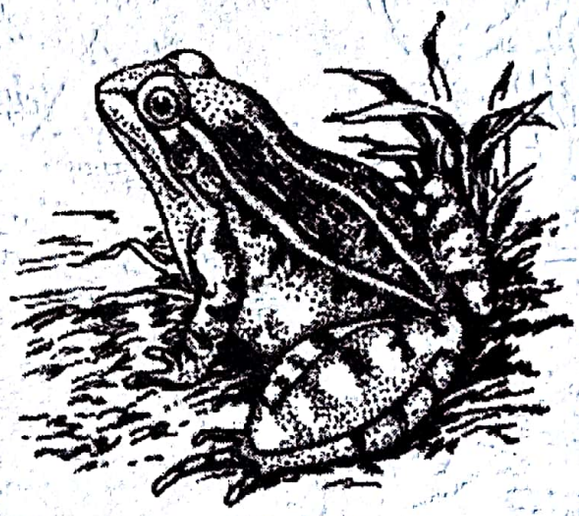
蛙鸣

第57期



中国科学技术大学数学系

《蛙鸣》编委会

2003年12月

刊首寄语

今次《蛙鸣》21 岁，正是风华正茂，走向成熟的一载。

《蛙鸣》让我们迈出了涂鸦的第一步。或闲暇偶拾，或郁闷苦求，所得虽不像数学大师们那样高屋建瓴，却也不失初生牛犊的锐意和朴实。《蛙鸣》将伴随我们在数学的世界中探索追寻。

又值初夏，“蛙鸣”时节，我们奉上本期《蛙鸣》，希望同学们能在个中听取“蛙声一片”，找到共鸣！

目　录

数学的印象

小平邦彦

什么是数学？不太清楚。但我以为关心数学的某些人会有这样的感觉，认为数学实际不就是这么回事吗？本文要叙述一个数学家看到数学的印象，即像我这样对数学专业以外的事情就不太懂的单纯的数学家，在研究数学时，感到数学是什么呢？我是直率而不加修饰的谈这一问题以提供读者参考。

一般认为数学是按严密的逻辑构成的科学，即使与逻辑不尽相同，却也大致一样。但是实际上，数学与逻辑没有什么关系。数学当然应该遵循逻辑，但逻辑在数学中的作用就像文法在文学中的作用那样。书写合乎文法的文章与照着文法去写小说完全是两码事；同样，进行正确的逻辑推理与堆砌逻辑去构成数学理论是性质完全不同的性质。通常的逻辑谁都明白，要是数学能归结到逻辑，那么谁都应该懂得数学了。但是初中高中很多学生理解不了数学却是众所周知的事实。精通语言学但数学成绩不好的学生不在少数。所以我认为数学在本质上与逻辑不同。

数学

考虑除数学外的自然科学，例如物理学可以说是研究自然现象中物理现象的科学。在同样的意义上，数学就是研究自然现象中数学现象的科学。因此，理解数学就要“观察”数学现象。这里说的“观察”不是用眼睛去看，而是根据某种感觉去体会。这种感觉虽然有些难以言传，但显然是不同于逻辑推理能力之类的纯粹感觉，我认为更接近于视觉。也可称之为直觉，为了强调是纯粹感觉，以下称此感觉为“数觉”。直觉包含着“一瞬领悟真谛”的含义，不太贴切。数学的敏锐，如同听觉的敏锐一样，与头脑好坏没有关系（指本质上没有关系的意思，而不是统计上没有相关关系）。但是要理解数学，不靠数学便一事无成。没有数觉的人不懂数学就像五音不全的人不懂音乐一样（这只要担当数学不行的孩子的家庭教师就马上明白。你眼前看到的事情孩子却怎么也看不见，说明起来很吃力）。数学家自己并不觉得如在证明定理时主要是具备了数觉，所以就认为是逻辑上作了严密

的证明，实际并非如此，如果把证明全部用形式逻辑记号写下看看就明白了。那就过份冗长，实际上不可能（当然不是说证明在逻辑上不严密。而是依照数觉，那些明显的事实就略去逻辑推理而已）。最近每每谈及数学的 sense（感受），而作为数学 sense 基础的感觉，可以说就是数觉。数学家因为都有敏锐的数觉，自己反倒不觉得了。

数学也以自然现象为对象

把数学的对象看作是自然现象的一部份，也许有人说这不讲道理，但是数学现象与物理现象同样是无可争辩的实际存在的，这明确表现在当数学家证明新定理时，不是说“发明”了定理，而是说“发现”了定理。我也证明过一些新定理，但绝不是觉得自己想出来的。只不过感到偶而被我发现了早就存在的定理。

正如大家不断指出的那样，数学对理论物理起着难以想象的作用。简直可以认为物理现象彷佛全都遵循着数学的法则。而且在许多场合，物理理论所需要的数学在该理论被发现以前很久就已经由数学家预先准备好了。典型的例子要算爱因斯坦广义相对论中的黎曼空间了。数学对物理如此起作用，其理由何在呢？过去的说法，归结起来是说数学是物理的语言。也许可以说，如广义相对论中黎曼几何的作用就是一种语言。但是在量子力学中，数学却真起了魔术般的神秘作用，在这里无论如何也不能认为数学只是语言了。

翻开量子力学教科书，首先看到的是光的干涉、电子的散射等实验的说明，然后表明，光子、电子等的粒子状态可以用波动函数（即属于某个 Hilbert 空间的向量）来表示并导出与若干状态的波动函数有关的迭加原理。迭加原理认为，状态 A 若是状态 B 与 C 的迭加，则 A 的波动函数就是 B 的波动函数与 C 的波动函数的线性组合，它是量子力学的基本原理。

什么叫粒子的状态呢？例如加速器内电子的状态就是由加速器决定的，所以，粒子状态可认为是该粒子所处的环境。因此在量子力学中就用唯一的波动函数（向量）来表示复杂至极的环境。这里首先是进行简单化、数学化的处理。状态 A 是状态 B 和 C 的迭加是怎么一回事呢？对于教科书中光的干涉等情形，其意义可以认为是显然的，而在一般场合，却很难理解环境 A 是环境 B 与 C 的迭加的意义。虽然根据普通观测的干扰可以说不确定性原理，例如不能同时观测粒子的位置与速度，但毕竟不能把粒子同时放在位置观测装置与速度观测装置中。就是说，粒子不能同时存在于二个环境中。那么什么又是这样二种环境的迭加呢？很难说清楚。另一方面，波动函数的线性组合演算在数学中却是完全初等的、简单明了的。迭加原理认为，这种简明的数学演算表现了复杂奇怪状态的迭加。就

是说数学的演算支配着量子力学的对象即物理现象。明白了迭加的物理意义，就知道不是用数式表示它，而是把线性组合表示的状态迭加当作公理，反过来按数学演算来确定迭加的意义。正如 R. Feynman 所说，迭加原理的说明只能到此为止。只能认为量子力学是基于数学不可思议的魔力。所以我认为，在物理现象的背后在着数学现象是无可争辩的。

数学是实验科学

物理学家研究自然现象，在同样意义上，数学家研究着数学现象。也许有人会说，物理学家做各种各样的实验，而数学家不就是思考吗？但是，这种情况的“思考”就是思考实验的意思，例如与“思考”考试题的性质不同。我们知道，对考试问题，只要适当组合某个确定范围内已知的事实，一小时内一定能够解决，思考的对象、思考的方法都摆在面前。而实验则是为了调查研究原先未知的自然现象，当然其结果就无法猜想，也许什么结果也得不到。数学也完全一样，它是探究未知的数学现象的思考实验，虽说是思考，但思考的对象是未知的，思考些什么为好也不知道。数学研究的最大困难就在于此。

思考实验中最容易理解的形式是调查实例。例如考虑偶数最少可表为几个素数的和的问题。检查一下实际的偶数，2 是素数不算，$4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 5 + 5, 100 = 47 + 53, \cdots$ 总可以表为二个素数的和。由这一实验结果，可以猜想“除 2 以外的一切偶数都可表为二个素数的和”的定理成立（这是早就有名的哥德巴赫猜想，现在还没有解决）。如果这样几次调查实例，能够猜想出定理的形式，以后就可以考虑证明该定理，那么研究的最初难关就被突破了。当然这是数学，光堆积几个实例还不是定理的证明，证明还必须另外考虑。

初等数论些定理就是首先从这样的实验结果出发引出猜想，然后才证明的。从上个世纪末到本世纪初，由 F. Enriques、G. Castelnuovo 等意大利代数几何学家得到的惊人成果中，依据实验的不在少数。实际上，J.A.Todd 在 1930 年左右发表的论文中曾明确断言：“代数几何是实验科学”。他们的定理全部得以严密的证明还是最近的事。值得注意的是，尽避他们给出的定理证明还很不完全，但是定理却是正确的。

发现新定理

最近数学的对象一般都非常抽象，实例也还是抽象的，难以想象，因此靠调查实例来猜想定理的形式，在许多情况下首先就不可能。我不知道在这种状况下，

发现新定理的思考实验的方式是什么样的。即使说只是含含糊糊地想想思考些什么，恐怕还是不行的。实际就是那样往往是不管怎么去思考都得不到相应的结果。这么说来，数学研究是不是非常困难的工作呢？倒也未必。有时你什么也没干，但却很自然地接二连三看到那些值得思考的事情，研究工作轻而易举地得到进展。这时感受充分表现在夏目漱石在《十夜梦》中描述运庆雕刻金刚力士的话上。引用其中的一部份：运庆现在横着刻完了一寸高的粗眉毛，凿刀一竖起，就斜着从上一锤打下。他熟练地凿着硬木，就在厚木屑随着锤声飞扬的时候，鼻翼已完全张开鼻孔的怒鼻的侧面已经显现出来。看起来他的进刀方法已无所顾忌，没有丝毫犹豫的样子。

“原来使用凿子那么容易，就把想象中的眉毛、鼻子作成了”，他颇为得意，自言自语道。于是，刚才的青年就说：“什么，那并非用凿子作出眉、鼻的，眉毛、鼻子本已埋在木材中了，只是靠凿子与锤子的力量挖了出来。就像从土中挖出石头一样，决不会错的”。

这种时刻，想想这世间没有比数学更容易的学科了。如果遇到有些学生对将来是否干数学还犹豫不定，就会劝告他“一定要选数学，因为再没有比数学更容易的了”。

接下去漱石的话的要点如下：他便觉得雕刻也不过如此，谁都能干的。因此他想自己也雕个金刚力士试试，回到家，便一个接一个雕刻起后院的那堆木材。不幸的是，一块木头里也没有发现金刚力士。他终于明白了，原来明治的木头里并没有埋着金刚力士。

数学也一样，普通的木头里没有埋着定理。但从外面却看不出里面究竟埋着什么，只好雕刻着看。数学中的雕刻就是一边进行繁复的计算，一边调查文献，决不是简单的。在许多情况下什么结果也没有。因此数学研究非常费时间。可以认为，研究的成败主要取决于运气的好坏。

定理与应用

现今的数学，由实例猜想定理是很困难的，不仅如此，定理与实例的关系看来也变了。在大学低年级的数学中；定理之为定理，乃是由于可应用于许多实例，没有应用的定理就没有意义。好的定理可以说就是应用广泛的定理。在这个意义上，函数论的柯西积分定理是最好的数学定理之一。但最近的数学中，有广泛应用的定理几乎见不着。岂止如此，几乎毫无应用的定理却不少。正如某君不客气地说：“现代数学只有两种，即有定理而没有应用例子的数学与只有例子而没有

