TẠP CHÍ KHOA HỌC TÍNH TOÁN VÀ ĐIỀU KHIỂN TẬP V(1989), SỐ 4 (28 - 32)

MỘT SỐ BÀI TOÁN ĐẢO NGẪU NHIÊN CÓ HẠN CHẾ

LÊ TRƯỜNG TÙNG

I - MỞ ĐẦU

Ký hiệu Q_B là tập hợp tất cả các hoán vị $(i_1, i_2, \ldots, i_n)$ của các số $(1, 2, \ldots, n)$ thỏa mãn một điều kiện B phụ thuộc vào một số tham số nào đó. Vấn đề tổng quát được đặt ra như sau :

1) Tìm điều kiện của các tham số để $Q_B \neq \emptyset$.

2) Đánh giá lực lượng (số phần tử) $|Q_B|$ theo giá trị các tham số.

3) Tìm thuật toán đảo các số $(1, 2, \ldots, n)$ để nhận được một hoán vị ngẫu nhiên trong Q_B.

Đây là một vấn đề có ý nghĩa thực tế. Nó xuất hiện khi nghiên cứu một số mô hình giản đơn của bài toán phân bố tần số hoặc khi tạo một số loại số liệu ngẫu nhiên mô phỏng một số quá trình trên máy tính điện tử. Trường hợp đảo không kèm theo điều kiện nào được khảo sát kỹ trong [1, 2]. Một trường hợp khác, khi điều kiện B là tồn tại đúng k cặp (i_j, i_{j+1}) để $i_j < i_{j+1}$ được xét đến trong [3]. Bài báo này sẽ khảo sát bài toán với hai loại điều kiện B khác. Các kết quả đã được sử dụng để tạo lập các quy ước vô tuyến đảm bảo một số yêu cầu về gián cách giữa các tần số.

II- ĐẢO NGẪU NHIÊN VỚI RÀNG BUỘC GIÁN CÁCH GIỮA HAI PHẦN TỬ KỀ NHAU

Điều kiện B phụ thuộc vào tham số n và được phát biểu như sau: Với mọi cặp phần tử (i_j, i_{j+1}) kề nhau, $1 \leq j \leq n-1$

$$|i_j - i_{j+1}| \geq m \tag{1}$$

Ta ký hiệu   là tập các hoán vị thỏa mãn (1).

Định lý 1. a) Với mọi $m > [n/2]$:

$$n! = |Q_1^n| \geq |Q_2^n| \geq \ldots |Q_{[n/2]}^n| \geq |Q_m^n| = 0$$

b)

$$|Q_n^{2m}| = 2$$

c) Với mọi $m \leq [n/2], |Q_m^n| \geq [n - 2(m-1)]$

Chứng minh :

a) Trong khẳng định này tất cả các đẳng thức và bất đẳng thức đều hiển nhiên trừ đẳng thức cuối bên phải. Ta chứng minh bằng phản chứng. Giả sử $m > [n/2]$ và tồn tại $(i_1, i_2, \ldots, i_n) \in Q_m^n$ Khi đó với $i_j = \left[\frac{n+1}{2}\right]$ tồn tại phần tử i_s kề nó ($s = j+1$ hoặc $s = j-1$) sao cho:

$$|i_s - i_j| \geq m > [n/2]$$

Mặt khác

$$|i_s - i_j| \leq \max(|i_j - 1|, |i_j - n|) = \max\left(\left[\frac{n+1}{2}\right] - 1,\ n - \left[\frac{n+1}{2}\right]\right)$$

Do đó
$$n - \left[\frac{n+1}{2}\right] > \left[\frac{n}{2}\right]$$

tức
$$n > \left[\frac{n}{2}\right] + \left[\frac{n+1}{2}\right] \qquad \text{- vô lý.}$$

b) Ký hiệu N1 = {1, 2, .., m}, N2 = {m+1, m+2,.., 2m}. Do |ij - ij+1| ≥ m nên nếu $i_j \in N_1$ thì $i_{j+1} \in N_2$ và ngược lại.

