离散数学：方法与挑战

Noga Alon

摘要 组合学不但是一门基本的数学学科，它本身也是很多数学领域的根本成分，其研究近年来发展惊人．如此发展的主要原因之一，是离散数学与理论计算机科学的紧密联系，以及后者的突飞猛进．以往很多基本的组合学结果主要靠巧思妙想与周密论证得到，近代理论则已超越这种早期阶段，经常依赖深刻和成熟的工具．本文综述对近代组合学发展起关键作用的两种主要的一般性技术：代数方法与概率方法，将通过实例阐明这两种方法的基本思想以及与其他领域的联系．

1. 引言

离散数学是研究有限结构的数学，其基本概念源自印度人．他们在 6 世纪已知道 n 个元素的排列个数以及 n 元集中 k 元子集的个数．我们今天所说的组合学则始于 17 世纪 Pascal 和 De Moivre 的工作，以及随后 18 世纪 Euler 在图论上影响深远的思想和他在整数分拆及其计数方面的工作，还有他对拉丁方的兴趣．这些古典结果构成了最近 20 年来计数方法研究，构形与设计的发展，以及图论的大量工作的部分根基．离散数学与理论计算机科学的紧密联系以及后者近年来的突飞猛进，导致组合技术备受关注和这一方向的惊人发展．同时还激发起对算法组合学与组合最优化的研究兴趣．

以往很多基本的组合学结果主要靠巧思妙想和周密论证得到，并不依赖很多深刻成熟的数学工具．组合学的近代理论则已超越这种早期阶段．已经有发达的计数方法，其中有些是基于深刻的代数工具．由 Erdős (以及某种程度上也由 Shannon) 创始的概率方法成为近代组合学理论的最有力工具之一，其研究既在组合学也在概率论上硕果累累．代数和拓扑方法在近代组合学理论中起关键作用，而多面体组合学、线性规划和设计的构作也大有发展．组合学的大部分新的重要成果不可避免地基于这些成熟的概念和技术，当然，纯粹的奇思妙想在离散数学中仍有相当的发挥空间，而由此取得的多数进展有赖于快速增长的知识积累．

离散数学的概念和问题自然地出现在很多数学分支中，它也在诸如信息论与电气工程、统计物理、化学、分子生物学，当然还有计算机科学等其他学科得到应用．一些组合学专题，象 Ramsey 理论、组合集论、拟阵理论、极图理论、组合几何以及偏差理论等，与一大片数学与科学领域相关，它们在其他领域已经有了众多的应用．有关组合学的众多专题、方法和应用的详细阐述可参看 R. L. Graham, M. Grötschel 和 L. Lovász 主编的《 Handbook of Combinatorics 》 (North Holland, Amsterdam, 1995).

本文主要综述对近代组合学发展起关键作用的两种主要的一般性技术：代数方法和概率方法，将通过实例阐明这两种方法的基本思想以及与其他领域的联系．论题和例子

原题：Discrete Mathematics: Methods and Challenges. 译自：Proceedings of the Internatinal Congress of Mathematicians, 2002, Vol. 1, p.119–135. 是 2002 年在北京召开的世界数学家大会 (ICM) 的一小时大会演讲的详细文本．

的选取无疑会有偏好，也不求全面．而希望用这种方式提供一些组合学的技术、问题和结果所特有的风味，这也许能引起研究者的兴趣，即便这些研究者的主要兴趣并不在离散数学．

2．维数，几何与信息论

多年来有各种代数技术成功地用来处理离散数学问题，其中包括表示论的工具广泛应用于计数问题、利用 (矩阵的) 谱技术研究高度正则的结构、把多项式的性质和代数几何的工具应用于纠错码理论和组合几何问题的研究等．这些技术有很多有趣的应用．而在组合学中应用得最有成效，大概也是最简单的一种代数技术是所谓的维数论证，其最简单的形式如下所述．为得到离散结构 A 的元素个数的上界，作集 A 到某线性空间的一个映射，再证明 A 的像集是线性无关的向量集，于是相应的线性空间的维数就是 A 中元素个数的上界．这种方法在解极端构形不唯一情况下的极值问题时常常奏效，因为一个线性空间可以有多个很不一样的基，而每个基中向量个数都相同．在 [13], [14], [37] 中可以找到这个基本方法的很多应用．

2.1 组合几何

下面是 1977 年的论文 [44] 给出的维数论证的一个早期应用．点集 $A \subset \mathbb{R}^n$ 称为 2 距离的，如果 A 中两不同点间的距离是至多两个正数值之一．$\mathbb{R}^n$ 中 2 距离点集的点数的最大可能值记为 $f(n,2)$．$\mathbb{R}^{n+1}$ 中恰有两个分量是 1 的 0/1 向量的集表明 $f(n,2) \geq n(n+1)/2$[1]，而 [49] 证明了 $f(n,2) \leq (n+1)(n+4)/2$．这个上界是通过对 2 距离集 A 的每一点结合一个 n 元多项式，再证明这些多项式都在一个 $(n+1)(n+4)/2$ 维空间中而且线性无关后得到的．Blokhuis 证明在此空间中还能在从 A 得到的多项式之外再添加 $n+1$ 个多项式并使全部多项式仍线性无关，从而把上界改进成 $(n+1)(n+2)/2$．详情可参看 [14] 及其参考文献．$f(n,2)$ 的确切值还不知道．

