數學傳播　42卷3期, pp. 25-42

Paul Erdős 與組合學中的機率方法

張鎮華

1. 計數的藝術–Erdős 的法寶

匈牙利數學家 Paul Erdős 可以說是二十世紀數學界的一位奇才, 有關他的傳記, 請參見柴契特 [1] 和 霍夫曼 [2] 的書。Erdős 在 1996 年以八十三歲高齡去世, 一生寫過的數學論文多達 1525 篇, 遠遠超過數百年來由 Leonhard Euler 所維持的紀錄, 成爲數學史上第一名。更可貴的是, 這些著作不只是數目多, 份量也很紮實, 其中有許多影響後來的發展十分深遠。這篇文章要談的是, 他使用機率方法證明組合問題的歷史, 以及後續的影響。

爲了慶祝 Erdős 的六十歲生日, 他的好朋友 Joel Spencer 從他的六百多篇論文當中精選了 78 篇, 集合成一本專輯, 綜觀這些文章的特點, 把書名取爲《計數的藝術》[3], 反映出 Erdős 精通計數, 而他計數的特點之一是, 經常使用「機率方法」或者「非建構性方法」。有關這一點, 可以參考 Frank Harary 在 Erdős 的一篇文章 [4] 前面的引言:「機率論證的精神是這樣的, 如果你想證明具有某種性質的圖存在, 就想辦法推估不具有這種性質的圖的數目, 如果確認這個數目小於具有 n 點的所有圖數, 那麼一定存在一個具有這種性質的圖。」在這樣的哲學下, 所謂機率方法其實不等同於現在人們熟知的機率論, 正確地說, 其實是計數方法加上反證法的一種非建構性證明。

Erdős 引進機率方法的源頭 (請參見 [5]), 可以追溯到他年輕時候, 與一群愛好數學的朋友討論下面的問題而來:「對於給定的正整數 n, 能不能找到正整數 $N(n)$, 使得平面上任意給定的、三點不共線的 $N(n)$ 點當中, 都能找到 n 點形成凸 n 邊形? 如果答案是肯定的, 那麼最小的答案 $N_0(n)$ 是多少?」

這個問題由可愛的 Esther Klein 證明 $N_0(4) = 5$ 的特例引發而來, George Szekeres 對於解答這個問題有強烈的動機, 他首先給出一個 $N(n)$ 有上界的證明, 獲得佳人的芳心, 後來和 Klein 結爲夫妻, Erdős 因此就把這個問題叫做「幸福結局問題」。

Szekeres 的證明裡有一個想法很像 Frank Ramsey 在一篇談論形式邏輯的文章 [6] 所提出的一種論述, 用後面將介紹的第 4 階 Ramsey 數的符號, 他的結果就是 $N_0(n) \le R(n, 5; 4)$。Erdős 瞭解了 Ramsey 數的道理以後, 很快地就用第 2 階 Ramsey 數 $R(n, n; 2)$、簡寫爲

$R(n,n)$ 的精神, 將上界大幅下降爲 $N_0(n) \le \binom{2n-4}{n-2} + 1$。他們把這兩個結果寫成一篇經典的文章 [7], 再加上他們大約在 30 年後得到的下界結果 [8], 總結爲

$$2^{n-2} + 1 \le N_0(n) \le \binom{2n-4}{n-2} + 1 \ll R(n, 5; 4)。$$

爲了估計第一個上界 $\binom{2n-4}{n-2} + 1$, 也爲了後面的許多估計, 考慮

Stirling 公式: $n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$, 其中 $e \approx 2.71828$ 是自然對數的底。

由這個公式推導得到 $\binom{2n-4}{n-2} = \frac{(2n-4)!}{(n-2)!(n-2)!} \approx \frac{4^{n-2}}{\sqrt{\pi(n-2)}}$, 可以看出來, 就算是 Erdős 得到的比較好的上界, 也和下界 $2^{n-2}+1$ 有一個很大差距。事實上他們猜想下界就是答案。

幸福結局問題猜想: $N_0(n) = 2^{n-2} + 1$。

因爲上述的機緣, Erdős 對 Ramsey 數特別偏愛, 終其一生都在嘗試估計 Ramsey 數。機率方法的源頭, 可以追溯到 Erdős 估計對角 Ramsey 數 $R(n,n)$ 下界的論證, 他 [9] 證明了「當 $n \ge 3$ 的時候 $R(n,n) > 2^{n/2}$」, 細節將後續解釋。

其實在更早, Tibor Szele [10] 就已經用類似的論述, 計算競賽圖的 Hamilton 路徑的個數, 但是 Erdős 可以說是獨具慧眼, 一再使用這種論述, 並且到處宣傳的一位。在他早期的一些文章, 例如 [11][12][13][14] 裏, Erdős 一再地使用、並強調機率方法。他的確是第一個瞭解這個方法的威力, 並且把它成功地運用到各種問題的人。

Erdős 把計數的方法改用機率論的語言描述的作法, 正如同機率學家 Joseph Leo Doob 的見解:「很好, 但是骨子裏還是計數罷了。」這樣的評論確實有道理, 不過 Doob 並沒有料到, 當越來越複雜的論證出現以候, 比較高明的機率證明, 確實使得一些論證變得精簡, 甚至回不到單純的計數說法。例如 Lovász 局部引理所能處理的論證, 如果硬要寫回計數方法, 可能是十分複雜的排容原理, 或者是更混亂的式子。

Spencer 幫 Erdős 一起寫了一本書 [15][1], 大力推廣機率方法, 並且把他的所有論證寫成較正式的機率語言, 於是一門新興的學問便告誕生。在同一個時期, László Lovázs 引進局部引理, 更確立了上乘的機率論推導是不容易被簡單的計數方法所取代。後來 Spencer 在 CBMS-NSF 會議上的《機率方法十講》[16], 還有 Noga Alon 和 Spencer 的專書《機率方法》[17] 更確定了機率方法在組合學、圖論、數論、組合幾何等各種領域的重要性。最近, 機率方法更被廣泛的用到有效的演算法, 以及各種計數問題。

接下來, 我們先介紹 Ramsey 理論, 再回來看 Erdős 如何求得對角線 Ramsey 數 $R(n,n)$ 的下界, 以及機率方法用於一些組合問題的論證。

[1] 猶太人朋友之間的義氣。

2. 第二層 Ramsey 數著兩種顏色的特例

這一節先來談第二層 Ramsey 數, 這是一般的 Ramsey 數 $R(n_1, n_2, \ldots, n_k; \ell)$ 當 $\ell = 2$ 時的特例, 爲了方便, 常常省略 ℓ 把它記作 $R(n_1, n_2, \ldots, n_k)$。但即使是 $k = \ell = 2$ 時的特例, 直到目前爲止, 知道精確值的 $R(m, n)$ 還是非常少。

人們常常用下面這個例子來介紹 $R(3, 3)$。有 6 個人, 兩兩之間或者互相認識、或者互相不認識, 那麼或者有 3 個人兩兩之間互相認識、或者有 3 個人兩兩之間互相不認識。這個敘述可以證明如下。任意選取一人 A, 則剩下的 5 個人當中, 至少有 3 個人和 A 認識、不然就有 3 個人和 A 不認識, 對稱起見, 不妨假設 B、C、D 和 A 認識。如果 B、C、D 之間兩兩互相不認識, 則證明完畢, 否則他們之間就有兩人互相認識, 不妨假設 B 和 C 互相認識, 則 A、B、C 之間兩兩互相認識, 所以得到證明。其實 6 個人也是能達到上述結論的最少人數。

我們也可以用圖論的語言描述這個例子。將這 6 個人看成完全圖 K_6 的點, 任意兩個人如果互相認識, 就把他們之間的邊著紅色, 如果互相不認識, 就把他們之間的邊著藍色, 則不管 K_6 的所有邊如何著色, 必定有一個三角形 K_3, 它的 3 條邊同色。

這個特例可以推廣如下。對正整數 m 和 n, **Ramsey 數** $R(m, n)$ 是最小的正整數 r (這個數的存在性是需要證明的), 使得把完全圖 K_r 的每一條邊任意著紅色或藍色以後, 總是存在一個子圖 K_m 它的邊都著紅色 (叫做紅色 K_m), 或是存在一個子圖 K_n 它的邊都著藍色 (叫做藍色 K_n)。由定義很容易得到下面三個性質: 對正整數 m 和 n 恆有

$$R(m, n) = R(n, m),$$
$$R(1, n) = 1,$$
$$R(2, n) = n。$$

和前面討論 $R(3, 3)$ 的證法類似, 可以得到下面的定理。

定理 1: 對正整數 m 和 n, Ramsey 數 $R(m, n)$ 總是存在。而且當 $m, n \geq 2$ 的時候, $R(m, n) \leq R(m-1, n) + R(m, n-1)$; 進一步, 如果 $R(m-1, n)$ 和 $R(m, n-1)$ 都是偶數, 則 $R(m, n) \leq R(m-1, n) + R(m, n-1) - 1$。