Giả sử $i_1 \in N_1$ khi đó $i_{2j-1} \in N_1$, $i_{2j} \in N_2$ với mọi j = 1, 2,.., m và

$$\begin{aligned} &i_2 - i_1 \geq m \\ &i_4 - i_3 \geq m \\ &\dots \\ &i_{2m} - i_{2m-1} \geq m \end{aligned} \tag{2}$$

Cộng các bất đẳng thức trong (2) với nhau, ta được:

$$\sum_{j=1}^{m} i_{2j} - \sum_{j=1}^{m} i_{2j-1} \geq m^2$$

Vế trái là tổng tất cả các số trong N2 trừ đi tổng các số trong N1, hiệu này bằng đúng m^2, như vậy mọi bất đẳng thức trong (2) đều là đẳng thức. Do i1 = i2 - m, i3 ≤ i2 - m và i1 ≠ i3 nên i3 < i1. Tương tự i5 < i3, i7 < i5 ... i2m-1 < i2m-3, tức i1 > i3 > i5 >..> i2m-1, suy ra i2j-1 = m - j + 1, và do các đẳng thức trong (2), i2j = 2m - j + 1.

Hoàn toàn tương tự, tồn tại một hoán vị duy nhất thỏa mãn (1) với i1 ∈ N2. Từ đó suy ra $|Q_m^{2m}| = 2$

c) Ta chứng minh bằng quy nạp theo n. Điều khẳng định đúng với n = 2m. Giả sử nó đúng với n - 1 ≥ 2m. Lấy hoán vị bất kỳ $(i_1, i_2, ..., i_{n-1} \in Q_m^{n-1}$. Dễ kiểm tra được rằng có không ít hơn n - 2(m-1) cách nhét in = n vào giữa hai số ij, ij+1, trước i1 hoặc sau in-1 sao cho (1) vẫn thỏa mãn. Tất cả các hoán vị nhận được theo cách này đều khác nhau, do đó:

$$|Q_m^n| \geq |Q_m^{n-1}|[n-2(m-1)] \geq [n-1-2(m-1)]!\,[n-2(m-1)] = [n-2(m-1)]!$$

Định lý chứng minh xong.

Sau đây ta mô tả hai thuật toán tạo hoán vị ngẫu nhiên thỏa mãn (1).

THUẬT TOÁN 1:

Xuất phát từ một trong hai hoán vị thuộc $Q_m^{n'}$ với n' = 2m, tức là từ hoán vị (m, 2m, m-1, 2m-1,..,1, m+1) hoặc (m+1, 1, m+2, 2, .., 2m, m), ta tăng dần n' lên cho đến khi bằng n, mỗi bước tăng 1 đơn vị theo phương pháp mô tả trong cách chứng minh phần c của định lý 1, tức là xây dựng hoán vị trong Q_m^{l+1} từ

$$(i_1, i_2, ..., i_l) \in Q_m^l,\ 2m \leq l \leq n-1$$

bằng cách nhét ngẫu nhiên số l +1 vào một vị trí nào đó giữa ij, ij+1, trước i1 hoặc sau il sao cho (1) đúng với l +1 và các phần tử cạnh nó.

Thuật toán này cho phép tạo được không ít hơn [n-2(m-1)]! hoán vị thuộc Q_m^n , số các số ngẫu nhiên cần tạo là n-2m, số các phép tính cần thiết là $O(n^2)$.

THUẬT TOÁN 2:

Từ (1, 2,..n) ta đảo ngẫu nhiên theo một trong các phương pháp mô tả trong [2] để nhận được (i1, i2,..in), sau đó biến đổi (i1, i2,..in) để nhận được hoán vị thỏa mãn (1) theo các bước xử lý sau:

Xử lý sơ bộ : Đầu tiên chọn số nguyên k bé nhất sao cho |i1 - ik| ≥ m rồi đổi vị trí của ik cho i2. Sau đó, giả sử các cặp kề nhau trong (i1, i2,..ij) đều thỏa mãn (1), chọn số nguyên tố k > j bé nhất sao cho |ij - ik| ≥ m rồi đổi vị trí của ik cho ij+1. Dễ dàng kiểm tra được rằng các bước trong quá trình xử lý sơ bộ đều có thể thực hiện được khi j ≤ n - 2m. Khi đạt đến j = n - 2m, ta chuyển sang giai đoạn xử lý tiếp theo.

Xử lý triệt để : Xét phần tử ij+1, j = n - 2m. Ta tìm vị trí gần ij+1 nhất trong các vị trí sau ij, giữa ij-1, ij, giữa ij-2, ij-1,.. giữa i1, i2, trước i1 sao cho cho có thể chuyển ij+1 vào đó mà không vi phạm (1) đối với ij+1 và các phần tử thuộc (i1, i2,..ij) kề nó. Sau đó đánh số lại j+1 phần tử đã thỏa mãn (1) và tăng j lên 1 đơn vị rồi lặp lại quá trình xử lý này. Dễ dàng kiểm tra được rằng nếu n-2m ≥ 2m-2, tức n ≥ 2(2m-1) thì các bước trong quá trình xử lý triệt để đều thực hiện được.