定理的数学”。从现代数学的立场出发，“不管有没有应用，好的定理就是好的定理”，但我却总觉得，没有应用的定理总有点美中不足。

数学的唯一理解方法

即使不作研究，只看看书与论文，数学也很费时间。比如只看定理而跳过证明，二三册书似乎很快就能读完的。但是实际上跳过证明去读，印象就不深，结果一无所知。要理解数学书，只有一步一止循着证明。数学的证明不只是论证，还有思考实验的意思。所谓理解证明，也不是确认论证中没有错误，而是自己尝试重新修改思考实验。理解也可以说是自身的体验。

难以想象的是，此外没有别的理解数学的方法。比如物理学，即使是最新的基本粒子理论，如果阅读通俗读物，总能大致明白、至少自己认为明白了，尽避很自然地与专家的理解方法不同。这就存在着老百姓的理解方法，它与专家的理解方法不同。但是，数学不存在老百姓的理解方法。大概不可能写出关于数学最近成果的通俗读物。

“丰富的”理论体系

现在数学的理论体系，一般是从公理体系出发，依次证明定理。公理系仅仅是假定，只要不包含矛盾，怎么都行。数学家当然具有选取任何公理系的自由。但在实际上，公理系如果不能以丰富的理论体系为出发点，便毫无用处。公理系不仅是无矛盾的，而且必须是丰富的。考虑到这点，公理系的选择自由就非常有限。

为了说明这件事，把数学的理论体系比作游戏，那么公理系就相当于游戏规则。所谓公理系丰富的意思就是游戏有趣。例如在围棋盘上布子的游戏，现在知道的只有围棋、五子棋和二类朝鲜围棋只 4 种类型。就是说，此刻所知道的公理系只有 4 个。除这 4 个以外，还有没有有趣的游戏呢？例如四子棋、六子棋、或者更一般的 n 子棋又如何呢？实际上下 n 子棋，当 n 在 4 以下，先手必胜，即刻分出胜负，所以索然无味；而当 n 在 6 以上时，则永远分不出胜负，也毫无意思。发现这种新的有趣的游戏并不容易。要找出跟围棋差不多有意思的游戏大概是不可能的。虽然这只是我的想法。数学也同样，发现丰富的公理系是极其困难的。公理系的选择自由实际上等于没有。

理论的丰富推广

数学家一般都本能地喜欢推广。例如假设存在以某个公理系 A 为基础的丰富的理论体系 S。这时谁都会想象到，从 A 中去掉若干个公理得到公理 B，从 B 出发推广 S 得到理论体系 T，再进行展开。稍加思索就觉得 T 是比 S 更丰富的体系，因为 T 乃是 S 的推广，但如果实际试验一下这种推广，许多场合与期待的相反，T 的内容贫乏得令人失望。这种时候，可以说 T 不过是 S 的稀疏化而不是推广。当然并非所有的推广都是稀疏化。数学从来是依据推广而发展起来的。最近推广不断堕入稀疏化，倒不能说是一种奇怪的现象。

那么，能发展成丰富的理论的推广，其特征是什么呢？进一步，公理系能作为丰富的理论体系的出发点的特征又是什么呢？现代数学对这种问题不感兴趣。例如，群论显然是比格论更为丰富的体系，但群的公理系优于格的公理系之点是什么呢？又在拓朴学、代数几何、多变量函数论等等中，基本层的理论的出发点（看来似乎）是毫无价值的推广，它不过是用及数替换以前的常数作为上同调群的系数。而实际上却是非常丰富的推广，其理由何在呢？与此相反，连续几何被看作是射影几何的令人惊叹的推广，但却没有什么发展，这又是为什么呢？当把数学作为一种现象直接观察时，所产生的这类问题不胜枚举。虽然我并不知道，它们是否都是不屑一顾的愚蠢问题，抑或能否建立一门的回答此类问题为目标、研究数学现象的学科，即数学现象学呢？但是如果能够建立，那一定是非常有意思的学科。为了研究数学现象，从开始起唯一明显的困难就是，首先必须对数学的主要领域有个全面的、大概的了解。正如前面说的，为此就得花费大量的时间。没有能够写出数学的现代史我想也是由于同样的理由。

作者简介：小平邦彦（KodairaKunihiko）是日本数学家，1915 年 3 月 16 日生于日本东京。1985 年荣获沃尔夫数学奖，时年 70 岁。主要成就：他对复流形、代数几何学作出了重大贡献。

量子场论、弦理论与数学

胡森

量子场论、弦理论与数学

人们通常认为，近代科学与以前的科学的区别是近代科学有实验。这种看法是值得商榷的。著名物理学家杨振宁教授和著名哲学家海德格尔认为近代科学的最根本的特征是数学和实验的结合，自然科学的定律用抽象的数学形式表达，从而达到前所未有的深度和广度。作为近代科学标志的两大发明，万有引力和微积分都是由牛顿创造的。在牛顿以后的科学发展中也反复印证了这一点。近代科学史上许多有伟大贡献的自然科学家也是数学家。这种状况一直延续到 20 世纪 20 年代。此后形式化的数学一度占据数学的中心，数学在很长一段时间内淡化了和其他科学，尤其是理论物理的联系。从 20 世纪 20 年代，量子场论开始出现并逐步成为理论物理的中心。到 20 世纪 70 年代中数学和量子场论才开始建立起密切的联系。从 80 年代以来，获得菲尔兹奖的数学家中其工作和量子场论或弦论有直接联系的占一半。

对称性和量子化：支配物理和数学的两个基本原则

也许我们要问：为什麼量子场论和弦论会和数学有密切的关系？一个答案是，它们被相同的原则所支配。其中最重要的原则是：*对称性和量子化*。

什麼是对称性？从一些建筑设计，巴赫的音乐和粒子物理中的 CPT 破缺（杨振宁和李政道的诺贝尔奖工作）中我们体验到各种离散对称性。伽罗瓦是第一个系统研究离散对称性并用于解决高次多项式方程不可解问题的。对于自然界连续对称性似乎更重要。例如我们有：

- 伽里略的相对性原理和牛顿第一定律；
- 伦茨对称性和导出狭义相对论；
- 从坐标变换不变性和局域洛伦茨不变性导出广义相对论；

- 经魏耳等人的努力，电动力学可以表述为阿贝尔规范场，即具有局域变换不变性，规范群是阿贝尔群；
- 非阿贝尔规范场，即杨 – Mills 场，是粒子物理的基础，也具有局域变换不变性，规范群是非阿贝尔群。

这里我们也许可以用两个原理来表述对称性的重要作用：

爱因斯坦原理：物理世界的规律应该和我们的表述无关。

杨振宁原理：对称性支配相互作用。

上述原理在几何中也是基本的。几何量，如长度，面积，体积等也是和描述他们的方式无关。这一点充分反映在以下理论中：

嘉当和陈省身：活动标架法。

在 70 年代中杨振宁意识到规范场和陈省身先生研究的联络是一回事，似乎就是局域对称性在物理和几何两个领域的各自实现。

以下我们解释一下什麼是量子化。

量子化原理：微观世界的描述不能用决定性的方式来描述，他们是几率式的。事件的几率全体组成 Hilbert 空间。动力学变量实现为 Hilbert 空间上的算子。

玻尔相容性原理：我们对于世界的每一种描述是不完备的，但是他们是相容，自洽的。

测不准原理是玻尔相容性原理的具体实现。

我们知道，量子力学已成为了解微观世界的基本工具。在量子力学发明后不久，人们把它用到电动力学的研究上。这时我们必须引入场的概念。经典的麦克斯韦方程是线性方程。它的解就是无穷多个波的叠加。其量子化乃是将无穷多个谐振子放在一起而无相互作用。当人们作计算时发现有许多无穷大。一直到 1948 年，量子电动力学才在引入重正化以后有了有限的定义并和实验吻合得极好。在 1954 年杨振宁 – Mills 将规范场推广到非阿贝尔群。其量子化经许多人的努力得到实现。人们发现量子规范场理论是唯一具有渐进自由性质的量子场论。物理学家对于围扰场论用费曼图给出了定义。到 1974 年物理学家建立了基本粒子的标准模型。从此物质场基本被标准模型所描述。在此过程中杨先生的” 对称性支配相互作用” 起了重要作用。拉氏量中的相互作用往往被对称性的考虑所决定。人们也试图在此框架下将引力量子化，但没有成功。实际上，引力场是不可重整的。

为什麼要研究超弦理论

由上我们也许可以得到一点启示，即相互作用的统一实际上是对称性的统

一。从 20 世纪 70 年代起，人们又发现了超对称。它是一种将对易和反对易关系非平凡的合在一起的代数结构。将这种代数局域化，我们便得到局域超对称。在此类变换下不变的就是所谓超引力。在超引力中我们所知道的 4 种相互作用合在一起。所以我们说在经典的意义下超引力把 4 种相互作用统一起来了。超引力的量子理论就是超弦理论。这就是为什麼我们认为超弦理论中包涵了量子引力。

弦理论把粒子不再看成一个点，而是看成一根弦。弦的运动扫出一条曲面，弦的振动给出粒子。当粒子碰撞时，他们不在某个特定的点碰撞，因而免去场论中令人头疼的无穷大问题。到了 1985 年人们发现共有 5 种协调的超弦理论。他们都在 10 维时空中运动。在我们将其中 6 维空间紧致化以后，我们可以得到通常的 4 维规范场论。从保持部分超对称的考虑，紧致化的 6 维空间必须是卡拉比－丘成桐空间。弦理论里自然包涵引力子，超引力是超弦理论的低能极限.

