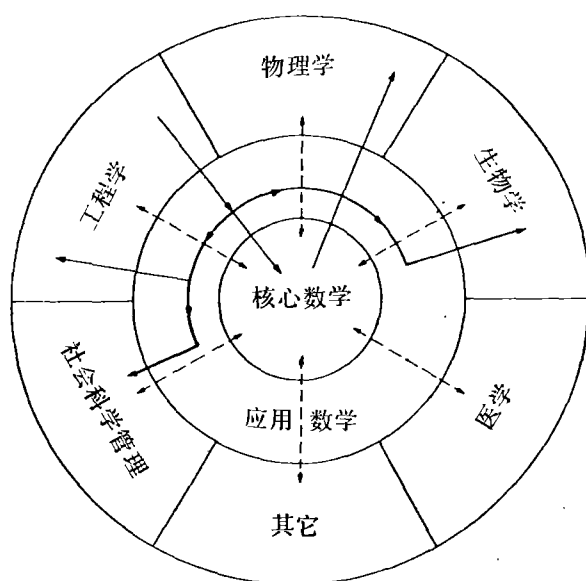
一种是把注意力集中于纯粹数学, 而把应用的领域看成是它的延伸或实例(因而是一个配角)。另一种是干脆把这个问题留给各学科中的理论家, 而不把应用数学看成是一种专业。第三种观点是把应用数学的各分支看成是互相关联的(正如纯粹数学的各分支一样), 从而主张让有才华的青年学生全面地了解各分支, 並希望能经过全体应用数学家的合作加强各分支之间的联系。这是三种基本的观点。

上述的第三种观点可称谓“全面的观点”。我在很多场合提倡过, 相信这是唯一的能把整个专业(以及这个专业的人们)结合起来的观点。

一般说来, 应用数学是介于经验科学与纯粹数学(pure mathematics)之间的一门学问(就其本质而言)。它有自己特征的态度、途径和思想方法。它的主题是数学和各门自然科学之间的相互依赖性。和纯粹数学工作者相同的是, 应用数学工作者对于促进数学的新发展是有兴趣的, 但是, 他们更侧重于那些直接地, 或者至少是强烈地以其他学科的问题为动机的方面。和自然科学理论工作者共同的是, 应用数学工作者通过运用数学方法来寻求对于科学事实和现实世界现象的知识和解释。

数学和其他科学之间的关系如图所示。位于图中央的是基本数学原理——纯粹数学的核心部分(或核

心数学); 位于外缘的是各门科学; 在两者之间的是应用数学。我想这张图不致引起很大争议。



数学与其它领域的关系示意图

从工程指向核心数学的箭头表示傅里叶分析。这是机械工程师发明的。可以在应用数学这一级上岔开, 把它应用于各个领域; 但也可以深入到核心中去。选择何种方向则由各人自己的目标而定。

应用数学的过程至少可分为以下三个步骤: (1) 表述, (2) 求解, (3) 解释。而其中又往往以表述为

最困难。建立一个科学问题的正确模型往往要经过对各种可能的模型进行成年累月的研究。

纯粹数学家和应用数学家应有区别，特别在培养途径上应有所不同。许多纯粹数学家坚持必须首先成为纯粹数学家才能谈应用。但数学既非易事，应用也颇困难，特别是表述和解释这两个方面。从这种观点出发，有人认为应用数学家必须是罕见的天才，所以应该干脆打消培养应用数学家的念头，换言之，应用数学教育的前景是暗淡的。

作为一个应用数学家，我不能同意这种认为应用数学家是超人的看法。我们对于纯粹数学的了解决不能也不必和纯粹数学家相比。在纯粹数学中，我们只知道那些与我们有关的数学基础：统计学家要知道概率论，物理学家要知道常、偏微分方程，等等。但他们都无须知道代数拓扑学。我们宁愿从图中的中层的圆（也许还是从靠边的地方）出发，就是说，从各学科的问题开始，采用研究特例的办法来推动数学理论。这样就可以较为直接地进入所关心的领域中去。

应用数学的发展确是如此。以福里叶级数为例，从热传导问题开始，很容易展现它可以用来表示各种函数的远景。于是，纯粹数学家就提出了福里叶级数的基本问题，即这种表示法可以用于哪一类函数的问题；这样，他们就得深入到纯粹数学分析中去（参看附图）。另一方面，应用数学家则止于逐段光滑函数，而转向福里叶变换，拉普拉斯变换，广义调和函数以及这些方法在各学科中大量的问题上的应用，如射电天文学与分子结构。由此可见，两者研究目标之不同。

