

**WYŻSZA SZKOŁA
INFORMATYKI STOSOWANEJ
I ZARZĄDZANIA**

pod auspicjami POLSKIEJ AKADEMII NAUK

**Wydział INFORMATYKI
studia inżynierskie i uzupełniające studia magisterskie**

**Wydział INFORMATYCZNYCH TECHNIK ZARZĄDZANIA
studia licencjackie, inżynierskie i uzupełniające studia
magisterskie**

ul. Newelska 6, 01-447 Warszawa

<http://www.wit.edu.pl>

ISBN 978-83-88311-96-3

M. Libura, J. Sikorski - WYKŁADY Z MATEMATYKI DYSKRETNIEJ. Cz. I - Wyd. 5

**WYŻSZA SZKOŁA
INFORMATYKI STOSOWANEJ
I ZARZĄDZANIA**



**Marek Libura
Jarosław Sikorski**

**WYKŁADY Z MATEMATYKI DYSKRETNIEJ
Cz. I: Kombinatoryka**

Warszawa 2008

dr hab. inż. Marek Libura

*Instytut Badań Systemowych Polskiej Akademii Nauk
ul. Newelska 6, 01-447 Warszawa*

*Wyższa Szkoła Informatyki Stosowanej i Zarządzania
ul. Newelska 6, 01-447 Warszawa*

dr inż. Jarosław Sikorski

*Instytut Badań Systemowych Polskiej Akademii Nauk
ul. Newelska 6, 01-447 Warszawa*

*Wyższa Szkoła Informatyki Stosowanej i Zarządzania
ul. Newelska 6, 01-447 Warszawa*



Copyright © by Marek Libura and Jarosław Sikorski
Warszawa 2008

All rights reserved

ISBN 978-83-88311-96-3

Druk:
Zakład Poligraficzny
Jerzy Kosiński, Warszawa

Przedmowa do Części I

Niniejsza książka jest pierwszą częścią dwutomowego podręcznika:

M. Libura, J. Sikorski – *Wykłady z matematyki dyskretniej.*

Część druga (wydanie czwarte) ukazała się w roku 2008 w Wydawnictwie WIT Wyższej Szkoły Informatyki Stosowanej i Zarządzania w Warszawie pod następującym tytułem ([16]):

M. Libura, J. Sikorski – *Wykłady z matematyki dyskretniej.
Część II: Teoria grafów.*

Obie części podręcznika mogą być czytane w znacznym stopniu niezależnie. Wymagało to wprowadzenia pewnych – stosunkowo niewielkich powtórzeń.

W tekście niniejszej książki znajdują się odnośniki do materiału z Części II. Odróżniają się one od innych cytowań pozycji literaturowych tym, że podają również strony, na których można znaleźć odpowiedni materiał.

Warszawa, wrzesień 2008 r.

Autorzy

Przedmowa

Książka ta powstała na podstawie wykładów z matematyki dyskretnej, które prowadziliśmy w latach 1998 – 2008 dla studentów trzeciego semestru Wydziału Informatyki w Wyższej Szkole Informatyki Stosowanej i Zarządzania w Warszawie. Przygotowując zajęcia korzystaliśmy z różnych książek i artykułów. Po to, by studenci nasi mogli używać tych źródeł nie mając jeszcze kompletnego tekstu podręcznika, staraliśmy się, aby poszczególne partie materiału w miarę możliwości zachowywały układ, terminologię i notację stosowane w tych tekstach. Nie zawsze było to możliwe, między innymi ze względu na konieczność ujednolicenia stosowanej notacji.

W niniejszej książce pozostały ślady pierwotnej postaci wykładu. Na przykład niektóre partie tekstu, dotyczące zliczania funkcji, naśladują w znacznym stopniu odpowiednie fragmenty z książki W. Lipskiego [17], teoria zliczania Pólya jest przedstawiona w układzie zbliżonym do książki C.L. Liu [19], fragmenty podrozdziałów, dotyczących teorii grafów, przypominają sposób prezentacji z książki R.J. Wilsona [33] itp. W trakcie kolejnych zmian w prowadzonym wykładzie, zmieniał się jednak również znacznic materiał w przygotowywanci przez nas książce. Dodane zostały nowe partie materiału, wielokrotnie zmieniano układ i sposób prezentacji. Starano się również ujednolicić stosowaną terminologię.

Jak większość podręczników, również i ten nie zawiera w zasadzie faktów, które nie były dotychczas prezentowane w innych monografiach i artykułach. Co więcej, należy stwierdzić, że wybór materiału z tak obserwnej dziedziny, jak matematyka dyskretna, jest z konieczności bardzo ograniczony. Tym niemniej, staraliśmy się, by podręcznik ten był w miarę możliwości samowystarczalny i prezentował w sposób możliwie nowoczesny podstawowe wiadomości. Z tego względu zamieszczone zostały zarówno najbardziej elementarne definicje i fakty, jak i twierdzenia oraz ich dowody, które bardzo trudno byłoby znaleźć Czytelnikowi w literaturze polskojęzycznej.

Matematyka dyskretna jest bardzo obszernym działem matematyki, złożącym się zbiorami skończonymi i przeliczalnymi. Liczne zastosowania matematyki dyskretnej w wielu dziedzinach sprawiają, że przeżywa ona w ostatnich latach ogromny rozwój. Niniejsza książka przedstawia jedynie skromny wybór zagadnień, które tradycyjnie zalicza się do matematyki dyskretnej. Zakres prezentowanego materiału jest dostosowany do programu studiów na Wydziale Informatyki WSISiZ i w związku z tym powinno się tu liczne działy matematyki dyskretnej, które znalazły się w innych prowadzonych na tym wydziale wykładach, takie jak na przykład kryptografia, teoria złożoności obliczeniowej, optymalizacja dyskretna itp.

Książka jest podzielona na dwie części, odpowiadające dwóm działom matematyki dyskretnej: kombinatoryce i teorii grafów.

Uzupełnieniem Części I jest *Dodatek*, w którym przypominamy niektóre podstawowe pojęcia z teorii mnogości, rachunku zdań i analizy matematycznej. W *Dodatku* do Części II zebrano zapisy wybranych procedur związanych z algorytmami grafowymi.

Pierwsza część książki, *Kombinatoryka*, składa się ze wstępu i trzech rozdziałów. Pierwszy z nich wprowadza podstawowe, używane dalej pojęcia, takie jak relacje, funkcje, zbiory z powtórzeniami, rozmieszczenia, podziały zbiorów i liczb, liczby specjalne, zbiory uporządkowane itp. Tam, gdzie jest to możliwe z wykorzystaniem dotychczas wprowadzonego aparatu, staramy się przedstawiać różnorodne zagadnienia zliczania, takie jak zliczanie funkcji różnych typów, zliczanie rozmieszczeń, podzbiorów zbiorów o zadanych właściwościach itd. Część zagadniców z tego zakresu wymaga jednak użycia bardziej zaawansowanych technik i dlatego rozważamy je dopiero w następnych rozdziałach.

Rozdział drugi, zatytułowany *Metody i techniki*, jest właśnie poświęcony prezentacji najważniejszych metod analizy kombinatorycznej. Szczególnie miejsce zajmuje tu technika funkcji tworzących ze względu na jej wszechstronność. W rozdziale tym omawiamy również dwie grupy metod, mazwane od zasad, na których są oparte, metodami włączania i wyłączenia oraz metodami szufla/kowymi. Różnorodne zagadnienia zliczania, które znalazły się w tym rozdziale, są przedstawione jako zastosowania omawianych technik.

Rozdział trzeci zawiera elementy ogólnej teorii zliczania. Obszerną jego część stanowi wprowadzenie, dotyczące właściwości permutacji oraz grup permutacji. Podstawowe twierdzenia teorii zliczania są ilustrowane różnymi przykładami ich zastosowań.

Druga część książki jest prezentacją wybranych zagadnień z zakresu Teorii grafów. Składa się z wprowadzenia oraz sześciu rozdziałów.

Pierwszy z nich przedstawia terminologię i podstawowe pojęcia dotyczące grafów nieskierowanych i skierowanych.

Drugi rozdział koncentruje się na badaniu dróg i cykli w grafach. Zaśadniczą częścią tego rozdziału jest przedstawienie warunków koniecznych i dostatecznych istnienia dróg oraz cykli Eulera i Hamiltona w grafach nieskierowanych i skierowanych.

Rozdział Drzewa i lasy omawia ważną klasę grafów bez cykli. Przedstawiane są właściwości takich grafów oraz ich zastosowania.

W rozdziale Spójność rozwijane są pojęcia spójności oraz k -spójności krawędziowej i wierzchołkowej grafów nieskierowanych i skierowanych.

Następny rozdział, zatytułowany Niezależność, obejmuje zagadnienia związane z pojęciem niezależności wierzchołków lub krawędzi grafów nieskierowanych. Znalazły się w nim zagadnienia zbiorów wewnętrznie stabilnych, problemy pokryć krawędziowych i wierzchołkowych oraz zagadnienia kolorowania wierzchołków albo krawędzi grafów.

Ostatni rozdział poświęcony jest jednemu wybranemu tematowi z zakresu problemów ekstremalnych na grafach, a mianowicie zagadnieniu przepływów w sieciach.

Obie części książki poprzedzone są krótkimi rozdziałami, w których wprowadzamy stosowaną notację.

Mimo że książka ma charakter podręcznika, celowo zrezygnowaliśmy z umieszczania w niej na końcach rozdziałów zadań do samodzielnego rozwiązania. Zamiast tego w treści książki znalazły się liczne przykłady. Stanowią one integralną część wykładu i nie powinny być pomijane przy lekturze. Oprócz tego, że stanowią one ilustrację rozważań, to czasem zawierają też pojęcia, które są wykorzystywane w dalszym toku wykładu.

Na koniec chcemy wspomnieć o stosowanej w książce konwencji, która może być uznana za dyskusyjną. Mianowicie, większość faktów matematycznych, dla których podajemy (a czasem – z konieczności – pomijamy) dowody, występuje pod nazwą *Twierdzeń*. Powoduje to wprawdzie nazywanie w ten sam sposób zarówno faktów bardzo prostych, jak i znacznie mniej oczywistych, ale uwalnia nas od ponawiania niefortunnych prób znajdowania odpowiednika dla angielskiego terminu *Proposition*.

Tekst tej książki został złożony przez Autorów w systemie L^AT_EX wyciągając pakietów MiK^TE_X 2.7 oraz CorelDRAW 12. Do obliczeń symbolicznych stosowano pakiet Mathematica 3.0.

Wielu naszych studentów i kolegów przekazało nam liczne sugestie, dotyczące wcześniejszych wydań niniejszego podręcznika; jesteśmy za nie wdzięczni. Pragniemy tu szczególnie podziękować Panu dr. Marcinowi Sydowowi za to, że przeczytał wstępную wersję tekstu pierwszego wydania książki i zechciał podzielić się z nami swoimi uwagami. Zdajemy sobie jednak sprawę z tego, że – mimo wielu wprowadzonych już zmian i poprawek – w tekście pozostały jeszcze błędy i uchybienia. Dziękujemy więc wdzięczni za wszelkie uwagi, które pozwolilyby nam na ich wyeliminowanie. Można je przesyłać na adres:

Marek Libura

Instytut Badań Systemowych Polskiej Akademii Nauk
ul. Newelska 6, 01-447 Warszawa

lub pocztą elektroniczną na adres:

Marek.Libura@ibspan.waw.pl

Warszawa, wrzesień 2008 r.

Autorzy

Spis treści

| | |
|---|-----------|
| 0.1 Notacja | ix |
| 1 Wprowadzenie | 1 |
| 1 Podstawowe pojęcia | 3 |
| 1.1 Relacje | 3 |
| 1.2 Funkcje | 8 |
| 1.2.1 Zliczanie funkcji | 10 |
| 1.3 Rozmieszczenia uporządkowane | 17 |
| 1.4 Podzbiory zbiorów | 21 |
| 1.4.1 Podzbiory k -elementowe zbiorów | 25 |
| 1.4.2 Współczynniki wielomianowe | 29 |
| 1.5 Zbiory z powtórzeniami | 34 |
| 1.6 Podziały zbioru | 37 |
| 1.6.1 Podziały zbiorów a relacje | 44 |
| 1.6.2 Podziały zbiorów a zliczanie surjekcji | 46 |
| 1.7 Podziały liczb | 48 |
| 1.8 Zbiory częściowo uporządkowane | 52 |
| 1.8.1 Łańcuchy i antylańcuchy w zbiorach częściowo upo- rządkowanych | 60 |
| 1.9 Podsumowanie | 64 |
| 2 Metody i techniki | 67 |
| 2.1 Funkcje tworzące | 67 |
| 2.1.1 Zastosowania funkcji tworzących | 76 |
| 2.2 Zasada włączania-wyłączania | 90 |
| 2.3 Zasada szufla | 97 |

| | |
|---|------------|
| 4 Elementy ogólnej teorii zliczania | 101 |
| 4.1 Wprowadzenie | 101 |
| 4.1.1 Permutacje i grupy permutacji | 103 |
| 4.1.2 Rozkład permutacji na cykle | 109 |
| 4.2 Orbita działania grupy permutacji | 118 |
| 4.2.1 Liczba orbit działania grupy | 121 |
| 4.3 Klasy równoważności funkcji | 131 |
| 4.4 Ogólne zagadnienie zliczania | 133 |
| Dodatek | 155 |

0.1 Notacja

Niniejszy podrozdział przedstawia podstawową notację, stosowaną w tej książce. Niektóre z używanych symboli są opisywane ponownie w miejscowościach, gdzie są po raz pierwszy wprowadzane. Ponadto, dodatkowe wyjaśnienia, związane z używaną notacją, są zawarte w *Dodatku*.

Dla dowolnego zdania Q , którego wartością logiczną może być „prawda” albo „fałsz”, stosujemy następujący zapis:

$$[Q] = \begin{cases} 1 & \text{jeśli zdanie } Q \text{ jest prawdziwe,} \\ 0 & \text{jeśli zdanie } Q \text{ jest fałszywe.} \end{cases}$$

Funktorzy zdaniotwórcze:

- \vee – *tub* (alternatywa, suma logiczna);
- \wedge – *i* (koniunkcja, iloczyn logiczny);
- \neg – *nie* (negacja);
- \Rightarrow – *jeśli ..., to ...* (implikacja);
- \Leftrightarrow – *wtedy i tylko wtedy, gdy* (równoważność).

Kwantyfikatory:

- \exists – *istnieje* (kwantyfikator egzystencjalny);
- \forall – *dla każdego* (kwantyfikator ogólny).

Dla zbioru X , zapis $x \in X$ oznacza, że x jest elementem tego zbioru, natomiast zapis $x \notin X$ oznacza, że x nie należy do zbioru X .

Symbol $|X|$ oznacza liczosć (moc) zbioru skońzonego X .

Oznaczenia zbiorów:

- $\mathbb{N} = \{0, 1, 2, \dots\}$ – zbiór liczb naturalnych;
- $\mathbb{N}_+ = \{1, 2, \dots\}$ – zbiór dodatnich liczb naturalnych;
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ – zbiór liczb całkowitych;
- $\mathbb{B} = \{0, 1\}$;
- \mathbb{R} – zbiór liczb rzeczywistych;
- \mathbb{C} – zbiór liczb zespolonych;
- \emptyset – zbiór pusty;
- $\{a\}$ – zbiór jednoelementowy, zawierający tylko element a ;
- $\{a_1, \dots, a_n\}$ – zbiór, którego elementami są a_i , $i = 1, \dots, n$;
- $\{x \in X : \mathcal{W}(x)\}$ – zbiór wszystkich elementów zbioru X , dla których wartością funkcji zdaniowej $\mathcal{W}(x)$ jest „prawda”.

Operacje na zbiorach:

- \cup – suma zbiorów;
- \cap – przeciecie zbiorów;
- \setminus – różnica zbiorów;
- \otimes – różnica symetryczna zbiorów;
- \times – iloczyn kartezjański zbiorów.

Dla zbiorów A, B , zapis $A \subseteq B$ oznacza, że A jest podzbiorem zbioru B , natomiast zapis $A \subset B$ jest używany wyłącznie w przypadku, gdy A jest podzbiorem właściwym zbioru B , tzn.

$$A \subset B \Leftrightarrow (A \subseteq B) \wedge (B \setminus A \neq \emptyset).$$

$\mathcal{P}(X)$ oznacza rodzinę wszystkich podzbiorów zbioru X .

Dla $a \in A, b \in B$, gdzie A i B są dowolnymi zbiorami, symbol (a, b) oznacza parę uporządkowaną o poprzedniku a i następniku b .

Podobnie, dla $n \in \mathbb{N}, n \geq 2$, symbolem (a_1, \dots, a_n) oznaczamy n -tkę uporządkowaną (wektor n -elementowy, ciąg n -elementowy).

Dla zbioru skończonego $X = \{x_1, \dots, x_n\}$ oraz jego podzbioru $Y \subseteq X$ symbolem $\xi(Y)$ oznaczamy wektor charakterystyczny zbioru Y , to znaczy $\xi(Y) = (\xi_1(Y), \dots, \xi_n(Y))$, gdzie $\xi_i(Y) = [x_i \in Y]$ dla $i = 1, \dots, n$.

Zbiór z powtórzeniami $Q = (X, p)$, dla którego zbiorem podstawowym jest n -elementowy zbiór $X = \{x_1, \dots, x_n\}$, a krotności elementów są dane przez ciąg liczb naturalnych $p = (k_1, \dots, k_n)$, jest oznaczany symbolem $\langle k_1 * x_1, \dots, k_n * x_n \rangle$.

Zbiór X uporządkowany przez relację częściowego porządku \preceq jest oznaczany symbolem (X, \preceq) . Dla zbioru częściowo uporządkowanego (X, \preceq) oraz dowolnego podzbiuru $A \subseteq X$, symbole $\inf A$ oraz $\sup A$ oznaczają, odpowiednio, kres dolny oraz kres góry zbioru A . Jeśli ponadto $a' = \inf A \in A$, to piszemy $a' = \min A$. Podobnie, jeśli $a'' = \sup A \in A$, to stosujemy zapis $a'' = \max A$.

Jeśli R jest relacją równoważności w zbiorze X i $x \in X$, to symbol x/R oznacza klasę abstrakcji relacji R wyznaczoną przez element x .

Zbiór wszystkich klas abstrakcji relacji R w zbiorze X oznaczamy symbolem X/R , tzn. $X/R = \{x/R : x \in X\}$.

0.1. NOTACJA

Dla funkcji, zdefiniowanych w iloczynie kartezjańskim $X \times Y$ zbiorów X i Y , stosujemy następujące oznaczenia:

- $\text{Fun}(X, Y)$ – zbiór wszystkich funkcji ze zbioru X w zbiór Y ;
- $\text{Inj}(X, Y)$ – zbiór wszystkich *iniekcji* w zbiorze $\text{Fun}(X, Y)$, czyli zbiór wszystkich funkcji różnowartościowych ze zbioru X w zbiór Y ;
- $\text{Sur}(X, Y)$ – zbiór wszystkich *surjekcji* w zbiorze $\text{Fun}(X, Y)$, czyli zbiór wszystkich funkcji ze zbioru X na zbiór Y ;
- $\text{Bij}(X, Y)$ – zbiór wszystkich *bijekcji* w zbiorze $\text{Fun}(X, Y)$, czyli zbiór wszystkich funkcji różnowartościowych ze zbioru X na zbiór Y .

Jeśli $f \in \text{Fun}(Y, Z)$ i $g \in \text{Fun}(X, Y)$, to symbolem fg oznaczamy funkcję ze zbioru $\text{Fun}(X, Z)$, będącą złożeniem funkcji f i g , to znaczy dla $x \in X$,

$$fg(x) = f(g(x)).$$

Dla dowolnej liczby rzeczywistej x używamy następujących oznaczeń:

$$\lfloor x \rfloor = \max\{y \in \mathbb{Z} : y \leq x\},$$

$$\lceil x \rceil = \min\{y \in \mathbb{Z} : y \geq x\}.$$

Funkcje $\lfloor \cdot \rfloor$ i $\lceil \cdot \rceil$ nazywamy – odpowiednio – podlogą oraz sufitem. Analogicznie, liczby całkowite $\lfloor x \rfloor$ i $\lceil x \rceil$ nazywamy podlogą oraz sufitem liczby rzeczywistej x .

Dla $x, y \in \mathbb{R}, y \neq 0$, symbol $x \bmod y$ oznacza resztę z dzielenia x przez y , czyli

$$x \bmod y = x - y \cdot \left\lfloor \frac{x}{y} \right\rfloor.$$

Macierz, której elementem w i -tym wierszu, gdzie $i = 1, \dots, n$, i j -tej kolumnie, gdzie $j = 1, \dots, m$, jest a_{ij} , oznaczamy symbolem

$$[a_{ij}]_{i=1, \dots, n, j=1, \dots, m}.$$

Zbiór wszystkich macierzy o n wierszach i m kolumnach, w których każdy z elementów należy do zbioru Q , oznaczamy symbolem $Q^{n \times m}$.

Wyznacznik macierzy A oznaczamy symbolem $\det A$.

Dla macierzy transponowanej macierzy A stosujemy oznaczenie A^T .

Dla $m, n \in \mathbb{N}$, gdzie $0 < n \leq m$, symbol m^n oznacza n -tą potęgę ubywającą liczby m , tzn.

$$m^n = m \cdot (m - 1) \cdot \dots \cdot (m - n + 1),$$

natomiast dla $m, n \in \mathbb{N}$, gdzie $n > 0$, zapis $m^{\bar{n}}$ oznacza n -tą potęgę przyrastającą liczby m , tzn.

$$m^{\bar{n}} = m \cdot (m + 1) \cdot \dots \cdot (m + n - 1).$$

Dla $k, n \in \mathbb{N}$ symbol

$$\binom{n}{k}$$

oznacza współczynnik dwumianowy o indeksie górnym n i indeksie dolnym k . Dla $m \in \mathbb{N}$ oraz $n, k_1, \dots, k_m \in \mathbb{N}$, gdzie $k_1 + \dots + k_m = n$, symbolem

$$\binom{n}{k_1 \dots k_m}$$

oznaczamy współczynnik wielomianowy o indeksie górnym n i indeksach dolnych k_1, \dots, k_m .

Dla $n, k \in \mathbb{N}$ stosujemy następujące oznaczenia:

$\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ – liczba Stirlinga pierwszego rodzaju;

$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ – liczba Stirlinga drugiego rodzaju.

Dla $n \in \mathbb{N}$ symbol B_n oznacza n -tą liczbę Bella.

Dla zbioru skończonego X i $k \in \mathbb{N}$ stosujemy następujące oznaczenia:

$\Pi_k(X)$ – zbiór wszystkich podziałów zbioru X na k bloków;

$\Pi(X)$ – zbiór wszystkich podziałów zbioru X na bloki.

0.1. NOTACJA

Dla liczb naturalnych n, k, t , używamy następujących oznaczeń:

$P(n)$ – liczba wszystkich podziałów liczby n na składniki;

$P(n, k)$ – liczba wszystkich podziałów liczby n na k składników;

$P_t(n)$ – liczba wszystkich podziałów liczby n na składniki nie przekraczające t ;

$P^t(n)$ – liczba wszystkich podziałów liczby n na składniki, z których największy jest równy t .

Dla dodatnich liczb naturalnych x, y , przyjmujemy następujące symbole:

$\gcd(x, y)$ – największy wspólny dzielnik liczb x, y ;

$\text{lcm}(x, y)$ – najmniejsza wspólna wielokrotność liczb x, y .

Dla $x \in \mathbb{R}$, gdzie $x > 0$, stosujemy następujące oznaczenia:

$\lg x$ – logarytm liczby x przy podstawie 2;

$\log x$ – logarytm liczby x przy podstawie 10;

$\ln x$ – logarytm naturalny liczby x .

Symbolem S_n oznaczamy zbiór wszystkich permutacji zbioru $\{1, \dots, n\}$.

D_n oznacza podzbiór wszystkich permutacji z S_n , które są nieporządkami.

Dla permutacji $\pi \in S_n$ stosujemy następujące oznaczenia:

$I(\pi)$ – liczba inwersji permutacji π ;

$sgn(\pi)$ – znak permutacji π ;

$Inv(\pi)$ – liczba niezmienników permutacji π .

Permutację $\pi \in S_n$, która jest cyklem wyznaczonym przez ciąg (k_1, \dots, k_n) , oznaczamy symbolem $[k_1, \dots, k_n]$.

Jeśli G jest grupą permutacji działającą na zbiorze S , to symbolem $o(G)$ oznaczamy liczbę wszystkich orbit tej grupy.

Symboliem \blacksquare oznaczany jest koniec Dowodu, natomiast symbolem \square koniec Przykładu.

Rozdział 1

Wprowadzenie

Kombinatoryka jest obszernym i ważnym dzialem matematyki dyskretnej, mającym liczne zastosowania zarówno w innych działach matematyki, jak i w różnorodnych zagadnieniach praktycznych.

Zasadniczym problemem, którym zajmuje się kombinatoryka, jest zliczanie obiektów o wskazanych cechach. Wiele wyników z tego zakresu to rezultaty klasyczne, znane często od bardzo dawna. Niniejszy wykład jest w zasadzie ograniczony do takich właśnie tematów i jest prowadzony w sposób bardzo elementarny. Wybór materiału – tak zresztą jak w całej książce – jest podyktyowany potrzebami naszych studentów. Podane tu wiadomości stanowią często wstęp do innych wykładów, takich jak optymalizacja dyskretna, badania operacyjne, rachunek prawdopodobieństwa i statystyka, teoria szyfrów itp.

Mimo że ta część książki dotyczy w większości zagadnień klasycznych, to sposób prezentacji materialu odbiega nieco od typowego układu podręczników z kombinatoryki. Staramy się mianowicie, aby większość problemów dotyczących zliczania formułować w sposób możliwie jednorodny jako zagadnienia zliczania funkcji o wybranych cechach. Wydaje się, że takie ujęcie problemów zliczania jest szczególnie proste, a ponadto ułatwia potem formułowanie i rozwiązywanie różnorodnych zagadnień praktycznych.

Takiemu potraktowaniu problemów zliczania jest podporządkowany cały układ tej części książki. Po wprowadzeniu pojęcia relacji binarnej w iloczynie kartezjańskim zbiorów, zaczynamy zatem od policzenia, ile spośród tych relacji jest funkcjami. Następnie zajmujemy się zliczaniem funkcji różnowartościowych, bijekcji i permutacji. Ponieważ do policzenia liczby wszystkich surjekcji są nam potrzebne podziały zbiorów na bloki,

poświęcamy im osobny rozdział. Również oddzielnny rozdział dotyczy podstawowych faktów z zakresu podziałów liczb naturalnych na składniki.

Wszystkie nasze rozważania ilustrowane są przykładami różnorodnych zagadnień, które mogą być formułowane w języku zliczania funkcji różnych typów. Rozdział drugi tej części książki kończy krótkie wprowadzenie w problematykę zbiorów częściowo uporządkowanych.

Rozdział trzeci prezentuje podstawowe metody i techniki stosowane w kombinatoryce. Centralne miejsce zajmuje w nim technika funkcji tworzących. Pokazujemy, jak różnorodne i jednocześnie proste są zastosowania tej techniki w takich zagadnieniach, jak na przykład wyznaczanie liczby rozwiązań równań diofantycznych z dodatkowymi warunkami, badanie ciągów liczbowych, rozwiązywanie liniowych równań rekurencyjnych itp. Dwie pozostałe standardowe techniki kombinatoryczne, to znaczy tak zwana zasada włączania-wyłączania oraz zasada szufla kowa, są potraktowane bardziej skrótnie.

Ostatni rozdział tej części książki jest elementarnym przedstawieniem teorii zliczania Pólya. Wprowadzeniem do tej teorii jest prezentacja podstawowych faktów, dotyczących bardzo ważnej klasy funkcji, jaką są permutacje. Prezentowana w Rozdziale czwartym teoria zliczania może być traktowany jako pewnego rodzaju podsumowanie wcześniej prezentowanych zagadnień kombinatorycznych, bowiem pojawia się tu znaczna część używanych dotychczas pojęć. Zamieszczone w tym rozdziale bardzo proste przykłady tylko w niewielkim stopniu sygnalizują ogromne możliwości zastosowań praktycznych tej teorii.

Rozdział 2

Podstawowe pojęcia

W tym rozdziale wprowadzimy podstawowe pojęcia, które są używane w kombinatoryce. Zaczniemy od przypomnienia definicji relacji binarnych i funkcji, a następnie przejdziemy do zliczania funkcji różnych typów, podzbiorów zbiorów, rozmieszczeń uporządkowanych itp. Omówimy też podziały liczb na składniki, zbory z powtórzeniami i najważniejsze fakty, dotyczące zbiorów uporządkowanych.

2.1 Relacje

Niech A oraz B będą dowolnymi zbiorami (skończonymi albo nieskończonymi).

Definicja 2.1 Iloczynem kartezjańskim zbiorów A i B nazywamy zbiór wszystkich par uporządkowanych o poprzednikach należących do zbioru A i następcach należących do zbioru B .

Iloczyn kartezjański zbiorów A i B oznaczamy symbolem $A \times B$. Mamy zatem,

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}.$$

Jeśli zbory A oraz B są skończone, to liczność zbioru $A \times B$ jest równa iloczynowi liczności zbiorów A i B , to znaczy $|A \times B| = |A| \cdot |B|$.

Zauważmy, że definiując iloczyn kartezjański dwóch zbiorów nie żądamy, by zbory te były różne; w szczególnym przypadku możemy mieć do czynienia z tym samym zbiorem. Jeśli więc $A = X$ oraz $B = X$, to iloczynem kartezjańskim tych zbiorów jest zbiór $X \times X$, który oznaczamy symbolem X^2 .

Przykład 2.1 Niech A będzie zbiorem znaków w nazwie *WIN98*, a B – zbiorem liter w nazwie *TeX*. Mamy więc $A = \{W, I, N, 9, 8\}$ oraz $B = \{T, e, X\}$. Iloczynem kartezjańskim zbiorów A i B jest piętnasto-elementowy zbiór C , którego elementami są następujące pary uporządkowane: (W, T) , (W, e) , (W, X) , (I, T) , (I, e) , (I, X) , (N, T) , (N, e) , (N, X) , $(9, T)$, $(9, e)$, $(9, X)$, $(8, T)$, $(8, e)$, $(8, X)$. Natomiast iloczynem kartezjańskim zbiorów B i A jest zbiór $C' = \{(T, W), (e, W), (X, W), (T, I), (e, I), (X, I), (T, N), (e, N), (X, N), (T, 9), (e, 9), (X, 9), (T, 8), (e, 8), (X, 8)\}$.

□

Pojęcie iloczynu kartezjańskiego odgrywa zasadniczą rolę w opisywaniu związków między elementami dwóch zbiorów. Dokonuje się tego poprzez podanie tak zwanej *relacji binarnej*¹ w iloczynie kartezjańskim.

Definicja 2.2 Relację binarną w iloczynie kartezjańskim zbiorów A i B nazywamy dowolny podzbiór zbioru $A \times B$.

W przypadku, gdy oba zbiorы są identyczne, tzn. $A = X$ oraz $B = X$, mówimy o *relacji binarnej w zbiorze X* .

Jeśli $R \subseteq A \times B$ jest relacją binarną w iloczynie kartezjańskim zbiorów A i B , to dla zaznaczenia faktu, że para (a, b) jest elementem relacji R piszemy: $(a, b) \in R$ albo aRb . Ostatni zapis jest wygodny w sytuacji, gdy symbol, który przypisujemy relacji, ma konkretną interpretację, na przykład działania albo operatora (patrz przykłady poniżej).

Zbiór wszystkich poprzedników par należących do relacji R nazywamy *dziedziną relacji R* , natomiast zbiór wszystkich następników par – *przeciwdziedziną relacji R* .

W iloczynie kartezjańskim zbiorów A i B możemy zdefiniować co najwyżej $2^{m \cdot n}$ różnych relacji binarnych, gdzie $m = |A|$ oraz $n = |B|$, bowiem dokładnie tyle elementów liczy rodzinę wszystkich podzbiorów zbioru $A \times B$ (patrz Rozdział 2.4). Dwie szczególne relacje: $R^o = \emptyset$ oraz $R^p = A \times B$ nazywane są, odpowiednio, relacją *pustą* i relacją *pełną*.

Przykład 2.2 Rozważmy dwa zbiorы skończone: zbiór $A = \{1, 2, 3, 4\}$ i zbiór $B = \{\{1, 2\}, \{1, 4\}\}$. Elementami zbioru A są więc cztery liczby naturalne, natomiast elementami zbioru B są dwa dwuelementowe podzbiory zbioru liczb naturalnych.

¹Czasem stosuje się termin: *relacja dwuczlonowa* w iloczynie kartezjańskim.

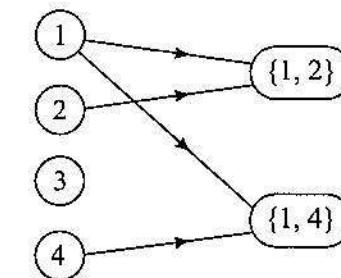
2.1. RELACJE

Niech $R \subseteq A \times B$ będzie relacją przynależności do zbioru w iloczynie kartezjańskim zbiorów A i B . Zbiór R zawiera zatem następujące cztery pary uporządkowane: $(1, \{1, 2\})$, $(1, \{1, 4\})$, $(2, \{1, 2\})$, $(4, \{1, 4\})$. Dziedziną relacji R jest zbiór $\{1, 2, 4\}$, będący podzbiorem właściwym zbioru A , natomiast jej przeciwdziedziną – zbiór $\{\{1, 2\}, \{1, 4\}\}$, pokrywający się w tym przypadku z całym zbiorem B . Gdybyśmy dla oznaczenia rozważanej relacji zamiast symbolu R zastosowali symbol \in , to dla zapisu faktu, że element 4 ze zbioru A jest w relacji \in z elementem $\{1, 4\}$ ze zbioru B , otrzymalibyśmy tradycyjnie używany zapis $4 \in \{1, 4\}$. □

Jeśli zbiorы A oraz B są zbiorami skończonymi, to dowolną relację R w iloczynie kartezjańskim $A \times B$ można zilustrować albo w postaci tak zwanego *rysunku grafu relacji*, albo w postaci *tablicy relacji*. Obie te postaci pozwalają na wygodne interpretowanie pewnych cech relacji, o których jest mowa w dalszej części tego rozdziału.

Rysunek grafu relacji $R \subseteq A \times B$ jest diagramem, zawierającym umowne symbole oraz łączące je strzałki.² Każdemu elementowi zbiorów A oraz B przypisany jest dokładnie jeden symbol (zwyczaj okrąg lub kwadrat), natomiast strzałka prowadzi od symbolu przyporządkowanego elementowi $a \in A$ do symbolu przyporządkowanego elementowi $b \in B$ wtedy i tylko wtedy, gdy $(a, b) \in R$. Zwykle wygodne jest ułożenie symboli, odpowiadających elementom zbiorów A oraz B , w dwóch różnych kolumnach.

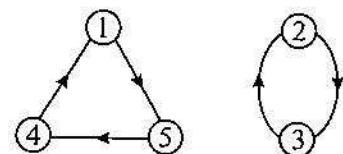
Poniżej pokazany jest rysunek grafu relacji R , która jest rozważana w Przykładzie 2.2.



Rysunek 2.1: Rysunek grafu relacji z Przykładu 2.2.

²W języku teorii grafów, której dotyczy Część II tej książki (patrz [16], str. 4), symbole te nazywane są *wierzchołkami* grafu skierowanego, a strzałki – *lukami* grafu skierowanego.

W przypadku, gdy mamy do czynienia z relacją R w zbiorze X , to znaczy dla $R \subseteq X \times X$, zwykle na rysunku grafu relacji nie powtarzamy symboli przyporządkowanych elementom zbioru X . Jeśli zatem na przykład $X = \{1, 2, 3, 4, 5\}$ i $R \subseteq X \times X$, gdzie $R = \{(1, 5), (5, 4), (4, 1), (2, 3), (3, 2)\}$, to graf relacji R przedstawiamy w postaci pokazanej na Rysunku 2.2.



Rysunek 2.2: Rysunek grafu relacji $R = \{(1, 5), (5, 4), (4, 1), (2, 3), (3, 2)\}$ w zbiorze $X = \{1, 2, 3, 4, 5\}$.

Tablica relacji $R \subseteq A \times B$ zawiera $|A|$ wierszy, odpowiadających poszczególnym elementom zbioru A , oraz $|B|$ kolumn, które odpowiadają kolejnym elementom zbioru B . Pole tablicy, leżące na przecięciu wiersza przyporządkowanego elementowi a oraz kolumny przyporządkowanej elementowi b , zawiera symbol \times albo symbol 1 wtedy i tylko wtedy, gdy $(a, b) \in R$. Pozostałe pola tablicy albo są puste, albo są wypełnione zerami. W przypadku użycia symboli 1 oraz 0, tablica relacji odpowiada zero-jedynkowej macierzy o wymiarach $|A| \times |B|$, która również może być używana do zapisu relacji R . Rysunek 2.3 przedstawia tablicę relacji R z Przykładu 2.2.

| | {1, 2} | {1, 4} |
|---|--------|--------|
| 1 | 1 | 1 |
| 2 | 1 | 0 |
| 3 | 0 | 0 |
| 4 | 0 | 1 |

Rysunek 2.3: Tablica relacji z Przykładu 2.2.

2.1. RELACJE

Niech R będzie relacją w zbiorze X , to znaczy $R \subseteq X \times X$. O relacji R mówimy, że jest:

zwrotna, jeśli xRx dla każdego $x \in X$;

przechodnia, jeśli $(xRy \wedge yRz) \Rightarrow xRz$ dla dowolnych $x, y, z \in X$;

symetryczna, jeśli $xRy \Rightarrow yRx$ dla dowolnych $x, y \in X$;

antysymetryczna, jeśli $(xRy \wedge yRx) \Rightarrow x = y$ dla dowolnych $x, y \in X$.

Czasem wyróżnia się jeszcze inne typy relacji: relację *przeciwzwrotną*, dla której $\neg xRx$ dla każdego $x \in X$, oraz relację *przeciwsymetryczną*, dla której warunki xRy i yRx wykluczają się nawzajem dla każdych dwóch elementów x oraz y zbioru X .

Wymienione wyżej cechy relacji pozwalają na wprowadzenie dwóch bardzo ważnych klas relacji: relacji *równoważności* w zbiorze oraz relacji *częściowego porządku* w zbiorze.

Definicja 2.3 Relację równoważności w zbiorze X nazywamy relację, która jest zurotna, przechodnia i symetryczna.

Relacja równoważności R w zbiorze X dzieli ten zbiór na podzbiory, nazywane *klasami równoważności* (albo – *klasami abstrakcji*) relacji R w zbiorze X . Mianowicie, dla $x \in X$ definiujemy zbiór oznaczany symbolem x/R , gdzie $x/R = \{y \in X : xRy\}$. Zbiór taki nazywamy *klassą abstrakcji relacji R wyznaczoną przez element x* . Zbiór wszystkich klas abstrakcji relacji R w zbiorze X oznaczamy symbolem X/R , to znaczy $X/R = \{x/R : x \in X\}$.

Przykład 2.3 Rozważmy relację oznaczoną symbolem \simeq , zdefiniowaną w zbiorze $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$ w sposób następujący:

$$x \simeq y \text{ wtedy i tylko wtedy, gdy } x - y \in \mathbb{Z}.$$

Łatwo zauważać, że relacja \simeq w zbiorze \mathbb{R}_+ jest symetryczna, zwrotna i przechodnia, a zatem jest relacją równoważności. Klasą abstrakcji tej relacji, wyznaczoną przez element $x \in \mathbb{R}_+$, jest zbiór liczb rzeczywistych, które mają tę samą część ułamkową co x . \square

Definicja 2.4 Relację częściowego porządku w zbiorze X nazywamy relacją, która jest zwrotna, przechodnia i antysymetryczna.

Parę uporządkowaną (X, \preceq) , gdzie X jest dowolnym zbiorem, a \preceq jest relacją częściowego porządku w tym zbiorze, nazywamy *zbioru częściowo uporządkowanym*.

Teoria zbiorów częściowo uporządkowanych odgrywa bardzo ważną rolę w zastosowaniach matematyki dyskretnej. Do zagadnień tych wróćmy w Rozdziale 2.8.

Przykład 2.4 Rozważmy relację podzielności, oznaczaną symbolem $|$, którą zdefiniujemy w zbiorze $\mathcal{N} = \mathbb{N} \setminus \{0\}$ w sposób następujący:

$$a | b \text{ dla } a, b \in \mathcal{N} \Leftrightarrow b \text{ mod } a = 0.$$

Łatwo sprawdzić, że tak zdefiniowana relacja podzielności w zbiorze \mathcal{N} jest zwrotna, przechodnia i antysymetryczna, a zatem jest relacją częściowego porządku w tym zbiorze.

□

2.2 Funkcje

Niech X i Y będą dowolnymi zbiorami. Bardzo ważną klasę relacji w iloczynie kartezjańskim $X \times Y$ stanowią *funkcje*.

Definicja 2.5 Funkcją ze zbioru X w zbiór Y nazywamy dowolną relację $f \subseteq X \times Y$, mającą tę właściwość, że dla każdego $x \in X$ istnieje dokładnie jeden element $y \in Y$, taki że $(x, y) \in f$.

Dziedziną relacji $f \subseteq X \times Y$, będącej funkcją, jest więc cały zbiór X . Ponieważ dla danego elementu x , należącego do dziedziny funkcji f , istnieje dokładnie jedna para $(x, y) \in f$, zwykle piszemy $y = f(x)$ na oznaczenie faktu, że $(x, y) \in f$. Taki element $y \in Y$ nazywamy *wartością funkcji f dla argumentu x* .

Dla zaznaczenia, że relacja $f \subseteq X \times Y$ jest funkcją, której dziedziną jest zbiór X , a wartości funkcji należą do zbioru Y , stosujemy zapis: $f : X \rightarrow Y$. Zbiór wszystkich funkcji $f : X \rightarrow Y$ oznaczamy symbolem $Fun(X, Y)$.

2.2. FUNKCJE

Dla dowolnego zbioru $A \subseteq X$ oraz funkcji $f \in Fun(X, Y)$, zbiór $f(A) \subseteq Y$, gdzie

$$f(A) = \{y \in Y : \text{istnieje } x \in A, \text{ taki że } y = f(x)\},$$

nazywamy *obrazem zbioru A przez funkcję f* . Podobnie, dla dowolnego zbioru $B \subseteq Y$, zbiór

$$f^{-1}(B) = \{x \in X : f(x) \in B\}$$

nazywamy *przeciwbrazem zbioru B przez funkcję f* .

Jeśli $f \in Fun(X, Y)$, to rodzinę przeciwbrazów wszystkich jednoelementowych podzbiorów zbioru Y , to znaczy rodzinę zbiorów

$$N(f) = \{f^{-1}(\{y\}), y \in Y\},$$

nazywamy *jądrem funkcji f* .

Funkcję $f \in Fun(X, Y)$, dla której zachodzi warunek $f(X) = Y$, nazywamy *surjekcją*. Funkcja o tej własności bywa też nazywana funkcją ze zbioru X na zbiór Y . Podzióbior wszystkich surjekcji w zbiorze $Fun(X, Y)$ oznaczamy symbolem $Sur(X, Y)$.

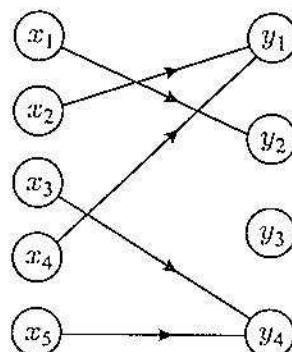
Jeśli $f \in Fun(X, Y)$ oraz dla dowolnych elementów $a, b \in X$ zachodzi warunek

$$a \neq b \Rightarrow f(a) \neq f(b),$$

to funkcję f nazywamy *iniekcją* lub *funkcją różnicowartąciową*. Podzióbior wszystkich iniekcji w zbiorze $Fun(X, Y)$ oznaczamy symbolem $Inj(X, Y)$.

Funkcja, która jest jednocześnie surjekcją i iniekcją, jest nazywana *bijekcją*; podzióbior wszystkich bijekcji w zbiorze $Fun(X, Y)$ oznaczamy symbolem $Bij(X, Y)$.

Przykład 2.5 Na Rysunku 2.4 przedstawiony jest rysunek grafu funkcji $f : X \rightarrow Y$, gdzie $X = \{x_1, x_2, x_3, x_4, x_5\}$ oraz $Y = \{y_1, y_2, y_3, y_4, y_5, y_6\}$. Z rysunku tego łatwo odczytać na przykład, że obrazem zbioru $\{x_1, x_3, x_5\}$ przez funkcję f jest zbiór $\{y_2, y_4\}$. Analogicznie, przeciwbrazem zbioru $\{y_1, y_2\}$ jest zbiór $\{x_1, x_2, x_4\}$, natomiast przeciwbrazem zbioru $\{y_3\}$ jest zbiór pusty. Jądro funkcji f jest czteroelementową rodziną podzbiorów zbioru X ; mamy tu $N(f) = \{\{x_2, x_4\}, \{x_1\}, \emptyset, \{x_3, x_5\}\}$. □



Rysunek 2.4: Graf funkcií z Przykładu 2.5.

W matematyce dyskretniej bardzo często mamy do czynienia z funkcjí, której dziedziną jest skończony k -elementowy zbiór liczb naturalnych X , a przeciwdziedziną – dowolny zbiór Y . Zwykle $X = \{1, 2, \dots, k\}$ albo $X = \{0, 1, 2, \dots, k-1\}$. Funkcję taką nazywamy *k -elementowym ciągiem o wyrazach ze zbioru Y* i zwykle oznaczamy – odpowiednio – symbolami (a_1, \dots, a_k) albo $(a_0, a_1, \dots, a_{k-1})$. Jeśli dla każdych dwóch różnych argumentów wartości tej funkcji są różne, to wówczas mówimy o *ciagu różnowartościowym*.

Podstawowym problemem, którym zajmuje się kombinatoryka, jest policzenie liczby funkcji, mających określone właściwości, na przykład funkcji różnowartościowych, surjekcji itp. Zagadnieniu temu poświęcone są następne podrozdziały.

2.2.1 Zliczanie funkcji

W zastosowaniach kombinatoryki często mamy do czynienia z pytaniami, które dotyczą liczby wszystkich możliwych rozmieszczeń zadanej liczby obiektów (na przykład kul, kart itp.), charakteryzujących się pewnymi cechami (takimi, jak wielkość, waga, kolor) w określonych miejscach (pułapkach, urnach). Zwykle na sposób rozmieszczenia obiektów nakładane są dodatkowo różne ograniczenia. Na przykład żąda się, by liczba obiektów, które umieszczane są w każdym pułapku, nie przekraczała zadanej wartości, albo wymaga się, by wszystkie pułapki były zapelnione itp.

Inne typowe sformułowanie problemów kombinatorycznych dotyczy liczby sposobów pokolorowania pewnego zbioru obiektów w sytuacji, gdy mamy do dyspozycji określoną liczbę kolorów oraz nakładane są różnorodne ograniczenia na sposób kolorowania obiektów.

Problemy tego typu mają istotne znaczenie praktyczne. W takim języku są na przykład formułowane zagadnienia przydziału programów do procesorów w systemach wieloprocesorowych, zagadnienia segmentacji złożonych projektów obliczeniowych itp. Problemy takie w elegancki i jednolity sposób mogą być formułowane w języku zliczania funkcji o zadanych właściwościach. Prezentację zagadnień zliczania funkcji zacznijemy od najprostszego pytania z tej dziedziny:

Ile jest wszystkich funkcji w iloczynie kartezjańskim dwóch zbiorów skończonych?

Niech X i Y będą zbiorami skończonymi, gdzie $|X| = n$, $|Y| = m$. Często wygodnie będzie przyjąć, że $X = \{1, \dots, n\}$ oraz $Y = \{1, \dots, m\}$. Nie ogranicza to ogólności rozumowania, bowiem można założyć, że elementy zbiorów są ponumerowane kolejnymi liczbami naturalnymi.

Twierdzenie 2.1 *Jeśli $|X| = n$ i $|Y| = m$, to liczba wszystkich funkcji $f : X \rightarrow Y$ jest równa m^n .*

Dowód. Bez straty ogólności rozważań możemy założyć, że $X = \{1, \dots, n\}$. Wówczas każdą funkcję $f : X \rightarrow Y$ można jednoznacznie identyfikować z n -elementowym wektorem (y_1, \dots, y_n) o wyrazach z m -elementowego zbioru Y . Każdy wyraz y_i , $i = 1, \dots, n$, można niezależnie od innych wyrazów wybrać na m różnych sposobów, co daje m^n różnych możliwych wektorów (y_1, \dots, y_n) . ■

Zauważmy, że z dowodu powyższego twierdzenia wynika natychmiast następujący wniosek:

Wniosek 2.1 *Liczba ciągów n -elementowych o wyrazach w zbiorze Y , gdzie $|Y| = m$, jest równa m^n .*

Tabela na Rysunku 2.5 zawiera wartości m^n dla $m, n = 0, 1, \dots, 9$. W tabeli tej przyjęto konwencję, że $0^0 = 1$, to znaczy, że istnieje dokładnie jedna funkcja ze zbioru pustego w zbiór pusty.

| m^n | $n=0$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ... |
|-------|-------|---|----|-----|------|-------|--------|---------|----------|-----------|-----|
| $m=0$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | |
| 2 | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | |
| 3 | 1 | 3 | 9 | 27 | 81 | 243 | 729 | 2187 | 6561 | 19683 | |
| 4 | 1 | 4 | 16 | 64 | 256 | 1024 | 4096 | 16384 | 65536 | 262144 | |
| 5 | 1 | 5 | 25 | 125 | 625 | 3125 | 15625 | 78125 | 390625 | 1953125 | |
| 6 | 1 | 6 | 36 | 216 | 1296 | 7776 | 46656 | 279936 | 1679616 | 10077696 | |
| 7 | 1 | 7 | 49 | 343 | 2401 | 16807 | 117649 | 823543 | 5764801 | 40353607 | |
| 8 | 1 | 8 | 64 | 512 | 4096 | 32768 | 262144 | 2097152 | 16777216 | 134217728 | |
| 9 | 1 | 9 | 81 | 729 | 6561 | 59049 | 531441 | 4782969 | 43046721 | 387420489 | |
| ... | | | | | | | | | | | |

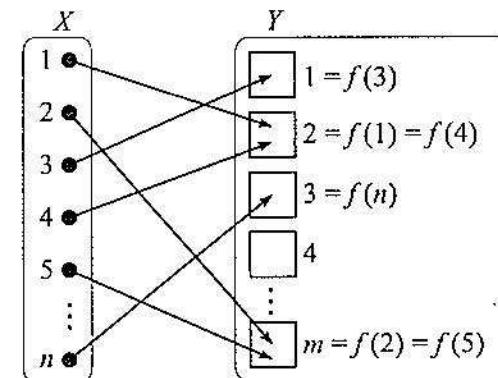
Rysunek 2.5: Liczby wszystkich funkcji ze zbioru n -elementowego w zbiór m -elementowy dla $m, n = 0, 1, \dots, 9$.

Twierdzenie 2.1, użyte do problemu rozmieszczenia n obiektów w m pudełkach, orzeka, że istnieje dokładnie m^n różnych sposobów rozmieszczenia tych obiektów w pudełkach. Dotyczy to sytuacji, gdy nie nakładamy żadnych ograniczeń na rozmieszczenia. Nie interesuje nas również kolejność obiektów w poszczególnych pudełkach, a jedynie fakt, czy obiekt i trafia do pudełka o numerze j . Jeśli $X = \{1, \dots, n\}$, $Y = \{1, \dots, m\}$ oraz dana jest dowolna funkcja $f : X \rightarrow Y$, to odpowiadające tej funkcji rozmieszczenia obiektów polega na umieszczeniu obiektu o numerze i w pudełku o numerze $j = f(i)$.

Rysunek 2.6 pokazuje przykład takiego rozmieszczenia. Zauważmy, że jeśli nie nakładamy żadnych dodatkowych warunków na funkcję f , to w niektórych pudełkach może się znaleźć więcej niż jeden obiekt, a niektóre pudełka mogą pozostać puste.

Twierdzenie 2.1 może być również zastosowane do znalezienia liczby różnych sposobów pokolorowania n obiektów w przypadku, gdy mamy do dyspozycji m różnych kolorów i nie wprowadzamy żadnych dodatkowych warunków na sposób kolorowania. Zakładamy przy tym, że każdy obiekt może być pokolorowany tylko jednym kolorem. Tu także możemy mieć do czynienia z sytuacją, w której ten sam kolor zostanie użyty do więcej niż jednego obiektu albo dany kolor nie zostanie wcale wykorzystany.

2.2. FUNKCJE



Rysunek 2.6: Rozmieszczenie obiektów ze zbioru X definiowane przez funkcję $f \in \text{Fun}(X, Y)$.

Załóżmy teraz, że interesuje nas liczba sposobów rozmieszczenia n obiektów w m pudełkach, gdzie $m \geq n$, ale z dodatkowym warunkiem, że w każdym pudełku jest umieszczony co najwyżej jeden obiekt. W przypadku problemu kolorowania obiektów warunek powyższy odpowiada wyimaginianiu, by żadne dwa obiekty nie były pokolorowane tym samym kolorem.

W języku zliczania funkcji oba powyższe problemy sprowadzają się do odpowiedzi na pytanie:

Ile jest wszystkich funkcji różniciwciowych (injekcji) ze zbioru n -elementowego w zbiór m -elementowy?

Poniższe twierdzenie podaje odpowiedź na to pytanie. Występuje w nim oznaczenie, które często jest używane w tym rozdziale. Mianowicie, niech dla $m, n \in \mathbb{N}$, gdzie $0 < n \leq m$,

$$m^n = m \cdot (m-1) \cdot \dots \cdot (m-n+1). \quad (2.1)$$

Jeśli $m < n$, to będziemy przyjmować, że $m^n = 0$. Ponadto, dla dowolnego $m \in \mathbb{N}$ przyjmujemy, że $m^0 = 1$.

Symbol m^n nazywamy n -tą potęgą ubywającą liczbą m .³ Potęgę ubywającą można zdefiniować w ten sam sposób dla $n \in \mathbb{N}$ oraz dowolnej liczby rzeczywistej m (patrz np. [10]), ale dla naszych potrzeb wystarczy ograniczyć się do liczb naturalnych.

³W niektórych książkach potęga ubywająca jest oznaczana symbolem $[m]^n$.

Twierdzenie 2.2 Jeżeli $|X| = n$ i $|Y| = m$, to liczba wszystkich funkcji różnowartościowych $f : X \rightarrow Y$ jest równa m^n .

Dowód. Rozważmy najpierw przypadek, gdy $m < n$. Wówczas zbiór funkcji różnowartościowych ze zbioru X w zbiór Y jest pusty, co jest zgodne z przyjętą definicją potęgi ubywającej, której wartość jest wtedy równa zeru.

Załóżmy więc, że $m \geq n$. Możemy przyjąć, podobnie jak w dowodzie Twierdzenia 2.1, że $X = \{1, \dots, n\}$, bowiem każdej funkcji ze zbioru n -elementowego w zbiór Y odpowiada wzajemnie jednoznacznie pewien n -elementowy ciąg (y_1, \dots, y_n) o wyrazach ze zbioru Y . Wyraz y_1 w tym ciągu można wybrać na m różnych sposobów. Z tego, że funkcja jest injekcją, wynika, że przy ustalonym już wyrazie y_1 , wyraz y_2 można wybrać na $m-1$ sposobów. Ogólnie, przy ustalonych już wyrazach y_1, \dots, y_{i-1} , gdzie $i \leq n$, wyraz y_i można wybrać na $m-i+1$ sposobów, jako dowolny element należący do $(m-i+1)$ -elementowego zbioru $X \setminus \{y_1, \dots, y_{i-1}\}$. Daje to łącznie $m \cdot (m-1) \cdot \dots \cdot (m-n+1)$ możliwości wyboru różnowartościowego wektora (y_1, \dots, y_n) . \square

Na Rysunku 2.7 zamieszczona jest tabela, której elementami są wartości potęg ubywających m^n dla $m, n = 0, 1, \dots, 10$, a tym samym liczności zbiorów $Inj(X, Y)$, gdzie $|X| = n$, $|Y| = m$, dla $m, n = 0, 1, \dots, 10$.