Borsuk 问：$\mathbb{R}^d$ 中至少含两点的任一紧集是否可分拆成至多 $d+1$ 个直径更小的子集 [21]? 令 $m(d)$ 是这种正整数 m 的最小值：$\mathbb{R}^d$ 中至少含两点的任一紧集可以分拆成至多 m 个直径更小的子集．则 Borsuk 的问题是 $m(d) = d+1$ 是否成立？ (注意到一个单形的 $d+1$ 个顶点说明 $m(d) \geq d+1$)．Kahn 和 Kalai[42] 利用 Frankl 和 Wilson 的一个定理 [30] 举例说明对所有足够大的 d 此等式不成立．之后，Nilli 在 1994, Raigorodski 在 1997, Hinrichs 在 2001, 以及 Hinrichs 和 Richter 在 2002 年都改进了 Kahn 和 Kalai 的构造．其中最后两个结果都基于 Leech 格的一些性质，所给出的构造说明当 $d = 298$ 时，$m(d) > d+1$．而以上所有构造及其证明都基于维数论证．下面是其中之一的概要．

设 $n = 4p$, p 是奇素数，令 $\mathcal{F} = \{\mathbf{x} = (x_1, \ldots, x_n) \in \{-1,1\}^n : x_1 = 1$，且有偶数个 $x_i = -1\}$．首先证明下述结论．

如果 $\mathcal{G} \subset \mathcal{F}$ 不含一对正交向量，则

$$|\mathcal{G}| \leq \sum_{i=0}^{p-1} \binom{n-1}{i}. \tag{1}$$

1) 原文如此．疑有误．—— 译注

证明是通过对 $\mathcal{G}$ 中每个向量结合一个 $n-1$ 元且至多 $p-1$ 次的多重线性多项式，使得它们线性无关. 在证得 (1) 后，再令 $S=\{\mathbf{x}*\mathbf{x}:\mathbf{x}\in\mathcal{F}\}$, $\mathbf{x}*\mathbf{x}$ 是 $\mathbf{x}$ 与自身的张量积，即 n^2 维向量 $(x_{ij}:1\le i,j\le n)$, 其中 $x_{ij}=x_ix_j$. S 中每个向量的模为 n 且 S 中任意两向量的内积非负. 由 (1) 可知， S 中元素个数大于 $\sum_{i=0}^{p-1}\binom{n-1}{i}$ 的子集必含一对正交向量，亦即距离等于 S 的直径的两点. 因此 S 不能分拆成少于 $2^{n-2}/\sum_{i=0}^{p-1}\binom{n-1}{i}$ 个直径更小的子集. 这说明有常数 $c_1>1$ 使得 $m(d)\ge c_1^{\sqrt{d}}$. 已知的上界是 $m(d)\le c_2^d$, $c_2=\sqrt{3/2}+o(1)$. 但仍不能确定 $m(d)$ 的阶. 下述猜想似乎言之有理.

猜想 2.1 有常数 $c>1$ 使得 $m(d)>c^d$ 对所有 $d\ge 1$ 成立.

度量空间中的 等边集(或单形) 是这样的集 $A:A$ 中任意一对不同元素间的距离都等于同一常数 $b\ne 0$. 易知对 (通常的)l_2 模来说， $\mathbb{R}^n$ 中这样一个集的最大基数是 $n+1$. 有点奇怪的是对 l_1 模来说问题极其复杂. 在 $\mathbb{R}^n$ 中两点 $\vec{a}=(a_1,\dots,a_n)$, $\vec{b}=(b_1,\dots,b_n)$ 的 l_1 距离是 $\|\vec{a}-\vec{b}\|_1=\sum_{i=1}^n|a_i-b_i|$. 令 $e(l_1^n)$ 是 l_1^n 中等边集的最大基数. 由标准基向量及其负向量所表示的点集表明 $e(l_1^n)\ge 2n$. Kusner 猜想其中等式对所有 n 成立，即对所有正整数 n 有 $e(l_1^n)=2n$ [39]. 当 $n\le 4$ 时这已得到证明. 而对一般的 n, 已知的最好上界是 $e(l_1^n)\le c_1 n\log n$, c_1 是某一正常数. 这是 [9] 中用恰当的维数论证得到的. 使用一种包括随机舍入在内的概率技巧把 $\mathbb{R}^n$ 中 m 个向量的等边集的每个向量映成 l_2^t 中的一个向量，这里的 $t=t(m,n)$ 是适当的正整数. 然后使用基于这些新向量的 Gram 阵的特征值的简单论证，说明它们张成的空间的维数 $\ge c_2m$, 从而 $c_2m\le t(m,n)$ 并借此证得所说上界. 详细说明这个证明要费点事 [9].

2.2 容量与图幂

设 $G=(V,E)$ 是无向简单图. G 的幂 G^n 是这样的图，其顶点集为 V^n, 两不同顶点 $(u_1,u_2,\dots,u_n)$ 与 $(v_1,v_2,\dots,v_n)$ 相邻接当且仅当对 1 与 n 之间的每个 i, 或者 $u_i=v_i$, 或者 $u_iv_i\in E$. G 的 Shannon 容量 $c(G)$ 定义为极限 $\lim_{n\to\infty}(\alpha(G^n))^{1/n}$, 这里的 $\alpha(G^n)$ 是 G^n 中无关顶点集的最大基数. 从性质 $\alpha(G^n)\le(\alpha((G))^n$ 可知上述极限存在且至多 $\alpha(G)$.