还有一个例子可以表现应用数学和纯粹数学的不同特点，就是数值分析和机器计算。为数值天气预报所需要的偏微分方程无法解析地解出，因此只好采用数值方法。但是，并没有这种微分方程的存在定理，也不能证明，当步长无限减小的时候这种计算过程会收敛于某个渐近的极限。但是，由于经验证明了这种方法的可靠性，所以人们对此仍有信心。否则的话，我们非把美国计算机上作的很大一部分计算停下来不可。而我听说，计算是个庞大的事业，每年收支可达10亿美元之多。

可见，应用数学教育方面的困难并不像有些人所说的那样大。

应用数学的教育

现在我们来谈谈应用数学的教育问题，先从一些一般的问题开始，然后再介绍一个具体的教学计划。

我主张用一种全面的办法，就是说，应该有一种共同的教学计划（至少在大学期间），以利于创造一种应用数学家的集体精神。

人们可能对采用这种全面的办法是否现实有疑问。从我自己的考察出发，我认为完全有可能实现。近来我读了一些生态学和群体的数学理论、经济学以及组合分析等方面的书，并未发现其中用到的数学彼此有

多么大的差异。我发现生物学中用到的数学方法与物理学中用到的数学方法本质上并无区别。大家使用的数值分析方法和计算工具也都是类似的。

如果各学科中使用的数学方法极不一致，要在应用数学家之间建立集体精神当然也就会困难得多，甚至是毫无意义的。

当然，应该要求教授们有特别的能力来把初等的课程组织好，使之既表现出共同性又表现出差异性。而且，这也正是他们的职责。

下面我们来讨论教学计划。

任何教学计划的最终目的必须包括以下三方面：

（1）态度、观点和价值判断力的培养；

（2）获得特定领域中的成熟的、值得世代相传的大量连贯的知识；

（3）某些才能，特别是在所研究的特定领域中的创造力的发展。

因此，我们期望，人们在创造活动中积累经验，将会发展出一种智慧，这种智慧使他们能够对他们的同行提出有益的建议，并能胜任年轻人的老师。作为师长，他应对总的工作情况提出总体性的见解，以便学生能够决定如何努力，向哪个方向努力，并且有信心地去进行工作。没有这种总体性的见解，常常徒劳而无益。

我们应该怎样安排应用数学的教学规划以达到上述目的呢？

首先，这种教育必须从大学时期，即青年的成长时期开始。

如果一个人已经形成这样一种态度，即认为证明代数中的一个巧妙的定理要比借助于数学方法去研究油田的探查，或者去解释在大气或星系中所观测到的现象远为有价值（或者认为后者是“别人的事”），要转变他的想法就会非常困难。如果他对于使用他的数学才能去阐明高能物理学中的某个问题有了强烈的兴趣，他就不太可能同样热心地致力于解决生物学或经济学中的问题。

于是，教学材料（或者应用数学学生学习的主要内容）必须以说明过去数学中典型而深远的成就作为基础，这些成就应该从各种不同的学科中选来。必须采用研究实例的方法。同时，应当使学生了解到，尽管在已经建立起来的领域（比如力学，或者更广泛地说，物理学）中，应用数学家有继续取得成就的机会，但未来的惊人成就却可能出现于其他的领域——那些至今尚未充分运用数学的领域。我们必须避免由于过分强调传统学科而造成的缺乏创造性的危险。

正是由于缺少具有这种广泛性的综述性课程，才使培养未来的全面的应用数学家困难起来。有志于此的青年常常发现他得自己从大学理工各系的课程中去筛选出那些数学方面的东西来，从而使他处于几乎不能胜任的境地。虽然让他作这种努力对他也有很大的教育价值，但是代价却太大了。于是，通常的学生就

把自己固定在某个传统的系科里，要么是数学系，要么是别的系。这种专业化使我们难以实现培养全面的应用数学家这一主要目的。

有经验的科学家一定要为那些有志的青年学生，作好从数学与其他科学的相互作用中，抽象和综合出总的图象这一工作。其实，这本是任何专业教师的主要责任。他们必须提供入门的或者概述性的课程，以便教给大学生有关整个领域的现状的总图像，使未来的研究工作可以最有效地进行。

另一类课程最好由专业应用数学家讲授，这就是那些通常称为“应用数学方法”的课程。应当开设不同程度的这种课程。除了这两类“专业课程”以外，学生还应当对基本的纯粹数学有良好的基础，并且要受过至少一个科学分支的一定深度的教育。