Poniższy przykład ilustruje możliwość wykorzystania Twierdzenia 2.2 w problemie wyznaczania liczby różnych nazw, w których litery nie mogą się powtarzać.

Przykład 2.6 W pewnym systemie operacyjnym nazwy plików mają stałą długość i muszą się składać dokładnie z ośmiu znaków, należących do dwudziestoznakowego alfabetu. Ponadto żąda się, aby wszystkie znaki w nazwie były różne.

Z Twierdzenia 2.2 wynika natychmiast, że maksymalna liczba różnych nazw plików w tym systemie jest równa 5 079 110 400, bowiem mamy $20^8 = 20 \cdot 19 \cdot \dots \cdot 14 \cdot 13 = 5 079 110 400$. \square

Załóżmy teraz, że liczności zbiorów X i Y są równe, to znaczy $n = m$. W tym przypadku każda injekcja $f : X \rightarrow Y$ jest również surjekcją, a zatem jest bijekcją. Zauważmy, że z Twierdzenia 2.2 wynika natychmiast następujący fakt:

Wniosek 2.2 Jeżeli $|X| = |Y| = n$, to liczba bijekcji w zbiorze $Fun(X, Y)$ jest równa $n^n = n \cdot (n-1) \cdot \dots \cdot 1$.

2.2. FUNKCJE

| m^n | $n=0$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... |
|-------|-------|-----|-----|-----|------|-------|--------|--------|---------|---------|---------|-----|
| $m=0$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 1 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 1 | 3 | 6 | 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 1 | 4 | 12 | 24 | 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 1 | 5 | 20 | 60 | 120 | 120 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 1 | 6 | 30 | 120 | 360 | 720 | 720 | 0 | 0 | 0 | 0 | 0 |
| 7 | 1 | 7 | 42 | 210 | 840 | 2520 | 5040 | 5040 | 0 | 0 | 0 | 0 |
| 8 | 1 | 8 | 56 | 336 | 1680 | 6720 | 20160 | 40320 | 40320 | 0 | 0 | 0 |
| 9 | 1 | 9 | 72 | 504 | 3024 | 15120 | 60480 | 181440 | 362880 | 362880 | 0 | 0 |
| 10 | 1 | 10 | 90 | 720 | 5040 | 30240 | 151200 | 604800 | 1814400 | 3628800 | 3628800 | 0 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |

Rysunek 2.7: Liczby wszystkich funkcji różnowartościowych ze zbioru n -elementowego w zbiór m -elementowy dla $m, n = 0, 1, \dots, 10$.

Wyrażenie n^n jest bardzo często używane w kombinatoryce i zwykle jest oznaczane specjalnym symbolem $n!$, który czytamy „ n silnia.” Mamy więc

$$n! = n^n = n \cdot (n-1) \cdot \dots \cdot 1. \quad (2.2)$$

Zauważmy też, że z naszej konwencji, dotyczącej wartości potęgi ubywającej dla $n = 0$ (patrz strona 13), wynika, że $0! = 1$.

Funkcja $n!$, a zatem i liczba bijekcji w zbiorze $Fun(X, Y)$, gdzie $|X| = |Y| = n$, rośnie bardzo szybko ze wzrostem n . Obliczanie przybliżonych wartości funkcji $n!$ dla dużych n ułatwia tak zwana formula Stirlinga, która zamieszczona jest w Dodatku (patrz str. 158).

Tabela na Rysunku 2.8 podaje wartości $n!$, a tym samym liczności zbiorów bijekcji $Bij(X, Y)$, gdzie $|X| = |Y| = n$, dla pierwszych trzydziestu sześciu liczb naturalnych n .

Rozważmy teraz dowolną bijekcję ze zbioru $Bij(X, Y)$ przy założeniu, że $Y = X$. Mamy zatem do czynienia z funkcją, która podaje odwzorowanie różnowartościowe zbioru X na ten sam zbiór. Funkcję taką nazywamy *permutacją* zbioru X .

| n | $n!$ |
|-----|--|
| 0 | 1 |
| 1 | 1 |
| 2 | 2 |
| 3 | 6 |
| 4 | 24 |
| 5 | 120 |
| 6 | 720 |
| 7 | 5 040 |
| 8 | 40 320 |
| 9 | 362 880 |
| 10 | 3 628 800 |
| 11 | 39 916 800 |
| 12 | 479 001 600 |
| 13 | 6 227 020 800 |
| 14 | 87 178 291 200 |
| 15 | 1 307 674 368 000 |
| 16 | 20 922 789 888 000 |
| 17 | 355 687 428 096 000 |
| 18 | 6 402 373 705 728 000 |
| 19 | 121 645 100 408 832 000 |
| 20 | 2 432 902 008 176 640 000 |
| 21 | 51 090 942 171 709 440 000 |
| 22 | 1 124 000 727 777 607 680 000 |
| 23 | 25 852 016 738 884 976 640 000 |
| 24 | 620 448 401 733 239 439 360 000 |
| 25 | 15 511 210 043 330 985 984 000 000 |
| 26 | 403 291 461 126 605 635 584 000 000 |
| 27 | 10 888 869 450 418 352 160 768 000 000 |
| 28 | 30 488 834 4611 713 860 501 504 000 000 |
| 29 | 8 841 761 993 739 701 954 543 616 000 000 |
| 30 | 265 252 859 812 191 058 636 308 480 000 000 |
| 31 | 8 222 838 654 177 922 817 725 562 880 000 000 |
| 32 | 263 130 836 933 693 530 167 218 012 160 000 000 |
| 33 | 8 683 317 618 811 886 495 518 194 401 280 000 000 |
| 34 | 295 232 799 039 604 140 847 618 609 643 520 000 000 |
| 35 | 10 333 147 966 386 144 929 666 651 337 523 200 000 000 |

Rysunek 2.8: Liczby wszystkich bijekcji w zbiorze $\text{Fun}(X, Y)$, dla $|X| = |Y| = n$, $n = 0, 1, \dots, 35$.

Definicja 2.6 Permutacją zbioru X nazywamy dowolną funkcję różnowartościową $f \in \text{Fun}(X, X)$.

Z Twierdzenia 2.2 otrzymujemy teraz następujący prosty fakt:

Wniosek 2.3 Liczba wszystkich permutacji zbioru n -elementowego jest równa $n!$.

Permutacje są bardzo ważną klasą funkcji w matematyce dyskretnej i poświęcimy im szczególnie dużo uwagi w Rozdziale 4.1.1.

Zanim jednak przejdziemy do zliczania innych funkcji zajmiemy się w następnym rozdziale pewnym pokrewnym zagadnieniem, a mianowicie wyznaczeniem liczby tak zwanych rozmieszczeń uporządkowanych.

2.3 Rozmieszczenia uporządkowane

Rozważmy ponownie zagadnenie rozmieszczenia obiektów w pudełkach. Założmy – jak poprzednio – że mamy n obiektów i m pudełek, ale tym razem interesować nas będzie również kolejność elementów umieszczanych w poszczególnych pudełkach. Przyporządkowanie wszystkich n obiektów do m pudełek, w którym rozróżniamy kolejność obiektów w pudełkach, będziemy nazywać *rozmieszczeniem uporządkowanym* tych obiektów. Dwa rozmieszczenia uporządkowane traktujemy jako równe wtedy i tylko wtedy, gdy do każdego pudelka $j = \{1, \dots, m\}$ w obu rozmieszczeniach przypisany jest ten sam ciąg o wartościach ze zbioru obiektów.

Rozmieszczenia uporządkowane można również przedstawić w języku funkcji. Mianowicie, każde rozmieszczenie uporządkowane elementów ze zbioru X w pudełkach należących do zbioru Y może być w sposób jednoznaczny przyporządkowane pewnej funkcji $f : X \rightarrow Y \times I$, gdzie $I = \{1, \dots, n\}$, o tej własności, że dla każdego $i = 2, \dots, n$, z faktu, iż $(y, i) \in f(X)$ wynika, że $(y, i-1) \in f(X)$.

Rysunek 2.9 przedstawia wszystkie możliwe rozmieszczenia uporządkowane obiektów z dwuelementowego zbioru $X = \{a, b\}$ w trzech pudełkach ponumerowanych elementami zbioru $Y = \{1, 2, 3\}$. Liczba tych rozmieszczeń jest równa 12.

Naszym celem będzie wyznaczenie liczby wszystkich różnych rozmieszczeń uporządkowanych dla dowolnych liczb naturalnych m oraz n .

| | | | | | | | | | | |
|----|-----------|-------|-------|---|--|-----|---|--|-----------|-----------|
| 1. | 1 (a) (b) | 2 | | 3 | | 7. | 1 | | 2 (a) | 3 (b) |
| 2. | 1 (b) (a) | 2 | | 3 | | 8. | 1 | | 2 (b) | 3 (a) |
| 3. | 1 (a) | 2 (b) | 3 | | | 9. | 1 | | 2 (a) (b) | 3 |
| 4. | 1 (b) | 2 (a) | 3 | | | 10. | 1 | | 2 (b) (a) | 3 |
| 5. | 1 (a) | 2 | 3 (b) | | | 11. | 1 | | 2 | 3 (a) (b) |
| 6. | 1 (b) | 2 | 3 (a) | | | 12. | 1 | | 2 | 3 (b) (a) |

Rysunek 2.9: Wszystkie rozmieszczenia uporządkowane obiektów ze zbioru $\{a, b\}$ w trzech pudełkach.

Zdefiniujmy najpierw pewne oznaczenie, które jest podobne do wprowadzonej w poprzednim rozdziale potęgi ubywającej. Mianowicie, dla $m, n \in \mathbb{N}$, $n > 0$, przyjmiemy:

$$m^{\bar{n}} = m(m+1)\dots(m+n-1). \quad (2.3)$$

Umówmy się, że dla $m \in \mathbb{N}$, $m^{\bar{0}} = 1$.

Wielkość $m^{\bar{n}}$ nazywamy⁴ *n-tą potęgą przyrastającą liczbę m*. Podobnie jak w przypadku potęgi ubywającej, potęgę przyrastającą można w ten sam sposób zdefiniować dla $m \in \mathbb{R}$. Na Rysunku 2.10 zamieszczona jest tabela wartości potęg przyrastających $m^{\bar{n}}$ dla $m, n = 0, 1, \dots, 9$.

Dla $m, n \in \mathbb{N}$, $n > 0$, zachodzi następujące twierdzenie:

Twierdzenie 2.3 *Liczba wszystkich rozmieszczeń uporządkowanych n obiektów w m pudełkach jest równa $m^{\bar{n}}$.*

Dowód. Skonstruujmy wszystkie rozmieszczenia uporządkowane n obiektów w m pudełkach dla $m, n \in \mathbb{N}$, $n > 0$. Zauważmy, że jeśli $m = 0$ i $n > 0$, to $m^{\bar{n}} = 0$; przyjmijmy więc, że $m > 0$ i ponumerujmy w dowolny sposób wszystkie obiekty. Pierwszy obiekt umieszczamy w dowolnym z

⁴W niektórych książkach n-tą potęgę przyrastającą liczbę m oznacza się symbolem $[m]^n$.

pudełek; można to więc zrobić na m różnych sposobów. Następnie rozmieszczamy obiekt drugi. Tym razem można to zrobić na $m+1$ sposobów, bowiem obiekt ten możemy umieścić albo w dowolnym spośród $m-1$ aktualnie pustych pudełek, albo – na dwa sposoby – w pudełku zajętym już przez pierwszy obiekt: przed tym obiektem albo za nim.

Załóżmy, że rozmieściliśmy już $i-1$ obiektów, przy czym w k -tym pudełku, gdzie $k = 1, \dots, m$, znajduje się r_k obiektów. Wówczas i -ty obiekt można dodać na $r_k + 1$ sposobów do k -tego pudełka, co w sumie daje

$$(r_1 + 1) + \dots + (r_m + 1) = (r_1 + \dots + r_m) + m = i - 1 + m$$

wszystkich możliwości rozmieszczenia i -tego obiektu.

Powtarzając to postępowanie dla pozostałych obiektów stwierdzamy, że liczba wszystkich rozmieszczeń uporządkowanych jest istotnie równa $m(m+1)\dots(m+n-1) = m^{\bar{n}}$. ■

| $m^{\bar{n}}$ | $n=0$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 \dots |
|---------------|-------|---|----|-----|-------|--------|---------|----------|-----------|------------|
| $m=0$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 2 | 6 | 24 | 120 | 720 | 5040 | 40320 | 362880 |
| 2 | 1 | 2 | 6 | 24 | 120 | 720 | 5040 | 40320 | 3628800 | 3628800 |
| 3 | 1 | 3 | 12 | 60 | 360 | 2520 | 20160 | 181440 | 1814400 | 19958400 |
| 4 | 1 | 4 | 20 | 120 | 840 | 6720 | 60480 | 604800 | 6652800 | 79833600 |
| 5 | 1 | 5 | 30 | 210 | 1680 | 15120 | 151200 | 1663200 | 19958400 | 259459200 |
| 6 | 1 | 6 | 42 | 336 | 3024 | 30240 | 332640 | 3991680 | 51891840 | 726485760 |
| 7 | 1 | 7 | 56 | 504 | 5040 | 55440 | 665280 | 8648640 | 121080960 | 1816214400 |
| 8 | 1 | 8 | 72 | 720 | 7920 | 95040 | 1235520 | 17297280 | 259459200 | 4151347200 |
| 9 | 1 | 9 | 90 | 990 | 11880 | 154440 | 2162160 | 32432400 | 518918400 | 8821612800 |
| ... | | | | | | | | | | ... |

Rysunek 2.10: Wartości potęg przyrastających dla $m, n = 0, 1, \dots, 9$.

Przykład 2.7 Rozważmy zawody sportowe, w których bierze udział dwudziestu zawodników. Każdy z nich musi wybrać dokładnie jedną z czterech możliwych konkurencji A, B, C, D. Wynikiem zawodów jest lista, składająca się z czterech kolejnych części, oznaczonych również literami A, B,

C, D. Każda z tych części odpowiada danej konkurencji i zawiera nazwiska zawodników w kolejności zajętych przez nich miejsc (zakładamy, że w żadnej konkurencji nie może być wyników *ex quo*).

Chcemy wyznaczyć liczbę wszystkich możliwych wyników takich zawodów, to znaczy liczbę wszystkich różnych list.

Z Twierdzenia 2.3 wynika natychmiast, że liczba ta jest równa liczbie rozmieszczeń uporządkowanych 20 obiektów w 4 pudełkach. Istnieje zatem dokładnie $4^{20} = 4 \cdot 5 \cdots 22 \cdot 23 = 4308669456480829440000$ różnych list, obrazujących wyniki zawodów.

□

Operowanie wyrażeniami zawierającymi potęgi ubywające i przyrastające oraz obliczanie wartości tych potęg ułatwiają proste związki między tymi wielkościami. W powiązaniu z podaną w Dodatku formułą Stirlinga dla funkcji $n!$ dają one wygodne wzory do przybliżonego wyznaczania tych wielkości. Ponieważ poniższe formuły są bardzo łatwe do uzasadnienia, pomijamy ich dowody.

Twierdzenie 2.4 *Dla dowolnych liczb naturalnych m, n , dla których poniższe wyrażenia są dobrze określone, zachodzą następujące tożsamości:*

$$1^{\overline{n}} = n! ; \quad (2.4)$$

$$m^{\overline{n}} = (m+n-1)^{\underline{n}} ; \quad (2.5)$$

$$m^{\underline{n}} = m^{\underline{n-1}} \cdot (m-n+1) ; \quad (2.6)$$

$$m^{\underline{n}} = (m-1)^{\underline{n-1}} \cdot m ; \quad (2.7)$$

$$m^{\underline{n}} = m^{\underline{m-n}} \cdot \frac{n!}{(m-n)!} ; \quad (2.8)$$

$$m^{\underline{n}} = (m-1)^{\underline{n}} \cdot \frac{m}{m-n} ; \quad (2.9)$$

$$m^{\underline{n}} = \frac{m!}{(m-n)!} \quad (2.10)$$

$$m^{\underline{n+1}} = (n+1) \sum_{0 \leq k < m} k^n . \quad (2.11)$$

2.4. PODZBIORY ZBIORÓW

2.4 Podzbiory zbiorów

W rozdziale tym zajmiemy się zliczaniem liczb podzbiorów danego zbioru skończonego, spełniających określone warunki.

Niech $X = \{x_1, \dots, x_n\}$ będzie zbiorem skończonym. Symbolem $\mathcal{P}(X)$ oznaczamy zbiór wszystkich podzbiorów zbioru X . Zbiór ten nosi nazwę *zbioru potęgowego* zbioru X .⁵ Najprostsze pytanie, dotyczące zliczania podzbiorów zbioru X , brzmi następująco:

Ille jest wszystkich podzbiorów zbioru X ?

Łatwo pokazać, że $|\mathcal{P}(X)| = 2^{|X|}$. Zauważmy bowiem, że istnieje wzajemnie jednoznaczna odpowiedniość między elementami zbioru $\mathcal{P}(X)$ a elementami zbioru \mathbb{B}^n , gdzie \mathbb{B}^n jest zbiorem wektorów zero-jedynkowych o długości $n = |X|$. Istotnie, każdemu podzbiorowi $Y \subseteq X$ odpowiada jednoznacznie wektor $\xi(Y) = (b_1, \dots, b_n) \in \mathbb{B}^n$, nazywany *wektorem charakterystycznym* zbioru Y , gdzie $b_i = [x_i \in Y]$ dla $i = 1, \dots, n$.⁶ Podobnie, dowolnemu wektorowi $b = (b_1, \dots, b_n) \in \mathbb{B}^n$ możemy w sposób jednoznaczny przyporządkować podzbiór Y zbioru $X = \{x_1, \dots, x_n\}$, biorąc $Y = \{x_i \in X : b_i = 1, i = 1, \dots, n\}$.

Wektory charakterystyczne $\xi(Y) \in \mathbb{B}^n$ dla $Y \subseteq X$, mogą więc być traktowane jako zapisy w dwójkowym systemie pozycyjnym wszystkich 2^n liczb naturalnych z przedziału domkniętego $[0, 2^n - 1]$.

Omwiana wyżej odpowiedniość między podzbiorami zbioru skończonego X a liczbami naturalnymi z przedziału $[0, 2^{|X|} - 1]$ sprawia, że generowanie wszystkich podzbiorów tego zbioru jest bardzo łatwe: wystarczy po prostu wypisać kolejno podzbiory, których wektory charakterystyczne są reprezentacjami dwójkowymi kolejnych liczb naturalnych z tego przedziału. Podejście to ma jednak pewną wadę.

Rozważmy dla przykładu zbiór $X = \{a, b, c\}$ i tabelę przedstawioną na Rysunku 2.11. W kolejnych wierszach tabeli wypisane są: podzbiór Y zbioru X , jego wektor charakterystyczny $\xi(Y)$ i liczba naturalna $\eta(Y)$, dla której ten wektor jest reprezentacją w systemie dwójkowym.

⁵W niektórych tekstach zbiór potęgowy zbioru skończonego X oznaczany bywa symbolem 2^X .

⁶Przypomnijmy, że zgodnie ze stosowaną przez nas notacją, zapis ten oznacza, że dla $i = 1, \dots, n$,

$$b_i = \begin{cases} 1 & \text{jeśli } x_i \in Y, \\ 0 & \text{jeśli } x_i \notin Y. \end{cases}$$

| Y | $\xi(Y)$ | $\eta(Y)$ |
|-------------|-----------|-----------|
| \emptyset | (0, 0, 0) | 0 |
| {c} | (0, 0, 1) | 1 |
| {b} | (0, 1, 0) | 2 |
| {b, c} | (0, 1, 1) | 3 |
| {a} | (1, 0, 0) | 4 |
| {a, c} | (1, 0, 1) | 5 |
| {a, b} | (1, 1, 0) | 6 |
| {a, b, c} | (1, 1, 1) | 7 |

Rysunek 2.11: Wektory charakterystyczne wszystkich podzbiorów zbioru $X = \{a, b, c\}$.

Zauważmy, że wiersze tej tabeli są wypisane zgodnie z naturalnym porządkiem liczb w ostatniej kolumnie. Następstwem takiej kolejności jest na przykład to, że w sąsiednich wierszach znalazły się podzbiory {b, c} oraz {a}. Jeśli policzymy różnicę symetryczną tych podzbiorów, to okaże się, że jej liczność jest równa 3, bowiem $\{b, c\} \otimes \{a\} = \{a, b, c\}$. Aby więc przejść od podzbioru {b, c} do podzbioru {a} należy wykonać aż trzy operacje, polegające albo na usuwaniu, albo na włączaniu pojedynczego elementu. W pewnych zastosowaniach jest to sytuacja bardzo niekorzystna (patrz Przykład 2.8).

Zauważmy jednak, że wszystkie podzbiory zbioru $\{a, b, c\}$ można łatwo ustawić w ciąg w taki sposób, że zawsze dla sąsiednich elementów tego ciągu liczność różnicy symetrycznej tych podzbiorów jest równa 1. Przykładem takiego ciągu jest następująca sekwencja podzbiorów:

$$(\emptyset, \{a\}, \{a, b\}, \{b\}, \{b, c\}, \{a, b, c\}, \{a, c\}, \{c\}).$$

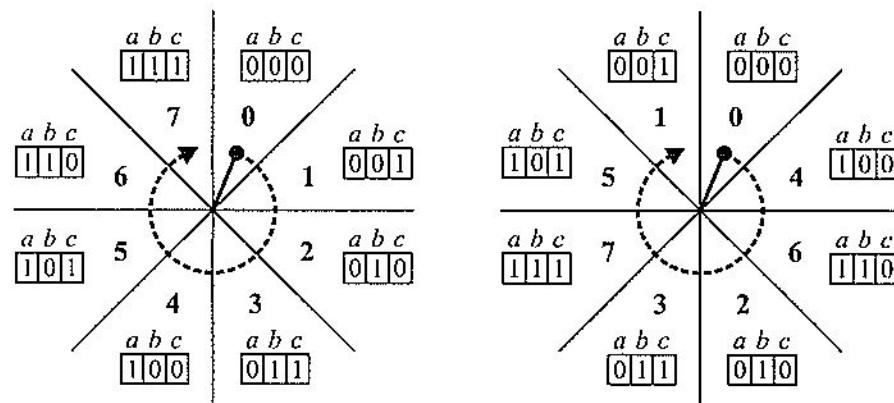
Istotnie, dla każdej pary sąsiednich podzbiorów, a także dla pary złożonej z pierwszego i ostatniego elementu tego ciągu, podzbiór sąsiedni można otrzymać wykonując dokładnie jedną operację dodania albo usunięcia pojedynczego elementu. Taka sytuacja jest bardzo pożądana w licznych zastosowaniach; jedno z nich jest przedstawione w poniższym przykładzie.

Przykład 2.8 Rozważmy urządzenie, w którym kodowane jest położenie pewnego obiektu na płaszczyźnie poprzez podanie sektora, w którym znajduje się ten obiekt (patrz Rysunek 2.12). Założymy, że rozważamy jedynie 8 sektorów. Sektory te możemy ponumerować kolejnymi liczbami naturalnymi od 0 do 7, które odpowiadają wektorom charakterystycznym pewnego zbioru $\{a, b, c\}$. W praktyce elementy tego zbioru reprezentują dwustanowe przełączniki, sygnalizujące położenie obiektu.

Zauważmy, że jeśli zastosujemy numerację sektorów w naturalnym porządku liczb od 0 do 7, to wystąpi opisana wyżej sytuacja, polegająca na tym, że przy przejściu obiektu z sektora o numerze 3 do sektora o numerze 4 musi nastąpić zmiana stanu aż trzech przełączników: a, b, c. W rzeczywistych układach fizycznych zmiana taka nigdy nie następuje jednocześnie, co prowadzi do niepożądanych stanów przejściowych, mogących spowodować niepoprawne odczyty. Jeśli natomiast numeracja sektorów będzie zgodna z podaną niżej sekwencją,

$$(\emptyset, \{a\}, \{a, b\}, \{b\}, \{b, c\}, \{a, b, c\}, \{a, c\}, \{c\}),$$

to przy każdym przejściu obiektu do sąsiedniego sektora nastąpi zmiana stanu dokładnie jednego przełącznika i szkodliwe stany przejściowe zostaną wyeliminowane. \square



Rysunek 2.12: Dwa sposoby kodowania położenia obiektu w ośmiu sektorach.

Powstaje naturalne pytanie, czy zawsze można uporządkować wszystkie podzbiory danego zbioru skończonego X w taki sposób, aby dowolne dwa sąsiednie podzbiory ciągu powstały w wyniku takiego uporządkowania (oraz podzbiory pierwszy i ostatni) różniły się dokładnie jednym elementem zbioru.

Pytanie to można sformułować w równoważnej postaci dla wektorów charakterystycznych podzbiorów zbioru X . Chodzi mianowicie o uporządkowanie wszystkich wektorów należących do zbioru \mathbb{B}^n , gdzie $n = |X|$, w taki sposób, aby sąsiednie wektory utworzonego ciągu (oraz wektory pierwszy i ostatni) różniły się dokładnie na jednej pozycji.

Okazuje się, że taki ciąg wektorów ze zbioru \mathbb{B}^n istnieje dla dowolnego $n \geq 1$ i nosi nazwę *kodu Graya*⁷ rzędu n . Na przykład w przypadku $n = 3$ następujący ciąg jest kodem Graya rzędu 3:

$$((0, 0, 0), (1, 0, 0), (1, 1, 0), (0, 1, 0), (0, 1, 1), (1, 1, 1), (1, 0, 1), (0, 0, 1)).$$

Łatwo zauważać, że kod Graya rzędu n dla $n > 0$ nie jest wyznaczony jednoznacznie. Na przykład odwrócenie porządku elementów ciągu daje również ciąg wektorów, spełniający wszystkie warunki kodu Graya. W istocie takich ciągów jest znacznie więcej (na przykład dla $n = 3$ jest ich dokładnie 12). Istnieją ponadto ścisłe związki między kodami Graya rzędu n a tak zwany cyklami Hamiltona w pewnym grafie nieskierowanym o n wierzchołkach. Do zagadnień tych powróćmy jeszcze w Części II tej książki w rozdziale poświęconym drogom i cyklom w grafach (patrz [16], str. 58).

Wygenerowanie jednego z możliwych kodów Graya⁸ rzędu n jest bardzo proste i opiera się na następującej obserwacji: Jeśli mamy kod Graya rzędu k dla pewnego $k \in \mathbb{N}$, $1 \leq k \leq n$, zapisany w postaci ciągu:

$$((C_1), (C_2), \dots, (C_{m-1}), (C_m)),$$

gdzie $m = 2^k$, $(C_i) \in \mathbb{B}^k$, to następujący ciąg wektorów należących do \mathbb{B}^{k+1} jest kodem Graya rzędu $k + 1$:

$$((C_1, 0), (C_2, 0), \dots, (C_{m-1}, 0), (C_m, 0), \\ (C_m, 1), (C_{m-1}, 1), \dots, (C_2, 1), (C_1, 1)).$$

⁷Nazwa pochodzi od nazwiska pracownika Bell Labs, Franka Graya, który opatentował ten sposób uporządkowania wektorów binarnych w roku 1953. Sam kod był wykorzystywany już wcześniej, bo w roku 1878, przez francuskiego inżyniera Émila Baudota.

⁸Kod ten bywa czasem nazywany *zwierciadlanym kodem Graya*.

2.4. PODZBIORY ZBIORÓW

Dla k -elementowego wektora (C_i) , gdzie $i = 1, \dots, m$, zapisy $(C_i, 0)$ oraz $(C_i, 1)$ oznaczają tu $(k+1)$ -elementowe wektory, otrzymywane przez uzupełnienie wektora (C_i) przez, odpowiednio, zero albo jedynkę na ostatniej pozycji.

Zaczynając od kodu Graya rzędu $k = 1$ w postaci na przykład ciągu $((0), (1))$ i postępując rekurencyjnie dla kolejnych $k \leq n - 1$, otrzymamy w końcu ciąg, będący kodem Graya rzędu n .

Poniższy przykład ilustruje sekwencję ciągów uzyskiwanych przy takim postępowaniu:

Przykład 2.9 Kody Graya rzędu n dla $n = 1, 2, 3, 4$ (dla uproszczenia zapisów pominięte są nawiasy i przecinki w oznaczeniach wektorów):

$$\begin{aligned} n = 1 & \quad 0 \quad 1 \\ n = 2 & \quad 00 \quad 10 \quad 11 \quad 01 \\ n = 3 & \quad 000 \quad 100 \quad 110 \quad 010 \quad 011 \quad 111 \quad 101 \quad 001 \\ n = 4 & \quad 0000 \quad 1000 \quad 1100 \quad 0100 \quad 0110 \quad 1110 \quad 1010 \quad 0010 \\ & \quad 0011 \quad 1011 \quad 1111 \quad 0111 \quad 0101 \quad 1101 \quad 1001 \quad 0001. \end{aligned}$$

□

W niniejszym rozdziale interesowało nas najprostsze pytanie z zakresu zliczania liczby podzbiorów zbioru skończonego, a mianowicie: ile jest wszystkich tych podzbiorów, jeśli nie nakładamy na nie żadnych dodatkowych warunków. W następnych rozdziałach zajmiemy się sytuacją, w której zasadniczą rolę będą odgrywały wymagania dotyczące liczności rozważanych podzbiorów.

2.4.1 Podzbiory k -elementowe zbiorów

Niech $X = \{x_1, \dots, x_n\}$ będzie zbiorem skończonym, a k dowolną liczbą naturalną. Chcemy policzyć:

Ile jest wszystkich różnych podzbiorów zbioru X , mających dokładnie k elementów?

Liczba k -elementowych podzbiorów zbioru n -elementowego będziemy oznaczać symbolem $\binom{n}{k}$ i czytać „ n po k ”. Symbol n w tym zapisie nazywamy *indeksem górnym*, natomiast symbol k – *indeksem dolnym*.

Symbol $\binom{n}{k}$ bywa czasem nazywany *współczynnikiem dwumianowym* ze względu na występowanie w tak zwanym wzorze dwumianowym.⁹ Mianowicie, dla $x, y \in \mathbb{R}$ oraz $n \in \mathbb{N}$ zachodzi następująca równość:

$$(x+y)^n = \sum_{i=0}^n \binom{n}{i} x^i y^{n-i}. \quad (2.12)$$

Wzór powyższy bardzo łatwo jest uzasadnić. Zauważmy bowiem, że jeśli mnożymy n razy przez siebie dwumian $(x+y)$, to otrzymujemy sumę jednomianów o postaci $x^i y^{n-i}$ dla $i = 1, \dots, n$. Każdy jednomian $x^i y^{n-i}$ powtarza się w tej sumie dokładnie tyle razy, na ile sposobów możemy w n wymnażanych czynnikach o postaci $(x+y)$ wybrać i -krotnie składnik x , a tym samym $(n-i)$ -krotnie składnik y . Każdy taki sposób odpowiada jednoznacznie i -elementowemu podzbiorowi zbioru n -elementowego, a zatem po prawej stronie równości (2.12) przed wyrazem $x^i y^{n-i}$ pojawia się symbol $\binom{n}{i}$.

Twierdzenie 2.5 Dla $n, k \in \mathbb{N}$, gdzie $n \geq k$,

$$\binom{n}{k} = \frac{n^k}{k!} = \frac{n!}{k!(n-k)!}. \quad (2.13)$$

Dowód. Dowolna funkcja różnowartościowa $f \in \text{Fun}(A, X)$, gdzie $|A| = k$ oraz $|X| = n$, wyznacza dokładnie jeden k -elementowy podzbiór $f(A)$ n -elementowego zbioru X . Liczba wszystkich takich funkcji jest równa n^k . Ale jednocześnie dla $f \in \text{Fun}(A, X)$ oraz dowolnej permutacji π zbioru A również funkcja $f\pi \in \text{Fun}(A, X)$ wyznacza ten sam podzbiór. Oznacza to, że liczba wszystkich różnych podzbiorów k -elementowych zbioru n -elementowego jest dokładnie $k!$ razy mniejsza niż liczba funkcji różnowartościowych w zbiorze $\text{Fun}(A, X)$, to znaczy jest równa $n^k / k!$. Ostatnią równość w (2.13) otrzymuje się wykorzystując zależność (2.10). ■

Współczynniki dwumianowe mają bardzo liczne zastosowania zarówno w zagadnieniach teoretycznych jak i problemach praktycznych. Z tego względu konieczna jest umiejętność przekształcania wyrażeń, w których

⁹ W niektórych teksthach spotykane są nazwy *współczynniki dwumianowe* albo *symbole Newtona*, a wzór dwumianowy nazywany bywa czasem *wzorem dwumianowym Newtona*. Wzór ten był jednak znany już przed Newtonem; za jego odkrywcę uważa się perskiego poety i matematyka Omara Khayyama (1048 – 1131).

współczynniki te występują. Pomagają w tym liczne tożsamości, związane z tymi współczynnikami. Podamy tu jedynie niektóre z nich. Obszerniejsze omówienie tych zagadnień można na przykład znaleźć w [10].

Zaczniemy od prostej tożsamości, na której opiera się konstrukcja tak zwanego *trójkąta Pascala*.¹⁰ Dla $n, k \in \mathbb{N}$, gdzie $n, k \geq 1$, tożsamość ta ma postać następującą:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \quad (2.14)$$

Tożsamość (2.14) bardzo łatwo uzasadnić. Mamy bowiem z Twierdzenia 2.13 oraz z tożsamości 2.8 i 2.10 następujące zależności:

$$\begin{aligned} \binom{n-1}{k} + \binom{n-1}{k-1} &= \frac{(n-1)^k}{k!} + \frac{(n-1)^{k-1}}{(k-1)!} = \\ &= \frac{n^k}{k!} \cdot \frac{n-k}{n} + \frac{n^k}{(k-1)!} \cdot \frac{1}{n} = \frac{n^k}{k!} = \binom{n}{k}. \end{aligned}$$

Tabela współczynników dwumianowych jest przedstawiona na Rysunku 2.13. Jej wiersze odpowiadają indeksowi górnemu współczynnika dwumianowego, natomiast kolumny – indeksowi dolnemu. Na przecięciu wiersza n -tego i kolumny k -tej umieszczona jest wartość współczynnika dwumianowego $\binom{n}{k}$. Zgodnie z tożsamością (2.14) wartość ta jest równa sumie wartości elementu, leżącego w tabeli bezpośrednio nad $\binom{n}{k}$, tzn. $\binom{n-1}{k}$, oraz elementu poprzedzającego element $\binom{n-1}{k}$ w wierszu $(n-1)$ -szym, to znaczy $\binom{n-1}{k-1}$.

Kolejna tożsamość opisuje symetrię w zbiorze wartości współczynników dwumianowych. Mamy bowiem z (2.13):

$$\binom{n}{k} = \binom{n}{n-k}. \quad (2.15)$$

Jeśli zsumujemy liczności wszystkich podzbiorów dowolnego zbioru n -elementowego X , to otrzymamy wartość $2^n = |\mathcal{P}(X)|$, a zatem,

$$\sum_{i=0}^n \binom{n}{i} = 2^n. \quad (2.16)$$

¹⁰ Od nazwiska Blaise'a Pascala, matematyka francuskiego, żyjącego w latach 1623 – 1662, który napisał rozprawę na temat tych współczynników i przyczynił się do ich popularyzacji. Współczynniki dwumianowe były wykorzystywane już znacznie wcześniej przez Hindusów i Chińczyków. Przypuszcza się, że sam „trójkąt Pascala” był tam znany już w XII wieku n.e., a być może nawet w VI wieku n.e.

| $\binom{n}{k}$ | $k=0$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | ... |
|----------------|-------|----|----|-----|-----|-----|-----|-----|-----|-----|----|----|----|-----|
| $n=0$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 2 | 1 | 2 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 3 | 1 | 3 | 3 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 4 | 1 | 4 | 6 | 4 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 5 | 1 | 5 | 10 | 10 | 5 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 6 | 1 | 6 | 15 | 20 | 15 | 6 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 7 | 1 | 7 | 21 | 35 | 35 | 21 | 7 | 1 | 0 | 0 | 0 | 0 | 0 | |
| 8 | 1 | 8 | 28 | 56 | 70 | 56 | 28 | 8 | 1 | 0 | 0 | 0 | 0 | |
| 9 | 1 | 9 | 36 | 84 | 126 | 126 | 84 | 36 | 9 | 1 | 0 | 0 | 0 | |
| 10 | 1 | 10 | 45 | 120 | 210 | 252 | 210 | 120 | 45 | 10 | 1 | 0 | 0 | |
| 11 | 1 | 11 | 55 | 165 | 330 | 462 | 462 | 330 | 165 | 55 | 11 | 1 | 0 | |
| 12 | 1 | 12 | 66 | 220 | 495 | 792 | 924 | 792 | 495 | 220 | 66 | 12 | 1 | |
| ... | | | | | | | | | | | | | | |

Rysunek 2.13: Wartości współczynników dwumianowych $\binom{n}{k}$ dla $k, n = 0, 1, \dots, 12$. Zerowe elementy w tabeli dla $k > n$ zostały wyróżnione.

2.4. PODZBIORY ZBIORÓW

Traktując obie strony równości (2.12) jako funkcje zmiennej x i różniczkując je po x , a następnie podstawiając $x = y = 1$, uzyskujemy tożsamość

$$\sum_{i=0}^n i \cdot \binom{n}{i} = n \cdot 2^{n-1}. \quad (2.17)$$

Często używaną w różnych przekształceniach, ważną tożsamością jest następująca równość, nazywana *tożsamością Vandermonde'a*:¹¹

$$\binom{m+n}{k} = \sum_{s=0}^k \binom{m}{s} \cdot \binom{n}{k-s}. \quad (2.18)$$

Podstawiając w (2.18) $m = k = n$ otrzymujemy

$$\binom{2n}{n} = \sum_{s=0}^n \binom{n}{s}^2. \quad (2.19)$$

Znane są liczne tożsamości dotyczące iloczynów współczynników dwumianowych. Jedną z częściej stosowanych jest następująca równość, którą łatwo uzasadnić rozpisując współczynniki dwumianowe zgodnie z zależnością 2.13:

$$\binom{n}{k} \cdot \binom{k}{m} = \binom{n}{m} \cdot \binom{n-m}{n-k}. \quad (2.20)$$

Współczynniki dwumianowe można uogólnić na przypadek, gdy indeksy górny i dolny są dowolnymi liczbami rzeczywistymi (patrz na przykład [10]).

Jednym z innych ważnych uogólnień, którym zajmiemy się w następnym punkcie, są tak zwane *współczynniki wielomianowe*.

2.4.2 Współczynniki wielomianowe

Współczynniki wielomianowe są bardzo naturalnym uogólnieniem współczynników dwumianowych. Założymy mianowicie, że mamy n obiektów i m pudełek, gdzie n oraz m są dowolnymi liczbami naturalnymi. Ponadto danc są liczby naturalne k_1, k_2, \dots, k_m , takie że $k_1 + k_2 + \dots + k_m = n$. Interesuje nas, jaka jest liczba wszystkich różnych rozmieszczeń n obiektów w m pudełkach, przy założeniu, że w i -tym pudełku dla $i = 1, \dots, m$,

¹¹ Równość tę udowodnił w roku 1772 francuski muzyk, matematyk i chemik Alexandre-Théophile Vandermonde (1735-1796), który w jednej ze swoich prac wprowadził również pojęcie potęgi ubywającej (patrz str. 13).

znajduje się dokładnie k_i obiektów. Dwa rozmieszczenia uważaemy przy tym za identyczne, jeśli w tych samych pudełkach znajdują się te same obiekty; nie jest zatem istotna kolejność obiektów w pudełkach. Liczbę takich rozmieszczeń oznaczamy symbolem

$$\binom{n}{k_1 \ k_2 \dots \ k_m}$$

i nazywamy współczynnikiem wielomianowym¹² o indeksie górnym n oraz indeksach dolnych k_1, k_2, \dots, k_m . Zauważmy, że współczynnik dwumianowy odpowiada przypadkowi, gdy $m = 2$. W pierwszym z pudełek umieszczamy wówczas $k = k_1$ obiektów, a w drugim pudełku umieszczamy pozostałe obiekty, których liczba jest równa $k_2 = n - k$.

W języku zliczania funkcji pytanie o liczbę takich rozmieszczeń n obiektów w m pudełkach, które spełniają powyższe warunki, może być sformułowane w sposób następujący:

Ille jest wszystkich funkcji $f \in \text{Fun}(X, Y)$, gdzie $|X| = n$, $Y = \{1, \dots, m\}$, dla których $|f^{-1}(\{i\})| = k_i$, $i = 1, \dots, m$?

Poniższe twierdzenie podaje odpowiedź na to pytanie.

Twierdzenie 2.6 *Dla $n \in \mathbb{N}$ oraz liczb naturalnych k_1, k_2, \dots, k_m , spełniających warunek $k_1 + k_2 + \dots + k_m = n$, zachodzi równość*

$$\binom{n}{k_1 \ k_2 \ \dots \ k_m} = \frac{n!}{k_1! \cdot k_2! \cdot \dots \cdot k_m!}. \quad (2.21)$$

Dowód. Rozmieszczenia n obiektów w m pudełkach można dokonać sekwencyjnie. Najpierw wybieramy k_1 obiektów spośród n do pierwszego pudełka. Można to zrobić na $\binom{n}{k_1}$ sposobów. Następnie – spośród pozostałych $n - k_1$ obiektów – wybieramy k_2 obiektów do drugiego pudełka. Można tego dokonać na $\binom{n-k_1}{k_2}$ sposobów. Powtarzamy to postępowanie dla kolejnych pudełek. Liczba sposobów, w jakie można rozmieścić wszystkie n obiektów w m pudełkach, jest więc równa iloczynowi liczb możliwości,

¹²Czasem wielkość ta bywa nazywana *współczynnikiem multimianowym*.

2.4. PODZBIORY ZBIORÓW

jakimi dysponujemy w kolejnych krokach, tzn.

$$\begin{aligned} & \binom{n}{k_1} \cdot \binom{n - k_1}{k_2} \cdot \binom{n - k_1 - k_2}{k_3} \cdot \dots \cdot \binom{n - k_1 - \dots - k_{m-1}}{k_m} = \\ & = \frac{n!}{k_1! (n - k_1)!} \cdot \frac{(n - k_1)!}{k_2! (n - k_1 - k_2)!} \cdot \dots \cdot \frac{(n - k_1 - \dots - k_{m-1})!}{k_m! (n - k_1 - \dots - k_m)!} = \\ & = \frac{n!}{k_1! \cdot k_2! \cdot \dots \cdot k_m!}. \end{aligned}$$

Zauważmy, że dla $m = 2$ oraz $k_1 = k$ i $k_2 = n - k$, gdzie $k, n \in \mathbb{N}$, $k \leq n$, mamy:

$$\binom{n}{k \ n - k} = \frac{n!}{k! (n - k)!} = \binom{n}{k} = \binom{n}{n - k}.$$

Współczynniki wielomianowe są wygodnym narzędziem, używanym w licznych problemach praktycznych. Poniższe przykłady ilustrują niektóre z takich zastosowań.

Przykład 2.10 Chcemy znaleźć liczbę wszystkich różnych nazw dziesięciocząiskowych, które można utworzyć zapisując w dowolnej kolejności następujące dziesięć liter: A, A, A, A, B, B, B, C, C, D.

W języku zliczania funkcji sformułowanie tego problemu jest bardzo naturalne. Mianowicie, każda nazwa dziesięciocząiskowa, w której występują wyłącznie litery A, B, C, D, jest wyznaczona przez pewną funkcję f ze zbioru $X = \{x_1, \dots, x_{10}\}$, gdzie x_i jest i -tym miejscem w nazwie, w zbiór $Y = \{A, B, C, D\}$. Dodatkowo żąda się, aby jądro takiej funkcji, to znaczy rodzinę zbiorów $\{f^{-1}(A), f^{-1}(B), f^{-1}(C), f^{-1}(D)\}$, spełniało następujące warunki: $|f^{-1}(A)| = k_A = 4$, $|f^{-1}(B)| = k_B = 3$, $|f^{-1}(C)| = k_C = 2$, $|f^{-1}(D)| = k_D = 1$. Problem polega więc na obliczeniu, ile jest takich funkcji w zbiorze $\text{Fun}(X, Y)$. Z Twierdzenia 2.6 wynika, że jest ich dokładnie

$$\binom{n}{k_A \ k_B \ k_C \ k_D} = \binom{10}{4 \ 3 \ 2 \ 1} = \frac{10!}{4! \cdot 3! \cdot 2! \cdot 1!} = 12600.$$

Przykład 2.11 Problem sekwencjonowania DNA lub RNA polega na odtworzeniu sekwencji nukleotydów w badanym łańcuchu. Założmy, że interesuje nas struktura fragmentu łańcucha RNA, o którym wiemy, że składa się z dziesięciu nukleotydów. Wiemy ponadto, że w łańcuchu występuje czterokrotnie adenina (A), trzykrotnie guanina (G), dwukrotnie cytozyna (C) i jeden raz uracyl (U). Dodatkowo wiemy, że na początku łańcucha znajduje się guanina. Chcemy policzyć, ile jest wszystkich różnych łańcuchów RNA zgodnych z taką analizą.

Powyższy problem jest niemal identyczny z problemem rozważanym w Przykładzie 2.10. Jedyna różnica polega na tym, że pierwszy element łańcucha jest już ustalony: jest to guanina (G). Należy więc tylko policzyć, ile jest wszystkich różnych łańcuchów, które można utworzyć ustawiając w dowolnej kolejności nukleotydy A, A, A, A, G, G, C, C, U na pozycjach od drugiej do dziesiątej. Mamy tutaj $m = |\{A, G, C, U\}| = 4$, $k_1 = 4$, $k_2 = 2$, $k_3 = 2$, $k_4 = 1$ oraz $n = 9$. Otrzymujemy zatem następującą liczbę wszystkich możliwych łańcuchów RNA, odpowiadających powyższym warunkom:

$$\binom{n}{k_1 \ k_2 \ k_3 \ k_4} = \binom{9}{4 \ 2 \ 2 \ 1} = \frac{9!}{4! \cdot 2! \cdot 2! \cdot 1!} = 3780.$$

□

W ten sam sposób można rozwiązać bardzo wiele analogicznych problemów praktycznych, na przykład policzyć liczbę różnych możliwych rozdzielnych kart w brydżu, liczbę zespołów o zadanym składzie, które można wyłonić z danego zbioru specjalistów itp.

Operowanie współczynnikami wielomianowymi ułatwiają liczne tożsamości, które są uogólnieniami zależności obowiązujących dla współczynników dwumianowych. Podamy tu tylko niektóre z nich. Obszerne omówienie tych zagadnień można znaleźć na przykład w [10].

Zaczniemy od naturalnego uogólnienia wzoru dwumianowego. W analogicznym sposobie, jak zrobiono to w przypadku zależności (2.12), można uzasadnić, że dla dowolnych $m, n \in \mathbb{N}$ oraz $x_1, \dots, x_m \in \mathbb{R}$ zachodzi następująca równość:

$$(x_1 + \dots + x_m)^n = \sum_{\substack{k_1, \dots, k_m \in \mathbb{N} \\ k_1 + \dots + k_m = n}} \binom{n}{k_1 \dots k_m} x_1^{k_1} \dots x_m^{k_m}. \quad (2.22)$$

Zależność powyższa nosi nazwę *wzoru wielomianowego*¹³. Podstawiając w (2.22) $x_i = 1$ dla $i = 1, \dots, m$, otrzymujemy tożsamość, która jest uogólnieniem równości (2.17):

$$\sum_{\substack{k_1, \dots, k_m \in \mathbb{N} \\ k_1 + \dots + k_m = n}} \binom{n}{k_1 \dots k_m} = m^n. \quad (2.23)$$

Równość powyższa ma prostą interpretację w języku zliczania funkcji. Zauważmy, że zgodnie z definicją współczynnika wielomianowego $\binom{n}{k_1 \dots k_m}$, jego wartość dla ustalonych n, m, k_1, \dots, k_m , jest równa liczbie funkcji ze zbioru n -elementowego X w zbiór m -elementowy $Y = \{1, \dots, m\}$, których jądro (patrz str. 9) spełnia warunki $|f^{-1}(\{i\})| = k_i$ dla $i = 1, \dots, m$. Sumując liczby takich funkcji po wszystkich wartościach k_i , takich że $k_i \geq 0, i = 1, \dots, m$, oraz $k_1 + \dots + k_m = n$, otrzymujemy liczbę wszystkich funkcji ze zbioru n -elementowego w zbiór m -elementowy, to znaczy m^n .

Odpowiednikiem zależności (2.14), na której oparta jest konstrukcja trójkąta Pascala, jest następująca, łatwa do uzasadnienia tożsamość:

$$\begin{aligned} \binom{n}{k_1 \ k_2 \ k_3 \ \dots \ k_m} &= \binom{n-1}{k_1 - 1 \ k_2 \ k_3 \ \dots \ k_m} + \\ &+ \binom{n-1}{k_1 \ k_2 - 1 \ k_3 \ \dots \ k_m} + \dots \\ &\dots + \binom{n-1}{k_1 \ k_2 \ k_3 \ \dots \ k_m - 1}. \end{aligned} \quad (2.24)$$

Powyższa nierówność mogłaby być podstawą tworzenia wielowymiarowej tablicy współczynników wielomianowych, chociaż korzystanie z niej byłoby znacznie bardziej skomplikowane niż z trójkąta Pascala.

Dotychczas zajmowaliśmy się zliczaniem podzbiorów „zwykłych” zbiorów, to znaczy takich, w których elementy nie mogą się powtarzać. W licznych problemach praktycznych wygodne jest rozważanie pewnego uogólnienia zbioru, nazywanego *zborem z powtórzeniami*. Następny rozdział dotyczy zliczania podzbiorów takich właśnie obiektów.

¹³Zależność ta została podana w roku 1697 przez żyjącego w Anglii matematyka francuskiego pochodzenia Abrahama de Moivre'a (1667-1754).

2.5 Zbiory z powtórzeniami

Niech $X = \{x_1, \dots, x_n\}$ będzie dowolnym zbiorem. Założymy, że chcemy opisać sytuację, w której mamy do czynienia z wielokrotnym występowaniem elementów tego zbioru. Tak jest na przykład przy zapisie fragmentu łańcucha RNA, rozważanym w Przykładzie 2.11. Mamy tu do czynienia ze zbiorem X , złożonym z czterech możliwych nukleotydów, tzn. $X = \{A, G, C, U\}$, i każdy z nich występuje w łańcuchu pewną liczbę razy. Taką sytuację wygodnie opisuje tak zwany *zbiór z powtórzeniami*.

Formalnie rzecz biorąc, zbiór z powtórzeniami jest parą uporządkowaną $Q = (X, k)$, gdzie X jest zbiorem n -elementowym, natomiast $k = (k_1, \dots, k_n)$ jest n -elementowym ciągiem o wartościach w zbiorze liczb naturalnych.

Zbiór X jest nazywany *zbiorem podstawowym*, natomiast liczba naturalna k_i dla $i = 1, \dots, k_n$, nosi nazwę *krotności* występowania elementu x_i w zbiorze z powtórzeniami Q .

Dla zbioru z powtórzeniami $Q = (X, (k_1, \dots, k_n))$ będziemy stosować następujące, wygodne oznaczenie:

$$Q = \langle k_1 * x_1, \dots, k_n * x_n \rangle.$$

W Przykładzie 2.11 mieliśmy $X = \{A, G, C, U\}$ oraz $k_1 = 4, k_2 = 2, k_3 = 2, k_4 = 1$, a zatem skład takiego fragmentu łańcucha RNA można opisać zbiorem z powtórzeniami $Q = \langle 4 * A, 2 * G, 2 * C, 1 * U \rangle$.

Zbiór z powtórzeniami można traktować jako naturalne uogólnienie zbioru rozważanego w teorii mnogości; w ‘wykłym’ zbiorze krotności wszystkich elementów są po prostu równe 1.

Liczność zbioru z powtórzeniami $Q = \langle k_1 * x_1, \dots, k_n * x_n \rangle$, oznaczaną symbolem $|Q|$, definiujemy w oczywisty sposób jako sumę krotności wszystkich jego elementów, to znaczy

$$|Q| = k_1 + \dots + k_n.$$

Równie naturalna jest definicja *podzbioru zbioru z powtórzeniami*. Mianowicie, zbiór z powtórzeniami $S = \langle m_1 * x_1, \dots, m_n * x_n \rangle$ jest podzbiorem zbioru z powtórzeniami $Q = \langle k_1 * x_1, \dots, k_n * x_n \rangle$ wtedy i tylko wtedy, gdy

$$0 \leq m_i \leq k_i \text{ dla każdego } i = 1, \dots, n. \quad (2.25)$$

2.5. ZBIORY Z POWTÓRZENIAMI

Dla zaznaczenia faktu, że zbiór z powtórzeniami S jest podzbiorem zbioru z powtórzeniami Q , używamy tego samego zapisu, co w przypadku zbiorów bez powtórzeń, to znaczy piszemy $S \subseteq Q$.

Podobnie, rodzinę wszystkich podzbiorów zbioru z powtórzeniami Q oznaczamy symbolem $\mathcal{P}(Q)$.

Latwo zauważyc, że liczba wszystkich podzbiorów zbioru z powtórzeniami $Q = \langle k_1 * x_1, \dots, k_n * x_n \rangle$ jest równa

$$|\mathcal{P}(Q)| = (1 + k_1) \cdot (1 + k_2) \cdot \dots \cdot (1 + k_n),$$

bowiem dokładnie tyle jest wszystkich ciągów (m_1, \dots, m_n) , w których liczby naturalne m_1, \dots, m_n , spełniają warunki (2.25).

Nieco trudniej jest znaleźć liczbę wszystkich podzbiorów zbioru z powtórzeniami, mających licznosć równą dokładnie k , gdzie k jest dowolną liczbą naturalną. Poniższe twierdzenie podaje rozwiązanie tego problemu w pewnym szczególnym przypadku, a mianowicie wówczas, gdy krotności wszystkich elementów zbioru z powtórzeniami nie są mniejsze niż k . Do przypadku ogólnego wróćmy w Rozdziale 3.

Twierdzenie 2.7 *Liczba wszystkich k -elementowych podzbiorów zbioru z powtórzeniami $\langle k_1 * x_1, \dots, k_n * x_n \rangle$, gdzie $k_i \geq k$ dla $i = 1, \dots, n$, jest równa*

$$\frac{n^{\bar{k}}}{k!} = \binom{n+k-1}{k}. \quad (2.26)$$

Dowód. Rozważmy wszystkie rozmieszczenia uporządkowane k obiektów w n pudełkach. Liczba takich rozmieszczeń jest równa $n^{\bar{k}}$. Ponadto, każde takie rozmieszczenie wyznacza jednoznacznie dokładnie jeden podzbiór k -elementowy $\langle r_1 * x_1, \dots, r_n * x_n \rangle$ zbioru z powtórzeniami $\langle k_1 * x_1, \dots, k_n * x_n \rangle$, gdzie r_i jest liczbą obiektów umieszczonych w pudełku i -tym oraz $r_1 + \dots + r_n = k$. Zauważmy jednak, że dokładnie $k!$ rozmieszczeń, powstacych w wyniku wszystkich możliwych permutacji k obiektów, wyznacza ten sam podzbiór, a zatem liczba wszystkich różnych podzbiorów zbioru z powtórzeniami $\langle k_1 * x_1, \dots, k_n * x_n \rangle$ jest równa

$$\frac{n^{\bar{k}}}{k!} = \frac{n(n+1)\dots(n+k-1)}{k!} = \frac{(n+k-1)}{k!(n-1)!} = \binom{n+k-1}{k}.$$

Twierdzenie 2.7 dotyczy sprawdzenia szczególnego przypadku zbioru z powtórzeniami, ale jest bardzo użyteczne w wielu praktycznych zastosowaniach. Jedno z takich zastosowań jest przedstawione w poniższym przykładzie.