对这一参数的研究是 Shannon 受到信息论中一个问题的启发而在 1956 年的论文 [61] 中引出的. 事实上，假设 V 是传输通路所用的字母集，以两个字母可能混淆为邻接关系，则 $\alpha(G^n)$ 是 n 次传输不会混淆的字母信息的最大数. 于是 $c(G)$ 代表通道 每次 可传输的互不混淆信息的个数.

计算 $c(G)$ 看上去极难. 例如 $c(C_5)=\sqrt{5}$ 直到 1979 年才由 Lovász 求得，而 $c(C_7)$ 至今未知. 已知道一些有多项式时间算法的 $c(G)$ 的上界，如 Lovász 的 θ 函数 $\theta(G)$, 以及 Haemers 和 Schrijver 的上界.

在 [3] 中给出基于维数论证并与 Haemers 的界 [40] 有关的另一上界，它还被用来解决 Shannon 关于两个图的不交并的容量问题、图 G 与 H 的 (不交) 并 $G+H$ 是这样的图：其顶点集是 G 与 H 的顶点集的不交并，边集是 G 与 H 的边集的 (不交) 并. 如果 G 与 H 是两个通道的图，则 $G+H$ 代表如下情况的通道之和：每个字母可经两个通道中任意一个传输. Shannon 证明了对每个 G 与 H, $c(G+H)\ge c(G)+c(H)$, 而且在很多情况

下等式成立. 他猜想事实上等式无例外地成立. [3] 证明了在下述强意义下猜想不成立.

定理 2.2 对每个 k 有图 G, 使得 G 及其补 $\overline{G}$ 的 Shannon 容量有 $c(G) \le k$, $c(\overline{G}) \le k$, 但 $c(G+\overline{G}) \ge k^{(1+o(1))\frac{\log k}{8\log\log k}}$, 其中 $o(1)$ 项当 k 趋于无穷时趋于零.

因此, 两个图的不交并的容量可以远大于每个图的容量. 很奇怪, 当 $c(G)$, $c(H)$ 都至多是 k 时, 甚至还不知道 $c(G+H)$ 是否有 k 的函数为上界. 不过看上去会有.

3. 多项式, 堆垒数论与图染色

研究代数簇, 也就是一组多项式的公共零点集, 是代数几何学的主要课题. 域上单变量多项式的最基本性质是它的根的个数不超过多项式的次. 这个基本性质竟然在组合学中大有作为: 它在纠错码理论中有重要作用, 还在有限几何的研究中有很多应用 [14]. 对多元多项式有类似的结果, 它也能在离散数学中有所作为. 本节叙述一个这种类型的一般结果, [4] 中称之为组合性零点定理 (Combinatorial Nullstellensatz), 再概要介绍它在堆垒数论 (Additive Number Theory) 以及图论中的应用.

3.1 组合性零点定理

Hilbert 的零点定理, 这个基本定理断言: 如果 F 是代数闭域, $f, g_1, \ldots, g_m$ 是多项式环 $F[x_1, \ldots, x_n]$ 中的多项式, 其中 f 在 $g_1, \ldots, g_m$ 的所有公共零点上为零, 则有正整数 k 和 $F[x_1, \ldots, x_n]$ 中多项式 $h_1, \ldots, h_m$, 使得

$$f^k = \sum_{i=1}^{m} h_j g_i.$$

当 $m = n$ 且每个 g_i 是形如 $\prod_{s\in S_i}(x_i - s)$ 的单变量多项式, 其中 $S_i \subset F$ 时有更强的结论. 若 F 是任意域, f, g_i, S_i 如上所述, 且 f 在 $g_1, \ldots, g_n$ 的所有公共零点上为零 (即 $f(s_1, \ldots, s_n) = 0$ 对所有 $s_i \in S_i$ 成立), 则有多项式 $h_1, \ldots, h_n \in F[x_1, \ldots, x_n]$ 满足 $\deg(h_i) \le \deg(f) - \deg(g_i)$, 使得

$$f = \sum_{i=1}^{n} h_j g_i.$$

由此可证如下推论.

定理 3.1 设 F 是任意域, $f = f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$, f 的次数 $\deg(f) = \sum_{i=1}^{n} t_i$, 其中每个 t_i 是非负整数, 且 f 中单项 $\prod_{i=1}^{n} x_i^{t_i}$ 的系数非零. 如果 S_i 是 F 的子集且 $|S_i| > t_i\,(i = 1, \ldots, n)$, 则有 $s_i \in S_i\,(i = 1, \ldots, n)$ 使得

$$f(s_1, \ldots, s_n) \ne 0.$$

在 [4] 中有详细证明和此定理的很多应用. 在 [5] 中有它最早的机智应用, 证明了: 对任一素数 p, 若无环图 $G = (V, E)$ 的平均度大于 $2p-2$ 而最大度至多 $2p-1$, 则 G 含有 p-正则子图.

为证此结果, 令 $(a_{v,e})_{v\in V, e\in E}$ 是 G 的点边关联矩阵: 当 $v \in e$ 时, $a_{v,e} = 1$, 否则 $a_{v,e} = 0$. 对 G 的每边 e 结合一个变量 x_e 并考察 $GF(p)$ 上的多项式

$$f = \prod_{v\in V}\left[1 - \left(\sum_{e\in E} a_{v,e}x_e\right)^{p-1}\right] - \prod_{e\in E}(1 - x_e).$$

在定理 3.1 中对每个 i 取 $t_i = 1$, $S_i = \{0,1\}$ 可知有 $x_e \in \{0,1\}$ 使得 $f(x_e : e \in E) \neq 0$. 不难验证由 E 中所有使 $x_e = 1$ 的边 e 所构成的子图中，每个度能被 p 整除. 但因最大度小于 $2p$, 可知每个非零度等于 p.