现在可以把培养全面的应用数学家的教学计划的主要内容总结一下了。这样一个教学计划应当包括：

(1) 对应用数学家的态度的教育，强调解决现实世界中的问题；

(2) 关于工作中常常用到的工具(应用数学方法)的教育；

(3) 应用数学概貌，强调其总图象；

(4) 纯粹数学的基本教育；

(5) 至少受到一个科学分支的深入教育。

以上(1)、(2)、(3)三项通常应由应用数学家讲授，(4)应用纯粹数学家讲授，而(5)则应由不同系科中的专家讲授。

研究生的教育自然应当是以上讨论的本科教学计划的延伸和扩充。它当然应包括发展学生作研究工作的能力和独立思考的能力。上节中我们已经对这种能力作了概述。在这一方面，和任何别的学科一样，专业化是不可避免的，所以在具体的机构中能进行哪些项目的研究，就要看那里有什么专门家而定。

我们应当注意项目(3)，即应用数学概貌课程的中心作用，这些课程应当在大学二、三年级连续开设，大体两年。

如果没有这些课程，我们就会只能培养下列两种人材：(1)可能偶而对应用数学感兴趣的纯粹数学家；(2)高度专业化的应用数学家，他们可能在与其各自的特殊领域有关的数学的某一狭窄的方面很有能力。这两种人对应用数学可能确有贡献。但是，单靠他们是不足以使应用数学作为一个专业而得到健康的发展的。要使这种发展能够成功，就要宣传全面的应用数学教育训练。我们必须鼓励大批有进取心而杰出的青年进入这一专业，并向他们提供良好的工作条件。后一点对于应用数学的成功和发展也许是最重要的。评价应用数学家要根据他在促进交流方面的总能力。他们应有机会训练未来的应用数学家。

显然，我们不能提倡先把人训练成纯粹数学家再培养成应用数学家。这样作，就会束缚他们的思想，就有不利于他们的创造性活动的危险。那些已经受过

纯粹数学训练的人可能愿意作应用数学工作，但是他们应该记住 Schwartz 教授在他最引人注目的一篇文章中提出的警告，这篇文章的题目是：“数学对自然科学的有害影响”(J. Schwartz, *The pernicious influence of mathematics in the sciences*, Proceedings of 1960 International Congress on Logic, Methodology and Philosophy of Science, Nagel, Suppes and Tarski, eds., Stanford University Press, Stanford, CA, 1962, pp. 356-360.)。

一个大学本科的应用数学教学计划

麻省理工学院数学系在其应用数学委员会的建议下，采用了一个培养数学学士(强调应用数学)的教学计划。除了完成该系的一般规定以外，该选科学生必须达到下列要求：

1. 基本课程(全部)

微积分

微分方程

线性代数与近世代数

复变函数

离散数学引论

连续数学引论

2. 专门化课程

以下两组课程共选四门，但每组至少选一门。

第一组：

(1) 概率论与随机变量或概率论

(2) 统计推断或应用统计学

(3) 应用组合分析

(4) 计算的数学理论引论

第二组：

(1) 数值分析

(2) 物理数学引论(一)

(3) 物理数学引论(二)

(4) 流体力学引论

3. 建议要进研究院的学生必须选修一门分析课程。

对这一选课总的评价如下：

1. 相信这一选科的设置对学生和教师都有好处。尤其是使学生对应用数学的科目更加了解了。

2. 在制定上述规划时，限制性的要求已尽量减少，这样可以适应该系教员的不同趣向。

3. 在这个规划中，各课程的要求应该不时修改；但可认为，总的规划则会维持相当长的时期。麻省理工学院开设的课程提供了很多选择的可能性；比如可以选统计推断或者应用统计学。不过，这并不是必要的。任何统计方面的初等课程都是合适的。

教学规划的某些实际方面

我们为大学本科学士制定应用数学的教学计划，至少有三个理由。

信息是一个长度为 n 的二进制向量 M , 编码的方法是

$$E(M) = MG + Z$$

此处 Z 是一个 n 元素中有 t 元素其值为一的随机向量。用户收到 $E(M)$ 后, 即计算

$$\begin{aligned}\hat{C} &= E(M)P^{-1} = MGP^{-1} + ZP^{-1} \\ &= MSG + ZP^{-1}\end{aligned}$$

因此 $\hat{C}$ 是一个哥帕码。用 Patterson 算法可以将码 $\hat{C}$ 译成 $\hat{M} = M\hat{S}$, 再乘以 S^{-1} , 即得原信息 M 。当第三者收到 $E(M)$ 时却因不知 P^{-1} 和 S^{-1} 而无法如上进行。但是直接从 $E(M)$ 译成 M 则如前述是一个 NP-complete 难题。

三 密码签名

当一种码的编码和译码方法可以互换时, 狄非和黑门二氏设计出下述的一套公钥密码签名法: 设 E_i 、 D_i 分别为用户 i 的编码译码函数。如 A 要将信息 M 传送给 B , 且要 B 确知 M 是 A 所发, 则 A 首先算出 $S = D_A(M)$, 再用 B 公布的编码法得到 $D_B(C) = S$, 再用 A 公布的编码法算出 $E_A(S) = M$ 。当 B 译出 M 时, 可推知 S 一定是 $D_A(M)$ 。但除 A 外无人知道 D_A 这一译码函数, 故 M 一定是 A 所发。

