Wojciech Kordecki

Matematyka dyskretna

dla informatyków

Wrocław 2005

Spis treści

1. Relacje, funkcje i rozmieszczenia

1.1. Zbiory częściowo uporządkowane

Niech X będzie dowolnym zbiorem (skończonym). Relacja binarna $\preccurlyeq$ na X nazywa się *częściowym porządkiem*, jeśli jest zwrotna, przechodnia i antysymetryczna, tzn. jeśli

$$\begin{gathered} x \preccurlyeq x, \\ x \preccurlyeq y \wedge y \preccurlyeq z \implies x \preccurlyeq z, \\ x \preccurlyeq y \wedge y \preccurlyeq x \implies x = y \end{gathered}$$

Posety

Parę $(X, \preccurlyeq)$ nazywa się *zbiorem częściowo uporządkowanym*, (partially ordered set = poset). Jeżeli wiadomo o jaki porządek chodzi, to zbiorem częściowo uporządkowanym nazywa się też sam zbiór X. Jeżeli dla pewnych elementów $x, y \in X$ zachodzi $x \preccurlyeq y$ lub $y \preccurlyeq x$, to elementy te są *porównywalne*. Jeżeli dowolne dwa elementy są porównywalne, to porządek nazywa się *liniowym*. Jeżeli $x \preccurlyeq y$ i $x \neq y$ to pisze się $x \prec y$. Element $x \in X$ jest

- *minimalny*, jeśli nie istnieje $y \in X$ taki, że $y \prec x$,
- *maksymalny*, jeśli nie istnieje $y \in X$ taki, że $x \prec y$,
- *najmniejszy*, jeśli $x \preccurlyeq y$ dla każdego $y \in X$,
- *największy*, jeśli $y \preccurlyeq x$ dla każdego $y \in X$.

Zero i jeden

Element najmniejszy nazywa się *zerem*, a największy *jedynką* zbioru częściowo uporządkowanego, oznaczane są one często przez **0** i **1**.

Przykład. Rodzina $\mathcal{R} = 2^Z$ wszystkich podzbiorów dowolnego zbioru Z z relacją zawierania $\subseteq$ jest zbiorem częściowo uporządkowanym $(\mathcal{R}, \subseteq)$. Elementem największym jest Z, a najmniejszym $\emptyset$. Również dowolna rodzina $\mathcal{S} \subseteq 2^Z$ podzbiorów zbioru Z z taką samą relacją $\subseteq$ jest zbiorem częściowo uporządkowanym, choć **0** i **1** mogą być inne lub nie istnieć.

Łańcuchy

Niech $(X, \preccurlyeq)$ będzie zbiorem częściowo uporządkowanym oraz $Y \subseteq X$. Jeśli każde dwa elementy zbioru Y są porównywalne, to Y jest *łańcuchem*, jeśli zaś żadne dwa różne nie są porównywalne, to Y jest *antyłańcuchem*. Każdy łańcuch ma element najmniejszy i największy, czyli *początek* i *koniec* łańcucha.

Ograniczeniem dolnym zbioru $Y \subseteq X$ nazywa się dowolny element $a \in X$ taki, że $a \preccurlyeq x$ dla każdego $x \in Y$, a ograniczeniem górnym zbioru $Y \subseteq X$ nazywa się dowolny element $b \in X$ taki, że $x \preccurlyeq b$ dla każdego $x \in Y$. Niech $A(Y)$ i $B(Y)$ będzą zbiorami wszystkich ograniczeń dolnych i górnych odpowiednio.

Własność 0. *Zbiory A i B ograniczeń dolnych i górnych są uporządkowane liniowo.*

Dowód. ???? □

Kresy zbiorów

Kresem dolnym zbioru Y nazywa się element największy w $A(Y)$, kresem górnym element najmniejszy w $B(Y)$. Kresy dolne i górne zbioru Y oznaczane są odpowiednio przez $\inf(Y)$ i $\sup(Y)$.

Używa się też oznaczeń:

$$x \vee y = \sup\{x, y\},$$
$$x \wedge y = \inf\{x, y\},$$

Kraty

Kratą jest zbiór X częściowo uporządkowany relacją $\preccurlyeq$ taki, że dla każdej pary $x, y \in X$ istnieje kres dolny $x \wedge y$ oraz kres górny $x \vee y$. Krata nazywa się się zupełną, istnieją $\inf(Y)$ i $\sup(Y)$ dla każdego podzbioru Y kraty $(X, \preccurlyeq)$. Krata nazywa się rozdzielną, gdy dla dowolnych elementów x, y, z kraty $(X, \preccurlyeq)$ zachodzą równości

$$x \vee (y \wedge z) = (x \vee y) \wedge (z \vee z),$$
$$x \wedge (y \vee z) = (x \wedge y) \vee (z \wedge z).$$

1.2. Funkcje i rozmieszczenia

Zbiory w pudełkach

Niech $|X|$ oznacza moc (liczbę elementów) zbioru skończonego X. Klasycznym zadaniem kombinatoryki jest następujący problem: dla danych zbiorów X i Y, gdzie $|X| = m$, $|Y| = n$ znaleźć liczbę wszytkich funkcji $f : X \to Y$ spełniających dane ograniczenia.

Twierdzenie 1.2.1. *Jeśli $|X| = m$ i $|Y| = n$, to liczba wszystkich funkcji $f : X \to Y$ jest równa n^m.*

Dowód. Oznaczmy $X = \{1, 2, \ldots, m\}$. Funkcje $f : X \to Y$ są ciągami długości m o wyrazach ze zbioru Y. Każdy wyraz można wybrać na n sposobów, wszystkich więc ciągów jest n^m. □

Zadanie powyższe formułuje się często jako zadanie znalezienia liczby rozmieszczeń m elementów w n pudełkach – element o numerze i znajduje się w pudełku o numerze j, gdy $f(i) = j$.

Elementy w pudełkach

Ograniczając się do funkcji różnowartościowych (wzajemnie jednoznacznych), otrzymujemy następujące wynik.

Twierdzenie 1.2.2. *Jeśli $|X| = m$ i $|Y| = n$, to liczba funkcji różnowartościowych $f : X \to Y$ jest dla $m \leqslant n$ równa*

$$(n)_m = n(n-1)\ldots(n-m+1), \tag{1.2.1}$$

gdzie dodatkowo przyjmuje się $(n)_0 = 1$. Dla $m > n$ liczba ta jest równa zeru.

Dowód. Niech $X = \{1, 2, \ldots, m\}$ oraz $m \leqslant n$. Pierwszy wyraz ciągu można wybrać na n sposobów, drugi na $n-1$, a ogólnie i-ty wyraz można wybrać na $m-(i-1) = m-i+1$ sposobów, co daje wzór (1.2.1). Dla $m > n$ nie ma funkcji $f : X \to Y$ różnowartościowych. □

Jest to zadanie znalezienia liczby rozmieszczeń m elementów w n pudełkach, gdy w każdym pudełku można umieścić co najwyżej jeden element.

Permutacje i silnie

Jeśli $m = n$, to $(n)_m$ jest oznaczane przez $n!$ i nazywane *silnią* liczby n. Jeśli $X = Y$, to różnowartościową funkcję $f : X \to X$ nazywa się permutacją zbioru X. Stąd

Twierdzenie 1.2.3. *Jeśli $|X| = |Y| = n$, to liczba funkcji różnowartościowych $f : X \to Y$ jest równa*

$$n! = n(n-1) \cdot \ldots \cdot 1 \,.$$

W szczególności istnieje $n!$ permutacji zbioru n-elementowego.

Wzór Stirlinga

Ponieważ $n!$ rośnie bardzo szybko, to bardzo użyteczny jest następujący asymptotyczny wzór Stirlinga[1]

$$n! = n^n \sqrt{2\pi n}\,(1 + o(1)) \,. \tag{1.2.2}$$

i jego udoskonalenie (wzór Robbinsa[2])

$$n^n e^{-n} \sqrt{2\pi n} e^{\frac{1}{12n+1}} < n! < n^n e^{-n} \sqrt{2\pi n} e^{\frac{1}{12n}} \,. \tag{1.2.3}$$

(patrz zad. 20).

Ciągi w pudełkach

Zagadnieniem podobnym do zagadnienia rozwiązanego w twierdzeniu 1.2.2 jest zagadnienie rozmieszczenia m elementów w n pudełkach, przy czym każde pudełko zawiera ciąg elementów, (pudełka mogą być też puste). Dwa rozmieszczenia są identyczne, gdy te same pudełka mają te same ciągi elementów. Rozmieszczenia tego typu nazywa się rozmieszczeniami uporządkowanymi m elementów w n pudełkach.

Twierdzenie 1.2.4. *Liczba rozmieszczeń uporządkowanych m elementów w n pudełkach jest równa*

$$(n)^m = n(n+1)\ldots(n+m-1),, \tag{1.2.4}$$

gdzie dodatkowo przyjmuje się $(n)^0 = 1$.

Dowód. Niech $X = \{x_1, x_2, \ldots, x_m\}$. Element x_1 można rozmieścić na n sposobów, tyle ile jest pudełek. Element x_2 można umieścić na $n-1$ sposobów w $n-1$ pustych pudełkach oraz na dwa sposoby w pudełku zawierającym x_1 – otrzymując ciąg (x_1, x_2) lub (x_2, x_1). Oznaczmy przez s_i liczbę elementów w pudełku i-tym po rozmieszczeniu elementów $\{x_1, \ldots, x_{k-1}\}$. Element x_k można teraz rozmieścić w i-tym pudełku na $s_i + 1$ sposobów, czyli w sumie na

$$\sum_{i=1}^{n} (s_i + 1) = m + \sum_{i=1}^{n} s_i = m + k - 1$$

sposobów. Stąd otrzymuje się wzór (1.2.4). □

Potrzebne wzory

Na koniec kilka wzorów, których dowody pozostawione są jako zadania.

$$(n)_m = (n-m+1)\,(n)_{m-1}\ , \tag{1.2.5}$$
$$(n)_m = n!/m!\,, \tag{1.2.6}$$
$$(n)^m = (m+n-1)_m\ . \tag{1.2.7}$$

Uwaga. We wzorach (1.2.1) i (1.2.4) można zamiast n podstawić liczbę rzeczywistą x, otrzymując definicje symboli $(x)_m$ i $(x)^m$. Wzory (1.2.5) i (1.2.7) pozostają prawdziwe i przyjmują postać Wtedy

$$(x)_m = (x-m+1)\,(x)_{m-1}\ , \tag{1.2.8}$$
$$(n)^m = (m+n-1)_m\ , \tag{1.2.9}$$

gdzie $(x)_0 = (x)^0 = 1$.

1.3. Zadania

1. Wypisz wszystkie funkcje ze zbioru $\{a, b\}$ w zbiór $\{A, B, C\}$. Ile wśród nich jest funkcji różnowartościowych?

2. Ile jest funkcji ściśle rosnących ze zbioru {a,b,c} w zbiór {1,2,3,...,100}?

3. Ile jest funkcji ściśle rosnących ze zbioru {1,2,3,...,97} w zbiór {1,2,3,...,100}?

4. Na ile sposobów możesz podzielić 20 osób na dwie (niekoniecznie niepuste) grupy? Na ile sposobów możesz podzielić 20 osób na trzy (niekoniecznie niepuste) grupy?

5. Wypisz wszystkie możliwe ustawienia dwu osób w kolejkach do dwóch (trzech) kas. Na ile sposobów można ustawić 20 osób w kolejkach do dwóch (trzech) kas.

6. Ile jest funkcji ze zbioru 10-elementowego na zbiór 2-elementowy? Ile na 3-elementowy?

7. Wyznacz liczbę par (A, B), gdzie $A \subseteq B \subseteq \{1, 2, \ldots, n\}$.

8. Pewną pracę należy podzielić pomiędzy 3 kobiety, 4 chłopców oraz 5 mężczyzn. Na ile sposobów można to zrobić, przy założeniu, że mamy 3 stanowiska pracy dla kobiet, 4 dla chłopców oraz 5 dla mężczyzn?

9. Jak w zadaniu 8, ale dla kobiet i chłopców mamy tylko po 2 stanowiska pracy.

10. Mały Arturek ma pięć par butów. Wkładając buty kieruje się dwiema zasadami:

[1] Stirling ???
[2] Robbins ???

a) nigdy nie wkłada lewego buta na lewą nogę, ani prawego na prawą,
b) nigdy nie wkłada dwu butów z tej samej pary.
Na ile sposobów może włożyć buty na obie nogi?

11. Pewien bar oferuje 5 zup i 10 drugich dań, drugi – 6 zup i 8 drugich dań. Ile różnych obiadów dwudaniowych masz do wyboru, jeżeli decydujesz się zjeść obiad w jednym z tych dwu barów?

12. Uogólnienie zadania 11. Bar KOMBINATORYKA oferuje n rodzajów dań: przystawki, drugie dania, desery etc. Menu i-tego rodzaju dania ma k_i pozycji. Na ile sposobów można zjeść posiłek m-daniowy, gdy $m \leqslant n$?

13*. Na ile sposobów można ustawić na zwykłej szachownicy 8 wież tak, aby się wzajemnie nie biły?

14. Oznaczmy $[N] = \{1, 2, \ldots, N\}$. W zbiorze $[N]$ wprowadzimy relację częściowego porządku w następujący sposób: $n \prec m$ wtedy i tylko wtedy, gdy m jest podzielne przez n. Wyznaczyć elementy minimalne i maksymalne dla danego N. Czy zbiorze $[N]$ istnieją elementy najmniejszy i największy?

15.** Pokazać, że liczba naturalna n ma nieparzystą liczbę dzielników (włączając 1 i n) wtedy i tylko wtedy, gdy $\sqrt{n}$ jest liczbą całkowitą.

16. Wyznaczyć wszystkie nieizomorficzne porządki częściowe na zbiorze czteroelementowym.

17. Czy zbiór kół na płaszczyźnie o dowolnym środku i dowolnym promieniu uporządkowany przez zawieranie tworzy kratę?

18*. Udowodnić, że w dowolnej kracie warunki

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$
$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

dla wszystkich x, y, z, są równoważne.

19*. Udowodnić, że

$$r!(r+1)^{n-r} \leqslant n! \leqslant r! n^{n-r}\,.$$

20. Sprawdzić, (przez napisanie programu), jaką dokładność ma oszacowanie $n!$ dane wzorem Robbinsa (1.2.3).

2. Permutacje

2.1. Grupy skończone

2.2. Rozkład permutacji na cykle

Permutację zbioru $X = \{x_1, x_2, \ldots, x_n\}$, czyli funkcję różnowartościową $f : X \to X$, gdzie elementy zbioru X wypisane są w dowolnym, ale ustalonym porządku $\prec$, oznacza się zwykle jako tablicę o dwóch wierszach

$$f = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ y_1 & y_2 & \ldots & y_n \end{pmatrix},$$

gdzie $y_j = f(x_j)$. Jeżeli w górnym wierszu porządek jest ustalony, a zwłaszcza, gdy $X = \{1, 2, \ldots, n\}$, to wystarczy napisać tylko dolny wiersz, a więc zamiast

$$f = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

gdzie $i_j = f(j)$, piszemy $(i_1, i_2, \ldots, i_n)$.

Złożenie permutacji

Zbiór wszystkich permutacji zbioru n-elementowego zbioru X, oznacza się przez S_n. Jeśli w zbiorze tym wprowadzi jako działanie złożenie permutacji $f \circ g$ określone wzorem $(f \circ g)(x) = f(g(x))$ dla każdego $x \in X$, to $(S_n, \circ)$ tworzy grupę.

Niech $f : X \to X$ będzie permutacją zbioru X. Załóżmy, że istnieje podział zbioru X na rozłączne części $X_1, X_2, \ldots, X_k$, tzn. $X = X_1 \cup X_2 \cup \cdots \cup X_k$ takie, że w każdym X_j, $x \in X_j \implies f(x) \in X_j$, a żadnego z X_j nie można już podzielić na dwie niepuste części o tej własności. Wtedy X można uporządkować w taki sposób, że każde X_j składa się z kolejnych elemenentów, $X_j = \{x_{j_1}, \ldots, x_{j_{m_j}}\}$ oraz

$$f(x_{j_1}) = x_{j_2}, f(x_{j_2}) = x_{j_3}, \ldots, f\left(x_{j_{m_j-1}}\right) = x_{j+m_j}, f\left(x_{j+m_j}\right) = x_{j_1}. \quad (2.2.1)$$

Rozkład permutacji na cykle

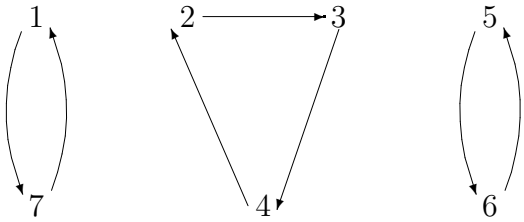
Każdy taki podzbiór (uporządkowany) $X_j \subseteq X$ nazywa się *cyklem*, a przedstawienie X w postaci sumy cykli, nazywa się *rozkładem permutacji na cykle*. Moc zbioru X_j nazywa się *długością* cyklu X_j.