證明: 用數學歸納法證明定理。由定義, 顯然 $R(1, n) = R(m, 1) = 1$ 存在。當 $m, n \geq 2$ 的時候, 由歸納法假設, $a = R(m-1, n)$ 和 $b = R(m, n-1)$ 都存在。對於 K_{a+b} 的任意 2-邊著色, 取圖中一點 x, 由鴿籠原理[2], x 或者有 a 個用紅邊相連的鄰居, 構成集合 A, 或者有 b 個用藍邊相連的鄰居, 構成集合 B。第一種情況由定義知道 A 中有紅色 K_{m-1} 或者藍色 K_n,

[2] 鴿籠原理是說:「假定有 $n+1$ 隻鴿子和 n 個鳥籠, 如果讓所有鴿子飛入籠中, 則存在某一個籠子裡面最少有兩隻鴿子。」鴿籠原理也叫做抽屜原理, 是十九世紀德國數學家 Johann Peter Gustav Lejeune Dirichlet 提出來, 用來解決數論上的一些問題, 所以也有人把它叫做 Dirichlet (抽屜) 原理。更一般的鴿籠原理是說:「假定有 $n_1 + n_2 + \ldots + n_k + 1$ 隻鴿子和 k 個鳥籠, 如果讓所有鴿子飛入籠中, 則存在某一個 i 使得第 i 個籠子裡面最少有 $n_i + 1$ 隻鴿子。」有關鴿籠原理也請參見 [5]。

前者加上 x 就是 K_{a+b} 的紅色 K_m, 而後者也是 K_{a+b} 的藍色 K_n。第二種情況也類似。所以 $R(m,n)$ 總是存在, 而且 $R(m,n) \le a+b = R(m-1,n)+R(m,n-1)$。

當 a 和 b 都是偶數的時候, 考慮 K_{a+b-1}。對於 K_{a+b-1} 當中任一點 x, 如果 x 有 a 個用紅邊相連的鄰居, 或者 b 個用藍邊相連的鄰居, 和上面的論述一樣可以導到 $R(m,n) \le a+b-1 = R(m-1,n)+R(m,n-1)-1$。不然的話就表示 K_{a+b-1} 用紅邊導出來的子圖中, 每一點的度數都是 $a-1$, 所有點的度數和 $(a-1)(a+b-1)$ 是紅色邊的兩倍, 這和 a 和 b 都是偶數, 因而 $(a-1)(a+b-1)$ 是奇數矛盾。 □

推論 2: 對正整數 m 和 n, 恆有 $R(m,n) \le \binom{m+n-2}{m-1}$。

證明: 用數學歸納法證明定理。當 $m=1$ 或 $n=1$ 的時候, 推論顯然成立。如果 $m,n \ge 2$, 由定理 1 和歸納法假設得知 $R(m,n) \le R(m-1,n)+R(m,n-1) \le \binom{m-1+n-2}{m-1-1} + \binom{m+n-1-2}{m-1} = \binom{m+n-2}{m-1}$, 最後一個等式是巴斯卡等式。 □

以下利用定理 1 來算一些 $R(m,n)$ 的值。爲了方便, 假設 K_r 的點集是 $\{1,2,\ldots,r\}$、將它簡寫成 $[r]$。

首先再來看一次 $R(3,3)$。因爲 $R(2,3)=R(3,2)=3$, 所以由定理 1 得到 $R(3,3) \le R(2,3)+R(3,2) = 3+3 = 6$。另一方面, 在 K_5 的邊中, 把一個 C_5 子圖的邊著紅色, 剩下的邊著藍色, 則這個 K_5 中既沒有紅色 K_3, 也沒有藍色 K_3, 所以 $5 < R(3,3)$, 導到 $R(3,3)=6$。這和本節開始的推論一致。

其次, 因爲 $R(2,4)=4$ 和 $R(3,3)=6$ 都是偶數, 所以由定理 1 得到 $R(3,4) \le R(2,4)+R(3,3)-1 = 4+6-1 = 9$。另一方面, 在 K_8 的邊中, 把一個用圖 $([8],E_8)$ (如圖 1 左圖所示) 當作子圖的邊著紅色, 剩下的邊著藍色, 其中 $E_8 = \{xy\colon x-y \equiv 1,4 \text{ 或 } 7 \pmod 8\}$, 則這個 K_8 中既沒有紅色 K_3, 也沒有藍色 K_4, 所以 $8 < R(3,4)$, 導到 $R(3,4)=9$。

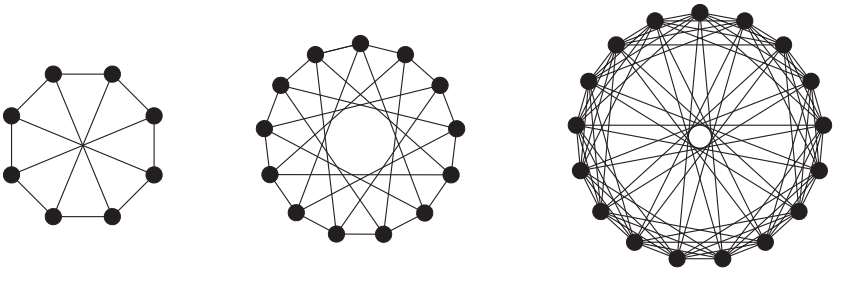

圖 1: 左圖 $([8],E_8)$、中圖 $([13],E_{13})$、右圖 $([17],E_{17})$。

接下來, 再由 $R(2,5)=5$ 和 $R(3,4)=9$ 得到 $R(3,5) \le R(2,5)+R(3,4)=14$。同

時考慮在 K_{13} 的邊中, 把一個用圖 $([13], E_{13})$ (如圖 1 中圖所示) 當作子圖的邊著紅色, 剩下的邊著藍色, 其中 $E_{13} = \{xy\colon x - y \equiv 1, 5, 8 \text{ 或 } 12 \pmod{13}\}$, 則這個 K_{13} 中既沒有紅色 K_3, 也沒有藍色 K_5。所以 $13 < R(3, 5)$, 導到 $R(3, 5) = 14$。

類似地, 由 $R(3, 4) = 9$ 可以得到 $R(4, 4) \leq 18$。而考慮在 K_{17} 的邊中, 把一個用圖 $([17], E_{17})$ (如圖 1 右圖所示) 當作子圖的邊著紅色, 剩下的邊著藍色, 其中 $E_{17} = \{xy\colon x - y \equiv 1, 2, 4, 8, 9, 13, 15 \text{ 或 } 16 \pmod{17}\}$, 則這個 K_{17} 中既沒有紅色 K_4, 也沒有藍色 K_4。所以 $17 < R(4, 4)$, 導到 $R(4, 4) = 18$。

到目前爲止, 已經知道的一些 $R(m, n)$ 的值如下面的表所示, 其中大多數都還只知道一個範圍 (用 a/b 表示 $a \leq R(m, n) \leq b$)。更多的資料可以參考 Radziszowski 的動態調查文章 [18]。

m \ n	3	4	5	6	7	8	9	10
3	6	9	14	18	23	28	36	40/42
4		18	25	36/41	49/61	58/84	73/115	92/149
5			43/49	58/87	80/143	101/216	126/316	144/442
6				102/165	113/298	132/495	169/780	179/1171
7					205/540	217/1031	241/1713	289/2826
8						282/1870	317/3583	?/6090
9							565/6588	581/12677
10								798/23556

Erdős 曾經做過下面這個著名的比喻:「想像有一支軍事能力遠超出地球人的外星人部隊降臨地球, 要求人們回答 $R(5, 5)$ 的值, 不然就要把地球毀滅, 這種情況下, 人們應該立刻集結全世界的數學家和電腦一起試著算出答案。但如果他們要問的是 $R(6, 6)$, 那人們應該試著直接消滅外星人。」這段幽默的談話充分地展現出, 要正確計算出 Ramsey 數是多麼困難的一件事。

當 $m = n$ 的時候, $R(n, n)$ 叫做 **對角 Ramsey 數**; 根據推論 2 的不等式, $R(n, n)$ 的一個上界是 $\binom{2n-2}{n-1}$, 利用 Stirling 公式可以得到 $\binom{2n-2}{n-1} = \frac{(2n-2)!}{(n-1)!(n-1)!} \approx \frac{4^{n-1}}{\sqrt{\pi(n-1)}}$, Erdős 利用機率方法證明了 $R(n, n)$ 的一個下界 $2^{n/2}$, 這開創了機率方法用於組合證明的理論。

