機率在算法上的應用

黃光明

傳統上算法的分析是考慮在最不利情況下的性質，有名的「不定性完備」(NP-complete)理論就是討論在最不利情況下一個算法所需的時間是否能以輸入量的一個多項式函數表示。學統計的人比較習慣於考慮平均情況而不是最不利情況，但在算法分析上平均情況往往比最不利情況爲難；因爲後者只要抓住一個情況而前者要掌握所有情況才能計算平均值。

1959 年翳木〔1〕和同仁們考慮一些計算幾何的問題（旅行售貨員、最短生成樹、最短斯坦納樹），提出了一個輸入點集合爲隨機而以平均值爲目標函數的模型。他們用一個分解（點集合）的方法得到了一些最佳算法的漸近性質，計算科學大師，也是不定性完備理論的創始人之一的Karp，秉承了上文的精神，在 1977 年發表了有名的旅行售貨員問題分解算法〔5〕，爲以平均值爲目標函數的算法分析打開了一條康莊大道。Princeton 大學教授 Steele 和他的一些博士生們〔8〕也在這方面作了不少工作，在非幾何問題上最著名的結果大概是 Smale〔7〕證明了線性規劃的單純形算法所需的平均時間和變數量成正比。在實用的排序（sorting）、合併（merging）問題上，平均值分析正開始邁步〔6,9,10〕。

除了輸入和分析可以有隨機的模型外，算法的本身也可以隨機。一般的想法隨機算法沒有什麼奧妙，一定表現不好，但在很多問題上專家們百思不得其解，大自然却借着隨機算法來展示它的法力和神奇。譬如我們要造一個有 n 個點m條線具有某種性質的圖，當 n 和m相當大時，由於選擇太多，正確的造法往往並不明顯。但是有一類的定理（參考〔3〕）告訴你，當 m／n 達到某一臨界值時，一個隨機圖具有所需性質的機率趨於一。在編碼〔2〕和篩選〔4〕問題上，隨機算法也被證明了在機率趨於一的條件下相同於最優算法。

類似的觀念也可用在一些表面上似與機率無干的組合問題上〔3〕。譬如欲證在某些條件下一定存在一個有某種性質的圖。我們可以先計算在這些條件下圖的總數，然後再列舉沒有所求性質的圖的類別，把各類的數目分別自總數中減去，如果所剩數不爲零，則證明即成立。（注意分類不一定要很嚴格，一個圖歸入好幾類也可以，只要每一無所求性質的圖都被歸類即可。）如果定義一個變數對無所求性質的圖其值爲零，對有所求性質的圖其值爲一，則上一問題也可看成是證明當圖在均勻分佈下時此變數的期望值不爲零。

寫這篇短文的目的是指出，雖然傳統上算法是離散數學的禁地，但近年來機率已佔領了若干橋頭堡，而且趨勢是愈演愈盛。對機率有興趣的朋友，何不佔此先機，猛著先鞭，先

入爲主、先馳得點呢？

〔本文亦刊登於泛華統計學會1989年會刊上（二月出版）〕

參考書目

1. J. Beardwood et al., The shortest path through many points, *Proc. Cambridge Philos. Soc.* 55(1959), 299-327.
2. A.G. D'yachkov, Bounds of the error probability for certain onsembles of random codes, *Problemy Peredachi Imformatsii* 15(1979), 23-35.
3. P. Erdös et al., *Probabilistic methods in Combinatorics*, Academic, New York, 1974.
4. V. L. Freidlina, One problem of design of screening experiments, *Teor. Veroyatn, Ee Primen* 20(1975), 100-114.
5. R. M. Karp, Probabilistic analysis of partitioning algorithms for the traveling-salesman problem in the plane, *Math. Oper. Res.* 2(1977), 209-224.
6. N. Linial, The information-theoretic bound is good for merging, *SIAM J. Comput* 13(1984), 795-801.
7. S. Smale, *On the number of steps of the simplex algorithm of linear programming* 27(1983), 241-262.
8. J.M. Steele, Subadditive Euclidean functionals and nonlinear growth in geometric probability, *Ann. Probab.* 9(1982), 365-376.
9. R. M. Tanner, Minimean merging and sorting; An algorithm, *SIAM J. Comput* 7(1978), 18-38.
10. M. Thanh et al., Optimal expected-time algorithms for merging, *J. Alg.* 7(1986), 341-357,

—本文作者任職於美國AT & T Bell實驗室—