Rozkład permutacji $(x_1, x_2, \ldots, x_n)$ na cykle oznacza się
$[x_1, \ldots, x_{m_1}]\,[x_{m_1+1}, \ldots, x_{m_1+m_2}] \ldots [x_{n-m_k}, \ldots, x_n]$,
gdzie m_j jest długością j-tego cyklu. Permutacja f jest typu $\langle \lambda_1, \ldots, \lambda_n \rangle$, jeśli w rozkładzie na cykle ma λ_i cykli długości i, dla $i = 1, 2, \ldots, n$. Typ ten zapisuje się symbolicznie $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$, opuszczając i^{λ_i} gdy $\lambda_i = 0$. Permutację typu $n^1 = 1^0 2^0 \ldots (n-1)^0 n^1$ nazywa się cykliczną.

Przykład. Graficznie rozkład permutacji na cykle można przedstawić jak na rysunku 1. Przedstawiono na nim rozkład permutacji $(7, 3, 4, 5, 6, 5, 1)$ na cykle $[1, 7][2, 3, 4][5, 6]$. Permutacja ta jest typu $2^2 3^1$.

Inwersja

Para (x_i, x_j), $i < j$ jest *inwersją* permutacji $(x_1, \ldots, x_n)$, jeśli $x_j \prec x_i$. Dla do-



Rysunek 1. Rozkład permutacji na cykle

wolnej permutacji f przez $I(f)$ oznacza się liczbę jej inwersji. Znak permutacji definiuje się wzorem

$$\operatorname{sgn}(f) = (-1)^{I(f)} .$$

Znak permutacji

Permutacja jest *parzysta*, gdy $\operatorname{sgn}(f) = 1$, a w przeciwnym przypadku jest *nieparzysta*. Permutacja tożsamościowa e jest zawsze parzysta.

Znak permutacji jest wykorzystany w znanej „permutacyjnej" definicji wyznacznika $\det(A)$ macierzy kwadratowej $A = [a_{ij}]$ wymiaru $n \times n$:

$$\det(A) = \sum_{(i_1,\ldots,i_n)} \operatorname{sgn}(i_1,\ldots,i_n) \prod_{j=1}^{n} a_{ji_j} ,$$

gdzie sumowanie przebiega po wszystkich permutacjach $(i_1,\ldots,i_n)$ ciągu $(1,\ldots,n)$.

Lemat 2.2.1. *Dowolną permutację f można przedstawić w postaci złożenia $I(f)$ transpozycji sąsiednich elementów.*

Dowód. ??? □

Lemat 2.2.2. *Dla dowolnych permutacji $f, g \in S_n$*

$$\operatorname{sgn}(f \circ g) = \operatorname{sgn}(f) \operatorname{sgn}(g) .$$

Dowód. ??? □

Lemat 2.2.3. *Jeśli permutacja f jest cyklem długości k, to jej znak wyraża się wzorem* $\operatorname{sgn}(f) = (-1)^{k-1}$.

Dowód. ??? □

Lemat 2.2.4. *Jeśli permutacja f jest typu $1^{\lambda_1} \ldots n^{\lambda_n}$, to jej znak wyraża się wzorem*

$$\operatorname{sgn}(f) = (-1)^{\sum_{j=1}^{\lfloor n/2 \rfloor} \lambda_{2j}} .$$

Dowód. ??? □

Porównaj z programem w C++

Poniższy program (w Pascalu) wyznacz znak permutacji.

Algorytm 2.2.1. *Wejście: dowolna permutacja* ($f \in S_n$) *dana w postaci ciągu* $P[1] \dots P[n]$.
Wyjście: znak permutacji $\operatorname{sgn}(f)$.

```
function sgn_perm(f:perm):integer;
var i,j:1..max_perm;
    s:integer;
    new_p:array[1..max_perm] of boolean;
begin
     s:=1;
     with f do
     begin
          for j:=1 to n do new_p[j]:=true;
          for i:=1 to n do
              if new_p[i] then
              begin
                   j:=p[i];
                   while j<>i do
                   begin
                        new_p[j]:=false;
                        s:=-s;
                        j:=p[j];
                   end;
              end;
     end;
     sgn_perm:=s;
end;
```

Działanie algorytmu 2.2.1 jest proste: ???

Następujące twierdzenie pochodzi od Cauchy'ego[3].

Twierdzenie 2.2.1. *Liczba permutacji typu* $1^{\lambda_1}2^{\lambda_2}\dots n^{\lambda_n}$ *zbioru n-elementowego jest równa*

$$\frac{n!}{1^{\lambda_1}2^{\lambda_2}\dots n^{\lambda_n}\lambda_1!\lambda_2!\dots\lambda_n!}.$$

Dowód. Zapis permutacji f typu $1^{\lambda_1}2^{\lambda_2}\dots n^{\lambda_n}$ jest znormalizowany, gdy jest postaci

$$f = [a_0^{(1)}a_1^{(1)}\dots a_{n_1-1}^{(1)}]\dots[a_0^{(k)}a_1^{(k)}\dots a_{n_k-1}^{(k)}],$$

gdzie występuje kolejno λ_1 cykli długości 1, λ_2 cykli długości 2 itd. Porządek w jakim występują cykle długości i można zmieniać na λ_i sposobów. Każdy taki cykl można przesuwać cyklicznie na i sposobów. Stąd każda permutacja typu $1^{\lambda_1}2^{\lambda_2}\dots n^{\lambda_n}$ jest określona przez $1^{\lambda_1}2^{\lambda_2}\dots n^{\lambda_n}\lambda_1!\lambda_2!\dots\lambda_n!$ zapisów znormalizowanych. □

[3]Cauchy

2.3. Liczby Stirlinga pierwszego rodzaju

Liczby Stirlinga[4] pierwszego rodzaju określa się jako współczynniki $s(n,k)$ przy kolejnych potęgach x wielomianu $(x)_n$, określonego wzorem:

$$(x)_n = \sum_{k=0}^{n} s(n,k)\, x^k . \tag{2.3.1}$$

Twierdzenie 2.3.1. *Liczby Stirlinga pierwszego rodzaju spełniają wzór rekurencyjny*

$$s(n,k) = s(n-1,k-1) - (n-1)\, s(n-1,k) \tag{2.3.2}$$

dla $0 < k < n$ *oraz* $s(n,n) = 1$ *dla* $n \geqslant 0$, $s(n,0) = 0$ *dla* $n > 0$.

Dowód. Niech $0 < k < n$. Wtedy $(x)_n = (x)_{n-1}(x-n+1)$, skąd

$$\begin{aligned}\sum_{k=0}^{n} s(n,k)\, x^k &= (x-n+1)\sum_{k=1}^{n-1} s(n-1,k)\, x^k \\ &= \sum_{k=1}^{n-1} s(n-1,k-1)\, x^k - (n-1)\sum_{k=0}^{n-1} s(n-1,k)\, x^k .\end{aligned}$$

Wzór (2.3.2) otrzymuje się przez porównanie współczynników przy x^k. □

Symetria do (2.3.1)

Ze wzorów (2.3.1) i (2.3.2) można otrzymać również wzór

$$x^n = \sum_{k=0}^{n} s(n,k)\,(x)^k. \tag{2.3.3}$$

Twierdzenie 2.3.2. *Wartość bezwzględna liczby Stirlinga pierwszego rodzaju jest równa liczbie permutacji zbioru n-elementowego, która ma rozkład na k cykli.*

Dowód. ??? □

Stąd jako prosty wniosek otrzymujemy

$$\sum_{k=0}^{n} |s(n,k)| = n! .$$

Inna definicja

Uwaga. Liczby Stirlinga definiuje się też wzorem (por. [3])

$$c(n,k) = c(n-1,k-1) + (n-1)\, c(n-1,k) . \tag{2.3.4}$$

Wtedy liczby obliczone przy pomocy wzoru (2.3.4) są równe wartościom bezwzględnym liczb obliczonych według wzoru (2.3.2), czyli $c(n,k) = |s(n,k)|$.

[4] Stirling

Liczby $c(n,k)$ zwane są też nieznakowanymi liczbami Stirlinga pierwszego rodzaju.

Twierdzenie 2.3.3. *Dla dowolnych $n \geqslant 0$ i $k \geqslant 0$*

$$c(n,k) = (-1)^{n+k} s(n,k) .$$

Dowód. ??? □

2.4. Zadania

1. Na ile sposobów można posadzić n osób przy okrągłym stole, gdy ważne jest tylko, kto przy kim siedzi?

2. Na ile sposobów można posadzić n osób przy okrągłym stole o m miejscach? Zakładamy, że $m < n$ oraz nie jest ważne, gdzie są umieszczone osoby, dla których zabrakło miejsc przy stole.

3. Ile jest takich permutacji zbioru n-elementowego w których ustalonych m elementów nie stoi jeden obok drugiego?

4. Tworzymy permutację zbioru $\{1, 2, \ldots, n\}$ w następujący sposób:

1. na pierwszym miejscu umieszczamy dowolny, na przykład losowo wybrany element n_1,
2. jeśli suma $n_1 + \cdots + n_{i-1}$ jest parzysta, to na miejscu i-tym umieszczamy największą z dotychczas nie wybranych liczb,
3. jeśli suma $n_1 + \cdots + n_{i-1}$ jest nieparzysta, to na miejscu i-tym umieszczamy najmniejszą z dotychczas nie wybranych liczb.

Utworzyć po dwie permutacje zbiorów o 5 i 7 elementach. Rozłożyć je na cykle i znaleźć ich znak.

5. Jak wyraża się znak permutacji utworzonej w zadaniu 4 w zależności od wyboru elementu n_1?

6^P. Napisać procedurę realizującą algorytm z zadania 4 dla dowolnego n.

7^P. Niech wybór elementu n_1 w zadaniu 4 będzie miał rozkład równomierny w zbiorze $\{1, 2, \ldots, n\}$. Poprze symulację komputerową znaleźć rozkład liczby cykli dla ustalonych n.

8. Ile jest możliwych rezultatów, którymi mogą się zakończyć zawody, w których startuje 8 osób w trzech konkurencjach, jeśli każda osoba startuje w jednej, dowolnie przez siebie wybranej konkurencji? Przez rezultat zawodów rozumiemy zestawienie kolejności wszystkich zawodników starujących w każdej konkurencji, przy czym mogą być konkurencje nie obsadzone.

9. *Inwolucją* nazywa się permutację f taką, że $f \cdot f = e$, gdzie e jest permutacją tożsamościową. Udowodnić, że f jest inwolucją zbioru n-elementowego wtedy i tylko wtedy, gdy jest typu $1^{\lambda_1} 2^{\lambda_2}$ oraz $\lambda_1 + 2\lambda_2 = n$.

10. Udowodnić, że $n^{n/2} < n! < n^n$.

11. Udowodnić, że dla $n > 6$

$$n^{n/2} < n! < \left(\frac{n}{2}\right)^n .$$

12. Udowodnić, że dla dowolnych naturalnych k i n, liczba $(k!)^n$ jest podzielnikiem liczby $(kn)!$.

13^P. Napisać program a) prosty (rekurencyjny), b) efektywny na obliczanie liczb Stirlinga pierwszego rodzaju.

14. Pokazać, że

$$(x)^n = \sum_{k=1}^{n} |s(n,k)| x^k .$$

15. Udowodnić, że średnia liczba cykli dla losowo wybranej permutacji zbioru n-elementowego wynosi

$$\sum_{k=1}^{n} \frac{1}{k} ,$$

czyli

$$\frac{1}{n!} \sum_{k=1}^{n} |s(n,k)| = \sum_{k=1}^{n} \frac{1}{k} .$$

3. Kombinacje

3.1. Współczynnik dwumianowy

Liczba podzbiorów k-elementowych zbioru n-elementowego, oznaczana jest symbolem $\binom{n}{k}$, zwanym *symbolem Newtona*[5] lub *współczynnikiem dwumianowym*. Podzbiory takie nazywa się również *kombinacjami k-wyrazowymi ze zbioru n-elementowego bez powtórzeń*. Zamiast symbolu $\binom{n}{k}$ używany jest też symbol C_n^k. Dla $k > n$ mamy oczywiście $\binom{n}{k} = 0$ oraz $\binom{0}{0} = 1$.
Nazwę „współczynnik dwumianowy" uzasadnia następujące twierdzenie.

Twierdzenie 3.1.1.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. \tag{3.1.1}$$

Dowód. ???? □

Symbol Newtona

Twierdzenie 3.1.2.

$$\binom{n}{k} = \frac{(n)_k}{k!} = \frac{n!}{k!\,(n-k)!}. \tag{3.1.2}$$

Dowód. Wiadomo, że $(n)_k$ jest liczbą ciągów różnowartościowych k-elementowych ze zbioru n-elementowego. Każdy taki ciąg daje zbiór k-elementowy, przy czym ten sam zbiór powstaje z dokładnie $k!$ ciągów będących wszystkimi permutacjami tego zbioru. □

Symbol Newtona można uogólnić na przypadek $\binom{x}{k}$, gdy x jest dowolną liczbą rzeczywistą lub zespoloną:

$$\binom{x}{k} = \frac{(x)_k}{k!},$$

gdzie $(x)_k = x(x-1)\dots(x-k+1)$ jest wielomianem stopnia k, określonym wzorem (1.2.8). Wtedy zgodnie ze wzorem (2.3.1), otrzymujemy

$$\binom{x}{k} = \sum_{j=0}^{k} \frac{s(k,j)}{k!}\, x^j.$$

W szczególności dla $k \geqslant 0$

$$\binom{n}{k} = (-1)^k \binom{k-n-1}{k}.$$

Do obliczeń $\binom{n}{k}$ wygodnie jest stosować następujący wzór rekurencyjny:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \tag{3.1.3}$$

Trójkąt Pascala

dla $n > 0$ i $k > 0$. Ze wzoru (3.1.3) otrzymuje się trójkąt Pascala:

[5] Newton

$$
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
\multicolumn{9}{c}{\dots\dots\dots\dots\dots\dots\dots\dots}
\end{array}
$$

Ze wzoru (3.1.2) wynika wzór

$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} > \binom{n}{\lceil n/2 \rceil + 1} \cdots > \binom{n}{n} \tag{3.1.4}$$

dla $n > 1$. Zauważyć trzeba, że dla parzystego n mamy $\lfloor n/2 \rfloor = \lceil n/2 \rceil$. Znane są proste oszacowania z góry:

$$\binom{n}{k} < \frac{n^k}{k!}\,, \tag{3.1.5}$$

$$\binom{n}{k} \leqslant \frac{n^n}{k^k (n-k)^{n-k}}\,. \tag{3.1.6}$$

Bardziej skomplikowane jest oszacowanie z dołu:

$$\binom{n}{k} \geqslant \frac{1}{2\pi} \frac{n^{n+\frac{1}{2}}}{k^{k+\frac{1}{2}} (n-k)^{n-k+\frac{1}{2}}} \exp\left(\frac{1}{12n} - \frac{1}{12k} - \frac{1}{12(n-k)}\right). \tag{3.1.7}$$

Z oszacowań tych wynika, że $\binom{n}{k}$ szybko rośnie wraz ze wzrostem n i k rosnącym proporcjonalnie do n. Łatwo to zauważyć, pisząc procedurę obliczającą wartości współczynników dwumianowych.

Twierdzenie 3.1.3.

$$\binom{l+r}{k} = \sum_{t=0}^{k} \binom{l}{t} \binom{r}{k-t}\,. \tag{3.1.8}$$

Równość (3.1.8) jest znana jako tożsamość Cauchy'ego.

Jak zmienia się k?

Z twierdzenia 3.1.3 wynikają dla nieujemnych l, m, n, q, r, s kolejne wzory:

$$\sum_k \binom{r}{m+k} \binom{s}{n-k} = \binom{r+s}{m+n}$$

$$\sum_k \binom{l}{m+k} \binom{s}{n+k} = \binom{l+s}{l-m+n}$$

$$\sum_k \binom{l}{m+k} \binom{s+k}{n} (-1)^k = (-1)^{l+m} \binom{s-m}{n-l}$$

Uogólnieniem współczynników dwumianowych są współczynniki wielomianowe.

$$\binom{a_1 + a_2 + \cdots + a_n}{a_1, a_2, \ldots, a_n} = \frac{(a_1 + a_2 + \cdots + a_n)}{a_1! a_2! \ldots a_n!}\,. \tag{3.1.9}$$

Nazwa pochodzi stąd, że

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{\substack{a_1+\cdots+a_n \\ 0 \leqslant a_i \leqslant n}} \binom{a_1 + a_2 + \cdots + a_n}{a_1, a_2, \ldots, a_n} x_1^{a_1} x_2^{a_2} \ldots x_k^{a_n} . \quad (3.1.10)$$

Wzory (3.1.9) i (3.1.10) są uogólnieniami wzorów (3.1.1) i (3.1.2) odpowiednio.

3.2. Generowanie podzbiorów

Porządek leksykograficzny

Niech $X = \{1, 2, \ldots, n\}$. Każdemu podzbiorowi k-elementowemu odpowiada rosnący podciąg k-elementowy. W zbiorze podciągów k-elementowych wprowadzimy porządek leksykograficzny (słownikowy) w następujący sposób: jeżeli $a = (a_1, a_2, \ldots, a_k)$ i $b = (b_1, b_2, \ldots, b_k)$ oraz dla pewnego j jest $a_i = b_i$ dla $i < j$ oraz $a_j < b_j$ to $a \prec b$. Oczywiście, jeśli $a_1 < b_1$ to również $a \prec b$. Tak określoną relację $\prec$ można przenieść z ciągów na podzbiory.

