8 - Algorytm Schreiera-Simsa

Saturday, 22 June 2024 11:23

Mamy dany zbiór permutacji Σ.

Ile elementów ma grupa A generowana przez Σ?

$\Sigma = \{\sigma_1, \dots, \sigma_k\}$

Stabilizator w grupie A

$A_i = \{\pi \in A : \pi(i) = i\}$

Orbita w grupie A

$O_i = \{\pi(i) : \pi \in A\}$

Lemat

$|A| = |A_1| \cdot |O_1|$

dowód:

$B_x = \{\pi \in A : \pi(1) = x\}$

$B_1 = A_1$

$B_i \neq \emptyset \Rightarrow i \in O_1$

Chcemy pokazać, że wszystkie niepuste B_x są równoliczne.

Wtedy $|A| = |A_1| \cdot |O_1|$, bo $\sum_x |B_x| = |A|$ Bierzemy dowolne π_x: $\pi_x(1) = x$ i dostajemy bijekcję.

A_1 to tak naprawdę $N-1$-elementowe permutacje, więc obliczamy $|O_1|$ i wywołujemy się rekurencyjnie.

- Obliczanie $|O_1|$ jest proste.

Robimy bfs na grafie z elementów permutacji. Σ wyznacza krawędzie.

Dla każdego elementu $x \in O_1$ wyznaczamy permutację π_x: $\pi_x(1) = x$.

Teraz potrzebujemy wygenerować generator grupy A_1.

Rozważmy permutację: $\tau_{i,x} = \overset{\sigma_i(x) \to 1}{\pi^{-1}_{\sigma_i(x)}} \circ \overset{x \to \sigma_i(x)}{\sigma_i} \circ \overset{1 \to x}{\pi_x}$

czyli permutacja przeprowadzająca x na i.

Zauważmy, że $\tau_{i,x}(1) = 1 \Rightarrow \tau_{i,x} \in A_1$

Lemat Schreiera

$\Sigma' = \{\tau_{i,x} : 1 \leq i \leq k, 1 \leq x \leq N\}$ generuje A_1

Weźmy dowolne $\mathcal{S} \in A_1$

$\mathcal{S} = \alpha_s \circ \alpha_{s-1} \circ \dots \circ \alpha_1$ gdzie $\alpha_i \in \Sigma$

Niech $y_j = \alpha_j \circ \alpha_{j-1} \circ \dots \circ \alpha_1(1)$

Między każde $j, j+1$ wstawmy $\pi_{y_j} \circ \pi_{y_j}^{-1}$

Wtedy:

$\mathcal{S} = \alpha_s \circ \pi_{y_s} \circ \pi_{y_s}^{-1} \circ \pi_{y_{s-1}} \circ \alpha_{s-1} \circ \dots \circ \pi_{y_1}^{-1} \circ \alpha_1$

dokładając $\pi_1^{-1} \circ \dots \circ \pi_1$ dostajemy postać $\tau_{i,x}$.

Filtr Simsa

Permutacja $\mathcal{S} \neq id$ jest klasy (i,j): $\mathcal{S}(i' < i) = i$, $\mathcal{S}(i) = j$

Można zredukować Σ' tak, aby była w nim tylko jedna permutacja każdej klasy.

Będziemy „filtrować" zbiór P do Q. Początkowo $Q := \emptyset$

Dwa niezmienniki

- $P \cup Q$ generują tę samą grupę
- W Q jest co najwyżej jeden element tej samej klasy.

Weźmy dowolną permutację $\mathcal{S} \in P$ klasy (i,j)

1. Jeśli w Q nie ma permutacji tego typu to przerzucamy $\mathcal{S}$ do Q.

2. Jeśli w Q jest permutacja ρ klasy (i,j) to zamieniamy $\mathcal{S}' := \rho^{-1} \circ \mathcal{S}$ i kontynuujemy.

Nie tracimy $\mathcal{S}$, bo $\mathcal{S} = \rho \circ \mathcal{S}'$.

Złożoność:

N - początkowa ilość elementów.

Szukanie orbity: $O(N \cdot |\Sigma|)$

Filtr: $O(N^2 \cdot |\Sigma'|) = O(N^3 \cdot |\Sigma|)$

Rekurencja: $O(N)$ $|\Sigma| = O(N^2)$

Całość: $O(N^6)$