Pyber 应用上述结果解决了一个 Erdős 和 Sauer 提出的问题，证明了当 n 顶点的简单图的边数至少 $200n\log n$ 时，一定含 3–正则子图. Pyber, Rödl 和 Szemerédi 利用概率论证说明此结论离可能的最佳结果并不远：他们证明有 n 顶点的简单图的边数至少 $cn\log\log n$ 但不含 3–正则子图. 关于其他有关结果可参看 [58].

3.2 堆垒数论

在堆垒数论中有众多应用的 Cauchy-Davenport 定理说：设 p 是素数， A, B 是 $\mathbb{Z}_p$ 的非空子集，则

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Cauchy 在 1813 年证得此定理，并用它给出 Lagrange 在 1770 年证明每个正整数是四个平方数之和的著名论文中一个引理的新证明. Davenport 把它表述为 Khintchine 关于两个整数列之和的 Schnirelman 密度的一个猜想的离散类比. 这一结果有很多推广 [56]. [7] 中给出它的一个简单的代数证明，其主要优点在于它容易推广和给出一些相关结果. 这个证明可叙述成定理 3.1 的简单应用. 如果 $|A|+|B| > p$, 结论是平凡的：因集 A 与 $g - B$ 对每个 $g \in \mathbb{Z}_p$ 都有交. 否则，若结论不成立而且 $|A+B| \leq |A|+|B|-2$, 令 C 是 $\mathbb{Z}_p$ 的子集，并满足 $A+B \subset C$ 与 $|C| = |A|+|B|-2$. 定义 $f = f(x,y) = \prod_{c\in C}(x+y-c)$, 并应用定理 3.1, 其中 $t_1 = |A|-1$, $t_2 = |B|-1$, $S_1 = A$, $S_2 = B$, 即得出矛盾.

使用类似 (但稍复杂一些) 的论证，[7] 中证明了下述结果.

命题 3.2 *设 p 是素数， $A_0, A_1, \ldots, A_k$ 是循环群 $\mathbb{Z}_p$ 的非空子集. 如果 $|A_i| \neq |A_j|$ 对所有 $0 \leq i < j \leq k$ 成立，且有 $\sum_{i=0}^{k}|A_i| \leq p + \binom{k+2}{2} - 1$, 则*

$$|\{a_0 + a_1 + \cdots + a_k : a_i \in A_i, a_i \neq a_j \text{ 对所有的 } i \neq j\}| \geq \sum_{i=0}^{k}|A_i| - \binom{k+2}{2} + 1.$$

当 $k = 1$, $A_0 = A$, $A_1 = A - \{a\}$, 其中 a 是 A 的任意元的特殊情形，由命题可知：如果 $A \subset \mathbb{Z}_p$, $2|A| - 1 \leq p+2$, 则 A 中两不同元 a_1, a_2 之和 $a_1 + a_2 \geq 2|A| - 3$. 这就给出了 Dias Da Silva 和 Hamidoune 的一个结果 [23] 的简短证明，而该结果解决了 Erdős 和 Heilbronn 的一个猜想 [27].

Snevily 猜想，对任意奇数阶 abel 群的任意两个基数相同的子集 A, B, 可以对 A, B 中元素分别标记为 a_i, b_i 使得所有的和 $a_i + b_i$ 两两不同 [62].

对素数 p 阶的循环群 $\mathbb{Z}_p$ 来说，在定理 3.1 中考察多项式 $f = \prod_{j<j}(x_i - x_j)\prod_{j<j}(a_i + x_i - a_j - x_j)$ 及 $S_1 = \cdots = S_k = B$ 即可知上述猜想成立.

更一般些，Dasgupta 等在 [24] 中应用多项式方法证明此猜想对任一奇数阶循环群成立，他们取 $Q[\omega]$ 中的多项式，这里 ω 是适当的单位根，并把群 G 看作为这个域的乘法群的子群. 在 [63] 中有更多相关结果.

定理 3.1 在堆垒数论中的另一些应用可参看 [4].

3.3 图染色

定理 3.1 在在图论的最广为人知的领域图染色的研究中有多种应用. 以下按 [12] 概述其基本处理方法, 其他方法还可参看 [52], [53].

图 G 的一种 (顶) 点染色就是对 G 的每一点指派一种颜色. 如果任意一对邻接点的颜色不同, 这种染色就称为 *正常的*. G 的 *色数* $\chi(G)$ 定义为对 G 作正常点染色所需的最少颜色数. 可以类似地定义 G 的 *边染色*, 即对 G 的每一边指派一种颜色, 如果任意一对关联边的颜色不同, 就称为 *正常*(边染色). G 的 *色指标* $\chi'(G)$ 定义为对 G 作正常边染色所需的最少颜色数, 它等于 G 的线图的色数.

图 $G=(V,E)$ 称为 *k–可选择的* (k-choosable), 如果对每一点 $v\in V$ 有 k 元整数集 $S(v)\subset\mathbb{Z}$, 使得有正常点染色 $c:V\mapsto\mathbb{Z}$, 对所有的 $v\in V$ 有 $c(v)\in S(v)$. G 的 *选择数* (choice number) $ch(G)$ 是使得 G 为 k–可选择的最小 k. 显然 $ch(G)\geq\chi(G)$. G 的线图的选择数记为 $ch'(G)$, 它通常称为 G 的 *列单色指标* (list chromatic index), 显然 $ch'(G)\geq\chi'(G)$.