3. 一般的 Ramsey 數

一般來說, 對正整數 $n_1, n_2, \ldots, n_k$, **Ramsey 數** $R(n_1, n_2, \ldots, n_k)$ 是最小的正整數

r (這個數的存在性也是需要證明的), 使得把完全圖 K_r 的邊任意著 k 種顏色, 總是存在一個 i 和一個子圖 K_{n_i} 它的邊都著第 i 種顏色 (叫做第 i 色 K_{n_i})。由定義不難看出, 對正整數 $n_1, n_2, \ldots, n_k$ 以及 $[k]$ 的任意排列 π 恆有

$$\begin{aligned} &R(n_1, n_2, \ldots, n_k) = R(n_{\pi_1}, n_{\pi_2}, \ldots, n_{\pi_k}),\\ &R(1, n_2, n_3, \ldots, n_k) = 1,\\ &R(2, n_2, n_3, \ldots, n_k) = R(n_2, n_3, \ldots, n_k)。\end{aligned}$$

和定理 1 類似的證明可以得到下面的結果, 它的證明省略。

定理 3: 對正整數 $n_1, n_2, \ldots, n_k$, Ramsey 數 $R(n_1, n_2, \ldots, n_k)$ 總是存在。當所有 $n_i \geq 2$ 時, $R(n_1, n_2, \ldots, n_k) \leq \sum_{i=1}^{k} R(n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_k) + 2 - k$。

最後要介紹 1930 年 Ramsey 得到的結論 [6]。爲了介紹這個結果, 我們把完全圖 K_r 的邊看成是點集 $[r]$ 的 2-子集, 因此要討論第 ℓ 層 Ramsey 數, 就要考慮 $[r]$ 的 ℓ-子集、視爲「超圖」的「超邊」, 也就是說, 現在考慮完全超圖 K_r^ℓ, 其點集是 $[r]$ 而邊集是 $\binom{[r]}{\ell} := \{A \subseteq [r] : |A| = \ell\}$。

對正整數 $n_1, n_2, \ldots, n_k, \ell$, 一般的 **Ramsey 數** $R(n_1, n_2, \ldots, n_k; \ell)$ 是最小的正整數 r (這個數的存在性也是需要證明的), 使得把完全超圖 K_r^ℓ 的邊任意著 k 種顏色, 總是存在一個 i 和一個超子圖 $K_{n_i}^\ell$ 它的邊都著第 i 種顏色 (叫做第 i 色 $K_{n_i}^\ell$)。由定義不難看出下面的事實。

(1) 對 $[k]$ 的任意排列 π 都有 $R(n_1, n_2, \ldots, n_k; \ell) = R(n_{\pi_1}, n_{\pi_2}, \ldots, n_{\pi_k}; \ell)$。

(2) $R(n_1; \ell) = n_1$。

(3) 如果有某個 $n_i < \ell$, 則 $R(n_1, n_2, \ldots, n_k; \ell) = \min\{n_1, n_2, \ldots, n_k\}$。

(4) 如果 $k \geq 2$ 且 $n_k = \ell$, 則 $R(n_1, n_2, \ldots, n_k; \ell) = R(n_1, n_2, \ldots, n_{k-1}; \ell)$。

(5) 如果 $\ell = 1$, 則 $R(n_1, n_2, \ldots, n_k; 1) = n_1 + n_2 + \cdots + n_k - k + 1$。

如果把 $\binom{[r]}{1}$ 視同 $[r]$, 由 (5) 的結果可以把鴿籠原理看成是第一層 Ramsey 數。而前述的 $R(n_1, n_2, \ldots, n_k)$ 當然就是第二層 Ramsey 數 $R(n_1, n_2, \ldots, n_k; 2)$。如同前面特殊 Ramsey 數的存在性, 也可以證明下面的定理 (請參見 [19] 定理 11.9)。

定理 4 (**Ramsey [6]**) : 對正整數 $n_1, n_2, \ldots, n_k, \ell$, Ramsey 數 $R(n_1, n_2, \ldots, n_k; \ell)$ 總是存在。如果所有 $n_i \geq \ell \geq 2$, 則當 $m_i = R(n_1, n_2, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_k; \ell)$ 時 $R(n_1, n_2, \ldots, n_k; \ell) \leq R(m_1, m_2, \ldots, m_k; \ell - 1) + 1$。

由定理 4 的遞迴不等式可以看出來, Ramsey 數每當 ℓ 增加 1, 它的值就增大很多。這有一點類似在整數的運算中, 加法是一個層級, 因應累加產生乘法就提升一個層級, 因應累乘產生冪次方又提升一個層級, Ackermann 函數 $A(m,n,\ell)$ 就是要來說明一層一層提升要如何定義, 它的定義如下。

$$\begin{cases} A(m,n,0) = m+n; \\ A(m,0,1) = 0; \\ A(m,0,2) = 1; \\ A(m,0,\ell) = m, & \text{如果 } \ell > 2; \\ A(m,n,\ell) = A(m, A(m,n-1,\ell), \ell-1), & \text{如果 } n > 0 \text{ 而且 } \ell > 0。 \end{cases}$$

在這個定義中, $A(m,n,0) = m+n$, $A(m,n,1) = mn$, $A(m,n,2) = m^n$。比較定理 4 中 $R(n_1, n_2, \ldots, n_k; \ell)$ 的上界不等式中 ℓ 所扮演的角色, 就類似於 Ackermann 函數 $A(m,n,\ell)$ 的定義中 ℓ 所扮演的角色, 可以感受到加一層後函數值快速增大的特性。

當年 Szekeres 得到 $N_0(n)$ 的上界就是第 4 層 Ramsey 數 $R(n,5;4)$ (參見 [5][19]), 這也說明了 Erdős 後來得到類似於第二層 Ramsey 數的答案 $\binom{2n-4}{n-2}+1$ 爲何改進很多。這個上界, 大約經過了 60 年, 才被 Chung 和 Graham [20] 改進了 1, 也就是 $N_0(n) \le \binom{2n-4}{n-2}$, 這雖然只是一個很小的改進, 卻引發了 Kleitman 和 Pachter [21] 更進一步改進到 $N_0(n) \le \binom{2n-4}{n-2} - 2n + 7$, 還有 Tóth 和 Valtr [22] 的 $N_0(n) \le \binom{2n-5}{n-3} + 2$。用 $n = 6$ 當作例子, 原先的範圍是 $17 \le N_0(6) \le 71$, 一路被改進到 $17 \le N_0(n) \le 37$, 上、下界的差距縮小了許多。

4. 再談 Erdős 的巧思

現在可以來看看 Erdős [9] 證明「當 $n \ge 3$ 時 $R(n,n) > 2^{n/2}$」的方法。這需要下面這個性質。

性質 5: 對正整數 $n \ge 3$ 恆有 $2 \cdot 2^{n/2} < n!$。

證明: 用數學歸納法來證明這個性質。當 $n = 3$ 時 $2 \cdot 2^{3/2} = 4\sqrt{2} < 6 = 3!$。假設 $n \ge 4$ 而且 $2 \cdot 2^{(n-1)/2} < (n-1)!$, 則 $2 \cdot 2^{n/2} = 2 \cdot 2^{(n-1)/2}\sqrt{2} < (n-1)!\sqrt{2} < n!$。性質得證。□

Erdős 在他的論文是這樣寫的。如果正整數 $r \le 2^{n/2}$, 因爲完全圖 K_r 有 $\frac{r(r-1)}{2}$ 條邊, 每一條邊有 2 種著色法, 所以它總共有 $2^{r(r-1)/2}$ 種 2-邊著色, 對於 K_r 中某個固定的 n 點所導出的子圖 K_n (共有 $\binom{r}{n}$ 個這種子圖), K_r 共有 $\frac{2 \cdot 2^{r(r-1)/2}}{2^{n(n-1)/2}}$ 種 2-邊著色使得這個 K_n 中的

$\frac{n(n-1)}{2}$ 條邊都著同色, 所以 K_r 的 2-邊著色中, 使得某一個 K_n 著同色的數目最多是

$$\binom{r}{n}\frac{2\cdot 2^{r(r-1)/2}}{2^{n(n-1)/2}} < \frac{r^n}{n!}\frac{2\cdot 2^{r(r-1)/2}}{2^{n(n-1)/2}} \le \frac{2^{n^2/2}}{n!}\frac{2\cdot 2^{r(r-1)/2}}{2^{n(n-1)/2}} < 2^{r(r-1)/2}, \tag{1}$$