Przykład 2.12 Rozważmy liniowe równanie diofantyczne¹⁴ w postaci

$$x_1 + x_2 + \dots + x_n = k. \quad (2.27)$$

Chcemy wyznaczyć liczbę wszystkich nieujemnych rozwiązań tego równania, to znaczy liczbę wektorów $(x_1, \dots, x_n) \in \mathbb{N}^n$, spełniających równość (2.27). Zauważmy, że każdy taki wektor jest wzajemnie jednoznacznie przyporządkowany k -elementowemu podzbiorowi $\langle x_1 * z_1, \dots, x_n * z_n \rangle$ zbioru z powtórzeniami $Q = \langle k * z_1, \dots, k * z_n \rangle$. Liczba wszystkich nieujemnych całkowitoliczbowych rozwiązań równania (2.27) jest więc równa liczbie wszystkich k -elementowych podzbiorów zbioru Q , a ta – zgodnie z Twierdzeniem 2.7 – jest równa $\binom{n+k-1}{k}$.

Równanie diofantyczne 2.27 występujące w tym przykładzie może być użyte do modelowania następującego problemu:

Mamy k programów i n procesorów, z których każdy może wykonywać (bez przerwań) dowolny z tych programów. Chcemy policzyć liczbę wszystkich możliwych schematów obciążenia procesorów przy wykonywaniu k programów. Oznacza to, że chcemy policzyć liczbę wszystkich wektorów całkowitoliczbowych nieujemnych (l_1, \dots, l_n) , gdzie l_i dla $i = 1, \dots, n$, mówi, ile programów przydzielono do wykonania procesorowi o numerze i . Zauważmy, że w tym zagadnieniu nie interesuje nas, które programy trafiają do którego procesora, ani w jakiej kolejności będą wykonywane, a jedynie ich liczba.

Przy takim postawieniu zagadnienia liczba możliwych schematów obciążenia procesorów jest właśnie równa liczbie rozwiązań całkowitoliczbowych nieujemnych równania diofantycznego 2.27.

□

¹⁴Równaniem diofantycznym nazywamy równanie, w którym zwykle wszystkie współczynniki są całkowitoliczbowe i dla którego poszukujemy wyłącznie rozwiązań całkowitoliczbowych. Nazwa pochodzi od nazwiska greckiego matematyka Diofantosa z Aleksandrii (ok. 200-284).

2.6 Podziały zbioru

Dotychczas zajmowaliśmy się wyznaczaniem liczby wszystkich podzbiorów danego zbioru skończonego. Niniejszy rozdział jest poświęcony wyznaczaniu liczby wszystkich różnych rodzin, złożonych z niepustych i rozłącznych podzbiorów, dających w sumie cały wyjściowy zbiór. Takie rodziny nazywamy *podziałami zbioru na bloki*.

Definicja 2.7 Podzieleniem zbioru skończonego X na k bloków, gdzie $k \in \mathbb{N}$, nazywamy rodzinę zbiorów $A = \{A_1, \dots, A_k\}$, spełniającą następujące warunki:

- (i) $A_i \neq \emptyset$ dla $1 \leq i \leq k$;
- (ii) $A_1 \cup \dots \cup A_k = X$;
- (iii) $A_i \cap A_j = \emptyset$ dla $1 \leq i < j \leq k$.

Podzbiory A_1, \dots, A_k , nazywamy *blokami* podziału A .

W wielu praktycznych zagadnieniach potrzebna jest umiejętność wyznaczenia liczby wszystkich różnych podziałów danego zbioru skończonego na określoną liczbę bloków. Poniższy przykład stanowi uproszczoną ilustrację takiego problemu.

Przykład 2.13 Założymy, że mamy do wykonania q programów i dysponujemy k procesorami, z których każdy może być użyty do wykonania dowolnego z programów. Interesuje nas, na ile sposobów wszystkie te programy mogą być podzielone na k rozłącznych podzbiorów, z których każdy zostanie w następnym etapie przydzielony jednemu z procesorów. Zakładamy przy tym, że każdy procesor musi otrzymać do wykonania co najmniej jeden program. (Porównaj to zadanie z problemem rozważanym w Przykładzie 2.12, gdzie nie było warunku, że każdy z procesorów musi otrzymać do wykonania co najmniej jeden program.)

Zagadnienie powyższe jest równoważne znalezieniu liczby wszystkich podziałów zbioru q -elementowego na k bloków.

Jeśli w przykładzie z programami i procesorami q jest małą liczbą, to łatwo jest wypisać wszystkie możliwe podziały zbioru q -elementowego na bloki. Założymy na przykład, że mamy cztery programy oznaczane literami a, b, c, d , i że dysponujemy trzema procesorami. Zatem $X = \{a, b, c, d\}$ oraz $k = 3$. Łatwo sprawdzić, że istnieje dokładnie sześć podziałów zbioru

X na trzy bloki. Oto one:

$$\begin{aligned}\mathcal{A}_1 &= \{\{a\}, \{b\}, \{c, d\}\}, \\ \mathcal{A}_2 &= \{\{a\}, \{b, c\}, \{d\}\}, \\ \mathcal{A}_3 &= \{\{a, b\}, \{c\}, \{d\}\}, \\ \mathcal{A}_4 &= \{\{a, c\}, \{b\}, \{d\}\}, \\ \mathcal{A}_5 &= \{\{a\}, \{b, d\}, \{c\}\}, \\ \mathcal{A}_6 &= \{\{a, d\}, \{b\}, \{c\}\}.\end{aligned}$$

Gdybyśmy jednak zwiększyli liczbę programów do siedmiu, to okazałoby się, że wypisanie wszystkich podziałów zbioru programów na trzy bloki jest już znacznie trudniejsze, bowiem – jak się wkrótce przekonamy – liczba tych podziałów jest równa 301. \square

Wprowadźmy następujące oznaczenia dla dowolnego zbioru skończonego X i liczby naturalnej k :

$\Pi_k(X)$ – zbiór wszystkich podziałów zbioru X na k bloków;

$\Pi(X)$ – zbiór wszystkich podziałów zbioru X na bloki.

Zachodzi następujący oczywisty związek między tak zdefiniowanymi zbiorami:

$$\Pi(X) = \Pi_1(X) \cup \dots \cup \Pi_n(X). \quad (2.28)$$

Naszym celem będzie wyznaczenie liczności zdefiniowanych wyżej zbiorów $\Pi(X)$ oraz $\Pi_k(X)$ dla $k \in \mathbb{N}$.

Zaczniemy od znalezienia liczby podziałów dowolnego zbioru n -elementowego na k bloków, to znaczy od wyznaczenia liczności zbioru $\Pi_k(X)$ dla $|X| = n$. Ponieważ wielkość ta występuje w bardzo wielu zastosowaniach, przyjmiemy dla niej specjalne oznaczenie $\binom{n}{k}$, przypominające symbol współczynnika dwumianowego.¹⁵ Mamy więc

$$\binom{n}{k} = |\Pi_k(X)|, \quad \text{gdzie } |X| = n.$$

Jeśli $k > n$, to – oczywiście – liczba podziałów zbioru n -elementowego na k bloków jest równa 0, a zatem $\binom{n}{k} = 0$ dla $k > n$. Przyjmiemy

¹⁵Zapis $\binom{n}{k}$ czytamy „ n na k ”. W niektórych tekstach stosowane są symbole $S(n, k)$ albo $S_n^{(k)}$. Notacja $\binom{n}{k}$, używana w tej książce, została wprowadzona w roku 1935 przez Jovana Karamatę i wydaje się być bardziej spójna z innymi stosowanymi oznaczeniami.

2.6. PODZIAŁY ZBIORU

również, że istnieje dokładnie jeden podział zbioru pustego na 0 bloków, tzn. $\binom{0}{0} = 1$.

Dla ustalonych liczb naturalnych n, k , wielkość $\binom{n}{k}$ nosi nazwę *liczby Stirlinga drugiego rodzaju* albo *podzbiorowej liczby Stirlinga*.¹⁶

Liczby Stirlinga drugiego rodzaju dla $n, k \in \mathbb{N}$ mogą być ulożone w tabelę (patrz Rysunek 2.14), która przypomina znany trójkąt Pascala. W tabeli tej zerowe wartości $\binom{n}{k}$ dla $k > n$ zostały wyróżnione.

Podstawą tworzenia tabeli liczb Stirlinga drugiego rodzaju są poniższe, oczywiste zależności:

$$\binom{n}{n} = 1 \quad \text{dla } n \geq 0, \quad \binom{n}{0} = 0 \quad \text{dla } n > 0, \quad (2.29)$$

oraz następujące twierdzenie:

Twierdzenie 2.8 Dla $n \in \mathbb{N}$ oraz $k \in \mathbb{N}$, gdzie $0 < k < n$, zachodzi następująca równość:

$$\binom{n}{k} = \binom{n-1}{k-1} + k \cdot \binom{n-1}{k}. \quad (2.30)$$

Dowód. Rozważmy zbiór $\Pi_k(X)$ wszystkich podziałów n -elementowego zbioru $X = \{1, \dots, n\}$ na k bloków. Dla dowolnego podziału \mathcal{A} , należącego do $\Pi_k(X)$, zachodzi dokładnie jeden z następujących dwóch wzajemnie wykluczających się przypadków:

- (i) podział \mathcal{A} zawiera blok jednoelementowy $\{n\}$;
- (ii) element n należy do bloku co najmniej dwuelementowego.

Liczba wszystkich podziałów należących do $\Pi_k(X)$, dla których zachodzi przypadek (i), jest równa liczbie podziałów zbioru $X = \{1, \dots, n-1\}$ na $k-1$ bloków, to znaczy jest równa $\binom{n-1}{k-1}$. Natomiast liczba podziałów ze zbioru $\Pi_k(X)$, dla których zachodzi przypadek (ii), jest równa $k \cdot \binom{n-1}{k}$, ponieważ podziały te otrzymujemy z $\binom{n-1}{k}$ podziałów zbioru $X = \{1, \dots, n-1\}$ na k bloków poprzez dodanie elementu n kolejno do każdego z bloków w każdym z tych podziałów. Sumując liczby podziałów dla obu wykluczających się przypadków otrzymujemy zależność (2.30). ■

¹⁶Nazwa pochodzi od nazwiska angielskiego matematyka Jamesa Stirlinga (1692–1770), który badał te wielkości w wydanej w roku 1730 roku książce *Methodus Differentialis*.

| | B_n | $\binom{n}{k}$ | | | | | | | | | | | |
|-------|--------|----------------|-----|-----|------|-------|-------|-------|------|-----|-----|-----|-----|
| | | $k=0$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... |
| $n=0$ | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 2 | 2 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 3 | 5 | 0 | 1 | 3 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 4 | 15 | 0 | 1 | 7 | 6 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 5 | 52 | 0 | 1 | 15 | 25 | 10 | 1 | 0 | 0 | 0 | 0 | 0 | ... |
| 6 | 203 | 0 | 1 | 31 | 90 | 65 | 15 | 1 | 0 | 0 | 0 | 0 | ... |
| 7 | 877 | 0 | 1 | 63 | 301 | 350 | 140 | 21 | 1 | 0 | 0 | 0 | ... |
| 8 | 4140 | 0 | 1 | 127 | 966 | 1701 | 1050 | 266 | 28 | 1 | 0 | 0 | ... |
| 9 | 21147 | 0 | 1 | 255 | 3025 | 7770 | 6951 | 2646 | 462 | 36 | 1 | 0 | ... |
| 10 | 115975 | 0 | 1 | 511 | 9330 | 34105 | 42525 | 22827 | 5880 | 750 | 45 | 1 | ... |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |

Rysunek 2.14: Tabela liczb Stirlinga drugiego rodzaju $\binom{n}{k}$ i liczb Bella B_n dla $k, n = 0, 1, \dots, 10$.

2.6. PODZIAŁY ZBIORU

Twierdzenie 2.8 podaje zależność rekurencyjną, pozwalającą wyznaczać kolejne wiersze tablicy liczb Stirlinga drugiego rodzaju. W Rozdziale 3 na stronie 93 podamy jeszcze jedną formułę, umożliwiającą znalezienie tych liczb w sposób nierekurencyjny.

W niektórych zastosowaniach potrzebna jest znajomość liczby wszystkich możliwych podziałów zbioru n -elementowego, to znaczy znajomość liczności zbioru $\Pi(X)$, gdy $|X| = n$. Tę wielkość dla danego $n \in \mathbb{N}$ nazywamy n -tą liczbą Bella¹⁷ i oznaczamy symbolem B_n . Z zależności (2.28) wynika, że dla $n \in \mathbb{N}$,

$$B_n = \sum_{k=0}^n \binom{n}{k}. \quad (2.31)$$

Wartości kolejnych liczb Bella, podane w pierwszej kolumnie tablicy z Rysunku 2.14, są więc równe sumom wszystkich pozostałych elementów w danym wierszu tablicy.

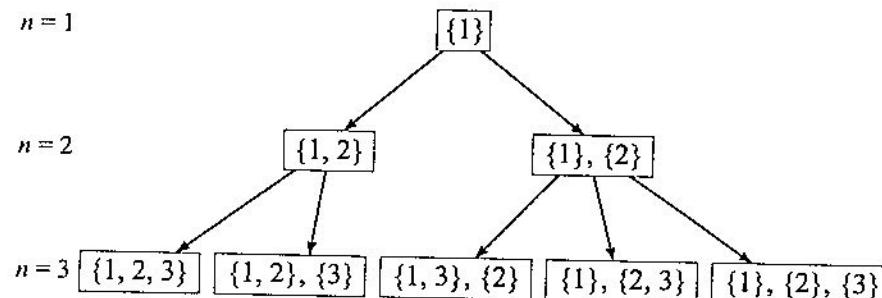
W niektórych sytuacjach potrzebne jest wyznaczenie wszystkich podziałów danego zbioru $X = \{1, \dots, n\}$. Można to łatwo zrobić dla niezbyt dużych wartości n stosując opisane niżej postępowanie rekurencyjne:

Załóżmy, że dla pewnego k , gdzie $1 \leq k < n$, mamy już rodzinę zbiorów $\mathcal{A} = \{A_1, \dots, A_l\}$, będącą podziałem zbioru $\{1, \dots, k-1\}$ na bloki. Wówczas łatwo zauważyc, że następujące rodziny zbiorów są podziałami zbioru $\{1, \dots, k\}$:

$$\begin{aligned} &\{A_1 \cup \{k\}, A_2, \dots, A_l\}, \\ &\{A_1, A_2 \cup \{k\}, \dots, A_l\}, \\ &\vdots \\ &\{A_1, A_2, \dots, A_l \cup \{k\}\}, \\ &\{A_1, A_2, \dots, A_l, \{k\}\}. \end{aligned}$$

Zaczynając od rodziny, która zawiera tylko jednoklementowy zbiór $\{1\}$, i powtarzając opisany wyżej krok procedury rekurencyjnej $n - 1$ razy, otrzymamy drzewo, którego liście odpowiadają wszystkim możliwym podziałom zbioru $\{1, \dots, n\}$ (patrz Rysunek 2.15).

¹⁷Odszwarcia amerykańskiego matematyka szkockiego pochodzenia Erica Temple'a Bella (1883-1960).

Rysunek 2.15: Drzewo podziałów zbioru $\{1, 2, 3\}$.

Podobnie jak w przypadku współczynników dwumianowych i wielomianowych, istnieje wiele tożsamości, w których występują liczby Stirlinga drugiego rodzaju i liczby Bella. Podamy tu jedynie niektóre z nich, pomijając przy tym wszystkie dowody. Uzasadnienia przytoczonych zależności oraz wiele innych tożsamości tego typu można znaleźć na przykład w [10].

Dla $k, n, x \in \mathbb{N}$ zachodzą następujące równości:

$$x^n = \sum_{k=0}^n \begin{Bmatrix} n \\ k \end{Bmatrix} \cdot x^k = \sum_{k=0}^n (-1)^{n-k} \cdot \begin{Bmatrix} n \\ k \end{Bmatrix} \cdot x^k. \quad (2.32)$$

Tożsamość (2.32) wyraża n -tą potęgę liczby x poprzez potęgi ubywałe albo przez potęgi przyrastające x .

Istnieją również zależności odwrotne, w których potęgi przyrastające x^n oraz potęgi ubywające x^n są wyrażone poprzez potęgi liczby x . W zależnościach tych przy wyrażeniu x^k występuje współczynnik oznaczany symbolem $\begin{Bmatrix} n \\ k \end{Bmatrix}$, który nosi nazwę *liczby Stirlinga pierwszego rodzaju*.

Liczby Stirlinga pierwszego rodzaju mają specjalną interpretację, związaną z własnościami permutacji zbiorów, o której będzie jeszcze mowa w Rozdziale 4 (patrz str. 112).

Dla $m, n, x \in \mathbb{N}$ zachodzą następujące równości:

$$x^n = \sum_{k=0}^n \begin{Bmatrix} n \\ k \end{Bmatrix} \cdot x^k \quad (2.33)$$

2.6. PODZIAŁY ZBIORU

oraz

$$x^n = \sum_{k=0}^n (-1)^{n-k} \cdot \begin{Bmatrix} n \\ k \end{Bmatrix} \cdot x^k. \quad (2.34)$$

Liczby Stirlinga pierwszego rodzaju, występujące w powyższych równościach, można wyznaczać z zależności rekurencyjnych, które są analogiczne do zależności (2.30). Zachodzą mianowicie następujące fakty:

$$\begin{Bmatrix} 0 \\ 0 \end{Bmatrix} = 1; \quad (2.35)$$

$$\begin{Bmatrix} n \\ k \end{Bmatrix} = 0 \text{ dla } k > n; \quad (2.36)$$

$$\begin{Bmatrix} n \\ k \end{Bmatrix} = \begin{Bmatrix} n-1 \\ k-1 \end{Bmatrix} + (n-1) \begin{Bmatrix} n-1 \\ k \end{Bmatrix} \text{ dla } 0 < k \leq n. \quad (2.37)$$

Liczby Stirlinga pierwszego rodzaju tworzą pokazaną na Rysunku 2.16 tabelę, której konstrukcja oparta jest na powyższych zależnościach rekurencyjnych i przypomina konstrukcję trójkąta Pascala oraz analogicznej tabeli dla liczb Stirlinga drugiego rodzaju. W tabeli tej zerowe wartości $\begin{Bmatrix} n \\ k \end{Bmatrix}$ dla $k > n$ zostały wyróżnione.

| $\begin{Bmatrix} n \\ k \end{Bmatrix}$ | $k=0$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | ... |
|--|-------|--------|---------|---------|--------|--------|-------|------|-----|----|----|-----|
| $n=0$ | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 2 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 3 | 0 | 2 | 3 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 4 | 0 | 6 | 11 | 6 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 5 | 0 | 24 | 50 | 35 | 10 | 1 | 0 | 0 | 0 | 0 | 0 | |
| 6 | 0 | 120 | 274 | 225 | 85 | 15 | 1 | 0 | 0 | 0 | 0 | |
| 7 | 0 | 720 | 1764 | 1624 | 735 | 175 | 21 | 1 | 0 | 0 | 0 | |
| 8 | 0 | 5040 | 13068 | 13132 | 6769 | 1960 | 322 | 28 | 1 | 0 | 0 | |
| 9 | 0 | 40320 | 109584 | 118124 | 67284 | 22449 | 4536 | 546 | 36 | 1 | 0 | |
| 10 | 0 | 362880 | 1026576 | 1172700 | 723680 | 269325 | 63273 | 9450 | 870 | 45 | 1 | |
| ... | | | | | | | | | | | | |

Rysunek 2.16: Tabela liczb Stirlinga pierwszego rodzaju.

Liczby Stirlinga pierwszego i drugiego rodzaju są powiązane ze sobą następującymi tożsamościami, które zachodzą dla dowolnych liczb naturalnych m, n (patrz np. [10, 28]):

$$\sum_{k=0}^n (-1)^{n-k} \begin{Bmatrix} n \\ k \end{Bmatrix} \begin{Bmatrix} k \\ m \end{Bmatrix} = [m = n] = \sum_{k=0}^n (-1)^{n-k} \begin{Bmatrix} n \\ k \end{Bmatrix} \begin{Bmatrix} k \\ m \end{Bmatrix}. \quad (2.38)$$

Przypomnijmy, że zgodnie z przyjętą przez nas notacją, wartość wyrażenia $[m = n]$ w (2.38) jest równa 1, jeśli $m = n$, i jest równa 0, dla $m \neq n$.

Tożsamości, w których występują liczby Bella, są również liczne, ale bywają rzadziej stosowane. Jedną z bardziej znanych jest następująca równość, która może być użyta do rekurencyjnego wyznaczania liczb Bella B_n dla $n \in \mathbb{N}$, przyjmując, że $B_0 = 1$:

$$B_{n+1} = \sum_{i=0}^n \binom{n}{i} B_i. \quad (2.39)$$

Jednym z ważnych zastosowań liczb Stirlinga drugiego rodzaju jest możliwość użycia ich do wyznaczenia liczby wszystkich funkcji ze zbioru n -elementowego X na zbiór m -elementowy Y , to znaczy liczby wszystkich surjekcji w zbiorze $\text{Fun}(X, Y)$. Zajmiemy się tym w Rozdziale 2.6.2. Zanim jednak do tego przejdziemy, przedstawimy w następnym rozdziale pewne naturalne związki podziałów zbioru z relacjami równoważności i częściowego porządku.

2.6.1 Podziały zbiorów a relacje

Niech X będzie zbiorem skończonym o liczności n i niech \mathcal{A} oznacza dowolny podział tego zbioru na bloki. Z podziałem \mathcal{A} można związać pewną relację, którą oznaczamy symbolem $R_{\mathcal{A}}$ i zdefiniujemy następująco:

$$R_{\mathcal{A}} = \bigcup_{A \in \mathcal{A}} A \times A. \quad (2.40)$$

Zauważmy, iż powyższy zapis oznacza, że $(x, y) \in R_{\mathcal{A}}$ wtedy i tylko wtedy, gdy elementy x i y należą do tego samego bloku podziału \mathcal{A} . Jeśli na przykład $X = \{a, b, c, d\}$ i $\mathcal{A} = \{\{a\}, \{b, d\}, \{c\}\}$, to relacja $R_{\mathcal{A}}$ jest następującym podzbiorem zbioru $X \times X$:

$$R_{\mathcal{A}} = \{(a, a), (b, b), (b, d), (d, b), (d, d), (c, c)\}.$$

2.6. PODZIAŁY ZBIORU

Łatwo stwierdzić, że dla dowolnego podziału \mathcal{A} zbioru X , relacja $R_{\mathcal{A}}$ zdefiniowana zależnością (2.40) jest symetryczna, zwrotna i przechodnia, a zatem jest relacją równoważności w zbiorze X .

I na odwrót – dowolnej relacji równoważności R w zbiorze X można przyporządkować jednoznacznie podział \mathcal{A}_R zbioru X na bloki. Podział ten jest po prostu zbiorem wszystkich klas abstrakcji relacji równoważności R w X , który to zbiór oznaczamy symbolem X/R (patrz str. 7).

Jeśli na przykład przyjmiemy, że $X = \{x \in \mathbb{N} : x \leq 10\}$ i jako relację równoważności weźmiemy relację R zdefiniowaną następująco:

$$xRy \Leftrightarrow x \bmod 3 = y \bmod 3, \quad (2.41)$$

to otrzymamy podział \mathcal{A}_R zbioru X na bloki, gdzie:

$$\mathcal{A}_R = X/R = \{\{0, 3, 6, 9\}, \{1, 4, 7, 10\}, \{2, 5, 8\}\}. \quad (2.42)$$

Powysze rozważania prowadzą do następującego, prostego wniosku:

Wniosek 2.4 *Liczba wszystkich różnych relacji równoważności w zbiorze n -elementowym jest równa n -tej liczbie Bella B_n .*

Zatem na przykład liczba wszystkich relacji równoważności, które można zdefiniować w zbiorze pięcioelementowym, jest równa 52, bowiem $B_5 = 52$ (patrz tabela liczb Bella na Rysunku 2.14).

W rodzinie $\Pi(X)$ wszystkich podziałów zbioru X na bloki można zdefiniować pewną relację częściowego porządku. Rozważmy mianowicie zbiór skończony X i dwa jego podziały na bloki: \mathcal{A} oraz \mathcal{A}' . Mówimy, że podział \mathcal{A}' zbioru X jest *rozdrobnieniem* podziału \mathcal{A} wtedy i tylko wtedy, gdy każdy blok podziału \mathcal{A} jest sumą mnogościową pewnej liczby bloków podziału \mathcal{A}' . Fakt ten zapisujemy następująco:

$$\mathcal{A}' \preceq \mathcal{A}$$

i mówimy, że podział \mathcal{A}' jest w *relacji rozdrobnienia* z podziałem \mathcal{A} .

Na przykład następujący podział zbioru $X = \{x \in \mathbb{N} : x \leq 10\}$ na bloki

$$\mathcal{A}' = \{\{0, 3\}, \{6, 9\}, \{1, 4, 7\}, \{10\}, \{2, 5, 8\}\} \quad (2.43)$$

jest rozdrobnieniem podziału (2.42).

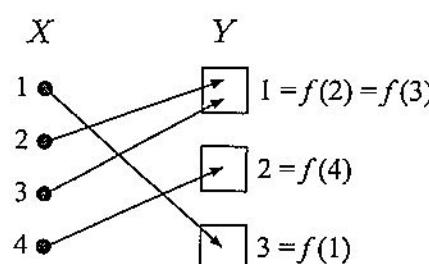
Łatwo się przekonać, że relacja rozdrobnienia jest zwrotna, przechodnia i antysymetryczna, a zatem jest relacją częściowego porządku w zbiorze podziałów danego zbioru na bloki.

2.6.2 Podziały zbiorów a zliczanie surjekcji

Rozważmy następujący prosty przykład:

Przykład 2.14 Mamy do dyspozycji m ponumerowanych procesorów i $n \geq m$ programów, z których każdy może być wykonany na dowolnym z tych procesorów. Chcemy przydzielić wszystkie programy do procesorów w taki sposób, by każdy procesor otrzymał co najmniej jeden program. (Zakładamy przy tym, że każdy program jest wykonywany w całości przez jeden procesor.) Należy policzyć, na ile sposobów można dokonać takiego przydziału.

Zadanie to przypomina problem rozważany w Przykładzie 2.13, ale z jedną istotną różnicą: tym razem interesują nas nie podziały zbioru programów na bloki, ale konkretne przyporządkowania programów procesorom. Każde takie przyporządkowanie może być opisane przez pewną funkcję z n -elementowego zbioru programów X w m -elementowy zbiór procesorów Y . Z warunku, że każdy procesor ma dostać do wykonania co najmniej jeden program, wynika, że funkcja ta musi być surjekcją.



Rysunek 2.17: Przydział wyznaczony przez surjekcję $f \in \text{Fun}(X, Y)$, gdzie $X = \{1, 2, 3, 4\}$, $Y = \{1, 2, 3\}$, $f(1) = 3$, $f(2) = 1$, $f(3) = 1$, $f(4) = 2$.

Na Rysunku 2.17 pokazany jest przykład przydziału czterech programów, oznaczanych cyframi 1, 2, 3, 4, do trzech procesorów, zadany przez surjekcję f . Wynika z niego, że program o numerze 1 powinien być przydzielony do wykonania procesorowi o numerze 3, programy o numerach 2 i 3 – procesorowi 1, a program o numerze 4 – procesorowi o numerze 2. Rozwiązaniem naszego problemu jest więc w tym konkretnym przypadku policzenie liczby wszystkich surjekcji w zbiorze $\text{Fun}(X, Y)$, gdzie $X = \{1, 2, 3, 4\}$ oraz $Y = \{1, 2, 3\}$. \square

2.6. PODZIAŁY ZBIORU

Niech X, Y będą dowolnymi zbiorami i niech $|X| = n$ oraz $|Y| = m$. Chcemy policzyć:

Ile jest wszystkich surjekcji w zbiorze $\text{Fun}(X, Y)$?

Liczبę wszystkich surjekcji w zbiorze $\text{Fun}(X, Y)$, gdzie $|X| = n$ oraz $|Y| = m$, będziemy oznaczać symbolem $s_{n,m}$.

Z podobieństwa Przykładów 2.13 i 2.14 można wnioskować, że istnieje ścisły związek między liczbą surjekcji $s_{n,m}$ a liczbą wszystkich możliwych podziałów zbioru n -elementowego na m bloków, tzn. liczbą Stirlinga drugiego rodzaju $\left\{ \begin{smallmatrix} n \\ m \end{smallmatrix} \right\}$. Tak istotnie jest. Zauważmy bowiem, że każdej surjekcji f ze zbioru $\text{Fun}(X, Y)$ można przyporządkować następujący podział $N(f)$ zbioru X na m bloków:

$$N(f) = \{f^{-1}(\{y\}) : y \in Y\}. \quad (2.44)$$

Przypomnijmy, że tak zdefiniowaną rodzinę zbiorów $N(f)$ nazywamy *jądrem* funkcji f (patrz str. 9).

Jeśli spojrzymy na graf funkcji f z Rysunku 2.17, to łatwo stwierdzić, że jądem tej funkcji jest podział \mathcal{A} zbioru $X = \{1, 2, 3, 4\}$ na $|Y| = 3$ bloki, gdzie $\mathcal{A} = \{\{1\}, \{2, 3\}, \{4\}\}$. Jądro funkcji f , definiującej pewien konkretny przydział programów do procesorów, określa więc, które programy zostaną przydzielone do tego samego procesora, ale nie wskazuje konkretnie tego procesora.

Zauważmy jednak, że jądra funkcji f oraz πf ze zbioru $\text{Fun}(X, Y)$ są identyczne dla dowolnej permutacji π zbioru Y , a zatem dokładnie $m! = |Y|!$ surjekcji ze zbioru $\text{Fun}(X, Y)$ ma to samo jądro $\mathcal{A} \in \Pi_m(X)$. Liczba wszystkich surjekcji w zbiorze $\text{Fun}(X, Y)$ jest więc $m!$ razy większa niż liczba wszystkich podziałów n -elementowego zbioru X na m bloków. Udowodniliśmy zatem następujące twierdzenie:

Twierdzenie 2.9 *Liczba $s_{n,m}$ surjekcji w zbiorze $\text{Fun}(X, Y)$, gdzie $|X| = n$, $|Y| = m$, spełnia zależność*

$$s_{n,m} = m! \cdot \left\{ \begin{smallmatrix} n \\ m \end{smallmatrix} \right\}. \quad (2.45)$$

W Rozdziale 3 poznamy technikę tak zwanych *funkcji tworzących*, która pozwoli na wyprowadzenie jeszcze innego wzoru, umożliwiającego obliczanie wartości $s_{n,m}$. Zanim jednak zajmiemy się funkcjami tworzącymi, przedstawimy krótko pewne zagadnienie, które przypomina nieco podziały zbioru. Chodzi mianowicie o tak zwany podział liczby naturalnej na składniki, który ma różnorodne zastosowania praktyczne.

2.7 Podziały liczby

Niech n i k będą dowolnymi liczbami naturalnymi.

Definicja 2.8 *Podziałem liczby n na k składników nazywamy ciąg liczb naturalnych (a_1, \dots, a_k) , spełniający następujące warunki:*

$$a_1 + \dots + a_k = n \quad \text{oraz} \quad a_1 \geq \dots \geq a_k > 0.$$

Liczبę wszystkich podziałów liczby $n \in \mathbb{N}$ na $k \in \mathbb{N}$ składników bę-dziemy oznaczać symbolem $P(n, k)$, a liczbę wszystkich podziałów liczby n – symbolem $P(n)$. Oczywiście, dla $n > 0$ mamy

$$P(n) = \sum_{k=1}^n P(n, k). \quad (2.46)$$

Przyjmiemy ponadto, że $P(0, 0) = P(0) = 1$.

Dla niewielkich liczb naturalnych można łatwo wypisać ich wszystkie możliwe podziały na składniki. Na przykład dla liczby 6, zbiór wszystkich jej podziałów składa się z następujących 11 ciągów:

- (6)
- (5, 1)
- (4, 2)
- (4, 1, 1)
- (3, 3)
- (3, 2, 1)
- (3, 1, 1, 1)
- (2, 2, 2)
- (2, 2, 1, 1)
- (2, 1, 1, 1, 1)
- (1, 1, 1, 1, 1, 1).

2.7. PODZIAŁY LICZBY

W zastosowaniach praktycznych interesujące są również podziały, na które nakładane są pewne dodatkowe warunki. Przykładem takiego wa- runku może być ograniczenie maksymalnej wartości każdego składnika podziału. W tym przypadku, dla danej liczby naturalnej n oraz $t \in \mathbb{N}$, liczbę wszystkich podziałów (a_1, \dots, a_k) liczby n na k składników, gdzie $k = 1, \dots, n$, dla których spełnione są nierówności

$$a_i \leq t, \quad i = 1, \dots, k,$$

będziemy oznaczać symbolem $P_t(n)$.

Powstają naturalne pytania o to, ile jest wszystkich podziałów liczby n na k składników, ile jest wszystkich podziałów liczby n , ilc jest wszyst- kich podziałów liczby n na składniki nie większe niż t dla dowolnego naturalnego t itp.

Mimo że istnieje bardzo wiele prac na temat podziałów liczb, to nat- dłu nie znamy zwartych formuł, pozwalających na wyznaczanie wartości $P(n)$, $P(n, k)$ i $P_t(n)$ dla dowolnych wartości parametrów n , k , t . Potra- llimy natomiast konstruować różne procedury rekurencyjne, umożliwiające policzenie tych wielkości. Opierają się one na prostych twierdzeniach, z których dwa udowodnimy poniżej.

Twierdzenie 2.10 *Dla $n, k \in \mathbb{N}$, gdzie $n \geq k > 0$, zachodzi zależność*

$$P(n, k) = P(n - 1, k - 1) + P(n - k, k). \quad (2.47)$$

Dowód. Rozbijmy zbiór wszystkich podziałów liczby n na k składni- ków na dwa rozłączne podzbiory: P_0 oraz P_1 , gdzie P_0 jest zbiorem tych podziałów, które nie zawierają żadnego składnika równego 1, natomiast P_1 jest zbiorem tych podziałów, które zawierają co najmniej jeden składnik równy 1. Przyporządkujmy teraz każdemu podziałowi (a_1, \dots, a_k) ze zbioru P_0 wzajemnie jednoznacznie wektor $(a_1 - 1, \dots, a_k - 1)$. Łatwo za-auważyc, że tak otrzymane wektory tworzą zbiór wszystkich podziałów liczby $n - k$ na k składników, a zatem ich liczba, a tym samym i moc zbioru P_0 , jest równa $P(n - k, k)$.

Podobnie, przyporządkujmy każdemu podziałowi (a_1, \dots, a_k) ze zbioru P_1 wzajemnie jednoznacznie wektor (a_1, \dots, a_{k-1}) . Otrzymamy w ten sposób zbiór wszystkich możliwych podziałów liczby $n - 1$ na $k - 1$ skład- ników. Oznacza to, że liczność zbioru P_1 jest równa $P(n - 1, k - 1)$. Sumując liczności zbiorów P_0 i P_1 uzyskujemy liczbę zbioru $P(n, k)$ zgodnie z zależnością (2.47). ■

| $P(n)$ | $P(n, k)$ | | | | | | | | | | | | | ... |
|--------|-----------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| | $k=0$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | ... |
| $n=0$ | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 2 | 2 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 3 | 3 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 4 | 5 | 0 | 1 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 5 | 7 | 0 | 1 | 2 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | ... |
| 6 | 11 | 0 | 1 | 3 | 3 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | ... |
| 7 | 15 | 0 | 1 | 3 | 4 | 3 | 2 | 1 | 1 | 0 | 0 | 0 | 0 | ... |
| 8 | 22 | 0 | 1 | 4 | 5 | 5 | 3 | 2 | 1 | 1 | 0 | 0 | 0 | ... |
| 9 | 30 | 0 | 1 | 4 | 7 | 6 | 5 | 3 | 2 | 1 | 1 | 0 | 0 | ... |
| 10 | 42 | 0 | 1 | 5 | 8 | 9 | 7 | 5 | 3 | 2 | 1 | 1 | 0 | 0 |
| 11 | 56 | 0 | 1 | 5 | 10 | 11 | 10 | 7 | 5 | 3 | 2 | 1 | 1 | 0 |
| 12 | 77 | 0 | 1 | 6 | 12 | 15 | 13 | 11 | 7 | 5 | 3 | 2 | 1 | 1 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | |

Rysunek 2.18: Liczności podziałów liczby naturalnej n na składniki.

Twierdzenie 2.10 pozwala na rekurencyjne obliczanie wartości $P(n, k)$ dla dowolnych liczb naturalnych $n \geq k > 0$, korzystając z faktu, że $P(0, k) = P(k, 0) = [k = 0]$. Mając dla danego n wszystkie wartości $P(n, k)$ dla $k \leq n$, możemy już łatwo wyznaczyć wartość $P(n)$ z zależności (2.46). Tabela zamieszczona na Rysunku 2.18 zawiera obliczone w ten sposób wartości $P(n, k)$ oraz $P(n)$ dla $n, k \leq 12$. Zerowe wartości elementów tablicy dla $k > n$ zostały wyróżnione.

Tabcę z Rysunku 2.18 można również wyznaczyć rekurencyjnie na podstawie następującego twierdzenia:

Twierdzenie 2.11 Dla $n, k \in \mathbb{N}$, gdzie $n \geq k$, zachodzi następująca zależność:

$$P(n, k) = \sum_{i=0}^k P(n - k, i). \quad (2.48)$$

Dowód. Rozbijmy zbiór podziałów liczby n na k składników na $k+1$ podzbiorów P^0, P^1, \dots, P^k , gdzie P^i , $i = 0, 1, \dots, k$, oznacza zbiór podziałów, w których dokładnie $k-i$ składników ma wartość równą 1.

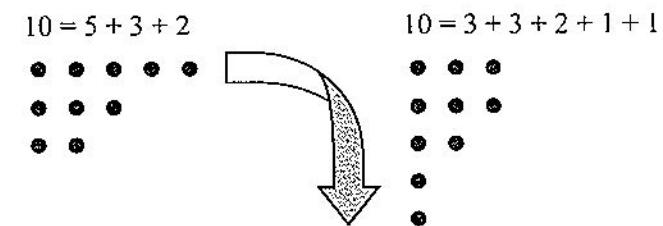
2.7. PODZIAŁY LICZBY

Każdemu podziałowi (a_1, \dots, a_k) ze zbioru P^i możemy teraz przyporządkować wzajemnie jednoznacznie wektor $(a_1 - 1, a_2 - 1, \dots, a_i - 1)$. Zauważmy, że zbiór tych wektorów jest zbiorem wszystkich podziałów liczby $n - (k - i) - i = n - k$ na i składników, a zatem liczność zbioru P^i jest równa $P(n - k, i)$. Sumując te liczności dla $i = 0, 1, \dots, k$, otrzymujemy wartość $P(n, k)$. ■

Do zagadnienia zliczania podziałów liczby na składniki wróćmy w następnym rozdziale przy omawianiu techniki funkcji tworzących. Tu natomiast przedstawimy jeszcze pewien wygodny schemat rysunkowy zapisywania podziałów liczb. Schemat ten nosi nazwę *diagramu Ferrersa*.

Rozważmy podział (a_1, \dots, a_k) liczby $n = a_1 + \dots + a_k$. Diagram Ferrersa, który odpowiada temu podziałowi, jest tablicą składającą się z dokładnic k wierszy, przy czym wiersz i -ty zawiera dokładnie a_i kropek (patrz Rysunek 2.19). Transpozycja tej tablicy, to znaczy zamiana wierszy na kolumny, definiuje tak zwany *podział sprzężony* liczby n .

Na Rysunku 2.19 przedstawione są diagramy Ferrersa dla pary podziałów sprzężonych: $(5, 3, 2)$ oraz $(3, 3, 2, 1, 1)$, liczby 10.

Rysunek 2.19: Diagramy Ferrersa dla podziałów sprzężonych $(5, 3, 2)$ oraz $(3, 3, 2, 1, 1)$ liczby 10.

Diagramy Ferrersa są nie tylko wygodnym sposobem zobrazowania podziałów liczb, ale pozwalają również na łatwe zaobserwowanie pewnych faktów z nimi związanych. Zestawiając podziały sprzężone liczby n , łatwo na przykład zauważyc, że każdemu podziałowi liczby n na k składników odpowiada dokładnie jeden podział sprzężony, którego największy składnik jest równy k . Prawdziwe jest więc następujące twierdzenie, w którym symbolem $P^k(n)$ oznaczamy liczbę zbioru wszystkich podziałów liczby n na dowolną liczbę składników, z których największy jest równy k .

Twierdzenie 2.12 Dla $n, k \in \mathbb{N}$, gdzie $k \leq n$,

$$P(n, k) = P^k(n). \quad (2.49)$$

Z twierdzenia powyższego można wysnuć prosty wniosek. Zauważmy mianowicie, że

$$P_k(n) = \sum_{i=1}^k P^i(n).$$

Korzystając z zależności (2.49) otrzymujemy:

Wniosek 2.5 Dla $n, k \in \mathbb{N}$, gdzie $n \geq k > 0$, zachodzi następująca równość:

$$P_k(n) = \sum_{i=1}^k P(n, i). \quad (2.50)$$

2.8 Zbiory częściowo uporządkowane

W rozdziale tym przedstawimy podstawowe fakty, dotyczące zbiorów częściowo uporządkowanych.

Przypomnijmy, że *zbiorem częściowo uporządkowanym* nazywamy parę uporządkowaną (X, \preceq) , gdzie X jest dowolnym zbiorem, a \preceq jest relacją częściowego porządku w tym zbiорze (patrz strona 8). Pierwszy element pary, to znaczy zbiór X , nazywamy *zbiorem podstawowym*, a relację \preceq – *relacją porządkującą* zbiór X .

Jeśli dla $x, y \in X$ mamy $x \preceq y$ lub $y \preceq x$, to elementy x, y , nazywamy *elementami porównywalnymi*. W przeciwnym przypadku x, y , nazywamy *elementami nieporównywalnymi*.

Jeśli każde dwa elementy x, y zbioru X są porównywalne, to parę uporządkowaną (X, \preceq) nazywamy *zbiorem liniowo uporządkowanym*.

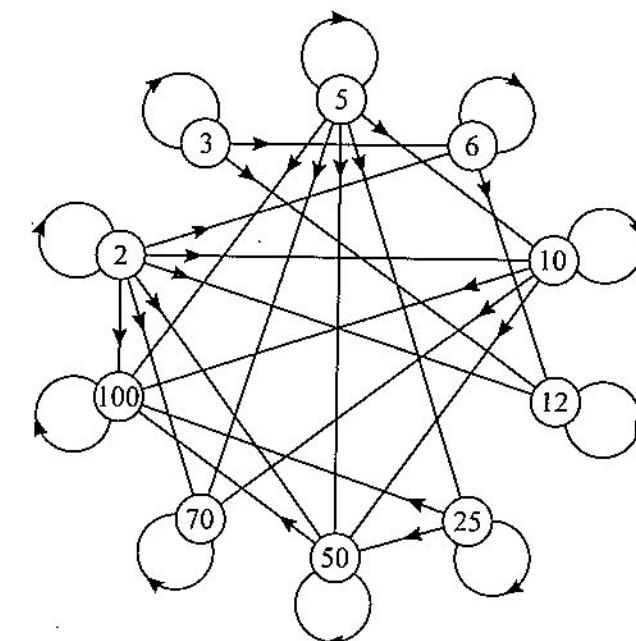
Rozważmy zbiór częściowo uporządkowany (X, \preceq) i niech $Y \subseteq X$. Podzbiorem zbiuru częściowo uporządkowanego (X, \preceq) nazywamy zbiór częściowo uporządkowany (Y, \preceq_Y) , gdzie symbol \preceq_Y oznacza relację \preceq zawężoną do zbiuru Y , to znaczy \preceq_Y jest zbiorem tych par uporządkowanych (u, v) , należących do relacji \preceq , dla których $u, v \in Y$.

2.8. ZBIORY CZEŚCIOWO UPORZĄDKOWANE

Przykład 2.15 Rozważmy następujący zbiór liczb naturalnych:

$$X = \{2, 3, 5, 6, 10, 12, 25, 50, 70, 100\}.$$

Oznaczmy symbolem $|$ relację podzielności w zbiорze X , to znaczy dla $a, b \in X$ mamy $a|b \Leftrightarrow b \text{ mod } a = 0$. Łatwo sprawdzić, że relacja $|$ w zbiorze X jest relacją częściowego porządku, bowiem jest zwrotna, przechodnia i antysymetryczna. A zatem para $(X, |)$ jest zbiorem częściowo uporządkowanym. Rysunek 2.20 przedstawia rysunek grafu relacji $|$ w zbiorze X .



Rysunek 2.20: Rysunek grafu relacji podzielności $|$ w zbiorze X , gdzie $X = \{2, 3, 5, 6, 10, 12, 25, 50, 70, 100\}$.

Zauważmy, że $(X, |)$ nie jest zbiorem liniowo uporządkowanym, bowiem na przykład żadna z dwu par: ani $(6, 10)$, ani $(10, 6)$, nie należy do relacji $|$ w zbiorze X . Jeśli jednak wybierzemy odpowiedni podzbiór zbiuru X , na przykład podzbiór $Y = \{2, 10, 50\}$, to otrzymamy zbiór liniowo uporządkowany $(Y, |_Y)$.

Niech (X, \preceq) będzie zbiorem częściowo uporządkowanym. Wprowadźmy następujące oznaczenie:

$$x \prec y \Leftrightarrow x \preceq y \wedge x \neq y.$$

Element $t \in X$ nazywamy *bezpośrednim następcą* elementu $s \in X$, jeśli $s \prec t$ i nie istnieje taki element $u \in X$, że $s \prec u$ oraz $u \prec t$. Element s nazywamy wówczas *bezpośrednim poprzednikiem* elementu t .

Na przykład w zbiorze częściowo uporządkowanym rozważanym w Przykładzie 2.15, element 10 jest bezpośrednim następcą elementu 2, a tym samym 2 jest bezpośredniem poprzednikiem 10. Natomiast element 12 nie jest bezpośredniem następcą elementu 2, bowiem istnieje w zbiorze X element 6, różny od elementów 2 oraz 12, dla którego zachodzą zależności $2|6$ oraz $6|12$.

Zbiór częściowo uporządkowany (X, \preceq) można zobrazować podając rysunek grafu relacji \preceq , tak jak to zrobiono w Przykładzie 2.15. Zauważmy jednak, że taki sposób przedstawienia zbioru częściowo uporządkowanego jest w istocie nadmiarowy, bowiem z faktu, że relacja \preceq jest relacją częściowego porządku, wynika, że dla każdego wierzchołka jej grafu istnieje pętla. Jest to konsekwencja zwrotności relacji \preceq . Ponadto z przechodniości tej relacji wynika, że jeśli istnieją luki (u, v) oraz (v, w) , to musi również istnieć luk (u, w) .

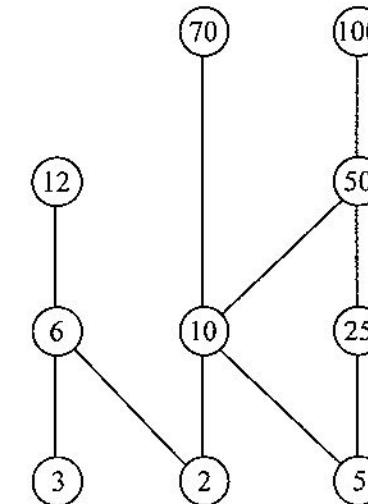
Wygodnym i bardziej oszczędnym sposobem przedstawienia zbioru częściowo uporządkowanego (X, \preceq) jest tak zwany *diagram Hassego* tego zbioru.

Diagram ten jest rysunkiem, na którym elementy zbioru X są reprezentowane w postaci umownych symboli, zwykle kółek z odpowiednimi etykietami, natomiast linie między nimi występują wtedy i tylko wtedy, gdy dla dancj pary elementów jeden z nich jest bezpośredniem następcą drugiego. Dodatkowo, na diagramie tym bezpośredni następnik występuje zawsze wyżej niż bezpośredni poprzednik.

Na Rysunku 2.21 pokazany jest diagram Hassego zbioru częściowo uporządkowanego z Przykładu 2.15.

Diagram Hassego zbioru częściowo uporządkowanego ułatwia prześledzenie poniższych definicji.

Definicja 2.9 Element $x_o \in X$ nazywamy elementem maksymalnym zbioru częściowo uporządkowanego (X, \preceq) , jeśli w zbiorze X nie istnieje element $x \neq x_o$, dla którego $x_o \preceq x$.



Rysunek 2.21: Diagram Hassego zbioru częściowo uporządkowanego $(X, |)$ z Przykładu 2.15.

Definicja 2.10 Element $x_o \in X$ nazywamy elementem minimalnym zbioru częściowo uporządkowanego (X, \preceq) , jeśli w zbiorze X nie istnieje element $x \neq x_o$, dla którego $x \preceq x_o$.

Definicja 2.11 Element $x_o \in X$ nazywamy elementem największym zbioru częściowo uporządkowanego (X, \preceq) , jeśli dla każdego $x \in X$ zachodzi zależność $x \preceq x_o$.

Definicja 2.12 Element $x_o \in X$ nazywamy elementem najmniejszym zbioru częściowo uporządkowanego (X, \preceq) , jeśli dla każdego $x \in X$ zachodzi zależność $x_o \preceq x$.

Łatwo zauważać, że w zbiorze $(X, |)$ rozważanym w Przykładzie 2.15, elementy elementy 2, 3, 5 są elementami minimalnymi. Występują one na samym dole diagramu Hassego tego zbioru.

Elementy 12, 70, 100 są elementami maksymalnymi i są umiejscowione na górze diagramu Hassego.

Rozważany zbiór $(X, |)$ nie zawiera ani elementu najmniejszego, ani elementu największego.

Gdybyśmy natomiast wybrali odpowiedni podzbiór zbioru X , na przykład podzbiór $X' = \{5, 10, 25, 50, 100\}$, to wówczas zbiór uporządkowany $(X', |_{X'})$ zawierałby zarówno elementy najmniejszy, jak i największy, w tym przypadku – odpowiednio – elementy 5 i 100.

Łatwo pokazać następujące fakty (dowody poniższych twierdzeń można znaleźć na przykład w [24]):

Twierdzenie 2.13 W zbiorze częściowo uporządkowanym istnieje co najwyżej jeden element największy i co najwyżej jeden element najmniejszy. Przy tym element największy jest elementem maksymalnym, natomiast element najmniejszy jest elementem minimalnym.

Twierdzenie 2.14 Dla każdego elementu x_o zbioru liniowo uporządkowanego (X, \preceq) następujące fakty są równoważne:

- x_o jest elementem największym;
- $x \preceq x_o$ dla każdego $x \in X \setminus \{x_o\}$;
- x_o jest elementem maksymalnym.

Twierdzenie 2.15 Dla każdego elementu x_o zbiuru liniowo uporządkowanego (X, \preceq) następujące fakty są równoważne:

- x_o jest elementem najmniejszym;
- $x_o \preceq x$ dla każdego $x \in X \setminus \{x_o\}$;
- x_o jest elementem minimalnym.

Twierdzenie 2.16 Jeśli (X, \preceq) jest zbiorem liniowo uporządkowanym oraz X jest zbiorem skończonym i niepustym, to w (X, \preceq) istnieją elementy największy i najmniejszy.

Rozważmy teraz zbiór częściowo uporządkowany (X, \preceq) i niech $A \subseteq X$.

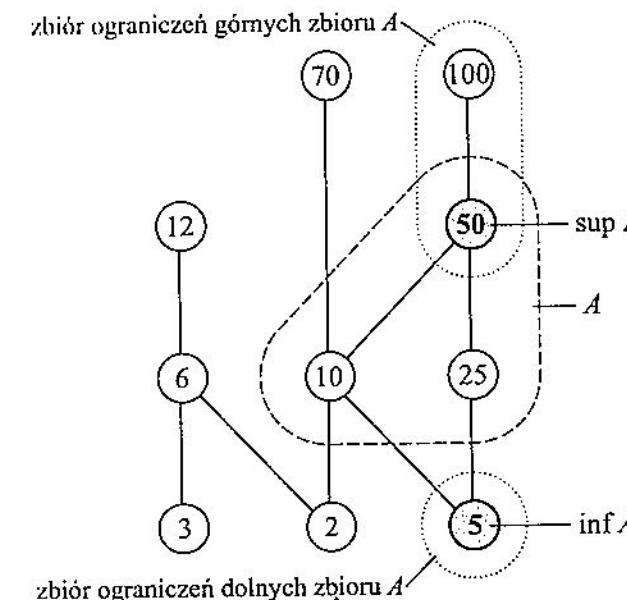
Definicja 2.13 Element $x_o \in X$ nazywamy ograniczeniem dolnym zbiuru A w zbiurze X , jeśli dla każdego $x \in A$ zachodzi zależność $x_o \preceq x$.

Definicja 2.14 Element $x_o \in X$ nazywamy ograniczeniem górnym zbiuru A w zbiurze X , jeśli dla każdego $x \in A$ zachodzi zależność $x \preceq x_o$.

Jeśli zbiór ograniczeń górnego zbiuru A ma element najmniejszy, to nazywamy go kresem górnym zbiuru A i oznaczamy symbolem $\sup A$.

Jeśli zbiór ograniczeń dolnych zbiuru A ma element największy, to nazywamy go kresem dolnym zbiuru A i oznaczamy symbolem $\inf A$.

Jeśli $x^o = \sup A$ oraz $x^o \in A$, to piszemy $x^o = \max A$. Podobnie, jeśli $x^o = \inf A$ oraz $x^o \in A$, to stosujemy zapis $x^o = \min A$.



Rysunek 2.22: Diagram Hassego zbiuru częściowo uporządkowanego $(X, |)$ z zaznaczonymi (elementy zacienione) kresami dolnym i górnym podzbioru $A = \{10, 25, 50\}$.

Przykład 2.16 Rozważmy ponownie zbiór częściowo uporządkowany X z Przykładu 2.15 i wybierzmy jako jego podzbiór zbiór $A = \{10, 25, 50\}$. Wówczas zbiorem ograniczeń dolnych zbiuru A jest zbiór jednoelementowy $\{5\}$. Zbiorem ograniczeń górnego jest $\{50, 100\}$.

W zbiurze ograniczeń dolnych istnieje element największy; jest nim element 5. A zatem kresem dolnym zbiuru A jest 5. Również w zbiurze ograniczeń górnego istnieje element najmniejszy. Jest nim element 50.

Mamy więc $\inf A = 5$ oraz $\sup A = 50$. Zauważmy, że w rozważanym przykładzie kres górnny zbioru A należy do tego zbioru, a zatem $50 = \max A$, natomiast kres dolny nie jest elementem A .

Rysunek 2.22 przedstawia diagram Hassego zbioru X z zaznaczonymi zbiorami oszacowań dolnych i górnych oraz kresami podzbioru A .

