

MATEMATYKA DYSKRETNA

dr hab. Mariusz Mészka

Akademia Górniczo-Hutnicza w Krakowie

<http://home.agh.edu.pl/~meszka>

Program wykładu

1. Zbiory, podzbiory i multizbiory. Generowanie podzbiorów.
2. Funkcje i rozmieszczenia. Permutacje. Metody generowania permutacji.
3. Zasada pudełkowania i przykłady jej zastosowań.
4. Zasada włączania-wyłączania. Nieporządki.
5. Podziały zbioru i liczby. Liczby Stirlinga.
6. Zależności rekurencyjne. Rozwiązywanie liniowych równań rekurencyjnych o stałych współczynnikach.
7. Funkcje tworzące; przykłady wykorzystania.
8. Zliczanie obiektów kombinatorycznych.

Program wykładu (cd.)

9. Pojęcia wstępne teorii grafów. Izomorfizm grafów. Spójność.
10. Droga Eulera. Cykle i ścieżki Hamiltona.
11. Grafy dwudzielne. Drzewa. Grafy planarne.
12. Kolorowanie wierzchołków i krawędzi w grafach. Zawężenie zagadnień kolorowania do poznanych rodzin grafów.
13. Przykłady dekompozycji grafów.

Literatura

- [1] W. Lipski, Kombinatoryka dla programistów, WNT 2007.
- [2] J. Jaworski, Z. Palka, J. Szymański, Matematyka dyskretna dla informatyków, WN UAM, 2011.
- [3] R.A. Brualdi, Introductory combinatorics 5th Edition, Prentice Hall 2010.
- [4] R.P. Grimaldi, Discrete and Combinatorial Mathematics 5th Edition, Pearson 2004.

Lemat

Liczba wszystkich podzbiorów zbioru n -elementowego wynosi 2^n .

Lemat

Liczba wszystkich podzbiorów k -elementowych zbioru n -elementowego wynosi $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Lemat

Prawdziwe są następujące zależności:

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

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

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

$$k \binom{n}{k} = n \binom{n-1}{k-1}$$

$$\binom{m+n}{k} = \sum_{i=0}^k \binom{m}{i} \binom{n}{k-i}$$

$$\sum_{i=0}^k \binom{k}{i}^2 \binom{n+2k-i}{2k} = \binom{n+k}{k}^2$$

Twierdzenie dwumienne

Niech $x, y \in \mathbb{R}$, $n \in \mathbb{N}$. Wówczas

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

W szczególności, dla $x = y = 1$,

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

Lemat

Liczba k -elementowych podzbiorów z powtórzeniami zbioru S , który zawiera n różnych elementów, każdy o nieograniczonej krotności, wynosi $\binom{n+k-1}{k}$.

Twierdzenie wielomienne

Niech $x_1, x_2, \dots, x_t \in \mathbb{R}$, $n \in \mathbb{N}$. Wówczas

$$(x_1 + x_2 + \dots + x_t)^n = \sum \binom{n}{n_1; n_2; \dots; n_t} x_1^{n_1} x_2^{n_2} \dots x_t^{n_t},$$

gdzie sumowanie przeprowadzone jest po wszystkich nieujemnych całkowitoliczbowych rozwiązaniach równania

$$n_1 + n_2 + \dots + n_t = n,$$

oraz

$$\binom{n}{n_1; n_2; \dots; n_t} = \frac{n!}{n_1! n_2! \dots n_t!}.$$

Generowanie wszystkich podzbiorów zbioru n -elementowego

```
generuj_podzbiory( $n, p$ )  
  if  $p == n$  then  
    for  $i := 0$  to  $n - 1$  do  
      if (ciag[ $i$ ] == 1) then  
        wypisz( $i$ )  
  else  
    ciag[ $p$ ] := 0  
    generuj_podzbiory( $n, p + 1$ )  
    ciag[ $p$ ] := 1  
    generuj_podzbiory( $n, p + 1$ )
```