其中第一個不等式是因爲 $r(r-1)\dots(r-n+1) < r^n$, 第二個不等式是因爲 $r \le 2^{n/2}$, 第三個不等式是因爲性質 5 的 $2\cdot 2^{n/2} < n!$。因爲這個緣故, 當 $r \le 2^{n/2}$ 時, 存在 K_r 的某種 2-邊著色, 其中沒有同色的 K_n, 所以 $R(n,n) > 2^{n/2}$。

不過 Erdős 在向人解釋 $R(n,n)$ 下界的前述證明時, 常常使用機率的說法。把每一條邊用 $\frac{1}{2}$ 的機率著紅色, $\frac{1}{2}$ 的機率著藍色, 這時候, 對於完全圖 K_r 的點集 $[r]$ 的任意 n-子集 S, 其所導出的子圖中的邊全部著同色的事件 A_S 發生的機率是 $2^{1-\binom{n}{2}}$, 所以有同色 K_n 的機率不超過 $\binom{r}{n}2^{1-\binom{n}{2}}$。這等同於式 (1) 最左邊的數除以樣本空間的大小 $2^{r(r-1)/2}$, 可以看得出來, 用機率的語言計算, 讓本來龐大的數變得簡單。在 $r \le 2^{n/2}$ 時這個機率小於 1, 所以存在一種 K_r 的 2-邊著色使得沒有同色的 K_n。

接下來我們要用比較正式的機率語言, 描述一些組合學的解題。我們要從初等機率方法一直到進階方法, 一步一步來看各種機率方法的應用。

5. 離散型的機率空間

一個離散型的**機率空間** 是指一個有限或可數的集合 $\mathcal{S}$, 它的每一個元素 s 都有一個對應的非負權重 p_s, 使得 $\mathcal{S}$ 中所有元素的權重總和 $\sum_{s\in\mathcal{S}} p_s = 1$。一個**事件** 指的是 $\mathcal{S}$ 的一個子集 $A \subseteq \mathcal{S}$, 而事件 A 的**機率** $P(A)$ 則是 A 中所有元素的權重總和 $\sum_{s\in A} p_s$。

如果 $P(A\cap B) = P(A)P(B)$ 的話, 就說事件 A 和 B 是**獨立的**, 其中 $A\cap B$ 代表「A 和 B 都發生」的事件。類似地, 用 $A\cup B$ 代表「A 或 B 發生」的事件。對於事件 A, 用 $\overline{A}$ 表示「A 不發生」的事件。首先有下面的性質。

性質 6: 若 $A_1, A_2, \dots, A_k$ 是一些事件, 則 $P(\cup_i A_i) \le \sum_i P(A_i)$。

證明: 右式重複加總了那些最少出現在一個事件當中的元素的權重, 而因爲權重是非負的, 所以不等式成立。 □

再回來看 Erdős 有關對角 Ramsey 數 $R(n,n)$ 下界的證明, 他的論證中主要的部分可以重新寫成下面的定理。

定理 7 (**Erdős [9]**): 若 $\binom{r}{n}2^{1-\binom{n}{2}} < 1$, 則 $R(n,n) > r$。

證明: 在完全圖 K_r 上隨機地進行 2-邊著色, 每條邊都獨立地用 $\frac{1}{2}$ 的機率著上兩種顏色之一;

所有 $2^{\binom{r}{2}}$ 種 2-邊著色合成一個機率空間 $\mathcal{S}$, 它的各個元素 c 的權重是 $p_c = 2^{-\binom{r}{2}}$。考慮事件 $A = \{c \in \mathcal{S} : \text{在 2-邊著色 } c \text{ 下 } K_r \text{ 有同色的 } K_n \text{ 子圖}\}$; 對大小是 n 的點集 N, 考慮事件 $A_N = \{c \in \mathcal{S} : \text{在 2-邊著色 } c \text{ 下 } K_N \text{ 是同色子圖}\}$; 則 $A = \cup_{|N|=n} A_N$。因爲 K_N 的 $2^{\binom{n}{2}}$ 條邊都塗同色的機率是 $P(A_N) = 2 \cdot 2^{-\binom{n}{2}}$, 而總共有 $\binom{r}{n}$ 那麼多個 N, 所以根據性質 6, $P(A) \le \sum_{|N|=n} P(A_N) = \binom{r}{n} 2^{1-\binom{n}{2}}$, 因此當這個值小於 1 的時候, 就有一種 2-邊著色不在 A 內, 在這種 2-邊著色下 K_r 沒有同色的 K_n, 於是就有 $R(n,n) > r$。 □

要取得一個 $R(n,n)$ 的好下界, 就需要去找一個儘量大的 r 使得 $\binom{r}{n} 2^{1-\binom{n}{2}} < 1$ 成立, 一個很粗略的估計是

$$\binom{r}{n} \approx r^n \text{ 且 } 2^{1-\binom{n}{2}} \approx 2^{-n^2/2},$$

所以可以期望 $r^n 2^{-n^2/2} \approx 1$, 也就是 $r \approx 2^{n/2}$。這個比較粗略的估計, 其實就是 Erdős 在 1947 年推導出來的結果。

推論 8 (**Erdős [9]**): 若 $n \ge 3$, 則 $R(n,n) > 2^{n/2}$。

證明: 取 $r = \lfloor 2^{n/2} \rfloor$, 則 $\binom{r}{n} 2^{1-\binom{n}{2}} < \frac{r^n}{n!} 2^{1-\binom{n}{2}} \le \frac{2^{n^2/2}}{n!} 2^{1-\binom{n}{2}} = \frac{2 \cdot 2^{n/2}}{n!} < 1$, 其中最後一個不等式由性質 5 得到, 所以由定理 7 知道 $R(n,n) > \lfloor 2^{n/2} \rfloor$, 也就是 $R(n,n) > 2^{n/2}$。 □

如果用 Stirling 公式就可以做更精確一點的估計

$$\binom{r}{n} = \frac{r(r-1)\dots(r-n+1)}{n!} \approx \frac{r^n}{n^n e^{-n}} \approx \left(\frac{re}{n}\right)^n,$$

那麼就可以期望 $\left(\frac{re}{n}\right)^n 2^{-n(n-1)/2} \approx 1$, 也就是 $r \approx \frac{n}{e\sqrt{2}} 2^{n/2}$, 這比前面的 $2^{n/2}$ 多出了 $\frac{n}{e\sqrt{2}}$ 的倍數。要得到這個比較好的下界, 需要下面的不等式。

性質 9: (1) 對非零實數 x 恆有 $e^x > 1 + x$。(2) 對正整數 n 恆有 $2n^n < n! e^n$。

證明: (1) 考慮函數 $f(x) = e^x - 1 - x$, 它的微分 $f'(x) = e^x - 1$。在 $x > 0$ 的時候 $f'(x) > 0$, 所以 f 遞增而有 $f(x) > f(0) = 0$, 就得到 $e^x > 1 + x$。在 $x < 0$ 的時候 $f'(x) < 0$, 所以 f 遞減而有 $f(x) > f(0) = 0$, 也得到 $e^x > 1 + x$。

(2) 當 $n = 1$ 時, $2 \cdot 1^1 < 1! e^1$ 成立。假設 $2n^n < n! e^n$, 則 $2(n+1)^{n+1} = 2n^n (n+1) \left(1 + \frac{1}{n}\right)^n < n! e^n (n+1)(e^{1/n})^n = (n+1)! e^{n+1}$, 其中的不等式由 (1) 取 $x = \dfrac{1}{n}$ 得到。由數學歸納法證得 (2)。 □

推論 10：如果 $n \geq 1$, 則 $R(n,n) > \dfrac{n}{e\sqrt{2}}2^{n/2}$。

證明: 取 $r = \left\lfloor \dfrac{n2^{n/2}}{e\sqrt{2}} \right\rfloor$, 則 $\binom{r}{n}2^{1-\binom{n}{2}} \leq \dfrac{r^n}{n!}2^{1-\binom{n}{2}} \leq \dfrac{n^n 2^{n(n-1)/2}}{n!e^n}2^{1-n(n-1)/2} = \dfrac{2n^n}{n!e^n} < 1$, 其中最後一個不等式是因爲性質 9 (2), 所以由定理 7 知道 $R(n,n) > \left\lfloor \dfrac{n2^{n/2}}{e\sqrt{2}} \right\rfloor$, 也就是 $R(n,n) > \dfrac{n}{e\sqrt{2}}2^{n/2}$。 □