Teraz można podać algorytm generujący wszystkie podzbiory k-elementowe zbioru X w porządku leksykograficznym. Wystarczy zauważyć, że ciągiem następującym po $a = (a_1, \ldots, a_k)$ jest ciąg

$$b = (b_1, \ldots, b_k) = (a_1, \ldots, a_{p-1}, a_p + 1, a_p + 2, \ldots, a_p + k - p + 1)$$

gdzie $p = \max\{i : a_i < n - k + 1\}$. Po ciągu b następuje ciąg

$$c = (c_1, \ldots, c_k) = \left(b_1, \ldots, b_{p'-1}, b'_p + 1, b'_p + 2, \ldots, b'_p + k - p + 1\right)$$

gdzie

$$p' = \begin{cases} p - 1 & \text{jeśli } b_k = n, \\ k & \text{jeśli } b_k < n. \end{cases}$$

Zakłada się, że ciągi a i b są różne od ciągu $(n - k + 1, \ldots, n)$ – ostatniego ciągu w tym porządku. Stąd algorytm.

????

```
procedure gen_k_subset(n,k:integer);
var i,j,p:integer;
    a:array[1..max_set] of integer;
begin
     for i:=1 to k do a[i]:=i; {pierwszy podzbiór}
     p:=k;
     while p>=1 do
     begin
          for j:=1 to k do write(a[j]:8);
          writeln;
          if a[k]=n then p:=p-1 else p:=k;
          if p>=1 then
             for i:=k downto p do a[i]:=a[p]+i-p+1;
     end;
end;
```

3.3. Zbiory z powtórzeniami

Uogólnieniem pojęcia zbioru (w którym każdy element występuje dokładnie raz), jest pojęcie zbioru z powtórzeniami. W takim zbiorze, każdy element może wystąpić kilkakrotnie, a liczba wystąpień nazywa się krotnością elementu. Istotna jest tu tylko krotność elementu, a nieistotna jest kolejność wystąpień. Zbiór taki oznacza się albo wypisując element tyle razy, ile wynosi jego krotność, albo gdy dla krotności równej k elementu a, pisząc $\{\ldots, k * a, \ldots\}$.

Przykład. Jeśli $X = \{2 * a, 3 * b, 1 * c\}$, to również $X = \{a, b, a, b, c, b\} = \{a, a, b, b, b, c\}$, ale $X \neq \{a, b, c\}$.

Zbiór A jest podzbiorem zbioru B, $A \subseteq B$, gdy krotność każdego elementu w A jest nie większa od krotności tego samego elementu w B. Liczbę elementów k w zbiorze $X = \{k_1 * x_1, \ldots, k_n * x_n\}$ (liczność zbioru X), definiuje się jako $k = k_1 + \cdots + k_n$.

Twierdzenie 3.3.1. *Liczba k-elementowych zbiorów z powtórzeniami o elementach ze zbioru n-elementowego (bez powtórzeń) jest równa*

$$\binom{n+k-1}{k}. \tag{3.3.1}$$

Twierdzenie 3.3.2. *????*

Twierdzenie to można również sformułować w terminach funkcji (patrz rozdział 1.2).

Twierdzenie 3.3.3. *Istnieje dokładnie $\binom{n+k-1}{k}$ funkcji niemalejących $f : \{1, \ldots, k\} \to \{1, \ldots, n\}$.*

Twierdzenie 3.3.4. *????*

Przykład. Niech $A = \{a, b, c\}$ (czyli $n = 3$) oraz $k = 2$. Zgodnie ze wzorem (3.3.1), z elemntów zbioru A można utworzyć

$$\binom{n+k-1}{k} = \binom{4}{2} = 6$$

dwuelementowych podzbiorów z powtórzeniami:

$$\{a, a\}, \{a, b\}, \{a, c\}, \{b, b\}, \{b, c\}, \{c, c\}.$$

Zbiorów czteroelementowych z powtórzeniami można zaś utworzyć

$$\binom{6}{4} = \binom{6}{2} = 15.$$

Zachodzi równość:

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

3.4. Zadania

1. Oblicz $\binom{10}{7}$.

2. Co jest większe $\binom{100}{37}$ czy $\binom{101}{55}$?

3. Na ile sposobów można utworzyć koalicję większościową w 459-osobowym sejmie? A na ile w 460-osobowym? Wynik podaj w możliwie prostej postaci.

4. Stoisz w lewym dolnym rogu szachownicy. W jednym kroku poruszasz się o jedno pole w prawo lub o jedno pole do góry. Po 14 krokach będziesz w prawym górnym rogu. Na ile sposobów możesz odbyć tę wędrówkę?

5. Na ile sposobów spośród 7 łysych i 8 rudych możesz wybrać pięcioosobową delegację w której składzie jest dokładnie 2, (0,1,3,4,5) rudych?

6. Udowodnić tożsamość

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$$

7. Pokazać korzystając z tożsamości Cauchy'ego, że

$$\binom{2n}{n} = \sum_{r=0}^{n} \binom{n}{r}^2 .$$

8. Udowodnić przez indukcję oraz czysto kombinatorycznie, że

$$\sum_{k=0}^{n} \binom{r+k}{k} = \binom{r+n+1}{n}$$

oraz

$$\sum_{k=r}^{n} \binom{k}{r} = \binom{n+1}{r+1} .$$

9. Pokazać, że

$$\sum_{r=0}^{n} (-1)^r \binom{n}{r} = 0 .$$

Wskazówka. Oblicz $(1-1)^n$ na dwa sposoby.

10. Udowodnić wzór

$$\sum_{k=0}^{m} \binom{m}{k}\binom{n+k}{m} = \sum_{k=0}^{m} \binom{n}{k}\binom{m}{k} 2^k .$$

11. Jak wiele istnieje zbiorów k-elementowych zbioru $\{1, 2, \ldots, n\}$, które nie zawierają żadnej pary dwóch kolejnych liczb?

12. Udowodnić wzór Leibniza

$$\frac{d^n\,(uv)}{dx^n} = \sum_{k=0}^{n} \binom{n}{k} \frac{d^k u}{dx^k}\,\frac{d^{(n-k)} v}{dx^{(n-k)}}\,,$$

gdzie u i v są funkcjami jednej zmiennej x.

13. Udowodnić wzór

$$\begin{aligned}\binom{n}{k_1, k_2, \ldots, k_m} &= \binom{n-1}{k_1 - 1, k_2, \ldots, k_m} \\ &+ \binom{n-1}{k_1, k_2 - 1, k_3, \ldots, k_m} \\ &+ \cdots + \binom{n-1}{k_1, k_2, \ldots, k_{m-1}, k_m},\end{aligned}$$

gdzie $n \geqslant 1$, $k_1 + k_2 + \cdots + k_m = n$, $k_i > 0$.

14. Udowodnić nierówność

$$\binom{n}{k} \leqslant \left(\frac{en}{k}\right).$$

15^P. Napisać procedurę wypisującą wszystkie k-elemntowe zbiory z powtórzeniami o elementach ze zbioru n elementowego, o którym mowa w twierdzeniu 3.3.1.

4. Podziały

4.1. Zasada włączania – wyłączania

Dwa zbiory Obliczmy liczbę elementów sumy zbiorów. Oczywisty jest wzór:

$$|A \cup B| = |A| + |B| - |A \cap B| \leqslant |A| + |B|\,, \tag{4.1.1}$$

Trzy zbiory prawdziwy dla dowolnych zbiorów A i B. Dla trzech zbiorów A, B i C mamy

$$\begin{aligned} |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap B| \leqslant \\ \leqslant |A \cup B \cup C| = \\ = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap B| + |A \cap B \cap C|\,. \end{aligned} \tag{4.1.2}$$

Jak widać ze wzorów (4.1.1) i (4.1.2), dodając do siebie liczby elementów dwóch zbiorów, dwukrotnie liczymy część wspólną – trzeba ją odjąć. Dla trzech zbiorów, odejmując trzykrotnie części wspólne par zbiorów, odejmujemy o jeden raz za dużo część wspólną wszystkich trzech podzbiorów – trzeba ją więc dodać. Powtarzając to rozumowanie, otrzymujemy następujący wynik, znany jako zasadę *włączanie-wyłączania*.

Zasada włączania-wyłączania

Twierdzenie 4.1.1. *Jeśli dla dowolnego ciągu $(A_1, \ldots, A_n)$ niekoniecznie różnych podzbiorów zbioru X:*

$$A = A_1 \cup \cdots \cup A_n\,,$$

to

$$\begin{aligned} |A| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| + \sum_{1 \leqslant i < j < k \leqslant n} |A_i \cap A_j \cap A_k| - \cdots + \\ + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|\,. \end{aligned} \tag{4.1.3}$$

Dowód. (Przez indukcję). Wzór (4.1.3) jest oczywisty dla $n = 1$, (także dla $n = 2$ – wzór (4.1.1) i dla $n = 3$ – wzór (4.1.2)). Przyjmijmy, że wzór (4.1.3) jest prawdziwy dla $n - 1$, czyli dla $A' = A_1 \cup \cdots \cup A_{n-1}$ prawdziwy jest wzór

$$\begin{aligned} |A'| = \sum_{i=1}^{n-1} |A_i| - \sum_{1 \leqslant i < j \leqslant n-1} |A_i \cap A_j| + \sum_{1 \leqslant i < j < k \leqslant n} |A_i \cap A_j \cap A_k| - \cdots + \\ + (-1)^{n-2} |A_1 \cap \cdots \cap A_{n-1}|\,. \end{aligned}$$

Ponieważ

$$A' \cap A_n = \bigcup_{i=1}^{n-1} (A_i \cap A_n)\,,$$

to

$$|A' \cap A_n| = \sum_{i=1}^{n-1} |A_i \cap A_n| - \sum_{1 \leqslant i < j \leqslant n-1} |A_i \cap A_j \cap A_n| + \cdots + \\ + (-1)^{n-2} |A_1 \cap \cdots \cap A_n| \,,$$

skąd

$$|A| = |A' \cup A_n| = |A'| + |A_n| - |A' \cap A_n| \,,$$

co daje wzór (4.1.3). □

Rozważmy problem ogólniejszy. Niech $D(r)$ oznacza liczbę elementów zbioru tych $x \in X$, które należą do dokładnie r zbiorów $A_1, A_2, \ldots, A_n$, $r \leqslant n$. Niech $1 \leqslant i_1 < \cdots < i_r \leqslant n$ będzie dowolnym ciągiem. Przyjmijmy oznaczenia:

$$N(i_1 \ldots, i_r) = |A_1 \cap \ldots A_{i_r}| \tag{4.1.4}$$

oraz

$$W(r) = \sum N(i_1, \ldots, i_r) \,, \tag{4.1.5}$$

gdzie sumowanie przebiega po wszystkich ciągach $1 \leqslant i_1 < \cdots < i_r \leqslant n$. Przyjmiemy też $W(0) = |X|$.

Twierdzenie 4.1.2. *Dla dowolnych $n > 0$ oraz $r \leqslant n$*

$$D(r) = \sum_{j=0}^{n-r} (-1)^{-1} \binom{r+j}{r} W(r+j) \,. \tag{4.1.6}$$

Dowód. Wzór (4.1.2) zapiszmy w postaci

$$\sum_{x \in X} L(x) = \sum_{x \in X} R(x)$$

gdzie

$$L(x) = \begin{cases} 1, & \text{gdy } x \text{ nalezy do dokładnie } r \text{ zbiorów } A_i, \\ 0 & \text{w przeciwnym przypadku.} \end{cases}$$

Podobnie

$$R(x) = \sum_{j=0}^{n-r} (-1)^j \binom{r+j}{r} R_{r+j}(x) \,, \tag{4.1.7}$$

gdzie $R_{r+j}(x)$ jest liczbą ciągów postaci $1 \leqslant i_1 < \cdots < i_{r+j} \leqslant n$ takich, że $x \in A_i \cap \cdots \cap A_{i_{r+j}}$. Trzeba pokazać, że dla każdego $x \in X$ zachodzi $L(x) = R(x)$.

Niech $x \in X$ oraz x należy do dokładnie u zbiorów A_i. Mamy tu trzy możliwe przypadki:

(i) $u < r$. Wtedy $L(x) = 0$ oraz $R(x) = 0$, bo $x \notin A_{i_1} \cap \cdots \cap A_{i_n}$.

(ii) $u = r$. Wtedy $l(x) = 1$ i $R(x) = 1$, bo $R_{r+j}(x) = 0$ dla $j > 0$ oraz $(-1)^0 \binom{r+0}{r} R_{r+0}(x) = R_r(x) = 1$.

(iii) $u > r$. Wtedy $L(x) = 0$ oraz $R_m(x) = \binom{u}{m}$. Podstawiając tę wartość do (4.1.7) i korzystając z tożsamości

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$$

(patrz zadanie 6) oraz

$$\sum_{r=0}^{n}(-1)^r \binom{n}{r} = 0\,.$$

(patrz zadanie 9 z rodz. 3.1) otrzymuje się

$$\begin{aligned} R(x) &= \sum_{j=0}^{n-r}(-1)^j \binom{r+j}{r}\binom{u}{r+j} = \sum_{j=1}^{u-r}(-1)^j \binom{r+j}{r}\binom{u}{r+j} \\ &= \sum_{j=1}^{u-r}(-1)^j \binom{u}{r}\binom{u-r}{u-r-j} = \binom{u}{r}\sum_{j=0}^{u-r}(-1)^j \binom{u-r}{j} = 0. \end{aligned}$$

□

Zasadę włączania-wyłączania można teraz sformułować jako

Twierdzenie 4.1.3.

$$D(0) = \sum_{j=0}^{n}(-1)^j W(j)\,.$$

Z twierdzenia 4.1.3 wynikają nastepujące twierdzenia.

Twierdzenie 4.1.4. *Jeśli $|X| = n$ oraz $|Y| = m$, to liczba s_{nm} funkcji z X na Y jest równa*

$$s_{nm} = \sum_{j=0}^{m}(-1)^j \binom{m}{j}(m-j)^n\,.$$

Nieporzadek na zbiorze X jest permutacją f taka, że $f(x) \neq x$ dla każdego $x \in X$. Liczba nieporządków D_n dla $|X| = n$ podana jest w nastepującym twierdzeniu.

Twierdzenie 4.1.5. *Liczba nieporządków D_n dla $|X| = n$ dana jest wzorem*

$$D_n = \sum_{j=0}^{n}(-1)^j \binom{n}{j}(n-j)! = n!\sum_{j=1}^{n}\frac{(-1)^j}{j!}\,. \tag{4.1.8}$$

Ze wzoru (4.1.8) wynika, że przy $n \to \infty$ nieporządki stanowią $e^{-1} = 0.36788\ldots$ wszystkich permutacji.

4.2. Liczby Stirlinga drugiego rodzaju

Niech $\pi = \{B_1, B_2, \ldots, B_k\}$ będzie rodziną podzbiorów zboru X taką, że $B_1 \cup B_2 \cup \cdots \cup B_k = X$, $B_i \cap B_j = \emptyset$ dla $i \neq j$ oraz $B_i \neq \emptyset$ dla $1 \leqslant i \leqslant k$. Rodzinę π nazywą się podziałem zbioru X na k bloków. Zbiór wszystkich podziałów zbioru X na k bloków oznacza się przez $\Pi_k(X)$, a zbiór wszystkich podziałów przez $\Pi(X)$.

Podział Π zbioru n-elementowego zbioru X jest typu $\lambda = (\lambda_1, \ldots, \lambda_n)$, jeśli zawiera λ_i bloków i-elementowych. Typ taki zapisujemy jako $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$.

Twierdzenie 4.2.1. *Liczba podziałów typu $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$ zbioru n-elementowego, $n = \lambda_1 + 2\lambda_2 + \cdots + n\lambda_n = n$ jest równa*

$$P(\lambda_1, \ldots, \lambda_n) = \frac{n!}{\lambda_1!\lambda_2! \ldots \lambda_n! \, (1!)^{\lambda_1} (2!)^{\lambda_2} \ldots (n!)^{\lambda_n}}.$$

Liczby Stirlinga drugiego rodzaju określa się wzorem

$$x^n = \sum_{k=0}^{n} S(n,k) (x)_k \tag{4.2.1}$$

lub równoważnie

$$(x)^n = \sum_{k=0}^{n} S(n,k) \, x_k. \tag{4.2.2}$$

Twierdzenie 4.2.2. *Definicje liczb Stirlinga określone wzorami* (4.2.1) *i* (4.2.2) *są równoważne.*

Dowód. ???? □

Twierdzenie 4.2.3. *Liczby Stirlinga drugiego rodzaju spełniają wzór rekurencyjny*

$$S(n,k) = S(n-1, k-1) + kS(n-1,k) \tag{4.2.3}$$

dla $0 < k < n$ oraz $S(n,n) = 1$ dla $n \geqslant 0$, $S(n,0) = 0$ dla $n > 0$.

Twierdzenie 4.2.4.

$$S(n,k) = |\Pi_k(X)| \tag{4.2.4}$$

gdzie $|X| = n$.