Start rekurencji od wywołania:

```
generuj_podzbiory( $n, 0$ )
```

Generowanie podzbiorów k -elementowych zbioru n -elementowego

```
for  $i := 0$  to  $k - 1$  do
  zbior[ $i$ ] :=  $i + 1$ 
do
  wypisz_zbior()
  if (zbior[ $k - 1$ ] <  $n$ ) then
     $j := k - 1$ 
  else
     $j := k - 2$ 
    while ( $j \geq 0$  && zbior[ $j$ ] + 1 == zbior[ $j + 1$ ]) do
       $j --$ 
    if ( $j \geq 0$ ) then
      zbior[ $j$ ] ++
      for  $i := j + 1$  to  $k - 1$  do
        zbior[ $i$ ] := zbior[ $i - 1$ ] + 1
  while ( $j \geq 0$ )
```

Generowanie podzbiorów k -elementowych z powtórzeniami

```
for  $i := 0$  to  $k - 1$  do
  zbior[ $i$ ] :=  $i + 1$ 
do
  wypisz_zbior()
  if (zbior[ $k - 1$ ] <  $n$ ) then
     $j := k - 1$ 
  else
     $j := k - 2$ 
    while ( $j \geq 0$  && zbior[ $j$ ]  $+ 1$  == zbior[ $j + 1$ ]) do
       $j --$ 
    if ( $j \geq 0$ ) then
      zbior[ $j$ ] ++
      for  $i := j + 1$  to  $k - 1$  do
        zbior[ $i$ ] := zbior[ $i - 1$ ]  $+ 1$ 
  while ( $j \geq 0$ )
```

Lemat

Jeśli $|X| = n$ oraz $|Y| = m$, to liczba wszystkich funkcji $f : X \mapsto Y$ wynosi m^n .

Lemat

Jeśli $|X| = n$ oraz $|Y| = m$, $m \geq n$, to liczba wszystkich funkcji różnowartościowych $f : X \mapsto Y$ wynosi $\frac{m!}{(m-n)!}$.

Lemat

Jeśli $|X| = n$ oraz $|Y| = m$, $m \geq n$, to liczba wszystkich funkcji rosnących $f : X \mapsto Y$ wynosi $\binom{m}{n}$.

Lemat

Jeśli $|X| = n$ oraz $|Y| = m$, to liczba wszystkich funkcji niemalejących $f : X \mapsto Y$ wynosi $\binom{m+n-1}{n}$.

Wniosek

Jeśli $|X| = |Y| = n$, to każda funkcja różnowartościowa $f : X \mapsto Y$ jest wzajemnie jednoznaczna (bijektywna). Wówczas liczba takich funkcji jest równa $n!$.

Definicja

Odwzorowanie bijektywne $f : X \mapsto X$ nazywamy *permutacją* zbioru X .

Wniosek

Liczba wszystkich permutacji zbioru n -elementowego wynosi $n!$.

Zbiór wszystkich permutacji zbioru n -elementowego oznaczamy symbolem S_n .

Permutację $f : X \mapsto X$ zapisujemy

$$f = \begin{pmatrix} x_1, & x_2, & \dots & x_n \\ f(x_1), & f(x_2), & \dots & f(x_n) \end{pmatrix}$$

Bez straty ogólności możemy założyć, że $X = \{1, 2, \dots, n\}$.

Wówczas

$$f = \langle f(1), f(2), \dots, f(n) \rangle .$$

Definicja

Niech $f, g \in S_n$. Złożeniem permutacji f i g nazywamy permutację $g \circ f$ zdefiniowaną następująco

$$\forall i \in X : (g \circ f)(i) = g(f(i)).$$

Definicja

Permutację $e = \langle 1, 2, \dots, n \rangle$ nazywamy *identycznościową*.

Wniosek

Dla dowolnej permutacji $f \in S_n$ zachodzi $f \circ e = e \circ f = f$.

Definicja

Każda permutacja $f \in S_n$ wyznacza jednoznacznie taką permutację $f^{-1} \in S_n$, że $f \circ f^{-1} = f^{-1} \circ f = e$. f^{-1} nazywamy permutacją *odwrotną* do f .

Lemat

Dla dowolnych permutacji $f, g, h \in S_n$ spełnione są warunki:

$$(1) (f \circ g) \circ h = f \circ (g \circ h)$$

$$(2) f \circ e = e \circ f = f$$

$$(3) f \circ f^{-1} = f^{-1} \circ f = e.$$

Stąd wynika, że (S_n, \circ) jest grupą, nazywaną *grupą symetryczną* stopnia n .