接著來看機率方法在集合極值問題的應用。如果 $\mathcal{F}$ 是 $[0..n-1] := \{0,1,\ldots,n-1\}$ 的一些子集的集合族, 也就是 $\mathcal{F} \subseteq 2^{[0..n-1]} := \{A : A \subseteq [0..n-1]\}$。若 $\mathcal{F}$ 中任意兩個集合都相交, 即 $A, B \in \mathcal{F}$ 時恆有 $A \cap B \neq \emptyset$, 則稱 $\mathcal{F}$ 爲一個**相交族**。例如對 $0 \leq i \leq n-1$, 集合族 $\mathcal{F}_i = \{A \subseteq [0..n-1] : i \in A\}$ 就是一個相交族, 而它的大小 2^{n-1} 也是所有相交族的大小中最大的。這個性質的證明不難, 只要將 $2^{[0..n-1]}$ 中的元素兩兩配對如下, 將 $[0..n-1]$ 的子集 A 和 其補集 $\overline{A} := [0..n-1]\backslash A$ 配對, 則總共有 2^{n-1} 對, 因爲 $A \cap \overline{A} = \emptyset$, 所以 A 和 $\overline{A}$ 中最多只有一個會在相交族 $\mathcal{F}$ 當中, 就得到 $|\mathcal{F}| \leq 2^{n-1}$。

如果要求相交族 $\mathcal{H}$ 內的集合都有固定的大小 k, 也就是 $\mathcal{H} \subseteq \binom{[0..n-1]}{k} := \{A \subseteq [0..n-1] : |A| = k\}$, 則 $|\mathcal{H}|$ 的極值就比較難求了。當 $2n \leq 2k-1$ 時, $\binom{[0..n-1]}{k}$ 本身就是一個相交族, 所以這時候的極值是 $\binom{n}{k}$。當 $n \geq 2k$ 時, 對 $0 \leq i \leq n-1$, 集合族 $\mathcal{H}_i = \{A \in \binom{[0..n-1]}{k} : i \in A\}$ 就是一個相交族, 而它的大小 $\binom{n-1}{k-1}$ 也是所有這種相交族的大小中最大的。這就是著名的Erdős-Ko-Rado 定理 [23], 它的證明並不容易, 這裡介紹一個 Katona [24] 用機率方法的簡單證法。

定理 11 (**Erdős - Ko - Rado 定理**): 若正整數 $n \geq 2k$ 且相交族 $\mathcal{F} \subseteq \binom{[0..n-1]}{k}$, 則 $|\mathcal{F}| \leq \binom{n-1}{k-1}$。

證明 (**Katona**): 對 $0 \leq j \leq n-1$ 令 $A_j = \{j, j+1, \ldots, j+k-1\}$, 其中加法取模 n。首先需要一個性質。

(甲) $\mathcal{F}$ 最多含有 k 個 A_j。
證明: 先固定某個 $A_j \in \mathcal{F}$。其他能和 A_j 相交的 A_t 可以分成 $k-1$ 對 $\{A_{j-i}, A_{j+k-i}\}$, 其中 $1 \leq i \leq k-1$, 每一對中的兩個集合都不相交, 所以 $\mathcal{F}$ 最多只包含每一對中的一個集合, 這和 A_j 合起來, 最多只有 k 個集合。□

考慮機率空間 $\mathcal{S} = \binom{[0..n-1]}{k}$, 其中每一集合 A 的權重都是 $p_A = \frac{1}{\binom{n}{k}}$。隨機、均勻、均等機率地取一個 $[0..n-1]$ 的排列 σ 和 $[0..n-1]$ 的一個元素 i, 並令 $A = \{\sigma(i), \sigma(i+$

$1), \ldots, \sigma(i+k-1)\}$, 其中加法取模 n。在選定 σ 的條件下, 由 (甲) 得到 $P(A \in \mathcal{F}) \leq \frac{k}{n}$。但是 A 是從所有 k-子集中均勻選出來的, 所以

$$\frac{|\mathcal{F}|}{\binom{n}{k}} = P(A \in \mathcal{F}) \leq \frac{k}{n},$$

也就是 $|\mathcal{F}| \leq \binom{n}{k}\frac{k}{n} = \binom{n-1}{k-1}$。 □

6. 隨機變數的期望值

爲了進一步探討機率方法更多的應用, 需要引入機率論的其他概念和工具。

一個**隨機變數**指的是一個從機率空間映射到實數上的函數 $X : \mathcal{S} \to \mathbb{R}$。對於隨機變數 X, 用「$X = k$」來代表所有 X-函數值是 k 的元素所構成的事件, 也就是 $\{s \in \mathcal{S} : X(s) = k\}$。而隨機變數 X 的**期望值** $E(X)$ 則是 X 在隨機空間中的取值平均, 也就是 $\sum_k kP(X = k)$ (當可能的取值有無窮多種的時候, 需假定這個和絕對收斂)。

關於期望值, 有一個基本性質。

性質 12: 如果 X 是有限個隨機變數 X_i 的和, 則 $E(X) = \sum_i E(X_i)$。如果 a 是常數, 則 $E(aX) = aE(X)$。

證明: 首先, $E(X) = \sum_k kP(X = k) = \sum_k k\left(\sum_{X(s)=k} p_s\right) = \sum_{s\in\mathcal{S}} p_s X(s) = \sum_{s\in\mathcal{S}}(p_s \sum_i X_i(s)) = \sum_i \sum_{s\in\mathcal{S}} p_s X_i(s) = \sum_i \sum_k \left(k \sum_{X_i(s)=k} p_s\right) = \sum_i \sum_k kP(X_i = k)$ $= \sum_i E(X_i)$。其次, $aE(X) = a\sum_k kP(X = k) = \sum_{ak} akP(aX = ak) = E(aX)$。 □

這個性質並沒有要求這些事件「$X_i = k$」之間是獨立的, 這會導到很大的便利性。在證明一些性質的時候, 常常會設置一些**指示變數**, 也就是當某個事件發生的時候是 1, 不然就是 0 的隨機變數。這樣的變數的期望值自然就會是事件發生的機率, 而藉由把那些指示變數加總起來, 就可以根據加總的期望值來判斷某個特定的事件總共到底發生了幾次。

根據期望值的定義, 有下面的性質, 它可以看成是鴿籠原理在機率論中的推廣。

性質 13: 對隨機變數 X, 如果 $E(X) \geq k^*$, 則在機率空間中存在一個元素 s 使得 $X(s) \geq k^*$; 如果 $E(X) \leq k^*$, 則在機率空間中存在一個元素 t 使得 $X(t) \leq k^*$。

現在來看比 Erdős 更早用機率方法的 Szele 的工作 [10]。一個 ***n*-競賽圖**是把完全圖 K_n 的每一條邊都給定一個方向後得到的有向圖。如果有 n 個人, 兩兩之間有一個競賽, 總有一個人輸一個人贏, 所有 n 個人之間兩兩競賽輸贏的結果, 就可以用一個 n-競賽圖來記錄。

一個傳統的結果是「任何 n-競賽圖都有一條 Hamilton 路徑。」它的證明如後。選取一條

最長的路徑 $v_1v_2\dots v_m$, 如果 $m=n$ 就得證; 否則存在一點 x 不在這條路徑中, 對於路徑上的每一點 v_i, xv_i 和 v_ix 恰有一個是有向邊。必定是 v_1x 是有向邊, 不然若 xv_1 是有向邊的話, 則 $xv_1v_2\dots v_m$ 會是一條更長的路徑, 矛盾。令 j 是使得 $v_1x, v_2x, \dots, v_jx$ 是有向邊的最大指標, 必然是 $j<r$, 要不然 $j=r$ 將迫使 $v_1v_2\dots v_rx$ 是一條更長的路徑, 矛盾。而在 $1\le j<m$ 的條件下, $v_1v_2\dots v_jxv_{j+1}v_{j+2}\dots v_m$ 是一條更長的路徑, 也是矛盾。

確實存在一個恰有一條 Hamilton 路徑的 n-競賽圖 T, 就是 $V(T)=\{1,2,\dots,n\}$ 而 $E(T)=\{ij: 1\le i<j\le n\}$。想問的是, 一個 n-競賽圖最多可以有多少條 Hamilton 路徑? Szele 給了一個不錯的下界。