在 1985 年人们面临的问题是，在 5 种超弦理论中，哪一种是描述自然的？超弦理论如何和实验建立联系？

在 1995 － 1998 的第二次超弦革命中，上述问题取得了突破。人们发现了对偶性，即不同理论在其适当的范围内可以相互等价。其中最让人惊奇的是一些强相互作用的理论和某些弱相互作用的理论等价。这就为人们研究强相互作用开辟了道路。人们最初在超引力方程中找到了孤立子解，p- 膜，后来在超弦中发现了在某些超对称变换下不变的超对称态，D －膜。由于保持某些超对称，他们的量子性质与相互作用强度无关。因而人们可以得到一些强耦合下的信息。人们发现上述 5 种超弦理论是等价的。他们都是 M 理论的极限，M 理论在低能下的极限就是 11 维的超引力。

上面所及的量子场论只是在微扰的情况下有意义。这相当于在很小的尺度下经典近似是非常好的近似。反过来，当尺度变大，相互作用变强，上述理论失效。在粒子物理里，人们猜测当尺度变大，相互作用变强，从而无法把夸克分开。这就是著名的夸克幽禁猜测。这是标准模型中的核心问题之一。弦论前几年的发展为我们建立夸克幽禁开辟了一条全新的道路。

实际上，前几年超弦理论的第二次革命使我们可以系统地处理非围扰的量子场论。在超导，超流等研究中，最困难的是处理强耦合的系统。超弦理论因为具有较高的超对称，目前还无法直接应用到超导，超流等系统中。

也许人们会认为，量子引力只在 Planck 尺度以下（10^{-33}cm）才起作用，这个尺度目前和我们没有多大关系。弦论前几年的进展从第一原理导出黑洞熵的公式。这对于超弦理论是强有力的实验支持。

另外，弦理论和数学有极其密切的关系。数学为弦理论提供了很多理想实验

并得到许多令人惊奇的结果。

量子场论和弦论的数学基础

从 70 年代以来，数学和场论及弦理论发生了密切的关系。70 年代中杨振宁先生的关于规范场和微分几何关系的工作。70 年代末指标定理和反常的关系等起了很重要的作用。

在代数的研究中，人们发现无穷维李代数如 Kac-Moody 代数及其表示理论为共形场论及围扰弦理论建立了基础。而由特征标的对偶性质也可建立其它量子场论的对偶性质。Borcherds 将顶点算子数学化和应用到理解例外有限群使他荣获菲尔兹奖。

80 年代，在低维拓扑的研究中有若干重大突破。有些数学事实很难被理解。例如 Donaldson（菲尔兹奖获得者）理论给出 4 维时空有无穷多种微分结构。这些结果被 Witten 在量子场论的框架下得到自然的解释。Donaldson 不变量即是某种 N = 2 超对称 Yang-Mills 场的相关函数。后来从对偶性考虑，Seiberg-Witten 引入新的不变量，使这一理论得到极大的简化。这一对偶性对于研究弦理论中的对偶性有启发性，是引发第二次弦理论革命的重要线索。

还有许多和量子场论有关的工作，例如纽结多项式、模空间的相交理论、椭圆上同调、镜对称等。这些工作大都是通过考虑场论的经典解并考虑附近的量子修正得到的。数学家们抛开物理背景直接从有限维构造这些理论。

我们对这种状况显然不能满意。到目前为止量子场论还没有建立起数学基础。量子场论的考虑可以提供猜测，但无法提供证明。我们希望这种状况能够改变。在量子场论的框架下直接考虑数学问题，使很多问题的理解变得直接明了。

如 Witten 最近在一些文章中所强调的，有两个问题是非常基本的。一个是量子 Yang-Mills 规范场的有限性，这可从渐进自由看出。但是目前数学上还没有证明。另一个是 Yang-Mills 场的质量界猜测，这和夸克幽禁有极其密切的联系。这也是 Clay 研究所提出的 7 个千僖年数学难题。目前这问题最有希望的解答是通过和弦理论的对偶得到。Maldacena 前几年猜测具有极大超对称的以 SU(N) 为规范群的场论和某些以 1/N 为耦合常数的弦论对偶. 这种规范场/引力对偶近两年拓展到 N=2,1 的超对称 Yang-Mills 场论。夸克幽禁问题很可能在不远的将来得到解决。

Witten 建议数学家在作 4 维的量子场论的问题之前作 2 维和 3 维的场论。对于 2 维 Sigma 模型，质量下界对于特定情形已经建立起来。我们应设法拓展到

广泛的情形并得到一些几何上的应用。对于 3 维场论他建议在 Chern-Simons 项前增加 Yang-Mills 项。这种场论的质量也应当是有下界的。

弦理论的对偶性为数学提出许多深刻的问题。例如 Sen 指出弦理论的某些对偶蕴涵某些模空间上调和形式的关系。从物理学家的角度考虑，Seiberg-Witten – Donaldson 的对偶性可从弦论的对偶性解释。Seiberg-Witten – Donaldson 的等价性是富有挑战性的问题。也许我们需要建立某种无穷维的微积分，在这里 BRST 算子相当于无穷维的微分算子。Seiberg-Witten 的工作相当于对于有超对称的特别的 Yang-Mills 场建立了夸克幽禁。

这些问题的实质性进展无疑将量子场论，弦论变为数学的一章。这是我们期待已久的。由于数学和物理长期的隔阂，在国外将两者真正结合起来作研究的也是凤毛麟角。这对于我们来说是个很好的机会。我们希望中国的科学家能在此过程中继续作出贡献。

杨辉三角形的结构特点及其应用

张子宇

所谓的“杨辉三角形”，指的是如下图这样的一个数表。

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
\cdots & & & \cdots & & & & \cdots & & & \cdots
\end{array}
$$

表 1：杨辉三角形

表中除了所有的 1 外，每一个数都等于紧挨在它左上方和右上方两个数之和。

为了简便起见，我们约定，将表中的各行自上而下分别称为第 0 行，第 1 行，第 2 行，$\cdots\cdots$ 而将第一行中的各数自左至右分别称为第 0 个数，第 1 个数，第 2 个数 $\cdots\cdots$

在这样的约定下，熟知，第 n 行第 k 个数恰为组合数 $\binom{n}{k}$。

命题 1 *杨辉三角中，第 n 行的各数均为奇数的充要条件是 $n=2^r-1.(r\in N\bigcup\{0\})$*

通常的做法是考虑三项式 $(1+x)^{\pi}$，利用同余式 $(1+x)^{2^4}\equiv 1+x^{2^r} \pmod 2$,$r\in N\bigcup\{0\}$ 来证明。本文将通过直接分析杨辉三角的结构特点来证明命题 1 及以下几个命题。

$$
\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & 1 & & 0 & & 1 & & & & & \\
 & & & & 1 & & 1 & & 1 & & 1 & & & & \\
 & & & 1 & & 0 & & 0 & & 0 & & 1 & & & \\
 & & 1 & & 1 & & 0 & & 0 & & 1 & & 1 & & \\
 & 1 & & 0 & & 1 & & 0 & & 1 & & 0 & & 1 & \\
1 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 & & 1 \\
\cdots & & & & \cdots & & & & \cdots & & & & \cdots & & \\
 & & & & & & & & & & & & & & \cdots
\end{array}
$$

表 2：简化的杨辉三角形

我们将表 2 称为“简化的杨辉三角形”，它由数字 0 和 1 的构成，任一位置上的数与杨辉三角形中相应位置上的数同奇偶。我们将表中自第 m 行至第 n 行 $(1 \le m \le n)$ 的全部 0 和 1 所构成的梯形子表记为 E_n^m，同时当 $m = n$ 时，E_n^m 简记为 E。

对较小的 n 可以直接验证。以下对 r 用归纳法证明：当 $2^r \le n < 2^{r+1}$ 时，当且仅当 $n = 2^{r+1} - 1$ 时，E_n 中各数均为 1，这里 $r \in N \bigcup \{0\}$。

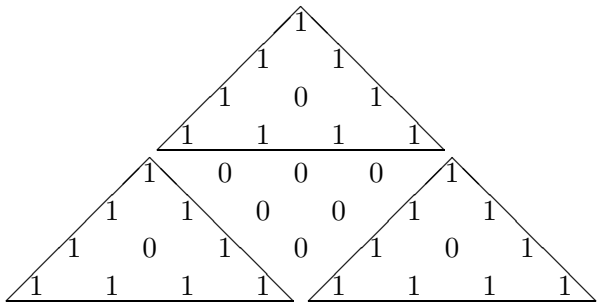


表 3：简化的杨辉三角形的结构特点

设结论对 r-1 成立，于是 E_{2^r-1} 中各数均为 1。考虑 E_{2^r}，由杨辉三角形的构造规则可知 E_{2^r} 中，除了首尾两数为 1 外，其余各数均为 2 个 1 相加而为 0。于是当继续向下构造 E_{2^r+1},E_{2^r+2},$\cdots$,$E_{2^{r+1}-1}$ 时，也就相当于由 2 个并排的 E_0 相互独立地向下构造 E_1,E_2,,$\cdots$,E_{2^r-1}，即 $E_{2^{r+1}-1}^{2^r}$ 相当于 2 个 $E_{2^r-1}^0$ 并排放置并空缺的位置上补满 0。此时只须注意到，$E_{2^{r+1}-1}$ 总共有 2^{r+1} 个数，恰好被 2 个 E_{2^r-1} 填满，故 $E_{2^{r+1}-1}$ 中各数均为 1，而 E_{2^r},E_{2^r+1},$\cdots$,$E_{2^{r+1}-2}$ 中分别至少含有 2^r-1,2^r-2,$\cdots$,1 个 0，于是结论对 r 成立。

$r = 2$ 的例子见表 3。

综上所述，命题 1 成立。

命题 2 *$n \in N$, 设 n 的二进制表示中有 S 个 1, 则杨辉三角形中，第 n 行中奇数的个数 $f(n) = 2^s$.*

有了命题 1 的铺垫，命题 2 变得十分简单。首先，因为 $E_{2^{r+1}-1}^{2^r}$ 可看成由 2 个 $E_{2^r-1}^0$ 并列而成，故对 $0 \le m \le 2^r - 1$，第 $m + 2^r$ 行 1 的个数便恰为第 m 行的 2 倍，即：

$$f(m + 2^r) = 2f(m) \tag{1}$$

将 n 写成二进制表示 $n = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_s}$, $k_1 > k_2 > \cdots > k_s \ge 0$, 由 (1) 可得：

$$
\begin{aligned}
f(n) &= f(2^{k_1}+2^{k_2}+\cdots+2^{k_s}) \\
&= 2f(2^{k_2}+2^{k_3}+\cdots+2^{k_s}) \\
&= 4f(2^{k_3}+\cdots+2^{k_s}) \\
&= \cdots \\
&= 2^{s-1}f(2^{k_s}) \\
&= 2^s f(0) \\
&= 2^s
\end{aligned}
\tag{2}
$$

于是命题 2 成立，进而可知，第 n 行中偶数的个数 $g(n)=n+1-2^s$。

命题 3 *在杨辉三角形中，对 $\forall n\in N$, 第 n 行中奇数和偶数的个数不相等。*

这一命题是命题 2 的简单推论。沿用命题中的记号，采用反证法。

设 $g(n)=f(n)=2^s$，则 $n+1=g(n)+f(n)=2^{s+1}$，即 $n=2^{s+1}-1=2^s+2^{s-1}+\cdots+2+1$，也就是说，n 的二进制表示中有 $s+1$ 个 1，矛盾。

利用杨辉三角形这一奇妙的结构特点还可以证明许多有趣的结论，例如：

命题 4 *组合数列 $\binom{n}{0},\binom{n}{1},\cdots,\binom{n}{n}$ 中恰为奇偶数交替出现的充要条件是 $n=2^r-2,r\in N,r\geq 2$.*

命题 5 *组合数列 $\binom{n}{0},\binom{n}{1},\cdots,\binom{n}{n}$ 中恰有 1 个偶数的充要条件是 $n=2$; 恰有 2 个偶数的充要条件是 $n=5$; 恰有 3 个偶数的充要条件是 $n=4$ 或 6; 恰有 2 个奇数的充要条件是 $n=2^s,s\in N\bigcup\{0\}$。*

杨辉三角形的这一奇妙结构不仅可用于解决组合数的奇偶性问题，还可以用于讨论组合数模 3(或其它数) 的余数。我们姑且将表 2 称为 “mod2 简化的杨辉三角形”，类似地，以下我们简单地讨论一下 “mod3 简化的杨辉三角形” 的结构特点。