Definicja

Cyklem długości k nazywamy permutację $f_k = (x_1^k x_2^k \dots x_k^k)$, w której $f_k(x_1^k) = x_2^k$, $f_k(x_2^k) = x_3^k$, $f_k(x_{k-1}^k) = x_k^k$, $f_k(x_k^k) = x_1^k$, oraz $f_k(x) = x$ dla każdego $x \in X \setminus \{x_1^k, x_2^k, \dots, x_k^k\}$.

Lemat

Każdą permutację można przedstawić jednoznacznie w postaci złożenia (niezależnych) cykli. Przedstawienie takie nazywamy *rozkładem na cykle*.

Definicja

Mówimy, że permutacja f jest *typu* $(\lambda_1, \lambda_2, \dots, \lambda_n)$ jeśli w rozkładzie na cykle zawiera dokładnie λ_i cykli długości i , dla $i = 1, 2, \dots, n$.

Do zapisu typu stosujemy zwykle notację $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ (pomijając i^{λ_i} jeśli $\lambda_i = 0$).

Lemat

Niech $X = \{x_1, x_2, \dots, x_t\}$ będzie multizbiorem o mocy n , który zawiera t parami różnych elementów; każdy element x_i ma krotność n_i , $i = 1, 2, \dots, t$. Wtedy $\sum_{i=1}^t n_i = n$.

Liczba wszystkich permutacji multizbioru X wynosi

$$\frac{n!}{n_1! n_2! \dots n_t!}.$$

Generowanie permutacji zbioru n -elementowego

```
for  $i := 0$  to  $n - 1$  do
  perm[ $i$ ] :=  $i + 1$ 
do
  wypisz_permutacje()
   $i := n - 2$ 
  while ( $i \geq 0$  && perm[ $i$ ] > perm[ $i + 1$ ]) do
     $i --$ 
  if ( $i \geq 0$ ) then
     $j := n - 1$ 
    while perm[ $j$ ] < perm[ $i$ ] do
       $j --$ 
    perm[ $i$ ] := perm[ $j$ ]
     $k := i + 1$ 
     $l := n - 1$ 
    while  $l > k$  do
      perm[ $k$ ] := perm[ $l$ ]
       $k ++$ 
       $l --$ 
  while ( $i \geq 0$ )
```

Zasada pudełkowania (Dirichleta)

Jeśli $n + 1$ obiektów zostanie rozmieszczonych w n pudełkach, to wśród tych pudełek znajdzie się takie, które zawiera co najmniej 2 obiekty.

Uogólniona zasada pudełkowania

Niech q_1, q_2, \dots, q_n będą liczbami naturalnymi. Jeśli $q_1 + q_2 + \dots + q_n + 1$ obiektów zostanie rozmieszczonych w n pudełkach, to znajdzie się pudełko o takim indeksie i , że zawiera ono $q_i + 1$ obiektów.

Niech X będzie danym zbiorem n -elementowym.

Niech P_1, P_2, \dots, P_t oznaczają pewne własności elementów z X .

Niech $A_i = \{x : x \in X \text{ oraz } x \text{ ma własność } P_i\}$, $1 \leq i \leq t$.

Twierdzenie

Liczba elementów zbioru X posiadających co najmniej jedną z własności P_1, P_2, \dots, P_t wynosi:

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_t| &= \sum_{1 \leq i \leq t} |A_i| - \sum_{1 \leq i < j \leq t} |A_i \cap A_j| + \\ &+ \sum_{1 \leq i < j < k \leq t} |A_i \cap A_j \cap A_k| - \dots + (-1)^{t+1} |A_1 \cap A_2 \cap \dots \cap A_t|. \end{aligned}$$

Wniosek

Liczba elementów zbioru X nieposiadających żadnej z własności P_1, P_2, \dots, P_t wynosi:

$$\begin{aligned} |\overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_t}| &= |X| - |A_1 \cup A_2 \cup \dots \cup A_t| = \\ |X| - \sum_{1 \leq i \leq t} |A_i| + \sum_{1 \leq i < j \leq t} |A_i \cap A_j| - \sum_{1 \leq i < j < k \leq t} |A_i \cap A_j \cap A_k| + \\ &+ \dots + (-1)^t |A_1 \cap A_2 \cap \dots \cap A_t|. \end{aligned}$$

Definicja

Permutację f nazywamy *nieporządkiem* jeśli, dla każdego $1 \leq i \leq n$, $f(i) \neq i$.