Số các số ngẫu nhiên cần tạo trong thuật toán này là n, số phép tính cần thiết là O(n^2). Thuật toán 2 chỉ áp dụng được với n ≥ 2(2m-1), trong khi thuật toán 1 áp dụng được cả cho trường hợp 2m ≤ n < 2(2m-1) nhưng nó lại có thể tạo được tất cả các hoán vị có thể có trong Q_m^n bởi vì nếu hoán vị xuất phát thuộc Q_m^n thì nó bất biến qua cả hai quá trình xử lý.

III - ĐẢO NGẪU NHIÊN ĐẢM BẢO GIÁN CÁCH LẪN NHAU GIỮA CÁC PHẦN TỬ TRONG TỪNG NHÓM

Trong bài toán này, n = lk và điều kiện B được phát biểu như sau: Với mỗi cặp phần tử (i_{j_1}, i_{j_2}) bất kỳ trong mỗi nhóm k phần tử Nj =(ij.k+1, ij.k+2,.., ij.k+l), j = 1, 2,.., l của hoán vị (i1, i2,.., in)

$$|i_{j_1} - i_{j_2}| \geq m \qquad (3)$$

Hai hoán vị
$$(i_1^1, i_2^1, ..., i_n^1) = (N_1^1, N_2^1, ..., N_l^1)$$

và
$$(i_1^2, i_2^2, ..., i_n^2) = (N_1^2, N_2^2, ..., N_l^2)$$

thỏa mãn (3) được gọi là tương đương với nhau nếu hoán vị thứ nhất có thể chuyển về hoán vị thứ hai bằng cách hoán vị các N_j^1 với nhau và hoán vị nội bộ các N_j^1. Đây là quan hệ tương đương, và tất cả hoán vị thỏa mãn (3) phân thành cac lớp, mỗi lớp chứa các hoán vị tương đương với nhau. Ký hiệu $Q_m^{l,k}$ là tập tất cả các hoán vị thỏa mãn (3), và $P_m^{l,k}$ là tập các lớp hoán vị tương đương. Dễ thấy rằng mỗi lớp tương đương chứa l! (k!)^l hoán vị, do đó:

$$|Q_m^{l,k}| = l!(k!)^l|P_m^{l,k}| \qquad (4)$$

Định lý 2. a) Với $k \geq 2$, $P_m^{l,k} \neq \emptyset$ khi và chỉ khi l ≥ m

b) $$|P_m^{l,k}| = |P_m^{m,k}| = 1$$

c) Với $l \geq m$, $|P_m^{l,k}| \geq [(l-m)!]^{k-1}(l-m)^{m(k-1)}$

Từ định lý 2 và (4) suy ra:

Hệ quả. a) Với k ≥ 2, $Q_m^{l,k} \neq \emptyset$ khi và chỉ khi l ≥ m

b) $$|Q_m^{m,k}| = m!(k!)^m, \quad |Q_m^{l,1}| = l!$$

c) với $l \geq m$, $|Q_m^{l,k}| \geq l!(k!)^l[(l-m)!]^{k-1}(l-m)^{m(k-1)}$

Chứng minh định lý 2:

a) $P_m^{l,k} \neq \emptyset$ khi và chỉ khi $Q_m^{l,k} \neq \emptyset$. Giả sử

$$(i_1, i_2, ..., i_n) = (N_1, N_2, ..., N_l) \in Q_m^{l,k}$$

Ký hiệu

$$a_j = \max N_j = \max(i_{j.k+1}, i_{j.k+2}, ..., i_{j.k+l}).$$

Khi đó rõ ràng aj ≥ 1 + (k-1)m. Do các số aj khác nhau và aj ≤ lk nên tồn tại jo sao cho $a_{j_0} \leq lk - l + 1$

Như vậy lk - l + 1 $\geq$ 1 + (k - 1)m, tức (k - 1)(l - m) $\geq$ 0

Suy ra l $\geq$ m. Ngược lại, nếu l $\geq$ m thì hoán vị (i1, i2,..,in) = (N1, N2,..,Nl) với

ij,k+1 = j

ij,k+s = ij,k+s-1 + l, s = 2, 3,.., k-1, j = 1, 2,.., l.