□

W powyższym przykładzie dla wybranego podzbioru A zbioru X istniały zarówno kres górnny, jak i kres dolny zbioru A . Tak jednak zawsze być nie musi i łatwo można wskazać taki podzbiór zbioru X , dla którego kresy te nie istnieją; wystarczy na przykład wybrać taki podzbiór, dla którego zbiór ograniczeń górnych lub dolnych jest pusty.

W rozmaitych zastosowaniach bardzo istotną rolę pełnią zbiory częściowo uporządkowane, w których możemy zagwarantować istnienie kresów górnych i dolnych dla dowolnych podzbiorów ich elementów. Zbiory częściowo uporządkowane o takich właściwościach noszą nazwę *krat*.

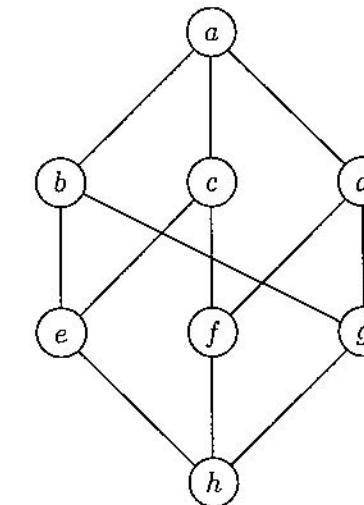
Definicja 2.15 *Zbiór częściowo uporządkowany (X, \preceq) nazywamy kratą, jeśli dla dowolnej pary elementów $x, y \in X$ istnieją kres górnny $\sup\{x, y\}$ oraz kres dolny $\inf\{x, y\}$.*

Można pokazać, że jeśli zbiór częściowo uporządkowany (X, \preceq) spełnia warunki z powyższej definicji, to dla dowolnego skończonego podzbioru $A \subseteq X$ istnieją zarówno $\sup A$, jak i $\inf A$.

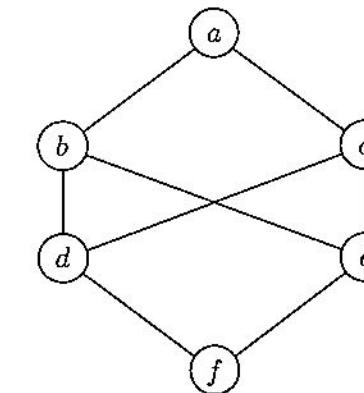
Rysunek 2.23 przedstawia przykład diagramu Hassego zbioru częściowo uporządkowanego, który jest kratą. Łatwo sprawdzić, że – istotnie – dla każdej pary elementów tego zbioru możemy wskazać kres górnny i kres dolny. Natomiast zbiór częściowo uporządkowany, którego diagram Hassego pokazano na Rysunku 2.24, nie jest kratą. Zauważmy bowiem, że na przykład dla podzbioru $\{d, e\}$ tego zbioru mamy wprawdzie niepusty zbiór ograniczeń górnych, którym w tym przypadku jest zbiór $\{a, b, c\}$, ale nie ma on elementu najmniejszego, a zatem kres górnny dla podzbioru $\{d, e\}$ nie istnieje.

Często używanym przykładem kraty jest zbiór częściowo uporządkowany $(\mathcal{P}(X), \subseteq)$, gdzie $\mathcal{P}(X)$ jest zbiorem potęgowym dowolnego zbioru skończonego X , to znaczy rodziną wszystkich podzbiorów zbioru X , natomiast \subseteq jest relacją zawierania zbiorów w tej rodzinie. W tym przypadku dla dowolnych dwóch elementów $S', S'' \in \mathcal{P}(X)$ mamy:

$$\sup\{S', S''\} = S' \cup S'', \quad \inf\{S', S''\} = S' \cap S''.$$



Rysunek 2.23: Diagram Hassego przykładowej kraty.



Rysunek 2.24: Przykład diagramu Hassego zbioru częściowo uporządkowanego, który nie jest kratą.

Wynika stąd, że kresem górnym dowolnej skończonej rodziny podzbiorów $\mathcal{P}(X)$ jest suma mnogościowa tych podzbiorów, natomiast kresem dolnym – ich część wspólna.

Innym ważnym przykładem kraty jest zbiór częściowo uporządkowany $(\mathcal{N}, |)$, gdzie $\mathcal{N} = \mathbb{N} \setminus \{0\}$ jest zbiorem dodatnich liczb naturalnych, a $|$ oznacza używaną już wcześniej (str. 8) relację podzielności w zbiorze \mathcal{N} . W przypadku tego zbioru mamy dla dowolnych elementów $x, y \in \mathcal{N}$:

$$\sup\{x, y\} = \text{lcm}(x, y), \quad \inf\{x, y\} = \gcd(x, y).$$

Kresem górnym skończonego podzbioru liczb ze zbioru \mathcal{N} jest więc ich najmniejsza wspólna wielokrotność, natomiast kresem dolnym – ich największy wspólny dzielnik.

2.8.1 Łańcuchy i antylańcuchy w zbiorach częściowo uporządkowanych

W paragrafie tym sformułujemy bardzo ważne twierdzenia, dotyczące zbiorów częściowo uporządkowanych. Wiele pozornie odległych faktów okazuje się być szczególnymi przypadkami tego twierdzenia dla odpowiednio dobranych zbiorów częściowo uporządkowanych. Do jego sformułowania będą nam potrzebne definicje dwóch szczególnych typów podzbiorów zbioru częściowo uporządkowanego: łańcuchów i antylańcuchów.

Definicja 2.16 *Łańcuchem w zbiorze częściowo uporządkowanym (X, \preceq) nazywamy taki podzbiór $L \subseteq X$, w którym dla dowolnych dwóch elementów $x, y \in L$ mamy $x \preceq y$ lub $y \preceq x$.*

Definicja 2.17 *Antylańcuchem w zbiorze częściowo uporządkowanym (X, \preceq) nazywamy taki podzbiór $A \subseteq X$, w którym dla dowolnych dwóch elementów $x, y \in A$ mamy $x \preceq y \Leftrightarrow x = y$.*

Innymi słowy, w łańcuchu każde dwa elementy są porównywalne, natomiast w antylańcuchu żadne dwa różne elementy nie są porównywalne.

Dla dowolnego zbioru X i rodzinę $\{Y_1, \dots, Y_k\}$ jego podzbiorów mówimy, że zbiory Y_1, \dots, Y_k , pokrywają zbiór X , jeśli $X = Y_1 \cup \dots \cup Y_k$. Taką rodzinę podzbiorów nazywamy *pokryciem* zbioru X .

Poniższe twierdzenie formułuje związek między największą liczbą antylańcucha i minimalną liczbą łańcuchów pokrywających zbiór częściowo uporządkowany.

2.8. ZBIORY CZĘŚCIOWO UPORZĄDKOWANE

Twierdzenie 2.17 (Dilworth, 1950)¹⁸ *W dowolnym skończonym zbiорze częściowo uporządkowanym (X, \preceq) maksymalna liczność antylańcucha jest równa minimalnej liczbie łańcuchów pokrywających zbiór X .*

Dowód. Zastosujemy indukcję względem liczności zbioru X . Dla $|X| = 1$ twierdzenie jest oczywiście prawdziwe. Założymy więc, że twierdzenie zachodzi, jeśli $|X| < k$ dla pewnego $k \geq 2$. Pokażemy, że z tego wynika, iż jest prawdziwe dla $|X| = k$.

Rozważmy dowolny zbiór częściowo uporządkowany (X, \preceq) , w którym $|X| = k$. Niech n będzie maksymalną liczbą antylańcucha w tym zbiorze. Jeśli $n = k$, to oznacza, że X jest antylańcuchem w (X, \preceq) oraz że $|X| = k = n$, a zatem twierdzenie jest w sposób oczywisty prawdziwe.

Załóżmy więc, że $n \neq k$ i wybierzmy w (X, \preceq) parę elementów porównywalnych: element maksymalny u oraz element minimalny v , a następnie rozważmy zbiór częściowo uporządkowany (Y, \preceq) , gdzie $Y = X \setminus \{u, v\}$.

Jesli liczność maksymalna antylańcucha w (Y, \preceq) jest mniejsza niż n , to – z założenia indukcyjnego – istnieje zbiór co najwyżej $n-1$ łańcuchów, które pokrywają zbiór Y . łańcuchy te wraz z łańcuchem $\{v, u\}$ stanowią pokrycie zbioru X , co oznacza, że twierdzenie jest prawdziwe dla (X, \preceq) .

Przyjmijmy więc, że maksymalna liczność antylańcucha w (Y, \preceq) jest równa n . Zauważmy, że implikuje to zależność $v \prec u$, bowiem gdyby $u = v = w$, to w (X, \preceq) istniałby antylańcuch o długości $n+1$, zawierający element w .

Niech $A = \{a_1, \dots, a_n\}$ będzie dowolnym antylańcuchem o liczności n w (Y, \preceq) . Zdefiniujmy dwa podzbiory zbioru X :

$$U = \{x \in X : a \preceq x \text{ dla pewnego } a \in A\},$$

$$V = \{x \in X : x \preceq a \text{ dla pewnego } a \in A\}.$$

Skoro $v \prec u$, to $u \in U \setminus V$ oraz $v \in V \setminus U$. Zbiory U i V mają więc liczbę mniejszą niż k , a zatem z założenia indukcyjnego wynika, że istnieją rodziny łańcuchów $\{L'_1, \dots, L'_n\}$ oraz $\{L''_1, \dots, L''_n\}$, pokrywające te zbiory. Zauważmy przy tym, że możemy ponumerować łańcuchy w tych rodzinach w taki sposób, by $a_i \in L'_i \cap L''_i$ dla $i = 1, \dots, n$. Ale wówczas

$$X = L'_1 \cup \dots \cup L'_n \cup L''_1 \cup \dots \cup L''_n,$$

gdzie $L_i = L'_i \cup L''_i$ dla $i = 1, \dots, n$. Uzyskaliśmy zatem pokrycie zbioru X co najwyżej n łańcuchami L_1, \dots, L_n , co dowodzi twierdzenia. ■

¹⁸Robert Palmer Dilworth – matematyk amerykański (1914-1993).

Okazuje się, że w sformułowaniu Twierdzenia 2.17 można zamiast słowa łańcuch i antyłańcuch i otrzymuje się również prawdziwe zdanie. Zadaje bowiem następujące twierdzenie, nazywane czasem dualnym twierdzeniem Dilwortha:

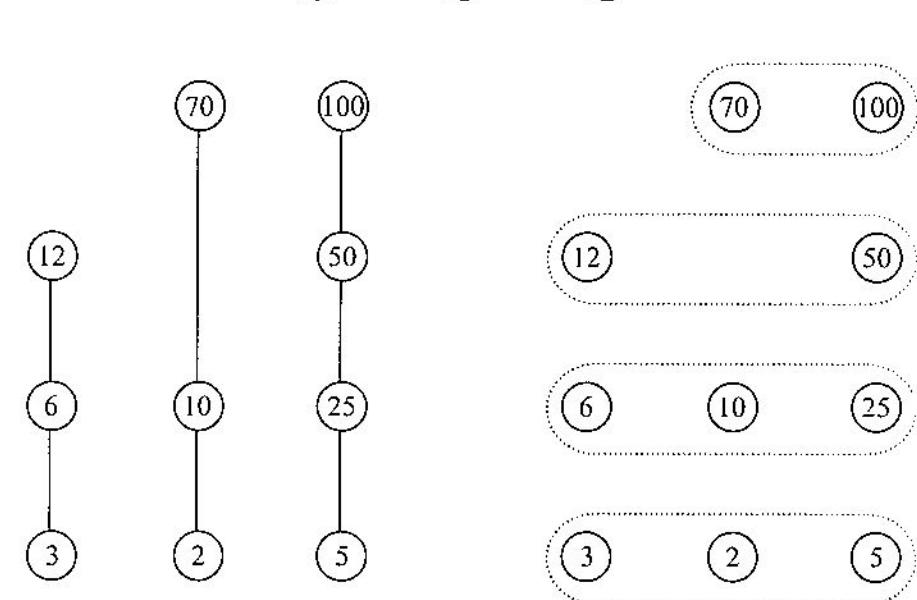
Twierdzenie 2.18 *W dowolnym skończonym zbiorze częściowo uporządkowanym (X, \preceq) maksymalna liczność łańcucha jest równa minimalnej liczbie antyłańcuchów pokrywających zbiór X .*

Dowód. Niech n oznacza maksymalną liczność łańcucha. Skonstruujemy rodzinę $\{A_1, \dots, A_n\}$ antyłańcuchów w (X, \preceq) , stanowiącą pokrycie zbioru X . Wystarczy w tym celu wybrać jako antyłańcuch A_1 zbiór wszystkich elementów maksymalnych zbioru X , a następnie dla $i = 1, \dots, n - 1$, przyjąć, że A_{i+1} jest zbiorem elementów maksymalnych w zbiorze $X \setminus \{A_1 \cup \dots \cup A_{i-1}\}$. ■

Przykład 2.17 Powróćmy raz jeszcze do zbioru częściowo uporządkowanego $(X, |)$ z Przykładu 2.15, gdzie $X = \{2, 3, 5, 6, 10, 12, 25, 50, 70, 100\}$.

Na Rysunku 2.25 pokazany jest ponownie diagram Hassego tego zbioru wraz z diagramami Hassego trzech łańcuchów $\{3, 6, 12\}$, $\{2, 10, 70\}$, $\{5, 25, 50, 100\}$, które pokrywają zbiór X . Z twierdzenia Dilwortha wynika, że jeśli istnieją trzy łańcuchy, które pokrywają X , to maksymalna długość antyłańcucha nie przekracza 3. W istocie jest to największa długość antyłańcucha w X . Przykładami antyłańcuchów o tej długości są $\{2, 3, 5\}$, $\{6, 10, 25\}$, $\{12, 25, 70\}$.

Najdłuższy z przedstawionych na Rysunku 2.25 łańcuchów ma cztery elementy. Z dualnego twierdzenia Dilwortha wynika więc, że potrzeba co najmniej czterech antyłańcuchów dla pokrycia zbioru X . Co więcej, jeśli znajdziemy dowolny czteroelementowy zbiór antyłańcuchów pokrywających X , to będziemy mieli pewność, że łańcuch $\{5, 25, 50, 100\}$ jest najdłuższym łańcuchem w X . Istotnie tak jest; przykładem czterech antyłańcuchów pokrywających X są następujące zbiory: $A_1 = \{2, 3, 5\}$, $A_2 = \{6, 10, 25\}$, $A_3 = \{12, 50\}$ oraz $A_4 = \{70, 100\}$. □



Rysunek 2.25: Diagramy Hassego zbioru częściowo uporządkowanego $(X, |)$ oraz łańcuchów i antyłańcuchów pokrywających X .

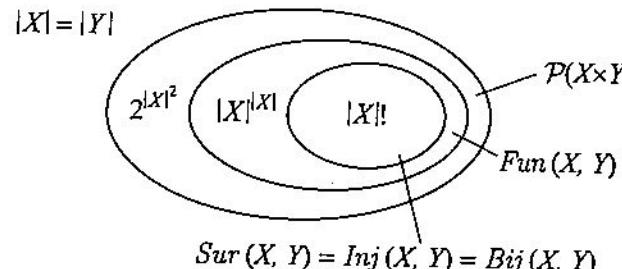
2.9 Podsumowanie

Dotychczasowe rozważania dotyczyły podstawowych obiektów spotykanych w kombinatoryce. Dowodzone fakty z zakresu zliczania były stosunkowo proste i nie było konieczne stosowanie żadnych specjalnych metod dla ich udowodnienia. Następny rozdział zostanie poświęcony wybranym technikom, które znacznie ułatwiają rozwiązywanie różnorodnych zadań kombinatorycznych.

Zanim jednak przejdziemy do prezentacji poszczególnych technik, podsumujemy na trzech poniższych rysunkach podstawowe fakty dotyczące zliczania funkcji, które udało się uzyskać dotychczasowymi metodami.

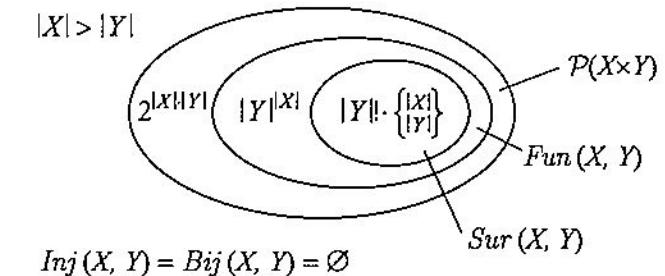
Wszystkie trzy rysunki obrazują liczności zbiorów poszczególnych typów funkcji: injekcji, surjekcji oraz bijekcji w zbiorze wszystkich funkcji, które można zdefiniować w iloczynie kartezjańskim zbiorów X oraz Y .

Rysunek 2.26 podaje moce zbiorów $\mathcal{P}(X \times Y)$, $\text{Fun}(X, Y)$, $\text{Inj}(X, Y)$, $\text{Sur}(X, Y)$ oraz $\text{Bij}(X, Y)$ dla przypadku, gdy $|X| = |Y|$. Rysunki 2.27 i 2.28 obrazują związki między tymi wielkościami odpowiednio dla przypadków, gdy $|X| > |Y|$ albo $|X| < |Y|$.

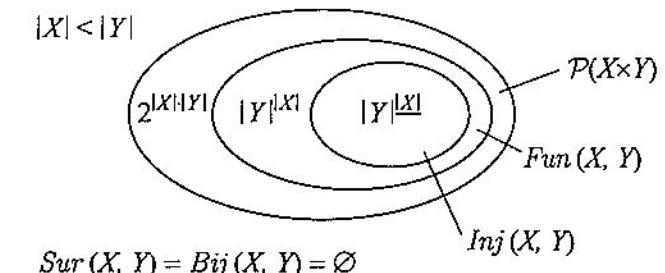


Rysunek 2.26: Związki między zbiorami $\mathcal{P}(X \times Y)$, $\text{Fun}(X, Y)$, $\text{Inj}(X, Y)$, $\text{Sur}(X, Y)$, $\text{Bij}(X, Y)$ oraz ich licznosciami dla $|X| = |Y|$.

2.9. PODSUMOWANIE



Rysunek 2.27: Związki między zbiorami $\mathcal{P}(X \times Y)$, $\text{Fun}(X, Y)$, $\text{Inj}(X, Y)$, $\text{Sur}(X, Y)$, $\text{Bij}(X, Y)$ oraz ich licznosciami dla $|X| > |Y|$.



Rysunek 2.28: Związki między zbiorami $\mathcal{P}(X \times Y)$, $\text{Fun}(X, Y)$, $\text{Inj}(X, Y)$, $\text{Sur}(X, Y)$, $\text{Bij}(X, Y)$ oraz ich licznosciami dla $|X| < |Y|$.

Rozdział 3

Metody i techniki

W tym rozdziale omówimy trzy najważniejsze techniki stosowane w kombinatoryce. Szczególną uwagę poświęcimy użyciu tak zwanych funkcji tworzących. Przedstawimy też dwie grupy twierdzeń, tradycyjnie określanych jako zasady włączania-wyłączania oraz metody szuflauskowe. Poszczególne techniki będą obszernie ilustrowane różnorodnymi zagadnieniami zliczania.

3.1 Funkcje tworzące

Rozdział ten jest poświęcony jednej z najważniejszych technik, z których korzysta się w kombinatoryce. Pozwala ona przede wszystkim na badanie ciągów i rozwiązywanie bardzo licznych zadań praktycznych, wymagających manipulowania ciągami.

Dotychczas mieliśmy do czynienia wyłącznie z ciągami skończonymi. Przypomnijmy (patrz strona 10.), że k -elementowym ciągiem o wyrazach ze zbioru Y nazywamy funkcję $f : X \rightarrow Y$, której dziedziną jest k -elementowy zbiór liczb naturalnych. Zwykle przyjmujemy, że $X = \{0, 1, \dots, k-1\}$. Wówczas ciąg k -elementowy oznaczamy symbolem $(a_0, a_1, \dots, a_{k-1})$ lub $(a_i)_{i=0}^{k-1}$.

Podejmie, ciągiem (nieskończonym) o wyrazach ze zbioru Y nazywamy dowolną funkcję $g : \mathbb{N} \rightarrow Y$. Funkcję tę oznaczamy zazwyczaj jednym z następujących symboli: (a_i) , $(a_0, a_1, \dots, a_i, \dots)$ lub $(a_i)_{i=0}^{\infty}$.

Zwykle, jeśli nie będzie to prowadziło do niejednoznaczności, będziemy operowali prostszymi oznaczeniami ciągów, to znaczy będąemy używali symboli $(a_0, a_1, \dots, a_{k-1})$ oraz (a_i) odpowiednio na oznaczenie ciągu

skończonego i nieskończonego. W niektórych sytuacjach korzystne jednakże okazuje się użycie zapisów z jawnie podanymi zakresami indeksów. Jeśli na przykład chcemy zapisać k -elementowy ciąg, którego każdy wyraz jest równy 1 i $k = 100$, to wygodnie jest go zapisać w postaci $(1)_{i=0}^{99}$.

Często okazuje się, że wygodniej jest operować ciągami nieskończonymi, mimo że w istocie mamy w konkretnym przypadku do czynienia z ciągami skończonymi o pewnej długości k . Możemy bowiem wówczas przyjąć na przykład, że wszystkie wyrazy ciągu dla $i > k$ są równe zeru. W dalszej części tego rozdziału – jeśli nie będzie to prowadziło do nieporozumień – będziemy zwykle zastępować ciąg skończony $(a_0, a_1, \dots, a_{k-1})$ ciągiem nieskończonym $(a_0, a_1, \dots, a_{k-1}, 0, \dots, 0, \dots)$. Powodem, dla którego decydujemy się na taką transformację jest to, że często wykonywanie pewnych operacji na ciągach nieskończonych jest łatwiejsze, a ponadto dla ciągu nieskończonego zazwyczaj łatwiej jest znaleźć „bardziej zwartą” postać jego zapisu. Jedną z takich zwartych postaci jest właśnie *funkcja tworząca ciągu*.

Definicja 3.1 Funkcją tworzącą ciągu (a_i) nazywamy szereg potęgowy o postaci

$$A(z) = \sum_{i=0}^{\infty} a_i z^i, \quad (3.1)$$

gdzie z jest zmienną zespoloną.

Zauważmy, że funkcje tworzące ciągów $(a_0, a_1, \dots, a_{k-1})$ oraz jego nieskończonego odpowiednika $(a_0, a_1, \dots, a_{k-1}, 0, \dots, 0, \dots)$ są identyczne.

W dalszym ciągu będziemy patrzyć na szereg $A(z)$ na dwa sposoby. Raz będziemy traktować $A(z)$ jako funkcję zmiennej z , innym razem używać będziemy funkcji tworzącej wyłącznie jako pewnego zapisu (*nazywanego szeregiem formalnym*). W tym ostatnim przypadku interesować nas będą jedynie możliwości manipulacji takim zapisem, a całkiem nieistotny będzie na przykład problem zbieżności szeregu (3.1).

Przykład 3.1 Rozważmy następujący ciąg liczb naturalnych:

$$(1, 8, 28, 56, 70, 56, 28, 8, 1, 0, \dots, 0, \dots). \quad (3.2)$$

Porównując ten ciąg z Rysunkiem 2.13 łatwo zauważyc, że elementy ciągu są kolejnymi elementami wiersza tablicy współczynników dwumianowych

3.1. FUNKCJE TWORZĄCE

dla $n = 8$. W tym przypadku wypisanie funkcji tworzącej ciągu (3.2) jest bardzo proste. Ze wzoru dwumianowego mamy bowiem:

$$(1+z)^8 = 1 + 8z^1 + 28z^2 + 56z^3 + 70z^4 + 56z^5 + 28z^6 + 8z^7 + z^8 + \sum_{i>8}^{\infty} \binom{8}{i} z^i.$$

Zauważmy, że ostatni składnik w powyższym wyrażeniu jest równy zeru. Prawa strona tego wyrażenia jest właśnie szeregiem (3.1), a zatem funkcją tworzącą ciągu (3.2) jest $(1+z)^8$. \square

Już powyższy bardzo prosty przykład pokazuje, że funkcja tworząca może być wygodnym i zwartym zapisem ciągu.

Znajomość funkcji tworzącej ciągu pozwala też na łatwe odtworzenie dowolnego jego elementu. Założymy bowiem, że szereg (3.1) jest zbieżny w pewnym otoczeniu zera. Wówczas suma $A(z)$ tego szeregu jest funkcją analityczną w tym otoczeniu (patrz na przykład [15]) oraz

$$a_i = \frac{A^{(i)}(0)}{i!}, \quad i = 0, 1, \dots, \quad (3.3)$$

gdzie $A^{(i)}(0)$ jest wartością i -tej pochodnej funkcji $A(z)$ w punkcie $z = 0$. Elementy ciągu (a_i) są więc po prostu kolejnymi współczynnikami w szeregu Maclaurina funkcji $A(z)$.

Dla wielu ciągów łatwo jest policzyć ich funkcje tworzące bezpośrednio z definicji (3.1). Poniższe przykłady ilustrują kilka takich prostych sytuacji.

Przykład 3.2 Rozważmy ciąg (a_i) , gdzie $a_i = [i = n]$ dla pewnego ustalonego $n \in \mathbb{N}$. Zatem jest to ciąg, w którym $a_n = 1$, a wszystkie pozostałe elementy są równe zeru. Należy pamiętać, że numerację elementów ciągu zaczynamy od zera, a zatem mamy tu do czynienia z następującym ciągiem:

$$(\underbrace{0, \dots, 0}_{n \text{ elementów}}, 1, 0, \dots, 0, \dots).$$

Funkcją tworzącą tego ciągu jest więc z^n , bowiem

$$\sum_{i=0}^{\infty} [i = n] z^i = z^n.$$

Zatem na przykład funkcją tworzącą ciągu $(0, 0, 0, 0, 0, 1, 0, \dots, 0, \dots)$ jest z^5 .

Łatwo jest uzyskać funkcję tworzącą ciągu złożonego z kolejnych potęg dowolnej ustalonej liczby zespolonej $c \in \mathbb{C}$, to znaczy ciągu

$$(c^0, c^1, c^2, c^3, \dots).$$

Z definicji (3.1) mamy bowiem $\sum_{i=0}^{\infty} c^i z^i = (1 - cz)^{-1}$, a zatem funkcja tworzącą powyższego ciągu jest $(1 - cz)^{-1}$. Jeśli na przykład $c = -1$, to mamy do czynienia z ciągiem $(1, -1, 1, -1, \dots)$ i jego funkcją tworzącą jest $(1 + z)^{-1}$. \square

Przykład 3.3 W wielu zastosowaniach przydatna jest funkcja tworząca ciągu (a_i) , gdzie $a_i = \lfloor m/i \rfloor$ dla pewnego ustalonego $m \in \mathbb{N}$, $m > 0$. Ciąg ten składa się więc z jedynek i zer, przy czym jedynkami są wyrazy $a_0, a_m, a_{2m}, a_{3m}, \dots$, a zerami – wszystkie pozostałe wyrazy ciągu. Licząc z definicji funkcję tworzącą tego ciągu otrzymujemy następujące wyrażenie:

$$\sum_{i=0}^{\infty} z^{m \cdot i} = \frac{1}{1 - z^m}.$$

A zatem na przykład funkcję tworzącą naprzemiennego ciągu złożonego z jedynek i zer

$$(1, 0, 1, 0, 1, 0, \dots)$$

jest funkcja $(1 - z^2)^{-1}$. \square

Funkcje tworzące wielu ważnych ciągów, występujących w rozmaitych zastosowaniach, są łatwe do zapamiętania, ponieważ szeregi Maclaurina odpowiednich funkcji analitycznych są często używane. Poniższy przykład pokazuje kilka takich funkcji, powszechnie występujących w rozmaitych zastosowaniach.

Przykład 3.4 Szereg Maclaurina funkcji wykładniczej e^z , gdzie $z \in \mathbb{C}$, ma postać

$$e^z = \sum_{i=0}^{\infty} \frac{z^i}{i!},$$

a zatem e^z jest funkcją tworzącą ciągu $((i!)^{-1})$. Podobnie, ponieważ

$$-\ln(1 - z) = \sum_{i=1}^{\infty} \frac{z^i}{i},$$

3.1. FUNKCJE TWORZĄCE

to wyrażenie $-\ln(1 - z)$ jest funkcją tworzącą ciągu

$$\left(0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots \right).$$

Na ciągach możemy wykonywać różnorodne operacje. Odpowiadają im wówczas operacje na funkcjach tworzących. Oto najważniejsze z nich:

Niech $A(z) = \sum_{i=0}^{\infty} a_i z^i$ i $B(z) = \sum_{i=0}^{\infty} b_i z^i$ będą – odpowiednio – funkcjami tworzącymi ciągów (a_i) oraz (b_i) . Wówczas funkcją tworzącą ciągu $(a_i + b_i)$ jest suma funkcji tworzących $A(z)$ i $B(z)$, bowiem

$$A(z) + B(z) = \sum_{i=0}^{\infty} (a_i + b_i) z^i.$$

Ciąg $(p \cdot a_i)$, który powstaje z ciągu (a_i) przez pomnożenie każdego elementu przez stałą $p \in \mathbb{C}$, ma funkcję tworzącą $p \cdot A(z)$, bowiem

$$p \cdot A(z) = \sum_{i=0}^{\infty} p \cdot a_i \cdot z^i.$$

Inną, często spotykaną operacją na ciągach jest *przesunięcie ciągu o m miejsc w prawo* dla pewnego ustalonego $m \in \mathbb{N}$, to znaczy zastąpienie ciągu

$$(a_0, a_1, a_2, \dots)$$

ciągiem

$$(0, \dots, 0, a_0, a_1, a_2, \dots),$$

gdzie liczba zer wprowadzonych na początku jest równa dokładnie m . Łatwo stwierdzić, że jeśli $A(z)$ jest funkcją tworzącą ciągu wyjściowego, to $z^m \cdot A(z)$ jest funkcją tworzącą ciągu przesuniętego o m miejsc w prawo.

Przykład 3.5 W Przykładzie 3.3 pokazaliśmy, że funkcją tworzącą ciągu

$$(1, 0, 1, 0, 1, 0, \dots)$$

jest $(1 - z^2)^{-1}$. Jeśli więc interesuje nas funkcja tworząca takiego ciągu, ale przesuniętego o jedno miejsce w prawo, to znaczy ciągu

$$(0, 1, 0, 1, 0, 1, 0, \dots),$$

to z poprzednich rozważań wynika, że należy pomnożyć otrzymane wyrażenie przez z^1 , a zatem dla ciągu naprzemiennego złożonego z zer i jedynek, zaczynającego się od zera, mamy funkcję tworzącą $z(1 - z^2)^{-1}$. Podobnie, z Przykładu 3.4 wynika, że funkcją tworzącą ciągu

$$\left(0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right)$$

jest $- \ln(1 - z)$. Jeśli więc chcemy mieć funkcję tworzącą ciągu

$$\left(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right),$$

to wystarczy zauważyć, że poprzedni ciąg powstaje z niego w wyniku przesunięcia o jedną pozycję w prawo, a zatem funkcję tworzącą ciągu $\left(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right)$ jest $-z^{-1} \ln(1 - z)$. \square

W wielu zastosowaniach mamy do czynienia z potrzebą zastąpienia ciągu (a_i) , gdzie $a_i \in \mathbb{C}$ dla $i \in \mathbb{N}$, przez ciąg $(p^i \cdot a_i)$ dla pewnej stałej $p \in \mathbb{C}$, $p \neq 0$. Latwo pokazać, że jeśli $A(z)$ jest funkcją tworzącą ciągu a_i , to $A(p \cdot z)$ jest funkcją tworzącą ciągu $(p^i \cdot a_i)$. Szczególnie często z transformacją taką mamy do czynienia dla $p = -1$. Poniższy przykład ilustruje taką właśnie sytuację.

Przykład 3.6 Rozważmy ciąg nieskończony złożony z samych jedynek:

$$(1, 1, 1, \dots).$$

Funkcja tworząca tego ciągu ma postać $(1 - z)^{-1}$, bowiem

$$\frac{1}{1 - z} = 1 + z + z^2 + z^3 + \dots.$$

Zatem funkcję tworzącą ciągu

$$(1, -1, 1, -1, 1, -1, \dots),$$

tzn. ciągu $((-1)^i \cdot 1)$, jest funkcja $(1 + z)^{-1}$. Otrzymaliśmy więc inną metodą ten sam wynik co w Przykładzie 3.2. \square

Czasem mamy do czynienia z ciągiem $(i \cdot a_i)$, który powstaje z wyjściowego ciągu (a_i) przez pomnożenie jego i -tego wyrazu przez i . Latwo pokazać, że jeśli $A(z)$ jest funkcją tworzącą ciągu (a_i) , to funkcja tworząca ciągu $(i \cdot a_i)$ ma postać $zA'(z)$, gdzie $A'(z)$ jest pierwszą pochodną funkcji $A(z)$.

3.1. FUNKCJE TWORZĄCE

Przykład 3.7 Rozważmy ciąg złożony z kolejnych liczb naturalnych: $(0, 1, 2, 3, \dots)$.

Zauważmy, że ciąg ten otrzymujemy z ciągu złożonego z samych jedynek $(1, 1, 1, \dots)$ poprzez pomnożenie jego i -tego elementu przez i . Z Przykładu 3.6 wynika, że funkcję tworzącą ciągu $(1, 1, 1, \dots)$ jest $A(z) = (1 - z)^{-1}$, a zatem poszukiwaną funkcję tworzącą ciągu liczb naturalnych $(0, 1, 2, 3, \dots)$ jest $B(z) = z \frac{d}{dz}(1 - z)^{-1} = z(1 - z)^{-2}$. \square

Bardzo ważną operację wykonywaną na ciągach jest tworzenie tak zwanego *splotu* ciągów.¹

Definicja 3.2 Splotem ciągów (a_i) oraz (b_i) nazywamy ciąg (c_i) , gdzie

$$c_i = \sum_{j=0}^i a_j \cdot b_{i-j}. \quad (3.4)$$

Rysunek 3.1 w poglądowy sposób ilustruje zasadę sumowania elementów przy tworzeniu splotu ciągów (a_i) oraz (b_i) .

Operację splotu ciągów oznaczamy symbolem $*$ i dla ciągów spełniających zależność (3.4) piszemy:

$$(c_i) = (a_i) * (b_i).$$

Z definicji splotu wynika natychmiast, że jest to operacja przemienne, to znaczy

$$(a_i) * (b_i) = (b_i) * (a_i).$$

Operacja splotu występuje często przy manipulowaniu ciągami. W tym przypadku uwidocznia się szczególnie wyraźnie wygoda operowania funkcjami tworzącymi, bowiem – jak łatwo pokazać – funkcję tworzącą splotu jest po prostu iloczyn funkcji tworzących ciągów, tzn.

$$\sum_{i=0}^{\infty} c_i z^i = A(z) \cdot B(z).$$

¹Inną często spotykaną nazwą jest *iloczyn Cauchy'ego* ciągów.

| | a_0 | a_1 | a_2 | a_3 | a_4 | a_5 | a_6 | \dots |
|-------|-----------------------------------|-------------------------------|-------------------------------|---------------------------|-----------------------|-------------------|---------------|---------|
| b_0 | $a_0 b_0$ | $a_1 b_0$ | $a_2 b_0$ | $a_3 b_0$ | $a_4 b_0$ | $a_5 b_0$ | $a_6 b_0$ | \dots |
| b_1 | $c_0 a_0 b_1$ | $c_1 a_1 b_1$ | $c_2 a_2 b_1$ | $c_3 a_3 b_1$ | $c_4 a_4 b_1$ | $c_5 a_5 b_1$ | $c_6 a_6 b_1$ | \dots |
| b_2 | $c_1 c_0 a_0 b_2$ | $c_2 c_1 a_1 b_2$ | $c_3 c_2 a_2 b_2$ | $c_4 c_3 a_3 b_2$ | $c_5 c_4 a_4 b_2$ | $c_6 c_5 a_5 b_2$ | \dots | |
| b_3 | $c_2 c_1 c_0 a_0 b_3$ | $c_3 c_2 c_1 a_1 b_3$ | $c_4 c_3 c_2 a_2 b_3$ | $c_5 c_4 c_3 a_3 b_3$ | $c_6 c_5 c_4 a_4 b_3$ | \dots | | |
| b_4 | $c_3 c_2 c_1 c_0 a_0 b_4$ | $c_4 c_3 c_2 c_1 a_1 b_4$ | $c_5 c_4 c_3 c_2 a_2 b_4$ | $c_6 c_5 c_4 c_3 a_3 b_4$ | \dots | | | |
| b_5 | $c_4 c_3 c_2 c_1 c_0 a_0 b_5$ | $c_5 c_4 c_3 c_2 c_1 a_1 b_5$ | $c_6 c_5 c_4 c_3 c_2 a_2 b_5$ | \dots | | | | |
| b_6 | $c_5 c_4 c_3 c_2 c_1 c_0 a_0 b_6$ | \dots | | | | | | |
| : | c_6 | \dots | | | | | | |

Rysunek 3.1: Zasada sumowania elementów przy tworzeniu splotu ciągów (a_i) oraz (b_i) .

W naturalny sposób możemy zdefiniować splot większej liczby ciągów. Mianowicie splotem ciągów² (a_i^j) , $j = 1, \dots, n$, nazywiemy ciąg $(s_i) = (a_i^1) * (a_i^2) * \dots * (a_i^n)$, gdzie dla $i \in \mathbb{N}$,

$$s_i = \sum_{\substack{k_1, \dots, k_n \in \mathbb{N} \\ k_1 + \dots + k_n = i}} a_{k_1}^1 \cdot a_{k_2}^2 \cdot \dots \cdot a_{k_n}^n.$$

Jeśli $A_j(z)$, $j = 1, \dots, n$, oznaczają – odpowiednio – funkcje tworzące ciągów (a_i^j) , to funkcja tworząca $S(z)$ splotu (s_i) tych ciągów ma postać

$$S(z) = \prod_{j=1}^n A_j(z).$$

Poniższe przykłady ilustrują użycie funkcji tworzącej dla splotów.

²W zapisie (a_i^j) symbol j jest indeksem, a nie j -tą potęgą wyrażenia a_i .

3.1. FUNKCJE TWORZĄCE

Przykład 3.8 Rozważmy dowolny ciąg (a_i) o wartościach w zbiorze liczb zespolonych i niech $A(z)$ oznacza jego funkcję tworzącą.

Ciągiem sum częściowych ciągu (a_i) nazywamy ciąg (b_i) , gdzie

$$b_i = \sum_{j=0}^i a_j, \quad i \in \mathbb{N}.$$

Chcemy wyznaczyć funkcję tworzącą ciągu (b_i) . Zauważmy, że ciąg ten jest w istocie splotem ciągu (a_i) oraz ciągu $(1, 1, 1, \dots)$. Funkcją tworzącą ciągu $(1, 1, 1, \dots)$ jest $(1 - z)^{-1}$, a zatem funkcja tworząca ciągu sum częściowych ciągu (a_i) ma postać $(1 - z)^{-1}A(z)$.

Jeśli na przykład wybierzemy jako ciąg (a_i) , ciąg złożony z samych jedynek, to otrzymamy jako ciąg jego sum częściowych ciąg złożony z kolejnych dodatnich liczb naturalnych:

$$(1, 2, 3, 4, \dots).$$

Ciąg powyższy jest splotem dwóch ciągów złożonych z samych jedynek, a zatem jego funkcja tworząca jest kwadratem wyrażenia $(1 - z)^{-1}$. Funkcję tworzącą ciągu dodatnich liczb naturalnych jest więc $(1 - z)^{-2}$.

Aby uzyskać funkcję tworzącą ciągu kolejnych liczb naturalnych (to znaczy z zerem jako pierwszym wyrazem ciągu):

$$(0, 1, 2, 3, 4, \dots),$$

wystarczy dokonać przesunięcia poprzedniego ciągu o jedno miejsce w prawo. Zatem funkcją tworzącą ciągu liczb naturalnych jest $z(1 - z)^{-2}$. Otrzymaliśmy więc raz jeszcze inną metodą to samo wyrażenie co w Przykładzie 3.7. \square

Przykład 3.9 Bardzo ważny w zastosowaniach jest ciąg tak zwanych liczb harmonicznych, oznaczany zwykle symbolem (H_i) . Element i -ty tego ciągu jest definiowany następująco:

$$H_i = \sum_{j=1}^i \frac{1}{j}, \quad i \in \mathbb{N}. \quad (3.5)$$

Pierwszymi kilkunastoma wyrazami ciągu (H_i) są:

$$0, 1, \frac{3}{2}, \frac{11}{6}, \frac{25}{12}, \frac{137}{60}, \frac{49}{20}, \frac{363}{140}, \frac{761}{280}, \frac{7129}{2520}, \frac{7381}{2520}, \frac{83711}{27720}, \frac{86021}{27720}, \dots$$

Liczby harmoniczne występują bardzo często w informatyce przy analizie złożoności obliczeniowej algorytmów (patrz np. [6, 11]). Z (3.5) wynika, że ciąg liczb harmonicznych jest ciągiem sum częściowych analizowanego już wcześniej ciągu

$$\left(0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right).$$

Z Przykładu 3.4 wynika więc, że funkcją tworzącą ciągu liczb harmonicznych jest iloczyn funkcji tworzących powyższego ciągu oraz ciągu złożonego z samych jedynek. W wyniku otrzymujemy następujące wyrażenie: $-(1-z)^{-1} \ln(1-z)$. \square

3.1.1 Zastosowania funkcji tworzących

W niniejszym punkcie przedstawimy kilka przykładów użycia funkcji tworzących w zagadnieniach kombinatorycznych. Mimo że wybór tych przykładów jest bardzo ograniczony, to jednak pozwoli zorientować się, jak silnym i pożytecznym narzędziem jest technika funkcji tworzących.

Liczba rozwiązań równania diofantycznego

Rozważmy dla ustalonych $k, n \in \mathbb{N}$ równanie diofantyczne o postaci

$$x_1 + \dots + x_n = k. \quad (3.6)$$

Załóżmy, że interesują nas rozwiązania powyższego równania, spełniające następujące dodatkowe warunki:

$$x_i \in X_i, \quad i = 1, \dots, n, \quad (3.7)$$

gdzie $X_i \subseteq \mathbb{N}$, $i = 1, \dots, n$, są danymi podzbiorami liczb naturalnych.

Naszym celem jest wyznaczenie liczby wszystkich takich rozwiązań równania (3.6) dla dowolnego naturalnego k . Oznaczmy tę liczbę symbolem s_k . Zadanie polega więc na znalezieniu wszystkich wyrazów ciągu (s_k) . Oznaczmy symbolem $S(z)$ funkcję tworzącą tego ciągu. Niech ponadto dla $i = 1, \dots, n$, $F_i(z)$ oznacza funkcję tworzącą ciągu³ $(c_j^i) = ([j \in X_i])$, wskazującego dopuszczalne wartości zmiennej x_i , to znaczy

$$F_i(z) = \sum_{j=0}^{\infty} [j \in X_i] \cdot z^j, \quad i = 1, \dots, n. \quad (3.8)$$

³W zapisie c_j^i wyrazów tego ciągu symbol i jest indeksem górnym, a nie potęgą wyrażenia c_j .

3.1. FUNKCJE TWORZĄCE

Łatwo pokazać, że ciąg (s_k) jest po prostu splotem ciągów (c_j^i) dla $i = 1, \dots, n$, co oznacza, że funkcje tworzące tych ciągów spełniają następującą zależność:

$$S(z) = \prod_{i=1}^n F_i(z). \quad (3.9)$$

Mamy bowiem

$$s_k = \sum_{\substack{k_1, \dots, k_n \in \mathbb{N} \\ k_1 + \dots + k_n = k}} [k_1 \in X_1] \cdot [k_2 \in X_2] \cdot \dots \cdot [k_n \in X_n].$$

Zauważmy, że każdy ze składników powyższej sumy jest równy 0 albo 1. Ponadto, jeśli $[k_1 \in X_1] \cdot [k_2 \in X_2] \cdot \dots \cdot [k_n \in X_n] = 1$, to składnik taki odpowiada jednoznacznie następującemu rozwiązaniu równania (3.6) z prawą stroną równą k :

$$x_i = k_i \quad i = 1, \dots, n.$$

Ponieważ sumowanie odbywa się po wszystkich możliwych n -tkach liczb naturalnych k_1, \dots, k_n , spełniających warunek $k_1 + \dots + k_n = k$, to s_k jest poszukiwaną liczbą rozwiązań równania diofantycznego

$$x_1 + \dots + x_n = k,$$

a funkcja $S(z)$, dana wzorem (3.9), jest poszukiwaną funkcją tworzącą ciągu (s_k) .

Liczba podzbiorów zbioru z powtórzeniami

Niech $X = \langle k_1 * a_1, k_2 * a_2, \dots, k_n * a_n \rangle$, gdzie $k_i \in \mathbb{N}$ dla $i = 1, \dots, n$, będąc danym zbiorem z powtórzeniami. W Rozdziale 2.5 zajmowaliśmy się pewnymi szczególnymi zagadnieniami zliczania podzbiorów zbioru X . Okazuje się, że funkcje tworzące są znakomitym narzędziem do tego typu analizy.

Zauważmy najpierw, że istnieje wzajemnie jednoznaczna odpowiedniość między podzbiorami k -elementowymi zbioru Z z powtórzeniami

$$X = \langle k_1 * a_1, k_2 * a_2, \dots, k_n * a_n \rangle$$

a rozwiązaniami następującego równania diofantycznego:

$$x_1 + x_2 + \dots + x_n = k \quad (3.10)$$

z dodatkowymi warunkami

$$x_i \in \{0, 1, \dots, k_i\} \quad i = 1, \dots, n. \quad (3.11)$$

Istotnie, jeśli zbiór $Y = \langle l_1 * a_1, l_2 * a_2, \dots, l_n * a_n \rangle$ jest k -elementowym podzbiorem zbioru X , to wektor (x_1, \dots, x_n) , gdzie

$$x_i = l_i, \quad i = 1, \dots, n, \quad (3.12)$$

jest rozwiązaniem równania (3.10). I na odwrót – rozwiązaniu (3.12) możemy jednoznacznie przyporządkować podzbiór $Y = \langle l_1 * a_1, \dots, l_n * a_n \rangle$ zbioru X .

Liczba k -elementowych podzbiorów zbioru X jest więc równa liczbie rozwiązań równania diofantycznego (3.10), spełniających warunki (3.11). Ale skoro tak, to teraz łatwo już możemy zastosować wyniki z poprzedniego paragrafu, dotyczące liczby rozwiązań równania diofantycznego. Mamy tu bowiem dla $i = 1, \dots, n$,

$$X_i = \{0, 1, \dots, k_i\},$$

a zatem odpowiednie funkcje tworzące ciągów $(c_j^i) = ([j \in X_i])$ mają postać:

$$A_i(z) = 1 + z + z^2 + \dots + z^{k_i}. \quad (3.13)$$

Jeśli więc symbolem $A_X(z)$ oznaczymy funkcję tworzącą ciągu (s_k) , w którym dla $k \in \mathbb{N}$, s_k jest liczbą podzbiorów k -elementowych zbioru X , to otrzymamy następującą zależność:

$$A_X(z) = A_1(z) \cdot A_2(z) \cdot \dots \cdot A_n(z).$$

Przykład 3.10 Rozważmy zbiór z powtórzeniami

$$X = \langle 3 * a_1, 1 * a_2, 2 * a_3 \rangle.$$

Funkcje tworzące $A_1(z)$, $A_2(z)$ i $A_3(z)$ mają – odpowiednio – postaci:

$$A_1(z) = 1 + z + z^2 + z^3,$$

$$A_2(z) = 1 + z,$$

$$A_3(z) = 1 + z + z^2.$$

Funkcją tworzącą ciągu (l_k) , gdzie dla $k \in \mathbb{N}$, l_k jest liczbą k -elementowych podzbiorów zbioru X jest więc następujące wyrażenie:

3.1. FUNKCJE TWORZĄCE

$$\begin{aligned} A_X(z) &= A_1(z) \cdot A_2(z) \cdot A_3(z) = \\ &= (1 + z + z^2 + z^3)(1 + z)(1 + z + z^2) = \\ &= 1 + 3z + 5z^2 + 6z^3 + 5z^4 + 3z^5 + z^6. \end{aligned}$$

Współczynniki przy kolejnych potęgach zmiennej z w funkcji $A_X(z)$ mówią, że zbiór z powtórzeniami $X = \langle 3 * a_1, 1 * a_2, 2 * a_3 \rangle$ ma dokładnie jeden podzbiór pusty, trzy podzbiory o liczności 1, pięć podzbiorów o liczności 2, sześć podzbiorów o liczności 3, pięć podzbiorów o liczności 4, trzy podzbiorów o liczności 5, jeden podzbiór o liczności 6 oraz nie ma podzbiorów o liczności większej niż 6. \square

Powyższy przykład pokazuje, jak wygodnym i silnym narzędziem jest technika funkcji tworzących dla znajdowania liczby podzbiorów zbioru z powtórzeniami. Zauważmy, że w wyniku bardzo prostych operacji algebraicznych otrzymaliśmy liczby podzbiorów zbioru X o wszystkich możliwych licznościach. Ponadto, analogiczne postępowanie można powtórzyć w przypadku, gdy na liczności wystąpienia danego elementu zbioru nałożone są różnorodne ograniczenia. Wystarczy w tym celu odpowiednio dobrze podzbiory X_i , $i = 1, \dots, n$, definiujące warunki nakładane na rozwiązanie równania diofantycznego (3.10), potem wyznaczyć odpowiadające im funkcje tworzące, a następnie skorzystać z zależności (3.9). Poniższy przykład ilustruje takie podejście.

Przykład 3.11 Rozważmy ponownie zbiór z powtórzeniami

$$X = \langle 3 * a_1, 1 * a_2, 2 * a_3 \rangle.$$

Tym razem jednak będą nas interesowały jedynie liczby podzbiorów tego zbioru, w których elementy o nieparzystych indeksach w zbiorze podstawowym, to znaczy elementy a_1 oraz a_3 , albo wcale nie występują, albo występują parzystą liczbę razy. Oznacza to, że zamiast mnożenia funkcji tworzących $A_1(z)$, $A_2(z)$ i $A_3(z)$ z poprzedniego przykładu należy pomnożyć następujące funkcje tworzące:

$$A'_1(z) = 1 + z^2,$$

$$A'_2(z) = 1 + z,$$

$$A'_3(z) = 1 + z^2,$$

odpowiadające ciągom $(1, 0, 1)$, $(1, 1)$ oraz $(1, 0, 1)$. Funkcją tworzącą ciągu (l_k) , gdzie dla $k \in \mathbb{N}$, l_k jest liczbą k -elementowych podzbiorów zbioru X , spełniających podany wyżej warunek, jest więc następujące wyrażenie:

$$\begin{aligned} A'_X(z) &= A'_1(z) \cdot A'_2(z) \cdot A'_3(z) = \\ &= (1+z^2)(1+z)(1+z^2) = \\ &= 1+z+2z^2+2z^3+z^4+z^5. \end{aligned}$$

Gdyby natomiast interesowały nas liczby podzbiorów zbioru X , w których każdy z elementów a_1, a_2, a_3 , występuje niezerową liczbę razy, to należałoby pomnożyć funkcje

$$\begin{aligned} A''_1(z) &= z+z^2+z^3, \\ A''_2(z) &= z, \\ A''_3(z) &= z+z^2, \end{aligned}$$

odpowiadające ciągom $(0, 1, 1, 1)$, $(0, 1)$ oraz $(0, 1, 1)$. W wyniku uzyskamy funkcję tworzącą

$$A''_X(z) = z^3 + 2z^4 + 2z^5 + z^6,$$

z której łatwo odczytać liczby wszystkich możliwych podzbiorów, zawierających po co najmniej jednym elemencie a_1, a_2, a_3 . \square

Zliczanie podziałów liczby na składniki

W Rozdziale 2.7 wprowadziliśmy podstawowe pojęcia związane z podziałami liczby naturalnej na składniki. Tutaj pokażemy, w jaki sposób technika funkcji tworzących może być użyta do wyznaczenia ciągu $(P_h(n))$ dla dowolnej ustalonej liczby naturalnej h .

Przypomnijmy, że dla $n, h \in \mathbb{N}$, gdzie $h \leq n$, symbol $P_h(n)$ oznacza liczby wszystkich podziałów liczby n na składniki nie przekraczające h . Przyjmiemy, że $P_h(0) = 1$ dla dowolnego $h \in \mathbb{N}$.

Niech dla ustalonego $n \in \mathbb{N}$ ciąg (a_1, \dots, a_k) będzie podzieleniem liczby n na $k \in \mathbb{N}$ składników. Z podzieleniem tym możemy związać w sposób wzajemnie jednoznaczny n -elementowy wektor $(\lambda_1, \dots, \lambda_n)$, którego elementy zdefiniowane są następująco:

$$\lambda_i = |\{j : a_j = i, 1 \leq j \leq k\}|.$$

Oznacza to, że dla $i = 1, \dots, n$, wartość λ_i jest liczbą tych składników w podziale (a_1, \dots, a_k) , które są równe i . Zachodzi oczywiście zależność

$$n = \sum_{i=1}^n i \cdot \lambda_i. \quad (3.14)$$

3.1. FUNKCJE TWORZĄCE

Jeśli interesują nas podziały, w których największy składnik nie przekracza $h \in \mathbb{N}$, to mamy $\lambda_i = 0$ dla $i = h+1, \dots, n$, a zatem wówczas

$$n = \sum_{i=1}^h i \cdot \lambda_i. \quad (3.15)$$

Wyznaczenie ciągu $(P_h(n))$ jest więc równoważne znalezieniu ciągu, którego elementami są liczby wektorów całkowitoliczbowych nieujemnych $(\lambda_1, \dots, \lambda_h)$, spełniających powyższą równość. Łatwo dowieść, że funkcja tworząca takiego ciągu ma postać:

$$F(z) = \prod_{i=1}^h (1+z^i+z^{2i}+z^{3i}+\dots) = \prod_{i=1}^h (1-z^i)^{-1}. \quad (3.16)$$

Tak istotnie jest. Aby to pokazać, potraktujmy zależność (3.15) jak równanie diofantyczne ze zmiennymi λ_i , oraz dokonajmy dla $i = 1, \dots, h$, podstawienia

$$x_i = i \cdot \lambda_i.$$

Otrzymujemy równanie diofantyczne w postaci (3.6) z prawą stroną równą n , w którym zbiory X_i , $i = 1, \dots, h$, ograniczające swobodę wyboru wartości zmiennych x_i , są następujące:

$$X_i = \{0, i, 2i, 3i, \dots\}, \quad i = 1, \dots, h.$$

Taka postać zbiorów X_i jest konsekwencją warunku całkowitoliczbowości zmiennych λ_i . Wyrażenie (3.16) wynika więc teraz bezpośrednio z zależności (3.9).

Przykład 3.12 Niech $h = 6$. Funkcja tworząca ciągu $(P_6(n))$ ma zgodnie z zależnością (3.16) – następującą postać:

$$F(z) = \prod_{i=1}^6 (1-z^i)^{-1} = 1+z+2z^2+3z^3+5z^4+7z^5+11z^6+14z^7+20z^8+\dots$$

Z powyższego wyrażenia łatwo na przykład odczytać, że liczba podziałów liczby 6 na składniki nie przekraczające 6 jest równa 11, bowiem taką wartość ma współczynnik przy z^6 , natomiast liczba podziałów liczby 7 na składniki nie przekraczające 6 jest równa 14 itd. \square

Funkcja tworząca dla ciągu liczb Fibonacciego

Ciąg (F_i) liczb Fibonacciego⁴ opisany jest zależnością rekurencyjną

$$F_{i+1} = F_i + F_{i-1}, \quad \text{dla } i \geq 1, \quad (3.17)$$

z warunkami początkowymi

$$F_i = [i = 1] \quad \text{dla } i = 0, 1. \quad (3.18)$$

Pierwszymi kilkunastoma wyrazami tego ciągu są:

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597...

