REVUE FRANÇAISE D'INFORMATIQUE ET DE RECHERCHE OPÉRATIONNELLE. SÉRIE ROUGE

JEAN-LOUIS NICOLAS

Calcul de l'ordre maximum d'un élément du groupe symétrique S_n

Revue française d'informatique et de recherche opérationnelle. Série rouge, tome 3, n° R2 (1969), p. 43-50

<http://www.numdam.org/item?id=M2AN_1969__3_2_43_0>

R.I.R.O.
(3e année, N° R-2/1969, p. 43-50)

CALCUL DE L'ORDRE MAXIMUM D'UN ELEMENT DU GROUPE SYMETRIQUE S_n

par Jean-Louis NICOLAS (1)

Résumé. — *Soit S_n le groupe des permutations de n objets. On désigne par $g(n)$ l'ordre maximal d'un élément de S_n. Cet article expose un algorithme de construction d'une table des valeurs de $g(n)$. On calcule pour cela des fonctions $g_k(n)$ par récurrence sur k, et pour k assez grand, on démontre : $g(n) = g_k(n)$. Dans les programmes, $g(n)$ qui est un entier trop gros pour pouvoir être traité comme tel en machine, est considéré comme un réel. On évite les erreurs de comparaison des nombres en virgule flottante, en constatant que le quotient des nombres à comparer n'est pas trop proche de 1. Les résultats obtenus sont les suivants :*
1) *une table de $g(n)$ jusqu'à $n = 8\,100$, avec la décomposition en facteurs premiers de $g(n)$.*
2) *Une table des valeurs de n pour lesquelles $g(n)$ est différent de $g(n-1)$ ainsi que les 8 premiers chiffres de $g(n)$ jusqu'à $n = 32\,000$.*

Soit S_n le groupe des permutations de n éléments. L'ordre d'une permutation $\sigma \in S_n$ est le plus petit entier $m \geqslant 1$ tel que σ^m soit la permutation identique. E. Landau [1], § 61 définit la fonction :

$$g(n) = \max_{\sigma \in S_n} [\text{ordre de } \sigma] \tag{1}$$

et démontre $\log g(n) \sim \sqrt{n \log n}$. Dans [2] et [4] nous avons démontré plusieurs propriétés arithmétiques de la fonction $g(n)$.

L'objet de cet article est d'exposer un algorithme de construction d'une table de valeurs de $g(n)$.

§ 1. CALCUL THEORIQUE

Un élément $\sigma \in S_n$ se décompose en cycles de façon unique. Par exemple, pour $n = 9$,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (1\ \ 9\ \ 5)(2\ \ 8\ \ 4\ \ 6)(3\ \ 7)$$

(1) Ce travail a été rédigé alors que l'auteur était détaché à l'Université de Sherbrooke, province de Québec, Canada.

L'ordre d'un élément est donc le p.p.c.m. des longueurs de ses cycles. Dans l'exemple ci-dessus, l'ordre est donc 12.

Si $\sigma \in S_n$, soient $n_1, n_2, ..., n_k$ les longueurs de ses cycles; on a :

$$n = n_1 + n_2 + ... + n_k$$

Ordre de σ = p.p.c.m. $(n_1, n_2, ..., n_k)$.

D'autre part une partition de n est un système quelconque d'entiers $\geqslant 1$: $(n_1, n_2, ..., n_k)$ tels que $n = n_1 + n_2 + ... + n_k$. Par exemple, le nombre $n = 5$ a 7 partitions :

$$5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1$$
$$= 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1$$

Il est facile de construire une permutation de n objets ayant k cycles de longueur $(n_1, n_2, ..., n_k)$. A $5 = 2 + 2 + 1$, on associe, par exemple :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{pmatrix}$$

Si $n = n_1 + n_2 + ... + n_k$ est une partition quelconque de n, il existe donc un élément de S_n dont l'ordre est : p.p.c.m. $(n_1, n_2, ..., n_k)$. On a donc :

$$g(n) = \max_{\mathfrak{P}(n)} [\text{p.p.c.m.}(n_1, n_2, ..., n_k)] \tag{2}$$

$\mathfrak{P}(n)$ désignant l'ensemble des partitions de n.