thỏa mãn (3), tức là $Q_m^{l,k} \neq \emptyset$

b) $P_m^{l,k}$ là lớp tất cả các hoán vị có thể có, do đó $|P_m^{l,1}| = 1$

Xét n = mk, tức l = m. Với mọi

$$(i_1, i_2, ..., i_n) = (N_1, N_2, ..., N_l) \in P_m^{m,k}$$

tồn tại jm sao cho $m \in N_{j_m}$. Nếu sắp xếp lại các phần tử trong N_{j_m} theo thứ tự tăng dần $i_{s_1} < i_{s_2} < ... < i_{s_k}$ thì do (3) nên

$$\begin{aligned} i_{s_1} &= m \\ i_{s_2} - i_{s_1} &\geq m \\ &\cdots \\ i_{s_k} - i_{s_{k-1}} &\geq m \end{aligned} \tag{5}$$

Cộng các đẳng thức và bất đẳng thức trong (5) lại ta được $i_{s_k} \geq km = n$ nhưng do $i_{s_k} \leq n$ nên $i_{s_k} = n$ và mọi bất đẳng thức trong (5) đều là đẳng thức, tức là sau khi sắp xếp lại $N_{j_m} =$ (m, 2m,..,km). Hoàn toàn tương tự, tồn tại jm-1 để $m - 1 \in N_{j_{m-1}}$. Với cách xếp lại theo thứ tự tăng dần như đối với N_{j_m} và để ý rằng $\max N_{j_{m-1}} \leq n - 1$ do $\max N_{j_m} = n$, lập luận tương tự ta được $N_{j_{m-1}}$=(m-1, 2m-1,..,km-1). Tiếp tục quá trình này cho m-2, m-3,..,3,2, ta suy ra (N1, N2,..,Nl) tương đương với $(\overline{N}_1, \overline{N}_2, ..., \overline{N}_l)$ trong đó:

$$\overline{N}_j = (j, m+j, 2m+j, ..., (k-l)m+j)$$

Như vậy
$$|P_m^{m,k}| = 1$$

c) Ta chứng minh qui nạp theo k với l, m cố định. Trường hợp k = 1 suy ra từ khẳng định ở phần b định lý 2. Giả sử điều khẳng định đúng cho k - 1, tức :

$$|P_m^{l,k-1}| \geq [(l-m)!]^{k-2}(l-m)^{m(k-2)} \tag{6}$$

Lấy một hoán vị (i1, i2,..,in) = (N1, N2,.., Nl) đại diện cho một lớp tương đương bất kỳ trong $P_m^{l,k-1}$. Ký hiệu aj = max Nj và giả sử

$$a_{j_1} < a_{j_2} < ... < a_{j_l} = (k-l)l$$

Khi đó

$$a_{j_s} \leq (k-2)l + s, \quad s = 1, 2, ..., l \tag{7}$$

Ta tìm cách xếp l số l(k-1)+1, l(k-1) + 2,.., lk vào các nhóm N1, N2,..,Nl, mỗi số vào một nhóm sao cho (3) không bị phạm. Để đạt được điều này chỉ cần đảm bảo giãn cách không bé hơn m giữa số được xếp vào Nj với aj là đủ.

Do (7) nên số (k-1)l + 1 có thể xếp vào một trong l - n nhóm khác nhau thỏa mãn giãn cách m đối với a_{j_s} tức là cũng thỏa mãn với các phần tử khác trong nhóm. Sau khi xếp xong (k-1)l + 1, số (k-1)l + 2 cũng có thể xếp vào một trong l-m nhóm khác nhau trong các nhóm còn lại. Điều này đúng cho tất cả các số (k-1)l+s, s $\leq$ m+1. Khi s > m+1, số nhóm còn lại ít hơn l - m, vì vậy số các nhóm có thể xếp (k-1)l + s vào sau khi đã xếp các số (k -1)l + 1, (k - 1)l + 2,.., (k - 1)l + s - 1 khi s > m+1 giảm dần từ (l - m) - 1 đến 1 khi s tăng dần từ m + 2 đến l. Bởi vậy với cách xếp này, ta nhận được (l - m)^m(l - m)! cách hoán vị ứng với (l - m)^m(l - m)! lớp tương đương khác nhau. Cũng dễ kiểm tra rằng với cách xây dựng này, các lớp tương đương khác nhau thuộc $P_m^{l,k-1}$ sinh ra các lớp khác nhau thuộc $P_m^{l,k}$. từ đó suy ra:

$$|P_m^{l,k}| \geq |P_m^{l,k-1}|(l-m)^m(l-m)! \tag{8}$$

Từ (8) và giả thiết qui nạp (6) suy ra điều cần chứng minh.