我们现在来检查一下在上一节所介绍的三个方法中, 哪些有编码译码互换性质。设 $M = (b_1, b_2, \dots, b_n)$ 是要传递的信息。

1. 用李夏艾法时, 用户将 M 编成 $D(M) = M^d \pmod{n}$, 顾客收到后可译回得 $E(M^d) = (M^d)^e = M^{e \cdot d} = M \pmod{n}$ 。

2. 用牟黑法时, 用户将 M 编成 $D(M) = \sum w^{-1} M$ 。顾客译码时得 $E(\sum w^{-1} M) = \sum_{i=1}^n w^{-1} a_i b_i = \sum_{i=1}^n \hat{a}_i b_i$ 。但顾客不知道 $\hat{a}_i$ 之值, 故不能获知 b_i 。

3. 用麦氏法, 用户将 M 编成 $D(M) = MP^{-1}$ 。顾客译码时得 $E(MP^{-1}) = MP^{-1}G + Z = MP^{-1}SGP + Z$, 也不能复原成 M 。故三法中只有李夏艾法可用来签名。

• 上接46页 •

1. 假如我们只提供研究生的教学计划, 则不得不把注意力集中于培养在某一专门领域中的研究能力上, 就没有足够的时间来进行广度方面的教育。这将导致应用数学工作的分裂, 从而削弱总体方面的努力。通常, 这会导致只有少数优秀学生进研究院学习应用数学。

2. 保持大学的教学规划, 会使应用数学的教师们的兴趣和工作有一个共同的中心。大学教学规划的内容是要变化的, 但是比较慢 (牛顿力学还在起作用, 量子力学也不会一夜间面目全非); 这就使教员有可能相对稳定地共同努力。而共同努力又造成稳定的局面。

在研究生的教学规划中, 教员的兴趣必然会有不同。况且, 他们的兴趣常常要随科学发展的趋势和学科的生命力而频繁地变化。这样一来, 只有同一专门

四 结 论

公钥密码制目前最大的缺点是在理论上尚不能证明第三者不能在实际可能的物力、时间内破译。其理由如下:

1. 虽然牟黑和麦氏法都把破译和 NP-complete 难题搭上关系, 但若加上陷阱函数的咨询后, NP-complete 的性质是否仍被保持则是一未知数。

2. NP-complete 的观念只应用在一个算法最不利的情形下, 而不论及其一般情形。因此一个破译法也许在最不利情形下需要天文数字的时间, 但在很多普通情况下可以很快破译。

3. 究竟一个 NP-complete 问题是否没有多项式算法迄今尚无严格证明。

最麻烦的是实际的经验也不足以来断定公钥译码的安全性。因为如果有人发现了有效的破译法, 国家将把它列为最高机密而不让它公布。站在国家的立场上, 有一破译法而不让别国知道, 让别国继续使用一个不安全的公钥密码制是其期望的。

在工商应用上, 公钥密码制为了安全的要求, 在编码时必须大量增加信息的长度, 因而减低了实际讯息传送的速度。一个可行的折衷办法是大量的信息仍以简捷没有陷阱性质的编码法作业, 但编码法的键却用公钥密码法传递。这种方法也叫做“公钥输送”(Public Key distribution), 其实键是密钥, 只是由公共网络输送而已。因为键的长度很短, 输送不化费什么时间, 所以可以经常换送新键。这样编码法虽然容易破译, 但破译的速度显然远跟不上换码的速度, 因此破译所得的信息可能早已明日黄花, 破不破已经无关紧要了。

(本文主要参考 Cryptology in transition: a survey. A. Lempel, Computing Surveys, March 1980)

□

领域的人们之间才可能进行交流。然而, 同事之间缺少交流, 对于任何集体来说都是不利的。

3. 数学方法课程, 包括概述性的课程, 对于纯粹数学、自然科学、以及工程方面的许多其他学生具有很重要的教学价值。的确, 系统地开设了数学方法的课程, 就不必再开设那些“服务性课程”了, 这种课程常常引起大学中极大的不满。

大学的教师有义务完成一定量的教学任务。有了大学本科的教学计划, 应用数学家的教学任务基本上就是去讲授哪些为培养未来的应用数学家而开设的课程。这些课程对于前述种种目的会产生一种自然的、良好的副作用。如果应用数学家总是得去教那些“服务性的课程”, 那就难怪他们会觉得自己是学术界的“二等公民”了。(马希文译)

□