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 0 & & 0 & & 1 & & & \\
 & & 1 & & 1 & & 0 & & 1 & & 1 & & \\
 & 1 & & 2 & & 1 & & 1 & & 2 & & 1 & \\
1 & & 0 & & 0 & & 2 & & 0 & & 0 & & 1 \\
\cdots & & & & \cdots & & & & \cdots & & & & \cdots
\end{array}
$$

表 4：mod 3 简化的杨辉三角形

我们仍沿用命题 1 证明中的记号。只不过下文中的 $E_n^m(0 \le m \le n)$ 将代表表 4 中第 m 行至第 n 行所有数所构成的子表。同时，我们用 $\widehat{E}_n^m$ 来表示将 E_m^n 中所有 1 换成都市 2，所有 2 换成 1，而将所有 0 仍保留后所得到的一张“反表”。

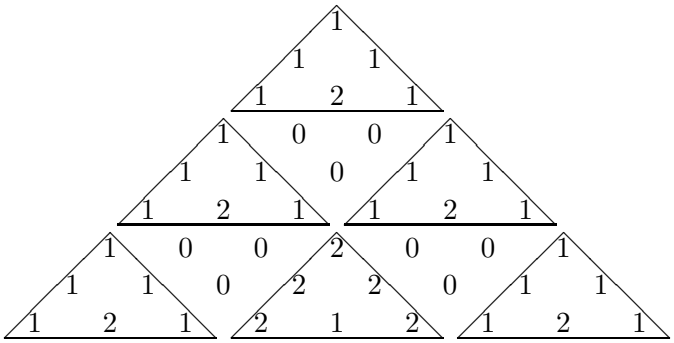


表 3：mod 3 简化的杨辉三角形的结构特点

我们很容易证明出（甚至观察到）若已给定了 $E_{3^r}^0$，注意到第 3^r-1 行的数字规律便知：将 2 个 $E_{3^r-1}^0$ 并列放置并将空缺处填满。即得到 $E_{2\cdot 3^r-1}^{3^r}$，将 $E_{3^r-1}^0$,$\widehat{E}_{3^r-1}^0$,$E_{3^r-1}^0$ 依次并列放置并将空缺处填满 0，即得到 $E_{3^{r+1}-1}^{2\cdot 3^r}$。至此便完成了由 $E_{3^r-1}^0$ 向 $E_{3^{r+1}-1}^0$ 的过渡。具体的证明过程这里不再赘述。$r=1$ 的例子如表 5 所示。

命题 6 *在杨辉三角中，对 $\forall n \in N \bigcup \{0\}$，设第 n 行中模 3 余 1 和余 2 的数的个数分别为 $A(n)$,$B(n)$，则 $A(n) > B(n)$。*

对较小的 n 可以直接验证。假设 $0 \le n \le 3^r-1(r \in N)$ 时结论成立，则由 mod3 简化的杨辉三角形的结构特点可以得到类似 (1) 那样的递推公式：对 $0 \le m \le 3^r-1$,

$$A(m+3^r) = 2A(m) \tag{3}$$

$$B(m+3^r) = 2B(m) \tag{4}$$

$$A(m+2\cdot 3^r) = 2A(m)+B(m) \tag{5}$$

$$B(m+2\cdot 3^r) = A(m)+2B(m) \tag{6}$$

进而由 (3),(4),(5),(6) 分别可以得到：

$$A(m+3^r) = 2A(m) > 2B(m) = B(m+3^r)$$

$$A(m+2\cdot 3^r) = 2A(m)+B(m) > A(m)+2B(m) = B(m+2\cdot 3^r)$$

于是命题已对 $0 \le n \le 3^{r+1}-1$ 成立。

进一步地，由公式 (3),(4),(5),(6) 可仿照命题 2 那样直接推得杨辉三角形第 n 行中模 3 余 1 和余 2 的数的个数，即下面的命题 7。

命题 7 $n \in N$, 设 n 的三进制表示中有 S_1 个 *1*, S_2 个 *2*, 则杨辉三角形第 n 行中模 *3* 余 *1* 和余 *2* 的数的个数分别为:

$$A(n) = 2^{S_1-1}(3^{S_2}+1);$$

$$B(n) = 2^{S_1-1}(3^{S_2}-1).$$

具体证明过程这里略去。

类似地, 我们还可以证明其它一些有趣的命题, 例如:

命题 8 组合数列 $\binom{n}{0},\binom{n}{1},\cdots,\binom{n}{n}$ 中所有数模 *3* 均余 *1* 的充要条件是 $n=0$ 或 1.

命题 9 组合数列 $\binom{n}{0},\binom{n}{1},\cdots,\binom{n}{n}$ 中所有数模 *3* 的余数恰为 *1*, *2* 交替出现的充要条件是 $n=3^r-1(r\in N)$.

命题 10 组合数列 $\binom{n}{0},\binom{n}{1},\cdots,\binom{n}{n}$ 中恰有一个数模 *3* 余 *2* 的充要条件是 $n=2\cdot 3^r, r\in N\bigcup\{0\}$; 恰有 *2* 个数模 *3* 余 *2* 的充要条件是 n 的三进制表示中恰有一个 *1* 和一个 *2*, 而其余各位均为 *0*; 恰有 *2* 个数模 *3* 余 *1* 的充要条件是 $n=3^r$ 或 $2\cdot 3^r, r\in N\bigcup\{0\}$。

****

[幽你一默]

物理学家、生物学家和数学家

一个数学家, 生物学家和物理学家坐在露天咖啡座上, 悠闲的看着对街商店的人来人往。

首先他们看到两个人走进商店, 过了一会儿发现却有三个人走出来; 三个朋友就他们的专业发表了彼此的看法:

物理学家: 这证明了测不准原理。

生物学家: 这些人自我繁殖了。

数学家: 若现在再有一人进入此商店则里面将空无一人。

An Application of Rolle Theory

0001 Huang Xiangdi

I. Introduction

In this paper we show some applications of Rolle theory and establish our theorem.

First we define some symbols as follows:

Suppose $P(x)$ is a polynomial real roots,and has the following factorizations:

$$P(x) = \prod_{i=1}^{k}(x - x_i)^{a_i}(a_i \in N)$$

where x_i are distinct real roots satisfying:

$$\sum_{i=1}^{k} a_i = n$$

We don't recount the meanings of the symbols in the following paragraph.

Now let's show the main theory of this paper:

Theorem 1 (Cauchy-Schwartz Inequality) *Let* $\{a_1, a_1, ...a_m\}$ *and* $\{b_1, b_2, ...b_m\}$ *be any two sets of real numbers.Then*

$$(\sum_{i=1}^{m} a_i b_i)^2 = (\sum_{i=1}^{m} a_i)^2(\sum_{i=1}^{m} b_i)^2 - \sum_{j=1}^{m}\sum_{i=1}^{m}(a_i b_j - a_j bi)^2/2$$

Consequently,

$$(\sum_{i=1}^{m} a_i b_i)^2 \leq (\sum_{i=1}^{m} a_i^2)(\sum_{i=1}^{m} b_i^2)$$

Theorem 2 (Rolle Theory) *Assume* f *is continuous on* $[a, b]$*, and is differentiable on* (a, b) *satisfying* $f(a) = f(b)$*,then there exists* $\xi \in (a, b), f(\xi) = 0$*. Since the proof of the theorems is classical, we aim at the application of the theory in this paper.*

II. Applications

We show our application of Rolle theory.

Suppose $x_1, x_2, ...x_n$ are $n(\geq 2)$ different real numbers,then the following equation

$$(\sum_{i=1}^{n} \frac{1}{x - x_i})^2 = r \sum_{i=1}^{n} \frac{1}{(x - x_i)^2} \tag{1}$$

1. has only n-2 different real roots,when $r = 1$.
2. has only 2n-2 different real roots,when $0 < r < n$ and $r \neq 1$.
3. has no real roots,otherwise.

Proof: Observe that x_i are not the root of the equation, we may convert the equation into a polynomial equation by multiplying(1)

$$\prod_{i=1}^{n} (x - x_i)^2$$

this will not damage the property of the root. III.has no real roots,otherwise.

In order to prove our theory, we introduce some main lemmas as follows:

Lemma 1 *Suppose $P(x)$ has n different real roots,then $P'(x)$ has n-1 real roots.*

Proof:Suppose $x_1, x_2, \cdots, x_n$ are n different real roots of $P(x)$, then with out loss of generality, We assume $x_1 < x_2 < \cdots < x_n$ and $P(x_1) = P(x_2) = \cdots = P(x_n) = 0$ Applying the Rolle theory, we have

there exist n-1 real numbers satisfying:

$$P'(\xi_i) = 0(1 \leq i \leq n - 1), \xi_i \in (x_i, x_{i+1})$$

Observe that (x_i, x_{i+1}) are different intervals,thus

$$\xi_i \in (x_i, x_{i+1})(1 \leq i \leq n - 1)$$

are n-1 different real roots of $P'(x)$.

Lemma 2 *Suppose $P(x)$ has n real roots (multiply roots included), then $P'(x)$ has n-1 real roots.*

Proof:Suppose

$$P(x) = \prod_{i=1}^{k} (x - x_i)_i^a (a_i \in N)$$

$$\sum_{i=1}^{k} a_i = n$$

$$x_1 < x_2 < \cdots < x_k$$

It's easy to show that

$$P(x_i) = P'(x_i) = \cdots = P^{(a_i-1)}(x_i) = 0$$

Then x_i is the $a_i - 1$ multiply roots of $P(x)$, again we apply Rolle theory, implying $P(x_i) = ... = p(x_k) = 0$ there existing k-1 different real numbers $\xi_1, \xi_2, \cdots, \xi_{k-1}$, $\xi_i, \in (x_i, x_{i+1})$,

$$P'(\xi_1) = P'(\xi_2) = \cdots = P'(\xi_{k-1}) = 0$$

Thus $P'(x)$ has $\sum_{i+1}^{k}(a_i - 1) + k - 1 = n - k + k - 1 = n - 1$ real roots,multiply roots included.

Lemma 3 *Suppose $P(x) = \prod_{i=1}^{n}(x - x_i)$, we have*

1.

$$P'(x) = P(x)(\sum_{i}^{n} \frac{1}{x - x_i})$$

2.

$$p''(x) = P(x)(\sum_{i=1}^{n} \frac{1}{x - x_i})^2 - \sum_{i=1}^{n} \frac{1}{(x - x_i)^2})$$

Proof: According to the Leibnitz formula, it's easy to compute the consequence step by step.Here we leave it to readers.

Lemma 4 *Suppose $F(x) = \frac{P(x)^s}{Q(x)^t}$, where $P(x) = \prod_{i=1}^{n}(x - x_i), Q(x) = \prod_{i=1}^{m}(x - y_i)$, x_i, y_i are $m + n$ different real numbers, s, t are integers.*

Denote $G(x) = sP'(x)Q(x) - tP(x)Q'(x)$ Then we have: $G(x) = 0$ has $m + n - 1$ different real roots.

Proof:According to Lemma 3,

In order to solve $G(x) = 0$, we need only to solve

$$s\sum_{j=1}^{n} \frac{1}{x - y_i} = t\sum_{i=1}^{n} \frac{1}{x - x_i}$$

we write $W(x) = s\sum j = 1^n \frac{1}{x-y_j} - t\sum_{i=1}^{m} \frac{1}{x-x_i}$, it's easy to find that.

