Permutations, prétraitement

Entrée: permutations $g_1, g_2, \ldots, g_r$ de $\{1, 2, \ldots, n\}$
Sortie: tableau $T[i,j]$, $1 \leq i \leq j \leq n$.

$T \leftarrow$ partout la permutation *Ident*
`pour` $k \leftarrow 1$ jusqu'à r
  tamiser(g_k)
`tantque` il reste dans T un couple g, h de permutations non considéré
  tamiser($g \star h$)

où tamiser(p) consiste à effectuer:

$\pi \leftarrow p$
`tantque` $\pi \neq$ *Ident* `faire`
  $i \leftarrow$ plus petit point non fixé par π
  $j \leftarrow$ image de i selon π
  `si` $T[i,j] =$ *Ident* `alors` $T[i,j] \leftarrow \pi$
  $\pi \leftarrow \pi \star (T[i,j])^{-1}$

$\boxed{\text{On obtient du tableau } T}$

<u>Test d'appartenance</u>:

Donnée: permutations h et $g_1, g_2, \ldots, g_r$

Déterminer: si $h \in \langle g_1, g_2, \ldots, g_r \rangle$.

```
former T en prétraitant g1, g2, ..., gr
si tamiser(h) ajoute à T alors retourner faux
sinon retourner vrai .
```

<u>Ordre du groupe engendré</u>:

Donnée: permutations $g_1, g_2, \ldots, g_r$

Déterminer: $|\langle g_1, g_2, \ldots, g_r \rangle|$.

```
former T en prétraitant g1, g2, ..., gr
ordre ← 1
pour i ← 1 jusqu'à n faire
      m ← 1 + |{j | j > i et T[i, j] ≠ Ident}|
      ordre ← ordre × m
retourner ordre.
```

$\boxed{\text{Principale propriété de tamiser}(p),\ p \neq \textit{Ident}}$

Soit:

- $s =$ plus petit point non fixé par p
- $T[t, j]$ = dernière entrée examinée lors du tamisage de p.

Alors:

- $s \leq t$
- après tamiser(p), p s'exprime sous la forme

$$T[t, j] \star T[t-1, j_{t-1}] \star \cdots \star T[s+1, j_{s+1}] \star T[s, j_s].$$

PREUVE: induction sur le nombre de tours de la boucle `tantque` lors du tamisage.

PREUVE: détails

Par inspection, notons d'abord que pour tout $1 \leq i < j \leq n$, $T[i,i]$ contiendra toujours `Ident` et $T[i,j]$ contiendra toujours une permutation qui fixe $1, 2, \ldots, i-1$ et qui envoie i à j.

Base de l'induction. Soit $n = 1$. Si p fut tamisée en un seul tour de boucle, alors

Cas 1: $T_{avant}[s, s^p] = \texttt{Ident}$. Dans ce cas

$$T[s, s^p] \leftarrow p$$

fut effectuée, d'où $T[s, s^p] = p$ à la fin du tour.

Cas 2: $T_{avant}[s, s^p] \neq \texttt{Ident}$. Puisqu'un seul tour a suffi, $p \star T_{avant}[s, s^p]^{-1} = \texttt{Ident}$. Donc $p = T_{avant}[s, s^p]$, et le tamisage de p laisse T inchangé.

Pas de l'induction: Soit $n-1 \geq 1$, et soit p tamisée en n tours de boucle. Après le premier tour, π avait la valeur $p \star T[s, s^p]^{-1}$. Puisque $p \star T[s, s^p]^{-1}$ fut tamisée en $n-1$ tours, l'hypothèse d'induction permet d'écrire

$$p \star T[s, s^p]^{-1} = T[t, j] \star a_{t-1} \star \cdots \star a_\sigma,$$

où le plus petit point non fixé par $p \star T[s, s^p]^{-1}$ est σ, où chaque a_k provient de la ligne k, et où $T[t, j]$ fut la dernière entrée considérée lors du tamisage de $p \star T[s, s^p]^{-1}$ (donc du tamisage de p). Notons que $T[s, s^p]$, du fait qu'elle provient de la ligne s, fixe $1, 2, \ldots, s-1$ et envoie s à s^p. Ainsi $p \star T[s, s^p]^{-1}$ fixe $1, 2, \ldots, s$. Donc $\sigma > s$. Puisque

$$p = T[t, j] \star a_{t-1} \star \cdots \star a_\sigma \star T[s, s^p],$$

on conclut en insérant au besoin des $T[i, i]$ entre a_σ et $T[s, s^p]$.

Fin de la PREUVE.