On a les propriétés suivantes : (voir [1])

— $g(n)$ divise $n!$

— $g(n)$ est croissante (soit $\sigma \in S_n$; l'élément $\sigma' \in S_{n+1}$, qui laisse invariant $(n + 1)$ et coïncide ailleurs avec σ a même ordre que σ).

— Tableau des valeurs :

n	3	4	5	6	7	8	9	10	11	12	13
$g(n)$	3	4	6	6	12	15	20	30	30	60	60
$\mathfrak{P}$	3	4	2, 3	1, 2, 3 6	3, 4	3, 5	4, 5	2,3,5	1, 2, 3, 5 5, 6	3, 4, 5	1, 3, 4, 5

La troisième ligne indique la (ou les) partition(s) de n d'ordre $g(n)$.

— $g(n)$ n'est pas strictement croissante : $g(12) = g(13)$.

— Pour $n = 6$, $n = 11$, on constate que plusieurs partitions sont d'ordre $g(n)$ (on appelle ordre d'une partition l'ordre d'un élément σ de S_n associé).

— Parmi les partitions d'ordre $g(n)$, il en existe une, telles que les $(n_i)_{1 \leqslant i \leqslant k}$ soient des puissances de nombres premiers ou des 1. En effet si :

$$n = n_1 + n_2 + \ldots + n_k$$

et si $n_1 = ab$, avec $a > 1$, $b > 1$, $(a, b) = 1$, $a, b \in \mathbf{N}$, on a :

$$ab - (a + b) = (a - 1)(b - 1) - 1 \geqslant 0$$

et les partitions :

$$n = a + b + n_2 + \ldots + n_k + \underbrace{1 + 1 + \ldots + 1}_{ab-(a+b)} = ab + n_2 + \ldots + n_k$$

ont même ordre, les multiples de ab étant les mêmes que ceux de a et b puisque $(a, b) = 1$.

Dans la formule (2) on peut donc se restreindre au cas où $n_i = p^r$:

$$g(n) = \max_{\Sigma p^r \leqslant n} \Pi p^r \tag{3}$$

le « max » s'étendant à tous les systèmes de couples p, r (p premier, $r \in \mathbf{N}$) de somme $\Sigma p^r \leqslant n$.

Nous allons maintenant définir une fonction arithmétique l à laquelle $g(n)$ est attachée de façon simple.

Définition : Soit $l : \mathbf{N}^* \to \mathbf{N}$ définie par

$$\begin{cases} l(1) = 0 \\ l\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \sum_{i=1}^{k} p_i^{\alpha_i} \quad \text{avec } p_i \text{ premier et } \alpha_i \text{ entier} \geqslant 1 \end{cases} \tag{4}$$

Autrement dit, pour calculer $l(n)$, on écrit la décomposition en facteurs premiers de n et on ajoute les facteurs ainsi écrits.

Par exemple pour $n = 36 = 2^2 \cdot 3^2$, on a : $l(n) = 4 + 9 = 13$.

La fonction arithmétique l est additive :

$$(m, n) = 1 \Rightarrow l(m, n) = l(m) + l(n)$$

et sa restriction aux nombres p^α (p premier, $\alpha \geqslant 1$) est l'application identique. On a $l(n) \leqslant n$ pour tout n et $l(n) = n$ entraîne $n = p^\alpha$.

La formule (3) devient alors :

$$g(n) = \max_{l(j) \leqslant n} j \tag{5}$$

On remarque que cette formule permet de définir $g(0) = 1$ et que l'on a pour tout n :

$$l(g(n)) \leqslant n. \tag{6}$$

La formule (5) nous servira désormais de définition de $g(n)$.

Les fonctions $g_k(n)$

On désigne par p_k le k-ième nombre premier ($p_1 = 2, p_2 = 3, \ldots$) et par H_k l'ensemble des nombres entiers qui n'ont pas d'autres diviseurs premiers que $p_1, p_2, \ldots, p_k$. Ainsi $H_1 = \{ 1, 2, 4, 8, 16, \ldots \}$,

$$H_2 = \{ 1, 2, 3, 4, 6, 8, 9, 12, 16, 24, \ldots \}.$$

On définit alors :

$$g_k(n) = \max_{\substack{l(j) \leqslant n \\ j \in H_k}} j \tag{7}$$

On constate que $g_1(0) = 1$ et que, pour $n \geqslant 1$, $g_1(n)$ est la puissance de 2 immédiatement inférieure ou égale à n.