选择数的研究是由 Vizing [67] 以及 Erdős, Rubin 和 Taylor [29] 独立地提出的. 有很多图 G 使得 $ch(G)>\chi(G)$ (每一种颜色有 3 个顶点的完全二部分图是其中一例). 考虑到这一情况, 下述由 Vizing, Albertson, Collins, Tucker 和 Gupta 等很多研究者独立提出的猜想就显得有些出乎意料.

猜想 3.3 (列单染色猜想) 对每个图 G 有 $ch'(G)=\chi'(G)$.

此猜想断言, 对 线图 来说, 选择数与色数的数值是相同的. 对此猜想的很多最有兴趣的结果是对一些特殊情形猜想成立的证明, 但仍有大量未决情况.

顶点集 $V=\{1,\ldots,n\}$ 上图 $G=(V,E)$ 的 *图多项式* $f_G=f_G(x_1,x_2,\ldots,x_n)$ 定义为 $f_G(x_1,x_2,\ldots,x_n)=\prod\{(x_i-x_j):i<j,ij\in E\}$. 从 Petersen[57] 在 1891 年开始, 图多项式被各种研究者所研究.

注意到若 $S_1,\ldots,S_n$ 是整数子集, 则存在对每个顶点 i 指派单子 S_i 中的一种颜色的正常染色当且仅当有 $s_i\in S_i$ 使得 $f_G(s_1,\ldots,s_n)\neq 0$. 这一条件正是定理 3.1 的结论中所说的, 因此自然期望这个定理在研究染色问题时发挥作用. 对可平面的 3 正则图的线图应用定理, 对相应的多项式的适当系数作组合解释, 并引用 Vigneron 的一个已知结果 [66] 和四色定理, 就可以证明每个 2–连通的 3 正则可平面图的列单色指标是 3. 这是比四色定理更强的结论, 大家知道四色定理等价于每个这种图的色指标是 3. [25] 中有这一结果的推广.

把上述代数处理用于图染色与选择数的其他结果在综述 [2] 中有描述. 这些结果中有: 每个可平面的二部分图的选择数至多是 3, 它解决了 [29] 中提出的一个猜想; [32] 证明了如果 G 是 $3n$ 个顶点的图, 而其边集是一个 Hamilton 圈和 n 个两两顶点不交的三角形的不交并, 则 G 的色数与选择数都是 3.

4. 概率方法

上世纪中叶就发现确定性陈述可用概率性推理证明, 并因此在分析、数论、组合学和信息论中得到一些令人瞩目的结果. 不久就了解到这种现在叫做 *概率方法* 的证明方

法是离散数学中证明结论的极为有力的工具. 它在早期是组合论证结合很初等的概率技术，而这种方法的近期发展则要求应用概率论中更复杂和先进的工具. 本节解说这种方法并叙述几个新近的结果. 在近著 [11], [16], [41] 和 [55] 的书中可找到更多资料.

4.1 随机性质的阈

对随机图的系统研究肇始于 Erdős 和 Rényi 在 1960 年发表的对这个论题的第一篇主要论文 [28]. 令 $G(n,p)$ 表示这样的概率空间：其点是在给定的 n 个标定顶点上的图，图中每对顶点随机并独立地以概率 p 连边. 文中 "随机图 $G(n,p)$" 一词的意思是上述概率空间中取出的一个随机点. 每个图性质 A (即在图同构下封闭的一个图族) 是该概率空间的一个事件，我们可以研究它的概率 $Pr[A]$, 就是此图族中随机图 $G(n,p)$ 的概率. 特别地，如果当 n 趋于无穷时，随机图 $G(n,p)$ 满足 A 的概率趋于 1, 则称 A *几乎肯定* 成立. 有大量研究随机图的论文，近著 [16], [41] 提供了这个课题已知结果的出色而且广泛的纪录.

阈函数 是 Erdős 和 Rényi 的重要发现之一. 函数 $r(n)$ 称为对于图性质 A 的阈函数，如果当 $p(n)/r(n)$ 趋于 0 时 $G(n,p(n))$ 几乎肯定不满足 A, 而当 $p(n)/r(n)$ 趋于无穷时 $G(n,p(n))$ 几乎肯定满足 A. 例如，Erdős 和 Rényi 精确地确定了对于图的连通性的阈函数：设 $p(n)=\frac{\ln n}{n}+\frac{c}{n}$, 则当 n 趋于无穷时，$G(n,p(n))$ 连通的概率趋向于 $e^{-e^{-c}}$.

一个图性质称为 *单调的*, 如果在图加边后仍保持此性质. 注意有很多有趣的图性质，诸如 Hamilton 圈、非可平面、连通或至少含有 10 个顶点不交的三边形等性质都是单调的.

Bollobás 和 Thomason [18] 证明：对 *任一* 单调的图性质有阈函数. 他们的证明适用于有限集的任一单调子集族，甚至不需要假定图性质 A 在图同构的意义下保持不变.

Friedgut 和 Kalai [30] 指出可利用图性质的对称性得到更为精确的结果. 他们证明，对任一单调的图性质 A, 如果 $G(n,p)$ 满足 A 的概率至少为 ϵ, 则 $G(n,q)$ 满足 A 的概率至少为 $1-\epsilon$, 其中 $q=p+O(\log(1/2\epsilon)/\log n)$.