Z twierdzenia 4.2.1 wynika wzór

$$S(n,k) = \sum_{\substack{\lambda_1 + \cdots + \lambda_n = k \\ \lambda_1 + n\lambda_n}} \frac{n!}{\lambda_1!\lambda_2! \ldots \lambda_n! \, (1!)^{\lambda_1} (2!)^{\lambda_2} \ldots (n!)^{\lambda_n}}.$$

Liczby Bella[6] definiuje się wzorem

$$B_n = \sum_{k=0}^{n} S(n,k) \ ,$$

czyli $B_n = |\Pi(X)|$.
Zachodzi równość

$$B_{n+1} = \sum_{i=0}^{n} \binom{n}{i} B_i \, ,$$

gdzie $B_0 = 0$.

Przykład zastosowania liczb Stirlinga

Twierdzenie 4.2.5. *Jeśli $|X| = n$, $|Y| = m$, to liczba wszystkich funkcji $f : X \overset{\text{na}}{\to} Y$, $(f(X) = Y)$, jest równa*

$$s_{n,m} = \sum_{i=0}^{m-1} (-1)^i \binom{m}{n} (m-i)^n \ . \tag{4.2.5}$$

Dowód. Niech $Y = \{y_1, \ldots, y_m\}$ oraz niech $A_i = \{f : y_i \notin f(X)\}$. Wtedy

$$f(X) = Y \iff f \in \bigcup_{i=1}^{m} A_i \, .$$

Wszystkich funkcji $f : X \to Y$ jest m^n, (twierdzenie 1.2.1). Szukamy więc $|A_1 \cup \cdots \cup A_m|$. Aby skorzystać z twierdzenia 4.1.1, trzeba znać liczebność iloczynu $A_{k_1} \cap \cdots \cap A_{k_j}$ dla dowolnego ciągu $1 \leqslant k_1 < \cdots < k_j \leqslant m$. Iloczyn ten jest zbiorem wszystkich funkcji $f : X \to Y \setminus \left\{y_{k_1}, \ldots, y_{k_j}\right\}$, więc jego liczebność wynosi $(m-j)^n$. Ciąg $1 \leqslant k_1 < \cdots < k_j \leqslant m$ można wybrać na $\binom{m}{j}$ sposobów, więc

$$\begin{aligned} s_{n,m} &= m^n - \left| \bigcup_{j=0}^{m-1} A_j \right| = m^n - \sum_{j=1}^{m-1} (-1)^j \binom{m}{j} (m-j)^n \\ &= \sum_{j=0}^{m-1} (-1)^j \binom{m}{j} (m-j)^n \ , \end{aligned}$$

co dowodzi wzoru (4.2.5). □

Pokażemy teraz, że

$$s_{n,m} = m! S(n,m) \ .$$

Istotnie ????
Stąd otrzymuje się wzór na liczby Stirlinga drugiego rodzaju:

$$S(n,k) = \frac{1}{k!} \sum_{j=0}^{k-1} (-1)^j \binom{k}{j} (k-j)^n \ .$$

Związek z dzielnikami liczb ????

[6] Bell

4.3. Zadania

1. Ile dzielników ma liczba 216000?

2. Na ile sposobów możesz rozbić zbiór 10-elementowy na zbiory 2-elementowe, a na ile sposobów możesz rozbić zbiór $2n$-elementowy na takie podzbiory?

3. Wyznaczyć liczbę ciągów długości $2n$ takich, że każda liczba $i \in \{1 \ldots, n\}$ występuje dokładnie dwa razy, przy czym żadne dwa kolejne wyrazy nie są równe.

4. Na pewnej wyspie mieszka 300 dzikusów, z których każdy jest matematykiem, filozofem lub ludożercą. Połowa ludożerców zajmuje się filozofią, połowa filozofów to matematycy, a połowa matematyków to ludożercy. Wiedząc, że żaden z ludożerców nie zajmuje się filozofią i matematyką jednocześnie, ustal z ilu osób składa się każda z tych grup.

5. Wyznaczyć liczbę podzbiorów 11-elementowych zbioru z powtórzeniami $\{4 * a, 3 * b, 7 * c\}$.

6. (Wzór Faa di Bruno). Udowodnić, że

$$\frac{d^n}{dx^n} f\left(g\left(x\right)\right) = \sum_{j=0}^{n} \sum_{\substack{k_1+k_2+\cdots+k_n=j \\ k_1+2k_2+\cdots+nk_n=n \\ k_1,k_2,\ldots,k_n \geqslant 0}} f^{(j)} \frac{n!\left(g^{(1)}\right)^{k_1} \ldots \left(g^{(n)}\right)^{k_n}}{k_1!\left(1!\right)^{k_1} \ldots k_n!\left(n!\right)^{k_n}}.$$

5. Funkcje tworzące

5.1. Szeregi formalne

Definicja. Niech a_k będzie ciągiem liczbowym. Funkcją tworzącą nazywa się szereg formalny

$$A(x) = \sum_{k=0}^{\infty} a_k x^k . \tag{5.1.1}$$

Nazwa „szereg formalny" oznacza, że wzór (5.1.1) określa takie własności szeregów jak ich dodawanie, mnożenie, mnożenie przez liczbę, natomiast nie bada się ich zbieżności.

Szereg formalny

$$\widehat{A}(x) = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!} \tag{5.1.2}$$

nazywa się wykładniczą funkcją tworzącą.

Operacje na szeregach

Dla szeregów $A(x) = \sum_{k=0}^{\infty} a_k x^k$ i $B(x) = \sum_{k=0}^{\infty} b_k x^k$ określa się operacje:

dodawanie:

$$A(x) + B(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k ,$$

mnożenie przez liczbę:

$$\alpha A(x) = \alpha A(x) = \sum_{k=0}^{\infty} a_k x^k ,$$

mnożenia:

$$A(x) B(x) = \sum_{k=0}^{\infty} c_k x^k ,$$

gdzie

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} .$$

Jeżeli szereg (5.1.1) jest zbieżny do funkcji $f(x) = A(x)$ dla pewnego promienia zbieżności $r > 0$, to będziemy utożsamiać szereg formalny (5.1.1) z funkcją $f(x)$ również dla $|x| > r$. Wtedy

$$A'(x) = \sum_{k=0}^{\infty} (k+1) a_{k+1} x^k .$$

Przykład.

$$e^x = \sum_{k=0}^{\infty} \frac{1}{k!}\, x^k$$

dla $a_k = 1/k!$,

$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k$$

dla $a_k = 1$,

$$(1+x)^n = \sum_{k=1}^{\infty} \binom{n}{k} x^k = \sum_{k=1}^{n} \binom{n}{k} x^k$$

dla $a_k = \binom{n}{k}$.

Twierdzenie 5.1.1. *Szereg* (5.1.1) *ma szereg odwrotny względem mnożenia wtedy i tylko wtedy, gdy jego wyraz wolny jest różny od zera.*

Przykład.

$$\left(\sum_{k=0}^{\infty} x^k \right)^{-1} = 1 - x\,.$$

Przykład. Następującą tożsamość można udowodnić, korzystając z funkcji tworzących:

$$\binom{m+k}{k} = \sum_{s=0}^{k} \binom{m}{s} \binom{n}{k-s}\,.$$

Porównamy współczynniki po obu stronach równości:

$$\begin{aligned} \sum_{k=0}^{m+n} \binom{m+n}{k} x^k &= (1+x)^{m+n} = (1+x)^m (1+x)^n \\ &= \sum_{i=0}^{m} \binom{m}{i} x^i \sum_{j=0}^{n} \binom{n}{j} x^j = \sum_{k=0}^{m+n} \sum_{s=0}^{k} \binom{m}{s} \binom{n}{k-s} x^k\,. \end{aligned}$$

5.2. Rozwiązywania rekurencji

Algorytm rozwiązywania

Problem: dla danego ciągu $\{g_n\}$ spełniającego pewne równanie rekurencyjne, znaleźć jawny wzór na g_n jako funkcji n. Rozwiązanie jest następujące.

1. Napisać równanie $g_n = f(g_n, \ldots, g_{n-k})$ dla całkowitych n i pewnego k, przy czym $g_{-1} = g_{-2} = \cdots = 0$.
2. Pomnożyć obie strony równania przez x^n i zsumować. Otrzyma się równanie

$$\sum_n g_n x^n = h\left(G\left(x\right)\right),$$

3. Rozwiązać równanie ze względu na $G(x)$.
4. Rozwinąć $G(x)$ w szereg potęgowy. Współczynnik przy x^n jest równy g_n.

Liczby Fibonacciego

Rozpatrzymy przykład z liczbami Fibonacciego[7], w oparciu o powyższy schemat. Liczby Fibonacciego są określone wzorem

1. Równanie rekurencyjne

$$g_n = \begin{cases} 0, & \text{dla } n \leqslant 0, \\ 1, & \text{dla } n = 1, \\ g_{n-1} + g_{n-2} & \text{dla } n > 1. \end{cases} \tag{5.2.1}$$

Inaczej

$$g_n = g_{n-1} + g_{n-2} + [n = 1]$$

2. Równanie na funkcję tworzącą

$$\begin{aligned} G(x) = \sum_n g_n x^n &= \sum_n g_{n-1} x^n + \sum_n g_{n_2} + \sum_n [n=1] x^n \\ &= \sum g_n x^{n+1} + \sum_n g_n x^{n+2} + x \\ &= xG(x) + x^2 G(x) + x. \end{aligned} \tag{5.2.2}$$

3. Rozwiązanie równania na funkcję tworzącą

$$G(x) = \frac{x}{1 - x - x^2}. \tag{5.2.3}$$

4. Rozkładamy na $G(x)$ na ułamki proste.

Pierwiastkami równania $1 - x - x^2 = 0$ są $a = \left(1 + \sqrt{5}\right)/2$ oraz $b = \left(1 - \sqrt{5}\right)/2$. Dla $A = a/(a-b)$ i $B = -b/(a-b)$ otrzymujemy

$$G(x) = \frac{A}{1 - ax} + \frac{B}{1 - bx} = \sum_{k=0}^{\infty} \frac{a^{k+1} - b^{k+1}}{a - b} x^k$$

Złoty podział

skąd

$$g_k = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^{k+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{k+1} \right). \tag{5.2.4}$$

5.3. Zastosowania funkcji tworzących

Funkcja tworząca dla współczynników dwumianowych dla ustalonego n:

$$\sum_{k=0}^{\infty} \binom{n}{k} x^k = \sum_{k=0}^{n} \binom{n}{k} x^k = (1 + x)^n.$$

[7] Leonardo Fibonacci, 1180 – 1250

Interpretacja kombinatoryczna: niech $X = \{e_1, \ldots, e_n\}$. W iloczynie $(1+x)^n = (1+x)\ldots(1+x)$, i-ty czynnik $(1+x)$ można traktować jako odpowiednik elementu e_i i reprezentujący liczby wystąpień elementu e_i – zero razy ($x^0 = 1$) i jeden raz ($x^1 = x$). Rozumowanie to można uogólnić na przypadek zbiorów z powtórzeniami, wtedy i-ty czynnik $(1 + x + \cdots + x^j)$ może reprezentować liczbę wystąpień elementu.

Przykład. Niech $X = \{3*a, 1*b, 2*c\}$ oraz niech c_k będzie liczbą podzbiorów k-elementowych tego zbioru. Wtedy

$$\begin{aligned}\sum_{k=0}^{\infty} c_k x^k &= \left(1 + x + x^2 + x^3\right)(1+x)\left(1 + x + x^2\right) \\ &= 1 + 3x + 5x^+ 6x^3 + 5x^4 + 3x^5 + x^6.\end{aligned}$$

Stąd liczba podzbiorów dwuelementowych wynosi 5.

Na liczbę wystąpień e_i można nakładać ograniczenia.

Twierdzenie 5.3.1. *Niech $X = \{e_1, \ldots, e_n\}$ oraz niech c_k oznacza liczbę k-elementowych zbiorów A z powtórzeniami, o elementach z X takich, że dla $i = 1, \ldots, n$ krotność elementu e_i należy do zbioru $\{r_{i1}, r_{i2}, \ldots\}$, gdzie $0 \leqslant r_{i1} \leqslant r_{i2}, \ldots$. Wtedy funkcja tworząca dla ciągu $c_0, c_1, \ldots$ jest równa*

$$C(x) = \sum_{k=0}^{\infty} c_k x^k = \left(x^{r_{11}} + x^{r_{12}} + \ldots\right)\left(x^{r_{21}} + x^{r_{22}} + \ldots\right)\ldots\left(x^{r_{n1}} + x^{r_{n2}} + \ldots\right).$$

Przykład. Jeżeli nie nakładamy żadnych ograniczeń, to

$$\left(1 + x + x^2 + \ldots\right)^n = \frac{1}{(1-x)^n}.$$

Rozwijając tę funkcję w szereg MacLaurina otrzymujemy

$$\begin{aligned}\frac{d^k}{dx^k}(1-x)^{-n} &= (-n)(-n-1)\ldots(-n-k+1)(1-x)^{-n-k}(-1)^k \\ &= (n)^k (1-x)^{-n-k}.\end{aligned}$$

Stąd

$$(1-x)^{-n} = \sum_{k=0}^{\infty} \frac{(n)^k}{k!} x^k = \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k,$$

(porównaj twierdzenie 3.3.1).

Jeżeli liczba wystąpień ma być różna od zera, to funkcja tworząca będzie równa

$$\left(x + x^2 + \ldots\right)^n = \frac{x^n}{(1-x)^n}.$$

Twierdzenie 5.3.2. *Niech $X = \{e_1, \ldots, e_n\}$ oraz niech c_k oznacza liczbę k-elementowych ciągów o elementach z X takich, że dla $i = 1, \ldots, n$ liczba*

wystąpień elementu e_i należy do zbioru $\{r_{i1}, r_{i2}, \dots\}$, gdzie $0 \leqslant r_{i1} \leqslant r_{i2}, \dots$. Wtedy wykładnicza funkcja tworząca dla ciągu $c_0, c_1, \dots$ jest równa

$$C(x) = \sum_{k=0}^{\infty} \frac{c_k x^k}{k!} = \left(\frac{x^{r_{11}}}{r_{11}!} + \frac{x^{r_{12}}}{r_{12}!} + \dots\right)\left(\frac{x^{r_{21}}}{r_{21}!} + \frac{x^{r_{22}}}{r_{22}!} + \dots\right)\dots\left(\frac{x^{r_{n1}}}{r_{n1}!} + \frac{x^{r_{n2}}}{r_{n2}!} + \dots\right).$$

5.4. Sploty

Sploty Fibonacciego. Należy znaleźć wzór na

$$F_n = \sum_{k=0}^{n} f_k f_{n-k},$$

gdzie f_k jest k-tą liczbą Fibonacciego. Ciąg $\{F_n\}$ jest splotem ciagu $\{f_n\}$ z sobą. Liczby Fibonacciego mają funkcję tworzącą daną wzorem (5.2.3)

$$G(x) = \frac{x}{1 - x - x^2},$$

Liczby F_n mają zaś funkcję tworzącą $F(x) = (G(x))^2$. Stąd, otrzymujemy

$$F(x) = \frac{1}{5}\sum_{n=0}^{\infty}(n+1)(2f_{n+1} - f_n)x^n - \frac{2}{5}\sum_{n=0}^{\infty} f_{n+1}x^n.$$

Ostatecznie otrzymujemy

$$F_n = \sum_{k=0}^{n} f_k f_{n-k} = \frac{2nf_{n+1} - (n+1)f_n}{5}.$$

Sploty harmoniczne. Efektywność algorytmu „samplesort" zależy od wartości sumy

$$t_{m,n} = \sum_{k=0}^{n-1} \binom{k}{m} \frac{1}{m-k}$$

dla całkowitych $m, n > 0$. Aby obliczyć $t_{m,n}$ zauważmy, że ciąg $\{t_{m,n}\}$ jest splotem ciągu

$$\binom{0}{m}, \binom{1}{m}, \binom{2}{m}, \dots$$

z ciągiem $0, 1/1, 1/2, \dots$. Ciągi te mają znane funkcje tworzące

$$\sum_{n=0}^{\infty}\binom{n}{m}x^n = \frac{x^m}{(1-x)^{m+1}}; \quad \sum_{n=0}^{\infty}\frac{x^n}{n} = \ln\frac{1}{1-x}.$$

Liczby harmoniczne

Stąd funkcja tworząca $T_m(x)$ dla ciągu $\{t_{m,n}\}$ wyraża się wzorem

$$T_m(x) = \frac{x^m}{(1-x)^{m+1}} \ln \frac{1}{1-x} = (H_n - H_m) \binom{n}{n-m},$$

gdzie

$$H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

są liczbami harmonicznymi.