Notice that

$$W(x_i+) = W(y_j-) = -\infty \quad , \quad W(x_i-) = W(y_j+) = +\infty \qquad (*)$$

Since $W(x)$ is continuous at $R\backslash\{x_1, \cdots, x_m, y_1, \cdots, y_n\}$, leaving out the break point, we array the sequence of $x_1, ...x_m, y_1, \cdots, y_n$ according to the real value.

From (*), we can select $m+n-1$ different real numbers satisfying $W(x)=0$

Thus, $W(x)$ has $m+n-1$ different real roots.

Now let's begin our proof.

1. Recall(1), since the left is nonnegative so the right must be nonnegative, we conclude r must be a positive number to make sense, that is if r be negative, we won't have any real roots of the equation.
2. r should be less than n.

$$r\sum_{i=1}^{n}\frac{1}{(x-x_i)^2}=(\sum_{i=1}^{n}\frac{1}{x-x_i})^2\leq(\sum_{i=1}^{n}\frac{1}{|x-x_i|})^2\leq n\sum_{i=1}^{n}\frac{1}{(x-x_i)^2}$$

Hence we have $r\leq n$ The equality holds if and only if x_i are the same, which is a contradiction to the assumption.

3. assume $0<r\leq 1$, and r is a rational number. Form (1) and Lemma 3, we have the following equality:

$$P(x)P''(x)=(r-1)P'(x)^2 \tag{2}$$

if $r=1$, (1) implies $P''(x)=0$. Apply the Lemma 2 twice, we have

(a) has n-2different real roots when r=1

(b) Otherwise, let $r=\frac{s}{t}<1$, where s,t are intergers.Then

$$G(x)=tP(x)P''(x)+(t-s)P'(x)^2=0 \tag{3}$$

Denote

$$F(x)=P(x)^{t-s}P'(x)^t$$

$F(x)$ is a polynomial with degree $n(t-s)+(n-1)t$, and its roots are consisted of all real numbers,derived from Lemma 2.

Then

$$F'(x)=P(x)^{t-s-1}P'(x)^{t-1}G(x)$$

Apply Lemma 2, $F'(x)=0$ has $n(t-s)+(n-1)t-1$ real roots. Observe that $P(x)^{t-s-1}P'(x)^{t-1}=0$ has $n(t-s-1)+(n-1)(t-1)$ real roots, so we conclude $G(x)$ has $2n-2$ real roots. Also repeat the proof of Lemma 2, it's easy to show that the $2n-2$ real roots of $G(x)$ are different. In fact, they are the different ξ_is.

4. Assume $1<r<n$, and r is a rational number. Let $r=\frac{s}{t}>1$, where s,t are integers.

Denote $Q(x)=p'(x), G(x)=tP(x)P''(x)-(s-t)P'(x)$

According to Lemma 4 $G(x)$ has $2n-2$ different real roots.

5. r is a real number, so there exists a sequence of rational numbers $\{r_i\}_{i=1}^{\infty}$ satisfying: $\lim r_i = r, (i \to \infty)$

   Denote a sequence of functions as follows:

$$f_i(x) = P(x)P''(x) - (r_i - 1)P'(x)^2$$

$$f(x) = P(x)P''(x) - (r - 1)P'(x)^2$$

then $f_i(x)$ converges uniformly to $f(x)$ on any compact sets, that is $f_i(x)$ satisfies the Closed Converging Theorem, according to the Real Hurwitz Theorem,For any curve γ,if $f_x = 0$ has no root at the margin of γ. the number of real roots of $f_i(x)$ is the same to the one of $f(x)$ in the inner part of γ.But from 3,and 4, $f_i(x)$ has $2n - 2$ different real roots. thus the result holds.

III. Corollary

We may not suppose x_i are different, then similar to the proof of the theorem,the following equation:

$$\left(\sum_{i=1}^{k} \frac{a_i}{x - x_i}\right)^2 = r \sum_{i=1}^{k} \frac{a_i}{(x - x_i)^2}$$

$$\sum_{i=1}^{k} a_i = n(a_i \in N)$$

where $x_1, x_2, ...x_k$ are different.

1. has only $n - 2$ real roots, when $r = 1$.
2. has only $2n - 2$ real roots, when $0 < r < n$ and $r \neq 1$.
3. has no real roots,otherwise.

图论中的几个小问题

0001 卢献

我们在学习图论时通常是把无向图当作有向图的特殊情形来处理的，但有时这样是不对的。例如无向图和有向图的线图的定义就是不一样的，它们的直径的意义也不同，这个时候就不能把无向图的线图和直径当作特殊有向图的线图和直径来对待。下面第一部分对几个简单问题的讨论可以澄清两种图在某些概念上的区别，也可以加深对这些概念和结论的理解；第二部分是我在学习代数图论时的一点小收获，求出这两种 Johnson 图的距离公式对学习它的结构很有帮助，例如可以很快知道它们的 intersection array。

§1　有向图与无向图的几点区别

1. G 为无向连通图，则 $L(G)\cong G$ 当且仅当 G 为 C_n。

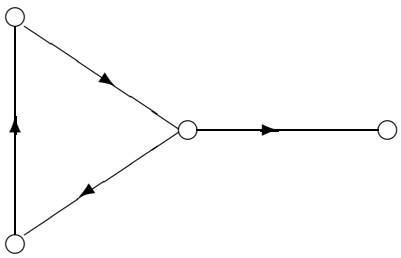
证明：首先，显然有当 G 为 C_n 时 $L(G)\cong G$。反过来，若 $L(G)\cong G$ 则 $\varepsilon(L)=\varepsilon(G)$。又有 $\varepsilon(G)=\nu(L)\,,\nu(L)=\nu(G)$，所以 $n=\nu(G)=\nu(L)=\varepsilon(G)=\varepsilon(L)\Rightarrow G,L(G)$ 中都只有含一个圈。设 G 中的圈为 C，若存在 $z\in\nu(G-C)$，由于 G 连通，则必存在 $x\in V(C)$ 使得 $xz\in E(G)$。记在 C 中与 x 相邻的点为 x_1,x_2，那么在 $L(G)$ 中 (xz,xx_1,xx_2,xz) 形成一个圈，$L(G)$ 中便至少含有了 2 个圈，矛盾，所以 G 为 C_n。

2. G 为有向连通图，若 $L(G)\cong G$ 则 G 中含有唯一的一个圈，且此圈为有向圈；但此时 G 并不一定为 C_n；当 G 为强连通图时 $L(G)\cong G$ 当且仅当 G 为 C_n。

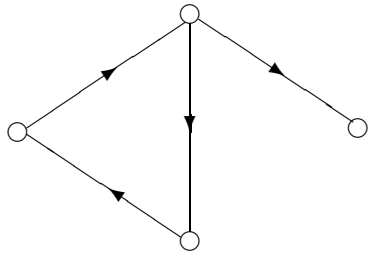
证明：同上有 $\nu(G)=\nu(L)=\varepsilon(G)=\varepsilon(L)$，所以 G 中含有唯一的圈 C，$L(G)$ 中也相应地含有唯一的圈 $\tilde{C}$。显然有 $C\cong\tilde{C}$。反设 $\tilde{C}$ 不为有向圈，则存在 $a,b\in V(\tilde{C})$ 满足 $d^+_{\tilde{C}}(a)=2$、$d^-_{\tilde{C}}(a)=0$、$d^+_{\tilde{C}}(b)=0$、$d^-_{\tilde{C}}(b)=2$。设 $N^+_{\mu G}(a)\bigcap V(\tilde{C})=\{a_1,a_2\}$，$N^-_{\mu G}(b)\bigcap V(\tilde{C})=\{b_1,b_2\}$，于是 $\mathrm{head}(a)$=$\mathrm{tail}(a_1)$=$\mathrm{tail}(a_2)$，$\mathrm{tail}(b)$= $\mathrm{head}(b_1)$=$\mathrm{head}(b_2)$。因为 $\mathrm{length}(\tilde{C})$=$\left|V(\tilde{C})\right|$，$\mathrm{length}(C)$=$|E(C)|$，而 $a,a_1,a_2,b,b_1,b_2\in V(\tilde{C}),a,a_1,a_2,b,b_1,b_2$ 分别有一个不在 $E(C)$ 中，于是 $\left|V(\tilde{C})\right|>|E(C)|$，这与 $\mathrm{length}(\tilde{C})$=$\mathrm{length}(C)$ 矛盾，所以 $\tilde{C}$ 是有向圈。又因为 $C\cong\tilde{C}$，C 也为有向圈。

例 1:

G :



$L(G)$:



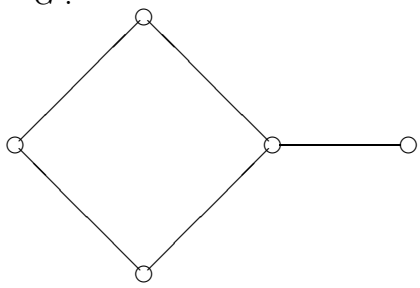
可以看出 $L(G) \cong G$ 时 G 并不一定为 C_n。

3. 若 G 为无向连通图，则有 $d(G)-1 \le d(L(G)) \le d(G)+1$。

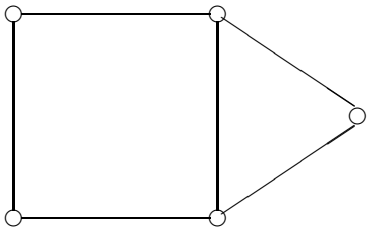
证明：设 $a,b \in E(G)$ 且 $d_L(a,b)=d(L)$，设此 ab-path 为 $ae_1e_3\cdots e_{d(L)-1}b$，$a=x'x$、$e_1=xx''$、$e_{d(L)-1}=y''y$、$b=yy'$，其中 $x,x',x'',y,y',y'' \in V(G)$。这条路径也是 G 中最短的 xy-path。于是 $d(G) \ge d_G(x,y) \ge d(L)-1$，即 $d(L) \le d(G)+1$。另一方面，设 $x,y \in V(G)$ 且 $d_G(x,y)=d(G)$。设此 xy-path 为 $xx_1x_2\cdots x_{d(G)-1}y$，这条路径也是 $L(G)$ 中 xx_1 与 $x_{d(G)-1}y$ 最短路径。于是 $d(L) \ge d_L(xx_1, x_{d(G)-1}y)=d(G)-1$，即 $d(G)-1 \le d(L)$。

例 2:

G :

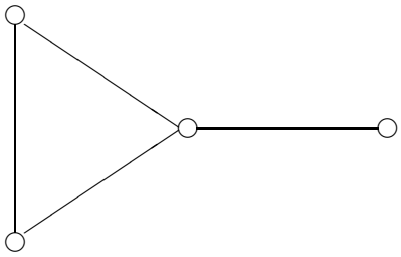


$L(G)$:

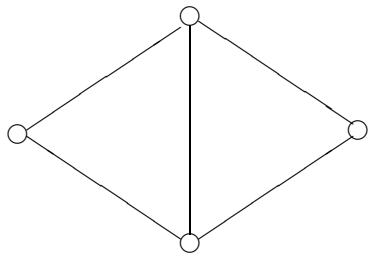


例 3:

G :