定理 14: 有一個至少有 $n!2^{1-n}$ 條 Hamilton 路徑的 n-競賽圖。

證明: 隨機地把 K_n 的每一條邊用 $\frac{1}{2}$ 的機率配置一種方向, 這樣有 $2^{-\binom{n}{2}}$ 的機會得到一個競賽圖, 所有這 $2^{\binom{n}{2}}$ 個競賽圖合成一個機率空間 $\mathcal{S}$。考慮隨機變數 $X:\mathcal{S}\to\mathbb{R}$, 其中 $X(T)$ 是 T 內 Hamilton 路徑的個數; 對於 K_n 當中的每一條 Hamilton 路徑 $Q: v_1, v_2, \dots, v_n$, 考慮隨機變數 $X_Q:\mathcal{S}\to\mathbb{R}$、其中當 Q 在 T 指定的方向下是 T 中的有向路徑時 $X_Q(T)=1$、否則 $X_Q(T)=0$; 於是 $X=\sum_Q X_Q$。而 Q 中各邊 v_iv_{i+1} 在 T 中是邊的機率是 $\frac{1}{2}$, 所以 $E(X_Q)=P(Q\text{是}T\text{中路徑})=2^{1-n}$, 而且那樣的 Q 總共有 $n!$ 種, 所以$E(X)=\sum_Q E(X_Q)$ $=n!2^{1-n}$。由性質 13 便得到某個 n-競賽圖 T 有 $X(T)\ge n!2^{1-n}$, 定理得證。 □

在前面的證明裡, 都詳細地描寫出機率空間 $\mathcal{S}$, 甚至其中每一點 s 的權重 p_s。在談到隨機變數 X 時, 也把 $X:\mathcal{S}\to\mathbb{R}$ 中 $X(s)$ 的定義用 s 描述出來。當讀者逐漸了解它們的涵意以後, 下面會省略 $\mathcal{S}$ 的描述和 $X(s)$ 用 s 的描述, 讀者心中自己可以有這些描述以便對照證明。

到這裡爲止的許多機率方法的證明, 常常能夠轉成計數方法的證明, 越往後面的論證, 就越難做到這件事情了。

7. 更動法–微調的技術

有些情況當中, 前面的方法並沒有辦法直接給出一個符合期望的結構出來, 但是它給出的結構卻和想要的並沒有相差太遠, 以致於可以把結構稍微調整以便得到想要的東西。這樣的一種技巧在機率方法當中叫做**更動法**、**刪除法**或**二步法**。

先來看一個更動法在圖論控制集問題的應用。圖 G 中的一個**控制集**是指一個點集 $D\subseteq V(G)$, 使得不在 D 中的任意點都和 D 中的某個點相鄰。圖 G 的**控制數** $\gamma(G)$ 是其控制集 D 的最小基數, 即 $\gamma(G)=\min\{|D|: D\text{是}G\text{的控制集}\}$。

控制集問題有很多應用, 例如設施選址問題。以消防站位置問題爲例, 某個縣決定建立一

些消防站, 以便服務該縣所有的城鎮; 消防站將設於一些城鎮, 使得每個城鎮或者有消防站、或者與某個有消防站的城鎮相鄰。爲了省錢, 該縣希望建立滿足上述要求的最少數量的消防站。以該縣所有城鎮爲點集造一圖 G, 相鄰兩城鎮之間連邊, 則上述消防站位置問題就是要求 $\gamma(G)$。

假設圖 G 有 n 點而最小度爲 δ, 文獻上有一序列文章以 n 和 δ 爲 $\gamma(G)$ 的上界。如果 G 沒有邊, 則顯然有 $\gamma(G)=n$。當 G 沒有孤立點、也就是 $\delta\geq 1$ 時, Øystein Ore [25] 得到 $\gamma(G)\leq\frac{1}{2}n$, 他的證明如下; 取 $V(G)$ 的一個最大獨立集 I, 也就是 I 中任兩點不相鄰、而再也沒有更大的集合滿足此條件, 因此 I 外的點一定和 I 中某點相連, 得知 I 是控制集; 另外, 因爲 $\delta\geq 1$, $V(G)\backslash I$ 外的點 (也就是 I 中的點 x) 必定和某個點 y 相鄰, 但是 y 不在 I 中, 所以必在 $V(G)\backslash I$ 中, 得知 $V(G)\backslash I$ 是控制集; 綜合得知 $\gamma(G)\leq\min\{|I|, n-|I|\}\leq\dfrac{1}{2}n$。

Balnd [26] 和 McCuaig-Shepherd [27] 先後獨立證明: 當 $\delta\geq 2$ 時, 除了七個小圖 (C_4 和六個有七點的圖) 以外都有 $\gamma(G)\leq\dfrac{2}{5}n$。接著 Reed [28] 得到著名的結果: 當 $\delta\geq 3$ 時, $\gamma(G)\leq\dfrac{3}{8}n$。以上這些結果, 有一個共同的型式:

$$\text{當 } 1\leq\delta\leq 3 \text{ 時, 除了七個例外, 都有}\gamma(G)\leq\frac{\delta}{3\delta-1}n。$$

隨即 Haynes-Hedetniemi-Slater [29] 猜測上面的不等式對所有 $\delta\geq 1$ 都成立。這個猜想當 $\delta=4$ 的情況被 Sohn-Xudong [30] 證明, 而當 $\delta=5$ 的情況被 Xing-Sun-Chen [31] 證明。更多介紹及結果可參見 Bujtás-Klavžar [32] 的文章。底下介紹 Alon-Spencer [17] 用更動法得到的一個上界。

定理 15 (**Alon - Spencer [17]**): 如果圖 G 有 n 個點和最小度數 δ, 則 $\gamma(G)\leq\frac{\ln(\delta+1)+1}{\delta+1}n$。

證明: 在 G 中隨機選取一個點集 S, 使得每個點都有機率 p (稍後決定) 被選入 S 當中。令 T 是不在 S 中的點而且不和 S 中任一個點相鄰的點的集合, 則 $D=S\cup T$ 是 G 的一個控制集。因爲每一個點在 S 中的機率是 p, 所以 $E(|S|)=np$。對每一個點 $v\in V(G)$, 令 Y_v 是「v 在 T 中」的指標變數, 由於 $v\in T$ 若且唯若 v 和它的鄰居都不在 S 當中, 它的機率 $(1-p)^{\deg(v)+1}\leq(1-p)^{\delta+1}\leq e^{-p(\delta+1)}$, 所以 $E(|T|)=\sum_v E(Y_v)\leq ne^{-p(\delta+1)}$。總結就得到 $E(|D|)=E(|S|)+E(|T|)\leq np+ne^{-p(\delta+1)}$, 取 $p=\frac{\ln(\delta+1)}{\delta+1}$, 可以得到 $E(|D|)\leq\frac{\ln(\delta+1)+1}{\delta+1}n$。所以定理由性質 13 得證。 □

上面的證明中, p 隨便取一個值就會得到一個上界, 只是 $p=\frac{\ln(\delta+1)}{\delta+1}$ 可以讓這個上界達到最小, 這是因爲, 在考慮函數 $f(p)=np+ne^{-p(\delta+1)}$ 最小值的時候, 需要它的微分 $f'(p)=n-n(\delta+1)e^{-p(\delta+1)}=0$, 也就是 $p=\frac{\ln(\delta+1)}{\delta+1}$。雖然不是真正需要, 但因爲 $f''(p)=n(\delta+1)^2e^{-p(\delta+1)}>0$ 可以確定 $f(\frac{\ln(\delta+1)}{\delta+1})$ 是極小值。

這個例子的作法是先隨便選一個集合出來, 再對它做一些必要的修改使得它變成獨立集, 然後設法設定一個機率參數使得「選取集合」和「修改」兩方面一同獲得最佳化。這就是更動法的核心精神所在。

利用更動法, 可以把推論 10 有關 $R(n,n)$ 的下界改進成 $\sqrt{2}$ 倍。

定理 16: 如果 $n \geq 1$, 則對於任意正整數 r 都有 $R(n,n) > r - \binom{r}{n}2^{1-\binom{n}{2}}$, 從而 $R(n,n) > (1-o(1))\frac{n}{e}2^{n/2}$。

證明: 隨機地把 K_r 進行 2-邊著色使得每條邊都有 $\frac{1}{2}$ 的機率被著上兩種顏色之一。對於每一個子圖 K_n 設置一個「邊都同色」的指示變數, 然後令 X 是那些指示變數的和 (所以 X 就是同色 K_n 的總數)。每個指示變數都有 $2^{1-\binom{n}{2}}$ 的機率是 1, 從而 $E(X) = \binom{r}{n}2^{1-\binom{n}{2}}$。這時候假如把每一個同色的 K_n 當中都刪除掉一個點, 那麼整個圖就不再有任何同色的 K_n 了, 但得到的圖的大小的期望值就縮小成 $r-\binom{r}{n}2^{1-\binom{n}{2}}$。這就表示, 一定存在一個大小最少是 $r-\binom{r}{n}2^{1-\binom{n}{2}}$ 的完全圖以及它上面的一種 2-邊著色使得沒有同色的 K_n 存在, 證得 $R(n,n) > r - \binom{r}{n}2^{1-\binom{n}{2}}$。