Czasem przyjmuje się inną postać warunków początkowych dla ciągu Fibonacciego, a mianowicie $F_i = 1$ dla $i = 0, 1$. Obie wersje ciągów różnią się więc przesunięciem o jedno miejsce.

Dla wyznaczenia funkcji tworzącej $F(z)$ ciągu (F_i) przepiszmy nieco inaczej zależność rekurencyjną (3.17), włączając od razu warunki początkowe i przyjmując, że $F_i = 0$ dla $i < 0$. Otrzymujemy dla $i \in \mathbb{N}$,

$$F_i = [i = 1] + F_{i-1} + F_{i-2}. \quad (3.19)$$

Z zależności (3.19) wynika, że ciąg F_i jest sumą następujących trzech ciągów: ciągu $[i = 1]$ oraz dwóch ciągów powstały z (F_i) przez przesunięcie – odpowiednio – o jedno miejsce i o dwa miejsca w prawo. Z Przykładu 3.3 i własności funkcji tworzących dla operacji przesunięcia wynika więc, że funkcja tworząca $F(z)$ ciągu liczb Fibonacciego spełnia następujące równanie:

$$F(z) = z + zF(z) + z^2F(z). \quad (3.20)$$

Rozwiązuje to równanie względem $F(z)$ otrzymujemy następujące wyrażenie:

$$F(z) = \frac{z}{1 - z - z^2}. \quad (3.21)$$

Aby uzyskać wartości liczb Fibonacciego F_i dla $i \in \mathbb{N}$, zauważmy, że

$$(1 - z - z^2) = (1 - az)(1 - bz),$$

⁴Nazwa pochodzi od nazwiska włoskiego matematyka Leonardo di Pisa, nazywanego Fibonacci, który zajmował się takim ciągiem liczbowym w wydanej w roku 1202 książce *Liber Abaci*.

3.1. FUNKCJE TWORZĄCE

gdzie $a = (1 - \sqrt{5})/2$ i $b = (1 + \sqrt{5})/2$. Mamy zatem

$$\begin{aligned} F(z) &= \frac{z}{(1 - az)(1 - bz)} = \frac{1}{(a - b)(1 - az)} - \frac{1}{(a - b)(1 - bz)} = \\ &= \frac{1}{a - b} \cdot \sum_{i=0}^{\infty} a^i z^i - \frac{1}{a - b} \cdot \sum_{i=0}^{\infty} b^i z^i = \\ &= \sum_{i=0}^{\infty} \frac{a^i - b^i}{a - b} \cdot z^i. \end{aligned}$$

Współczynnik przy i -tej potędze z w powyższej sumie jest właśnie równy elementowi F_i ciągu Fibonacciego, a zatem

$$F_i = \frac{a^i - b^i}{a - b} \quad \text{dla } i \in \mathbb{N}.$$

Podstawiając wartości a i b otrzymujemy:

$$F_i = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^i - \left(\frac{1 - \sqrt{5}}{2} \right)^i \right], \quad i \in \mathbb{N}. \quad (3.22)$$

Liczby Fibonacciego odgrywają ogromną rolę w wielu różnych dziedzinach. Bardzo istotne jest też zastosowanie tych liczb w konstrukcji i analizie algorytmów obliczeniowych. Poniższy przykład ilustruje jedno z takich zastosowań.

Przykład 3.13 Wyznaczanie ekstremum lokalnego funkcji rzeczywistej.

Załóżmy, że poszukujemy minimum lokalnego funkcji $f : \mathbb{R} \rightarrow \mathbb{R}$ w przedziale $[a, b]$. O funkcji f wiemy tylko, że jest funkcją unimodalną na przedziale $[a, b]$, to znaczy, że ma w tym przedziale dokładnie jedno minimum lokalne. Ponadto umiemy wyznaczać wartości funkcji f w dowolnych punktach wewnętrznych tego przedziału i znamy wartości $f(a)$ oraz $f(b)$. Nie zakładamy natomiast różniczkowalności funkcji f w punktach przedziału $[a, b]$.

Zadanie polega na takim doborze N punktów (gdzie $N > 3$ jest ustaloną wcześniej liczbą naturalną) z odcinka $[a, b]$, aby możliwie najbardziej określić przedział, w którym znajduje się minimum lokalne funkcji f .

Istnieją różne algorytmy dla rozwiązywania tak postawionego problemu (patrz np. [3]). W pewnym sensie najlepszym z nich, dającym najbardziej ścisłe oszacowanie przedziału, w którym leży minimum funkcji, jest algorytm wykorzystujący ciąg Fibonacciego.

Jest to algorytm iteracyjny. W każdej iteracji jest liczona wartość funkcji f w pewnym punkcie wewnętrznym aktualnego przedziału, a następnie przedział ten jest odpowiednio zawiążany.

Inicjalizacja algorytmu polega na podzieleniu przedziału $[a, b]$ na F_N równych odcinków, gdzie F_N jest N -tą liczbą Fibonacciego. Dla wygody prezentacji możemy przyjąć, że zamiast rozważać dowolny przedział $[a, b]$, na wstępnie dokonujemy takiego przekształcenia argumentów funkcji, że jest ona określona na przedziale $[F_0, F_N]$. Wówczas punktami podziału rozważanego zakresu zmienności funkcji f są punkty całkowitoliczbowe z odcinka $[0, F_N]$. Inicjalizacja kończy się policzeniem wartości funkcji f w dwóch punktach внутренnych przedziału $[0, F_N]$: $x' = F_{N-2}$ oraz $x'' = F_{N-1}$.

Załóżmy dla ustalenia uwagi, że $f(0) < f(F_N)$ i zauważmy, że policzenie wartości funkcji f w dwóch punktach внутренnych odcinka $[0, F_N]$ pozwala na zawiążenie przedziału, w którym znajduje się minimum funkcji. Jeśli bowiem $f(F_{N-2}) < f(F_{N-1})$, to z faktu, iż funkcja f jest unimodalna wynika, że minimum lokalne musi należeć do przedziału $[0, F_{N-1}]$. Jeśli natomiast $f(F_{N-2}) \geq f(F_{N-1})$, to minimum funkcji musi być osiągane w przedziale $[F_{N-2}, F_N]$ (patrz przykład wykresu funkcji unimodalnej na Rysunku 3.2). Zauważmy, że w obu przypadkach długość przedziału jest zmniejszana z początkowej wartości F_N do wartości F_{N-1} .

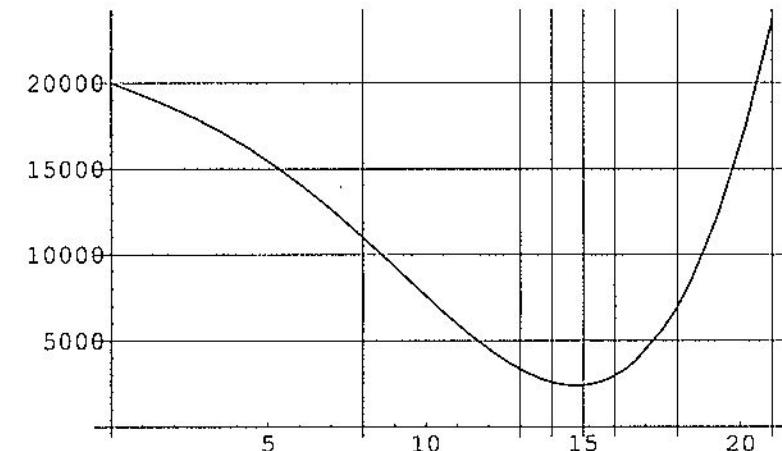
Właściwości ciągu Fibonacciego sprawiają, że możemy teraz powtórzyć iterację algorytmu dla zawiązanego przedziału, wybierając w nim ponownie dwa punkty внутренne, przy czym – co jest bardzo istotne – wartość funkcji f w jednym z tych punktów jest już znana. Punkty te są bowiem oddalone od brzegów zawiązanego przedziału o wartość kolejnej liczby Fibonacciego (w drugiej iteracji jest to F_{N-3}). Jeśli zatem stwierdziliśmy, że minimum funkcji jest osiągane w przedziale $[0, F_{N-1}]$, to punktami tymi są $x = 0 + F_{N-3}$ oraz $x = F_{N-1} - F_{N-3} = F_{N-2}$. Jeśli natomiast minimum funkcji leży w przedziale $[F_{N-2}, F_N]$, to wybieramy jako punkty внутренne $x = F_{N-2} + F_{N-3} = F_{N-1}$ oraz $x = F_N - F_{N-3}$.

Kolejne iteracje są powtórzeniem powyższego postępowania. W każdej z nich liczymy wartość funkcji tylko w jednym nowym punkcie i zawiązamy długość aktualnego przedziału do wartości kolejnej mniejszej liczby Fibonacciego. W chwili, gdy aktualna długość przedziału jest równa $F_3 = 2$, następuje nieznaczna modyfikacja iteracji kończącej algorytm. Zauważmy mianowicie, że gdybyśmy zawiązili przedział z obu stron o wartość $F_2 = 1$, to otrzymalibyśmy tylko jeden punkt внутренny przedziału, będący jego środkiem. Co więcej, w punkcie tym wartość funkcji jest już znana.

3.1. FUNKCJE TWORZĄCE

Dlatego w ostatniej iteracji obliczamy wartość f w punkcie przesuniętym o dowolnie małą liczbę ϵ od środka aktualnego przedziału. Poniższy przykład numeryczny ilustruje to postępowanie.

Na Rysunku 3.2 przedstawiony jest wykres funkcji unimodalnej, na której prześledzimy działanie algorytmu. Jest to funkcja $f(x) = 0,7x^4 - 13x^3 + 6x^2 - 700x + 2000$, określona na przedziale $[0, 21]$. Zauważmy, że przykład jest tak dobrany, że końcami przedziału zmienności funkcji są punkty $x = 0 = F_0$ oraz $x = 21 = F_8$. Jeśli więc przyjmiemy $N = 8$, to mamy od razu zadanie określone na wymaganym przedziale $[F_0, F_N]$.



Rysunek 3.2: Wykres funkcji unimodalnej $f(x) = 0,7x^4 - 13x^3 + 6x^2 - 700x + 2000$ z Przykładu 3.13.

W pierwszej iteracji mamy przedział $[0, 21]$ i dwa punkty внутренne, w których należy policzyć wartość funkcji. Są to punkty $x = F_6 = 8$ i $x = F_7 = 13$. Mamy $f(8) = 10995,2$ oraz $f(13) = 3345,7$. Ponieważ $f(8) > f(13)$, wiemy, że minimum funkcji f musi leżeć w przedziale $[F_6, F_8] = [8, 21]$. Zgodnie z przyjętą regułą wybieramy w tym przedziale dwa punkty внутренne odległe od brzegów o $F_5 = 5$. Są to: punkt $x = F_6 + F_5 = F_7 = 13$, w którym wartość funkcji f już znamy, oraz nowy punkt $x = F_8 - F_5 = 16$, w którym tę wartość należy dopiero wyznaczyć. Otrzymujemy $f(16) = 2963,2 < f(13)$, a zatem minimum funkcji f znajduje się w przedziale $[F_7, F_8] = [13, 21]$. Dwoma punktami внутrenymi, odległymi o $F_4 = 3$ od brzegów tego przedziału, są: $x = 16$

i $x = 18$. Licząc wartość $f(18) = 7011,2 > f(16)$ stwierdzamy, że minimum funkcji f musi leżeć w przedziale $[13, 18]$. Kolejne dwa punkty wewnętrzne tego przedziału, wyznaczone tym razem przez wartość $F_3 = 2$, to $x = 15$ i $x = 16$. Ponieważ $f(15) = 2412,5 < f(16)$, stwierdzamy, że minimum funkcji f znajduje się w przedziale $[13, 16]$. Kolejna iteracja z użyciem $F_2 = 1$ daje dwa punkty wewnętrzne: $x = 14$ i $x = 15$. Liczymy nową wartość funkcji $f(14) = 2595,2$ i wiemy, że minimum f należy do przedziału $[14, 16]$. Długość tego przedziału jest równa $F_3 = 2$, a zatem pozostaje tylko jedna iteracja, wymagająca policzenia wartości funkcji w punkcie odległym o pewną niewielką wartość ϵ od środka przedziału czyli punktu $x = 15$. Biorąc na przykład $\epsilon = 0,1$ i licząc wartość f w punkcie $x = 15,1$ otrzymujemy $f(15,1) = 2431,69 > f(15)$, a zatem ostatecznie stwierdzamy, że minimum funkcji f musi leżeć w przedziale $[14, 15]$. Tak istotnie jest; funkcja f osiąga minimum w punkcie $x = 14,7827\dots$.

Zauważmy na koniec, że jeśli problem nasz polega na oszacowaniu przedziału, w którym leży minimum funkcji, zadaną z góry dokładnością, to stosując powyższy algorytm trzeba na początku dobrać odpowiednio dużą liczbę z ciągu Fibonacciego i dopiero na jej podstawie wyznaczyć wartość N . \square

Rozwiązywanie liniowych równań rekurencyjnych

Liniowym równaniem rekurencyjnym z zadanyimi warunkami początkowymi $a_0, a_1, \dots, a_{k-1} \in \mathbb{R}$, nazywamy zależność o postaci

$$a_i = q(i) + q_1 \cdot a_{i-1} + q_2 \cdot a_{i-2} + \dots + q_k \cdot a_{i-k}, \quad i \in \mathbb{N}, \quad (3.23)$$

gdzie q_1, \dots, q_k , są danymi liczbami rzeczywistymi, a $q(i)$ jest wartością danej funkcji rzeczywistej q dla argumentu i . Funkcja ta spełnia warunki

$$q(i) = a_i - \sum_{j=1}^i q_j \cdot a_{i-j}, \quad i = 0, 1, \dots, k-1.$$

Rozwiązaniem tego równania jest ciąg (a_i) , którego wyrazy spełniają zależność (3.23) przy dodatkowym założeniu, że $a_i = 0$ dla $i < 0$.

Zauważmy, że rozważana w poprzednim podrozdziale zależność (3.17) jest właśnie przykładem liniowego równania rekurencyjnego, w którym $a_0 = F_0 = 0$, $a_1 = F_1 = 1$, $a_i = F_i$ dla $i \geq 2$, $q_1 = q_2 = 1$ oraz $q(i) = [i = 1]$ dla $i \in \mathbb{N}$. Użyta tam technika może być z łatwością przeniesiona na przypadek równania (3.23) i pozwala na uzyskanie funkcji tworzącej poszukiwanego ciągu (a_i) .

3.1. FUNKCJE TWORZĄCE

Oznaczmy funkcję tworzącą ciągu (a_i) symbolem $A(z)$ i niech $A_0(z)$ oznacza funkcję tworzącą ciągu $(q(i))$. Podobnie jak poprzednio, zauważmy, że ciąg (a_i) jest – zgodnie z zależnością (3.23) – sumą ciągu $(q(i))$ oraz k -krotnie powtórzonego tego samego ciągu, przesuniętego o $j = 1, 2, \dots, k$, miejsc w prawo i przemnożonego odpowiednio przez stała q_k . Z omawianych wcześniej właściwości funkcji tworzących mamy więc:

$$A(z) = A_0(z) + q_1 \cdot zA(z) + q_2 \cdot z^2A(z) + \dots + q_k \cdot z^kA(z). \quad (3.24)$$

Z powyższego równania łatwo już po prostych przekształceniach wyznaczyć funkcję tworzącą $A(z)$. Otrzymujemy

$$A(z) = \frac{A_0(z)}{1 - q_1z - q_2z^2 - \dots - q_kz^k}. \quad (3.25)$$

Bardzo często mamy do czynienia z tak zwanym jednorodnym równaniem rekurencyjnym,⁵ w którym funkcja $q(i)$ jest równa zeru dla $i \geq k$. Wówczas funkcja tworząca ciągu $(q(i))$ ma postać

$$A_0(z) = q(0) + q(1)z + q(2)z^2 + \dots + q(k-1)z^{k-1},$$

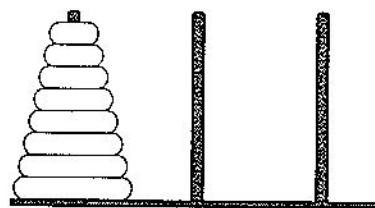
a zatem funkcją tworzącą ciągu rozwiązań jednorodnego równania rekurencyjnego z warunkami początkowymi a_0, a_1, \dots, a_{k-1} , jest następujące wyrażenie:

$$A(z) = \frac{q(0) + q(1)z + q(2)z^2 + \dots + q(k-1)z^{k-1}}{1 - q_1z - q_2z^2 - \dots - q_kz^k}.$$

Przykład 3.14 W znanej łamigłówce, zaproponowanej w roku 1883 przez francuskiego matematyka Edouarda Lucasa, nazywanej *problemem wież w Hanoi*, mamy do czynienia z trzema prętami oraz i krążkami różnej wielkości, umieszczonymi pierwotnie na jednym z prętów (patrz Rysunek 3.3).

Problem polega na przeniesieniu wszystkich krążków na inny pręt w minimalnej liczbie ruchów, przy czym w każdym ruchu można przenieść tylko jeden krążek oraz nie wolno kłaść większego krążka na mniejszym.

⁵Rozwiązywanie jednorodnego równania rekurencyjnego z użyciem funkcji tworzących podał w roku 1718 Abraham de Moivre.

Rysunek 3.3: Wieże w Hanoi dla $i = 8$.

Niech T_i oznacza minimalną liczbę ruchów, niezbędnych dla rozwiązania problemu z i krążkami. Łatwo pokazać, że T_i spełnia następujące równanie rekurencyjne:

$$T_i = 2T_{i-1} + 1, \quad i \in \mathbb{N}, i \geq 1, \quad (3.26)$$

z oczywistym warunkiem początkowym $T_0 = 0$. Zauważmy bowiem, że dla $i > 1$ musi zachodzić nierówność

$$T_i \leq 2T_{i-1} + 1,$$

wynikająca z faktu, że problem dla i krążków możemy rozwiązać (patrz Rysunek 3.4) dokonując najpierw przeniesienia $n - 1$ krążków (bez największego) na wolny pręt (w T_{i-1} ruchach), następnie przenosząc (w jednym ruchu) największy krążek na drugi z wolnych prętów, a na koniec układając na krążku największym $i - 1$ mniejszych krążków (w T_{i-1} ruchach). Musi również zachodzić nierówność odwrotna, tzn. $T_i \geq 2T_{i-1} + 1$. W chwili bowiem, gdy po raz pierwszy dokonujemy przeniesienia największego z krążków, to wówczas musimy już mieć za sobą co najmniej T_{i-1} ruchów związanych z przeniesieniem $i - 1$ pozostałych krążków na inny pręt. Pozostałe operacje, to znaczy przeniesienie największego krążka oraz ułożenie na nim pozostałych, również muszą pochłonąć co najmniej $(1 + T_{i-1})$ ruchów.

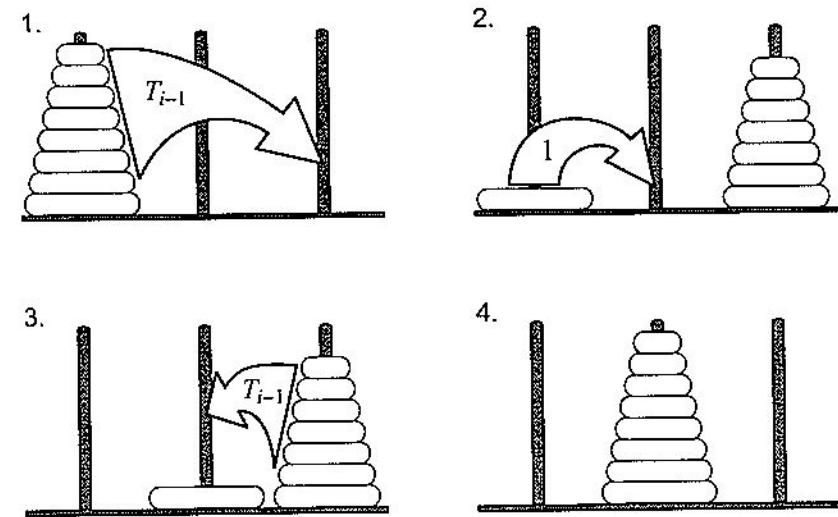
Równanie (3.26) z warunkiem $T_0 = 0$ jest szczególnym przypadkiem liniowego równania rekurencyjnego (3.23), w którym $a_i = T_i$ dla $i \in \mathbb{N}$, $q_1 = 2$ oraz

$$q(i) = 1 \cdot [i > 0] \quad \text{dla } i \in \mathbb{N}.$$

Mamy więc (przyjmując, że $T_k = 0$ dla $k < 0$):

$$T_i = q(i) + 2T_{i-1}, \quad i \in \mathbb{N}.$$

3.1. FUNKCJE TWORZĄCE



Rysunek 3.4: Zasada rekurencyjnego rozwiązywania problemu wież w Hanoi.

Niech $T(z)$ oznacza funkcję tworzącą poszukiwanego ciągu (T_i) i niech $T_0(z)$ będzie funkcją tworzącą ciągu $(q(i)) = (0, 1, 1, \dots, 1, \dots)$. Mamy zatem

$$T_0(z) = (1 - z)^{-1} - 1.$$

Podstawiając odpowiednie wielkości do wzoru (3.25) otrzymujemy następującą funkcję tworzącą ciągu (T_i) :

$$T(z) = z(1 - 2z)^{-1}(1 - z)^{-1}.$$

Po prostych przekształceniach powyższego wzoru mamy

$$T(z) = (1 - 2z)^{-1} - (1 - z)^{-1}.$$

Z własności funkcji tworzących wynika, że ciąg (T_i) jest sumą dwóch ciągów: ciągu (2^i) , którego funkcją tworzącą jest $(1 - 2z)^{-1}$, oraz ciągu (-1) , który ma funkcję tworzącą $-(1 - z)^{-1}$. Otrzymujemy zatem proste wyrażenie, podające dla dowolnego $i = 1, 2, \dots$, minimalną liczbę ruchów, niezbędną do rozwiązywania problemu i wież z Hanoi :

$$T_i = 2^i - 1.$$

□

3.2 Zasada włączania-wyłączania

W rozdziale tym omówimy drugą z ważnych technik, stosowanych często przy rozwiązywaniu zagadnień zliczania. Zacznijmy od prostego przykładu praktycznego zadania, w którym technika ta okazuje się pomocna.

Przykład 3.15 Rozważmy następujący problem: Zbadano 50 samochodów, sprawdzając trzy grupy emitowanych przez nie zanieczyszczeń:

- (a) – tlenki azotu (NO_x),
- (b) – węglowodorki (HC),
- (c) – tlenek węgla (CO).

W wyniku tych badań stwierdzono, że tylko jeden samochód nie spełnia żadnej z norm (a), (b), (c). Natomiast trzy samochody mają przekroczone normy (a) i (b), dwa – normy (a) i (c) oraz jeden – normy (b) i (c). Ponadto w sześciu samochodach stwierdzono przekroczenie normy (a), w czterech – normy (b) oraz w trzech – normy (c). Powstaje pytanie: Ille spośród badanych samochodów spełnia wszystkie normy?

□

Powyzsze zadanie jest typowym przykładem problemu, który łatwo jest rozwiązać stosując twierdzenie nazywane tradycyjnie *zasadą włączania-wyłączania*. Twierdzenie to dotyczy następującej sytuacji:

Dany jest zbiór skończony X oraz rodzina jego podzbiorów

$$\mathcal{A} = \{A_1, \dots, A_n\}.$$

Problem polega na wyznaczeniu liczności sumy mnogościowej wszystkich zbiorów rozważanej rodziny. Zauważmy, że jeśli elementy rodziny \mathcal{A} są parami rozłączne, to liczność zbioru $A_1 \cup \dots \cup A_n$ jest po prostu równa sumie liczności wszystkich zbiorów rodziny \mathcal{A} . W przeciwnym przypadku sytuacja jest nieco bardziej skomplikowana. Poniższe twierdzenie pozwala na wyznaczenie liczności zbioru $A_1 \cup \dots \cup A_n$, jeśli znane są liczności wszystkich możliwych przecięć zbiorów należących do rodziny \mathcal{A} , to znaczy liczności zbiorów

$$A_{p_1} \cap A_{p_2} \cap \dots \cap A_{p_i}$$

dla dowolnych indeksów p_1, p_2, \dots, p_i , gdzie $i = 1, \dots, n$, spełniających warunki

$$1 \leq p_1 < p_2 < \dots < p_i \leq n.$$

3.2. ZASADA WŁĄCZANIA-WYŁĄCZANIA

Twierdzenie 3.1 (Zasada włączania-wyłączania) Dla dowolnej niepustej rodziny zbiorów $\mathcal{A} = \{A_1, \dots, A_n\}$, której elementami są podzbiory zbioru skończonego X , zachodzi następująca zależność:

$$|\bigcup_{i=1}^n A_i| = \sum_{i=1}^n (-1)^{i-1} \sum_{1 \leq p_1 < p_2 < \dots < p_i \leq n} |A_{p_1} \cap A_{p_2} \cap \dots \cap A_{p_i}|. \quad (3.27)$$

Dowód. Dowiedziemy twierdzenia metodą indukcji względem liczby elementów rodziny \mathcal{A} . Dla $n = 1$ twierdzenie jest oczywiście prawdziwe. Przyjmijmy więc, że jest prawdziwe dla pewnego $n = k \geq 1$ i pokażemy, że jest wówczas prawdziwe dla $n = k + 1$. Zakładamy zatem, że

$$|\bigcup_{i=1}^k A_i| = \sum_{i=1}^k (-1)^{i-1} \sum_{1 \leq p_1 < p_2 < \dots < p_i \leq k} |A_{p_1} \cap A_{p_2} \cap \dots \cap A_{p_i}|. \quad (3.28)$$

Rozważmy sumę dwóch zbiorów: $\bigcup_{i=1}^k A_i$ oraz A_{k+1} . Mamy równość:

$$|\bigcup_{i=1}^{k+1} A_i \cup A_{k+1}| = |\bigcup_{i=1}^k A_i| + |A_{k+1}| - |\bigcup_{i=1}^k A_i \cap A_{k+1}|. \quad (3.29)$$

Ale z (3.28) wynika, że

$$|\bigcup_{i=1}^k A_i \cap A_{k+1}| = \sum_{i=1}^k (-1)^{i-1} \sum_{1 \leq p_1 < p_2 < \dots < p_i \leq k} |A_{p_1} \cap A_{p_2} \cap \dots \cap A_{p_i} \cap A_{k+1}|.$$

Wstawiając powyższe wyrażenie do (3.29) oraz zastępując w (3.29) składnik $|\bigcup_{i=1}^k A_i|$ prawą stroną równości (3.28) otrzymujemy po prostych przekształceniach:

$$|\bigcup_{i=1}^{k+1} A_i| = \sum_{i=1}^{k+1} (-1)^{i-1} \sum_{1 \leq p_1 < p_2 < \dots < p_i \leq k+1} |A_{p_1} \cap A_{p_2} \cap \dots \cap A_{p_i}|. \quad \blacksquare$$

Przykład 3.15 (kontynuacja)

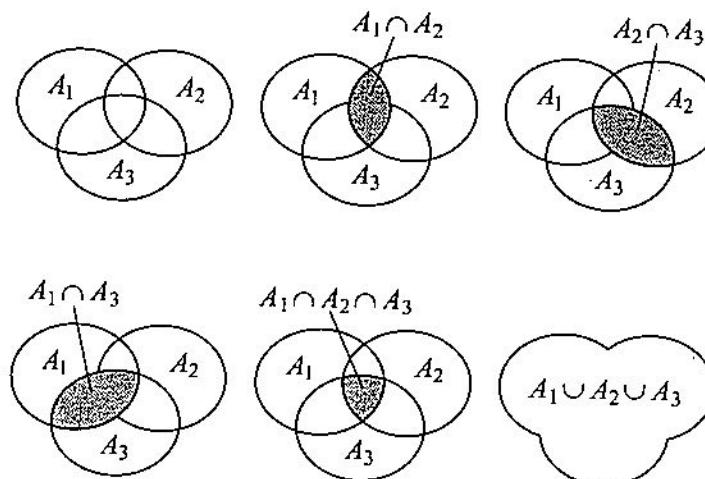
Twierdzenie 3.1 pozwala w łatwy sposób wyznaczyć liczbę samochodów spełniających wszystkie normy zanieczyszczeń. Niech A_1 , A_2 , A_3 będą zbiorami tych samochodów, które nie spełniają – odpowiednio – norm (a), (b), (c) (patrz Rysunek 3.5).

Wiemy, że $|A_1| = 6$, $|A_2| = 4$ oraz $|A_3| = 3$. Ponadto $|A_1 \cap A_2| = 3$, $|A_1 \cap A_3| = 2$ i $|A_2 \cap A_3| = 1$. Wiemy również, że $|A_1 \cap A_2 \cap A_3| = 1$. Zatem

z zasady włączania-wyłączania wynika, że liczba wszystkich samochodów, które nie spełniają jednej lub więcej norm, to znaczy liczba samochodów należących do zbioru $A_1 \cup A_2 \cup A_3$ jest równa:

$$|A_1 \cup A_2 \cup A_3| = 6 + 4 + 3 - 3 - 2 - 1 + 1 = 8.$$

Wynika stąd, że pozostałe 42 samochody spełniają wszystkie normy zańieczyszczeń. \square



Rysunek 3.5: Diagramy Venna dla zbiorów z Przykładu 3.15.

Zasada włączania-wyłączania może być użyta do rozwiązywania różnych zagadnień zliczania. W dalszej części tego rozdziału przedstawimy dwa takie zastosowania omawianego twierdzenia.

Zastosowanie zasady włączania-wyłączania do wyznaczania liczby surjekcji

Niech X i Y będą zbiorami skończonymi i niech $|X| = n$ oraz $|Y| = m$. W Rozdziale 2.6.2 podaliśmy twierdzenie, które pozwala na wyznaczenie liczby $s_{n,m}$ wszystkich surjekcji, należących do zbioru $\text{Fun}(X, Y)$. Mianowicie,

$$s_{n,m} = m! \begin{Bmatrix} n \\ m \end{Bmatrix}, \quad (3.30)$$

3.2. ZASADA WŁĄCZANIA-WYŁĄCZANIA

gdzie $\begin{Bmatrix} n \\ m \end{Bmatrix}$ jest liczbą Stirlinga drugiego rodzaju, to znaczy liczbą wszystkich podziałów zbioru n -elementowego na m -bloków.

Poniższe twierdzenie podaje zwartą formułę umożliwiającą obliczanie wartości $s_{n,m}$ bez odwoływanego się do tabeli liczb Stirlinga drugiego rodzaju.

Twierdzenie 3.2 Jeżeli $|X| = n$ oraz $|Y| = m$, gdzie $m > 0$, to liczba wszystkich surjekcji w zbiorze $\text{Fun}(X, Y)$ jest równa

$$s_{n,m} = \sum_{i=0}^{m-1} (-1)^i \binom{m}{i} (m-i)^n. \quad (3.31)$$

Dowód. Niech $Y = \{y_1, \dots, y_m\}$ i niech dla $i = 1, \dots, m$, symbol A_i oznacza podzbiór wszystkich takich funkcji $f \in \text{Fun}(X, Y)$, dla których $y_i \notin f(X)$. Zbiór $A_1 \cup \dots \cup A_m$ jest więc podzbiorem tych wszystkich funkcji ze zbioru $\text{Fun}(X, Y)$, które nie są surjekcjami. Ponieważ liczność całego zbioru $F(X, Y)$ jest równa m^n , to mamy równość

$$s_{n,m} = m^n - |A_1 \cup \dots \cup A_m|.$$

Aby skorzystać z zasady włączania-wyłączania do obliczenia wartości $|A_1 \cup \dots \cup A_m|$, należy wyznaczyć liczności zbiorów $A_{p_1} \cap \dots \cap A_{p_i}$ dla $i = 1, \dots, m$, $1 \leq p_1 < \dots < p_i \leq m$. Zauważmy, że

$$A_{p_1} \cap \dots \cap A_{p_i} = \text{Fun}(X, Y \setminus \{y_{p_1}, \dots, y_{p_i}\}),$$

a zatem $|A_{p_1} \cap \dots \cap A_{p_i}| = (m-i)^n$. Ponieważ podzbiór $\{y_{p_1}, \dots, y_{p_i}\}$ można wybrać ze zbioru Y na $\binom{m}{i}$ sposobów, to – wykorzystując zależność (3.27) – po prostych przekształceniach otrzymujemy:

$$\begin{aligned} s_{n,m} &= m^n - |A_1 \cup \dots \cup A_m| = \\ &= m^n - \sum_{i=1}^m (-1)^{i-1} \binom{m}{i} (m-i)^n = \\ &= \sum_{i=0}^{m-1} (-1)^i \binom{m}{i} (m-i)^n. \end{aligned}$$

Porównując wyrażenia (3.30) i (3.31), uzyskujemy następującą równość, która może być użyta do nierekurencyjnego wyznaczania liczb Stirlinga drugiego rodzaju:

$$\begin{Bmatrix} n \\ m \end{Bmatrix} = \frac{1}{m!} \sum_{i=0}^{m-1} (-1)^i \binom{m}{i} (m-i)^n. \quad (3.32)$$

Zastosowanie zasady włączania-wyłączania do wyznaczania liczb nieporządków

Rozważmy zbiór S_n wszystkich permutacji zbioru $\{1, \dots, n\}$.

Definicja 3.3 Nieporządkiem na zbiorze $\{1, \dots, n\}$ nazywamy dowolną permutację $f \in S_n$, spełniającą warunek

$$f(i) \neq i \quad \text{dla } i \in \{1, \dots, n\}.$$

Niech $D_n \subseteq S_n$ oznacza zbiór wszystkich nieporządków na zbiorze $\{1, \dots, n\}$. Poniższe twierdzenie pozwala na wyznaczenie liczności zbioru nieporządków.⁶

Twierdzenie 3.3 Dla $n \in \mathbb{N}$, gdzie $n \geq 1$,

$$|D_n| = n! \sum_{i=0}^n \frac{(-1)^i}{i!}. \quad (3.33)$$

Dowód. Niech

$$A_i = \{f \in S_n : f(i) = i\}, \quad i = 1, \dots, n.$$

Mamy więc:

$$|D_n| = |S_n| - |A_1 \cup \dots \cup A_n|.$$

Stosując zasadę włączania-wyłączania i podstawiając $|S_n| = n!$, otrzymujemy z powyższej równości następujące wyrażenie:

$$|D_n| = n! - \sum_{i=1}^n (-1)^{i-1} \sum_{1 \leq p_1 < \dots < p_i \leq n} |A_{p_1} \cap \dots \cap A_{p_i}|.$$

Dla dowolnego ciągu (p_1, \dots, p_i) , gdzie $1 \leq p_1 < \dots < p_i \leq n$, przecięcie $A_{p_1} \cap \dots \cap A_{p_i}$ jest zbiorem wszystkich tych permutacji $f \in S_n$, dla których $f(p_j) = p_j$ dla $j = 1, \dots, i$, a zatem

$$|A_{p_1} \cap \dots \cap A_{p_i}| = (n-i)!.$$

⁶Twierdzenie to zostało udowodnione z użyciem zasady włączania-wyłączania przez Abrahama de Moivre'a w roku 1718.

3.2. ZASADA WŁĄCZANIA-WYŁĄCZANIA

Ponieważ ciąg (p_1, \dots, p_i) , gdzie $1 \leq p_1 < \dots < p_i \leq n$, można wybrać na $\binom{n}{i}$ sposobów, otrzymujemy

$$\begin{aligned} |D_n| &= n! - \sum_{i=1}^n (-1)^{i-1} \binom{n}{i} (n-i)! = \\ &= \sum_{i=0}^n (-1)^i \frac{n!}{i!} = n! \sum_{i=0}^n \frac{(-1)^i}{i!}. \end{aligned}$$

W tabeli na Rysunku 3.6 podane są liczby nieporządków w zbiorach S_n dla $n = 1, \dots, 20$.

| n | $ D_n $ |
|-----|--------------------|
| 1 | 0 |
| 2 | 1 |
| 3 | 2 |
| 4 | 9 |
| 5 | 44 |
| 6 | 265 |
| 7 | 1854 |
| 8 | 14833 |
| 9 | 133496 |
| 10 | 1334961 |
| 11 | 14684570 |
| 12 | 176214841 |
| 13 | 2290792932 |
| 14 | 32071101049 |
| 15 | 481066515734 |
| 16 | 7697064251745 |
| 17 | 130850092279664 |
| 18 | 2355301661033953 |
| 19 | 44750731559645106 |
| 20 | 895014631192902121 |

Rysunek 3.6: Liczba nieporządków w S_n dla $n = 1, \dots, 20$.

Traktując liczności $|D_n|, |S_n|$, to znaczy liczności zbiorów wszystkich nieporządków oraz wszystkich permutacji, jako funkcje zmiennej n i licząc granice ilorazu $|D_n|/|S_n|$ dla $n \rightarrow \infty$, otrzymujemy następujący wniosek:

Wniosek 3.1 *Dla $n \rightarrow \infty$ udział nieporządków w zbiorze S_n wszystkich permutacji zbioru $\{1, \dots, n\}$ dąży do wartości*

$$e^{-1} = \sum_{i=0}^{\infty} (-1)^i \frac{1}{i!} \approx 0,36787944\dots,$$

gdzie $e \approx 2,71828183\dots$ jest podstawą logarytmów naturalnych.

Udział nieporządków w zbiorze wszystkich permutacji zbiega bardzo szybko do granicznej wartości e^{-1} ; na przykład dla $n = 10$ wartość ilorazu $|D_{10}|/|S_{10}|$ jest równa około 0,36787946.

Twierdzenie 3.3 i powyższy Wniosek przekonują nas, że udział nieporządków w zbiorze wszystkich permutacji jest zaskakująco duży. Poniższy przykład ilustruje zastosowanie tego faktu w praktycznym problemie.

Przykład 3.16 Założymy, że zdajemy test, w którym danych jest pięć pytań i pięć odpowiedzi na te pytania. Wiadomo, że w zbiorze odpowiedzi jest dokładnie jedna poprawna odpowiedź na każde z pytań oraz że dana odpowiedź pasuje tylko do jednego pytania. Zadanie polega na przyporządkowaniu wszystkich odpowiedzi do pytań. Wynik testu jest pozytywny, jeśli przynajmniej jedna odpowiedź jest poprawnie dopasowana do pytania. Mamy więc łącznic $5! = 120$ możliwych przyporządkowań odpowiedzi do pytań, odpowiadających zbiorowi wszystkich permutacji zbioru pięcioelementowego. Wynik testu jest negatywny, jeśli żadna odpowiedź nie jest poprawnie przyporządkowana, co odpowiada nieporządkowi na zbiorze $\{1, \dots, 5\}$. Z zależności (3.33) wynika, że

$$|D_5| = 5! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!}\right) = 44.$$

A zatem dobierając losowo odpowiedzi do pytań mamy aż 44 szanse na 120, że wynik tego pozornie prostego testu będzie negatywny. \square

3.3. ZASADA SZUFLADKOWA

3.3 Zasada szufladkowa

W rozdziale tym omówimy zastosowania bardzo prostego twierdzenia, nazywanego zwykle *zasadą szufladkową* albo *zasadą Dirichleta*.⁷ W najprostszej postaci wyraża ono oczywisty fakt, że jeśli chcemy rozmieścić n obiektów w m szufladach i $n > m$, to w przynajmniej jednej szufladzie musi się znaleźć więcej niż jeden obiekt. Poniższe twierdzenie formuluje tę obserwację w nieco ogólniejszej postaci.

Twierdzenie 3.4 *Jeśli X oraz Y są niepustymi zbiorami skończonymi i $f \in \text{Fun}(X, Y)$ oraz $|X| > r \cdot |Y|$ dla pewnego $r > 0$, to co najmniej jeden ze zbiorów $f^{-1}(\{y\})$, $y \in Y$, ma więcej niż r elementów.*

Dowód. Rozważmy rodzinę zbiorów $\{f^{-1}(\{y\}), y \in Y\}$, czyli tak zwane jądro funkcji f (patrz strona 47.). Zauważmy, że niepuste elementy tej rodziny stanowią podział zbioru X na k bloków A_1, \dots, A_k , gdzie $k \leq |Y|$. Wartość średnia liczności zbiorów A_i , $i = 1, \dots, k$, jest równa $\frac{1}{k} \cdot (|A_1| + \dots + |A_k|) = \frac{1}{k} \cdot |X|$. Zatem najliczniejszy ze zbiorów A_i , $i = 1, \dots, k$, musi mieć co najmniej $\lceil \frac{1}{k} \cdot |X| \rceil$ elementów. A ponieważ $k \leq |Y|$ oraz $|X| > r \cdot |Y|$, to taki zbiór ma więcej niż r elementów. ■

Zasada szufladkowa pozwala na łatwe uzasadnianie różnych faktów, które często mogą wydawać się zaskakujące lub trudne do udowodnienia. Poniżej podam kilka przykładów (patrz np. [2]) użycia zasady szufladkowej.

Przykład 1.

Wybierzmy dowolne dziesięć różnych liczb naturalnych dodatnich, mniejszych od 107. Można pokazać, że istnieją dwa rozłączne podzbiory tych liczb, które mają takie same sumy elementów.

Uzasadnienie powyższego faktu na podstawie zasady szufladkowej jest bardzo łatwe. Założymy, że wybraliśmy dowolne dziesięć różnych dodatnich liczb naturalnych mniejszych niż 107. Niech X będzie rodziną wszystkich podzbiorów tego zbioru liczb. Oczywiście, mamy $|X| = 2^{10} = 1024$. Ponadto, niech Y oznacza zbiór wszystkich możliwych sum elementów w takich podzbiorach. Łatwo zauważyć, że zbiór Y musi być podzbiorem liczb naturalnych z przedziału $[1, 1015]$, bowiem największa suma dziesięciu liczb naturalnych mniejszych niż 107 jest równa

$$97 + 98 + \dots + 106 = 1015.$$

⁷Odsłownie niemieckiego matematyka Lejeuna P. G. Dirichleta (1805-1859).

Mamy więc zależność $|X| > r \cdot |Y|$, gdzie $r = 1$. Niech $f : X \rightarrow Y$ będzie funkcją, która przyporządkowuje każdemu zbiorowi rodziny X sumę należących do niego liczb. Z Twierdzenia 3.4 wynika, że istnieje taka liczba $y \in Y$, że dla co najmniej dwóch elementów rodziny X (oznaczmy je symbolami S' i S'') zachodzi zależność $f(S') = f(S'') = y$, to znaczy sumy liczb w tych zbiorach są równe. A zatem dwoma rozłącznymi podzbiorami zbioru liczb naturalnych z przedziału $[1, 1015]$, mającymi identyczne sumy elementów, są $S' \setminus S''$ oraz $S'' \setminus S'$. \square

Przykład 2.

Niech A będzie dowolnym dziesięcioelementowym podzbiorem zbioru $\{1, 2, \dots, 50\}$. Chcemy pokazać, że w zbiorze A istnieją dwa różne podzbiory pięcioelementowe, dla których sumy elementów są równe.

Oznaczmy symbolem X rodzinę wszystkich pięcioelementowych podzbiorów zbioru A . Mamy więc $|X| = \binom{10}{5} = 252$. Niech Y oznacza zbiór wszystkich możliwych sum elementów dla zbiorów należących do X .

Łatwo zauważyc, że Y musi być podzbiorem liczącego 226 elementów zbioru $\{15, 16, \dots, 240\}$, bowiem najmniejsza wartość sumy pięciu liczb ze zbioru $\{1, 2, \dots, 50\}$ jest równa $15 = 1 + 2 + 3 + 4 + 5$, a największa, odpowiednio, $240 = 50 + 49 + 48 + 47 + 46$. Zatem $|X| > |Y|$ i – tak jak w poprzednim przykładzie – muszą istnieć co najmniej dwa podzbiory: S' oraz S'' , należące do X i mające tę samą sumę elementów. \square

Przykład 3.

Rozważmy zbiór n osób, z których część wita się ze sobą przez podanie rąk. Założmy, że żadna para osób nie wita się ze sobą więcej niż jeden raz oraz że nikt nie wita się ze samym sobą. Stosując zasadę szufladkową uzasadnimy, że istnieją co najmniej dwie osoby, które ściskły tę samą liczbę dloni.

Tak istotnie jest. Niech bowiem X będzie rozważanym zbiorem osób i niech $f(x) \in Y = \{0, 1, \dots, n-1\}$ oznacza liczbę powitań osoby x z tego zbioru. Mamy więc $|X| = n$ oraz $|Y| = n$, a zatem nie jest tu spełniony warunek $|X| > |Y|$, pozwalający na zastosowanie zasady szufladkowej. Zauważmy jednak, że $f(X) \neq Y$, bowiem nie jest możliwa sytuacja, że istnieje zarówno osoba, która nie witała się z nikim, jak i równocześnie inna osoba, która wymieniła $n-1$ uścisków dloni. Możemy więc mieć do czynienia albo z przypadkiem, gdy $f : X \rightarrow Y \setminus \{0\}$, albo z przypadkiem $f : X \rightarrow Y \setminus \{n-1\}$. W każdej z tych sytuacji możemy zastosować zasadę szufladkową, wnioskując, że dla co najmniej dwóch osób wartości funkcji f są identyczne. \square

3.3. ZASADA SZUFLADKOWA

Przykład 4. Założmy, że a_1, \dots, a_n , są dowolnie wybranymi dodatnimi liczbami naturalnymi. Użyjemy zasady szufladkowej do uzasadnienia, że w każdym takim zbiorze n liczb naturalnych istnieje taki ich podzbiór, że suma liczb w tym podzbiorze jest podzielna przez n .

Niech $X = \{\{a_1\}, \{a_1, a_2\}, \dots, \{a_1, a_2, \dots, a_n\}\}$ i niech dla $S \in X$ wartość funkcji $f(S)$ będzie resztą z dzielenia sumy liczb w podzbiorze S przez n . Zbiorem możliwych reszt jest zatem n -elementowy zbiór $Y = \{0, 1, \dots, n-1\}$. Mogą zajść dwa przypadki:

1^o W zbiorze X istnieje podzbiór S , dla którego $f(S) = 0$ i jest on właśnie poszukiwanym podzbiorem, w którym suma liczb jest podzielna przez n .

2^o Takiego podzbioru nie ma, a zatem wówczas $f : X \rightarrow Y \setminus \{0\}$. Możemy więc zastosować zasadę szufladkową i stwierdzić, że w tym przypadku muszą istnieć w zbiorze X dwa podzbiory S' i S'' , dla których spełniona jest zależność $f(S') = f(S'')$. A z tego już łatwo wynika, że suma liczb w podzbiorze $S' \otimes S''$ jest podzielna przez n . \square

Ważnym i głębokim rozwinięciem zasady szufladkowej jest tak zwana teoria Ramsey'a (patrz na przykład [2, 12]).

Rozdział 4

Elementy ogólnej teorii zliczania

4.1 Wprowadzenie

Zacznijmy od dwóch typowych przykładów problemów, które rozwiązuje się metodami omawianymi w niniejszym rozdziale.

Przykład 4.1 Na jednym z egzaminów nasi studenci rozwiązywali (wyłącznie teoretycznie) następujące zadanie:

Agentka S przekazuje Tajne Wiadomości agentowi (specjalnemu) M stosując kod węzełkowy. Polega to na tym, że wysyła mu swoją pończochę, mającą osiem ustalonych, dobrze znanych agentowi S, miejsc (dla treści zadania nie jest istotne - skąd). Na każdym z tych miejsc agentka S może zawiązać węzeł albo nie. Kłopot z agentem (specjalnym) M jest taki, że nie jest on w stanie zapamiętać, gdzie jest początek, a gdzie koniec pończochy. Ile w związku z tym różnych Tajnych Wiadomości agentka S może przekazać agentowi M?

Każda kodowana wiadomość odpowiada tu pewnej funkcji ze zbioru ośmiu miejsc w zbiór dwuelementowy. Łatwo jednak zauważyc, że liczba różnych wiadomości, które można zakodować w sposób opisany w powyższym przykładzie, jest mniejsza niż liczba wszystkich funkcji ze zbioru ośmioelementowego w zbiór dwuelementowy, bowiem niektóre z tych funkcji musimy traktować jak „równoważne”.

W tym konkretnym przypadku liczba wszystkich funkcji ze zbioru ośmioelementowego w zbiór dwuelementowy jest równa, oczywiście, $2^8 = 256$,

ale – jak się okaże w punkcie 4.2.1 (patrz str. 127) – jedynie 136 spośród nich odpowiada „różnym wiadomościom”. \square

Z podobną sytuacją mamy do czynienia w poniższym przykładzie.

Przykład 4.2 Cząstki chemiczne, które mają ten sam skład, ale różną strukturę połączeń między atomami, nazywane są izomerami. Założmy, że interesują nas izometry organiczne, w których występuje sześć atomów węgla (C), połączonych w tak zwany pierścień aromatyczny (patrz Rysunek 4.1). Ponadto przyjmijmy, że do każdego z atomów węgla dołączony jest¹ dokładnie jeden atom wodoru (H) albo innego pierwiastka, który oznaczymy symbolem (R). Każda z takich cząsteczek ma ten sam wzór chemiczny $C_6H_iR_{6-i}$, ale ich struktury przestrzenne – a przez to również ich właściwości – mogą być różne.

Na Rysunku 4.1 pokazane są przykłady trzech możliwych izomerów benenu, w których liczba podstawianych atomów wodoru jest równa 2, a pierwiastkiem (R) jest chlor (Cl).



Rysunek 4.1: Przykłady izomerów benenu o wzorze chemicznym $C_6H_4Cl_2$.

Naszym celem jest policzenie wszystkich możliwych izomerów o postaci $C_6H_iR_{6-i}$ dla dowolnej liczby naturalnej $i = 1, \dots, 6$. Każda z cząstek o takim składzie chemicznym, zawierająca ponadto pierścień aromatyczny, jest reprezentowana przez funkcję, która wskazuje, jakie pierwiastki

¹W terminologii chemicznej mówimy, że pierścień aromatyczny jest „podstawiany” atomami pierwiastków lub związkami chemicznymi.

są podstawiane w wierzchołkach pierścienia. Jednakże musimy uwzględnić fakt, że niektóre z tych funkcji są „równoważne”, bowiem wyznaczają te same – z dokładnością do obrotów – struktury przestrzenne cząsteczek. \square

Oba podane wyżej przykłady mają wspólną cechę. Należy mianowicie policzyć, ile jest różnych, zadanych w pewien określony sposób, podzbiorów funkcji przy założeniu, że funkcje należące do każdego z tych podzbiorów traktujemy jako równoważne. Aby zdefiniować, jak rozumiemy w poszczególnych przypadkach tę „równoważność”, konieczne będzie omówienie właściwości szczególnej klasy funkcji, nazywanych *permutacjami*.

4.1.1 Permutacje i grupy permutacji

Rozdział ten jest przede wszystkim przygotowaniem do teorii zliczania, której podstawowe elementy przedstawione są w Rozdziałach 4.2 i 4.3. W teorii tej permutacje odgrywają zasadniczą rolę. Należy jednak podkreślić, że permutacje są również bardzo ważne w różnego rodzaju zastosowaniach matematyki dyskretniej. Dzieje się tak dlatego, że wiele praktycznych zadań z zakresu badań operacyjnych daje się sformułować jako zadania optymalizacyjne na zbiorach permutacji (patrz na przykład [14, 26, 32]). Niektóre z tych problemów zostaną zasygnalizowane w następnych rozdziałach.

Przypomnijmy, że permutacją zbioru n -elementowego X nazywamy dowolną funkcję różnicową $f : X \rightarrow X$. Funkcję taką można przedstawić na wiele sposobów. Ponieważ permutacja f jest pewną relacją w zbiorze X , to takimi sposobami jej zapisu mogą być na przykład graf relacji f albo tablica relacji f .

W dalszych rozważaniach często będziemy się posługiwać wygodnym zapisem permutacji f w postaci tablicy, w której górnym wierszu umieszczone są elementy zbioru X , to znaczy argumenty funkcji f , a pod nimi w dolnym wierszu wypisywane są odpowiednie wartości funkcji f dla tych argumentów.

Przykład 4.3 Niech $X = \{a, b, c, d\}$ oraz $f(a) = d, f(b) = a, f(c) = c, f(d) = b$. Łatwo sprawdzić, że – istotnie – funkcja $f : X \rightarrow X$ jest permutacją zbioru X , bowiem jest funkcją różnicową. Zapis permutacji f w postaci tablicy jest następujący:

$$f = \begin{pmatrix} a & b & c & d \\ d & a & c & b \end{pmatrix}.$$

\square

W ogólnym przypadku kolejność wypisywania elementów górnego wiersza tablicy jest całkowicie dowolna. Zauważmy jednak, że jeśli wszystkie elementy zbioru X są uporządkowane, to wówczas permutacja f jest w sposób jednoznaczny określona poprzez podanie wektora, który jest dolnym wierszem tablicy. W omawianym wyżej przykładzie – przy leksykograficznym uporządkowaniu elementów zbioru X (traktowanego jako podzbiór liter alfabetu łacińskiego) – jest to wektor (d, a, c, b) . Będziemy więc w tym przypadku pisać $f = (d, a, c, b)$.

W dalszej części tego rozdziału najczęściej będziemy mieli do czynienia z sytuacją, gdy $X = \{1, \dots, n\}$. W tym przypadku permutacje zbioru X są po prostu n -elementowymi ciągami różnowartościowymi o wyrazach ze zbioru X , a permutację $f : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ identyfikujemy jednoznacznie z wektorem (a_1, \dots, a_n) , gdzie $a_i = f(i)$, dla $i = 1, \dots, n$.

Zbiór wszystkich $n!$ permutacji zbioru $\{1, \dots, n\}$ będziemy oznaczać symbolem S_n .

Permutacje składamy w taki sam sposób, jak inne funkcje. Wynikiem złożenia dwóch permutacji f i g ze zbioru S_n jest również – co łatwo sprawdzić – permutacja należąca do S_n , którą oznaczamy symbolem fg . Zgodnie z zasadą składania funkcji mamy:

$$fg(i) = f(g(i)) \text{ dla } i = 1, \dots, n.$$

Podobnie jak w przypadku innych funkcji, przy składaniu permutacji f i g , permutację f nazywamy permutacją *zewnętrzną*, natomiast permutację g – permutacją *wewnętrzna*.