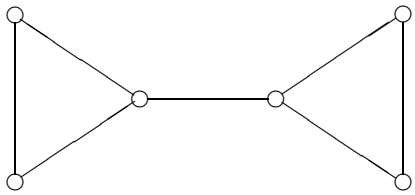


$L(G)$:

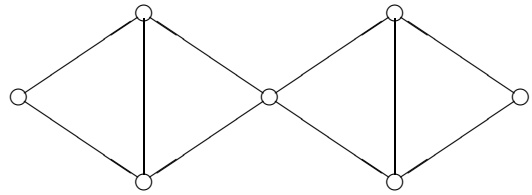


例 4:

$G:$



$L(G):$



例 2、例 3、例 4 中分别有 $d(L)=d(G)-1$、$d(G)$、$d(G)+1$，这说明 $d(L)$ 可以取到 $d(G), d(G)\pm 1$。

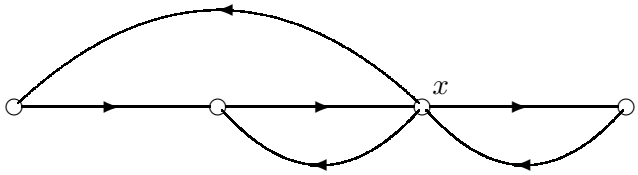
4. 当 G 为强连通图时，$d(G)\le d(L)\le d(G)+1$，$d(G)=d(L)$ 当且仅当 G 为有向圈。但是从上面的讨论看出无向图并无此性质。

5. 若 G 是无向连通图，则有 $\mathrm{rad}(G)\le d(G)\le 2\mathrm{rad}(G)$。

证明：记 $\rho(x)=\max\limits_{y\in V(G)}\{d_G(x,y)\}$，则 $\mathrm{rad}(G)=\min\limits_{x\in V(G)}\{\rho(x)\}$、$d(G)=\max\limits_{x\in V(G)}\{\rho(x)\}$。设 $x_0,y_0\in V(G)$，且 $d(x_0,y_0)=d(G)$。那么对于 $\forall x\in V(G)$ 有 $\max\limits_{y\in V(G)}\{d(x,x_0),d(x,y_0)\}\ge \frac{1}{2}d(G)$。若不然，$d(x,x_0),d(x,y_0)<\frac{1}{2}d(G)$，$d(x_0,y_0)\le d(x_0,x)+d(x,y_0)<d(G)$，矛盾。所以 $\rho(x)\ge\frac{1}{2}d(G),\forall x\in V(G)\Rightarrow \mathrm{rad}(G)=\min\limits_{x\in V(G)}\{\rho(x)\}\ge\frac{1}{2}d(G)$，即 $d(G)\le 2\mathrm{rad}(G)$。

6. 若 G 是有向强连通图却不一定有 $d(G)\le 2\mathrm{rad}(G)$，反例如下：

例 5：下图中显然 $d(G)$=3，但 $\rho(x)=1$，于是 G $=1$。



§2 两种 Johnson 图的距离公式

Johnson 图是代数图论中一类重要的图，下面计算两种 Johnson 图的距离公式作为练习。

1. Johnson 图 $J(v,k,k-1)$ 中任意两点间的距离：$d(A,B)=k-1$，其中 $|A\bigcap B|=i$。

解：先证明两个结论，以下记 $J=J(v,k,k-1)$。

结论 1：若 J 中有一条长为 s 的 AB-path，则 $|A\bigcap B|\ge k-s$。对 s 进行归纳，$s=1$ 时有定义假设成立；假设 $s=m$ 时结论成立，$s=m+1$ 时记这条长为 $m+1$

的 AB-path 为 $AC_1\cdots C_mB$。由假设知 $|A\bigcap C_m|\geq k-m$，而 $|c_m\bigcap B|=k-1$，又由于 $|A|=|B|=|C_m|=k$，所以 $|A\bigcap B|\geq|A\bigcap B\bigcap C_m|\geq|A\bigcap C_m|-1\geq k-(m+1)$，于是结论 1 成立。

结论 2：若 $|A\bigcap B|=k-i$，则 J 中存在一条长为 i 的 AB-path。事实上 $|A-B|=|B-A|=i$。任取 $a_1\in B-A, b_1\in A-B$，记 $C_1=A\bigcup\{a_1\}-\{b_1\}$，则 $|A\bigcap C_1|=k-1, |B\bigcap C_1|=k-i+1$，同样，取 $a_{j+1}\in B-C_j, b_{j+1}\in C_j-B$，记 $C_{j+1}=C_j\bigcup\{a_{j+1}\}-\{b_{j+1}\}(j=1,2,\cdots,i-1)$。易知 $|C_{j+1}\bigcap C_j|=k-1, |C_{j+1}\bigcap B|=k-(i-j-1)$，因此 $C_i=B$，$AC_1\cdots C_{i-1}B$ 是 J 中长为 i 的 AB-path，结论 2 成立。

已知 $|A\bigcap B|=i$，由结论 2 知 J 中存在长为 $k-i$ 的 AB-path，故 $d(A,B)\leq k-i$。如果这条路径不是 A,B 间的的最短路径，那么一定存在长为 $k-s$ 的 AB-path，其中 $s>i$。由结论 1 知 $|A\bigcap B|\geq s$，矛盾。所以 $d(A,B)=k-i$ 反过来也可以看出若 $d(A,B)=i$，则 $|A\bigcap B|=k-i$。

2. Johnson 图 $J(2k+1,k,0)$ 中任意两点间的距离：

$$d(A,B)=\begin{cases}2i+1, & 2i<k\\ 2(k-i), & 2i\geq k\end{cases}，其中 i=|A\cap B|$$

解：记 $J=J(2k+1,k,0)$。对 $\forall A,B\in V(J)$ 且 $|A\bigcap B|=i,(0\leq i\leq k-1)$。记集合 $N^{j+1}(A)=N_n(N^j(A))$，特别地有 $N^0(A)=A$；记集合 $N_i=\{i|\exists C\in N^j(A)s.t.|B\bigcap C|=i\}$，特别地有 $N_0=\{i\}$。可以看出 $N^j(A)$ 为 J 中所有与 A 的距离不超过 i 的点的集合，N_j 为 $N^j(A)$ 中的元素与 B 的交集的势的集合。由于

$$|A\bigcap B|=i,\left|\bigcup_{A\in V(J)}A-A\bigcup B\right|=i+1,|B-A|=k-i$$

所以 $N^1(A)$ 中所有 $i+1$ 个元素与 B 的交集的势为 $k-i$，有 $k-i$ 个元素与 B 的交集的势为 $k-i-1$，即 $N_1=\{k-i,k-i-1\}$。以此递推可知 $N_{2\alpha}=\{i-\alpha,i-\alpha+1,\cdots,i+\alpha\}$，$N_{2\alpha+1}=\{k-i-(\alpha+1),k-i-\alpha,\cdots,k-i+\alpha\}$，其中 $\alpha=0,1,\cdots$。于是 $d(A,B)=\min\{j|k\in N_j\}$。若 $d(A,B)=2\alpha$，则 $i+\alpha=k\Rightarrow\alpha=k-i, d(A,B)=2(k-i)$，此时有 $k\notin N_{2\alpha-1}\Rightarrow k-i+\alpha-1<k\Rightarrow 2i\geq k$；若 $d(A,B)=2\alpha+1$，则 $k-i+\alpha=k\Rightarrow\alpha=i\Rightarrow d(A,B)=2i+1$，此时有 $k\notin N_{2\alpha}\Rightarrow i+\alpha<k\Rightarrow 2i<k$。综上所述可得到距离公式。

A problem in the group theory

pb00012015 Song Qijiang

As we see: if G is finite, $U \leq V \leq G$, then it is immediate by Lagrange's theorem that $|G : U| = |G : V||V : U|$. suppose now that G is infinite but that $|G : U| < \infty$, with $U \leq V \leq G$ as before, Is it still true that $|G : U| = |G : V||V : U|$? we need some Lemmas to answer this question.

Lemma 1 *Let $U \leq G$ have finite index, then there exists a normal subgroup N of G and $N \subseteq U$.*

proof.Let G act by right multiplication on the set $\Omega = \{Ux|x \in G|\}$ and let N be the kernel of this action (define the map $\theta : G \to Sym(\Omega)$ by $\theta(g) = \pi_g \in Sym(\Omega)$ where $\pi_g : \Omega \to \Omega$ by $\pi_g(Ux) = Uxg$. It's clear that θ is a homomorphism $N = Ker\theta$) So $N \lhd G$, To see that $N \subseteq U$, observe that if $x \in N$,then since $U \in \Omega$, we have $x \in Ux = U\dot{x} = U$ where the last equality holds by the definition of the kernel of the action. So $N \subseteq U$.

Lemma 2 *Let $\varphi : G \to H$ be a surjective homomorphism and let $N = Ker\varphi$. Define the following sets of subgroups: $S = \{U|N \subseteq U \subseteq G\}$ and $T = \{V|V \subseteq H\}$ Then φ and φ^{-1} are inverse bijections between S and T.*

Furthermore $U_1 \leq U_2 \Longleftrightarrow V_1 \leq V_2$ and in this case $|U_2 : U_1| = |V_2 : V_1|$ (suppose $U_1, U_2 \in S, V_1, V_2$ are the corresponding elements of T)

proof.It's clear that φ and φ^{-1} do define maps between S and T and we need to show that they are inverses of each other. For $U \in S$, it's immediate from the definitions that $U \subseteq \varphi^{-1}\varphi(U)$ If $g \in \varphi^{-1}(\varphi(U))$.then $\varphi(g) \in \varphi(U)$ and $N_g = N_u$ for some $u \in U$ $(\varphi(x) = \varphi(y)\ iff\ N_x = N_y$. Thus, $g \in N_u \subseteq U$ since $N \subseteq U$ and we have $\varphi^{-1}(\varphi(U)) = U$.

Now let $V \in T$, clearly $\varphi^{-1}(\varphi(V)) \subseteq V$. if $v \in V$,then since φ is surjective,there exists $g \in G$ with $\varphi(g) = v$. Thus, $g \in \varphi^{-1}(V)$ and $v = \varphi(g) \in \varphi(\varphi^{-1}(V))$ now we have $\varphi(\varphi^{-1}(V)) = V$, and so φ and φ^{-1} are indeed inverse bijections.

Now suppose $U_1 \subseteq U_2$,with $U_i \in S, i = 1, 2, \ldots$ and $V_i = \varphi(U_i), U_i = \varphi^{-1}(V_i)$. We construct a bijection form $\{U_1x|x \in U_2\}onte\{V_1z|z \in V_2\}$. Note that $\varphi(U_1x) = V_1\varphi(x)$ and so φ maps cosets to cosets. To show that this map is surjective, Let $z \in V_2$, then $z = \varphi(x)$ for some $x \in U_2$, and we have $\varphi(U_1x) = V_1z$.

Finally, if $\varphi(U_1x) = \varphi(U_2y)$ for $x, y \in U_2$. we have $V_1\varphi(x) = V_1\varphi(y)$, and so $\varphi(x)\varphi(y)^{-1} \in V_1$. Thus $\varphi(xy^{-1}) \in V_1$ and $xy^{-1} \in \varphi^{-1}(V_1) = U_1$. Therefore, $x \in U_1y$ and $U_1x = U_1y$. This shows that the map is injective, and the proof is complete.