Calcul de g_2. Écrivons

$$H_2 = \bigcup_{i \geqslant 0} H_2^i, \qquad \text{avec} \qquad H_2^0 = H_1, H_2^1 = 3H_1, \text{etc}, \ldots,$$

$$H_2^i = 3^i H_1 = \{ 3^i, 2 \cdot 3^i, 4 \cdot 3^i, \ldots \}$$

On aura :

$$g_2(n) = \max_{\substack{l(j) \leqslant n \\ j \in H_2}} j = \max_{i \geqslant 0} \left(\max_{\substack{l(j) \leqslant n \\ j \in H_2^i}} j \right) \tag{8}$$

Si $i = 0$,

$$\max_{\substack{l(j) \leqslant n \\ j \in H_2^i}} j = \max_{\substack{l(j) \leqslant n \\ j \in H_1}} j = g_1(n)$$

Si $i > 0$,

$$\max_{\substack{l(j) \leqslant n \\ \in H_2^i}} j = 3^i \cdot \max_{\substack{3^i + l(j') \leqslant n \\ j' \in H_1}} = 3^i g_1(n - 3^i)$$

La formule (8) devient :

$$g_2(n) = \max [g_1(n), 3g_1(n-3), 9g_1(n-9), \ldots, 3^i g_1(n-3^i)]$$

le dernier terme du crochet étant tel que $3^i \leqslant n$.

Exemple $g_2(18) = \max [16, 3 \cdot 8, 9 \cdot 8] = 72$.

Formule de récurrence. Par la même méthode, on démontre que, pour tout $k \geqslant 2$, on a :

$$g_k(n) = \max [g_{k-1}(n), p_k g_{k-1}(n - p_k), \ldots, p_k^i g_{k-1}(n - p_k^i)] \tag{9}$$

Cette formule nous permet de calculer de proche en proche les $g_k(n)$.

Calcul de $g(n)$. Soit $p = p_k$ le plus grand nombre premier divisant $g(n)$. Alors pour $k' \geqslant k$, $g_{k'}(n) = g(n)$. En effet :

$$g(n) = \max_{l(j) \leqslant n} j \qquad \text{et} \qquad g(n) \in H_{k'}$$

donc :

$$g(n) = \max_{\substack{l(j) \leqslant n \\ j \in H_{k'}}} j = g_{k'}(n)$$

La formule (3) ou la formule (6) indiquent : $p \leqslant n$. En fait, on démontre (voir [2] ou [4] que $p \sim \sqrt{n \log n}$ et il est possible d'adapter la démonstration pour montrer que $p \leqslant a\sqrt{n \log n}$ avec $a > 1$. Pour dresser la table de $g(n)$ pour $n = 1$ à N, il suffit donc de calculer $g_k(n)$ de $n = 1$ à N avec k assez grand.

Pour $N = 32\,000$, $\sqrt{N \log N} = 575$, on prend $k = 140$, $p_k = 809$ ce qui correspond à : $a = 1{,}4$. En fait le plus grand nombre premier utilisé est $641 = p_{116}$ ce qui fait que :

$$\text{pour } n \leqslant 32\,000 \quad , \quad g(n) = g_{116}(n) = g_k(n) \text{ pour } k \geqslant 116$$

§ 2. PROGRAMME DE CALCUL POUR $g_k(n)$ EN LANGAGE FORTRAN

Au début du programme, la machine a en mémoire les nombres premiers $P(K)$ de $K = 1$ à $KMAX$ et $G(N)$ est égal à $g_1(N)$ de $N = 1$ à $NMAX$.

```
    DØ 12  K = 2, KMAX
    N = NMAX
 5  I = 1
    Z = P(K)
 6  IF(G(N) — Z* G(N — Z)) 9, 9, 8
 9  G(N) = Z* G(N — Z)
 8  I = I + 1
    Z = Z* P(K)
16  IF(N — Z) 11, 11, 6
11  N = N — 1
17  IF(N — P(K)) 12, 80, 5
80  IF(K · EQ · 2)  G(3) = 3
12  CØNTINUE
```

Il est commode de faire décroître N (Instruction étiquetée 11). En effet, le calcul étant arrivé à $K = K_0$ et $N = N_0$, l'ordinateur a en mémoire pour $G(N)$:

$$\text{si} \quad N > N_0 \qquad G(N) = g_{K_0}(N)$$

$$\text{si} \quad N \leqslant N_0 \qquad G(N) = g_{K_0-1}(N)$$

En particulier, dans l'instruction étiquetée 6, $G(N-Z)$ représente $g_{K-1}(N-Z)$ et $G(N)$ représente le nombre que l'on augmente petit à petit (lorsque I augmente) par l'instruction étiquetée 9, pour devenir $g_K(N)$.