Ta mô tả hai thuật toán tạo hoán vị ngẫu nhiên đảm bảo giãn cách lẫn nhau giữa các phần tử trong từng nhóm.

THUẬT TOÁN 3:

Trong chứng minh phần c định lý 2 ta chỉ ra phương pháp xây dựng ngẫu nhiên một lớp hoán vị $P_m^{l,k}$ từ một lớp hoán vị ngẫu nhiên thuộc $P_m^{l,k-1}$. Ta xuất phát từ $P_m^{l,1}$ là lớp tất cả các hoán vị l phần tử có thể có, thực hiện k-1 lần phép xây dựng trên, mỗi bước chuyển từ $P_m^{l,s}$ sang $P_m^{l,s+1}$. Hoán vị cần tìm nhận được từ hoán vị đại diện nào đó trong $P_m^{l,k}$ qua phép đảo ngẫu nhiên các nhóm N_s, $s = 1,2,\ldots,l$ với nhau và đảo nội bộ trong các nhóm N_s theo một phương pnáp nào đó mô tả trong (3).

Thuật toán này có thể tạo ra $l!\,(k!)^{l}\,[(l-m)!]_{2}^{k-1}\,(l-m)^{m(k-1)}$ hoán vị khác nhau thỏa mãn (3). Số các số ngẫu nhiên cần tạo là 2n và thời gian tính toán là $O(n^2)$

THUẬT TOÁN 4:

Thuật toán này áp dụng cho trường hợp l chẵn và $l \geq 2m$ tức $l' = l/2 \geq m$. Thuật toán gồm các bước sau đây:

Bước 1: Chọn số i_0 ngẫu nhiên trong $(1,2,\ldots,l')$ và tạo các tập A_s $(1 \leq s \leq 2k-1)$:

$$A_s = (i_0 + (s-1)l' + 1, i_0 + (s-1)l' + 2, \ldots, i_0 + sl')$$

$$A_{2k} = (1, 2, \ldots, i_0, n - (l' - i_0) + 1, n - (l' - i_0) + 2, \ldots, n)$$

Bước 2: Đảo ngẫu nhiên các tập A_s, $s = \overline{1,\ 2k}$, sau đó tạo các tập N_i, $N_{i+l'}$, $i = \overline{1,\ l'}$, trong đó N_i là tập các phần tử thứ i của $A_1, A_3, \ldots, A_{2k-1}$, còn $N_{i+l'}$ là tập các phần tử thứ i của $A_2, A_4, \ldots, A_{2k}$. Nếu xem (A_{2s-1}, A_{2s}), $s = \overline{1,\ k}$ là k cột của ma trận kích thước $k \times 2l'$, thì N_i là các hàng của ma trận này.

Bước 3: Đảo ngẫu nhiên nội bộ từng N_s, $s = \overline{1,\ l}$ và đảo các N_s với nhau.

Thuật toán này cho phép tạo nên $l[(l'/2)!]^{2k}(k!)^{l}\, l/2$ hoán vị khác nhau thỏa mãn (3), số các số ngẫu nhiên cần tạo là 2n+l+1, tuy nhiên thời gian tính toán giảm xuống còn O(n).

Nhận ngày 12-3-1988.

TÀI LIỆU THAM KHẢO

1. D. E. Knuth, The Art of Computer Programming, Vol.2: Seminumerial Algorithms - Addison - Wesley, Reading Press, 1969.

2. Lê Trường Tùng, Về các phương pháp tạo bộ tên sóng ngẫu nhiên cho các máy vô tuyến trong hệ thống thông tin quân sự, Khoa học kỹ thuật về tự động hóa chỉ huy, 3-4/1986.

3. Сачков В. Н., Вероятностные методы в комбинаторике. М. Наука, 1982.

РЕЗЮМЕ

НЕКОТОРЫЕ ЗАДАЧИ СЛУЧАЙНОГО ПЕРЕМЕЩЕНИЯ С ОГРАНИЧЕНИЕМ

В статьи рассмотрены две задачи случайного перемещения с ограничением между элементами, найдены условия существования и оценки количества возможных перемещения, предложены алгоритмы, позволяющие получить эти случайные перемещения.