Up to now ,we can answer the question:

If we write $\overline{G} = G/Nand\overline{U}, \overline{V}$ denote the images of U and V under the canonical homomorphism $G \to \overline{G}$. Since $\overline{G}$ is finite, we have $|\overline{G} : \overline{U}| = |\overline{G} : \overline{V}||\overline{V} : \overline{U}|$. However,$|\overline{G} : \overline{U}| = |G : U|$ by Lemma 2.Similarly $|\overline{G} : \overline{V}| = |G : V|$ and $|\overline{V} : \overline{U}| = |V : U|$. But $|\overline{G} : \overline{U}| = |\overline{G} : \overline{V}||\overline{V} : \overline{U}|$, So we have $|G : U| = |G : V||V : U|$, and complete this article.

参考文献

[1] I. Martin Isaacs, *A*lgebra
[2] Fong Keqing, *M*odern algebra
[3] Liu Shaoxue, *M*odern algebra

****

[幽你一默]

消　防

一天，数学家觉得自己已受够了数学，于是他跑到消防队去宣布他想当消防员。消防队长说："您看上去不错，可是我得先给您一个测试。"

消防队长带数学家到消防队后院小巷，巷子里有一个货栈，一只消防栓和一卷软管。消防队长问："假设货栈起火，您怎么办？"数学家回答："我把消防栓接到软管上，打开水龙，把火浇灭。"

消防队长说："完全正确！最后一个问题：假设您走进小巷，而货栈没有起火，您怎么办？"数学家疑惑地思索了半天，终于答道："我就把货栈点着。"消防队长大叫起来："什么？太可怕了！您为什么要把货栈点着？"数学家回答："这样我就把问题化简为一个我已经解决过的问题了。"

关于酉相似的一个判定方法

0001 蔡云峰

给定两个矩阵，我们可以通过把其化为 Jordan 标准型，来判断它们是否相似。然而，对给定的两个矩阵，我们是否有方法来判断它们是否酉相似？通过这篇文章，我们可以知道答案在理论上是肯定的，虽然对待实际问题不太实用。

在参考文献 [1] 中，有如下结论：

定理 1 如果矩阵 $A, B \in M_n$ 酉相似，则有

$$\sum_{i,j=1}^{n} |b_{i,j}|^2 = \sum_{i,j=1}^{n} |a_{i,j}|^2 \tag{1}$$

证：略。

上述定理说明 $trAA^*$ 是酉相似不变量。

两个矩阵酉相似，意味着相似，但反之却不成立。例如:

$$\begin{pmatrix} 3 & 1 \\ -2 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}.$$

相似，但却不是酉相似的。

定理中给予我们判定酉相似的一个必要条件，从中我们可以得到启示，从而可以得到判定酉相似的充分条件。

假设 s, t 是两个不可交换的变量。我们把型如

$$W(s,t) = s^{m_1} t^{n_1} s^{m_2} t^{n_2} \cdots s^{m_k} t^{n_k}, \quad m_1, n_1, \cdots m_k, n_k \geq 0 \tag{2}$$

的称为关于 s, t 的一个字 (word)。把非负整数

$$m_1 + n_1 + m_2 + n_2 + \cdots + m_k + n_k \tag{3}$$

称为 $W(s,t)$ 的阶数 (degree)。

给定矩阵 $A \in M_n$，我们定义关于 A, A^* 的字如下:

$$W(A, A^*) = A^{m_1}(A^*)^{n_1}A^{m_2}(A^*)^{n_2}\cdots A^{m_k}(A^*)^{n_k}. \tag{4}$$

如果矩阵 $A, B \in M_n$ 酉相似，则存在酉方阵 U，使得

$$A = UBU^* \tag{5}$$

则有：

$$\begin{aligned} W(A, A^*) &= (UBU^*)^{m_1}(UB^*U^*)^{n_1}\cdots(UBU^*)^{m_k}(UB^*U^*)^{n_k} \\ &= UB^{m_1}(B^*)^{n_1}\cdots B^{m_k}(B^*)^{n_k}U^* \\ &= UW(B, B^*)U^* \end{aligned} \tag{6}$$

所以，

$$trW(A, A^*) = trUW(B, B^*)U^* = trW(B, B^*) \tag{7}$$

如果我们取 $W(s,t) = ts$，我们就可以得到定理 1。

如果我们考虑字 $W(s,t)$ 的所有可能，当然这种可能无穷多，我们就可以给出矩阵酉相似的充分条件。

我们给出定理 2 和定理 3。证明这里没有给出。有兴趣的读者可以分别在参考文献 [3], [4] 中找到定理 2 和定理 3 的证明。

定理 2 矩阵 $A, B \in M_n$ 是酉相似的当且仅当 $trW(A, A^*) = tr(B, B^*)$ 对所有字 $W(s,t)$ 成立。其中 s, t 是不可交换的变量。

定理 3 矩阵 $A, B \in M_n$ 是酉相似的当且仅当 $trW(A, A^*) = tr(B, B^*)$ 对所有字 $W(s,t)$ 成立。其中 s, t 是不可交换的变量，且 $W(s,t)$ 的阶数不超过 $2n^2$。

定理 2 中的字 $W(s,t)$ 有无穷多，在应用中是不切实际的，但我们却可以借此来判断两矩阵不是酉相似的。例如

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

是相似的，且满足定理 1 中的等式，但计算 $W(A, A^*) = AA^*A$ 与 $W(B, B^*) = BB^*B$ 的迹，他们是不等的，从而得出不是酉相似的结论。

定理 3 指出，我们只需要对有限的情况进行讨论就可以了。然而定理 3 中的上限是保守的。例如，对 $n = 2$ 的情况，我们只需考虑 $W(s,t) = s, s^2, ts$，3 种情况而不必是 $2 \times 2^2 = 8$ 种。对 $n = 3$，我们只需考虑 $W(s,t) = s, s^2, ts, s^3, ts^2, t^2s^2, tsts, ts^2ts, ts^2t^2s$，9 种情况，而不必是 $2 \times 3^2 = 18$ 种情况。

参考文献

[1] 线形代数 李炯生, 查建国

[2] Matrix analysis ROGER A.HORN, CHARLES R.JOHNSON, CAMBRIDGE UNIVERSITY PRESS

[3] W.Specht, "Zur Theorie der Matrizen II," Jahresbericht der Deutsxhen Mathematiker Vereinigung 50 (1940),19-23.

[4] C.Pearcy, "A Complete Set of Unitary Invariants for Operators Generating Finite W -Algebras of Type I,", Pacific J. Math 12 (1962) ,1405-1406.

****

[趣味数学]

数字陷井

介绍给你一个十分简单但又有趣的游戏：任意写下一正整数。如果偶数，把它除于 2：如是奇数，乘 3 加 1。对每次算得的结果，也用上面两条法则去处理，继续下去，你会发现，最后会进入一个“圈子”：4, 2, 1, 4, 2, 1.....

例如，你先写下 7，根据法则，乘 3 加 1，写下 22。现是偶数，根据法则，除于 2，写下 11。即写出：7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1·····，进入“圈子”了。有人从 1 一直写到 60, 000, 000，发现无一整数例外。

如果允许你写下任意一个负整数，而两条法则不改变，你试试看，结果怎样？

****

[趣味数学]

特制扑克

有一副奇怪的扑克牌，共有 45 张，1 点（A）有 1 张：2 点有 2 张.....9 点有 9 张。搅和以为背面放在桌上，让某人来秘密地抽一张。

你问他几个问题，他只回答是或非，设法把他手中的点数问出来。你怎样使你必须问的问题数目尽可能地少？

请注意，我们要找的是无论他选到什么牌都能问出的通用程序。如你设计的第一个问题是：“你的牌是不是 5 点？”那么当他的牌正是 5 点时，你一次就问出来了。但这不是通用程序，因为如若不是 5 点，你的第一个问题起的作用就太小了。

CIP 方法简介及其隐式格式的一个改进

0001 李元

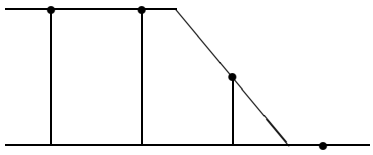
§1 CIP 简介

CIP 是一种偏微分方程数值方法。因为格式考虑到一阶导数项，故保存了相当的网格内信息，有比较好的结果。下面以最简单的一维平移方程:

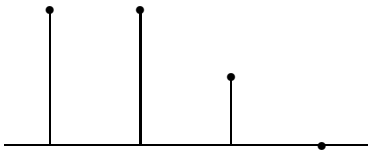
$$\frac{\partial f}{\partial t} + u\frac{\partial f}{\partial x} = 0, \qquad u = const > 0$$

为例来说明它的基本思想。

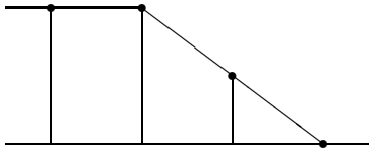
方程表示波以速度 u 向右传播。在某一时刻，一般的方法只计算在节点处的函数值，这样损失了大量的网格内的信息。假定在某时刻本来波形如图一所示，若只知节点处的函数值（见下图二），这样重构（线性重构）出来的波形（见下图三）与实际波形相差很多。若我们可以同时求得节点处的函数值及其一阶导数值，就可以通过相邻节点的函数值和一阶导数值来构节点间的波形（见下图四）。显然，这样重构出来的波形很接近于实际波形。进而有比较高的精度。



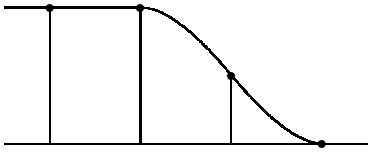
图一



图二



图三



图四

这个想法的关键是:

- 如何求得节点的函数值及一阶导数值;
- 如何由相邻节点的函数值和一阶导数值来重构网格间的波形。

这两点都是很容易实现的。在某一时刻(不妨记为第 n 层),假定已经知道各节点的函数值和一阶导数值,我们可以在每个网格内部通过二重 Hermite 插值来构造网格内的波形。由 Rolle 定理立知,这个波形具有四阶精度。再由特征线立知,下一时刻(不妨设为第 $n+1$ 层),各节点的函数值及一阶导数值,分别对应于第 n 层相应点左边 $a\triangle t$ 处点的函数值和一阶导数值。

由此可见,CIP 方法在大 CFL 条件下依然有用,这有别于其它大多数差分方法。

现总结一下 CIP 基本算法:

1. 初始化(计算 t^0 层的结果):进行网格分割,求 f_i^0 及 $f_i'^0$,令 $n=0$。
2. 在第 n 层上,用二重 Hermite 插值重构上面的函数值 $F(\frac{x-x_i}{\triangle x})$ 及其导数 $F'(\frac{x-x_i}{\triangle x})$。
3. 由特征线可知,第 $n+1$ 层的结果为:

$$f_i^{n+1}=F(\frac{-u\triangle t-x_i}{\triangle x}),\quad f_i'^{n+1}=F'(\frac{-u\triangle t-x_i}{\triangle x})$$