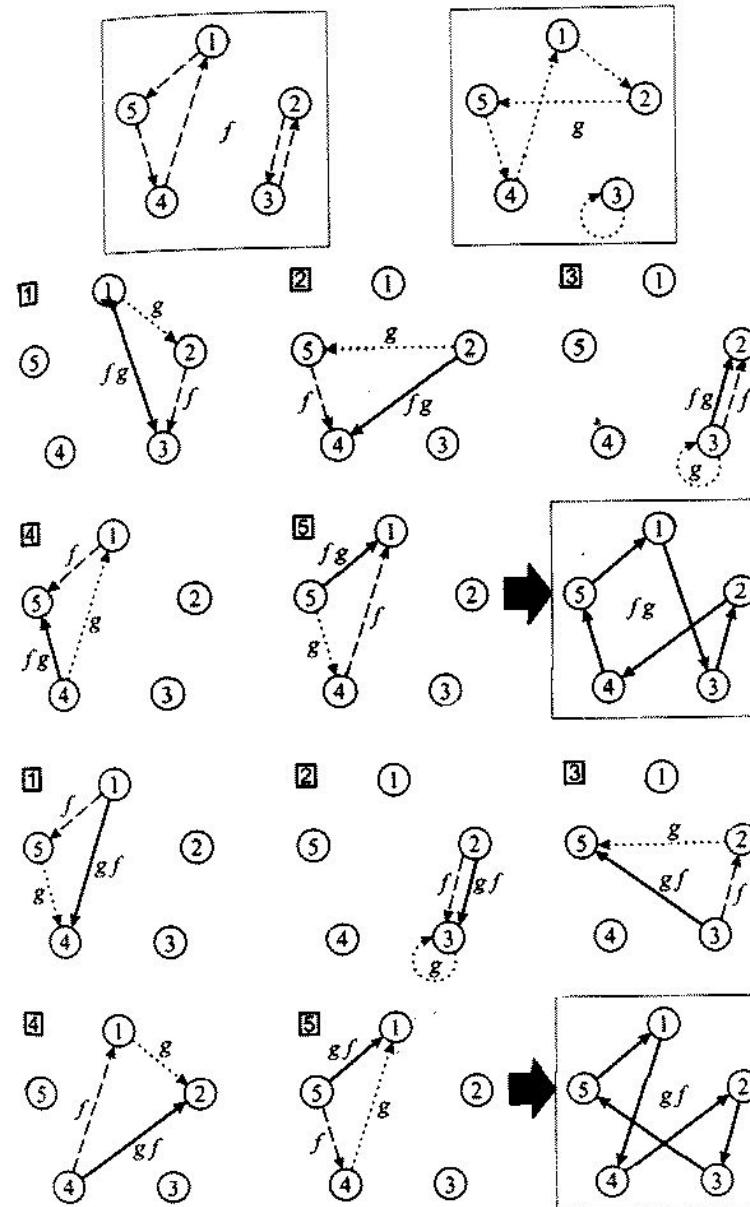
Przy składaniu permutacji istotna jest ich kolejność. Zatem w ogólnym przypadku permutacja fg jest różna od permutacji gf , co pokazuje poniższy przykład.

Przykład 4.4 Rozważmy dwie permutacje f oraz g zbioru $\{1, \dots, n\}$, gdzie

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}.$$

Złożeniem permutacji f i g jest następująca permutacja fg :

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



Rysunek 4.2: Rysunki grafów permutacji f i g z Przykładu 4.4 i kolejne kroki, wykonywane przy składaniu f z g oraz g z f . Łuki w grafach wynikowych permutacji są zaznaczone liniami ciągłymi.

Natomiast złożeniem permutacji g i f jest permutacja gf , gdzie

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

Rysunek 4.2 ilustruje kolejne kroki wykonywane przy składaniu permutacji f z g oraz g z f . \square

Złożenie permutacji jest przykładem tak zwanego *działania dwuargumentowego*.²

Definicja 4.1 Jeśli S oraz T są danymi zbiorami, to działaniem dwuargumentowym na zbiorze S nazywamy dowolną funkcję ze zbioru $S \times S$ w zbiór T .

Zauważmy, że w ogólnym przypadku zbory S i T nie muszą być różne. W przypadku składania permutacji mamy $S = T = S_n$.

Zwykle dla oznaczenia działania dwuargumentowego stosujemy specjalny symbol (na przykład $*$, $+$, $-$ itp.). Na oznaczenie faktu, że element $c \in T$ jest wartością funkcji $*$ dla argumentu, będącego parą uporządkowaną $(a, b) \in S \times S$, piszemy $a * b = c$. W przypadku złożenia permutacji dla uproszczenia zapisu nie stosujemy symbolu działania, co jest zgodne z naszą konwencją oznaczania permutacji będącej wynikiem złożenia.

Zbiór permutacji S_n z działaniem złożenia ma pewne właściwości, które są bardzo istotne w dalszych rozważaniach. Omówimy je kolejno, pomijając proste dowody podawanych faktów.

Wyróżnionym elementem zbioru S_n jest tak zwana *permutacja identycznościowa*, oznaczana symbolem e , dla której $e(i) = i$ dla każdego $i \in \{1, \dots, n\}$, to znaczy

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Zauważmy, że przy składaniu permutacji identycznościowej z dowolną permutacją ze zbioru S_n nie jest istotna kolejność permutacji, bowiem dla każdego $f \in S_n$ mamy

$$ef = fe = f. \quad (4.1)$$

²Inną stosowaną tu nazwą jest: *operacja binarna*.

Permutacje są przykładem funkcji, dla których istnieje funkcja odwrotna.

Definicja 4.2 Permutację odwrotną do permutacji $f \in S_n$ nazywamy permutację $f^{-1} \in S_n$, spełniającą warunek $f^{-1}f = e$.

Zauważmy, że dla każdej permutacji $f \in S_n$ permutacja odwrotna jest określona jednoznacznie. Jeśli bowiem

$$\text{-- } f = \begin{pmatrix} \dots & i & \dots \\ \dots & j & \dots \end{pmatrix}, \text{ to } f^{-1} = \begin{pmatrix} \dots & j & \dots \\ \dots & i & \dots \end{pmatrix}.$$

Zatem na przykład permutacją odwrotną do rózważanej wyżej permutacji

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

jest permutacja

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}.$$

Latwo jest również pokazać, że dla dowolnej permutacji i jej permutacji odwrotnej kolejność składania obu tych funkcji nie jest istotna, to znaczy

$$f^{-1}f = ff^{-1} = e. \quad (4.2)$$

Zauważmy ponadto, że dla dowolnych permutacji $f, g \in S_n$ zachodzi zależność

$$(fg)^{-1} = g^{-1}f^{-1}, \quad (4.3)$$

obowiązująca dla tych wszystkich funkcji, dla których istnieją odpowiednie funkcje odwrotne.

Rozważmy teraz trzy dowolne permutacje $f, g, h \in S_n$. Nietrudno dowieść, że zarówno w wyniku złożenia permutacji f z permutacją gh , jak i w wyniku złożenia permutacji fg z permutacją h otrzymujemy ten sam element zbioru S_n , tzn.

$$f(gh) = (fg)h. \quad (4.4)$$

Oznacza to, że składanie permutacji jest działaniem łącznym.

Spełnienie warunków (4.1), (4.2) oraz (4.4) świadczy o tym, że dla dowolnego $n \in \mathbb{N}$, $n > 0$, zbiór permutacji S_n z działaniem złożenia tworzy tak zwaną grupę (patrz np. [24]).

Definicja 4.3 Parę uporządkowaną $(S, *)$, gdzie S jest zbiorem, a symbol $*$ oznacza działanie dwuargumentowe na tym zbiorze, nazywamy grupą, jeśli spełnione są następujące warunki:

- (i) dla dowolnych $a, b \in S$ mamy $a * b \in S$;
- (ii) dla dowolnych $a, b, c \in S$ zachodzi zależność $(a * b) * c = a * (b * c)$;
- (iii) istnieje taki element $e \in S$, że dla każdego $a \in S$ mamy $a * e = a$;
- (iv) dla każdego $a \in S$ istnieje taki element $a^{-1} \in S$, że $a * a^{-1} = e$.

Liczność zbioru S nazywamy *rzędem grupy* $(S, *)$. Element e zbioru S , spełniający warunek (iii) powyżej definicji, nazywamy *elementem neutralnym grupy*. Element a^{-1} , dla którego $a * a^{-1} = e$, nazywamy *elementem odwrotnym* elementu a .

Łatwo pokazać, że element neutralny grupy jest wyznaczony jednoznacznie oraz że dla każdego elementu grupy istnieje dokładnie jeden element odwrotny.

Jeśli rząd grupy spełnia warunek $|S| < \infty$, to grupę taką nazywamy *grupą skończoną*. Teoria grup skończonych stanowi bardzo ważny i rozbudowany dział matematyki dyskretnej. W dalszym ciągu będą nam potrzebne jedynie najbardziej podstawowe pojęcia z tego zakresu.

Zauważmy, że zbiór permutacji S_n z działaniem złożenia spełnia istotnie wszystkie warunki Definicji 4.3.

Grupa S_n występuje w wielu zastosowaniach i jest nazywana *grupą symetryczną stopnia n*.

Może się zdarzyć, że również dla pewnego podzbioru właściwego zbioru S_n spełnione są wszystkie warunki z definicji grupy. Dlatego wprowadzimy pojęcie *grupy permutacji stopnia n*:

Definicja 4.4 Grupą permutacji stopnia n nazywamy dowolny podzbiór $G \subseteq S_n$, spełniający następujące warunki:

- (i) $f \in G \wedge g \in G \Rightarrow fg \in G$ dla wszystkich $f, g \in G$;
- (ii) $f \in G \Rightarrow f^{-1} \in G$ dla każdego $f \in G$.

Przykład 4.5 Rozważmy zbiór $S_4 = \{\pi_1, \dots, \pi_{24}\}$, składający się ze wszystkich permutacji zbioru $\{1, 2, 3, 4\}$. Niech $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ będzie podzbiorem zbioru S_4 , przy czym

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},$$

4.1. WPROWADZENIE

$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \quad \pi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Łatwo sprawdzić, że zbiór G z działaniem złożenia jest grupą permutacji stopnia 4. Wystarczy bowiem pokazać, że permutacja $\pi_i \pi_j$ jest elementem zbioru G dla dowolnych $i, j = 1, 2, 3, 4$ oraz że $\pi_i^{-1} \in G$ dla każdego $i = 1, 2, 3, 4$. Tak istotnie jest, bowiem z faktu, że π_1 jest permutacją identycznościową mamy:

$$\pi_1 \pi_i = \pi_i \pi_1 = \pi_i \text{ dla } i = 1, 2, 3, 4.$$

Sprawdzając kolejno wszystkie możliwe pary i, j dla $i, j \in \{2, 3, 4\}$, otrzymujemy w każdym przypadku jako wynik złożenia permutacji element zbioru G . Na przykład:

$$\pi_2 \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \pi_1,$$

$$\pi_2 \pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \pi_4,$$

$$\pi_2 \pi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \pi_3.$$

Łatwo również sprawdzić, że dla każdego $i = 1, 2, 3, 4$, mamy $\pi_i^{-1} = \pi_i$, a zatem spełnione są warunki (i) i (ii) z Definicji 4.4. \square

4.1.2 Rozkład permutacji na cykle

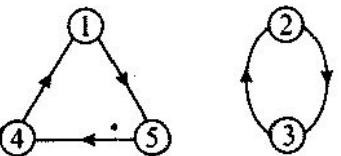
W rozdziale tym wszystkie rozważania dotyczą permutacji ze zbioru S_n . Tym niemniej fakty tu dowodzone pozostają prawdziwe dla permutacji dowolnego zbioru uporządkowanego. Ograniczenie się do zbioru S_n upraszcza nieco zapisy.

Zacznijmy od prostego przykładu permutacji $f \in S_5$, gdzie

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

Permutacja f jest relacją binarną w zbiorze $X = \{1, 2, 3, 4, 5\}$. Możemy więc narysować jej graf (następna strona 6). Jest on przedstawiony na

Rysunku 4.3. Zawiera pięć wierzchołków, odpowiadających elementom zbioru X , oraz pięć łuków, łączących te wierzchołki. Ponieważ permutacja f jest odwzorowaniem wzajemnie jednoznacznym zbioru X na siebie, to z każdego wierzchołka, odpowiadającego elementowi $x \in X$, wychodzi dokładnie jeden łuk do wierzchołka, który reprezentuje element $f(x) \in X$. Jednocześnie, do każdego wierzchołka $y \in X$ dochodzi dokładnie jeden łuk prowadzący z wierzchołka $f^{-1}(y)$.



Rysunek 4.3: Grafi permutacji $f = (5, 3, 2, 1, 4)$.

Charakterystyczną cechą grafi z Rysunku 4.3 jest to, że składa się on z fragmentów, z których każdy jest zamknięta, skierowaną drogą, prowadzącą przez pewien podzbiór wierzchołków grafi.³ Okazuje się, że nie jest to sytuacja przypadkowa i że każdy grafi permutacji ma tego typu strukturę. Wiąże się to z ważną cechą permutacji, a mianowicie z możliwością tak zwanego rozkładu permutacji na cykle rozłączne.

Niech k będzie liczbą naturalną, spełniającą warunki $1 \leq k \leq n$. Rozważmy dowolny k -elementowy ciąg różnowartościowy $(a_{i_1}, \dots, a_{i_k})$ o wyrazach w zbiorze $\{1, \dots, n\}$.

Definicja 4.5 Permutację $\pi \in S_n$ nazywamy cyklem wyznaczonym przez ciąg różnowartościowy $(a_{i_1}, \dots, a_{i_k})$ o wyrazach w zbiorze $\{1, \dots, n\}$, jeśli spełnione są następujące warunki:

$$\pi(a_{i_j}) = a_{i_{j+1}} \quad \text{dla } j = 1, \dots, k-1;$$

$$\pi(a_{i_k}) = a_{i_1};$$

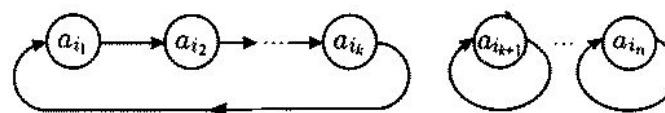
$$\pi(a_l) = a_l \quad \text{dla } l \neq i_1, \dots, i_k.$$

³Droga taka w języku teorii grafiów (patrz np. [16], str. 22) nosi nazwę cyklu. Ten sam termin jest stosowany na określenie pewnej permutacji, wyznaczonej przez ten podzbiór wierzchołków.

4.1. WPROWADZENIE

Dla ustalonej liczby naturalnej n oraz $k \leq n$, permutację, będącą cyklem wyznaczonym przez ciąg $(a_{i_1}, \dots, a_{i_k})$, oznaczamy symbolem $[a_{i_1}, \dots, a_{i_k}]$. Liczbę k nazywamy długością cyklu. Zauważmy przy tym, że dowolny ciąg jednoelementowy o wartościach w zbiorze $\{1, \dots, n\}$ wyznacza permutację identycznościową w S_n .

Jeśli narysujemy grafi cyklu $[a_{i_1}, \dots, a_{i_k}]$ ze zbioru S_n , gdzie $k > 1$, to zauważymy, że składa on się z jednego cyklu o długości k oraz $n - k$ cykli o długości 1 (patrz Rysunek 4.4). Cykle o długości 1 na rysunku grafi permutacji nazywamy pętlami.



Rysunek 4.4: Grafi permutacji, będącej cyklem wyznaczonym przez ciąg $(a_{i_1}, \dots, a_{i_k})$.

Cykle wyznaczone przez ciągi $(a'_{i_1}, \dots, a'_{i_k})$ oraz $(a''_{i_1}, \dots, a''_{i_l})$ nazywamy cyklami rozłącznymi, jeśli $\{a'_{i_1}, \dots, a'_{i_k}\} \cap \{a''_{i_1}, \dots, a''_{i_l}\} = \emptyset$. Cykle rozłączne odpowiadają właśnie fragmentom, na które rozpadła się grafi permutacji.⁴

W przypadku permutacji f , której grafi jest przedstawiony na Rysunku 4.3, mamy dwa cykle rozłączne: $f' = [1, 5, 4]$ oraz $f'' = [2, 3]$.

Zauważmy, że jeśli złożymy permutacje f', f'' , w dowolnej kolejności, to w wyniku otrzymamy zawsze permutację f . Łatwo się o tym przekonać wypisując obie permutacje w postaci tablicowej. Mamy bowiem

$$f' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}, \quad f'' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$$

oraz

$$\begin{aligned} f'f'' &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix} = f. \end{aligned}$$

⁴W języku teorii grafiów fragmenty te nazywane są składowymi spójnymi grafiu.

Podobnie,

$$\begin{aligned} f''f' &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix} = f. \end{aligned}$$

Fakt powyższy możemy zapisać w następującej postaci:

$$f = [1, 5, 4][2, 3] = [2, 3][1, 5, 4].$$

Tak jest również w ogólnym przypadku, bowiem łatwo można pokazać, że wynik złożenia dwóch dowolnych cykli rozłącznych nie zależy od kolejności ich składania. Zauważmy również, że dla dowolnej permutacji $f \in S_n$ zbiór cykli rozłącznych występujących w jej grafie jest wyznaczony jednoznacznie. Uzasadnione jest w związku z tym przyjęcie następującej definicji:

Definicja 4.6 Rozkładem permutacji $f \in S_n$ na cykle rozłączne nazywamy zbiór wszystkich cykli parami rozłącznych, występujących w grafie permutacji f .

Rozkład na cykle rozłączne permutacji f ze zbioru S_n zawiera od jednego do n elementów. Z pierwszą sytuacją mamy do czynienia w przypadku permutacji, która sama jest cyklem o długości n , natomiast druga dotyczy permutacji identycznościowej.

Dla dowolnej liczby naturalnej k z przedziału $[1, n]$ zachodzi następujące twierdzenie, którego dowód można znaleźć na przykład w [10]:

Twierdzenie 4.1 Liczba permutacji ze zbioru S_n , których rozkład na cykle rozłączne zawiera dokładnie k elementów, gdzie $1 \leq k \leq n$, jest równa liczbie Stirlinga pierwszego rodzaju $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$.

Prostym wnioskiem z tego twierdzenia jest następująca tożsamość:

$$\sum_{k=1}^n \left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right] = n!.$$

W zastosowaniach permutacji istotną rolę odgrywa pojęcie typu permutacji. Mówimy mianowicie, że permutacja $f \in S_n$ jest typu $(\lambda_1, \dots, \lambda_n)$,

4.1. WPROWADZENIE

jeśli jej rozkład na cykle rozłączne zawiera dokładnie λ_i cykli o długości i dla $i = 1, \dots, n$.

Typ permutacji będziemy również podawać w postaci następującego równoważnego zapisu:

$$1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}.$$

Często, dla uproszczenia, będziemy pomijać w takim zapisie elementy i^{λ_i} , dla których $\lambda_i = 0$.

Przykład 4.6 Rozważmy permutację $f \in S_9$, gdzie

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

Rozkład tej permutacji na cykle rozłączne ma postać:

$$f = [1, 7, 6, 3][2, 5][4][8, 9].$$

Permutacja f jest więc typu $(1, 2, 0, 1, 0, 0, 0, 0, 0)$, co możemy również zapisać w postaci $1^1 2^2 4^1$. \square

Definicja 4.7 Inwersją permutacji $f = (a_1, \dots, a_n) \in S_n$ nazywamy parę (a_i, a_j) , dla której $i < j \leq n$ oraz $a_i > a_j$.

Liczبę wszystkich inwersji permutacji f oznaczamy symbolem $I(f)$.

Definicja 4.8 Znakiem permutacji $f \in S_n$ nazywamy liczbę $sgn(f)$, gdzie

$$sgn(f) = (-1)^{I(f)}.$$

Permutację f nazywamy permutacją parzystą, jeśli $sgn(f) = 1$, albo permutacją nieparzystą, jeśli $sgn(f) = -1$.

Przykład 4.7 Rozważmy ponownie permutację $f \in S_5$, gdzie

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

Inwersjami tej permutacji są następujące pary: $(5,3), (5,2), (5,1), (5,4), (3,2), (3,1)$ oraz $(2,1)$. Zatem $I(f) = 7$ i $sgn(f) = (-1)^7 = -1$. Permutacja f jest więc permutacją nieparzystą. \square

Obliczenie znaku permutacji $f \in S_n$ bezpośrednio z Definicji 4.8 wymaga w ogólnym przypadku sprawdzenia wszystkich możliwych par elementów (a_i, a_j) , $i, j = 1, \dots, n$, $i \neq j$, co prowadzi do algorytmu o złożoności obliczeniowej $O(n^2)$. Możliwe jest jednak skonstruowanie znacznie lepszego algorytmu dla obliczenia znaku permutacji. Konstrukcja tego algorytmu jest związana z własnościami pewnych szczególnych permutacji w zbiorze S_n , nazywanych transpozycjami.

Definicja 4.9 Transpozycję nazywamy permutację, która jest cyklem o długości 2.

Zauważmy, że permutacją odwrotną do dowolnej transpozycji jest ta sama permutacja. Jeśli permutacja jest transpozycją o postaci $[i, i+1]$ dla pewnego $i \in \{1, \dots, n-1\}$, to taką permutację nazywamy *transpozycją sąsiednich elementów*.

Twierdzenie 4.2 Dowolną permutację $f \in S_n$ można przedstawić w postaci złożenia $I(f)$ transpozycji sąsiednich elementów.

Dowód. Zauważmy najpierw, że jeśli $f = (a_1, \dots, a_n)$ oraz $t = [i, i+1]$ dla pewnego $i = 1, \dots, n-1$, to $ft = (a_1, \dots, a_{i-1}, a_{i+1}, a_i, a_{i+2}, \dots, a_n)$. Wprowadźmy dla $i = 1, \dots, n$, następujące oznaczenie:

$$r_i = |\{j \in \{1, \dots, n\} : j < f^{-1}(i) \text{ oraz } a_j > i\}|.$$

Wartość r_i jest więc liczbą wszystkich inwersji permutacji f , w których element i jest następnikiem, to znaczy inwersji o postaci (j, i) dla $j > i$. Stąd wynika, że $r_1 + \dots + r_n = I(f)$.

Zauważmy teraz, że element i , gdzie $i = 1, \dots, n$, stojący w wektorze (a_1, \dots, a_n) na pozycji $f^{-1}(i)$, można sprowadzić na pozycję i -tą dokonując r_i transpozycji sąsiednich elementów. Powtarzając takie postępowanie dla $i = 1, \dots, n$, otrzymamy po $I(f) = r_1 + \dots + r_n$ krokach permutację identycznościową $(1, 2, \dots, n)$. Oznacza to, że $ft_1 \dots t_{I(f)} = e$, gdzie $t_1, \dots, t_{I(f)}$ są pewnymi transpozycjami sąsiednich elementów. Stąd, korzystając z zależności (4.3) i uwzględniając fakt, że dla dowolnej transpozycji t zachodzi równość $t^{-1} = t$, otrzymujemy

$$f = (t_1 \dots t_{I(f)})^{-1} = t_{I(f)}^{-1} \dots t_1^{-1} = t_{I(f)} \dots t_1.$$

Przykład 4.8 Rozważmy permutację $f \in S_5$, gdzie $f = (2, 4, 3, 5, 1)$. Mamy tu $r_1 = 4$, $r_2 = 0$, $r_3 = 1$, $r_4 = 0$, $r_5 = 0$ oraz $I(f) = 5$.

Zacznijmy od sprowadzenia elementu 1, znajdującego się na pozycji $f^{-1}(1) = 5$, na pozycję 1. Możemy tego dokonać składając permutację f kolejno z następującymi transpozycjami sąsiednich elementów: $[4, 5]$, $[3, 4]$, $[2, 3]$, $[1, 2]$. Wynikiem tych operacji jest permutacja $f' = [1, 2, 4, 3, 5]$.

Aby uzyskać permutację identycznościową wystarczy teraz zamienić elementy 3 i 4, stojące w f' odpowiednio na pozycjach 4 i 3. Dokonujemy tego składając f' z transpozycją $[3, 4]$. Z dowodu Twierdzenia 4.2 wynika teraz, że

$$f = ([4, 5][3, 4][2, 3][1, 2][3, 4])^{-1} = [3, 4][1, 2][2, 3][3, 4][4, 5].$$

□

Zanim udowodnimy twierdzenie, które pozwala na skonstruowanie efektywnego algorytmu wyznaczania znaku permutacji, wykażemy kilka prostych twierdzeń pomocniczych związanych ze znakami permutacji.

Twierdzenie 4.3 Dla dowolnych permutacji $f, g \in S_n$,

$$\operatorname{sgn}(fg) = \operatorname{sgn}(f) \cdot \operatorname{sgn}(g).$$

Dowód. Jeśli g jest transpozycją sąsiednich elementów, tzn. $g = t$, gdzie $t = [i, i+1]$, oraz $f = (a_1, \dots, a_n)$, to wówczas

$$fg = ft = (a_1, \dots, a_{i-1}, a_{i+1}, a_i, \dots, a_n),$$

a zatem

$$I(fg) = I(ft) = \begin{cases} I(f) + 1 & \text{jeśli } a_i < a_{i+1}, \\ I(f) - 1 & \text{jeśli } a_i > a_{i+1}. \end{cases}$$

Stąd wynika, że dla dowolnej transpozycji t sąsiednich elementów

$$\operatorname{sgn}(ft) = -\operatorname{sgn}(f).$$

Na podstawie Twierdzenia 4.2 dowolną permutację g można przedstawić w postaci

$$g = t_1 \dots t_{I(g)},$$

gdzie $t_1, \dots, t_{I(g)}$, są transpozycjami sąsiednich elementów, a zatem

$$\operatorname{sgn}(fg) = \operatorname{sgn}(f t_1 \dots t_{I(g)}) = \operatorname{sgn}(f) \cdot (-1)^{I(g)} = \operatorname{sgn}(f) \cdot \operatorname{sgn}(g).$$

Zauważmy, że jeśli $g = f^{-1}$, to w wyniku złożenia f i g otrzymujemy permutację identycznościową, dla której liczba inwersji jest równa zero, a zatem jest ona permutacją parzystą. Otrzymujemy więc następujący prosty wniosek:

Wniosek 4.1 Dla dowolnej permutacji $f \in S_n$,

$$\operatorname{sgn}(f^{-1}) = \operatorname{sgn}(f).$$

Z dowodu Twierdzenia 4.3 wynika też, że jeśli permutacja t jest transpozycją sąsiednich elementów, to jest ona permutacją nieparzystą. Poniższe twierdzenie mówi, że tak jest również dla dowolnej transpozycji.

Twierdzenie 4.4 Każda transpozycja jest permutacją nieparzystą.

Dowód. Rozważmy dowolną transpozycję $[i, j]$, gdzie $i, j \in \{1, \dots, n\}$, $i < j$, to znaczy

$$[i, j] = (1, \dots, i-1, j, i+1, \dots, j-1, i, j+1, \dots, n).$$

Dokonajmy zamiany elementów i oraz j w transpozycji $[i, j]$ poprzez złożenie jej z transpozycjami sąsiednich elementów. W wyniku otrzymamy permutację identycznościową. W tym celu najpierw dokonamy złożenia transpozycji $[i, j]$ kolejno z następującymi transpozycjami sąsiednich elementów:

$$[j-1, j], [j-2, j-1], \dots, [i, i+1].$$

Liczba tych transpozycji jest równa $j - i$. W wyniku otrzymujemy permutację o postaci

$$\pi = (1, \dots, i-1, i, j, i+1, \dots, j-1, j+1, \dots, n).$$

Aby z powyższej permutacji otrzymać permutację identycznościową należy ją złożyć kolejno z następującymi transpozycjami sąsiednich elementów:

$$[i+1, i+2], [i+2, i+3], \dots, [j-1, j].$$

Powyższa sekwencja zawiera $j - i - 1$ transpozycji. Zatem łączna liczba transpozycji sąsiednich elementów, które doprowadzają transpozycję $[i, j]$ do permutacji identycznościowej, jest równa $2(j-i)-1$. Jest to zawsze liczba nieparzysta, a ponieważ złożenie z każdą transpozycją sąsiednich elementów powoduje zmianę znaku, to z tego wynika, że transpozycja $[i, j]$ jest permutacją nieparzystą. ■

Twierdzenie 4.5 Znak cyklu o długości k jest równy $(-1)^{k-1}$ dla dowolnego $k \geq 1$.

Dowód. Rozważmy permutację $[a_1, \dots, a_k]$, będącą cyklem o długości k . Latwo sprawdzić, że

$$[a_1, \dots, a_k] = [a_1, a_2][a_2, a_3] \dots [a_{k-1}, a_k].$$

Zatem każdy cykl o długości k jest złożeniem $k-1$ transpozycji. Z Twierdzeń 4.3 oraz 4.4 wynika więc, że jego znak jest równy $(-1)^{k-1}$. ■

Twierdzenie 4.6 Znak dowolnej permutacji f typu $1^{\lambda_1} \dots n^{\lambda_n}$ wyraża się wzorem

$$\operatorname{sgn}(f) = (-1)^{\sum_{j=1}^{\lfloor n/2 \rfloor} \lambda_{2j}}. \quad (4.5)$$

Dowód. Permutacja typu $1^{\lambda_1} \dots n^{\lambda_n}$ ma w rozkładzie na cykle rozłączne dokładnie λ_i cykli o długości i dla $i = 1, \dots, n$. Z Twierdzeń 4.5 i 4.3 wynika więc, że

$$\operatorname{sgn}(f) = \prod_{i=1}^n \left[(-1)^{i-1} \right]^{\lambda_i} = \prod_{j=1}^{\lfloor n/2 \rfloor} (-1)^{\lambda_{2j}} = (-1)^{\sum_{j=1}^{\lfloor n/2 \rfloor} \lambda_{2j}}.$$

Przykład 4.9 Rozważmy permutację

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

Rozkładając tę permutację na cykle rozłączne otrzymujemy

$$f = [1 \ 7 \ 6 \ 3][2 \ 5][4][8 \ 9].$$

Permutacja f jest więc typu $1^1 2^2 4^1$. Z Twierdzenia 4.6 mamy teraz

$$\operatorname{sgn}(f) = (-1)^{\sum_{j=1}^4 \lambda_{2j}} = (-1)^{\lambda_2 + \lambda_4 + \lambda_6 + \lambda_8} = (-1)^{2+1} = -1.$$

Permutacja f jest zatem permutacją nieparzystą. \square

Twierdzenie 4.6 prowadzi do bardzo prostego algorytmu wyznaczania znaku permutacji. Aby skorzystać ze wzoru (4.5) wystarczy znać jedynie liczbę cykli o parzystej długości w rozkładzie permutacji na cykle rozłączne. Rozkład ten może być dokonany algorymem o złożoności $O(n)$, a tym samym również znak permutacji można wyznaczyć algorytem o liniowej złożoności obliczeniowej.

4.2 Orbity działania grupy permutacji

Niech S będzie dowolnym zbiorem skończonym i niech G oznacza pewną grupę permutacji zbioru S . Zdefiniujmy w zbiorze S relację R_G w sposób następujący:

$$aR_G b \text{ dla } a, b \in S \Leftrightarrow \text{istnieje taka permutacja } \pi \in G, \text{ że } \pi(a) = b.$$

Tak zdefiniowaną relację nazwiemy *relacją indukowaną* w zbiorze S przez grupę G . Będziemy mówić również, że grupa G działa na zbiorze S .

Przykład 4.10 Niech $S = \{1, 2, 3, 4\}$ i niech $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$, gdzie

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix},$$

$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \quad \pi_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

W Przykładzie 4.5 sprawdziliśmy, że – istotnie – G jest grupą permutacji zbioru S . Na Rysunku 4.5 przedstawiona jest tablica relacji R_G indukowanej w zbiorze S przez grupę G . \square

Łatwo sprawdzić, że relacja R_G z Przykładu 4.10 jest relacją równoważności. Wskazuje na to blokowo-diagonalna postać tablicy relacji R_G . Okazuje się, że tak jest zawsze w przypadku dowolnej relacji indukowanej przez grupę. Zachodzi bowiem następujące twierdzenie:

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | x | x | | |
| 2 | x | x | | |
| 3 | | | x | x |
| 4 | | | x | x |

Rysunek 4.5: Tablica relacji R_G indukowanej w zbiorze $S = \{1, 2, 3, 4\}$ przez grupę $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ z Przykładu 4.10.

Twierdzenie 4.7 Relacja binarna $R_G \subseteq S \times S$, która jest relacją indukowaną w zbiorze S przez grupę permutacji G tego zbioru, jest relacją równoważności.

Dowód. Należy wykazać, że relacja R_G jest zwrotna, przechodnia i symetryczna. Kolejno pokażemy, że relacja R_G ma wszystkie te cechy.

(i) Relacja R_G jest zwrotna, to znaczy dla każdego $s \in S$ mamy $sR_G s$, bowiem grupa G zawiera permutację identycznościową e , dla której $e(s) = s$ dla dowolnego $s \in S$.

(ii) Dla wykazania, że relacja R_G jest przechodnia należy dowieść, że dla każdej trójki $a, b, c \in S$, z faktu, iż $aR_G b$ oraz $bR_G c$, wynika, że $aR_G c$. Tak istotnie jest, bowiem warunki $aR_G b$ oraz $bR_G c$ oznaczają, że istnieją permutacje π' oraz π'' , należące do G i takie, że $\pi'(a) = b$ oraz $\pi''(b) = c$. Ale skoro G jest grupą, to permutacja $\pi = \pi''\pi'$ należy do G , a ponieważ $\pi(a) = c$, to oznacza to, że $aR_G c$, a zatem relacja R_G jest przechodnia.

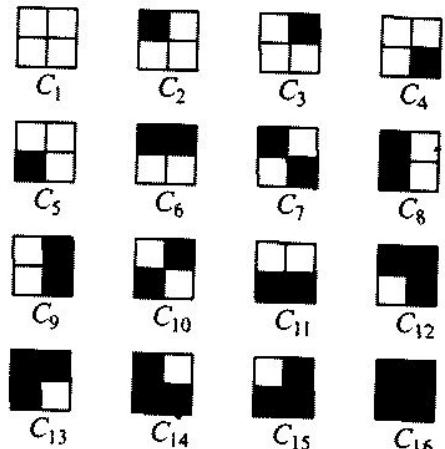
(iii) Aby pokazać, że relacja R_G jest symetryczna, wystarczy zauważyc, że z faktu, iż G jest grupą wynika, że dla każdej permutacji $\pi \in G$ istnieje w G permutacja odwrotna π^{-1} . Tym samym z faktu, że $aR_G b$, co jest równoważne temu, że dla pewnego $\pi \in G$ mamy $\pi(a) = b$, wynika, że $bR_G a$, bowiem $\pi^{-1}(b) = a$. ■

Każda relacja równoważności w zbiorze S dzieli ten zbiór na klasy abstrakcji (patrz strona 7). W przypadku relacji R_G te klasy abstrakcji mają specjalną nazwę:

Definicja 4.10 Elementy zbioru S/R_G , to znaczy zbioru klas abstrakcji relacji indukowanej przez grupę G działającą na zbiorze S , nazywamy orbitami działania grupy G .

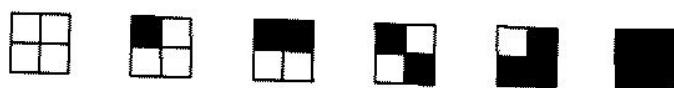
Liczبę orbit działania grupy G będziemy oznaczać symbolem $o(G)$. Wyznaczenie liczby orbit jest celem rozważań w dalszej części tego rozdziału. Poniższy przykład ilustruje praktyczną wagę tego problemu.

Przykład 4.11 Rozważmy zbiór $S = \{C_1, \dots, C_{16}\}$ szesnastu biało-czarnych tablic, pokazanych na Rysunku 4.6.



Rysunek 4.6: Rysunek tablic z Przykładu 4.11.

Załóżmy, że chcemy przekazać przy pomocy tych tablic możliwie największą liczbę wiadomości w sytuacji, gdy dopuszczać możliwość obrotów tych tablic. W tej sytuacji niektóre z tablic musimy traktować jak „równoważne”, ponieważ po dokonaniu odpowiednich obrotów nie potrafimy ich odróżnić. Dlatego na przykład cztery tablice: C_2, C_3, C_4 oraz C_5 , mogą kodować tylko jedną wiadomość. Podobnie jest z tablicami C_6, C_8, C_9 i C_{11} . Okazuje się, że w zbiorze 16 tablic istnieje jedynie 6 różnych „wzorów”, pokazanych na Rysunku 4.7. Łatwo sprawdzić, że wszystkie



Rysunek 4.7: Wszystkie różne „wzory” tablic z Przykładu 4.11.

pozostałe tablice jesteśmy w stanie uzyskać z tych „wzorów” przez obroty odpowiednio o $0^\circ, 90^\circ, 180^\circ$ i 270° zgodnie z ruchem wskazówek zegara.

4.2. ORBITY DZIAŁANIA GRUPY PERMUTACJI

Oznaczmy symbolami $\{\pi_1, \pi_2, \pi_3, \pi_4\}$ permutacje zbioru S , odpowiadające tym obrotom (patrz Rysunek 4.8).

$$\pi_1 = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} \\ C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} \\ C_1 & C_3 & C_4 & C_5 & C_2 & C_9 & C_{10} & C_6 & C_{11} & C_7 & C_8 & C_{15} & C_{12} & C_{13} & C_{14} & C_{16} \end{pmatrix}$$

$$\pi_3 = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} \\ C_1 & C_4 & C_5 & C_2 & C_3 & C_{11} & C_7 & C_9 & C_8 & C_{10} & C_6 & C_{14} & C_{15} & C_{12} & C_{13} & C_{16} \end{pmatrix}$$

$$\pi_4 = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 & C_5 & C_6 & C_7 & C_8 & C_9 & C_{10} & C_{11} & C_{12} & C_{13} & C_{14} & C_{15} & C_{16} \\ C_1 & C_5 & C_2 & C_3 & C_4 & C_8 & C_{10} & C_{11} & C_6 & C_7 & C_9 & C_{13} & C_{14} & C_{15} & C_{12} & C_{16} \end{pmatrix}$$

Rysunek 4.8: Permutacje, odpowiadające obrotom tablic o $0^\circ, 90^\circ, 180^\circ$ i 270° z Przykładu 4.11.

Łatwo zauważyc, że zbiór permutacji $\{\pi_1, \pi_2, \pi_3, \pi_4\}$ z działaniem złożenia tworzy grupę; oznaczmy ją symbolem G . Klasy abstrakcji S/R_G , czyli orbity działania tej grupy na zbiorze S , odpowiadają właściwie różnym „wzorom”, których możemy użyć do zakodowania różnych sześciu wiadomości.

Rysunek 4.9 przedstawia tablicę relacji R_G indukowanej w zbiorze S przez grupę obrotów G . Aby uwidoczyć blokowo-diagonalną strukturę tej tablicy, zbiór S został odpowiednio uporządkowany, a wierszom i kolumnom przyporządkowano odpowiednie rysunki tablic. Rysunek 4.10 przedstawia wszystkie orbity działania grupy G na zbiorze S . □

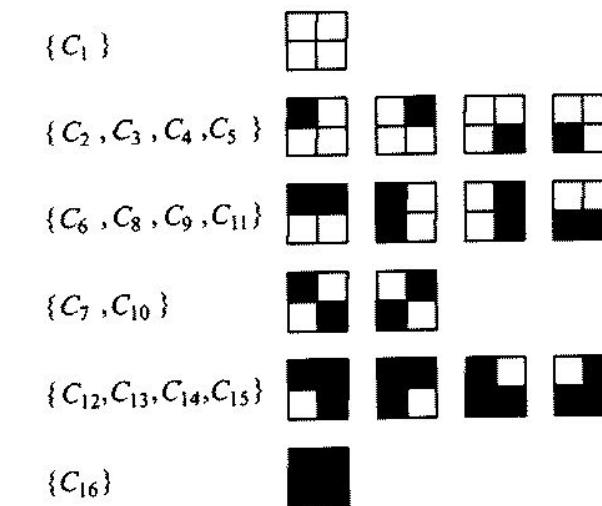
4.2.1 Liczba orbit działania grupy

Rozważmy zbiór skończony S i grupę permutacji G , działającą na tym zbiorze. W rozdziale tym udowodnimy twierdzenie, które pozwala na wyznaczenie liczby wszystkich orbit grupy G . W tym celu potrzebne jest wyznaczenie liczby wszystkich punktów stałych dla każdej z permutacji należącej do grupy G . Takie punkty stałe noszą nazwę *niezmienników permutacji* i są definiowane w sposób identyczny, jak w przypadku innych funkcji.

| | C_1 | C_2 | C_3 | C_4 | C_5 | C_6 | C_8 | C_9 | C_{11} | C_7 | C_{10} | C_{12} | C_{13} | C_{14} | C_{15} | C_{16} |
|----------|-------|-------|-------|-------|-------|-------|-------|-------|----------|-------|----------|----------|----------|----------|----------|----------|
| C_1 | X | | | | | | | | | | | | | | | |
| C_2 | | X | X | X | X | | | | | | | | | | | |
| C_3 | | X | X | X | X | | | | | | | | | | | |
| C_4 | | X | X | X | X | | | | | | | | | | | |
| C_5 | | X | X | X | X | | | | | | | | | | | |
| C_6 | | | | | | X | X | X | X | | | | | | | |
| C_8 | | | | | | X | X | X | X | | | | | | | |
| C_9 | | | | | | X | X | X | X | | | | | | | |
| C_{11} | | | | | | X | X | X | X | | | | | | | |
| C_7 | | | | | | | | | X | X | | | | | | |
| C_{10} | | | | | | | | | X | X | | | | | | |
| C_{12} | | | | | | | | | | | X | X | X | X | | |
| C_{13} | | | | | | | | | | | X | X | X | X | | |
| C_{14} | | | | | | | | | | | X | X | X | X | | |
| C_{15} | | | | | | | | | | | X | X | X | X | | |
| C_{16} | | | | | | | | | | | | | | | X | |

Rysunek 4.9: Tablica relacji R_G indukowanej przez grupę obrotów G z Przykładu 4.11.

4.2. ORBITY DZIAŁANIA GRUPY PERMUTACJI



Rysunek 4.10: Orbity działania grupy obrotów G na zbiorze tablic z Przykładu 4.11.

Definicja 4.11 Element $s \in S$ nazywamy niezmiennikiem permutacji π zbioru S , jeśli $\pi(s) = s$.

Liczبę niezmienników permutacji π będziemy oznaczać symbolem $Inv(\pi)$.

Przykład 4.12 Rozważmy raz jeszcze zbiór $S = \{C_1, \dots, C_{16}\}$ tablic pokazanych na Rysunku 4.6 oraz grupę permutacji $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ z Rysunku 4.8, działającą na tym zbiorze. Z tego ostatniego rysunku łatwo odczytać niezmienniki wszystkich permutacji, należących do grupy G . Mianowicie, zbiór niezmienników permutacji identycznościowej π_1 liczy szesnaście elementów, bowiem niezmiennikiem tej permutacji jest dowolny element zbioru S . Niezmiennikami permutacji π_2 oraz π_4 są te same dwa elementy C_1 oraz C_{16} zbioru S , bowiem mamy zarówno $\pi_2(C_1) = C_1$ oraz $\pi_2(C_{16}) = C_{16}$, jak i $\pi_4(C_1) = C_1$, $\pi_4(C_{16}) = C_{16}$. Natomiast zbiorem niezmienników permutacji π_3 jest czteroelementowy zbiór $\{C_1, C_7, C_{10}, C_{16}\}$.

Zauważmy też, że bardzo łatwo jest wypisać niezmienniki dowolnej permutacji, jeśli dysponujemy rysunkiem grafu tej permutacji. Niezmiennikom odpowiadają bowiem wszystkie te wierzchołki grafu, dla których istnieją pętle. □

Znajomość liczby niezmienników dla wszystkich permutacji, tworzących daną grupę G działającą na zbiorze S , pozwala na łatwe wyznaczenie liczności zbioru S/R_G , czyli liczby $o(G)$ wszystkich orbit działania grupy. Zachodzi następujące twierdzenie, nazywane zwykle Lematem Burnside'a⁵ albo Twierdzeniem o Zliczaniu Orbit.

Twierdzenie 4.8 *Liczba klas abstrakcji, na które relacja równoważności indukowana przez grupę G działającą na zbiorze S , dzieli ten zbiór, dana jest równością*

$$o(G) = \frac{1}{|G|} \sum_{\pi \in G} Inv(\pi). \quad (4.6)$$

Dowód. Niech dla $s \in S$, $\eta(s)$ oznacza liczbę permutacji grupy G , dla których element s jest niezmiennikiem⁶. Mamy oczywiście równość

$$\sum_{\pi \in G} Inv(\pi) = \sum_{s \in S} \eta(s).$$

Niech a oraz b będą dowolnymi elementami zbioru S , należącymi do tej samej klasy abstrakcji relacji R_G . Pokażemy, że istnieje dokładnie $\eta(a)$ permutacji odwzorowujących element a w element b .

Tak istotnie jest; skoro bowiem oba elementy a, b należą do tej samej klasy abstrakcji, to w grupie G musi istnieć permutacja (nazwijmy ją π_{ab}), dla której $\pi_{ab}(a) = b$. Niech $\{\pi^1, \dots, \pi^{\eta(a)}\}$ będzie zbiorem wszystkich permutacji, dla których element a jest niezmiennikiem. Wówczas zbiór $\Pi_{ab} = \{\pi_{ab}\pi^1, \dots, \pi_{ab}\pi^{\eta(a)}\}$ jest zbiorem wszystkich permutacji, które odwzorowują element a w element b . Aby to pokazać, wystarczy zauważyć, że składając z permutacją π_{ab} różne permutacje zbioru $\{\pi^1, \dots, \pi^{\eta(a)}\}$ otrzymujemy w wyniku takiego złożenia także różne permutacje. Ponadto, dla żadnej permutacji π ze zbioru $G \setminus \Pi_{ab}$ nie może zachodzić równość $\pi(a) = b$. Gdyby bowiem tak było, to mielibyśmy $\pi_{ab}^{-1}\pi(a) = \pi_{ab}^{-1}b = a$, a to pociągałoby zależność $\pi_{ab}(\pi_{ab}^{-1}\pi) = \pi \in \Pi_{ab}$, co byłoby sprzeczne z założeniem, że permutacja π jest wybierana ze zbioru $G \setminus \Pi_{ab}$.

Istnieje zatem dokładnie $\eta(a)$ permutacji, które odwzorowują element a w element b . Ponieważ b został wybrany jako dowolny element należący

⁵Od nazwiska matematyka brytyjskiego Williama Burnside'a (1852-1927), który przytoczył ten fakt w wydanej w roku 1911 książce dotyczącej teorii grup skończonych. Twierdzenie to było jednak znane już wcześniej na przykład z prac Georga Frobeniusa (1848-1917) i jest elementarnym faktem w teorii grup.

⁶Permutacje te bywają czasem nazywane stabilizatorami elementu s .

do klasy abstrakcji a/R_G , to znaczy, że liczba permutacji odwzorowujących a w każdy z elementów z a/R_G jest taka sama i równa $\eta(a)$. Każda permutacja z G musi odwzorowywać a w jakiś element z a/R_G , a zatem w przypadku, gdy $|a/R_G| = k$, mamy $\eta(a) = |G|/k$ dla dowolnego $a \in a/R_G$. Sumując wartości $\eta(s)$ dla wszystkich elementów z dowolnej klasy abstrakcji, zawsze otrzymujemy więc w wyniku rząd grupy G .

Rozciągając to sumowanie na wszystkie elementy zbioru S i dzieląc wynik przez rząd grupy G otrzymamy liczbę orbit $o(G)$. ■

| s | C_1 | C_2 | C_3 | C_4 | C_5 | C_6 | C_8 | C_9 | C_{11} | C_7 | C_{10} | C_{12} | C_{13} | C_{14} | C_{15} | C_{16} |
|----------------------------|---------|---------|---------|---------|---------|---------|---------|---------|----------|---------|----------|----------|----------|----------|----------|----------|
| $\eta(s)$ | 4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 1 | 1 | 1 | 4 |
| | π_1 | π_1 | π_1 | π_1 | π_1 | π_1 | π_1 | π_1 |
| stabilizatory elementu s | π_2 | | | | | | | | | | | | | | | π_2 |
| | π_3 | | | | | | | | | | | π_3 | π_3 | | | π_3 |
| | π_4 | | | | | | | | | | | | | | | π_4 |

Rysunek 4.11: Niezmienniki permutacji z grupy G i stabilizatory elementów zbioru S .

Przykład 4.13 Rozważmy ponownie zbiór tablic $S = \{C_1, \dots, C_{16}\}$ z Przykładu 4.12 oraz grupę permutacji $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ działającą na tym zbiorze. Na Rysunku 4.11 zaznaczone są zarówno niezmienniki wszystkich permutacji z grupy G , jak i wartości $\eta(s)$ dla wszystkich elementów zbioru S . Rząd grupy G jest równy 4, a zatem z Twierdzenia 4.8 wynika, że liczba orbit działania grupy G na zbiorze S jest równa

$$o(G) = \frac{1}{|G|} \sum_{\pi \in G} Inv(\pi) = \frac{1}{4} (16 + 2 + 4 + 2) = \frac{24}{4} = 6.$$

Przypomnijmy, że orbity te odpowiadają jednoznacznie wszystkim różnym wzorom tablic pokazanych na Rysunku 4.7. □

Przykład 4.14 Zastosujmy Twierdzenie 4.8 do policzenia, ile jest wszystkich różnych łańcuszków, które składają się trzech koralików. Zakładamy przy tym, że każdy z koralików może być albo biały, albo niebieski. Będziemy przyporządkowywać każdemu z łańcuszków trzyliterowy ciąg złożony

z liter b albo n (dla uproszczenia zapisu pominiemy nawiasy i przecinki w zapisie ciągów). Ponadto przyjmiemy, że nie rozróżniamy końców łańcusków, a zatem na przykład łańcuszki bnn i nbb będąemy traktować jak identyczne.

Gdyby nie było tego ostatniego warunku, to zbiór wszystkich możliwych łańcuszków odpowiadałby następującemu ósmioelementowemu zbiorowi trzyliterowych ciągów:

$$S = \{bbb, bbn, bnb, nbb, bnn, nbn, nnb, nnn\}.$$

Fakt, że nie rozróżniamy końców łańcuszków, możemy uwzględnić przyjmując, że na zbiorze S działa dwuelementowa grupa permutacji $G = \{\pi_0, \pi_1\}$, w której permutacja π_0 jest permutacją identycznoscową, natomiast permutacja π_1 odpowiada zamianie końców łańcuszków. Mamy więc

$$\pi_0 = \begin{pmatrix} bbb & bbn & bnb & nbb & bnn & nbn & nnb & nnn \\ bbb & bbn & bnb & nbb & bnn & nbn & nnb & nnn \end{pmatrix}$$

oraz

$$\pi_1 = \begin{pmatrix} bbb & bbn & bnb & nbb & bnn & nbn & nnb & nnn \\ bbb & nbb & bnb & bbn & nnb & nbn & bnn & nnn \end{pmatrix}.$$

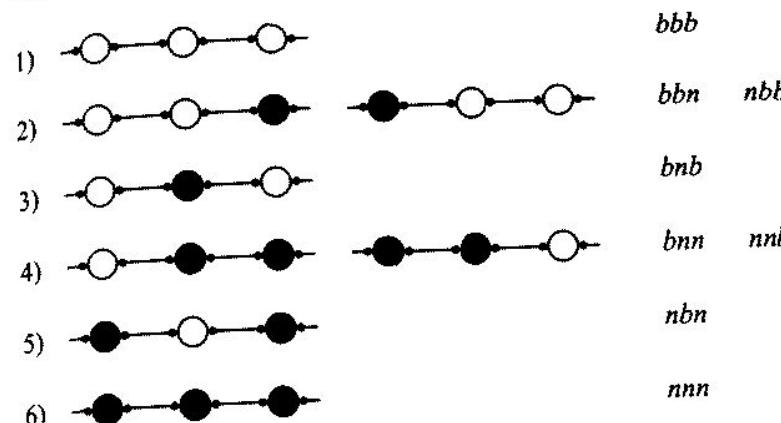
Łatwo sprawdzić, że – istotnie – G jest grupą permutacji. Wszystkie nierozróżnialne łańcuszki odpowiadają więc po prostu orbitom tej grupy. Liczba niezmienników permutacji π_0 jest oczywiście równa liczbie elementów zbioru S , natomiast w przypadku permutacji π_1 łatwo zauważać, że dokładnie cztery elementy są niezmiennikami. Są to ciągi bbb , bnb , nbn oraz nnn .

Z Twierdzenia 4.8 otrzymujemy więc, że liczba orbit grupy G jest równa

$$o(G) = \frac{1}{|G|} (Inv(\pi_0) + Inv(\pi_1)) = \frac{1}{2} (8 + 4) = 6.$$

Istnieje więc dokładnie sześć podzbiorów nierozróżnialnych łańcuszków spełniających powyższe warunki. Wszystkie one pokazane są na Rysunku 4.12. \square

W powyższym przykładzie mamy do czynienia z problemem zliczania wszystkich różnych łańcuszków, w których nie rozróżniamy końców. Zauważmy jednak, że w identyczny sposób możemy potraktować również



Rysunek 4.12: Wszystkie podzbiory nierozróżnialnych łańcuszków z Przykładu 4.14 i odpowiadające im trzyliterowe ciągi ze zbioru S .

problem z Przykładu 4.1. Tam także interesują nas orbity tej samej co w Przykładzie 4.14 dwuelementowej grupy, działającej na zbiorze wszystkich ósmioelementowych ciągów o wyrazach z dwuelementowego zbioru. Łatwo możemy policzyć, że suma liczb niezmienników dla obu permutacji tej grupy jest równa 272. Z Twierdzenia 4.8 wynika więc, że liczba różnych wiadomości, które Agentka S może przesłać w opisany sposób Agentowi (specjalnemu) M jest równa 136.

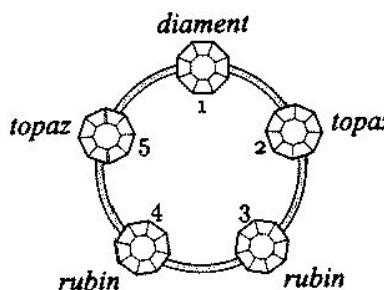
W następnym przykładzie pokażemy jeszcze jedno proste zastosowanie twierdzenia o liczbie orbit grupy. Problem również będzie dotyczył liczenia wszystkich możliwych naszyjników wykonanych z zadanego podzbioru kamieni. Tym niemniej w identyczny sposób możemy na przykład policzyć wszystkie możliwe konfiguracje sieci procesorów, połączonych w tak zwany pierścień, przy założeniu, że każdy z procesorów może być wybrany z ustalonego podzbioru typów, a przy tym nie wyróżniamy procesora, od którego zaczynamy numerowanie procesorów w sieci.

Przykład 4.15 Rozważmy naszyjniki (patrz Rysunek 4.13) złożone z pięciu kamieni, z których każdy może być diamentem, topazem albo rubinem. Przyjmijmy, że kamienie danego typu są nierozróżnialne. Założymy ponadto, że nie rozróżniamy dwóch naszyjników, które stają się identyczne po odpowiednim obrocie płaszczyzny. Innymi słowy, przy rozróżnianiu naszyjników istotne są typy kamieni i ich kolejność przy ustalonym kie-

runku numerowania kamieni, ale nie jest istotne, od którego kamienia zaczynamy numerację.

Chcemy policzyć, ile jest wszystkich różnych naszyjników przy powyższych założeniach.

Ponumerujmy miejsca, w których umieszczane są kamienie naszyjnika, liczbami naturalnymi od 1 do 5, wybierając w dowolny sposób pierwsze z miejsc i dokonując numeracji kolejnych miejsc na przykład zgodnie z ruchem wskazówek zegara. Każdy z naszyjników może być teraz opisany pięcioelementowym ciągiem symboli, odpowiadającym typom użytych w nim kamieni. (Możemy przyjąć na przykład, że symbolami tymi są pierwsze litery nazw kamieni, to znaczy *d*, *t*, *r*. Dla uproszczenia zapisu pominiemy też nawiasy i przecinki w ciągach.)



Rysunek 4.13: Naszyjnik z Przykładu 4.15, odpowiadający ciągowi *dtrt*.

Gdyby nie było warunku o nieroróżnialności obróconych naszyjników, to mielibyśmy dokładnie $3^5 = 243$ różnych ciągów, bowiem tyle jest funkcji z pięcioelementowego zbioru miejsc w trzyelementowy zbiór typów kamieni.

