MAT3 - RSA

Duży projekt

Jakub Howorus, Bartosz Polus, Kinga Konieczna, Jan Czechowski

Politechnika Warszawska

4 czerwca 2025

Spis treści

1. Zadania teoretyczne

2. Zadania praktyczne

Zadanie 1 - polecenie

Polecenie

Dla każdego $g \in G$, niech $\operatorname{Fix} g = \{x \in X \mid \varphi_g(x) = x\}$ będzie zbiorem elementów stałych ze względu na permutację φ_g. Pokazać, że jeśli N jest liczbą orbit działania φ, to

$$N = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix} g|.$$

Zadanie 1 - dowód

Lemat Burnside'a

W tym zadaniu mamy udowodnić Lemat Burnside'a. Zacznijmy od przedstawienia twierdzenia o orbitach i stabilizatorach, które mówi nam, że dla dowolnego $x \in X$ zachodzi nam taka równość:

$$|\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)| = |G|$$

Zdefiniujmy zbiór:

$$A = \{(g, x) \in G \times X \mid \varphi_g(x) = x\},$$

czyli zbiór wszystkich par, w których element $g \in G$ ustala punkt $x \in X$ na niego samego.

Zadanie 1 - dowód cd.

Krok 1: Liczenie $|A|$ przez sumowanie po g

Z jednej strony:

$$|A| = \sum_{g \in G} \mathrm{Fix}(g).$$

Krok 2: Liczenie $|A|$ przez sumowanie po x

Z drugiej strony:

$$|A| = \sum_{x \in X} |\mathrm{Stab}(x)|,$$

Z twierdzenia o orbicie-stabilizatorze:

$$|\mathrm{Stab}(x)| = \frac{|G|}{|\mathrm{Orb}(x)|}.$$

Zadanie 1 - dowód cd.

Krok 2: Liczenie $|A|$ przez sumowanie po x

Zatem:

$$|A| = \sum_{x \in X} \frac{|G|}{|\mathrm{Orb}(x)|}.$$

Krok 3: Grupowanie po orbitach

Niech $\mathcal{O}_1, \ldots, \mathcal{O}_r$ będą orbitami działania G na X.
Dla każdej orbity $\mathcal{O}_i$, wszystkie punkty $x \in \mathcal{O}_i$ mają tę samą wartość $|\mathrm{Orb}(x)| = |\mathcal{O}_i|$, więc:

$$\sum_{x \in \mathcal{O}_i} \frac{|G|}{|\mathrm{Orb}(x)|} = |\mathcal{O}_i| \cdot \frac{|G|}{|\mathcal{O}_i|} = |G|.$$

Zadanie 1 - dowód cd.

Grupowanie po orbitach

Suma po wszystkich orbitach daje:

$$|A| = \sum_{i=1}^{N} |G| = N \cdot |G|.$$

Krok 4: Porównanie wyrażeń

Porównując dwie wyrażone wcześniej postacie $|A|$, mamy:

$$\sum_{g \in G} \mathrm{Fix}(g) = N \cdot |G|,$$

czyli:

$$N = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g).$$

Zadanie 2 - polecenie

Polecenie

Obliczyć, na ile sposobów można pokolorować wierzchołki sześcianu n kolorami.

Rozwiązanie

Grupa symetrii sześcianu (izometrii zachowujących sześcian) jest znana jako grupa ośmiościenna i ma rząd $|G|=24$. Składa się z następujących elementów:

- 1 - identyczność,
- 9 obrotów wokół osi przechodzących przez środki przeciwległych ścian (kąty 90°, 180°, 270°),
- 6 obrotów wokół osi przechodzących przez przeciwległe wierzchołki (kąty 120°, 240°),
- 8 obrotów wokół osi przechodzących przez środki przeciwległych krawędzi (kąt 180°).

Zadanie 2

Rozwiązanie cd.

Liczba orbit, czyli nieidentycznych kolorowań jest równa (korzystamy z zadania 1):

$$N = \frac{1}{|G|} \sum_{g \in G} |Fixg|$$

gdzie Fix_g to zbiór kolorowań niezmienniczych względem działania g.

Zadanie 2

$|Fix_g|$

Teraz policzmy $|Fix_g|$ dla każdego typu elementów grupy:

- **Identyczność** (1 element) - wszystkie kolorowania są niezmiennicze, zatem:

$$|Fixg| = n^8$$

- **Obroty o 90° i 270°** (6 elementów) - aby kolorowanie było niezmiennicze, wszystkie 4 wierzchołki na ścianie muszą mieć ten sam kolor. Zatem są to dwie ściany, każda jednolita:

$$|Fixg| = n^2$$

- **Obroty o 180°** (3 elementy) - wierzchołki muszą być w parach przeciwległych.

$$|Fixg| = n^4$$

Zadanie 2

$|Fix_g|$ cd.