证明来自两个结果的结合. 第一个是 Margulis [51] 和 Russo [60] 的简单然而基本的引理，它在逾渗理论 (Percolation Theory) 中有用. 可用于此引理把满足 A 的 $G(n,p)$ 的概率对 p 的导数表示成每一可能出现的边的贡献之和；第 2 个结果是 [19] 中用调和分析证得的一个定理，定理断言这些贡献中至少有一个总是相当大的，而对称性意味着各边的贡献相同，从而证得结果. 对有关的其他结果也可参看 [64]. 这些结果对每个对称性的可迁群都成立. [20] 指出，当考虑到由完全图的顶点置换导出边对称性的具体群时，实际上还可以证明更精确的图性质的阈函数. 对每个单调图性质以及每个给定的 $\epsilon>0$, 在其中具有该性质的概率从 ϵ 增大到 $1-\epsilon$ 的区间的宽度不超过 $c_\delta/(\log n)^{2-\delta}$, 其中 δ 是任一正数. 而性质 "含有 $\lfloor 2\log_2 n\rfloor$ 个顶点的完全子图" 说明这里的幂次 2 已不能改进.

自然地，一个单调图性质的阈函数称为 *精确的* (sharp), 如果对每个给定的 $\epsilon>0$, 在其中具有该性质的概率从 ϵ 增大到 $1-\epsilon$ 的区间的宽度 w 满足 $w=o(p)$, 这里的 p 是区间内任意一点. Friedgut 在 [31] 得到使阈函数是精确的所有单调图性质的一个漂亮的特

征刻划. 粗略地说，一种图性质没有精确的阈函数当且仅当它可以在概率 p 的相关范围内，通过常数规模证据确定的性质来很好地近似. 于是，例如性质 "含 5 个点不交三角形" 不具有精确阈函数，而性质 "色数大于 10" 却具有. 对超图也有类似结果. 证明则结合了概率与组合论证以及调和分析中的技巧.

4.2 Ramsey 数

设 $H_1,\ldots,H_k$ 是 k 个有限无向简单图的序列. 所谓 (多色) *Ramsey* 数 $r(H_1,\ldots,H_k)$ 是满足下述性质的最小正整数 r: 用标记为 $1,2,\ldots,k$ 的 k 种色对 r 点完全图 K_r 作任意边染色后，一定有某一色 i, $0\le i\le k$, 使得边染色后的 r 点完全图中含有各边都是 i 色的子图同构于 H_i. 作为著名的 Ramsey 定理 [38] 的推论，对任意给定的图序列 $H_1,H_2,\ldots,H_k$, 这种有限正整数 r 一定存在.

确定或估计 Ramsey 数通常极难. 当所有的图 H_i 都是不止两点的完全图时，迄今已知的确切值只有 $r(K_3,K_m)$, $m\le 9$, $r(K_4,K_4)$, $r(K_4,K_5)$ 和 $r(K_3,K_3,K_3)$. 即使要想确定 Ramsey 数的除不计常数因子外的渐近性质也很难，尽管各种研究者为此倾注了大量心力 (如 [38], [22] 及其文献), 也只对少数几类图的无限族确定了其 Ramsey 数的渐近性质.

作为在组合学中应用概率方法的首批成果之一, Erdős 证明 [26]: 如果 $\binom{n}{k}2^{1-\binom{k}{2}}<1$, 则 $r(K_k,K_k)>n$, 即有 K_n 的边的一种 2 染色，使得染色后没有各边同色的 k 个完全子图. 证明很简单: 对 K_n 作任意的边 2 染色，使得染色后含有各边同色的 K_k 的概率至多 $\binom{n}{k}2^{1-\binom{k}{2}}$, 因此当这个上界小于 1 时，就一定存在所要求的边染色.

已知其 Ramsey 数的渐近性质的少数无限图族中，下述 Kim[43] 的结果连同 Ajtai, Komlós 和 Szemerédi [1] 的结果特别有意义.

定理 4.1 ([43], [1]) *存在正常数 c_1,c_2 使得*

$$c_1m^2/\log m\le r(K_3,K_m)\le c_2m^2/\log m$$

对所有 $m>1$ 成立.

定理 4.1 中的上界是用概率方法证明的，还应用了某种随机的贪心算法. 下界则用 "半随机" 构造分步证得，其细致的分析基于某种大偏差不等式，相当精巧.

对至少三色的 Ramsey 数的渐近性质所知更少. 例如，至今对 $r(K_3,K_3,K_m)$ 的渐近性质还了解很少. Erdős 和 Sós 在 1979 年的猜想 [22]:

$$\lim_{m\to\infty}\frac{r(K_3,K_3,K_m)}{r(K_3,K_m)}=\infty.$$

最近它在更强的意义下得到证明 [10], 事实上 $r(K_3,K_3,K_m)$ 除不计一对数因子外等于 m^3. [10] 还证明了下述更复杂的结果，它给出了不计常数因子外的无限族 Ramsey 数的渐近性质.

定理 4.2 *对每个 $t\ge 1$ 和 $s\ge(t-1)!+1$, 存在正常数 c_1,c_2 使得对每个 $m>1$ 有*

$$c_1\frac{m^t}{\log^t m}\le r(K_{t,s},K_{t,s},K_{t,s},K_m)\le c_2\frac{m^t}{\log^t m},$$

其中 $K_{t,s}$ 是完全二部分图，每部分分别有 t 和 s 个顶点染以同色.

证明综合利用了谱技巧，特征和估计以及概率论证.