由性質 9 (2) 得知 $\binom{r}{n} \leq \frac{r^n}{n!} < \frac{1}{2}\left(\frac{re}{n}\right)^n$, 所以 $R(n,n) > r - \binom{r}{n}2^{1-\binom{n}{2}} > r - \left(\frac{re}{n}\right)^n 2^{-\binom{n}{2}}$。選取 $r = \left\lfloor \frac{n2^{n/2}}{e} \right\rfloor$, 則 $r \leq \frac{n}{e}2^{n/2} < r+1$, 也就是 $\left(\frac{re}{n}\right)^n \leq 2^{n^2/2}$, 於是就得到

$$R(n,n) > \frac{n}{e}2^{n/2} - 1 - 2^{n^2/2}2^{-\binom{n}{2}} = \left(1-\frac{e}{n}\right)\frac{n}{e}2^{n/2} - 1 = (1-o(1))\frac{n}{e}2^{n/2}。 \quad \square$$

8. Lovász 局部引理

在機率方法當中, 爲了構造出具有某種性質的事物, 往往需要證明所考慮的事件發生的機率是正的。但是許多證明往往得到更多, 也就是, 不但證明所考慮的事件發生的機率是正的, 甚至還很大。事實上, 許多機率證明中, 處理的事件發生的機率常常很高, 甚至趨近於 1。

另一方面, 在一些比較簡單的例子, 往往可以證明所考慮的事件發生的機率雖然很小, 卻是正的。事實上, 如果有 n 個互相獨立的事件, 每個事件發生的機率最少是 $p > 0$, 則所有事件發生的機率最少是 p^n, 這個機率在 n 大的時侯雖然很小, 卻是正的。

很自然的會期望, 所有事件互相獨立這個條件, 可以推廣到只有少數事件互相不獨立的情況, 用這樣的結論來證明, 某些事件發生的機率雖然很小, 卻是正的。這樣的推廣確實存在, 它就是著名的 **Lovász 局部引理** (首見於 Erdős 和 Lovász 的文章 [33])。

對於事件 $A_1, A_2, \ldots, A_n$, 一個**複合事件**是指一個事件, 針對了特定的互斥集 $S, T \subseteq [n]$, 指定了對那些 $i \in S$ 的 A_i 要發生, 而對那些 $i \in T$ 的 A_i 不發生 (其他的 A_i 則發不發生無所謂)。舉例來說, 「恰好 i 是奇數的 A_i 發生了」就是一個複合事件。稱事件 B 和 $A_1, A_2, \ldots, A_n$

互相獨立, 如果 B 和任何 $A_1, A_2, \ldots, A_n$ 的複合事件都是獨立的話。

對於事件 A 和 B, 所謂的**條件機率** $P(A|B)$ 是「在 B 發生的前提之下 A 發生的機率」, 它的定義是 $P(A|B) = \frac{P(A\cap B)}{P(B)}$。如果 A 和 B 獨立, 那麼就有 $P(A|B) = P(A)$。局部引理的主要功能在於釐清, 什麼時候可以使得一些想避開的事件 $A_1, A_2, \ldots, A_n$ 通通都不發生。

定理 17 (Lovász 局部引理, 一般情形): 假設 $A_1, A_2, \ldots, A_n$ 是事件, 對每一個 i, 令 $D_i \subseteq [n]\backslash\{i\}$ 是一個使得 A_i 和 $\{A_j : j \notin D_i \cup \{i\}\}$ 互相獨立的集合。如果存在一些權重 $x_1, x_2, \ldots, x_n$ 使得 $0 \le x_i < 1$ 而且 $P(A_i) \le x_i \prod_{j\in D_i}(1 - x_j)$, 那麼 $P(\cap_i \overline{A_i}) \ge \prod_i (1 - x_i) > 0$。

證明: 下面用 I_S 表示事件 $\cap_{j\in S}\overline{A_j}$。要證明這個定理, 只需要證明「對任何 $i \notin S \subseteq [n]$ 都有 $P(A_i|I_S) \le x_i$, 也就是 $P(\overline{A_i}|I_S) \ge 1 - x_i$」, 因爲這麼一來

$$P(\cap_i \overline{A_i}) = P(I_{[n]}) = \prod_{i=1}^{n} P(\overline{A_i}|I_{[i-1]}) \ge \prod_{i=1}^{n}(1 - x_i) > 0。$$

要證明前面的宣稱, 對 $|S|$ 做數學歸納法證明。令 $T = S \cap D_i$ 而 $\overline{T} = S\backslash T$。則

$$P(A_i|I_S) = \frac{P(A_i \cap I_T|I_{\overline{T}})}{P(I_T|I_{\overline{T}})}, \tag{2}$$

而由於 A_i 和 $\{A_j : j \in \overline{T}\}$ 是互相獨立的, 得知

$$P(A_i \cap I_T|I_{\overline{T}}) \le P(A_i|I_{\overline{T}}) = P(A_i) \le x_i \prod_{j\in D_i}(1 - x_j), \tag{3}$$

於是如果 $T = \emptyset$, 那麼式 (2) 的分母就是 1, 從而 $P(A_i|I_S) \le x_i$ 成立。特別是 $|S| = 0$ 的時候, 所要證明的前面的宣稱成立, 所以可以假設 $|S| > 0$。而當 $T \ne \emptyset$ 時, 重新編號, 不失一般性可以假設 $T = \{1, 2, \ldots, r\}$, 而根據歸納法假設就有

$$P(I_T|I_{\overline{T}}) = P(I_{[r]}|I_{\overline{T}}) = \prod_{j=1}^{r} P(\overline{A_j}|I_{[j-1]\cup\overline{T}}) \ge \prod_{j=1}^{r}(1 - x_j) = \prod_{j\in T}(1 - x_j), \tag{4}$$

把式 (3) 和式 (4) 代入式 (2), 就得到想要證明的不等式

$$P(A_i|I_S) \le \frac{x_i \prod_{j\in D_i}(1 - x_j)}{\prod_{j\in T}(1 - x_j)} \le x_i。$$ □

推論 18 (Lovász 局部引理, 對稱情形): 如果 $A_1, A_2, \ldots, A_n$ 是事件, 每個 A_i 都和其他 A_j 中除了最多 d 個以外的 A_j 所成的集合互相獨立, 而且 $P(A_i) \le p$。如果 $ep(d + 1) \le 1$, 就有 $P(\cap_i \overline{A_i}) > 0$。

證明: 取 $D_i \subseteq [n]\backslash\{i\}$ 使得 A_i 和 $\{A_j : j \in D_i \cup \{i\}\}$ 是互相獨立的, 則所給的條件表示 $|D_i| \le d$。取 $x_1 = x_2 = \ldots = x_n = \frac{1}{d+1}$, 則由 $\left(1+\frac{1}{d}\right)^d < e$、也就是 $\frac{1}{e} < \left(1-\frac{1}{d+1}\right)^d$ 知道

$$P(A_i) \le p \le \frac{1}{e(d+1)} \le \frac{1}{d+1}\left(1-\frac{1}{d+1}\right)^d \le x_i \prod_{j\in D_i}(1-x_j)$$

成立, 所以由定理 17 便得到結論。 □

Shearer [34] 曾經證明對稱情形的局部引理中的 e 是沒有辦法再改進的。

接著來看看局部引理的一些應用。首先考慮 Erdős 和 Lovász 討論實數的 k-著色的問題。把實數集 $\mathbb{R}$ 作 k-著色, 也就是考慮 $c : \mathbb{R} \to \{1, 2, \ldots, k\}$。如果 $c(T) = \{1, 2, \ldots, k\}$ 的話, 就叫 $T \subseteq \mathbb{R}$ 是 ***c*-多色**。

定理 19: 如果正整數 m 和 k 滿足 $e(m(m-1)+1)k(1-1/k)^m \le 1$, 則對任何含 m 個實數的集合 S, 都存在 $\mathbb{R}$ 的 k-著色 c 使得對任意 $x \in \mathbb{R}$ 都有 $x + S$ 是 c-多色。

證明: 先固定一個 $\mathbb{R}$ 的有限子集 X, 證明存在 $Y = \cup_{x\in X}(x + S)$ 的 k-著色 c 使得對任意 $x \in X$ 都有 $x + S$ 是 c-多色。首先, 令 $c : Y \to \{1, 2, \ldots, k\}$ 是 Y 中元素的均勻隨機 k-著色。對任意 $x \in X$, 令 A_x 是 $x + S$ 不是 c-多色的事件, 則顯然有 $P(A_x) \le k(1-1/k)^m$; 尤有進者, 除非 $(x + S) \cap (x' + S) \ne \emptyset$, A_x 和其他 $A_{x'}$ 都互相獨立, 而這樣不互相獨立的 $A_{x'}$ 最多只有 $m(m-1)$ 個。由 $e(m(m-1)+1)k(1-1/k)^m \le 1$ 和對稱情形的局部引理知道 $P(\cap_x \overline{A_x}) > 0$, 也就是, 對任意 $x \in X$ 都有 $x + S$ 是 c-多色。