L'instruction étiquetée 80 est introduite pour compenser la lacune suivante. Le programme précédent ne tient pas compte du cas $n = p_k^i$ de la formule de récurrence (9). Si dans cette formule, c'est $p_k^i g_{k-1}(0)$ qui réalise le maximum, alors $g_k(n)$ est une puissance exacte de nombre premier. On montre facilement que ça n'arrive pour $k \geqslant 2$ que lorsque $k = 2$ et $n = 3$.

Enfin, lorsque $p_k^2 \geqslant NMAX$, la formule de récurrence (9) devient :

$$g_k(n) = \max\left[g_{k-1}(n), p_k g_{k-1}(n-p_k)\right]$$

et le programme se simplifie.

§ 3. PROGRAMME G 32000

L'ordinateur utilisé est le C.D.C. 3600 de l'Institut Blaise-Pascal de la Faculté des Sciences de Paris. Sa mémoire est de 32 767 mots de 48 bits.

On fixe $NMAX = 32\,000$, $KMAX = 140$, $P(140) = 809$. On prend $G(N)$ en virgule flottante. La comparaison étiquetée 6 peut être douteuse. On la remplace par :

6 $IF(G(N) - A*Z*G(N-Z))$ 7, 7, 8

7 $IF(G(N) - B*Z*G(N-Z))$ 9, 9, 10

On prend initialement $A = 1.01$ et $B = 1/A$. Si l'on arrive à l'instruction étiquetée 7 et si le nombre $G(N) - B*Z*G(N-Z)$ est positif, c'est que le quotient $G(N)/Z*G(N-Z)$ est compris entre B et A. Dans l'instruction étiquetée 10 et les suivantes, on imprime les nombres K, N, Z et le quotient $G(N)/Z*G(N-Z)$ et l'on remplace A et B par des valeurs plus voisines de 1. La valeur finale de A est : $AMIN = 1{,}000\,009\,299\,3$, ce qui fait que tous les quotients sont ou bien supérieurs à $AMIN$ ou inférieurs à $1/AMIN$.

On détermine également pour chaque i la plus petite valeur $m_k(i)$ de n telle que p_k^i divise $g_k(n)$. C'est la plus petite valeur de n pour laquelle l'instruction étiquetée 9 est utilisée. Il suffit de rajouter après l'instruction étiquetée 9 l'instruction suivante :

$$M(I) = N$$

et d'imprimer $M(I)$ avant d'augmenter K. C'est ainsi que l'on voit que les nombres premiers au-delà de 641 ne servent pas.

Enfin, cette table permet de déterminer les intervalles sur lesquels $g(n)$ est constante. En effet, on peut montrer que si les nombres $g(n)$ et $g(n-1)$ sont différents, alors $\frac{g(n)}{g(n-1)} \geqslant AMIN$. On pose $A = \frac{1 + AMIN}{2}$ et on imprime N et $G(N)$ lorsque $G(N) \geqslant A * G(N-1)$. La table contient ainsi 10 923 valeurs différentes de $g(n)$. On obtient :

$$g(32\,000) = g(31\,999) = 2{,}785\,921\,329 \cdot 10^{261}$$

§ 4. PROGRAMME G 8100

Dans ce programme, on limite la table à $NMAX = 8\,100$ et $KMAX = 90$. (En fait les résultats du programme précédent auraient permis de prendre $KMAX = 63$.) Mais on va obtenir la décomposition en facteurs premiers de $g(n)$. Cette décomposition va être inscrite sur trois nombres entiers : $MU1(N)$, $MU2(N)$, $MU3(N)$. Si la décomposition en facteurs premiers de $g(n)$ s'écrit :

$$g(n) = 2^{\alpha_1} 3^{\alpha_2}, \ldots p_k^{\alpha_k} \ldots,$$

On a :

$$2^{\alpha_1} \leqslant 8\,100,\ 3^{\alpha_2} \leqslant 8\,100, \ldots p_k^{\alpha_k} \leqslant 8\,100, \text{ d'après (6)}$$