Drzewem binarnym T o n wierzchołkach nazywa się drzewo puste $T = \emptyset$, gdy $n = 0$ lub trójkę $T = (L, r, P)$, gdzie r jest wierzchołkiem zwanym *korzeniem drzewa*, L jest drzewem binarnym o l wierzchołkach P jest drzewem binarnym o p wierzchołkach oraz $l + p + 1 = n$. Drzewa binarne T_1 i T_2 są izomorficzne, $T_1 \approx T_2$ gdy $T_1 = T_2 = \emptyset$ lub gdy $T_1 = (L_1, r, P_1)$, $T_2 = (L_2, r, P_2)$ oraz $L_1 \approx L_2$ i $P_1 \approx P_2$. Niech c_k oznacza liczbę nieizomorficznych drzew binarnych o k wierzchołkach. Oczywiście $c_0 = 1$ oraz dla $0 \leqslant s \leqslant k$ istnieje $c_s c_{k-1-s}$ nieizomorficznych drzew binarnych (L, r, P) takich, że L ma s wierzchołków. Wobec tego dla $k > 0$

$$c_k = c_0 c_{k-1} + c_1 c_{k-2} + \cdots + c_{k-1} c_0\,, \tag{5.4.1}$$

Niech

$$C(x) = \sum_{k=0}^{\infty} c_k x^k$$

będzie funkcją tworzącą dla ciagu określonego wzorem (5.4.1). Ponieważ prawa strona wzoru (5.4.1) jest splotem ciągu $\{c_i\}$ z przesuniętym ciągiem $c'_i = c_{i-1}$, $c'_0 = 0$, to

$$C(x) = xC^2(x) + 1,$$

a więc

$$xC^2(x) - C(x) + 1 = 0.$$

Rozwiązując to równanie ze względu na $C(x)$ otrzymujemy dla $x \neq 0$

$$C(x) = \frac{1 \pm \sqrt{1-4x}}{2x}\,. \tag{5.4.2}$$

Rozwijając $(1-4x)^{1/2}$ w szereg Maclaurina otrzymujemy

$$\sqrt{1-4x} = 1 - 2\sum_{k=1}^{\infty} \frac{1}{k} \binom{2k-2}{k-1} x^k.$$

Aby otrzymać rozwiązanie o dodatnich współczynnikach, należy w (5.4.2) wybrać znak minus. Stąd

$$C(x) = \frac{1-\sqrt{1-4x}}{2x} = \sum_{k=1}^{\infty} \frac{1}{k} \binom{2k-2}{k-1} x^{k-1} = \sum_{k=0}^{\infty} \frac{1}{k+1} \binom{2k}{k} x^k.$$

Ostatecznie

$$c_k = \frac{1}{k}\binom{2k}{k}.$$

Liczby c_k nazywa się liczbami Catalana[8].

5.5. Zadania

1. Znaleźć funkcje tworzące dla ciągów $a_k = k$, $b_k = 2^k$ oraz $c_k = \binom{m+k}{m}$ dla $k = 0, 1, \ldots$.

2. Znaleźć funkcję tworzącą dla ciągu Fibonacciego, z modyfikacją taką, że $f_0 = 0$, $f_1 = 1$, $f_{n+1} = f_n + f_{n-1}$.

3. Niech a_n będzie liczbą ciągów różnowartościowych o elementach ze zbioru n-elementowego. Udowodnić, że

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} x^n = \frac{e^x}{1-x}\,.$$

4. Na ile sposobów można zbudować kolumnę rozmiaru $2 \times 2 \times n$ z cegieł rozmiaru $2 \times 2 \times 1$?

5. Liczby Fibonacciego drugiego rodzaju $\mathcal{F}_n$ są określone następująco. $\mathcal{F}_0 = 0$, $\mathcal{F}_1 = 1$ oraz $\mathcal{F}_{n+1} = \mathcal{F}_n + \mathcal{F}_{n-1} + f_{n+1}$ dla $n > 0$. Podać $\mathcal{F}_n$ jako funkcję liczb Fibonacciego f_n.

6. Niech c_k będzie liczbą funkcji różnowartościowych ze zbioru k-elementowego w zbiór n-elementowy. Znaleźć funkcję tworzącą dla ciągu c_k i obliczyć c_k.

7. Niech p_n będzie liczbą możliwych rozmieszczeń nawiasów w iloczynie $x_0 \ldots x_n$. Udowodnić, że $p_n = c_n$, gdzie c_k są liczbami Catalana.

8. Udowodnić, że liczba sposobów, w jaki $(n+2)$-kąt wypukły na płaszczyźnie można podzielić na rozłączne trójkąty za pomocą $n-1$ przekątnych nieprzecinających się wewnątrz tego $(n+2)$-kąta, jest równa liczbie Catalana c_n.

9. Niech B_n będa liczbami Bella. Udowodnić, że

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}$$

i korzystając z tej rekurencji znaleźć wykładniczą funkcję tworzącą dla liczb Bella.

[8] Catalan ???

6. Ciała skończone i skończone przestrzenie wektorowe

6.1. Ciała skończone

Zbiór X z działaniami + i $\cdot$ tworzy ciało $(X, +, \cdot)$, gdy spełnione są warunki: (w zapisie, zgodnie ze zwyczajem, na ogół nie piszemy kropki)

C1 $a + b = b + a$,
C2 $(a + b) + c = a + (b + c)$,
C3 $ab = ba$,
C4 $(ab)c = a(bc)$,
C5 $a(b + c) = ab + ac$,
C6 Istnieje zero: $a + 0 = 0 + a = a$,
C7 Istnieje element przeciwny $a + (-a) = 0$,
C8 Istnieje jedynka $a \cdot 1 = 1 \cdot a = a$,
C9 Istnieje element odwrotny $aa^{-1} = a^{-1}a = 1$ dla $a \neq 0$,
C10 $0 \neq 1$.

Grupa addytywna
Grupa multiplikatywna

Jeżeli spełnione są warunki C1, C2, C6, C7, to $(X, +)$ jest grupą addytywną przemienną, jeżeli spełnione są warunki C4, C8, C9, to $(A, \cdot)$ jest grupą multiplikatywną (niekonieczne przemienną), jeśli dodatkowo jest spełniony warunek C3, to jest grupą multiplikatywną przemienną. Jeżeli spełnione są warunki C1–C8 i C10, to $(X, +, \cdot)$ jest pierścieniem.

Twierdzenie 6.1.1. *Jeżeli p jest liczbą pierwszą, to działania $+$ i $\cdot$ określone jako reszty z dzielenia przez p w zwykłym dodawaniu i dzieleniu w zbiorze liczb całkowitych, (czyli działania $\bmod p$), tworzą ciało skończone na zbiorze $X = \{0, 1, \ldots, p-1\}$.*

Pieścień Z_p

Jeżeli p nie jest liczbą pierwszą, to X z działaniami dodawania i mnożenia $\bmod p$ jest pierścieniem Z_p, ale nie ciałem.

Charakterystyką ciała jest najmniejszą liczbą całkowitą k taką, że $\sum_{i=1}^{k} 1 = 0$.

Twierdzenie 6.1.2. *Charakterystyka dowolnego ciała skończonego jest liczbą pierwszą.*

Ciała Galois

Można udowodnić, że każde ciało skończone ma $q = p^m$ elementów, gdzie p jest liczbą pierwszą, a m jest liczbą naturalną. Wszystkie ciała skończone o tej samej liczbie elementów są izomorficzne. Takie q-elementowe ciało oznaczamy przez $GF(q)$ – ciało Galois[9] (Galois field). Dla $m > 1$ są to ciała wielomianów (nie wszystkich –. problem ten rozważymy ogólnie w następnym paragrafie). Gdy $q = p^m$, to charakterystyka takiego ciała wynosi p.

Ciała wielomianów

Przykład. Ciało o $2^2 = 4$ elementach:

$$0,\ 1,\ x,\ x + 1\,.$$

[9] Galois

Wielomian $x^2 + x + 1$ jest nierozkładalny nad $GF(2)$, bo

$$\begin{aligned} x \cdot x &= x^2, \\ x(x+1) &= x^2 + x, \\ (x+1)(x+1) &= x^2 + 2x + 1. \end{aligned}$$

Następnie

$$\begin{aligned} x \cdot x(&\mod x^2 + x + 1) = x + 1, \\ x(x+1)(&\mod x^2 + x + 1) = 1, \\ (x+1)(x+1)(&\mod x^2 + x + 1) = x, \end{aligned}$$

Stąd $GF(4)$:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Natomiast Z_4:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

6.2. Ciała wielomianów

6.3. Skończone przestrzenie wektorowe

Przestrzenie liniowe

Przestrzeń liniowa n-wymiarowa nad ciałem $GF(q)$ jest określona jako zbiór wektorów $\mathbf{x} = (x_1, \ldots, x_n)$, gdzie $x_i \in GF(q)$. Działaniami są

- Dodawanie $\mathbf{x} + \mathbf{y} = (x_1 + y_1, \ldots, x_n + y_n)$,
- Mnożenie przez liczbę $\lambda\mathbf{x} = (\lambda x_1, \ldots, \lambda x_n)$.

Przestrzeń taką oznaczymy przez $V(n, q)$.

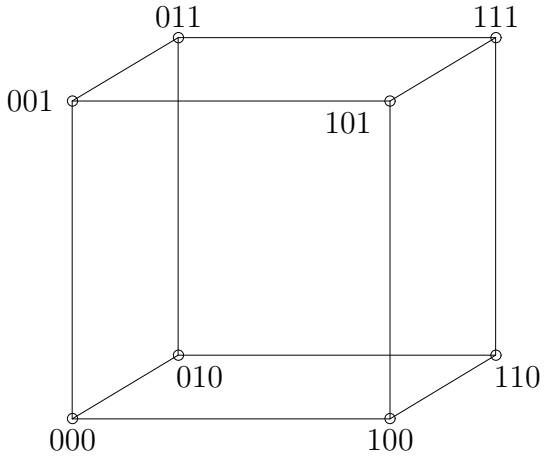
Kraty podprzestrzeni

Rodzina podprzestrzeni przestrzeni $V(n, q)$ tworzy kratę, gdzie dla podprzestrzeni Z oraz T określamy

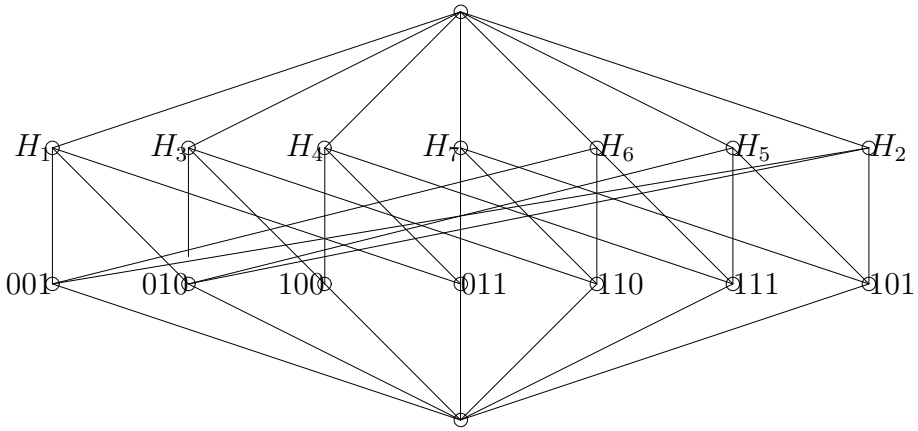
$$\begin{aligned} Z \wedge T &= Z \cap T, \\ Z \vee T &= \{z + t : z \in Z, t \in T\}. \end{aligned}$$

Zero kraty **0** to przestrzeń zerowa składająca się z jednego wektora $(0, \ldots, 0)$. Jedynką kraty **1** jest cała przestrzeń $V(n, 1)$.

Atomy kraty Atomem a kraty L nazywa się taki jej element, że $\mathbf{0} \preccurlyeq a$ oraz jeśli $\mathbf{0} \preccurlyeq b \preccurlyeq a$, to albo $b = \mathbf{0}$ albo $b = a$. W kracie podprzestrzeni, atomami są podprzestrzenie jednowymiarowe.



Rysunek 2. Przestrzeń $V(3, 2)$



Rysunek 3. Krata podprzestrzeni $V(3, 2)$

Dla $V(3, 2)$ podprzestrzeniami dwuwymiarowymi są: H_1, H_2, H_3 – ściany zawierające $(0, 0, 0)$, H_4, H_5, H_6 – „płaszczyzny" przechodzące przez krawędź zawierającą $(0, 0, 0)$ i krawędź równoległą do niej zawierającą $(1, 1, 1)$, $H_7 = \{000, 011, 110, 101\}$.

Oznaczmy

$$[x] = \frac{q^x - 1}{q - 1}\,. \tag{6.3.1}$$

Własność 0. *Jeśli n jest liczba naturalną, to $[n]$ określone wzorem (6.3.1) jest liczbą atomów w kracie podprzestrzeni, przestrzeni $V(n,q)$ nad ciałem $GF(q)$.*

Przyjmijmy oznaczenia:

$$\begin{aligned}
&[x]_k = [x][x-1]\dots[x-k+1], \quad (x)_k = x(x-1)\dots(x-k+1),\\
&[k]! = [k]_k, \quad k! = (k)_k,\\
&\begin{bmatrix} x \\ k \end{bmatrix} = \frac{[x]_k}{[k]!}\,, \quad \binom{x}{k} = \frac{(x)_k}{k!}\,.
\end{aligned}$$

Twierdzenie 6.3.1.

$$\lim_{q\to 1}[x]_k = (x)_k\,, \quad \lim_{q\to 1}\begin{bmatrix} x \\ k \end{bmatrix} = \binom{x}{k}\,.$$

Symbol Gaussa

Symbol $\begin{bmatrix} x \\ k \end{bmatrix}$ nazywa się symbolem Gaussa i ma własności podobne do symbolu Newtona.

Twierdzenie 6.3.2.

$$\begin{bmatrix} x \\ k \end{bmatrix} = \begin{bmatrix} x \\ x-k \end{bmatrix}$$

oraz

$$\begin{bmatrix} x+1 \\ k+1 \end{bmatrix} = \begin{bmatrix} x \\ k \end{bmatrix} + q^{k+1}\begin{bmatrix} x \\ k+1 \end{bmatrix},.$$

Dowód. □

Twierdzenie 6.3.3. *Liczba podprzestrzeni wymiaru k przestrzeni $V(n,q)$ czyli elementów kraty rzędu k jest równa*

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}\,.$$

Dowód. □

Twierdzenie 6.3.4.

$$x^n = \sum_{k=0}^{n}\begin{bmatrix} n \\ k \end{bmatrix}(x-1)(x-q)\dots\left(x-q^{k-1}\right). \tag{6.3.2}$$

Dowód. □

6.4. Zadania

1. Sprawdzić, że wielomian $x^3 + x + 1 \in Z_2$ jest nierozkładalny nad ciałem Z_2. Wypisać wszystkie elementy ciała $GF(8)$ rozumianego jako ciało reszt z dzielenia przez $x^3 + x + 1$ w pierścieniu Z_2.

2. Sprawdzić, że wielomian $x^2 + x + 2 \in Z_3$ jest nierozkładalny nad ciałem Z_3. Wypisać wszystkie elementy ciała $GF(9)$ rozumianego jako ciało reszt z dzielenia przez $x^2 + x + 2$ w pierścieniu Z_3.

3. W ciele $GF(8)$ z zadania 1 obliczyć:
$(1 + x) + (x + x^2)$, $(1 + x)(x + x^2)$, x^4.

4. W ciele $GF(9)$ z zadania 2 obliczyć:

$(1 + x) + (2 + x)$, $(2 + x) - (1 + 2x)$,

$(1 + x)(1 + 2x)$, x^3 .

5. W ciele $GF(8)$ z zadania 1 rozwiązać równania kwadratowe o niewiadomej t:

$t^2 + (x^2 + 1)t + 1 = 0$, $t^2 + t + x = 0$,

$t^2 + t + x^2 = 0$, $t^2 + t + (x^2 + 1) = 0$,

$t^2 + (x^2 + 1)t + (x^2 + 1) = 0$.

6. Udowodnić, że

$$\begin{bmatrix} n \\ 0 \end{bmatrix} < \begin{bmatrix} n \\ 1 \end{bmatrix} < \cdots < \begin{bmatrix} n \\ \lfloor n/2 \rfloor \end{bmatrix} = \begin{bmatrix} n \\ \lceil n/2 \rceil \end{bmatrix} > \cdots > \begin{bmatrix} n \\ n \end{bmatrix}.$$

7. Udowodnić, że dla $q > 1$

$$q^{k(n-k)} \leqslant \begin{bmatrix} n \\ k \end{bmatrix} \leqslant q^{k(n-k-1)}$$

8. Udowodnić, że dla $q > 1$

$$q^{kn-\binom{k}{2}} \geqslant (q-1)^k \, [n]_k \geqslant \beta q^{kn-\binom{k}{2}},$$

gdzie

$$\beta = \prod_{i=1}^{\infty} \left(1 - q^{-i}\right),$$

9. Udowodnić, że dla $q > 1$

$$(q-1)^k \, [n]_k \sim q^{kn-\binom{k}{2}}$$

o ile $kq^{-n+k} = o\,(n)$.

7. Geometrie rzutowe i afiniczne

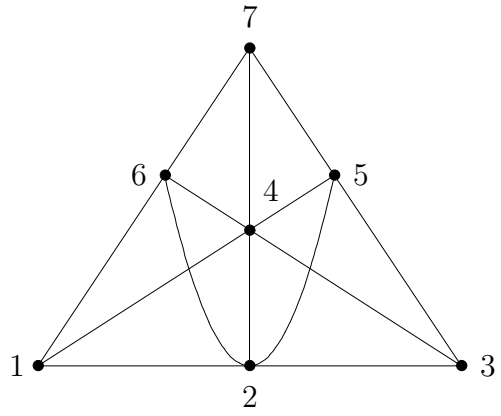
7.1. Skończone geometrie rzutowe

Geometrie rzutowe

Geometrią rzutową nazywa się zbiór punktów X i rodzinę podzbiorów zwanych prostymi, spełniających warunki:

(i) dowolne dwa punkty leżą na dokładnie jednej prostej,
(ii) dla dowolnych czterech punktów x, y, z, t nie leżących na jednej prostej, jeżeli xy przecina zt, to xz przecina yt,
(iii) każda prosta ma co najmniej trzy punkty.