- **Obroty o 120° i 240°** (8 elementów) - wierzchołki muszą być w trójkach związanych obrotem wokół przekątnej sześcianu. Mamy 4 niezależne wybory: 2 kolory dla trójek + 2 kolory dla wierzchołków stałych), zatem:

$$|Fixg| = n^4$$

- **Obroty o 180° wokół osi przez środki krawędzi** (6 elementów) - wierzchołki muszą być w czterech parach związanych obrotem.

$$|Fixg| = n^4$$

Punkty stałe i liczba orbit

Sumowanie punktów stałych:

$$\sum_{g \in G} |Fixg| = 1 \cdot n^8 + 6 \cdot n^2 + 3 \cdot n^4 + 8 \cdot n^4 + 6 \cdot n^4$$

$$\sum_{g \in G} |Fixg| = n^8 + 17n^4 + 6n^2$$

Obliczenie liczby orbit:

$$N = \frac{1}{24}(n^8 + 17n^4 + 6n^2)$$

Zatem ostateczna liczba nieidentycznych kolorowań wierzchołków sześcianu przy użyciu n kolorów wynosi:

$$N = \frac{n^8 + 17n^4 + 6n^2}{24}$$

Zadanie 3

Polecenie

Wyznaczyć liczbę obwodów z trzema przełącznikami, nierównoważnych względem permutacji sygnałów wejściowych.

Rozwiązanie

Dwa obwody logiczne są równoważne względem permutacji sygnałów wejściowych, jeśli po zamianie miejscami wejść (przełączników) jeden obwód zachowuje się identycznie jak drugi.

Dla trzech przełączników A, B, C, otrzymujemy $2^3 = 8$ możliwych kombinacji na wejściu obwodu.

Obwód z trzema przełącznikami to dowolna funkcja logiczna

$$f : \{0,1\}^3 \to \{0,1\}$$

Zadanie 3

Rozwiązanie cd.

Ponieważ dla każdej z kombinacji możemy otrzymać na wyjściu 0 lub 1 istnieje liczba obwodów z trzema przełącznikami wynosi

$$|X| = 2^8 = 256$$

Zbiór G jest zbiorem wszystkich permutacji g zbioru trzyelementowego i wynosi

$$|G| = 6$$

Permutacje g działają na zbiorze $X = \{0,1\}^3$ (8-elementowym) i dzielą go na rozłączne orbity. Funkcja f należy do Fix_g wtedy i tylko wtedy, gdy ma taką samą wartość na wszystkich elementach każdej orbity.
Jeśli permutacja g dzieli X na m orbit, to:

$$|\mathrm{Fix}_g| = 2^m.$$

Zadanie 3

Rozwiązanie cd.

Dla wszystkich $g \in S_3$:

- id — permutacja tożsamościowa: $m = 8$, więc $|\mathrm{Fix}_{\mathrm{id}}| = 2^8 = 256$.
- Trzy transpozycje (np. (AB)): $m = 6$, więc każda ma $|\mathrm{Fix}_g| = 2^6 = 64$.
- Dwa cykle 3-elementowe $((ABC), (ACB))$: $m = 4$, więc każda ma $|\mathrm{Fix}_g| = 2^4 = 16$.

Podstawiamy do wzoru z zadania 1:

$$N = \frac{1}{6}\left(256 + 3 \cdot 64 + 2 \cdot 16\right) = \frac{1}{6}(256 + 192 + 32) = \frac{480}{6} = 80$$

Zadanie 4 (Praktyczne)

Polecenie

Znaleźć wszystkie kolorowania wierzchołków sześcianu dwoma kolorami.

To zadanie zostało zrealizowane w środowisku **Wolfram Mathematica**.

Zadanie 5 (Praktyczne)

Polecenie

Znaleźć wszystkie, nierównoważne względem permutacji sygnałów wejściowych, obwody z trzema przełącznikami.

To zadanie zostało zrealizowane w środowisku **Wolfram Mathematica**.

Dziękujemy za uwagę!

Pytania?

Prezentację przygotowali:

Kinga Konieczna
Jan Czechowski
Jakub Howorus
Bartosz Polus