4. 重复 2-3 直至最后一时间层。
5. 用二重 Hermite 插值重构这一层上面的函数值。

§2 隐式 CIP 及其改进

§2.1 隐式 CIP

为了保证格式是稳定的,我们常把格式改进成隐式的。

格式的详细推导及其精度的证明可见参考文献 [2]。下面简述一下其方法。

我们在第 $n+1$ 层 $[x_{i-1},x_i]$ 进行二重 Hermite 插值 $F(\frac{x-x_i}{\triangle x})$,再由特征线可知第 n 层的节点 x_i 对应的函数值 f_i^n 及其一阶导数 $f_i'^n$ 对应于第 $n+1$ 层上点的值 $F(\frac{u\triangle t-x_i}{\triangle x})$ 及 $F'(\frac{u\triangle t-x_i}{\triangle x})$。由此可得到由两个方程组成的方程组,解这个方程组,即可得到格式;

$$f_i^{n+1}=(c+1)^{-3}[c(c+1)(cf_{i-1}'^{n+1}-f_i'^n)\triangle x+c^2(c+3)f_{i-1}^{n+1}+(3c+1)f_i^n]$$

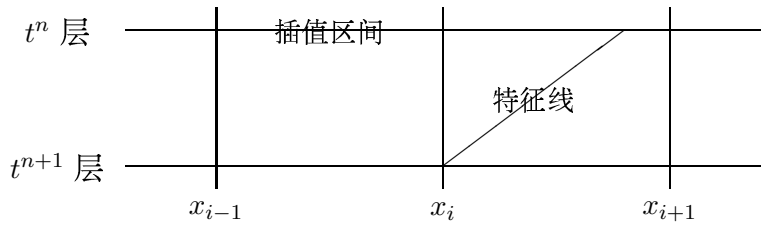
$$f_i'^{n+1}=(c+1)^{-3}[(c+1)(c(c-2)f_{i-1}'^{n+1}-(2c-1)f_i'^n)-6c(f_{i-1}^{n+1}-f_i^n)/\triangle x]$$

其中,c 为 Courant 数 $u\triangle t/\triangle x$。

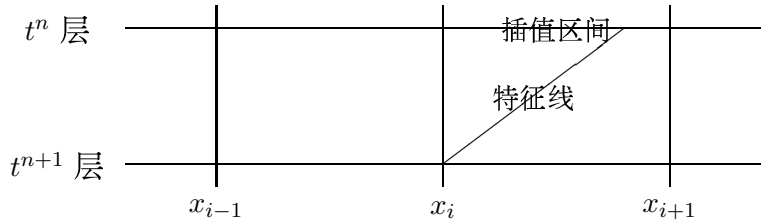
§2.2　一个小的改进

在上面的讨论中，我们可以发现在隐式格式的推导过程中，只是依照习惯选取了节点模板 $\{f_i^n, f_{i-1}^{n+1}, f_i^{n+1}, f_i'^n, f_{i-1}'^{n+1}, f_i'^{n+1}\}$，并未注意到特征线的走向。从而导致与 f_i^n 相应的第 $n+1$ 层的点不在插值区间内。如下图所示：

隐式 CIP 选取的节点模板示图



改进格式选取的节点模板示图



这里，我们很自然的想到要将上述格式改为符合特征线走向的格式。取节点模板 $\{f_i^n, f_i^{n+1}, f_{i+1}^{n+1}, f_i'^n, f_i'^{n+1}, f_{i+1}'^{n+1}\}$，或将之同时向左移动一个网格，得到模板 $\{f_{i-1}^n, f_{i-1}^{n+1}, f_i^{n+1}, f_{i-1}'^n, f_{i-1}'^{n+1}, f_i'^{n+1}\}$。用与隐式 CIP 相同的方法，可以得到格式：

$$f_i^{n+1} = c^{-3}[(3c-2)(f_{i-1}^n - cf_{i-1}'^{n+1} - f_{i-1}^{n+1}) - c(c-2)(f_{i-1}'^n - f_{i-1}'^{n+1})]$$

$$f_i'^{n+1} = c^{-3}[(6c-6)(f_{i-1}^n - cf_{i-1}'^{n+1} - f_{i-1}^{n+1}) - c(2c-3)(f_{i-1}'^n \triangle x - f_{i-1}'^{n+1})]$$

具体的推导过程与原格式基本相同，仅修改个别下标即可。在此不赘述。

§2.3　一些结论、想法

原来的隐式格式与改进格式差别有些类似于差分格式 FTBS 与 FTCS 的差别，只是隐式 CIP 本身就是稳定的，故其改进格式与原格式相比，准确性提高的非常有限。

参考文献

[1] 张瑞：CIP 方法

[2] M.Ida and T.Yable: *Implicit CIP(Cubic-Interpolated Propagation) method in one dimension.* Comput.Phys.Commun.92(1995)21-26.

$F_q[x]$ 中不可解多项式的计数公式

0101 沈明民

设 F 是域，$F[x]$ 为其上的一元多项式环，$F[x]$ 中的不可约元总是具有特殊的重要性。当 F 是有限域 F_q 时，F_q 中给定次数的多项式个数是有限的，从而可以考虑其中不可约多项式的计数问题。我们用 $r_q(n)$ 来表示 $F_q[x]$ 中的 n 次首一不可约多项式的个数，在不引起混淆时，简记为 $r(n)$。

§1 $r(n)$ 满足的组合关系式

用 S_n 表示 $f_q[x]$ 中 n 次首一多项式的全体，用 T_n 表示 $f_q[x]$ 中 n 次首一不可约多项式的全体。

一方面，$S_n = \{a_0 + a_1x + \cdots + a_nx^n : a_i \in F_q.i = 0, \ldots, n-1, a_n = 1 \in F_q\}$，故 $|S_n| = q^n$。

另一方面，$F_q[x]$ 是 UFD。考虑 S_n 中多项式的标准分解，用 $S_n(k_1, \cdots, k_n)$ 表示 S_n 中 k_1 个 1 次首一不可约多项式，k_2 个 2 次首一不可约多项式，$\cdots$，k_n 个 n 次首一不可约多项式的乘积，这里 $1k_1 + 2k_2 + \cdots + nk_n = n$，于是

$$S_n = \bigcup_{1k_1+2k_2+\cdots+nk_n=n} S_n(k_1, \ldots, k_n)$$

$$|S_n| = \sum_{1k_1+2k_2+\cdots+nk_n=n} |S_n(k_1, \ldots, k_n)|$$

$S_n(k_1, \cdots, k_n)$ 可看成是从 T_1 中可重地取 k_1 个元素，T_2 中可重地取 k_2 个元素，$\cdots$，T_n 中可重地取 k_n 个元素，于是有

$$\begin{aligned}|S_n(k_1, \cdots, k_n)| &= \binom{|T_1| + k_1 - 1}{k_1}\binom{|T_2| + k_2 - 1}{k_2}\cdots\binom{|T_n| + k_n - 1}{k_n} \\ &= \prod_{i=1}^{n}\binom{r(i) + k_i - 1}{k_i}\end{aligned}$$

从而

$$|S_n| = \sum_{k_1+\cdots+nk_n=n} \prod_{i=1}^{n} \binom{r(i)+k_i-1}{k_i}$$

于是我们得到如下定理:

定理 1 r_q 为 $F_q[x]$ 中 n 次首一不可约多项式的个数, 则

$$q^n = \sum_{1k_1+\cdots+nk_n=n} \prod_{i=1}^{n} \binom{r_q(i)+k_i-1}{k_i} \tag{1}$$

§2 问题的求解

为了使讨论方便, 这里不加证明地引用有限域的一些基本性质:(见 [1])

定理 2 设 F_q 是 q 元域, 则

1. F_q 的特征是某个素数 p, 并且它是 p 元域 F_p 的有限扩张。令 $n=[F_q:F_p]$, 则 $q=p^n$, 且作为加法群的 F_q 是 n 个 p 阶循环群的直积。
2. $F_q^* = F_q - \{0\}$ 是 p^n-1 阶的乘法循环群, 令 F_q^* 是由元素 u 生成的, 则 $F_q = F_p(u)$。
3. 设 Ω_p 是 F_q 的一个代数闭包, 则 F_q 恰好由 x^q-x 在 Ω_q 中的 q 个根组成。
4. 对于每个 $n\geq 1$, Ω_p 中有且只有唯一的 p^n 元域 F_{p^n}, 而 $\Omega_p = \bigcup\limits_{n\geq 1} F_{p^n}$。
5. 任意两个阶数相同的有限域必同构。

令 $\Phi_n(x) = \prod\limits_{f\in T_n} f(x)$, 则 $\deg \Phi_n(x) = nr(n)$。

定理 3 在 $F_q[x]$ 中,

1. 设 $f(x)$ 为一不可约多项式, 则 $f(x)|x^{q^n}-x \Leftrightarrow \deg f|n$
2. 又有

$$x^{q^n}-x = \prod_{d|n} \Phi_d(x) \tag{2}$$

证明:

1. 设不可约多项式 $f(x)|x^{q^n}-x$, $\deg f(x)=d$, 取 $f(x)$ 的一个根 u, 则 F_q 是 q^d 元域, 而且它是 F_{q^n} 的子域。$(F_q(u))^*$ 是 $F_{q^n}^*$ 的乘法子群而后者是 q^n-1 阶循环群, 故

$$|F_q(u)^*| \,\big|\, |F_{q^n}^*| \text{ 即} q^d-1 \,|\, q^n-1 \Rightarrow d|n$$

设 $d|n$, $f(x)$ 为 d 次不可约多项式。取 $f(x)$ 的根 u, 则 $F_q(u)$ 是 q^d 元域。由于 $d|n$, 故 $x^{q^d}-x \,\big|\, x^{q^n}-x$, 从而 F_{q^n} 包含某个 q^d 元子域, 由于 Ω_p 中 q^d 元子域是唯一的, 故 $F_q(u)\subset F_{q^n} \Rightarrow u\in F_{q^n} \Rightarrow u$是$x^{q^n}-x$ 的根, 故 $f(x)\,\big|\,x^{q^n}-x$。

2. 由上面直接推得。

由 2 式，比较两边的次数，$q^n = \sum_{d|n} \deg \Phi_d(x) = \sum_{d|n} dr(d)$，于是得到：

定理 4 $r_q(x)$ 为 $F_q[x]$ 中的 n 次首一不可约多项式的个数，则

$$q^n = \sum_{d|n} dr_q(d) \tag{3}$$

至此，我们得到了主要结论：

定理 5 $r_q(n)$ 为 $F_q[x]$ 中 n 次首一不可约多项式，则

$$r_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \tag{4}$$

证明：对 3 式进行莫比乌斯反演得：(见 [2])

$$nr_q(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$

于是我们得到 4 式的关系式 1 式的解。实际上我们可以得到：

定理 6 关系式

$$m^n = \sum_{1k_1+\cdots+nk_n} \prod_{i=1}^{n} \binom{f(i)+k_i-1}{k_i},\ m \in \mathbb{N}$$

的解为

$$f(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) m^d$$

证明：$x = p$ 是多项式方程

$$x^n = \sum_{1k_1+\cdots+nk_n} \prod_{i=1}^{n} \binom{\frac{1}{i}\sum_{d|i} \mu\left(\frac{i}{d}\right) x^d + k_i - 1}{k_i}$$

的根，故这是恒等式，将 $x = m$ 代入即可。

参考文献

[1] 冯克勤等编, 近世代数引论, 中国科学技术大学出版社.
[2] 嘉裕著, 组合数学, 同济大学出版社.