On a donc : $\alpha_1 \leqslant 12$, $\alpha_2 \leqslant 9$, ..., $\alpha_{14} \leqslant 9$;

$$p_{15} = 47 \quad \text{donc} \quad \alpha_{15} \leqslant 2, \ldots, \alpha_{43} \leqslant 2$$
$$p_{44} = 193 \quad \text{donc} \quad \alpha_{44} \leqslant 1, \ldots, \alpha_{90} \leqslant 1$$

$MU1(N)$ représente le nombre dont les chiffres décimaux sont $\alpha_1, \alpha_2, \ldots, \alpha_{14}$. $MU2(N)$ sera écrit en base 3 et $MU3(N)$ en base 2. On aura :

$$MU1(N) = \sum_{k=1}^{14} \alpha_k 10^{14-k} \ ; \ MU2(N) = \sum_{k=15}^{43} \alpha_k 3^{43-k} \ ; \ MU3(N) = \sum_{k=43}^{90} \alpha_k 2^{90-k}$$

Le calcul de ces nombres se fait en posant initialement :

$$MU1(N) = 10^{13} g_1(N) \qquad \text{et} \qquad MU2(N) = MU3(N) = 0.$$

On sépare la boucle K en 3 parties : $K = 2$ à 14; de 15 à 43; de 44 à 90. Et à chaque fois que l'on modifie la valeur de $G(N)$ par l'instruction étiquetée 9, on modifie la valeur de $MU1$:

```
9  G(N) = Z*G(N - Z)
   MU1(N) = MU1(N - Z) + 10**(14 - K)*I
```

Lorsque $15 \leqslant K \leqslant 43$, cela devient :

```
109  G(N) = Z*G(N - Z)
     MU1(N) = MU1(N - Z)
     MU2(N) = MU2(N - Z) + 3**(43 - K)*I
```

Résultats. — Là encore, on n'imprime pas $G(N)$ si $G(N) = G(N-1)$ c'est-à-dire si $MU_i(N) = MU_i(N-1)$ pour $i = 1, 2, 3$. Au moment de l'impression, on décodifie $MU1$, $MU2$, $MU3$ pour avoir les valeurs de α_k. On trouve ainsi pour $n = 8\,003$, $g(n) = 4{,}465\,189\,084 \cdot 10^{120}$

$$\alpha_1 = 5,\ \alpha_2 = 4,\ \alpha_3 = 2,\ \alpha_4 = 2,\ \alpha_5 = 2,\ \alpha_6 = \alpha_7 = \ldots = \alpha_{56} = 1,$$
$$\alpha_{57} = 0,\ \alpha_{58} = \alpha_{59} = 1,\ \alpha_{60} = 1,\ \alpha_{61} = 0\ \alpha_{62} = 1,$$

et pour $k > 62$, $\alpha_k = 0$. On remarque que $269 = p_{57}$ et $283 = p_{61}$ ne divisent pas $g(8\,003)$.

Il me reste à remercier M. le professeur R. de Possel qui a dirigé ce travail qui constituait mon deuxième sujet de thèse et M. Tréhel qui a bien voulu relire mon manuscrit.

REFERENCES

[1] E. LANDAU, «Handbuch der Lehre Von der Verteilung der Primzahlen» Leipzig und Berlin, B. G. Teubner 1909 (2te Auflage, New York, 1953).

[2] J. L. NICOLAS, « Sur l'ordre maximum d'un élément dans le groupe S_n des permutations », *Acta Arithmetica* (14), 1968, pp. 315-332.

[3] J. L. NICOLAS, Ordre maximal d'un élément du groupe des permutations et nombres très hautement abondants », *C.R. Acad. Sc. Paris* (266), 1968, p. 513-515.

[4] J. L. NICOLAS, « Ordre maximal d'un élément du groupe des permutations et highly composite numbers » (Thèse) à paraître au *Bulletin de la Soc. Math. de France* (1969).