Oznaczmy zbiór wszystkich ciągów reprezentujących naszyjniki symbolem S . Warunek nieroróżnialności sprawia, że na przykład naszyjniki *stddt* i *dtstd* traktujemy jako identyczne, bowiem drugi z nich otrzymujemy z pierwszego w wyniku obrotu pierwszego o 124° zgodnie z ruchem wskazówek zegara. Zauważmy też, że wystarczy rozważyć jedynie pięć różnych obrotów naszyjników zgodnie z ruchem wskazówek zegara o kąty $i \cdot \frac{360^\circ}{5}$ dla $i = 0, 1, 2, 3, 4$.

Niech $\pi_0, \pi_1, \pi_2, \pi_3, \pi_4$, oznaczają odpowiadające tym obrotom permutacje zbioru S . Łatwo się przekonać, że zbiór $G = \{\pi_0, \pi_1, \pi_2, \pi_3, \pi_4\}$ tworzy grupę permutacji. Podzbiory nieroróżnialnych naszyjników od-

powiadają więc po prostu orbitom tej grupy. Aby wyznaczyć liczbę orbit grupy G na podstawie Twierdzenia 4.8, należy zatem znaleźć liczbę niezmienników dla każdej z permutacji grupy.

Permutacja π_0 jest permutacją identycznościową, a zatem $Inv(\pi_0) = |S| = 243$. Latwo też zauważyć, że jedynymi niezmiennikami permutacji $\pi_1, \pi_2, \pi_3, \pi_4$, są ciągi złożone z pięciu identycznych symboli, to znaczy następujące trzy ciągi: *ddddd*, *ttttt* oraz *sssss*. A zatem liczba niezmienników każdej z permutacji $\pi_1, \pi_2, \pi_3, \pi_4$ jest taka sama i równa 3. Z Twierdzenia 4.8 mamy:

$$o(G) = \frac{1}{5} (243 + 3 + 3 + 3 + 3) = 51.$$

Istnieje więc dokładnie 51 podzbiorów nieroróżnialnych naszyjników wykonanych z pięciu kamieni trzech różnych typów. \square

W powyższych przykładach zastosowanie twierdzenia o liczbie orbit było bardzo proste, bowiem wyznaczenie liczby niezmienników wszystkich permutacji grupy było niemal natychmiastowe. Poniższy przykład pokazuje zastosowanie, w którym znalezienie liczby niezmienników jest nieco bardziej skomplikowane, ale przebiega w sposób analogiczny jak poprzednio.

Przykład 4.16 Założymy, że chcemy przekazywać wiadomości używając słów kodowych złożonych z dokładnie trzech cyfr. Przyjmijmy ponadto, że sposób przekazywania wiadomości uniemożliwia w niektórych przypadkach stwierdzenie, gdzie jest „góra”, a gdzie „dół” zapisu. Bierze się to stąd, że cyfry 0, 6, 8, 9, mogą być odczytywane w pozycji „odwrócone” jako 0, 9, 8, 6. (Zwróćmy uwagę, iż przyjmujemy tu, że „odwrócona” jedynka jest rozróżnialna od „nieodwróconej”.) W związku z tym niektóre pary zapisów, na przykład 689 i 986, mogą reprezentować tylko jedną wiadomość. Zauważmy też, że jeśli zapis zawiera jakieś cyfry, których nie można poprawnie odczytać w pozycji „odwróconej”, to znaczy dowolną z cyfr: 1, 2, 3, 4, 5, 7, to problem niejednoznaczności znika, bowiem umiemy stwierdzić, gdzie jest „góra”, a gdzie „dół” zapisu.

Chcemy policzyć, ile różnych wiadomości można reprezentować przy powyższych założeniach.

Liczba wszystkich możliwych ciągów trójelementowych, złożonych z cyfr 0, 1, ..., 9, jest oczywiście równa 10^3 . Oznaczmy ten zbiór ciągów symbolem S . Tak jak w Przykładzie 4.14, grupa G permutacji działających na zbiorze S , liczy dwa elementy: π_0 oraz π_1 . Permutacja π_0 jest permutacją

identycznościową. Natomiast permutacja π_1 jest zdefiniowana następująco:

(i) jeśli ciąg $s \in S$ zawiera przynajmniej jedną z cyfr nie dających się poprawnie odczytać w pozycji „odwróconej”, to znaczy dowolną z cyfr: 1, 2, 3, 4, 5, 7, to wówczas $\pi_1(s) = s$;

(ii) w przeciwnym przypadku permutacja π_1 przekształca dany ciąg w odpowiedni ciąg „odwrócony”, to znaczy na przykład $\pi_1(608) = 809$.

Łatwo się przekonać, że tak zdefiniowana para permutacji stanowi grupę permutacji. Liczba niezmienników permutacji π_0 jest oczywiście równa liczności zbioru S . Aby skorzystać z Twierdzenia 4.8, należy więc jeszcze tylko wyznaczyć liczbę niezmienników permutacji π_1 . Rozważmy w tym celu dwa omawiane wyżej przypadki (i) oraz (ii).

Każdy ciąg opisany w (i) jest oczywiście niezmiennikiem. Trzeba zatem policzyć, ile jest wszystkich ciągów trójelementowych, które zawierają co najmniej jedną z cyfr 1, 2, 3, 4, 5, 7, albo - co łatwiej zrobić - policzyć, ile jest ciągów, które żadnej takiej cyfry nie zawierają, a następnie odjąć tę liczbę od liczby wszystkich możliwych ciągów.

Rozważmy zatem zbiór trójelementowych ciągów o wyrazach ze zbioru $\{0, 6, 8, 9\}$. Istnieje dokładnie $4^3 = 64$ takich ciągów, a zatem liczba niezmienników permutacji π_1 , odpowiadających przypadkowi (i), jest równa $64 - 4^3 = 32$.

Aby wyznaczyć liczbę niezmienników permutacji π_1 , związanych z przypadkiem (ii), wystarczy zauważyc, że niezmienniki te są trójelementowymi ciągami, w których środkowym elementem jest jedna z cyfr 0, 8, natomiast elementy pierwszy i ostatni tworzą jedną z następujących czterech par: (0,0), (8,8), (6,9), (9,6). Liczba wszystkich takich ciągów jest równa $2 \cdot 4 = 8$, a zatem liczba wszystkich niezmienników permutacji π_1 , odpowiadających obu przypadkom (i) oraz (ii), jest równa $32 + 8 = 40$.

Dodając liczby niezmienników dla obu permutacji π_0 i π_1 i dzieląc wynik przez rzad grupy G , otrzymujemy liczbę orbit tej grupy:

$$|S/R_G| = \frac{1}{2} (1000 + 944) = 972.$$

Istnieją zatem dokładnie 972 różne słowa kodowe, spełniające podane założenia. \square

4.3 Klasy równoważności funkcji

Niech X oraz Y będą dowolnymi zbiorami skończonymi i niech G będzie grupą permutacji zbioru X . Rozważmy zbiór $Fun(X, Y)$ wszystkich funkcji w $X \times Y$. Wprowadźmy w tym zbiorze relację F_G , związaną z grupą permutacji G . Przyjmijmy mianowicie dla $f_1, f_2 \in Fun(X, Y)$, że funkcja f_1 jest w relacji F_G z funkcją f_2 wtedy i tylko wtedy, gdy istnieje permutacja π , należąca do grupy G , dla której spełniony jest następujący warunek:

$$f_1(d) = f_2(\pi(d)) \text{ dla każdego } d \in X.$$

Łatwo sprawdzić, że tak zdefiniowana relacja w zbiorze $Fun(X, Y)$ jest zwrotna, symetryczna i przechodnia, a zatem jest relacją równoważności. Klasy abstrakcji relacji F_G w zbiorze $Fun(X, Y)$ nazwiemy wzorami.

Przykład 4.17 Niech $X = \{x_1, x_2, x_3, x_4\}$ oraz $Y = \{b, c\}$. Zbiór $Fun(X, Y)$ liczy $|Y|^{|X|} = 2^4 = 16$ funkcji; wszystkie one są przedstawione w tabeli na Rysunku 4.14 poprzez podanie ich wartości dla poszczególnych argumentów ze zbioru X .

Rozważmy czteroelementowy zbiór $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ permutacji zbioru X , gdzie

$$\pi_1 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & x_1 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_4 & x_1 & x_2 \end{pmatrix},$$

$$\pi_3 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_4 & x_1 & x_2 & x_3 \end{pmatrix}, \quad \pi_4 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}.$$

Łatwo się przekonać, że zbiór G tworzy grupę permutacji. Łatwo też sprawdzić, że zdefiniowana wyżej relacja równoważności F_G dzieli zbiór $Fun(X, Y)$ na sześć wypisanych niżej klas abstrakcji (wzorów):

- $\{f_1\}$,
- $\{f_2, f_3, f_4, f_5\}$,
- $\{f_6, f_8, f_9, f_{11}\}$,
- $\{f_7, f_{10}\}$,
- $\{f_{12}, f_{13}, f_{14}, f_{15}\}$,
- $\{f_{16}\}$.

| funkcja f_i | $f_i(x_1)$ | $f_i(x_2)$ | $f_i(x_3)$ | $f_i(x_4)$ |
|---------------|------------|------------|------------|------------|
| f_1 | b | b | b | b |
| f_2 | c | b | b | b |
| f_3 | b | c | b | b |
| f_4 | b | b | c | b |
| f_5 | b | b | b | c |
| f_6 | c | c | b | b |
| f_7 | c | b | c | b |
| f_8 | c | b | b | c |
| f_9 | b | c | c | b |
| f_{10} | b | c | b | c |
| f_{11} | b | b | c | c |
| f_{12} | c | c | c | b |
| f_{13} | c | c | b | c |
| f_{14} | c | b | c | c |
| f_{15} | b | c | c | c |
| f_{16} | c | c | c | c |

Rysunek 4.14: Tabela wartości wszystkich funkcji należących do zbioru $\text{Fun}(\{x_1, x_2, x_3, x_4\}, \{b, c\})$.

Aby pokazać, że na przykład funkcje f_2 i f_3 są w relacji równoważności F_G wystarczy sprawdzić, że w zbiorze $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ istnieje permutacja π (w tym przypadku jest nią permutacja π_1), dla której $f_2(x) = f_3(\pi(x))$ dla każdego $x \in X$. Istotnie, mamy:

$$\begin{aligned} f_2(x_1) &= c, & f_3(\pi_1(x_1)) &= f_3(x_2) = c, \\ f_2(x_2) &= b, & f_3(\pi_1(x_2)) &= f_3(x_3) = b, \\ f_2(x_3) &= b, & f_3(\pi_1(x_3)) &= f_3(x_4) = b, \\ f_2(x_4) &= b, & f_3(\pi_1(x_4)) &= f_3(x_1) = b. \end{aligned}$$

Patrząc na zbiór wzorów związanych z relacją równoważności F_G łatwo zauważać całkowitą zbieżność ze zbiorem orbit pokazanych na Rysunku 4.10. Związek ten nie jest oczywiście przypadkowy. Zauważmy bowiem, że połom tablic z Przykładu 4.11 możemy przyporządkować elementy zbioru X zgodnie z poniższym rysunkiem

| | |
|-------|-------|
| x_1 | x_2 |
| x_4 | x_3 |

4.4. OGÓLNE ZAGADNIENIE ZLICZANIA

Jeśli teraz elementowi b ze zbioru Y przyporządkujemy biały kolor pola, a elementowi c – kolor czarny, to szesnaście tablic C_1, \dots, C_{16} , z Przykładu 4.11 będzie wzajemnie jednoznacznie odpowiadało kolejnym szesnastu funkcjom f_1, \dots, f_{16} , ze zbioru $\text{Fun}(X, Y)$. Grupa permutacji G będzie natomiast reprezentowała obroty tablic o 90° , 180° , 270° i 0° zgodnie z ruchem wskazówek zegara. \square

4.4 Ogólne zagadnienie zliczania

W rozdziale tym postawimy pewien problem, który nazwiemy *ogólnym zagadnieniem zliczania*, oraz podamy klasyczne twierdzenie (twierdzenie Pólya⁷), które pozwoli na jego rozwiązanie. W szczególnym przypadku z twierdzenia tego będziemy mogli uzyskać liczbę orbit działania grupy na zbiorze, co pozwoli również na rozwiązywanie zagadnień zliczania, którymi zajmowaliśmy się w poprzednim punkcie.

W teorii zliczania używana jest zwykle pewna specyficzna terminologia, którą i my będziemy stosować; zaczniemy więc od jej wprowadzenia. Terminologia ta może nieco różić na początku, ale jej stosowanie ułatwia formułowanie poszczególnych faktów i w rezultacie okazuje się wygodne.

Niech, jak poprzednio, będą dane dwa zbiory skończone, oznaczane symbolami X oraz Y , i niech $\text{Fun}(X, Y)$ będzie zbiorem wszystkich funkcji ze zbioru X w zbiór Y . Zbiór X (dziedzinę tych funkcji) będziemy nazywać zbiorem *miejsc*, natomiast zbiór Y – zbiorem *figur*.

Elementy zbioru $\text{Fun}(X, Y)$, to znaczy poszczególne funkcje, nazwijmy *konfiguracjami*. Dodatkowo, każdemu elementowi y ze zbioru Y , to znaczy każdej figurze, przyporządkujemy wagę figury $w(y)$. Ponieważ w dalszym ciągu będziemy korzystać głównie z przekształcania symbolicznych zapisów, to wagi figur będą również dowolnymi symbolami.

Zinterpretujmy wprowadzone wyżej nazwy dla przykładu z dwubarwnymi czteropolowymi tablicami. Miejscami są tam cztery pola tablicy, figurami – kolory, którymi te pola możemy pomalować, natomiast wagami figur – symbole b oraz c , odpowiadające kolorom białemu i czarnemu. Zbiór konfiguracji, to – w tym przypadku – zbiór wszystkich możliwych szesnastu sposobów pomalowania tablic.

⁷George Pólya – amerykański matematyk węgierskiego pochodzenia, który w napisanej w roku 1937 pracy przedstawił podwaliny teorii zliczania i użył jej do wyznaczenia liczby izomerów związków chemicznych. Istnieją wprawdzie różne uogólnienia teorii zliczania Pólya, ale dla naszych celów wygodne będzie pozostawienie terminu: ogólnego zagadnienia zliczania.

Wprowadzimy następujące określenia:

Szeregiem zliczającym figur nazwiemy wyrażenie

$$\sum_{y \in Y} w(y). \quad (4.7)$$

Przez *wagę konfiguracji* $f \in \text{Fun}(X, Y)$ będziemy rozumieć wyrażenie

$$W(f) = \prod_{x \in X} w(f(x)). \quad (4.8)$$

Podobnie jak w przypadku omawianych w Rozdziale 3. funkcji tworzących, oba powyższe wyrażenia będąmy traktować głównie jak formalne zapisy, które będąmy jedynie przekształcać. Zauważmy też, że jeśli G jest grupą permutacji zbioru X i dwie konfiguracje należą do tej samej klasy abstrakcji relacji F_G , to – oczywiście – ich wagi są równe.

Niech F będzie dowolnym podzbiorem konfiguracji. *Szeregiem zliczającym konfiguracji* należących do zbioru $F \subseteq \text{Fun}(X, Y)$ nazwiemy wyrażenie o postaci

$$\sum_{f \in F} W(f). \quad (4.9)$$

Przykład 4.18 Niech będą dane zbiór miejsc $X = \{d_1, d_2, d_3\}$ oraz zbiór figur $Y = \{r_1, r_2, r_3\}$. Rozważmy następujący podzbiór $F = \{f_1, f_2, f_3\}$ zbioru konfiguracji $\text{Fun}(X, Y)$, gdzie grafy poszczególnych funkcji przedstawione są na Rysunku 4.15.

Przyjmijmy następujące wagi figur:

$$w(r_1) = u,$$

$$w(r_2) = v,$$

$$w(r_3) = u.$$

Zgodnie z przyjętą definicją, szereg zliczający figur ma w tym przypadku postać poniższego wyrażenia:

$$2u + v.$$

Policzmy wagi poszczególnych konfiguracji:

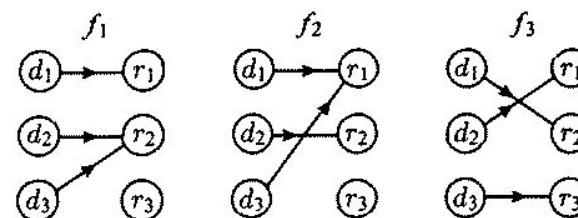
$$W(f_1) = uv^2,$$

$$W(f_2) = u^2v,$$

$$W(f_3) = u^2v.$$

Zatem szeregiem zliczającym konfiguracji należących do zbioru F jest następujące wyrażenie:

$$uv^2 + 2u^2v.$$



Rysunek 4.15: Rysunki grafów funkcji z Przykładu 4.18.

Niech teraz I będzie liczbą wszystkich różnych wag konfiguracji ze zbioru $\text{Fun}(X, Y)$. Oznaczmy te wagi symbolami W_1, \dots, W_I , i niech dla $i = 1, \dots, I$, $F_i \subseteq \text{Fun}(X, Y)$ oznacza podzbiór funkcji o wadze W_i . Zauważmy, że każdy taki podzbiór jest sumą pewnej liczby wzorów (konfiguracji równoważnych).

Niech m_i oznacza liczbę wszystkich wzorów należących do podzbioru F_i , $i = 1, \dots, I$. Naszym celem będzie podanie wyrażenia

$$W = \sum_{i=1}^I m_i W_i, \quad (4.10)$$

które nazwiemy *szeregiem zliczającym wzorów*. Znajomość tego wyrażenia pozwoli nam na łatwą odpowiedź na wszystkie interesujące pytania, dotyczące konfiguracji równoważnych.

Zanim jednak przejdziemy do opisu metody wyznaczania wyrażenia 4.10, powróćmy jeszcze raz do przykładu z tablicami, którego używamy do ilustrowania większości rozważań w tym rozdziale.

Przykład 4.19 Rozważmy raz jeszcze parę zbiorów: zbiór miejsc $X = \{x_1, x_2, x_3, x_4\}$ oraz zbiór figur $Y = \{b, c\}$. Niech – jak w Przykładzie 4.17 – zbiór X reprezentuje cztery pola tablicy, natomiast zbiór Y – kolory przypisywane tym polom. Na zbiorze X działa czteroelementowa grupa permutacji $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$, której elementy odpowiadają obrotom tablicy odpowiednio o 90° , 180° , 270° i 0° zgodnie z ruchem wskazówek zegara. Wszystkie możliwe tablice C_1, \dots, C_{16} , odpowiadają jednoznacznie szesnastu funkcjom (konfiguracjom) f_1, \dots, f_{16} , ze zbioru $\text{Fun}(X, Y)$. Zbiór tych szesnastu konfiguracji dzieli się jednak zaledwie na sześć następujących podzbiorów konfiguracji równoważnych (wzorów):

$\{f_1\}$,
 $\{f_2, f_3, f_4, f_5\}$,
 $\{f_6, f_8, f_9, f_{11}\}$,
 $\{f_7, f_{10}\}$,
 $\{f_{12}, f_{13}, f_{14}, f_{15}\}$,
 $\{f_{16}\}$.

Jeśli teraz rozważymy wagi konfiguracji, to otrzymamy następujące pięć możliwych wag:

$$\begin{aligned}W_1 &= b^4, \\W_2 &= b^3c^1, \\W_3 &= b^2c^2, \\W_4 &= b^1c^3, \\W_5 &= c^4.\end{aligned}$$

Waga $W_1 = b^4$ odpowiada więc tablicy, w której wszystkie cztery pola są białe, waga $W_2 = b^3c^1$ – tablicom, w których są trzy pola białe i jedno czarne itd. Pięciu różnym wagom możemy przyporządkować następujące, zdefiniowane wyżej, podzbiory F_i , $i = 1, \dots, 5$, zbioru $Fun(X, Y)$:

$$\begin{aligned}F_1 &= \{f_1\}, \\F_2 &= \{f_2, f_3, f_4, f_5\}, \\F_3 &= \{f_6, f_7, f_8, f_9, f_{10}, f_{11}\}, \\F_4 &= \{f_{12}, f_{13}, f_{14}, f_{15}\}, \\F_5 &= \{f_{16}\}.\end{aligned}$$

Na Rysunku 4.16 podzbiory te wypisane są wraz z odpowiadającymi im podzbiorami tablic.

Porównując Rysunek 4.16 z Rysunkiem 4.10 zauważymy jedną różnicę. Mianowicie, dwa z podzbiorów tablic (odpowiadające na Rysunku 4.10 orbitom $\{C_6, C_8, C_9, C_{11}\}$ oraz $\{C_7, C_{10}\}$) zostały połączone w jeden podzbiór F_3 . Dzieje się tak dlatego, że wagi konfiguracji, odpowiadające elementom tych orbit, są identyczne; w przypadku wszystkich wymienionych tablic waga jest równa $W_3 = b^2c^2$, tzn. dwa pola tablicy są białe, a dwa czarne. Istnieją więc dokładnie dwa wzory, których waga jest równa W_3 , a zatem $m_3 = 2$. Zauważmy też, że dla wszystkich pozostałych wag, to znaczy dla $i = 1, 2, 4, 5$, mamy $m_i = 1$.

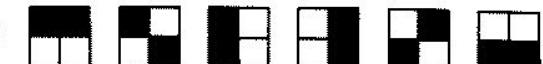
$$F_1 = \{f_1\}$$



$$F_2 = \{f_2, f_3, f_4, f_5\}$$



$$F_3 = \{f_6, f_7, f_8, f_9, f_{10}, f_{11}\}$$



$$F_4 = \{f_{12}, f_{13}, f_{14}, f_{15}\}$$



$$F_5 = \{f_{16}\}$$



Rysunek 4.16: Podzbiory funkcji F_i , $i = 1, \dots, 5$, oraz odpowiadające im zbiory tablic.

Szereg zliczający wzorów W ma zatem postać:

$$W = b^4 + b^3c^1 + 2b^2c^2 + b^1c^3 + c^4.$$

Wyrażenie to można interpretować następująco:

Istnieje dokładnie sześć (tyle, ile jest równa suma współczynników liczbowych w powyższej sumie) różnych wzorów tablic o czterech polach białych albo czarnych; wszystkie inne można otrzymać z nich w wyniku obrotów o wielokrotności kąta prostego. Jeden z tych wzorów zawiera cztery pola białe, jeden – trzy pola białe i dwa czarne, dwa – dwa pola białe i jedno czarne, jeden – jedno pole białe i trzy czarne oraz jeden wzór zawierający cztery pola czarne. □

W powyższym, bardzo prostym przykładzie, szereg zliczający wzorów został wypisany na podstawie znajomości wszystkich konfiguracji równoważnych i ich wag. Celem naszym będzie podanie w dalszej części tego rozdziału efektywnej metody, pozwalającej na wypisanie takiego szeregu w bardziej złożonych przypadkach i bez potrzeby generowania wszystkich konfiguracji równoważnych.

Zanim jednak podamy taką metodę, potrzebne będzie wprowadzenie kilku dodatkowych pojęć i udowodnienie pewnych pomocniczych faktów.

Dla $\pi_j \in G$ oraz zbioru wzorów F_i , gdzie $i = 1, \dots, I$, zdefiniujemy funkcję $\pi_j^{(i)} : F_i \rightarrow F_i$ w sposób następujący:

$$\pi_j^{(i)}(f) = g \Leftrightarrow f(x) = g(\pi_j(x)) \quad \text{dla każdego } x \in X.$$

Zauważmy, że funkcja g istotnie należy do F_i , bowiem jej waga jest taka sama jak waga funkcji f , to znaczy jest równa W_i . Zachodzi poniższy prosty fakt:

Twierdzenie 4.9 Funkcja $\pi_j^{(i)}$ jest permutacją zbioru F_i dla $i = 1, \dots, I$.

Dowód. Wystarczy pokazać, że $\pi_j^{(i)}$ jest injekcją. Przypuśćmy, że tak nie jest; pokażemy, że założenie takie prowadzi do sprzeczności. Istotnie, gdyby $\pi_j^{(i)}$ nie była funkcją różnowartościową, to istniałyby dwie funkcje $f', f'' \in F_i$, $f' \neq f''$, dla których $\pi_j^{(i)}(f') = (f'') = f$. Ale to oznaczałoby, że dla każdego $x \in X$ spełnione byłyby równości $f'(x) = f(\pi_j^{(i)}(x))$ oraz $f''(x) = f(\pi_j^{(i)}(x))$, a zatem musiałaby zachodzić równość $f' = f''$. Otrzymaliśmy więc sprzeczność, a stąd wynika, że funkcja $\pi_j^{(i)}$ jest injekcją i w konsekwencji jest permutacją zbioru F_i . ■

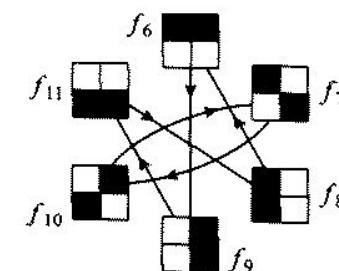
Przykład 4.20 Rozważmy ponownie przykład z dwukolorowymi tablicami. Niech $i = 3$. Na Rysunku 4.17 pokazane są grafy wszystkich czterech funkcji $\pi_1^{(3)}, \pi_2^{(3)}, \pi_3^{(3)}, \pi_4^{(3)}$, odpowiadających czterem elementom grupy permutacji G . □

Niech $\sigma = \{B_1, \dots, B_k\}$ będzie dowolnym podziałem zbioru X na bloki (patrz Rozdział 2.6). Oznaczmy symbolem $F^\sigma \subseteq Fun(X, Y)$ podzbiór funkcji stałych na blokach podziału σ . Oznacza to, że dla każdej funkcji $f \in F^\sigma$ mamy $f(x') = f(x'')$, jeśli x' oraz x'' należą do tego samego bloku podziału σ . Innymi słowy, dla $f \in F^\sigma$ obrazem dowolnego bloku podziału zbioru X przez tę funkcję jest jednoelementowy zbiór figur. Zachodzi następujące twierdzenie:

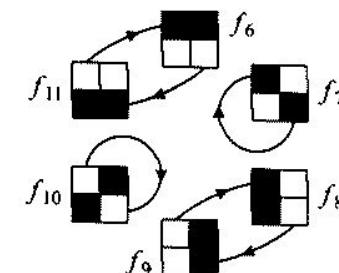
Twierdzenie 4.10 Dla dowolnego podziału $\sigma = \{B_1, \dots, B_k\}$ zbioru X szereg zliczający konfiguracji należących do F^σ jest dany następującym wyrażeniem:

$$\prod_{i=1}^k \left[\sum_{y \in Y} w^{|B_i|}(y) \right]. \quad (4.11)$$

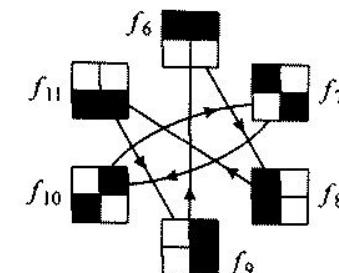
$$\pi_1 = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$$



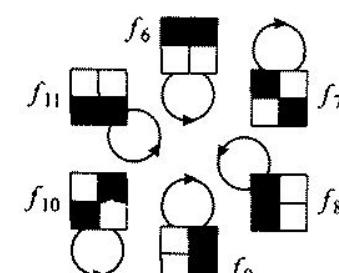
$$\pi_2 = \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}$$



$$\pi_3 = \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}$$



$$\pi_4 = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$$



Rysunek 4.17: Permutacje należące do grupy G oraz odpowiadające im grafy funkcji $\pi_1^{(3)}, \pi_2^{(3)}, \pi_3^{(3)}, \pi_4^{(3)}$.

Dowód. Dla dowodu wystarczy rozpisać wyrażenie 4.11. Mamy

$$\prod_{i=1}^k \left[\sum_{y \in Y} w^{|B_i|}(y) \right] = \sum_{y_1, \dots, y_k \in Y} w^{|B_1|}(y_1) \cdot \dots \cdot w^{|B_k|}(y_k).$$

Zauważmy, że wyrażenie $w^{|B_1|}(y_1) \cdot \dots \cdot w^{|B_k|}(y_k)$ jest wagą takiej funkcji f ze zbioru F^σ , dla której $f(B_i) = \{y_i\}$, gdzie $y_i \in Y$, $i = 1, \dots, k$. Powstałe wyrażenie jest więc istotnie szeregiem zliczającym konfiguracji należących do zbioru F^σ . ■

Zanim sformułujemy podstawowe twierdzenie tego rozdziału, wprowadzimy jedno ważne pojęcie, związane z grupą permutacji, a mianowicie pojęcie indeksu cykli grupy.

Niech $G = \{\pi_1, \dots, \pi_{|G|}\}$ będzie grupą permutacji zbioru X , gdzie $|X| = n$, i niech $(\lambda_1^k, \dots, \lambda_n^k)$ oznacza typ permutacji $\pi_k \in G$.

Definicja 4.12 Indeksem cykli grupy G nazywamy wyrażenie

$$P_G(z_1, z_2, \dots, z_n) = \frac{1}{|G|} \sum_{\pi_k \in G} z_1^{\lambda_1^k} z_2^{\lambda_2^k} \dots z_n^{\lambda_n^k}. \quad (4.12)$$

Podobnie jak w przypadku funkcji tworzących, w zasadzie nie interesuje nas to, czym są zmienne z_1, \dots, z_n . Możemy więc przyjąć, że są to pewne zmienne zespolone, chociaż nigdy nie będzie nas interesowała na przykład zbieżność tego szeregu. Innymi słowy, wyrażenie 4.12 będzie my traktować głównie jako szereg formalny, na którym można dokonywać pewnych przekształceń.

Przykład 4.21 Obliczmy indeks cykli grupy obrotów z Przykładu 4.19. Mamy tam czteroelementową grupę permutacji $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$, gdzie

$$\begin{aligned} \pi_1 &= \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & x_1 \end{pmatrix}, & \pi_2 &= \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_3 & x_4 & x_1 & x_2 \end{pmatrix}, \\ \pi_3 &= \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_4 & x_1 & x_2 & x_3 \end{pmatrix}, & \pi_4 &= \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}. \end{aligned}$$

Aby wypisać indeks cykli grupy G , należy najpierw wyznaczyć typy wszystkich należących do niej permutacji. Zaczynamy od rozkładu poszczególnych permutacji na cykle rozłączne. Otrzymujemy następującą tabelę:

4.4. OGÓLNE ZAGADNIENIE ZLICZANIA

| permutacja | typ |
|-----------------------------------|-------|
| $\pi_1 = [x_1 x_2 x_3 x_4]$ | 4^1 |
| $\pi_2 = [x_1 x_3] [x_2 x_4]$ | 2^2 |
| $\pi_3 = [x_1 x_4 x_3 x_2]$ | 4^1 |
| $\pi_4 = [x_1] [x_2] [x_3] [x_4]$ | 1^4 |

Teraz już możemy bardzo łatwo wypisać indeks cykli grupy G zgodnie z zależnością 4.12. Mamy:

$$P_G(z_1, \dots, z_4) = \frac{1}{4} (z_4^1 + z_2^2 + z_4^1 + z_1^4) = \frac{1}{4} (z_1^4 + z_2^2 + 2z_4^1). \quad \square$$

Poniższe twierdzenie pozwala na wyznaczenie szeregu zliczającego wzorów na podstawie znajomości indeksu cykli grupy i szeregu zliczającego figur.

Twierdzenie 4.11 (Pólya, 1937) Szereg zliczający wzorów W ma postać następującą:

$$W = P_G \left(\sum_{y \in Y} w^1(y), \sum_{y \in Y} w^2(y), \dots, \sum_{y \in Y} w^n(y) \right). \quad (4.13)$$

Zanim podamy dowód powyższego twierdzenia, zauważmy, że jeśli znamy zarówno indeks cykli grupy G , jak i szereg zliczający figur, to wyznaczenie szeregu zliczającego wzorów jest już bardzo proste. Wystarczy bowiem tylko w indeksie cykli grupy G dokonać dla $k = 1, \dots, n$, podstawienia wyrażenia $\sum_{y \in Y} w^k(y)$ zamiast zmiennej z_k . Poniższy przykład ilustruje to postępowanie dla problemu z dwubarwnymi tablicami.

Przykład 4.22 W Przykładzie 4.21 wyznaczyliśmy już indeks cykli grupy obrotów G ; ma on następującą postać:

$$P_G(z_1, \dots, z_4) = \frac{1}{4} (z_1^4 + z_2^2 + 2z_4^1).$$

Znamy również szereg zliczający figur; w naszym problemie mamy do czynienia z polem białym – b oraz polem czarnym – c , a zatem szereg zliczający figur ma postać

$$b + c.$$

Wystarczy teraz dokonać podstawienia zgodnie z 4.13: mianowicie, zamiast z_1 należy podstawić wyrażenie $b+c$, zamiast z_2 – wyrażenie b^2+c^2 , a zamiast z_4 – wyrażenie b^4+c^4 . W wyniku tych operacji otrzymujemy następujący szereg zliczający wzorów:

$$W = \frac{1}{4}[(b+c)^4 + (b^2+c^2)^2 + 2(b^4+c^4)] = b^4 + b^3c + 2b^2c^2 + bc^3 + c^4.$$

Zauważmy, że uzyskaliśmy to samo wyrażenie, które wyznaczyliśmy już w Przykładzie 4.19, wypisując kolejno, a następnie sumując wszystkie wagi konfiguracji równoważnych. \square

Dowód Twierdzenia 4.11. Niech m_i oznacza liczbę klas równoważności w zbiorze funkcji o wagie W_i . Zgodnie z definicją, szeregiem zliczającym wzorów jest wówczas wyrażenie

$$W = \sum_{i=1}^I m_i W_i. \quad (4.14)$$

Z twierdzenia 4.8 mamy

$$m_i = \frac{1}{|G|} \sum_{\pi \in G} Inv(\pi^{(i)}).$$

Podstawiając powyższe wyrażenie w 4.14 otrzymujemy:

$$W = \sum_{i=1}^I \frac{1}{|G|} \sum_{\pi \in G} Inv(\pi^{(i)}) W_i = \frac{1}{|G|} \sum_{\pi \in G} \left[\sum_{i=1}^I Inv(\pi^{(i)}) W_i \right]. \quad (4.15)$$

Zauważmy, że wyrażenie $\sum_{i=1}^I Inv(\pi^{(i)}) W_i$ jest szeregiem zliczającym funkcji $f \in Fun(X, Y)$, spełniających warunek $f(x) = f(\pi(x))$ dla każdego $x \in X$. Dla każdej takiej funkcji wartość $f(x)$ musi być taka sama dla każdego elementu x , należącego do tego samego cyklu permutacji π . Zatem, na podstawie Twierdzenia 4.10 szereg zliczający tych funkcji jest następujący:

$$\sum_{i=1}^I Inv(\pi^{(i)}) W_i = \left[\sum_{y \in Y} w^1(y) \right]^{\lambda_1(\pi)} \left[\sum_{y \in Y} w^2(y) \right]^{\lambda_2(\pi)} \cdots \left[\sum_{y \in Y} w^n(y) \right]^{\lambda_n(\pi)},$$

4.4. OGÓLNE ZAGADNIENIE ZLICZANIA

gdzie $(\lambda_1(\pi), \lambda_2(\pi), \dots, \lambda_n(\pi))$ jest typem permutacji π . Po podstawieniu powyższego wyrażenia do 4.15 otrzymujemy zależność 4.13:

$$W = P_G \left(\sum_{y \in Y} w^1(y), \sum_{y \in Y} w^2(y), \dots, \sum_{y \in Y} w^n(y) \right). \quad \blacksquare$$

Twierdzenie 4.11 pozwala na łatwe wyznaczenie liczby wszystkich wzorów w zbiorze $Fun(X, Y)$. Zauważmy bowiem, że jeśli przyjmiemy, że waga każdej figury ze zbioru Y jest równa 1, to wówczas każda z funkcji ze zbioru $Fun(X, Y)$ będzie miała wagę równą 1. Ale w takim przypadku dla dowolnej grupy G działającej na zbiorze X wartością szeregu zliczającego wzorów W jest po prostu liczba wszystkich wzorów. Otrzymaliśmy więc następujący prosty wniosek z twierdzenia Pólyi:

Wniosek 4.2 Dla grupy G działającej na zbiorze X liczba konfiguracji równoważnych w zbiorze $Fun(X, Y)$ jest równa $P_G(|Y|, |Y|, \dots, |Y|)$.

Twierdzenie 4.11 oraz Wniosek 4.2 pozwala na łatwe rozwiązywanie różnorodnych zagadnień zliczania. Dwa z takich zagadnień przedstawimy w poniższych przykładach.

Przykład 4.23 Założymy, że chcemy policzyć, ile jest wszystkich różnych naszyjników (patrz Rysunek 4.18) złożonych z sześciu kamieni, z których każdy może być szmaragdem albo topazem. Za różne uważamy takie dwa naszyjniki, których nie można otrzymać z siebie w wyniku dowolnych obrotów. Możliwe osie wszystkich takich obrotów pokazane są na Rysunku 4.18. Kamienie tego samego rodzaju uważamy za nieroróżnicalne.

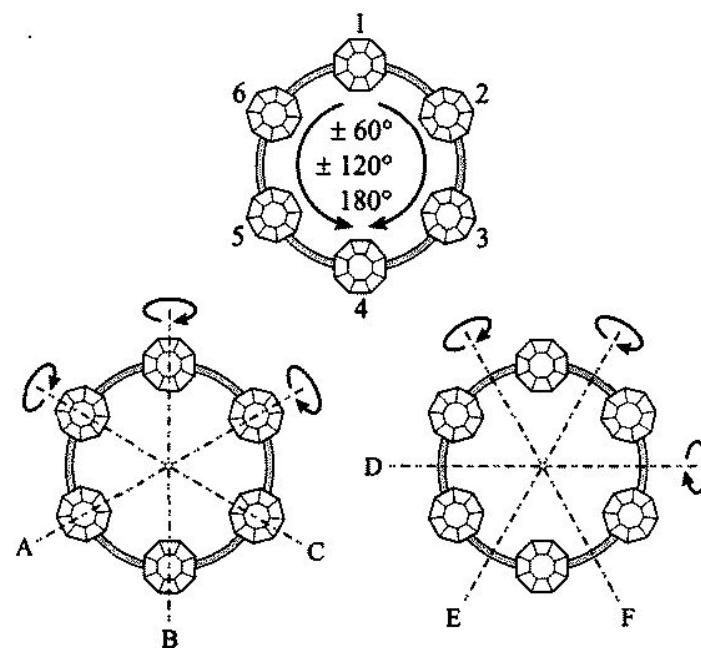
Zbiorem miejsc w tym problemie jest zbiór sześcioelementowy, odpowiadający sześciu miejscom osadzenia kamieni w naszyjniku. Oznaczmy zbiór miejsc symbolem X i przyjmijmy $X = \{1, 2, 3, 4, 5, 6\}$.

Zbiór figur Y w naszym przykładzie zawiera dwa elementy y_1 oraz y_2 , odpowiadające typom kamieni. Wygodnie będzie oznaczyć wagi tych elementów pierwszymi literami typów kamieni. Niech zatem $w(y_1) = s$ (szmaragd) oraz $w(y_2) = t$ (topaz).

Na zbiorze miejsc X działa grupa permutacji G , której wszystkie elementy przedstawione są w poniższej tabeli. Każda z permutacji reprezentuje albo obrót naszyjnika wokół środka okręgu w płaszczyźnie naszyjnika o wielokrotności kąta 60° (zgodnie lub przeciwnie do ruchu wskazówek zegara), albo obrót płaszczyzny naszyjnika wokół jednej z osi A, B, C, D,

E, F (patrz Rysunek 4.18) o 180° . W poszczególnych kolumnach tabeli zapisane są permutacje, odpowiadające im obroty, a także typy tych permutacji, niezbędne do wypisania indeksu cykli grupy G .

| permutacja | obrót | typ |
|---------------------------------|--|-----------|
| $\pi_1 = (1, 2, 3, 4, 5, 6)$ | obrót o 0° wokół środka okręgu | 1^6 |
| $\pi_2 = (2, 3, 4, 5, 6, 1)$ | obrót o $+60^\circ$ wokół środka okręgu | 6^1 |
| $\pi_3 = (6, 1, 2, 3, 4, 5)$ | obrót o -60° wokół środka okręgu | 6^1 |
| $\pi_4 = (3, 4, 5, 6, 1, 2)$ | obrót o $+120^\circ$ wokół środka okręgu | 3^2 |
| $\pi_5 = (5, 6, 1, 2, 3, 4)$ | obrót o -120° wokół środka okręgu | 3^2 |
| $\pi_6 = (4, 5, 6, 1, 2, 3)$ | obrót o 180° wokół środka okręgu | 2^3 |
| $\pi_7 = (3, 2, 1, 6, 5, 4)$ | obrót wokół osi A | $1^2 2^2$ |
| $\pi_8 = (1, 6, 5, 4, 3, 2)$ | obrót wokół osi B | $1^2 2^2$ |
| $\pi_9 = (5, 4, 3, 2, 1, 6)$ | obrót wokół osi C | $1^2 2^2$ |
| $\pi_{10} = (4, 3, 2, 1, 6, 5)$ | obrót wokół osi D | 2^3 |
| $\pi_{11} = (2, 1, 6, 5, 4, 3)$ | obrót wokół osi E | 2^3 |
| $\pi_{12} = (6, 5, 4, 3, 2, 1)$ | obrót wokół osi F | 2^3 |



Rysunek 4.18: Obroty naszyjnika z Przykładu 4.23.

Rysunek 4.19: Permutacje należące do grupy obrotów z Przykładu 4.23.

Tabela na Rysunku 4.19 zawiera wszystkie dane, które są niezbędne do wypisania szeregu zliczającego figur, a tym samym do wyznaczenia wszystkich możliwych różnych naszyjników. Mamy bowiem $|G| = 12$ oraz

$$P_G(z_1, \dots, z_6) = \frac{1}{12} (z_1^6 + 4z_2^3 + 2z_3^2 + 2z_6 + 3z_1^2 z_2^2). \quad (4.16)$$

Szeregiem zliczającym figur jest w naszym problemie wyrażenie

$$s + t.$$

Podstawiając szereg zliczający figur do indeksu cykli grupy G , to znaczy zastępując zmienną z_1 wyrażeniem $s + t$, zmienną z_2 – wyrażeniem $s^2 + t^2$, zmienną z_3 – wyrażeniem $s^3 + t^3$ oraz zmienną z_6 – wyrażeniem $s^6 + t^6$, otrzymujemy następujący szereg zliczający wzorów:

$$W = s^6 + s^5t + 3s^4t^2 + 3s^3t^3 + 3s^2t^4 + st^5 + t^6.$$

Z powyższego wyrażenia możemy już odczytać wszystkie informacje o wzorach, to znaczy o różnych (z dokładnością do obrotów) naszyjnikach. Analizując kolejne składniki W dowiadujemy się mianowicie, że istnieje

dokładnie jeden wzór naszyjnika złożonego z samych szmaragdów, jeden złożony z pięciu szmaragdów i jednego topaza, trzy różne wzory naszyników złożonych z czterech szmaragdów oraz dwóch topazów itd.

Jeśli interesuje nas jedynie liczba wszystkich wzorów, to zamiast korzystać z twierdzenia Pólya i liczyć szereg zliczający wzorów, wystarczy użyć Wniosku 4.2, to znaczy podstawić w zależności (4.16) zamiast zmiennych z_1, \dots, z_6 , liczbę 2, czyli licznosć zbioru figur. Dokonując takiego podstawienia otrzymujemy

$$P_G(2, \dots, 2) = 13.$$

Istnieje zatem dokładnie 13 różnych wzorów naszyjników o sześciu kamieniach, z których każdy może być szmaragdem albo topazem.

□

Przykład 4.24 Powróćmy do wspomnianego na początku tego rozdziału (patrz Przykład 4.2) problemu zliczania izomerów związków chemicznych, zawierających pierścień aromatyczny.

Zauważmy, że rozwiązany w poprzednim przykładzie problem zliczania różnych naszyjników jest w istocie identyczny z problemem zliczania takich izomerów. Zamiast bowiem mówić o umieszczeniu kamienia w sześciocolumnowym naszyjniku, możemy rozważyć tak zwane podstawianie pierścienia aromatycznego odpowiednimi atomami lub związkami (nazywanymi podstawnikami) w wierzchołkach tego pierścienia. Jedyna różnica polega więc na interpretacji wag figur.

Jeśli na przykład interesują nas izomery, w których pierścień aromatyczny podstawiany jest atomami wodoru i chloru, to wówczas wagami figur są: H (wodór) i Cl (chlor), a zatem szereg zliczający figur ma postać $H + Cl$. Używając takich wag figur otrzymujemy odpowiednik szeregu zliczającego wzorów z poprzedniego przykładu w następującej postaci:

$$W = H^6 + H^5Cl + 3H^4Cl^2 + 3H^3Cl^3 + 3H^2Cl^4 + HCl^4 + Cl^6.$$

Z powyższego zapisu łatwo możemy na przykład odczytać liczbę wszystkich izomerów chlorobenzenu o wzorze chemicznym $C_6H_2Cl_4$, w częsteczkach których oprócz sześciu atomów węgla w pierścieniu aromatycznym, występują jeszcze dwa atomy wodoru i cztery atomy chloru. Współczynnik przy składniku H^2Cl^4 w zapisanym wyżej szeregu zliczającym wzorów mówi nam, że teoretycznie mogą istnieć trzy takie izomery (i rzeczywiście istnieją; wszystkie one są pokazane na Rysunku 4.1).

Wyznaczenie indeksu cykli dla grupy obrotów sześciokąta pozwala nam również na rozwiązanie problemu zliczania izomerów, w których pierścień aromatyczny jest podstawiany dowolnymi sześcioma podstawnikami. Jeśli dopusczamy, że wszystkie one mogą być ewentualnie różne, to należy przyjąć następujący szereg zliczający figur:

$$p_1 + p_2 + \dots + p_6,$$

gdzie p_i zastępuje symbol i -tego możliwego podstawnika. Wstawiając powyższy szereg zliczający figur do indeksu cykli grupy obrotów sześciokąta 4.16, otrzymujemy następujące wyrażenie:⁸

$$\begin{aligned} W' = & p_1^6 + p_1^5 p_2 + 3 p_1^4 p_2^2 + 3 p_1^3 p_2^3 + 3 p_1^2 p_2^4 + p_1 p_2^5 + p_2^6 + p_1^5 p_3 + 3 p_1^4 p_2 p_3 + \\ & 6 p_1^3 p_2^2 p_3 + 6 p_1^2 p_3^3 + 3 p_1 p_2^4 p_3 + p_2^5 p_3 + 3 p_1^4 p_3^2 + 6 p_1^3 p_2 p_3^2 + 11 p_1^2 p_2^2 p_3^2 + \\ & 6 p_1 p_2^3 p_3^2 + 3 p_2^4 p_3^2 + 3 p_1^3 p_3^3 + 6 p_1^2 p_2 p_3^3 + 6 p_1 p_2^2 p_3^3 + 3 p_2^3 p_3^3 + 3 p_1^2 p_3^4 + \\ & 3 p_1 p_2 p_3^4 + 3 p_2^2 p_3^4 + p_1 p_3^5 + p_2 p_3^5 + p_3^6 + p_1^5 p_4 + 3 p_1^4 p_2 p_4 + 6 p_1^3 p_2^2 p_4 + \\ & 6 p_1^2 p_2^3 p_4 + 3 p_1 p_2^4 p_4 + p_2^5 p_4 + 3 p_1^4 p_3 p_4 + 10 p_1^3 p_2 p_3 p_4 + 16 p_1^2 p_2^2 p_3 p_4 + \\ & 10 p_1 p_2^3 p_3 p_4 + 3 p_2^4 p_3 p_4 + 6 p_1^3 p_3^2 p_4 + 16 p_1^2 p_2 p_3^2 p_4 + 16 p_1 p_2^2 p_3^2 p_4 + \\ & 6 p_2^3 p_3^2 p_4 + 6 p_1^2 p_3^3 p_4 + 10 p_1 p_2 p_3^3 p_4 + 6 p_2^2 p_3^3 p_4 + 3 p_1 p_3^4 p_4 + 3 p_2 p_3^4 p_4 + \\ & p_3^5 p_4 + 3 p_1^4 p_4^2 + 6 p_1^3 p_2 p_4^2 + 11 p_1^2 p_2^2 p_4^2 + 6 p_1 p_2^3 p_4^2 + 3 p_2^4 p_4^2 + 6 p_1^3 p_3 p_4^2 + \\ & 16 p_1^2 p_2 p_3 p_4^2 + 16 p_1 p_2^2 p_3 p_4^2 + 6 p_2^3 p_3 p_4^2 + 11 p_1^2 p_3^2 p_4^2 + 16 p_1 p_2 p_3^2 p_4^2 + \\ & 11 p_2^2 p_3^2 p_4^2 + 6 p_1 p_3^3 p_4^2 + 6 p_2 p_3^3 p_4^2 + 3 p_3^4 p_4^2 + 3 p_1^3 p_4^3 + 6 p_1^2 p_2 p_4^3 + \\ & 6 p_1 p_2^2 p_4^3 + 3 p_2^3 p_4^3 + 6 p_1^2 p_3 p_4^3 + 10 p_1 p_2 p_3 p_4^3 + 6 p_2^2 p_3 p_4^3 + 6 p_1 p_3^2 p_4^3 + \\ & 6 p_2 p_3^2 p_4^3 + 3 p_3^3 p_4^3 + 3 p_1^2 p_4^4 + 3 p_2^2 p_4^4 + 3 p_1 p_3 p_4^4 + 3 p_2 p_3 p_4^4 + \\ & 3 p_3^2 p_4^4 + p_1 p_5^5 + p_2 p_5^5 + p_3 p_5^6 + p_1^5 p_5 + 3 p_1^4 p_2 p_5 + 6 p_1^3 p_2^2 p_5 + 6 p_1^2 p_2^3 p_5 + \\ & 3 p_1 p_2^4 p_5 + p_2^5 p_5 + 3 p_1^4 p_3 p_5 + 10 p_1^3 p_2 p_3 p_5 + 16 p_1^2 p_2^2 p_3 p_5 + 10 p_1 p_2^3 p_3 p_5 + \\ & 3 p_2^4 p_3 p_5 + 6 p_1^3 p_2^2 p_5 + 16 p_1^2 p_2 p_3^2 p_5 + 16 p_1 p_2^2 p_3^2 p_5 + 6 p_2^3 p_3^2 p_5 + \\ & 6 p_1^2 p_3 p_5 + 10 p_1 p_2 p_3^2 p_5 + 6 p_2^2 p_3^2 p_5 + 3 p_1 p_3^4 p_5 + 3 p_2 p_3^4 p_5 + p_3^5 p_5 + \\ & 3 p_1^4 p_4 p_5 + 10 p_1^3 p_2 p_4 p_5 + 16 p_1^2 p_2^2 p_4 p_5 + 10 p_1 p_2^3 p_4 p_5 + 3 p_2^4 p_4 p_5 + \\ & 10 p_1^3 p_3 p_4 p_5 + 30 p_1^2 p_2 p_3 p_4 p_5 + 30 p_1 p_2^2 p_3 p_4 p_5 + 10 p_2^3 p_3 p_4 p_5 + \\ & 16 p_1^2 p_3^2 p_4 p_5 + 30 p_1 p_2 p_3^2 p_4 p_5 + 16 p_2^2 p_3^2 p_4 p_5 + 10 p_1 p_3^3 p_4 p_5 + \\ & 10 p_2 p_3^3 p_4 p_5 + 3 p_3^4 p_4 p_5 + 6 p_1^3 p_2^4 p_5 + 16 p_1^2 p_2 p_4^2 p_5 + 16 p_1 p_2^2 p_4^2 p_5 + \\ & 6 p_2^3 p_4^2 p_5 + 16 p_1^2 p_3 p_4^2 p_5 + 30 p_1 p_2 p_3 p_4^2 p_5 + 16 p_2^2 p_3 p_4^2 p_5 + 16 p_1 p_3^2 p_4^2 p_5 + \\ & 16 p_2 p_3^2 p_4^2 p_5 + 6 p_3^3 p_4^2 p_5 + 6 p_1^2 p_4^3 p_5 + 10 p_1 p_2 p_4^3 p_5 + 6 p_2^2 p_4^3 p_5 + \\ & 10 p_1 p_3 p_4^3 p_5 + 10 p_2 p_3 p_4^3 p_5 + 6 p_3^4 p_4^3 p_5 + 3 p_1 p_4^4 p_5 + 3 p_2 p_4^4 p_5 + 3 p_3 p_4^4 p_5 + \\ & p_4^5 p_5 + 3 p_1^4 p_5^2 + 6 p_1^3 p_2 p_5^2 + 11 p_1^2 p_2^2 p_5^2 + 6 p_1 p_2^3 p_5^2 + 3 p_2^4 p_5^2 + 6 p_1^3 p_3 p_5^2 + \\ & 16 p_1^2 p_2 p_3 p_5^2 + 16 p_1 p_2^2 p_3 p_5^2 + 6 p_2^3 p_3 p_5^2 + 11 p_1^2 p_3^2 p_5^2 + 16 p_1 p_2 p_3^2 p_5^2 + \\ & 11 p_2^2 p_3^2 p_5^2 + 6 p_1 p_3^3 p_5^2 + 6 p_2 p_3^3 p_5^2 + 3 p_3^4 p_5^2 + 6 p_1^3 p_4 p_5^2 + 16 p_1^2 p_2 p_4 p_5^2 + \end{aligned}$$

⁸Nie jest prawdą, że nasi studenci są zmuszani do wypisywania z pamięci na egzaminie całego tego wyrażenia.