接著說明存在 $\mathbb{R}$ 的 k-著色滿足定理所要求的性質。因爲含有 k 點的離散空間是緊緻的, 由 Tckhonov 定理, 任意這樣的一些空間的乘積也是緊緻的, 特別是, 由 $\mathbb{R}$ 到 $\{1, 2, \ldots, k\}$ 的所有函數、也就是 $\mathbb{R}$ 的 k-著色, 所成的集合是一個緊緻的空間, 在這空間中, 對每一固定 $x \in \mathbb{R}$, 所有使得 $x + S$ 是 c-多色的 k-著色所成的集合 C_x 是閉集。由前一段證明, 任意有限個 C_x 的交集都不是空集合, 由緊緻性, 所有 C_x 的交集也不是空集合, 在這個交集中的每一個 k-著色 c 都是所求。 □

最後來看 Lovász 局部引理如何將定理 16 有關 $R(n, n)$ 的下界改進成 $\sqrt{2}$ 倍。

定理 20 (**Spencer [35]**): $R(n, n) \ge (1 + o(1))\frac{\sqrt{2}n}{e}2^{n/2}$。

證明: 隨機而且獨立地把 K_r 的邊圖上兩種顏色。對於每一個具有 n 個點的點集 S, 令 A_S 代表「S 所導出的子圖 K_n 是同色」這個事件。希望避開所有的 A_S。注意到 A_S 之間不一定獨立: 當 S 和 S' 有兩個以上的共用點的時候 (令 d 是所有這樣的 S' 之個數) A_S 和 $A_{S'}$ 就不

是獨立的, 不過除了這種情況之外 A_S 和其他所有的 $A_{S'}$ 是互相獨立。爲了估計 d 的上限, 首先從 S 中選取兩個點, 然後再選 $n-2$ 個 $K_r - S$ 中的點給 S'; 這樣做的結果會重複計算那些跟 S 有三個以上共用點的集合, 不過總會得到

$$d < \binom{n}{2}\binom{r-2}{n-2} < \binom{n}{2}\binom{r}{n-2} < \frac{n^2}{2}\left(\frac{re}{n-2}\right)^{n-2}。$$

另外, 知道有 $P(A_S) = 2^{1-\binom{n}{2}}$, 令這個機率是 p。於是

$$ep(d+1) < e\frac{n^2}{2}\left(\frac{re}{n-2}\right)^{n-2} 2^{1-\binom{n}{2}}。 \tag{5}$$

取 $c = \left(\frac{2}{en^2}\right)^{1/(n-2)} \frac{n-2}{n}$, 就可以驗證當 $p \le c\frac{\sqrt{2}n}{e}2^{n/2}$ 的時候, 式 (5) 右邊小於 1, 從而可以套用對稱情形的局部引理而得到 $P(\cap_S \overline{A_S}) > 0$, 也就是說 $R(n,n) > r$。而由於當 $n \to \infty$ 的時候 $c \to 1$, 定理的結論於是得證。 □

參考文獻

1. 布魯斯·柴契特著, 曾蕙蘭譯。不只一點瘋狂: 天才數學家艾狄胥傳奇。先覺出版社, 1999。
2. 保羅·霍夫曼著, 米緒軍、章曉燕、繆衛東譯。數字愛人: 數學奇才保羅. 艾狄胥的故事。台灣商務印書館, 2001。
3. J. Spencer, ed., *Paul Erdős: The Art of Counting, Selected Writings*, The MIT Press, Cambridge, 1973.
4. P. Erdős, Applications of probabilistic methods to graph theory, *A Seminar on Graph Theory*, ed. by F. Harary, Holt, Rinohart and Wilson, New York, 1971, 60-69.
5. 張鎮華。幸福結局問題 — 鴿籠原理與拉姆西定理。數學傳播季刊, 28 (2), 28-42, 2004。
6. F. P. Ramsey, On a problem of formal logic, *Proc. London Math. Soc., Ser.* 2, 30 (1930), 264-286.
7. P. Erdős and G. Szekeres, A combinatorial problem in geometry, *Composito Math.*, 2 (1935), 251-257.
8. P. Erdős and G. Szekeres, On some extremum problems in elementary geometry, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.*, 3-4 (1961), 53-62. Reprinted in [3], 680-689.
9. P. Erdős, Some remarks on the theory of graphs, *Bull. Amer. Math. Soc.*, 53 (1947), 292-294.
10. T. Szele, Kombinatorikai vizsgálatok az irányitott teljes gráffal kapcsolatban, *Mat. Fiz. Lapok.*, 50 (1943), 223-256. 德文翻譯: T. Szele, Kombinatorische Untersuchungen über gerichtete vollständige Graphen, *Publ. Math. Debrecen*, 13 (1966), 145-168.
11. P. Erdős, Graph theory and probability I, *Canad. J. Math.*, 11 (1959), 34-38.
12. P. Erdős, Graph theory and probability II, *Canad. J. Math.*, 13 (1961), 346-352.
13. P. Erdős, On the number of complete subgraphs conatins in certain graphs, *Publ. Math. Inst. Hung. Acad. Sci.*, 7 (1962), 459-464.

14. P. Erdős, On a problem in graph theory, *Math. Goz.*, 47 (1963), 220-223.
15. P. Erdős and J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press/Akademiai Kiado, New York-Budapest, 1974.
16. J. Spencer, Ten Lectures on the Probabilistic Method, CBMS-NSF Reginal Conference Series in Applied Mathematics, SIAM, Pennsylvanis, 1987.
17. N. Alon and J. H. Spencer, *The Probabilistic Method*, Third Edition, with an appendix on the life and work of Paul Erdős, Wiley-Interscience Series in Discrete Math. and Optimization, John Wiley & Sons, Inc., Hoboken, NJ, 2008.
18. S. P. Radziszowski, Small Ramsey numbers, *Elect. J. Combin.*, Dynamic Survey Version #14, 2014.
19. 張鎮華。演算法觀點的圖論。臺大出版中心, 2017。
20. F. R. K. Chung and R. L. Graham, Forced convex n-gons in the plane, *Discrete Comput. Geo.*, 19 (1998), 367-371.
21. D. J. Kleitamn and L. Pachter, Finding convex sets among points on the plane, *Discrete Comput. Geo.*, 19 (1998), 405-410.
22. G. Tóth and P. Valtr, Note on Erdős-Szekeres problem, *Discrete Comput. Geo.*, 19 (1998), 457-459.
23. P. Erdős, C. Ko and R. Rado, Intersection theorems for systems of finite sets, *Quart. J. Math., Oxford Second Ser.*, 12 (1961), 313-320.
24. G. O. H. Katona, A simple proof of the Erdős-Ko-Rado theorem, *J. Combin. Theory, Ser. B*, 13 (1972), 183-184.
25. O. Ore, *Theory of Graphs*, Amer. Math. Soc., Providence, R.I., 1962.
26. M. M. Blank, An estimate of the external stability number of a graph without suspended vertices (in Russian), *Prikl. Mat. i Programmirovanie*, 10 (1973), 3-11.
27. W. McCuaig and B. Shepherd, Domination in graphs with minimum degree two, *J. Graph Theory*, 13 (1989), 749-762.
28. B. Reed, Paths, stars and the number three, *Combin. Probab. Comput.*, 5 (1996), 277-295.
29. W. Haynes, S. T. Hedetniemi and P. J. Slater, *Fundamentals of Domination in Graphs*, Marcel Dekker, New York, 1998, p. 48.
30. M. Y. Sohn and Y. Xudong, Domination in graphs of minimum degree four, *J. Korean Math. Soc.*, 46 (2009), 759-773.
31. H.-M. Xing, L. Sun and X.-G. Chen, Domination in graphs of minimum degree five, *Graphs Combin.*, 22 (2006), 127-143.
32. C. Bujtás and S. Klavžar, Improved upper bounds on the domination number of graphs with minimum degree at least five, manuscript, April 16, 2015.
33. P. Erdős and L. Lovász, Problems and results on 3-chromatic hypergraphs and some related questions, *Infinite and Finite Sets*, North Holland, Amsterdam-New York, 1975.
34. J. B. Shearer, On a problem of Spencer, *Combinatorica*, 5 (1985), 241-245.
35. J. Spencer, Ramsey's theorem–a new lower bound, *J. Combin Theory (A)*, 18 (1975), 108-115.

—本文作者爲台大數學系退休教授—