Jeżeli za punkty przyjmiemy atomy kraty podprzestrzeni $V(n,q)$, to podprzestrzenie rzędu 2 są prostymi. Taką geometrię oznaczamy symbolem $PG(n-1,q)$. Geometrię rzutową rzędu $PG(2,2)$ nazywamy płaszczyzną Fano (rys. 4). Na rys. 5 przedstawiona jest płaszczyzna $PG(2,3)$.



Rysunek 4. Płaszczyzna Fano $PG(2,2)$

Twierdzenie 7.1.1. *Liczba podprzestrzeni k-wymiarowych n-wymiarowej geometrii $PG(n-1,q)$ jest równa $\begin{bmatrix} n \\ k \end{bmatrix}$.*

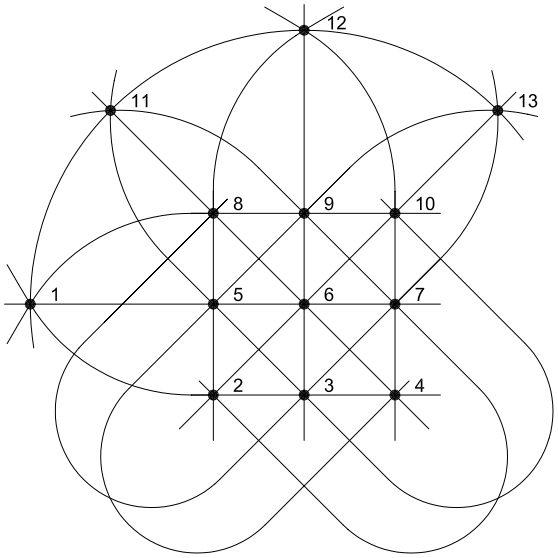
Płaszczyzny rzutowe

Płaszczyzny rzutowe można określić aksjomatycznie w następujący sposób.

(i) dowolne dwa punkty leżą na dokładnie jednej prostej,
(ii) każde dwie różne proste mają dokładnie jeden punkt wspólny,
(iii) istnieją cztery różne punkty, z których żadne trzy nie leżą na jedej prostej.

Istnieją płaszczyny rzutowe nieizomorficzne z $PG(2,q)$, natomiast geometrie rzutowe, które nie są płaszczyznami są izomorficzne z $PG(n-1,q)$ dla pewnych n i q.

Twierdzenie 7.1.2. *Płaszczyna $PG(2,q)$ zawiera q^2+q+1 punktów oraz q^2+q+1 prostych. Każda prosta zawiera dokładnie $q+1$ punktów, a przez każdy punkt przchodzi $q+1$ prostych.*



Rysunek 5. Płaszczyzna rzutowa $PG(2,3)$

7.2. Skończone geometrie afiniczne

Geometrie afiniczne

Geometrią afiniczną nazywa się zbiór punktów X i rodzinę podzbiorów zwanych prostymi, spełniających warunki:

Geometrię afiniczną $AG(n,g)$ konstruujemy następująco. Niech $V(n,q)$ będzie n-wymiarową przestrzenią liniową nad ciałem $GF(q)$, a Z – jej podprzestrzenią. Relacja $\equiv$ określona wzorem

$$a \equiv b \iff a - b \in Z \tag{7.2.1}$$

jest relacją równoważności. Atomy w kracie warstw tej relacji są punktami geometrii afinicznej $AG(n,q)$, podprzestrzenie rzędu 2, są prostymi.

Twierdzenie 7.2.1. *Liczba podprzestrzeni k-wymiarowych n-wymiarowej geometrii $AG(n,q)$ jest równa $q^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}$.*

Płaszczyzny afiniczne

Płaszczyzny afiniczne można określić aksjomatycznie w następujący sposób.

(i) dowolne dwa punkty leżą na dokładnie jednej prostej,
(ii) dla każdej prostej L i każdego punktu $p \notin L$ istnieje dokładnie jedna prosta L' równoległa do L ($L' \parallel L$) taka, że $p \in L$.
(iii) istnieją cztery różne punkty, z których żadne trzy nie leżą na jednej prostej.

Istnieją płaszczyzny afiniczne nieizomorficzne z $AG(2,q)$, natomiast geometrie afiniczne, które nie są płaszczyznami są izomorficzne z $AG(n-1,q)$ dla pewnych n i q.

Twierdzenie 7.2.2. *Płaszczyna $AG(2,q)$ zawiera q^2 punktów oraz q^2+q prostych. Każda prosta zawiera dokładnie q punktów, a przez każdy punkt*

przechodzi $q+1$ prostych.

7.3. Zadania

1. Udowodnić, że każda geometria $PG(2,q)$ jest płaszczyzną rzutową, tzn. spełnia warunki (i) – (iii).

2. Wyprowadzić wzór na liczbę różnych czworokątów, tzn. czwórek punktów z których żadne trzy nie leżą na jednej prostej, płaszczyzny $PG(2,q)$.

3. Udowodnić, że liczba podprzestrzeni rzędu s zawierających ustaloną podprzestrzeń rzędu u geometrii $PG(n-1,q)$, jest równa

$$\begin{bmatrix} n-u \\ s-u \end{bmatrix}.$$

8. Matroidy

8.1. Definicje

Bazy matroidu

Niech E będzie zbiorem skończonym. Matroidem (matroidem baz) nazywamy parę $M = (E, \mathcal{B})$ taką, że niepusta rodzina $\mathcal{B}$ podzbiorów zbioru E spełnia następujące postulaty:

(b_1) żadna baza nie jest podzbiorem właściwym innej bazy,
(b_2) jeśli $B_1 \in \mathcal{B}$, $B_2 \in \mathcal{B}$, $e \in B_1$ to istnieje $f \in B_2$ takie, że $(B_1 \setminus \{e\} \cup \{f\}) \in \mathcal{B}$.

Własności takie mają bazy w skończonych przestrzeniach liniowych nad dowolnym ciałem, w szczególności $GF(q)$ (własność Steiniza).

Twierdzenie 8.1.1. *Wszystkie bazy matroidu M mają tę samą liczbę elementów $r = \rho(M)$.*

Liczbę $r = \rho(M)$ nazywa się rzędem matroidu.

Zbiory niezależne

Definicja. Zbiorem niezależnym nazywa się dowolny podzbiór dowolnej bazy. Rodzinę zbiorów niezależnych oznaczamy przez $\mathcal{I}$. Parę $M = (E, \mathcal{I})$ nazywa się matroidem zbiorów niezależnych.

Cykle

Cyklem nazywa się każdy minimalny zbiór zależny (tzn. taki, który nie jest niezależny). Rodzinę cykli oznaczamy przez $\mathcal{C}$. Parę $M = (E, \mathcal{C})$ nazywa się matroidem cykli.

Rząd

Rzędem $\rho(A)$ zbioru $A \subseteq E$ nazywa się liczbę elementów maksymalnego zbioru niezależnego $I \subseteq A$. Parę $M = (E, \rho)$ nazywa się matroidem z funkcją rzędu.

Rozpięcie

Rozpięciem $\sigma(A)$ zbioru $A \subseteq E$ nazywa się maksymalny zbiór B taki, że $A \subset B$ i $\rho(A) = \rho(B)$. Parę $M = (E, \mathcal{I})$ nazywa się matroidem rozpięć.

Zbiory niezależne, cykle, rząd i rozpięcie można scharakteryzować również aksjomatycznie, przyjmując warunki konieczne i dostateczne z poniższych twierdzeń 8.1.2 – 8.1.5 jako postulaty.

Twierdzenie 8.1.2. *Rodzina $\mathcal{I}$ jest rodziną zbiorów niezależnych wtedy i tylko wtedy, gdy są spełnione warunki:*

(i_1) *jeśli $I_1 \subseteq I_2 \in \mathcal{I}$, to $I_1 \in \mathcal{I}$,*
(i_2) *jeśli $I_1, I_2 \in \mathcal{I}$, $|I_1| < |I_2|$, to istnieje $e \in I_2$, $e \notin I_1$ taki, że $I_1 \cup \{e\} \in \mathcal{I}$.*

Twierdzenie 8.1.3. *Rodzina $\mathcal{C}$ jest rodziną cykli wtedy i tylko wtedy, gdy są spełnione warunki:*

(c_1) *jeżeli $C_1 \subset C_2 \in \mathcal{C}$, to $C_1 \notin \mathcal{C}$,*
(c_2) *jeżeli $C_1, C_2 \in \mathcal{C}$, $C_1 \neq C_2$, $e \in C_1 \cap C_2$, to istnieje $C \in \mathcal{C}$ taki, że $C \subseteq C_1 \cup C_2 \setminus \{e\}$.*

Twierdzenie 8.1.4. *Funkcja $\rho : 2^E \to \mathbb{R}$ jest funkcją rzędu wtedy i tylko wtedy, gdy są spełnione warunki:*

(r_1) $0 \leqslant \rho(A) \leqslant |A|$,
(r_2) *jeżeli $A \subseteq B \subseteq E$, to $\rho(A) \leqslant \rho(B)$,*
(r_3) $\rho(A \cup B) + \rho(A \cap B) \leqslant \rho(A) + \rho(B)$.

Twierdzenie 8.1.5. *Funkcja $\sigma : 2^E \to 2^E$ jest funkcją rozpięcia wtedy i tylko wtedy, gdy są spełnione warunki:*
(s_1) $A \subseteq \sigma(A)$,
(s_2) *jeśli* $A \subseteq B$, *to* $\sigma(A) \subseteq \sigma(B)$,
(s_3) $\sigma(\sigma(A)) = \sigma(A)$,
(s_4) *jeśli* $f \notin \sigma(A)$, $f \in \sigma(A \cup \{e\})$, *to* $e \in \sigma(A \cup \{f\}$.

Zbiory $A \subseteq E$ takie, że $\sigma(A) = A$ nazywa się zbiorami domkniętymi.

Określmy własność (s_4') następująco:
(s_4') *jeśli* $f \notin \sigma(A)$, $f \in \sigma(A \cup \{e\})$, $f \neq e$ *to* $e \notin \sigma(A \cup \{f\}$.

Parę (E, σ) spełniającą warunki (s_1) – (s_4') nazywamy antymatroidem.

Pętlą nazywa się cykl jednoelementowy $\{e\}$, czyli gdy $\{e\} \in \mathcal{C}$ lub $\rho(\{e\}) = 0$.

Przykład. Matroidy trywialne – jedynym zbiorem niezależnym jest $\emptyset$. Wtedy $\rho(M) = 0$. Inaczej mówiąc, każdy element tworzy pętlę.

Przykład. Matroidy wolne – wszystkie podzbiory są niezależne.

Przykład. Matroidy jednorodne (k-jednorodne) – bazami są wszystkie zbiory k-elementowe. Wtedy $\rho(M) = k$.

Przykład. Matroidy reprezentowalne nad ciałem F – izomorficzne z matroidami, których zbiorami niezależnymi w sensie warunków (i_1) – (i_2) są zbiory wektorów liniowo niezależnych w przestrzeni wektorowej V nad ciałem F. Ciało F nie musi być skończone. Matroidy binarne, to matroidy reprezentowalne nad ciałem $GF(2)$.

Przykład. Niech

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{bmatrix},$$

Matroid macierzy

gdzie elementy a_{ij} należą do dowolnego ciała F. Niech E będzie zbiorem kolumn macierzy A. Rodziną zbiorów niezależnych matroidu $M(A) = (E, \mathcal{I})$ będzie teraz rodzina zbiorów kolumn liniowo niezależnych. Takie matroidy nazywane są matroidami macierzowymi. Matroidy macierzowe są oczywiście reprezentowalne nad ciałem F.

Przykład. Niech A będzie podzbiorem punktów skończonej geometrii rzutowej $PG(r-1, q)$ lub afinicznej $AG(r, q)$. Określmy $\sigma(A)$ jako najmniejszą podprzestrzeń zawierającą A. Łatwo sprawdzić, że tak określone σ spełnia warunki (s_1) – (s_4) z twierdzenia 8.1.5, a więc jest rozpięciem. Jeżeli tą podprzestrzenią jest $PG(r'-1, q)$ lub $AG(r', q)$, to $\rho(A) = r'$.

Oznacza to, że geometrię można traktować jako matroid, w którym podprzestrzenie (podgeometrie) są zbiorami domkniętymi. Matroidy te są reprezentowalne nad $GF(q)$.

8.2. Dualność

Matroid dualny M^* do matroidu M można określić na różne, choć równoważne sposoby.

Definicja. Jeżeli $M = (E, \mathcal{B})$ jest matroidem, to dla rodziny $\mathcal{B}^*$ określonej wzorem

$$\mathcal{B}^* = \{B^* : B^* = E \setminus B, B \in \mathcal{B}\},$$

para $M^* = (E, \mathcal{B}^*)$ jest matroidem dualnym do M.

Definicja. Jeżeli $M = (E, \rho)$ jest matroidem, to dla funkcji ρ^* określonej wzorem

$$\rho^*(A) = |A| + \rho(E \setminus A) - \rho(E)$$

dla dowolnego $A \subseteq E$, para $M^* = (E, \rho^*)$ jest matroidem dualnym do M.

Można udowodnić, że obie powyższe definicje są równoważne. Oczywista natomiast jest równość $M^{**} = M$.

Kobazy i kocykle

Mając dane $\mathcal{B}^*$ lub ρ^* można również określić $\mathcal{C}^*$ jako rodzinę cykli w matroidzie dualnym $(E, \mathcal{B}^*)$ lub (E, ρ^*). Zbiory z rodziny $\mathcal{B}^*$ nazywa się kobazami, a zbiory z rodziny $\mathcal{C}^*$ nazywa się kocyklami.

Twierdzenie 8.2.1. *Jeżeli $C \in \mathcal{C}$, $B^* \in \mathcal{B}^*$, to $C \cap B^* \neq \emptyset$. Jeżeli $C^* \in \mathcal{C}^*$, $B \in \mathcal{B}$, to $C^* \cap B \neq \emptyset$.*

Twierdzenie 8.2.2. *Rodzina $\mathcal{C}^*$ podzbiorów zbioru E jest rodziną kocykli wtedy i tylko wtedy, gdy zbiory z $\mathcal{C}^*$ są minimalnymi niepustymi podzbiorami $C^* \subseteq E$ takimi, że $|C \cap C^*| \neq 1$ dla każdego $C \in \mathcal{C}$.*

8.3. Algorytmy zachłanne

Niech E będzie zbiorem skończonym oraz $w : E \to \mathbb{R}^+$. Wartość funkcji $w(e)$ nazywa się wagą elementu e. Niech $\mathcal{S}$ będzie pewną rodziną podzbiorów zbioru E. Liczbę

$$w(A) = \sum_{e \in A} w(e)$$

nazywa się wagą zbioru A.

Algorytm zachłanny

Rozważmy problem znalezienia zbioru $A \in \mathcal{I}$ o największej wadze. W tym celu sformułujemy następujący algorytm, zwany zachłannym. Algorytm ten sformułowany został w języku C–podobnym. Załóżmy, że `A` jest zmienną reprezentującą zbiór, a `I` zmienną reprezentującą rodzinę zbiorów (w rzeczywistości mogą to być odpowiednie listy) oraz że `+` jest przeciążonym operatorem dodawania elementu do zbioru. Funkcja `in(A,I)` sprawdza, czy zbiór `A` należy do rodziny `I`.

Algorytm zachłanny

```
// Sortujemy elementy e wg niemalejących wag
// w ciąg e[0]>=e[1]>= ... >=e[n-1]
A=0; // 0 oznacza zbiór pusty
for(i=0;i<n;i++)
{
   if(in(A+e[i],I){A+=e;}
     // wybieramy zachłannie największy możliwy
}
return A;
```

Twierdzenie 8.3.1. *(Rado, Edmonds). Jeżeli $M = (E, \mathcal{I})$ jest matroidem, to A znalezione przez algorytm zachłanny jest zbiorem niezależnym o największej wadze. Jeżeli $(E, \mathcal{I})$ nie jest matroidem, to istnieje funkcja $w : E \to \mathbb{R}^+$ taka, że A nie jest zbiorem o największej wadze.*

8.4. Zadania

1. Niech E będzie zbiorem skończonym, $|E| = n$ oraz niech $m < n$. Niech $\mathcal{P} = \{A : |A| = k,\ k < m\}$. Sprawdzić, czy rodzina $\mathcal{P}$ jest dla pewnych m

(i) rodziną baz,
(ii) rodziną cykli,
(iii) rodziną zbiorów niezależnych

pewnego matroidu. Jeżeli jest rodziną baz, to wyznaczyć cykle i kocykle, jeżeli jest rodziną cykli, to wyznaczyć bazy i kocykle.