$$\begin{aligned}
& 16 p_1^2 p_2^2 p_4 p_5^2 + 6 p_2^3 p_4 p_5^2 + 16 p_1^2 p_3 p_4 p_5^2 + 30 p_1 p_2 p_3 p_4 p_5^2 + 16 p_2^2 p_3 p_4 p_5^2 + \\
& 16 p_1 p_3^2 p_4 p_5^2 + 16 p_2 p_3^2 p_4 p_5^2 + 6 p_3^3 p_4 p_5^2 + 11 p_1^2 p_4^2 p_5^2 + 16 p_1 p_2 p_4^2 p_5^2 + \\
& 11 p_2^2 p_4^2 p_5^2 + 16 p_1 p_3 p_4^2 p_5^2 + 16 p_2 p_3 p_4^2 p_5^2 + 11 p_3^2 p_4^2 p_5^2 + 6 p_1 p_4^2 p_5^2 + \\
& 6 p_2 p_4^3 p_5^2 + 6 p_3 p_4^3 p_5^2 + 3 p_4^4 p_5^2 + 3 p_1^3 p_5^3 + 6 p_1^2 p_2 p_5^3 + 6 p_1 p_2^2 p_5^3 + 3 p_2^3 p_5^3 + \\
& 6 p_1^2 p_3 p_5^3 + 10 p_1 p_2 p_3 p_5^3 + 6 p_2^2 p_3 p_5^3 + 6 p_1 p_3^2 p_5^3 + 6 p_2 p_3^2 p_5^3 + 3 p_3^3 p_5^3 + \\
& 6 p_1^2 p_4 p_5^3 + 10 p_1 p_2 p_4 p_5^3 + 6 p_2^2 p_4 p_5^3 + 10 p_1 p_3 p_4 p_5^3 + 10 p_2 p_3 p_4 p_5^3 + \\
& 6 p_3^2 p_4 p_5^3 + 6 p_1 p_4^2 p_5^3 + 6 p_2 p_4^2 p_5^3 + 6 p_3 p_4^2 p_5^3 + 3 p_4^3 p_5^3 + 3 p_1^2 p_5^4 + 3 p_1 p_2 p_5^4 + \\
& 3 p_2^2 p_5^4 + 3 p_1 p_3 p_5^4 + 3 p_2 p_3 p_5^4 + 3 p_3^2 p_5^4 + 3 p_1 p_4 p_5^4 + 3 p_2 p_4 p_5^4 + 3 p_3 p_4 p_5^4 + \\
& 3 p_4^2 p_5^4 + p_1 p_5^5 + p_2 p_5^5 + p_3 p_5^5 + p_4 p_5^5 + p_5^6 + p_1^5 p_6 + 3 p_1^4 p_2 p_6 + 6 p_1^3 p_2^2 p_6 + \\
& 6 p_1^2 p_2^3 p_6 + 3 p_1 p_2^4 p_6 + p_2^5 p_6 + 3 p_1^4 p_3 p_6 + 10 p_1^3 p_2 p_3 p_6 + 16 p_1^2 p_2^2 p_3 p_6 + \\
& 10 p_1 p_2^3 p_3 p_6 + 3 p_2^4 p_3 p_6 + 6 p_1^3 p_3^2 p_6 + 16 p_1^2 p_2 p_3^2 p_6 + 16 p_1 p_2^2 p_3^2 p_6 + \\
& 6 p_2^3 p_3^2 p_6 + 6 p_1^2 p_3^3 p_6 + 10 p_1 p_2 p_3^3 p_6 + 6 p_2^2 p_3^3 p_6 + 3 p_1 p_3^4 p_6 + 3 p_2 p_3^4 p_6 + \\
& p_3^5 p_6 + 3 p_1^4 p_4 p_6 + 10 p_1^3 p_2 p_4 p_6 + 16 p_1^2 p_2^2 p_4 p_6 + 10 p_1 p_2^3 p_4 p_6 + \\
& 3 p_2^4 p_4 p_6 + 10 p_1^3 p_3 p_4 p_6 + 30 p_1^2 p_2 p_3 p_4 p_6 + 30 p_1 p_2^2 p_3 p_4 p_6 + \\
& 10 p_2^3 p_3 p_4 p_6 + 16 p_1^2 p_3^2 p_4 p_6 + 30 p_1 p_2 p_3^2 p_4 p_6 + 16 p_2^2 p_3^2 p_4 p_6 + \\
& 10 p_1 p_3^3 p_4 p_6 + 10 p_2 p_3^3 p_4 p_6 + 3 p_3^4 p_4 p_6 + 6 p_1^3 p_4^2 p_6 + 16 p_1^2 p_2 p_4^2 p_6 + \\
& 16 p_1 p_2^2 p_4^2 p_6 + 6 p_2^3 p_4^2 p_6 + 16 p_1^2 p_3 p_4^2 p_6 + 30 p_1 p_2 p_3 p_4^2 p_6 + 16 p_2^2 p_3 p_4^2 p_6 + \\
& 16 p_1 p_3^2 p_4^2 p_6 + 16 p_2 p_3^2 p_4^2 p_6 + 6 p_3^3 p_4^2 p_6 + 10 p_1 p_2 p_3^2 p_4^2 p_6 + \\
& 6 p_2^2 p_4^3 p_6 + 10 p_1 p_3 p_4^3 p_6 + 10 p_2 p_3 p_4^3 p_6 + 6 p_3^2 p_4^3 p_6 + 3 p_1 p_4^4 p_6 + \\
& 3 p_2 p_4^4 p_6 + 3 p_3 p_4^4 p_6 + p_4^5 p_6 + 3 p_1^4 p_5 p_6 + 10 p_1^3 p_2 p_5 p_6 + 16 p_1^2 p_2^2 p_5 p_6 + \\
& 10 p_1 p_2^3 p_5 p_6 + 3 p_2^4 p_5 p_6 + 10 p_1^3 p_3 p_5 p_6 + 30 p_1^2 p_2 p_3 p_5 p_6 + 30 p_1 p_2^2 p_3 p_5 p_6 + \\
& 10 p_2^3 p_3 p_5 p_6 + 16 p_1^2 p_3^2 p_5 p_6 + 30 p_1 p_2 p_3^2 p_5 p_6 + 16 p_2^2 p_3 p_5 p_6 + \\
& 10 p_1 p_3^3 p_5 p_6 + 10 p_2 p_3^3 p_5 p_6 + 3 p_3^4 p_5 p_6 + 10 p_1^3 p_4 p_5 p_6 + 30 p_1^2 p_2 p_4 p_5 p_6 + \\
& 30 p_1 p_2^2 p_4 p_5 p_6 + 10 p_2^3 p_4 p_5 p_6 + 30 p_1^2 p_3 p_4 p_5 p_6 + 60 p_1 p_2 p_3 p_4 p_5 p_6 + \\
& 30 p_2^2 p_3 p_4 p_5 p_6 + 30 p_1 p_3^2 p_4 p_5 p_6 + 30 p_2 p_3^2 p_4 p_5 p_6 + 10 p_3^3 p_4 p_5 p_6 + \\
& 16 p_1^2 p_4^2 p_5 p_6 + 30 p_1 p_2 p_4^2 p_5 p_6 + 16 p_2^2 p_4^2 p_5 p_6 + 30 p_1 p_3 p_4^2 p_5 p_6 + \\
& 30 p_2 p_3 p_4^2 p_5 p_6 + 16 p_3^2 p_4^2 p_5 p_6 + 10 p_1 p_4^3 p_5 p_6 + 10 p_2 p_4^3 p_5 p_6 + \\
& 10 p_3 p_4^3 p_5 p_6 + 3 p_4^4 p_5 p_6 + 6 p_1^3 p_5^2 p_6 + 16 p_1^2 p_2 p_5^2 p_6 + 16 p_1 p_2^2 p_5^2 p_6 + \\
& 6 p_2^3 p_5^2 p_6 + 16 p_1^2 p_3 p_5^2 p_6 + 30 p_1 p_2 p_3 p_5^2 p_6 + 16 p_2^2 p_3 p_5^2 p_6 + 16 p_1 p_3^2 p_5^2 p_6 + \\
& 16 p_2 p_3^2 p_5^2 p_6 + 6 p_3^3 p_5^2 p_6 + 16 p_1^2 p_4 p_5^2 p_6 + 30 p_1 p_2 p_4 p_5^2 p_6 + \\
& 16 p_2^2 p_4 p_5^2 p_6 + 30 p_1 p_3 p_4 p_5^2 p_6 + 30 p_2 p_3 p_4 p_5^2 p_6 + 16 p_3^2 p_4 p_5^2 p_6 + \\
& 16 p_1 p_4^2 p_5^2 p_6 + 16 p_2 p_4^2 p_5^2 p_6 + 16 p_3 p_4^2 p_5^2 p_6 + 6 p_4^3 p_5^2 p_6 + 6 p_1^2 p_5^3 p_6 + \\
& 10 p_1 p_2 p_5^3 p_6 + 6 p_2^2 p_5^3 p_6 + 10 p_1 p_3 p_5^3 p_6 + 10 p_2 p_3 p_5^3 p_6 + 6 p_3^2 p_5^3 p_6 + \\
& 10 p_1 p_4 p_5^3 p_6 + 10 p_2 p_4 p_5^3 p_6 + 10 p_3 p_4 p_5^3 p_6 + 6 p_4^2 p_5^3 p_6 + 6 p_1^3 p_5^4 p_6 + \\
& 3 p_2 p_5^4 p_6 + 3 p_3 p_5^4 p_6 + 3 p_4 p_5^4 p_6 + 3 p_1 p_5^5 p_6 + 3 p_2 p_5^5 p_6 + 3 p_3 p_5^5 p_6 + \\
& 3 p_4 p_5^5 p_6 + 3 p_5^6 p_6 + p_1 p_6^5 + p_2 p_6^5 + p_3 p_6^5 + p_4 p_6^5 + p_5 p_6^5 + p_6^6.
\end{aligned}$$

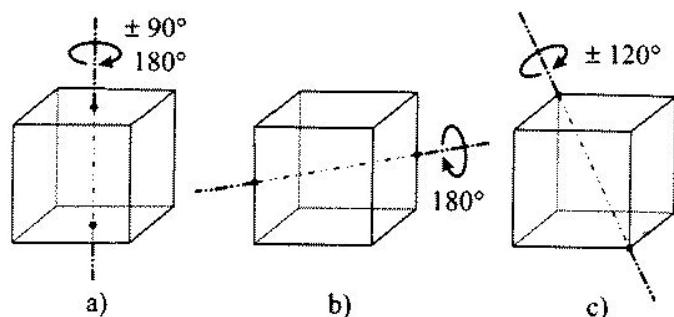
4.4. OGÓLNE ZAGADNIENIE ZLICZANIA

$$\begin{aligned}
& 11 p_1^2 p_4^2 p_6^2 + 16 p_1 p_2 p_4^2 p_6^2 + 11 p_2^2 p_4^2 p_6^2 + 16 p_1 p_3 p_4^2 p_6^2 + 16 p_2 p_3 p_4^2 p_6^2 + \\
& 11 p_3^2 p_4^2 p_6^2 + 6 p_1 p_4^3 p_6^2 + 6 p_2 p_4^3 p_6^2 + 6 p_3 p_4^3 p_6^2 + 3 p_4^4 p_6^2 + 6 p_1^3 p_5 p_6^2 + \\
& 16 p_1^2 p_2 p_5 p_6^2 + 16 p_1 p_2^2 p_5 p_6^2 + 6 p_2^3 p_5 p_6^2 + 16 p_1^2 p_3 p_5 p_6^2 + 30 p_1 p_2 p_3 p_5 p_6^2 + \\
& 16 p_2^2 p_3 p_5 p_6^2 + 16 p_1 p_3^2 p_5 p_6^2 + 16 p_2 p_3^2 p_5 p_6^2 + 6 p_3^3 p_5 p_6^2 + 16 p_1^2 p_4 p_5 p_6^2 + \\
& 30 p_1 p_2 p_4 p_5 p_6^2 + 16 p_2^2 p_4 p_5 p_6^2 + 30 p_1 p_3 p_4 p_5 p_6^2 + 30 p_2 p_3 p_4 p_5 p_6^2 + \\
& 16 p_3^2 p_4 p_5 p_6^2 + 16 p_1 p_4^2 p_5 p_6^2 + 16 p_2 p_4^2 p_5 p_6^2 + 16 p_3 p_4^2 p_5 p_6^2 + 6 p_4^3 p_5 p_6^2 + \\
& 11 p_1^2 p_5 p_6^2 + 16 p_1 p_2 p_5 p_6^2 + 11 p_2^2 p_5 p_6^2 + 16 p_1 p_3 p_5 p_6^2 + 16 p_2 p_3 p_5 p_6^2 + \\
& 11 p_3^2 p_5 p_6^2 + 16 p_1 p_4 p_5 p_6^2 + 16 p_2 p_4 p_5 p_6^2 + 16 p_3 p_4 p_5 p_6^2 + 11 p_4^2 p_5 p_6^2 + \\
& 6 p_1 p_5^3 p_6^2 + 8 p_2 p_5^3 p_6^2 + 6 p_3 p_5^3 p_6^2 + 6 p_4 p_5^3 p_6^2 + 3 p_5^4 p_6^2 + 3 p_1^3 p_6^3 + \\
& 6 p_1^2 p_2 p_6^3 + 6 p_1 p_2^2 p_6^3 + 3 p_2^3 p_6^3 + 6 p_1^2 p_3 p_6^3 + 10 p_1 p_2 p_3 p_6^3 + 6 p_2^2 p_3 p_6^3 + \\
& 6 p_1 p_3^2 p_6^3 + 6 p_2 p_3^2 p_6^3 + 3 p_3^3 p_6^3 + 6 p_1^2 p_4 p_6^3 + 6 p_2^2 p_4 p_6^3 + 6 p_3^2 p_4 p_6^3 + \\
& 10 p_1 p_3 p_4 p_6^3 + 10 p_2 p_3 p_4 p_6^3 + 6 p_4^2 p_6^3 + 6 p_1 p_5 p_6^3 + 6 p_2 p_5 p_6^3 + 6 p_3 p_5 p_6^3 + \\
& 6 p_4 p_5 p_6^3 + 3 p_5^2 p_6^3 + 6 p_1^2 p_5 p_6^3 + 10 p_1 p_2 p_5 p_6^3 + 6 p_2^2 p_5 p_6^3 + 10 p_1 p_3 p_5 p_6^3 + \\
& 10 p_2 p_3 p_5 p_6^3 + 6 p_3^2 p_5 p_6^3 + 10 p_1 p_4 p_5 p_6^3 + 10 p_2 p_4 p_5 p_6^3 + 10 p_3 p_4 p_5 p_6^3 + \\
& 6 p_4^2 p_5 p_6^3 + 6 p_1 p_5^2 p_6^3 + 6 p_2 p_5^2 p_6^3 + 6 p_3 p_5^2 p_6^3 + 6 p_4^3 p_5 p_6^3 + 3 p_5^4 p_6^3 + \\
& 3 p_1^3 p_6^4 + 3 p_2^2 p_6^4 + 3 p_3^2 p_6^4 + 3 p_4^2 p_6^4 + 3 p_5^2 p_6^4 + 3 p_1 p_6^5 + 3 p_2 p_6^5 + 3 p_3 p_6^5 + \\
& 3 p_4 p_6^5 + 3 p_5 p_6^5 + 3 p_6^6.
\end{aligned}$$

Powyższe wyrażenie jest już znacznie bardziej skomplikowane niż używany poprzednio szereg zliczający wzorów dla dwóch podstawników. Zawiera jednak informacje o wszystkich możliwych różnych strukturach związków opartych na jednym pierścieniu aromatycznym. Analizując powyższe wyrażenie możemy na przykład stwierdzić, że zawsze istnieje dokładnie 11 różnych struktur, w których używamy trzech różnych podstawników i każdy z nich jest wykorzystywany dwukrotnie. Mówi o tym współczynnik liczbowy równy 11, stojący przy każdym z wyrażeń o postaci $p_{i_1}^2 p_{i_2}^2 p_{i_3}^2$, gdzie i_1, i_2, i_3 , są dowolnymi różnymi indeksami ze zbioru $\{1, 2, \dots, 6\}$. \square

Przykład 4.25 Zadanie, które rozwiążemy w tym przykładzie, jest bardzo podobne do problemu zliczania dwukolorowych tablic z Przykładu 4.11. Chcemy mianowicie policzyć, na ile sposobów można pokolorować dwoma kolorami wierzchołki sześcianu. Interesują nas przy tym jedynie różne sposoby pokolorowania, to znaczy takie, których nie da się otrzymać z siebie w wyniku dowolnych obrotów sześcianu. Wszystkie takie obroty przedstawione są na Rysunku 4.20.

Zbiorem miejsc w naszym problemie są wierzchołki sześcianu. Ponumerujemy je liczbami naturalnymi od 1 do 8. Mamy więc $X = \{1, \dots, 8\}$.



Rysunek 4.20: Obroty sześciangu z Przykładu 4.25.

Figurami są kolory, którymi możemy pomalować wierzchołki. Przyjmijmy, że mogą to być kolor biały albo czarny, a następnie przyporządkujmy figurom wagę: b dla koloru białego i c – dla czarnego. Szeregiem zliczającym figur jest więc następujące wyrażenie:

$$b + c.$$

Należy teraz wyznaczyć indeks cykli grupy obrotów sześciangu. Tym razem nie będziemy już szczegółowo wypisywać wszystkich permutacji i odpowiadających im obrotów, a jedynie w poniżej tabeli zestawimy najważniejsze dane, które są niezbędne do wyznaczenia indeksu cykli interesującej nas grupy permutacji. Postępowanie prowadzące do wyznaczeniu tych danych jest analogiczne jak w poprzednich przykładach.

| obroty sześciangu | typ permutacji |
|---|----------------|
| brak obrotu (permutacja identycznościowa) | 1^8 |
| 3 obroty typu a) o 180° | 2^4 |
| 6 obrotów typu a) o 90° | 4^2 |
| 6 obrotów typu b) | 2^4 |
| 8 obrotów typu c) | $1^2 3^2$ |

Z powyższej tabeli wynika, że grupa G obrotów sześciangu liczy 24 elementy, a indeks cykli tej grupy ma następującą postać:

$$P_G(z_1, \dots, z_8) = \frac{1}{24} (z_1^8 + 9z_2^4 + 6z_4^2 + 8z_1^2 z_3^2). \quad (4.17)$$

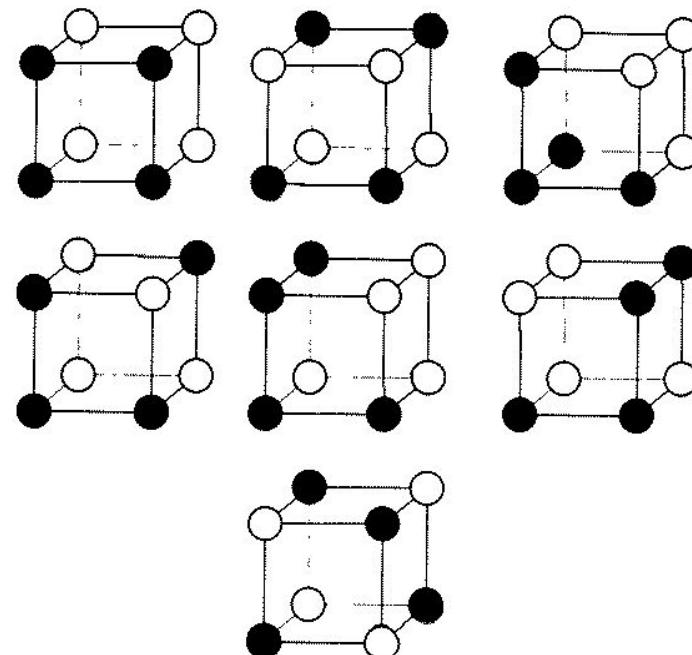
4.4. OGÓLNE ZAGADNIENIE ZLICZANIA

Wstawiając szereg zliczający figur do powyższego wyrażenia otrzymujemy poszukiwany szereg zliczający wzorów:

$$\begin{aligned} W &= \frac{1}{24} [(b+c)^8 + 9(b^2+c^2)^4 + 6(b^4+c^4)^2 + 8(b+c)^2(b^3+c^3)^2] = \\ &= b^8 + b^7 c + 3b^6 c^2 + 3b^5 c^3 + 7b^4 c^4 + 3b^3 c^5 + 3b^2 c^6 + b c^7 + c^8. \end{aligned}$$

Wyrażenie powyższe zawiera wszystkie informacje o różnych sposobach pomalowania wierzchołków sześcianu, jeśli w każdym z tych wierzchołków możemy użyć jednego z dwóch kolorów: białego albo czarnego.

Wiemy na przykład, że jeśli zdecydujemy się na takie pokolorowanie, w którym cztery wierzchołki mają kolor czarny, a pozostałe cztery – kolor biały, to istnieje dokładnie siedem różnych sposobów dokonania tego. Wszystkie one pokazane są na Rysunku 4.21.



Rysunek 4.21: Siedem różnych sposobów pokolorowania wierzchołków sześciangu, w których połowa wierzchołków ma kolor czarny, a połowa – biały.

Podobnie jak w poprzednich przykładach, interpretacja wag figur może być różna od przyjętej powyżej. Na przykład, zamiast mówić o kolorowaniu wierzchołków sześciianu, możemy rozważać liczbę różnych struktur wieloprocesorowych, tworzących tak zwany hipersześcian (patrz np. [4]). Dla przypadku $n = 3$ wszystkie informacje o liczbie takich struktur, w których rozważamy dwa typy procesorów, zawarte są w wyprowadzonym właśnie szeregu zliczającym wzorów W .

Gdyby natomiast interesowały nas struktury, w których każdy z procesorów może być jednego z trzech typów (na przykład a , b albo c), to wówczas należałoby do indeksu cykli grupy obrotów sześciianu wstawić następujący szereg zliczający figur:

$$a + b + c.$$

Otrzymalibyśmy wtedy następujący szereg zliczający wzorów:

$$\begin{aligned} W' = & a^8 + a^7 b + 3 a^6 b^2 + 3 a^5 b^3 + 7 a^4 b^4 + 3 a^3 b^5 + 3 a^2 b^6 + a b^7 + b^8 + \\ & a^7 c + 3 a^6 b c + 7 a^5 b^2 c + 13 a^4 b^3 c + 13 a^3 b^4 c + 7 a^2 b^5 c + 3 a b^6 c + b^7 c + \\ & 3 a^6 c^2 + 7 a^5 b c^2 + 22 a^4 b^2 c^2 + 24 a^3 b^3 c^2 + 22 a^2 b^4 c^2 + 7 a b^5 c^2 + 3 b^6 c^2 + \\ & 3 a^5 c^3 + 13 a^4 b c^3 + 24 a^3 b^2 c^3 + 24 a^2 b^3 c^3 + 13 a b^4 c^3 + 3 b^5 c^3 + 7 a^4 c^4 + \\ & 13 a^3 b c^4 + 22 a^2 b^2 c^4 + 13 a b^3 c^4 + 7 b^4 c^4 + 3 a^3 c^5 + 7 a^2 b c^5 + 7 a b^2 c^5 + \\ & 3 b^3 c^5 + 3 a^2 c^6 + 3 a b c^6 + 3 b^2 c^6 + a c^7 + b c^7 + c^8. \end{aligned}$$

Wyrażenie powyższe jest już nieco bardziej skomplikowane, ale jego interpretacja jest równie łatwa, jak poprzednio.

Jest oczywiste, że w miarę jak zwiększamy liczbę typów procesorów, to szereg zliczający wzorów ma coraz więcej elementów. Na przykład, jeśli interesują nas cztery typy procesorów a, b, c, d , to uzyskujemy następujące wyrażenie:

$$\begin{aligned} W'' = & a^8 + a^7 b + 3 a^6 b^2 + 3 a^5 b^3 + 7 a^4 b^4 + 3 a^3 b^5 + 3 a^2 b^6 + a b^7 + b^8 + a^7 c + \\ & 3 a^6 b c + 7 a^5 b^2 c + 13 a^4 b^3 c + 13 a^3 b^4 c + 7 a^2 b^5 c + 3 a b^6 c + b^7 c + 3 a^6 c^2 + \\ & 7 a^5 b c^2 + 22 a^4 b^2 c^2 + 24 a^3 b^3 c^2 + 22 a^2 b^4 c^2 + 7 a b^5 c^2 + 3 b^6 c^2 + 3 a^5 c^3 + \\ & 13 a^4 b c^3 + 24 a^3 b^2 c^3 + 24 a^2 b^3 c^3 + 13 a b^4 c^3 + 3 b^5 c^3 + 7 a^4 c^4 + 13 a^3 b c^4 + \\ & 22 a^2 b^2 c^4 + 13 a b^3 c^4 + 7 b^4 c^4 + 3 a^3 c^5 + 7 a^2 b c^5 + 7 a b^2 c^5 + 3 b^3 c^5 + 3 a^2 c^6 + \\ & 3 a b c^6 + 3 b^2 c^6 + a c^7 + b c^7 + c^8 + a^7 d + 3 a^6 b d + 7 a^5 b^2 d + 13 a^4 b^3 d + \\ & 13 a^3 b^4 d + 7 a^2 b^5 d + 3 a b^6 d + b^7 d + 3 a^6 c d + 14 a^5 b c d + 35 a^4 b^2 c d + \\ & 48 a^3 b^3 c d + 35 a^2 b^4 c d + 14 a b^5 c d + 3 b^6 c d + 7 a^5 c^2 d + 35 a^4 b c^2 d + \\ & 70 a^3 b^2 c^2 d + 70 a^2 b^3 c^2 d + 35 a b^4 c^2 d + 7 b^5 c^2 d + 13 a^4 c^3 d + 48 a^3 b c^3 d + \\ & 70 a^2 b^2 c^3 d + 48 a b^3 c^3 d + 13 b^4 c^3 d + 13 a^3 c^4 d + 35 a^2 b c^4 d + 35 a b^2 c^4 d + \\ & 13 b^3 c^4 d + 7 a^2 c^5 d + 14 a b c^5 d + 7 b^2 c^5 d + 3 a c^6 d + 3 b c^6 d + c^7 d + 3 a^6 d^2 + \end{aligned}$$

4.4. OGÓLNE ZAGADNIENIE ZLICZANIA

$$\begin{aligned} & 7 a^5 b d^2 + 22 a^4 b^2 d^2 + 24 a^3 b^3 d^2 + 22 a^2 b^4 d^2 + 7 a b^5 d^2 + 3 b^6 d^2 + 7 a^5 c d^2 + \\ & 35 a^4 b c d^2 + 70 a^3 b^2 c d^2 + 70 a^2 b^3 c d^2 + 35 a b^4 c d^2 + 7 b^5 c d^2 + 22 a^4 c^2 d^2 + \\ & 70 a^3 b c^2 d^2 + 114 a^2 b^2 c^2 d^2 + 70 a b^3 c^2 d^2 + 22 b^4 c^2 d^2 + 24 a^3 c^3 d^2 + \\ & 70 a^2 b c^3 d^2 + 70 a b^2 c^3 d^2 + 24 b^3 c^3 d^2 + 22 a^2 c^4 d^2 + 35 a b c^4 d^2 + 22 b^2 c^4 d^2 + \\ & 7 a c^5 d^2 + 7 b c^5 d^2 + 3 c^6 d^2 + 3 a^5 d^3 + 13 a^4 b d^3 + 24 a^3 b^2 d^3 + 24 a^2 b^3 d^3 + \\ & 13 a b^4 d^3 + 3 b^5 d^3 + 13 a^4 c d^3 + 48 a^3 b c d^3 + 70 a^2 b^2 c d^3 + 48 a b^3 c d^3 + \\ & 13 b^4 c d^3 + 24 a^3 c^2 d^3 + 70 a^2 b c^2 d^3 + 70 a b^2 c^2 d^3 + 24 b^3 c^2 d^3 + 24 a^2 c^3 d^3 + \\ & 48 a b c^3 d^3 + 24 b^2 c^3 d^3 + 13 a c^4 d^3 + 3 c^5 d^3 + 7 a^4 d^4 + 13 a^3 b d^4 + \\ & 22 a^2 b^2 d^4 + 13 a b^3 d^4 + 7 b^4 d^4 + 13 a^3 c d^4 + 35 a^2 b c d^4 + 35 a b^2 c d^4 + \\ & 13 b^3 c d^4 + 22 a^2 c^2 d^4 + 35 a b c^2 d^4 + 22 b^2 c^2 d^4 + 13 a c^3 d^4 + 13 b c^3 d^4 + \\ & 7 c^4 d^4 + 3 a^3 d^5 + 7 a^2 b d^5 + 7 a b^2 d^5 + 3 b^3 d^5 + 7 a^2 c d^5 + 14 a b c d^5 + \\ & 7 b^2 c d^5 + 7 a c^2 d^5 + 7 b c^2 d^5 + 3 c^3 d^5 + 3 a^2 d^6 + 3 a b d^6 + 3 b^2 d^6 + 3 a c d^6 + \\ & 3 b c d^6 + 3 c^2 d^6 + a d^7 + b d^7 + c d^7 + d^8. \end{aligned}$$

Jak poprzednio, liczbę wszystkich możliwych struktur możemy odczytać analizując współczynniki liczbowe przy odpowiednich wyrażeniach. Na przykład współczynnik przy $a^2 b^2 c^2 d^2$ mówi nam, że dla $n = 3$ istnieje dokładnie 114 różnych struktur typu hipersześcianu, zawierających cztery pary różnych procesorów. \square

Dodatek

Rachunek zdań

Na poniższych rysunkach podane są tak zwane tabele prawdy dla najważniejszych zdań złożonych.

Obszerne wprowadzenie do rachunku zdań i predykatów można znaleźć na przykład w [24, 29].

| $[p]$ | $[q]$ | $[\neg q]$ | $[p \vee q]$ | $[p \wedge q]$ | $[p \Rightarrow q]$ | $[p \Leftrightarrow q]$ |
|-------|-------|------------|--------------|----------------|---------------------|-------------------------|
| 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 |

| $[p]$ | $[q]$ | $[\neg p]$ | $[\neg q]$ | $[p \wedge q]$ | $[\neg(p \wedge q)]$ | $[\neg p \vee \neg q]$ |
|-------|-------|------------|------------|----------------|----------------------|------------------------|
| 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 |

Rysunek 4.22: Tabele prawdy dla negacji, alternatywy, koniunkcji, implikacji i równoważności.

| $[p]$ | $[q]$ | $[\neg p]$ | $[\neg q]$ | $[p \vee q]$ | $[\neg(p \vee q)]$ | $[\neg p \wedge \neg q]$ |
|-------|-------|------------|------------|--------------|--------------------|--------------------------|
| 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 |

| $[p]$ | $[q]$ | $[p \Rightarrow q]$ | $[\neg p \vee q]$ | $[\neg q \Rightarrow \neg p]$ |
|-------|-------|---------------------|-------------------|-------------------------------|
| 0 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 |

| $[p]$ | $[p \Rightarrow p]$ | $[p \Leftrightarrow p]$ | $[p \vee \neg p]$ | $[\neg(p \wedge \neg p)]$ |
|-------|---------------------|-------------------------|-------------------|---------------------------|
| 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 |

| $[p]$ | $[q]$ | $[(p \vee q) \Rightarrow (\neg p \Rightarrow q)]$ |
|-------|-------|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

Rysunek 4.23: Tabele prawdy dla wybranych zdań złożonych.

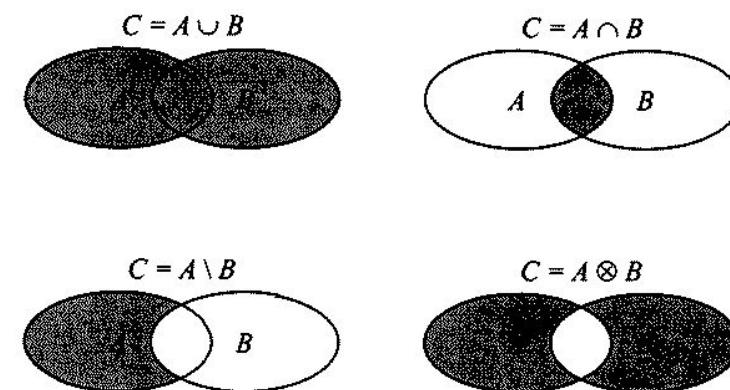
Zbiory i działania na zbiorach

Zbiór jest pojęciem podstawowym w matematyce, służącym do opisu rzeczywistych obiektów. Mówimy o zbiorach liczb, zbiorach symboli alfabetu, zbiorach instrukcji programu komputerowego itp. Zbiory oznaczamy zwykle dużymi literami alfabetu łacińskiego.

Liczبę elementów zbioru skończonego A nazywamy *licznością* (albo *mocą*) *zbioru A* i oznaczamy symbolem $|A|$.

Zbiór, który nie zawiera żadnego elementu, nazywany jest *zbiorem pustym* i oznaczany jest symbolem \emptyset . Liczność zbioru pustego jest równa 0.

Na zbiorach można wykonywać różne działania. Wygodną ilustracją zbiorów i dokonywanych na nich działań są tak zwane *diagramy Venna*⁹. Zbiory są w nich reprezentowane przez wyróżnione obszary płaszczyzny, na przykład koła lub elipsy. Rysunek 4.24 przedstawia diagramy Venna dla czterech podstawowych działań na zbiorach: sumy, przecięcia, różnicy i różnicy symetrycznej.



Rysunek 4.24: Diagramy Venna dla działań na zbiorach. Zbiór C, będący wynikiem działania, jest zacieniowany

⁹John Venn (1834–1923), matematyk angielski, który podał w wydanej w roku 1881 książce pt. *Symbolic Logic* wykresy obrazujące zależności między zakresami znaczeniowymi nazw.

Formuła Stirlinga do obliczania wartości $n!$

Formuła Stirlinga do obliczania przybliżonej wartości funkcji $n!$ należy do najbardziej znanych formuł aproksymujących. Dla $n \in \mathbb{N}$, $n > 0$, ma ona postać następującą:

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n.$$

gdzie $\pi \approx 3,14159$ jest ilorazem długości okregu przez jego średnicę, a $e \approx 2,7182$ jest podstawą logarytmów naturalnych.

Należy przy tym pamiętać, że wprawdzie błąd względny aproksymacji dla tej formuły dąży do zera przy $n \rightarrow \infty$, ale błąd bezwzględny dąży do nieskończoności. Poniższy przykład ilustruje tę sytuację.

Zastosujmy formułę Stirlinga do obliczenia przybliżonych wartości liczb 5 i 100. Otrzymujemy:

$$5! \approx 118,019.$$

Ponieważ $5! = 120$, to błąd bezwzględny jest tu równy około 1,98, a błąd względny jest stosunkowo duży i wynosi około 1,65%. Natomiast dla $n = 100$ otrzymujemy:

$$100! \approx 9,33 \cdot 10^{157}.$$

W tym przypadku błąd względny jest już bardzo mały i wynosi około 0,008%, natomiast błąd bezwzględny jest równy ok. $7,77 \cdot 10^{154}$.

W przypadkach, kiedy niezbędna jest większa dokładność, można użyć następującej wersji formuły Stirlinga:

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \left(1 + \frac{1}{12n} + \frac{1}{288n^2} - \frac{139}{51840n^3}\right).$$

Licząc przybliżoną wartość $n!$ dla $n = 5$ na podstawie powyższego wyrażenia otrzymamy $5! \approx 120,0000141$.

Własności funkcji sufit i podloga

Na stronie xi wprowadzone są oznaczenia dla dwóch ważnych funkcji, używanych w matematyce dyskretnej: *sufitu* i *podlogi*. Szczegółowe omówienie właściwości tych funkcji można znaleźć na przykład w [10]. Tu podamy bez dowodów jedynie najważniejsze z tych faktów.

Przypomnijmy, że dla dowolnej liczby rzeczywistej x ,

$$\lfloor x \rfloor = \max\{y \in \mathbb{Z} : y \leq x\},$$

$$\lceil x \rceil = \min\{y \in \mathbb{Z} : y \geq x\}.$$

Funkcję $\lfloor \cdot \rfloor$ nazywamy podlogą, natomiast funkcja $\lceil \cdot \rceil$ nosi nazwę sufitu. Analogicznie, liczby całkowite $\lfloor x \rfloor$ i $\lceil x \rceil$ nazywamy, odpowiednio, podlogą oraz sufitem liczby rzeczywistej x .

Podloga i sufit mogą być użyte do łatwego obliczania liczności zbioru liczb całkowitych, należących do dowolnego przedziału. Niech $a, b \in \mathbb{R}$. Jeśli $a \leq b$, to prawdziwe są następujące zależności:

$$|\mathbb{Z} \cap [a, b]| = \lceil b \rceil - \lfloor a \rfloor + 1,$$

$$|\mathbb{Z} \cap [a, b))| = \lceil b \rceil - \lceil a \rceil,$$

$$|\mathbb{Z} \cap (a, b])| = \lfloor b \rfloor - \lfloor a \rfloor.$$

Jeśli $a < b$, to zachodzi zależność:

$$|\mathbb{Z} \cap (a, b))| = \lceil b \rceil - \lfloor a \rfloor - 1.$$

Jeśli $f : \mathbb{R} \rightarrow \mathbb{R}$ jest ciągłą, monotonicznie rosnącą funkcją, dla której z faktu, że $f(x) \in \mathbb{Z}$ wynika, że $x \in \mathbb{Z}$, to wówczas zachodzą równości:

$$\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor,$$

oraz

$$\lceil f(x) \rceil = \lceil f(\lceil x \rceil) \rceil.$$

Bibliografia

- [1] M. Aigner, G.M. Ziegler – *Proofs from THE BOOK*. Springer-Verlag, Berlin, Heidelberg, New York 2001.
- [2] V. Bryant – *Aspekty kombinatoryki*. Wydawnictwa Naukowo-Techniczne, Warszawa 1997.
- [3] E.K.P. Chong, S.H. Żak – *An Introduction to Optimization*. John Wiley & Sons, Inc., New York 1996.
- [4] J. Chudzikiewicz – *Sieci komputerowe o strukturze logicznej typu hipersześcianu*. Instytut Automatyki i Robotyki WAT, Warszawa 2002.
- [5] J.H. Conway, R.K. Guy – *Księga liczb*. Wydawnictwa Naukowo-Techniczne, Warszawa 1999.
- [6] T.H. Cormen, C.E.L. Leiserson, R.L. Rivest – *Wprowadzenie do algorytmów*. Wydawnictwa Naukowo-Techniczne, Warszawa 1998.
- [7] M.S. Garey, D.S. Johnson – *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H. Freeman, New York 1979.
- [8] R.S. Garfinkel, G.L. Nemhauser – *Programowanie całkowitoliczbowe*. Państwowe Wydawnictwo Naukowe, Warszawa 1978.
- [9] R.L. Graham, M. Grötschel, L. Lovász – *Handbook of Combinatorics*. Elsevier, Amsterdam 1995.
- [10] R.L. Graham, D.E. Knuth, O. Patashnik – *Matematyka konkretna*. Wydawnictwo Naukowe PWN, Warszawa 1996.
- [11] D.H. Greene, D.E. Knuth – *Mathematics for the Analysis of Algorithms*. Birkhäuser, Boston 1982.

- [12] M. Hall, Jr. – *Combinatorial Theory*. John Wiley & Sons, Inc., New York 1998.
- [13] J.M. Harris, J.L. Hirst, M.J. Mossinghoff – *Combinatorics and Graph Theory*. Springer-Verlag, New York, Berlin, Heidelberg 2000.
- [14] E.L. Lawler, J.K. Lenstra, A.G. Rinnoy Kan, D. Shmoys (eds.) – *The Traveling Salesman Problem: A Guided Tour of Combinatorial Optimization*. John Wiley & Sons, Chichester, New York 1985.
- [15] R. Leitner – *Zarys matematyki wyższej dla studentów*. Wydawnictwa Naukowo-Techniczne, Warszawa 1997.
- [16] M. Libura, J. Sikorski – *Wykłady z matematyki dyskretnej. Część II: Teoria grafów*. Wydawnictwo WIT, Wyższa Szkoła Informatyki Stosowanej i Zarządzania, Warszawa 2008.
- [17] W. Lipski – *Kombinatoryka dla programistów*. Wydawnictwa Naukowo-Techniczne, Warszawa 2004.
- [18] W. Lipski, W. Marek – *Analiza kombinatoryczna*. Państwowe Wydawnictwo Naukowe, Warszawa 1986.
- [19] C.L. Liu – *Introduction to Combinatorial Mathematics*. McGraw-Hill Book Company, New York 1968.
- [20] L. Lovász, J. Pelikán, K. Vesztergombi – *Discrete Mathematics. Elementary and Beyond*. Springer-Verlag, New York, Berlin, Heidelberg 2003.
- [21] A.A. Milne – *Kubuś Puchatek*, Nasza Księgarnia, Warszawa 1971.
- [22] Z. Palka, A. Ruciński – *Niekonstruktywne metody matematyki dyskretniej*. Wydawnictwa Naukowo-Techniczne, Warszawa 1996.
- [23] Z. Palka, A. Ruciński – *Wykłady z kombinatoryki*. Wydawnictwa Naukowo-Techniczne, Warszawa 1998.
- [24] H. Rasiowa – *Wstęp do matematyki współczesnej*. Państwowe Wydawnictwo Naukowe, Warszawa 1969.
- [25] E.M. Reingold, J. Nievergelt, N. Deo – *Algorytmy kombinatoryczne*. Państwowe Wydawnictwo Naukowe, Warszawa 1985.

- [26] M. Rejewski – *An application of the theory of permutations in breaking the Enigma cipher*. Applicationes Mathematicae, XVI (1980) 543-559.
- [27] F.R. Roberts – *Applied Combinatorics*. Prentice- Hall, Inc. Englewood Cliffs, New Jersey 1984.
- [28] K.H. Rosen (ed.) – *Handbook of Discrete and Combinatorial Mathematics*. CRC Press, Boca Raton, London, New York, Washington, D.C. 2000.
- [29] K.A. Ross, Ch.R.B. Wright – *Matematyka dyskretna*. Wydawnictwo Naukowe PWN, Warszawa 1996.
- [30] A. Schrijver - *Combinatorial Optimization. Polyhedra and Efficiency*. Springer-Verlag, Berlin, Heidelberg, New York 2003.
- [31] M.M. Sysło – *Algorytmy*. Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1997.
- [32] M.M. Sysło, N. Deo, J.S. Kowalik – *Algorytmy optymalizacji dyskretnej*. Wydawnictwo Naukowe PWN, Warszawa 1995.
- [33] R.J. Wilson – *Wprowadzenie do teorii grafów*. Wydawnictwo Naukowe PWN, Warszawa 1998.

Spis rysункów

| | |
|---|----|
| 2.1 Rysunek grafu relacji z Przykładu 2.2. | 5 |
| 2.2 Rysunek grafu relacji $R = \{(1, 5), (5, 4), (4, 1), (2, 3), (3, 2)\}$ w zbiorze $X = \{1, 2, 3, 4, 5\}$ | 6 |
| 2.3 Tablica relacji z Przykładu 2.2. | 6 |
| 2.4 Graf funkcji z Przykładu 2.5. | 10 |
| 2.5 Liczby wszystkich funkcji ze zbioru n -elementowego w zbiór m -elementowy dla $m, n = 0, 1, \dots, 9$ | 12 |
| 2.6 Rozmieszczenie obiektów ze zbioru X definiowane przez funkcję $f \in Fun(X, Y)$ | 13 |
| 2.7 Liczby wszystkich funkcji różnowartościowych ze zbioru n -elementowego w zbiór m -elementowy dla $m, n = 0, 1, \dots, 10$ | 15 |
| 2.8 Liczby wszystkich bijekcji w zbiorze $Fun(X, Y)$, dla $ X = Y = n$, $n = 0, 1, \dots, 35$ | 16 |
| 2.9 Wszystkie rozmieszczenia uporządkowane obiektów ze zbioru $\{a, b\}$ w trzech pudełkach. | 18 |
| 2.10 Wartości potęg przyrastających dla $m, n = 0, 1, \dots, 9$. . . | 19 |
| 2.11 Wektory charakterystyczne wszystkich podzbiorów zbioru $X = \{a, b, c\}$ | 22 |
| 2.12 Dwa sposoby kodowania położenia obiektu w ośmiu sektorach. | 23 |
| 2.13 Wartości współczynników dwumianowych $\binom{n}{k}$ dla $k, n = 0, 1, \dots, 12$ | 28 |
| 2.14 Tabela liczb Stirlinga drugiego rodzaju $\{\binom{n}{k}\}$ i liczb Bella B_n dla $k, n = 0, 1, \dots, 10$ | 40 |
| 2.15 Drzewo podziałów zbioru $\{1, 2, 3\}$ | 42 |
| 2.16 Tabela liczb Stirlinga pierwszego rodzaju. | 43 |
| 2.17 Przydział wyznaczony przez surjkcję $f \in Fun(X, Y)$. . . | 46 |

| | | |
|------|---|-----|
| 2.18 | Liczności podziałów liczby naturalnej n na składniki | 50 |
| 2.19 | Diagramy Ferrersa dla podziałów sprzężonych $(5, 3, 2)$ oraz $(3, 3, 2, 1, 1)$ liczby 10 | 51 |
| 2.20 | Rysunek grafu relacji podzielności $ $ w zbiorze X , gdzie $X = \{2, 3, 5, 6, 10, 12, 25, 50, 70, 100\}$ | 53 |
| 2.21 | Diagram Hassego zbioru częściowo uporządkowanego $(X,)$ z Przykładu 2.15. | 55 |
| 2.22 | Diagram Hassego zbioru częściowo uporządkowanego $(X,)$ z zaznaczonymi (elementy zacieniowane) kresami dolnym i górnym podzbioru $A = \{10, 25, 50\}$ | 57 |
| 2.23 | Diagram Hassego przykładowej kraty. | 59 |
| 2.24 | Przykład diagramu Hassego zbioru częściowo uporządkowanego, który nie jest kratą. | 59 |
| 2.25 | Diagramy Hassego zbioru częściowo uporządkowanego $(X,)$ oraz łańcuchów i antylańcuchów pokrywających X | 63 |
| 2.26 | Związki między zbiorami $\mathcal{P}(X \times Y)$, $\text{Fun}(X, Y)$, $\text{Inj}(X, Y)$, $\text{Sur}(X, Y)$, $\text{Bij}(X, Y)$ oraz ich licznosciami dla $ X = Y $ | 64 |
| 2.27 | Związki między zbiorami $\mathcal{P}(X \times Y)$, $\text{Fun}(X, Y)$, $\text{Inj}(X, Y)$, $\text{Sur}(X, Y)$, $\text{Bij}(X, Y)$ oraz ich licznosciami dla $ X > Y $ | 65 |
| 2.28 | Związki między zbiorami $\mathcal{P}(X \times Y)$, $\text{Fun}(X, Y)$, $\text{Inj}(X, Y)$, $\text{Sur}(X, Y)$, $\text{Bij}(X, Y)$ oraz ich licznosciami dla $ X < Y $ | 65 |
| 3.1 | Zasada sumowania elementów przy tworzeniu splotu ciągów (a_i) oraz (b_i) | 74 |
| 3.2 | Wykres funkcji unimodalnej $f(x) = 0,7x^4 - 13x^3 + 6x^2 - 700x + 2000$ z Przykładu 3.13. | 85 |
| 3.3 | Wieże w Hanoi dla $i = 8$ | 88 |
| 3.4 | Zasada rekurencyjnego rozwiązywania problemu wież w Hanoi. | 89 |
| 3.5 | Diagramy Venna dla zbiorów z Przykładu 3.15. | 92 |
| 3.6 | Liczba nieporządków w S_n dla $n = 1, \dots, 20$ | 95 |
| 4.1 | Przykłady izomerów benzenu. | 102 |
| 4.2 | Rysunki grafów permutacji f i g z Przykładu 4.4 i kolejne kroki, wykonywane przy składaniu f z g oraz g z f | 105 |
| 4.3 | Graf permutacji $f = (5, 3, 2, 1, 4)$ | 110 |
| 4.4 | Graf permutacji, będącej cyklem wyznaczonym przez ciąg $(a_{i_1}, \dots, a_{i_k})$ | 111 |
| 4.5 | Tablica relacji R_G indukowanej w zbiorze $S = \{1, 2, 3, 4\}$ przez grupę $G = \{\pi_1, \pi_2, \pi_3, \pi_4\}$ z Przykładu 4.10. | 119 |

| | | |
|------|--|-----|
| 4.6 | Rysunek tablic z Przykładu 4.11. | 120 |
| 4.7 | Wszystkie różne „wzory” tablic z Przykładu 4.11. | 120 |
| 4.8 | Permutacje, odpowiadające obrotom tablic o $0^\circ, 90^\circ, 180^\circ$ i 270° z Przykładu 4.11. | 121 |
| 4.9 | Tablica relacji R_G indukowanej przez grupę obrotów G z Przykładu 4.11. | 122 |
| 4.10 | Orbita działania grupy obrotów G na zbiorze tablic z Przykładu 4.11. | 123 |
| 4.11 | Niezmiennejnik permutacji z grupy G i stabilizatory elementów zbioru S | 125 |
| 4.12 | Wszystkie podzbiory nieroróżnicalnych łańcuszków z Przykładu 4.14 i odpowiadające im trzyliterowe ciągi ze zbioru S | 127 |
| 4.13 | Naszyjnik z Przykładu 4.15, odpowiadający ciągowi $dtrrt$ | 128 |
| 4.14 | Tabela wartości wszystkich funkcji należących do zbioru $\text{Fun}(\{x_1, x_2, x_3, x_4\}, \{b, c\})$ | 132 |
| 4.15 | Rysunki grafów funkcji z Przykładu 4.18. | 135 |
| 4.16 | Podzbiory funkcji F_i , $i = 1, \dots, 5$, oraz odpowiadające im zbiory tablic. | 137 |
| 4.17 | Permutacje należące do grupy G oraz odpowiadające im grafy funkcji $\pi_1^{(3)}, \pi_2^{(3)}, \pi_3^{(3)}, \pi_4^{(3)}$ | 139 |
| 4.18 | Obroty naszyjnika z Przykładu 4.23. | 144 |
| 4.19 | Permutacje należące do grupy obrotów z Przykładu 4.23. | 145 |
| 4.20 | Obroty sześcianu z Przykładu 4.25. | 150 |
| 4.21 | Siedem różnych sposobów pokolorowania wierzchołków sześcianu, w których połowa wierzchołków ma kolor czarny, a połowa – biały. | 151 |
| 4.22 | Tabele prawdy dla negacji, alternatywy, koniunkcji, implikacji i równoważności. | 155 |
| 4.23 | Tabele prawdy dla wybranych zdań złożonych. | 156 |
| 4.24 | Diagramy Venna dla działań na zbiorach. | 157 |

Skorowidz

n-tka uporządkowana, x
 alternatywa, ix
 Bella liczby, 41
 bijekcja, 9, 14
 Cauchy'ego iloczyn, 73
 ciąg, 10, 67

- liczb harmonicznych, 75
- różnowartościowy, 10

 iloczyn Cauchy'ego, 73
 przesunięcie ciągu, 71
 splot, 73
 zliczanie ciągów, 11
 cykl, 110

- cykle rozłączne, 111
- długość cyklu, 111
- indeks cykli grupy, 140

 diagram

- Hassego, 54

 Dirichleta zasada, 97
 dwumianowe współczynniki, 26
 tożsamości, 27
 trójkąt Pascala, 27
 dwumianowy wzór, 26
 działanie dwuargumentowe, 106

- łączne, 107

 element

- maksymalny w zbiorze częściowo uporządkowanym, 55

- minimalny w zbiorze częściowo uporządkowanym, 55
 - najmniejszy w zbiorze częściowo uporządkowanym, 55
 - największy w zbiorze częściowo uporządkowanym, 55
 Ferrersa diagram, 51
 funkcja, 8, 11

- różnowartościowa, xi, 9, 13
- tworząca ciągu, 68
- unimodalna, 83

 bijekcja, 9
 ciąg, 10
 dziedzina funkcji, 8
 injekcja, 9
 jądro funkcji, 9, 47
 obraz zbioru przez funkcję, 9
 podłoga, xi, 159
 przeciowobraz zbioru przez funkcję, 9
 sufit, xi, 159
 surjekcja, 9
 wartość funkcji, 8
 zliczanie funkcji, 10
 zliczanie surjekcji, 47
 graf

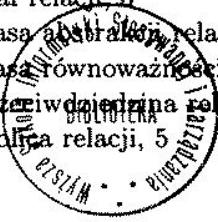
- funkcji, 9
- relacji, 5

 Graya kod, 24
 zwierciadlany, 24

SKOROWIDZ

- grupa, 107
 - permutacji stopnia n , 108
 - skończona, 108
 - symetryczna stopnia n , 108
- element neutralny grupy, 108
 element odwrotny, 108
 indeks cykli, 140
 orbity działania grupy, 119
 relacja indukowana przez grupę
 - pę, 118
- rzad grupy, 108
- Hassego diagram, 54
- iloczyn Cauchy'ego ciągów, 73
 iloczyn logiczny, ix
 implikacja, ix
 indeks
 - cykli grupy, 140
 - dolny we współczynniku dwumianowym, 25
 - górny we współczynniku dwumianowym, 25
- injekcja, 9
 izomery, 102
- kombinatoryka, 1
 konfiguracja, 133
 - waga konfiguracji, 134
- koniunkcja, ix
 krata, 58
 kres dolny zbioru, 57
 kres gorny zbioru, 57
 kwantyfikator, ix
 - egzystencjalny, ix
 - ogólny, ix
- liczby
 - Bella, 41
 - Stirlinga drugiego rodzaju, 39
- Stirlinga pierwszego rodzaju, 42, 112
 - harmoniczne, 75
 - podzbiorowe Stirlinga, 39
- Maclaurina szereg, 69
- najmniejsza wspólna wielokrotność, xiii, 60
 największy wspólny dzielnik, xiii, 60
 negacja, ix
 Newtona wzór, 26
 niezmiennik permutacji, 121
- ograniczenie dolne zbioru, 56
 ograniczenie górnne zbioru, 57
 operacja binarna, 106
 orbity działania grupy, 119
- pętla, 111
 para uporządkowana, x
 Pascala trójkąt, 27
 permutacja, 15
 - identycznościowa, 106
 - nieparzysta, 113
 - odwrotna, 107
 - parzysta, 113
- grupa permutacji, 108
 indeks cykli grupy permutacji, 140
 inwersja permutacji, 113
 nieporządek, 94
 niezmiennik permutacji, 121
 rozkład na cykle rozłączne, 110, 112
 stabilizator elementu, 124
 transpozycja, 114
 typ permutacji, 112
 złożenie permutacji, 104
 znak permutacji, 113, 115

podział liczby, 48
 podział sprzężony, 51
 podział zbioru na bloki, 37
 rozdrobnienie podziału, 45
 pokrycie zbioru, 60
 potęga przyrastająca liczby, 18
 tożsamości, 20
 potęga ubywająca liczby, 13
 tożsamości, 20
 równanie
 diofantyczne, 36
 równoważność, ix
 rachunek zdań, 155
 relacja, 4
 – antysymetryczna, 7
 – binarna, 4
 – częściowego porządku, 8
 – dwuczłonowa, 4
 – indukowana przez grupę, 118
 – pełna, 4
 – podzielności, 8
 – przechodnia, 7
 – przeciwsymetryczna, 7
 – przeciwwrotna, 7
 – pusta, 4
 – równoważności, 7
 – rozdrobnienia, 45
 – symetryczna, 7
 – w iloczynie kartezjańskim zbiorów, 4
 – w zbiorze, 4
 – zwrotna, 7
 dziedzina relacji, 4
 graf relacji, 5
 klasa abstrakcji relacji, 7
 klasa równoważności relacji, 7
 przeciwdziedzina relacji, 4
 tabela relacji, 5



rozmieszczenia uporządkowane, 17
 zliczanie, 18
 silnia, 15
 splot ciągów, 73
 stabilizator elementu, 124
 Stirlinga formula, 15, 158
 Stirlinga liczby
 – drugiego rodzaju, 39
 – pierwszego rodzaju, 42
 – tożsamości, 42
 suma logiczna, ix
 surjekcja, 9
 zliczanie surjekcji, 92
 szereg
 – Maclaurina, 69
 – formalny, 68
 – zliczający figur, 134
 – zliczający konfiguracji, 134, 138
 – zliczający wzorów, 135
 transpozycja, 114
 transpozycja sąsiednich elementów, 114
 typ permutacji, 112
 Venna diagramy, 157
 waga
 – figury, 133
 – konfiguracji, 134
 wektor, x
 – charakterystyczny zbioru, 21
 wielomianowe współczynniki, 29
 tożsamości, 33
 wielomianowy wzór, 33
 wzór
 – Newtona, 26
 – dwumianowy, 26
 – wielomianowy, 33

zasada
 – Dirichleta, 97
 – szufladkowa, 97
 – włączania-wyłączania, 90
 zbiór, 157
 – częściowo uporządkowany, 8, 52
 – liniowo uporządkowany, 52
 – potęgowy, 21
 – pusty, ix, 157
 – z powtórzeniami, 34
 generowanie podzbiorów, 21
 iloczyn kartezjański zbiorów, x, 3
 liczność zbioru, ix, 157
 moc zbioru, 157
 permutacja zbioru, 15
 podstawowy, 34
 podzbiór, x
 podzbiór właściwy, x
 podzbiory k -elementowe, 25
 podział na bloki, 37
 pokrycie zbioru, 60
 przecięcie zbiorów, x, 157
 różnica symetryczna zbiorów, x, 157
 różnica zbiorów, x, 157
 suma zbiorów, x, 157
 wektor charakterystyczny zbioru, 21
 zliczanie podzbiorów, 21
 zbiór częściowo uporządkowany, 52
 bezpośredni następnik elementu, 54
 bezpośredni poprzednik elementu, 54
 diagram Hassego zbioru, 54
 element maksymalny, 55
 element minimalny, 55