4.3 Turán 型结果

对图 H 与正整数 n, Turán 数 $ex(n,H)$ 定义为不含同构于 H 的子图的 n 点图中边数的最大可能值. 当 $\chi(H)=3$ 时, $ex(n,H)$ 的渐近性质是熟知的 [15]. 但当 $\chi(H)=2$, 即 H 是二部分图时却知之甚少，只对少数几种非平凡的二部分图 H 知道 $ex(n,H)$ 的数量级.

Füredi 的一个结果 [34] 蕴含这样的结论：对给定的二部分图 H, 如果 H 的一个同色顶点类，即二部分顶点中一部分的每点的度都至多 r, 则有 $c=c(H)>0$ 使得 $ex(n,H)\le cn^{2-\frac{1}{r}}$. 文 [6] 注意到可以从一个简单然而出奇有效的概率引理导出此结果. 从 Rödl 开始，象 Kostochka, Gowers 以及 Sudakov 等研究者分别证明了这一引理的各种变形并加以应用 ([46], [36], [47]). 概略地说，这个引理断言：有足够多边的每个图有大的顶点子集 A, 使得其中每 a 个顶点都有很多公共邻点. 为找出这种集合 A, 使用了一种可称之为 *相关随机选取* 的方法， A 就是一适当选取的随机集 R 的所有公共邻点的集合. 直观上很清楚，如果某 a 个顶点只有少量公共邻点，则 R 的元不大可能从这些邻点中选取，所以不期望 A 会包含任一这样 a 个顶点的子集. 这个简单想法可以推广. 特别地，可以用来得到退化二部分图的 Turán 数的界.

一个图称为 r *退化的*, 如果它的每个子图含有度至多 r 的一点. Erdős 的一个老的猜想说：每个给定的 r 退化二部分图 H 有 $ex(n,H)\le O(n^{2-1/r})$, 而用前面所说的技巧可以证明，存在常数 $c>0$, 使得对每个这种 H 有 $ex(n,H)\le n^{2-c/r}$.

在 [6], [15] 及其文献中有关于 Turán 数的更多问题与结果.

5. 算法与明确构造

理论计算机科学的快速发展以及它与离散数学的紧密联系，推动了对代数和概率技巧的算法方面的研究. 一个用代数或概率方法证明其存在的组合结构，或所给组合结构的子结构，能否 *明确地* 构造出来 (即通过有效的确定性算法给出)? 能否给出相应于存在性证明的有效算法？研究这些问题常常要用其他数学分支的工具.

在 3.3 已指出，如果 $3n$ 个顶点的图 G 的边集可以分拆成 Hamilton 圈和 n 个两两点不交的三角形的不交并，则 G 的色数是 3. 能否给出相应于这一结果的有效算法？即是否有多项式时间的确定性或随机性算法，当输入上述图 G 后能得出 G 的正常 3 染色？类似地，3.3 还指出，每个 2 连通的 3 正则可平面图的列单色指标是 3. 我们能否用多项式时间具体给出这种对边的 3 染色？

这些问题以及定理 3.1 的应用的算法形式都尚待解决. 当然，定理的算法形式本身将提供解决问题的有效方法. 这种算法的输入是通过多项式规模的算术回路 (arithmetic circuit) 给出的所在域上的 n 元多项式. 设此多项式满足定理 3.1 的假设条件，而且可有效地检验确实满足. 则算法应能有效地找到一点 $(s_1,s_2,\ldots,s_n)$ 满足定理 3.1 的结论.

遗憾的是看上去不大可能有这种一般结果，因为否则将蕴涵没有单向置换 (one-way permutation). 事实上, 设 $F:\{0,1\}^n\mapsto\{0,1\}^n$ 是 1-1 函数, 而且对每个 $x=(x_1,\ldots,x_n)\in$

$\{0,1\}^n$, $F(x)$ 的值可以有效计算. 每个 Boole 函数可表示为 $GF(2)$ 上的多重线性多项式, 因此当我们想找到 x 使 $F(x)=y=(y_1,\ldots,y_n)$, 我们可以把它写成 $GF(2)$ 上的一组多重线性多项式: $F_i(x)=y_i$, $1\le i\le n$. 这又可以等价地写成 $\prod_{i=1}^{n}(F_i(x)+y_i+1)\neq 0$. 最后的方程有唯一解蕴涵其左边写成的多重多项式的次数是 n (因否则容易检验它偶数次取值 1). 由此可知当 $f=\prod_{i=1}^{n}(F_i(x)+y_i+1)$, $t_i=1$ 和 $S_i=GF(2)$ 时定理 3.1 的假设成立. 于是, 如有上面所说的有效算法, 则我们可以有效地得到 F 的逆, 这蕴涵不会有任何单向置换. 因为后者不大可能, 所以试图去解决相应于定理所得结果的特定的算法问题也许更有成效.

概率证明也使人想到研究相应的算法问题. 这关系到研究随机化算法 —— 这一课题在最近 10 年中得到极大发展, 可参见 [54] 及其众多参考文献. 特别地, 它关注由概率论证得知其存在的组合结构的明确构作. "明确" 的意思是有一个有效算法, 它可以在结构规模的多项式函数时间内构造出这个结构. 此类构造除了本身的意义外还在其他领域有应用. 例如, 明确构造出与随机构造相当的纠错码在信息论中有意义, 明确构造某种 Ramsey 型的染色也许可用于去随机化 (derandomization)—— 把随机化算法转化成确定性算法.