2. Dla matroidu $PG(2, 2)$ wyznaczyć bazy i cykle. Wyznaczyć matroid dualny.

3. Niech rodzinę $\mathcal{P}$ tworzą dopełnienia prostych na płaszczyźnie Fano. Sprawdzić, czy rodzina $\mathcal{P}$ jest dla pewnych m

(i) rodziną baz,
(ii) rodziną cykli,
(iii) rodziną zbiorów domkniętych

pewnego matroidu. Jeżeli jest rodziną baz, to wyznaczyć cykle i kocykle, jeżeli jest rodziną cykli, to wyznaczyć bazy i kocykle, jeśli jest rodziną zbiorów domkniętych, to wyznaczyć bazy.

4. Wykazać, że z dokładnością do izomorfizmu istnieją dokładnie cztery matroidy na zbiorze dwuelementowym i osiem na zbiorze trzyelementowym.

5^P. Niech A będzie macierzą o nieujemnych elementach. Niech w matroidzie macierzowym $M(A)$ wagą kolumny będzie suma jej elementów. Wykorzystując metodę eliminacji Gaussa, napisać algorytm zachłanny dla matroidu macierzowego.

6^P. Niech $M = PG(r-1, 2)$, tzn. niech M będzie matroidem, którego elementami są punkty $PG(r-1, 2)$, (niezerowe wektory przestrzeni liniowej $V(r, 2)$ a

bazami matroidu bazy $V(r, 2)$. Wagą elementu niech będzie liczba jedynek odpowiedniego wektora. Napisać algorytm znajdujący bazę o maksymalnej sumie wag.

9. Transwersale i matroidy

9.1. Transwersale

Niech E będzie zbiorem niepustym, a $\mathcal{F} = (S_1, \ldots, S_m)$ rodziną jego niepustych, niekoniecznie różnych podzbiorów. Niech $t : \{1, \ldots, m\} \to E$ będzie funkcją różnowartościową taką, że $t(i) \in S_i$. *Tanswersala* T rodziny $\mathcal{F}$, to zbiór wartości takiej funkcji t. Inaczej mówiąc, do transwersali do transwersali wybieramy dokładnie m elementów, po jednym z każdego zbioru rodziny $\mathcal{F}$. Nie dla każdej rodziny $\mathcal{F}$ istnieje transwersala.

Transwersala częściowa

Transwersala podrodziny $\mathcal{F}'$ rodziny $\mathcal{F}$ jest *transwersalą częściową* rodziny $\mathcal{F}$. Rzecz jasna, każdy podzbior transwersali częściowej jest transwersalą częściową.

Przykład. Niech $E = \{1, 2, 3, 4, 5, 6\}$ oraz $S_1 = S_2 = \{1, 2\}$, $S_3 = S_4 = \{2, 3\}$, $S_5 = \{1, 4, 5, 6\}$. Taka rodzina $\mathcal{F}$ nie ma transwersali. Rodzina $\mathcal{F}' = \{S_1, S_2, S_3, S_5\}$ ma traswersale, np. $T' = \{1, 2, 3, 4\}$, która jest transwersalą częściową dla $\mathcal{F}$. Transwersalami częściowymi są też na przykład $\{1, 2, 3, 6\}$, $\{2, 3, 6\}$, $\{1, 5\}$, $\emptyset$

Warunek konieczny i dostateczny istnienia traswersali podaje następujące twierdzenie Halla.

Twierdzenie 9.1.1. *Niech E będzie niepustym zbiorem skończonym i niech $\mathcal{F} = (S_1, \ldots, S_m)$ będzie rodziną niepustych podzbiorów zbioru E. Rodzina $\mathcal{F}$ ma transwersalę wtedy i tylko wtedy, gdy suma dowolnych k podzbiorów S_i ma co najmniej k elementów, $1 \leqslant k \leqslant m$.*

Dowód. (Szkic). Konieczność warunku jest oczywista. Dla dowodu dostateczności wystarczy pokazać, że jeżeli pewien podzbiór ma więcej niż jeden element, to można usunąć z niego jeden element, nie naruszając przy tym warunku. Powtarzając tę procedurę, otrzymuje w końcu zbiory jednoelementowe. Dowodzi się tego nie wprost. □

Wniosek 9.1.1. *Jeśli E i $\mathcal{F}$ są takie jak w tw. 9.1.1, to rodzina $\mathcal{F}$ ma transwersalę częściową mającą t elementów wtedy i tylko wtedy, gdy suma dowolnych k podzbiorów ma co najmniej $k + t - m$ elementów.*

Twierdzenie 9.1.2. *Niech E będzie niepustym zbiorem skończonym i niech $\mathcal{F} = (S_1, \ldots, S_m)$ i $\mathcal{G} = (R_1, \ldots, R_m)$ będą dwiema rodzinami niepustych podzbiorów zbioru E. Wówczas rodziny $\mathcal{F}$ i $\mathcal{G}$ mają wspólną transwersalę wtedy i tylko wtedy, gdy dla dowolnych podzbiorów A i B zbioru $\{1, 2, \ldots, m\}$ zachodzi nierówność*

$$\left| \left(\bigcup_{i \in A} S_i \right) \cap \left(\bigcup_{j \in B} T_j \right) \right| \geqslant |A| + |B| - m.$$

9.2. Matroidy transwersalne

Twierdzenie 9.2.1. *Rodzina $\mathcal{I}$ wszystkich transwersali częściowych rodziny $\mathcal{F}$ podzbiorów zbioru E jest rodziną zbiorów niezależnych matroidu $M = (E, \mathcal{I})$.*

Matroid traswersalny

Dowód tego twierdzenia jest treścią zadania 2.

Matroid, w którym zbiorami niezależnymi są transwersale częściowe, nazywa się *matroidem transwersalnym*.

Przyjmijmy teraz, że w zbiorze E jest dodatkowo wprowadzona struktura matroidu. Czy istnieje transwersala rodziny $\mathcal{G}$ będąca zbiorem niezależnym matroidu? Odpowiedź na to pytanie daje twierdzenie Rado.

Twierdzenie 9.2.2. *Niech $M = (E, \mathcal{I})$ będzie matroidem i niech $\mathcal{F}$ będzie rodziną niepustych podzbiorów zbioru E. Wówczas rodzina $\mathcal{F}$ ma transwersalę $T \in \mathcal{I}$ wtedy i tylko wtedy, gdy dla każdego k takiego, że $1 \leqslant k \leqslant m$, suma dowolnych k podzbiorów S_i zawiera zbiór niezależny mający co najmniej k elementów.*

Uwaga. Jeśli M jest matroidem wolnym, to twierdzenie 9.2.2 sprowadza się do twierdzenia 9.1.1.

9.3. Zadania

1. Niech E będzie zbiorem liter w słowie *MATROIDS*. Wykazać, że rodzina

(*STAR*, *ROAD*, *MOAT*, *RIOT*, *RIDS*, *DAMS*, *MIST*)

podzbiorów zbioru E ma dokładnie osiem transwersal.

2. Niech T_1 i T_2 będą transwersalami rodziny $\mathcal{F}$. Niech $x \in T_1$. Wykazać, że istnieje $y \in T_2$ taki, że $T_1 \setminus \{x\} \cup \{y\}$ jest również transwersalą rodziny $\mathcal{F}$.

3. Wykaż prawdziwość twierdzenia Rado w przypadku, gdy M jest matroidem Fano oraz $\mathcal{F} = (\{1\}, \{1, 2\}, \{2, 4, 5\})$.

10. Niezmienniki Tutte'a–Gröthendiecka

10.1. Operacje na matroidach

Ograniczenie Niech $M = (E, \mathcal{C})$ będzie matroidem cykli oraz niech $A \subseteq E$. Ograniczeniem matroidu M do do zbioru $E \setminus A$ nazywa się nazywa się matroid $M \setminus A$, którego cyklami są tylko te cykle, które są zawarte w $M \setminus A$, czyli $M \setminus A = (E \setminus A, \mathcal{C}')$ gdzie

$$\mathcal{C}' = \{C \in \mathcal{C} : C =\subseteq A\}.$$

Redukcja Redukcją (ściągnięciem) matroidu M do do zbioru $E \setminus A$ nazywa się nazywa się matroid M/A, którego cyklami są zbiory minimalne zbioru

$$\mathcal{C}'' = \{C : C = C' \cap (E \setminus A), C' \in \mathcal{C} \ . \tag{10.1.1}$$

Suma prosta Sumą prostą matroidów $M_1 = (E_1, \mathcal{C}_1)$ i $M_2 = (E_2, \mathcal{C}_2)$ jest matroid

$$M_1 \oplus M_2 = (E_1 \cup E_2, \mathcal{C}_1 \cup \mathcal{C}_2).$$

Rodziną baz matroidu $M_1 \oplus M_2$, jest rodzina

$$\mathcal{B} = \{B : B = B_1 \cup B_2, B_1 \in \mathcal{B}_1, B_2 \in \mathcal{B}_2\},$$

gdzie $\mathcal{B}_i$ jest rodziną baz matroidu M_i.

Minor Matroid M' otrzymany matroidu M poprzez kolejne operacje ograniczenia lub ściągnięcia, nazywa się *minorem* matroidu M.

Przykład. Niech F_3 będzie matroidem Fano, tzn. którego bazami są wszystkie trzyelementowe podzbiory punktów nie będące prostymi płaszczysny Fano (patrz. rys. 4). Cyklami w F_3 są proste i ich dopełnienia. Niech $A = \{6, 7\}$. Wtedy cyklami w $F_3 \setminus A$ są $\{1, 2, 3\}$, $\{1, 4, 5\}$ i $\{2, 3, 4, 5\}$. Zgodnie ze wzorem (10.1.1), mamy

$$\mathcal{C}'' = \{1, 2, 3\}, \{1, 4, 5\}, \{2, 3, 4, 5\}, \{2, 4\}, \{3, 5\}, \{1\}, \},$$

a więc cyklami w F_3/A są $\{1\}, \{2, 4\}, \{3, 5\}$.

10.2. Wielomiany Tutte'a

Niezmiennikiem (izomorfizmu) nazywa się każdą funkcję f określoną na klasie matroidów $\mathcal{M} = \{M_i\}$ taką, że dla izomorficznych M' i M'', zachodzi równość:

$$f(M') = f(M''). \tag{10.2.1}$$

Funkcja tworząca rząd:

$$R(M; u, v) = \sum_{A \subseteq E} u^{\rho(E)-\rho(A)} v^{|A|-\rho(A)}. \tag{10.2.2}$$

Wtedy

$$T(M;x,y) = R(M;x-1,y-1). \tag{10.2.3}$$

Wzór (10.2.2) określa funkcję tworzącą rzędu, a wzór (10.2.3) wielomian Tutte, które dla matroidu M oznaczamy $R(M;u,v)$ i $T(M;x,y)$ odpowiednio.

Własność 0. *Dla matroidów M prawdziwy jest wzór*

$$T(M;x,y) = T(M^*;y,x), \tag{10.2.4}$$

Dowód. Ponieważ sumowanie we wzorze (10.2.2) jest po wszystkich podzbiorach $A \subseteq E$ to można podstawić $A \leftarrow A' = E \setminus A$, więc

$$R(M^*;u,v) = \sum_{A\subseteq E} u^{r^*(E)-r^*(A')} v^{|A'|-r^*(A')}.$$

Ponieważ $r^*(E) = |E| - \rho(E)$, to:

$$r^*(E) - r^*(A') = |E| - \rho(E) - |E| + \rho(E) + |A| - \rho(A) = |A| - \rho(A),$$

oraz

$$|A| - \rho(A') = \underbrace{|E \setminus A| - |E|}_{-|A|} + \rho(E) + |A| - \rho(A) = \rho(E) - \rho(A).$$

Stąd i ze wzoru (10.2.3) otrzymujemy (10.2.4). □

Przykład. Matroid 2-jednorodny na trzech elementach, tzn. składający się z jednego cyklu. Oznaczmy go przez C_3.

$$\begin{array}{lll} & & T(C_3;x,y) \\ |A|=0: & = & (x-1)^2 \\ |A|=1: & + & 3(x-1) \\ |A|=2: & + & 3 \\ |A|=3: & + & y-1 \\ & = & (x-1)^2 + 3(x-1) + 3 + y - 1 \\ & = & x^2 + x + y. \end{array}$$

Poniższe „twierdzenie – receptę" udowodnili Oxley i Welsh.

Twierdzenie 10.2.1. *Niech $\boldsymbol{C}$ będzie klasą matroidów zamkniętych ze względu na sumy proste $M_1 \oplus M_2$ oraz $M \setminus e$ i M/e dla $e \in E(M)$. Niech f będzie określone na $\boldsymbol{C}$ spełniając równania*

$$f(M) = af(M \setminus e) + bf(M/e), \tag{10.2.5}$$

$$f(M_1 \oplus M_2) = f(M_1)f(M_2). \tag{10.2.6}$$

Wtedy f jest dana wzorem

$$f(M) = a^{|E|-\rho(E)} b^{\rho(E)} T\left(M; \frac{x_0}{b}, \frac{y_o}{a}\right),$$

gdzie $x_0 = f(I)$ oraz $y_0 = f(L)$. □

Każdy niezmiennik f spełniający (10.2.5) – (10.2.6) nazywa się *niezmiennikiem Tutte-Gröthendiecka*, ((TG)-niezmiennikiem).

Niektóre z niezmienników Tutte'a–Gröthendiecka.

1. W punkcie $(1,1)$, T zlicza bazy M.
2. W punkcie $(2,1)$, T zlicza zbiory niezależne w M.

Szczególną rolę pełnią wartości wielomianów Tutte'a w niektórych punktach płaszczyzny, a szczególnie wzdłuż hiperboli

$$H_\alpha = \{(x,y) : (x-1)(y-1) = \alpha\}$$

Przykład. Ponieważ $T(C_3; x, y) = x^2 + x + y$, to liczba baz wynosi $T(C_3; 1, 1) = 1+1+1 = 3$, a liczba zbiorów niezależnych wynosi $T(C_3; 2, 1) = 4 + 2 + 1 = 7$. Matroidem dualnym do C_3 jest matroid C_3^*, którego bazami są zbiory jednoelementowe, cyklami – zbiory dwuelementowe. Ze wzoru (10.2.4) wynika, że $T(C_3^*; x, y) = y^2 + x + y$, a więc liczba baz wynosi $T(C_3^*; 1, 1) = 3$, a liczba zbiorów niezależnych wynosi $T(C_3^*; 2, 1) = 1 + 1 + 2 = 4$.

10.3. Zadania

1. Niech M będzie matroidem na zbiorze E oraz $A \subseteq B \subseteq E$. Pokazać, że

a) $(M \setminus A) \setminus B = M \setminus A$,

b) $(M/A)/B = M/A$.

2. Pokazać, że

$$(M/A)^* = (M^* \setminus A).$$

3. Wyznaczyć wielomian Tutte'a dla matroidów F_3 i $F_4 = F_3^*$. Na tej podstawie obliczyć liczbę baz w tych matroidach.

4. Skonstruować dowolną funkcję $f \in \boldsymbol{C}$ o której mowa w „twierdzeniu – recepcie" dla matroidu C_3.

5. Uogólnić wynik z zadania 4 na matroid $F_3 \setminus A$, gdzie A jest dowolnym dwuelementowym podzbiorem zbioru punktów płaszczyzny Fano.

11. Konfiguracje kombinatoryczne

11.1. Podstawowe własności

Konfiguracje

Niech X będzie zbiorem skończonym oraz niech $\mathcal{B} = \{B_1, \ldots, B_b\}$ będzie rodziną jego podzbiorów. Podzbiory B_i mogą się powtarzać. Elementy $x \in X$ nazywane są punktami, a zbiory B_i blokami. Konfiguracją nazywa się parę $(X, \mathcal{B})$ o parametrach v, k, λ, gdy spełnione są warunki:

(i) $|X| = v$,
(ii) $|B_i| = k$ dla $1 \leqslant i \leqslant b$,
(iii) każdy dwuelementowy zbiór $\{x, y\} \subseteq X$ jest podzbiorem dokładnie λ bloków należących do $\mathcal{B}$,
(iv) $\lambda > 0$ oraz $k < v - 1$.

Niech x będzie ustalonym punktem oraz niech r będzie liczbą bloków B_i dla których $x \in B_i$. Łatwo pokazać (zadanie), że

$$\lambda(v-1) = r(k-1). \tag{11.1.1}$$

Wynika stąd, że r jest wyznaczone przez parametry v, k, λ i nie zależy od wyboru punktu x. Stąd

Własność 0. *Każdy punkt konfiguracji należy do dokładnie r bloków, gdzie*

$$r = \frac{\lambda(v-1)}{k-1}. \tag{11.1.2}$$

Podobnie otrzymuje się (zadanie), że

$$vr = bk,$$

skąd

$$b = \frac{\lambda v(v-1)}{k(k-1)}. \tag{11.1.3}$$

Konfiguracja taka ma oznaczenie (v, b, r, k, λ)-BIBD, (ang. *balanced incomplete block design*).

Przykład. Niech $k = 3$, $v \geqslant 5$, $\lambda = 1$. Łatwo sprawdzić, że nie istnieje taka konfiguracja dla $v = 5$ i $v = 6$. Wystarczy bowiem sprawdzić, że nie są spełnione równości (11.1.2) i (11.1.3). Istnieje natomiast taka konfiguracja dla $v = 7$. Wystarczy bowiem za X przyjąć punkty płaszczyzny Fano (patrz rys. 4), a za bloki przyjąć proste z tej płaszczyzny.

Macierze incydencji

Konfiguracje można reprezentować za pomocą macierzy incydencji $A = [a_{ij}]$, gdzie

$$a_{ij} = \begin{cases} 1, & \text{gdy } x_i \in B_j, \\ 0, & \text{gdy } x_i \notin B_j. \end{cases}$$

Nierówność Fishera.

Twierdzenie 11.1.1. *Dla każdego (v, b, r, k, λ)-BIBD jest $b \geqslant v$.*

Dowód. Niech $X = \{x_1, \ldots, x_v\}$, $\mathcal{B} = \{B_1, \ldots, B_b\}$, M – macierz incydencji oraz niech s_j będzie j-tym wierszem w M^T. Wektory s_j rozpinają podprzestrzeń $\boldsymbol{S} \subseteq \boldsymbol{R}^v$. Wystarczy dowieść, że $\boldsymbol{S} = \boldsymbol{R}^v$. W tym celu pokażemy, że $e_i \in \boldsymbol{S}$, gdzie $e_i = (0, \ldots, 1, 0, \ldots, 0)$ (1 na i-tej pozycji).

Ponieważ

$$\sum_{j=1}^{b} s_j = (r, \ldots, r)\,,$$

to

$$\frac{1}{r}\sum_{j=1}^{b} s_j = (1, \ldots, 1)\,, \tag{11.1.4}$$

Dalej, ustalamy i, $1 \leqslant i \leqslant v$. Wtedy

$$\sum_{j:x_i \in B_j} s_j = (r-\lambda)\, e_i + (\lambda, \ldots, \lambda)\,. \tag{11.1.5}$$

Porównując (11.1.4) i (11.1.5) otrzymujemy

$$e_i = \sum_{j:x_i \in B_j} \frac{1}{r-\lambda} s_j - \sum_{j=1}^{b} \frac{\lambda}{r\,(r-\lambda)}\, s_j\,. \tag{11.1.6}$$

Wzór (11.1.6) daje e_i jako liniową kombinację wektorów $s_1, \ldots, s_b$. □

Przykład. Nie istnieje konfiguracja dla $v = 16$, $k = 6$, $\lambda = 1$, bo ze wzoru (11.1.3) wyliczamy

$$b = \frac{1 \cdot 16 \cdot 15}{6 \cdot 5} = 8 < 16 = v.$$

11.2. Konfiguracje kwadratowe

Konfiguracje kwadratowe to takie, w których liczba punktów jest równa liczbie bloków. Równanie (11.1.1) ma wtedy postać

$$\lambda(v-1) = k(k-1).$$

Konfiguracje kwadratowe są symetryczne, tzn. że nie tylko każdy punkt należy do λ bloków, ale również każde dwa bloki mają λ wspólnych punktów:

Twierdzenie 11.2.1. *Jeśli $(X, \mathcal{B})$, gdzie $\mathcal{B} = (B_1, \ldots, B_v)$ jest konfiguracją kwadratową o parametrach v, k, λ, to $|B_i \cap B_j| = \lambda$ dla dowolnych $i \neq j$.*

Stąd

Wniosek 11.2.1. *Jeśli A jest macierzą incydencji kwadratowej, to A^T jest macierzą incydencji pewnej konfiguracji kwadratowej o tych samych parametrach.*

Własność 0. *Para $(X, \mathcal{B})$ jest skończoną płaszczyzną rzutową wtedy i tylko wtedy, gdy jest konfiguracją kwadratową z $\lambda = 1$.*

Twierdzenie 11.2.2. (Bruck, Ryser, Chowla). *Jeśli istnieje konfiguracja kwadratowa o parametrach v, k, λ oraz $n = k - \lambda$, to*

(i) *jeśli v jest parzyste, to n jest kwadratem liczby całkowitej,*
(ii) *Jeśli v jest nieparzyste, to istnieją liczby całkowite x, y, z, nie wszystkie równe zeru, spełniające równanie*

$$z^2 = nx^2 + (-1)^{(v-1)/2}\lambda y^2. \tag{11.2.1}$$

Wniosek 11.2.2. *Nie istnieje płaszczyzna rzutowa rzędu 6.*

Twierdzenie 11.2.3. (Singer). *Geometria rzutowa $PG(n-1, q)$ określa konfigurację kwadratową o parametrach*

$$v = \frac{q^n - 1}{q - 1}, \quad k = \frac{q^{n-1} - 1}{q - 1}, \quad \lambda = \frac{q^{n-2} - 1}{q - 1},$$

gdzie punktami konfiguracji są punkty geometrii rzutowej, a blokami konfiguracji są podprzestrzenie rzędu $n - 1$ geometrii rzutowej.

11.3. Macierze Hadamarda

Macierz H wymiaru $n \times n$ o elementach $+1$ i -1 nazywa się macierzą Hadamarda rzędu n, jeśli

$$HH^T = nI, \tag{11.3.1}$$

gdzie I jest macierzą jednostkową.

Własność 0. *Dowolne dwa wiersze macierzy Hadamarda są ortogonalne.*

Wniosek 11.3.1. *H jest macierzą Hadamarda wtedy i tylko wtedy, gdy H^T jest macierzą Hadamarda.*

Łatwo zauważyć, że permutacja wierszy lub kolumn, a także ich mnożenie przez -1 nie narusza ortogonalności i prowadzi do macierzy Hadamarda.

Przykład.

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

jest macierzą Hadamarda rzędu 2.

Twierdzenie 11.3.1. *Macierz Hadamarda rzędu $4t$ istnieje wtedy i tylko wtedy, gdy istnieje konfiguracja kwadratowa o parametrach $v = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$.*

Konstrukcja. Normalizujemy macierz Hadamarda, tzn. permutujemy wiersze i kolumny i mnożymy przez -1 tak, aby w pierwszy wierszu i w pierwszej kolumnie były same $+1$. Usuwamy z takiej macierzy Hadamarda pierwszy wiersz

i pierwszą kolumnę i zamieniamy -1 na 0. Jest macierz incydencji konfiguracji kwadratowej. Konstrukcja ta jest odwracalna.

Twierdzenie 11.3.2. *Jeżeli istnieje macierz Hadamarda rzędu n, to $n = 1$, $n = 2$ lub $n \equiv 0 \mod 4$.*

Hipoteza. Macierz Hadamarda istnieje wtedy i tylko wtedy, gdy $n \equiv 0 \mod 4$ dla $n \geqslant 4$.

Iloczynem Kroneckera macierzy $A = a_{ij}$ wymiaru $n \times m$ i B wymiaru $r \times s$ nazywa się macierz wymiaru $nr \times ms$:

$$A \oplus B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ a_{21}B & a_{22}B & \dots & a_{2m}B \\ \vdots & \vdots & & \vdots \\ a_{n1}B & a_{n2}B & \dots & a_{nm}B \end{bmatrix}$$

Twierdzenie 11.3.3. *Jeśli H_1 i H_2 są macierzami Hadamarda rzędów n_1 i n_2, to $H = H_1 \otimes H_2$ jest macierzą Hadamarda rzędu $n = n_1 n_2$.*

11.4. Zadania

1. Zbudować konfiguracje o parametrach:
(a) $v = b = 7$, $k = r = 3$, $\lambda = 1$,
(b) $v = b = 13$, $k = r = 4$, $\lambda = 1$,
(c) $v = 9$, $b = 12$, $r = 4$, $k = 3$, $\lambda = 1$,
(d) $v = 6$, $b = 10$, $r = 5$, $k = 3$, $\lambda = 2$.

2. Czy istnieją konfiguracje o parametrach:
(a) $v = 15$, $b = 21$, $r = 7$, $k = 4$, $\lambda = 2$, (b) $v = b = 23$, $r = k = 7$, $\lambda = 2$, (c) $v = b = 43$, $r = k = 7$, $\lambda = 1$, (d) $v = 36$, $b = 42$, $r = 7$, $k = 6$, $\lambda = 1$.

3. Sprawdzić, czy spełniony jest warunek konieczny istnienia symetrycznych ($b = v$, $r = k$) konfiguracji:
(a) $v = 21$, $k = 5$, $\lambda = 1$,
(b) $v = 15$, $k = 7$, $\lambda = 3$,
(c) $v = 19$, $k = 9$, $\lambda = 4$,
(d) $v = 29$, $k = 8$, $\lambda = 2$.

4. Pokazać, że dla konfiguracji o parametrach v, k, λ zachodzi równość $\lambda(v - 1) = r(k - 1)$.

5. Pokazać, że dla konfiguracji o parametrach v, k, λ zachodzi równość $vr = bk$.

6. Jaką konfigurację tworzą dopełnienia prostych na płaszczyźnie Fano?

7. Niech $\lambda = 2$. Dla $k = 6$ i $k = 7$ znaleźć najmniejsze $v \geqslant 10$, dla którego z twierdzenia Brucka, Rysera i Chowli wynika nieistnienie konfiguracji kwadratowej rzędu v.

8. Niech

$$A = \begin{bmatrix} 1 & 1 \\ 1 & \text{-1} \end{bmatrix}.$$

Napisać macierze Hadamarda $B = A \otimes A$ oraz $C = A \otimes B$. Czy macierz C jest identyczna z macierzą Hadamarda D otrzymaną z macierzy incydencji konfiguracji o parametrach $v = 7$, $k = 3$ oraz $\lambda = 1$ po ewentualnych permutacjach wierszy lub kolumn?

12. Trójki Steinera

12.1. Quasigrupy i kwadraty łacińskie

System trójek Steinera oznaczany przez $\mathrm{STS}(v)$, to $(v,3,1)$-BIBD. Inaczej mówiąc, $\mathrm{STS}(v)$ to rodzina trójek takich, że każda para należy do dokładnie jednej trójki.

Przykład. Płaszczyzna Fano, to $\mathrm{STS}(7)$, gdzie blokami (trójkami) są proste na płaszczyźnie.

Płaszczynę $AG(2,3)$ na 9 elementach, można skonstruować następująco:

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}.$$

Prostymi (blokami) są wszystkie wiersze i kolumny macierzy A oraz takie trójki, że żadne ich dwa elementy nie leżą w jednym wierszu lub kolumnie macierzy A. Proste na płaszczyźnie $AG(2,3)$ to trójki Steinera w $\mathrm{STS}(9)$.

Warunek konieczny

Lemat 12.1.1. *Jeśli istnieje* $\mathrm{STS}(v)$, *to* $v \equiv 1 \vee 3 \mod 6$, $v \geqslant 7$.

Niech X będzie zbiorem skończonym, a $\circ$ będzie działaniem takim, że

(i) dla każdych $x, y \in X$, równanie $x \circ z = y$ ma dokładnie jedno rozwiązanie,
(ii) dla każdych $x, y \in X$, równanie $z \circ x = y$ ma dokładnie jedno rozwiązanie.

Quasigrupa

Parę $(X, \circ)$ nazywa się quasigrupą. Jeśli $x \circ x = x$, to quasigrupa jest *idempotentna*, a jeśli $x \circ y = y \circ x$, to jest *symetryczna*.

Niech X będzie zbiorem skończonym, $|X| = n$ oraz miech A będzie macierzą $n \times n$ o elementach $a_{x,y}$ taką, że każda kolumna i każdy wiersz jest permutacją zbioru X. Taką macierz nazywa się *kwadratem łacińskim*.

Kwadrat łaciński

Twierdzenie 12.1.1. *Niech X będzie zbiorem skończonym, $|X| = n$, $x, y \in X$. Jeżeli $A = [a_{x,y}]_{n \times n}$ jest kwadratem łacińskim oraz $x \circ y = a_{x,y}$, to $(X, \circ)$ jest quasigrupą.*

Przykład. Niech $X = \{1, 2\}$. Istnieją dokładnie dwa kwadraty łacińskie

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

Oba są symetryczne, ale żaden nie jest idempotentny.

Przykład. Niech $X = \{1, 2, 3\}$. Istnieje 12 kwadratów łacińskich, w tym cztery symetryczne, a tylko jeden idempotentny:

$$\begin{bmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{bmatrix}$$

Lemat 12.1.2. *Idempotentna quasigrupa o n elementach istnieje wtedy i tylko wtedy, gdy n jest nieparzyste.*

12.2. Konstrukcje Bosego i Skolema

Konstrukcja Bose daje trójki Steinera w przypadku $v \equiv 3 \mod 6$. Zmodyfikowana konstrukcja Skolema daje trójki Steinera w przypadku $v \equiv 1 \mod 6$.

Konstrukcja Bosego

Załóżmy, że relacja $\prec$ porządkuje liniowo zbiór X oraz załóżmy, że $(X, \circ)$ jest symetryczną idempotentną quasigrupą, $|X| = 2t+1$, $t \geqslant 1$. Niech $Y = X \times Z_3$, gdzie Z_3 jest pierścieniem, z dodawaniem $\mod 3$. Dla każdego $x \in X$ określamy blok

$$\Lambda_x = \{(x,0),(x,1),(x,2)\}. \tag{12.2.1}$$

Następnie, dla każdej pary $x, y \in X$, $\prec$ i każdego $i \in Z_3$ określamy blok

$$B_{x,y,i} = \{(x,i),(y,i),(x \circ y,(i+1) \mod 3)\}. \tag{12.2.2}$$

Niech

$$\mathcal{B} = \{\Lambda_x : x \in X\} \cup \{B_{x,y,i} : x, y \in X, x \prec y, i \in Z_3\}. \tag{12.2.3}$$

Twierdzenie 12.2.1. *Rodzina $\mathcal{B}$ zdefiniowana wzorami* (12.2.1), (12.2.2) *i* (12.2.3), *tworzy* STS(v) *dla* $v \equiv 3 \mod 6$.

Niech $X = Z_n$ gdzie n jest parzyste. Określamy permutację π zbioru X wzorem

$$\pi(i) = \begin{cases} \frac{x}{2} & \text{gdy } x \text{ jest parzyste,} \\ \frac{x+n-1}{2} & \text{gdy } x \text{ jest nieparzyste.} \end{cases}$$

Działanie quasigrupowe określamy wzorem

$$x \circ y = \pi((x+y) \mod n).$$

Konstrukcja Skolema

Niech $v = 6t+1$, $t \geqslant 1$ oraz niech $Y = (Z_{2t} \times Z_3) \cup \{\infty\}$. Dla $0 \leqslant x \leqslant t-1$ określamy blok

$$\Lambda_x = \{(x,0),(x,1),(x,2)\}. \tag{12.2.4}$$

Następnie, dla każdej pary $x, y \in Z_{2t}$ i każdego $i \in Z_3$ określamy blok

$$B_{x,y,i} = \{(x,i),(y,i),(x \circ y,(i+1) \mod 3)\}. \tag{12.2.5}$$

W końcu, dla $0 \leqslant x \leqslant t-1$ i każdego $i \in Z_3$ określamy blok

$$C_{x,i} = \{\infty,(x+t,i),(x,(i+1) \mod 3)\}. \tag{12.2.6}$$

Niech

$$\begin{aligned} \mathcal{B} = \{\Lambda_x : 0 \leqslant x \leqslant t-1\} &\cup \{B_{x,y,i} : x, y \in Z_{2t}, x < y, i \in Z_3\} \\ &\cup \{C_{x,i} : 0 \leqslant x \leqslant t-1, i \in Z_3\}. \end{aligned} \tag{12.2.7}$$

Twierdzenie 12.2.2. *Rodzina $\mathcal{B}$ zdefiniowana wzorami* (12.2.4) – (12.2.7), *tworzy* STS(v) *dla* $v \equiv 1 \mod 6$.

Z lematu 12.1.1 oraz twierdzeń 12.2.1 i 12.2.2 wynika

Twierdzenie 12.2.3. *$STS(v)$ istnieje wtedy i tylko wtedy, gdy* $v \equiv 1 \vee 3 \mod 6$, $v \geqslant 7$.

12.3. Zadania

1. Korzystając z konstrukcji Bosego, zbudować $STS(9)$

2. Korzystając z konstrukcji Skolema, zbudować $STS(13)$

3. Podać algorytm i napisać program budujący $STS(n)$ wg konstrukcji Bosego i Skolema.

Literatura

[1] T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein, *Wprowadzenie do algorytmów*, WNT 2004.

[2] J. Flachsmeyer, *Kombinatoryka*, PWN 1977.

[3] R. L. Graham, D. E. Knuth, O. Patashnik, *Matematyka konkretna*, PWN 1996.

[4] W. Lipski, *Kombinatoryka dla programistów*, WNT 2004.

[5] W. Lipski, W. Marek, *Analiza kombinatoryczna*, PWN 1986.

[6] Z. Palka, A. Ruciński, *Niekonstruktywne metody matematyki dyskretnej*, WNT 1996.

[7] Z. Palka, A. Ruciński, *Wykłady z kombinatoryki*, część 1, WNT 1998.

[8] E. M. Reingold, J. Nievergelt, N. Deo, *Algorytmy kombinatoryczne*, PWN 1985.

[9] K. A. Ross, C. R. B. Wright, *Matematyka dyskretna*, PWN 1996.

[10] K. A. Rybnikow (red.) *Analiza kombinatoryczna w zadaniach*, PWN 1988.

[11] R. J. Wilson, *Wprowadzenie do teorii grafów*, PWN 1998.

[12] M. Zakrzewski, T. Żak, *Kombinatoryka, prawdopodobieństwo i zdrowy rozsądek*, Quadrivium 1998.