不过寻找好的明确构造通常很难, 即使象在 4.2 所说的 Erdős 对于 "$\lfloor 2^{m/2}\rfloor$ 个顶点的完全图一定存在边的 2 染色使得不含各边同色的 K_m" 所给出的简单证明, 要找到其明确的染色也是尚待解决的难题. 是否能在 n 的多项式时间内明确给出 K_n 的所要求的边的 2 染色, 这里的 $n\ge(1+\epsilon)^m$, ϵ 是任给的正数?

虽然作了努力, 但这个问题仍未解决. Frankl 和 Wilson [33] 给出了迄今最好的结果: 当 $n=m^{(1+o(1))\frac{\log m}{4\log\log m}}$ 时, 给出了 K_n 的明确的边 2 染色, 使得染色后不含各边同色的 K_m.

对于给定的 s 和大的 m, 要给出大的 K_n 的红、蓝边染色使得既没有红边的 K_s, 又没有蓝边的 K_m 看来极难. 而用概率方法可证对于 n 是 $c(\frac{m}{\log m})^{(s+1)/2}$, c 是正常数时存在这种 2 染色. 但由 [8] 给出的迄今最好的明确构作的 2 染色只有当 n 是 $m^{\delta\sqrt{\log s/\log\log s}}$, 其中 δ 是正常数时才行. 描述其构作并不复杂, 但证明其性质要用到多种数学领域的工具. 其中包括 [45] 所得到的一些代数几何中的想法, Weil 关于特征和的著名界, 谱技巧及其与图的伪随机性质的关联, [48] 中对 Zarankiewich 问题的界, 以及关于存在 $\Delta-$系统的著名的 Erdős-Rado 界等.

上面的例子有代表性, 它说明这样的事实: 在设计组合结构的明确构造时常常要用到多种数学分支的工具. 说明这个事实的另外实例是代数几何码, 还有构作称为扩展子 (expander) 的稀疏伪随机图.

6. 一些挑战

前面已提到离散数学中若干专门的待解问题, 它们以及另外一些问题为这一领域的进一步研究提供了有意义的挑战. 在结束本文时我们对两个更加一般的未来挑战作简略评注. (下转 267 页)

说，他知道为什么他攻这个问题不奏效，而这正可用来指出他人证明中的漏洞) 发现了问题. 为了绕过 Haken 的证明中的死胡同,Rourke 添加了一种叫标记分裂瀑布 (tag-breaking cascade) 的技术, Gabai 和 Casson 都不相信它. 当天下午 Casson 就证明中可疑部分的一张图提了一个问题, Rourke 给了看似可靠的一个回答. 过了一会, Gabai 又让他解释另外一个问题. Rourke 看了一会说 "但是我们已经分开了瀑布" "不！你没有分开，你只能分裂标记，但这是一个伪标记，或者是一个别的什么东西."

这个错误应该是 Haken 在 6 个月前指出的一个错误的翻版，当时 Rourke 以为他解决了它. 最后一天早上, Rourke 最终宣布证明失败，他承认自己 "有点失落和灰心". 讨论班主持人 Robion Kirby[1] 总结说 "Poincaré 猜想是一个孤注一掷的命题，或者你得到全部，或者你什么也不到. 如果说 Rourke 是一个攀登者，那么他已经死去."

讨论班后的第 2 天, Gabai 用计算机给他的导师 Thurston 发了一份电报，其标题是 "Poincaré 猜想遭到了核攻击！ (PC Nuked！)".

直到 1986 年 12 月, Rourke 感到他仍然能证明 Poincaré 猜想. 他说 "这个问题十分诱人，证明被归结为一些奇妙的技术细节. Kirby 是对的，除非每个细节都写下来，否则什么也得不到."[2] [7, p.75–77]

• 下一个 Poincaré 猜想的证明是不是会被接受，看来取决于这个人做数学的态度. Rourke 的一个学生 Will Kazez 说 "如果 Thurston 说他证明了猜想并把它写在一张纸上，人们会相信它并争着去读它；如果 Gabai 说他证明了 Poincaré 猜想，人们也会相信它，但很不情愿去读他的证明. 这是个信誉的问题. 如果你证明了一个著名的问题，那么人们会读你的证明. 但是如果你只是一个一般的数学家，假如你的头 20 页写得很精彩，并有一些新东西能吸引读者，他们会去读. 否则 ..."[7, p.77]

(未完待续)

(刘小扬 陆柱家 编译　　陆柱家 校)

****

(上接 212 页) 看来有把握预期未来将会继续有来自其他数学领域的方法进入组合学. 但这些方法通常提供的是非构造性的证明技术，把它们转化成算法性的很可能会是这一领域未来的主要挑战之一. 近来，组合学的另一有意义的发展是计算机辅助证明日渐增多，开始是四色定理的证明，包括发现和证明超几何恒等式的自动方法 [59]. 成功地引进这种方法而又不损伤其特有的美和吸引力是另一个挑战. 这些挑战连同这一领域本质上的属性，它与其他分支的紧密联系，还有研究中的众多奇妙的待解问题，保证了离散数学在未来科学的发展中仍将大有可为.

参考文献 (略)　　(李乔 译　　姚景齐 校)

1) 美国数学家，1938 年出生，低维拓扑领域的领军人物. 1965 年在芝加哥大学获博士学位. 1971 年获美国数学会颁发的几何学 Veblen 奖. 2001 年被选为美国国家科学院院士. 现为 Berkeley 加州大学数学系教授. —— 校注

2) Colin Rourke 对于 Poincaré 猜想的兴趣至今未减. 在其网上主页中仍有一链接 "Essay on the Poincaré conjecture". —— 校注