Twierdzenie

Niech D_n oznacza liczbę nieporządków zbioru n -elementowego X .
Wówczas

$$D_n = \sum_{i=0}^n (-1)^i \binom{n}{i} (n-i)!$$

Lemat

$$\lim_{n \rightarrow \infty} \frac{D_n}{n!} = e^{-1} \approx 0,368.$$

Lemat

Jeśli $|X| = n$ oraz $|Y| = m$, $n \geq m$, to liczba wszystkich odwzorowań suriektywnych $f : X \mapsto Y$ wynosi:

$$m^n - \binom{m}{1}(m-1)^n + \binom{m}{2}(m-2)^n - \binom{m}{3}(m-3)^n + \dots \\ + (-1)^{m-1} \binom{m}{m-1} 1^n.$$

Definicja

Przez *podział* n -elementowego zbioru X na k bloków rozumiemy taką rodzinę $\mathcal{B} = \{B_1, B_2, \dots, B_k\}$ podzbiorów zbioru X , że $B_i \neq \emptyset$, $B_i \cap B_j = \emptyset$ oraz $B_1 \cup B_2 \cup \dots \cup B_k = X$, dla każdego $i, j \in \{1, 2, \dots, k\}$.

Definicja

Liczbę podziałów zbioru n -elementowego na k bloków nazywamy *liczbą Stirlinga drugiego rodzaju* i oznaczamy $S(n, k)$.

Lemat

Dla liczb Stirlinga drugiego rodzaju zachodzi zależność

$$S(n, k) = S(n-1, k-1) + k \cdot S(n-1, k) \quad \text{dla } 0 < k < n$$

$$S(n, n) = 1 \quad \text{dla } n \geq 0$$

$$S(n, 0) = 0 \quad \text{dla } n > 0$$

Definicja

Liczbę podziałów zbioru n -elementowego nazywamy *liczbą Bella* i oznaczamy symbolem $B(n)$.

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

Lemat

$$B(n+1) = \sum_{i=0}^n \binom{n}{i} B(i)$$

Generowanie wszystkich podziałów zbioru

```
generuj_bloki( $p, l$ )  
  if  $p == n$  then  
    wypisz_blok()  
    return  
  for  $i := 1$  to  $l + 1$  do  
    blok[ $p$ ] :=  $i$   
    if  $i < l + 1$  then  
      generuj_bloki( $p + 1, l$ )  
    else  
      generuj_bloki( $p + 1, l + 1$ )
```

Start rekurencji od wywołania:

```
generuj_bloki(0, 0)
```

Generowanie podziałów zbioru na k bloków

```
generuj_bloki( $p, l$ )
  if  $p == n$  then
    wypisz_blok()
    return
  for  $i := 1$  to  $l + 1$  do
    blok[ $p$ ] :=  $i$ 
    if  $i < l + 1$  then
      generuj_bloki( $p + 1, l$ )
    else
      generuj_bloki( $p + 1, l + 1$ )           if  $l + 1 \leq k$ 
then
      generuj_bloki( $p + 1, l + 1$ )         if
 $n - 1 - p \geq k - l$  then
      generuj_bloki( $p + 1, l$ )
else
  if  $l + 1 \leq k$  then
    generuj_bloki( $p + 1, l + 1$ )
```

Definicja

Podziałem liczby n na k składników nazywamy taki ciąg liczb naturalnych $\langle b_1, b_2, \dots, b_k \rangle$, że $b_1 \geq b_2 \geq \dots \geq b_k > 0$ oraz $b_1 + b_2 + \dots + b_k = n$.

Niech $P(n, k)$ oznacza liczbę podziałów liczby n na k składników, natomiast $P(n)$ liczbę wszystkich podziałów.

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

$$P(0, 0) = P(0) = 1$$

Lemat

Liczba podziałów liczby n na k składników jest równa liczbie tych podziałów liczby n , w których największy składnik ma wartość k .

$$P(n, k) = 0 \quad \text{dla} \quad n < k$$

$$P(n, n) = 1 \quad \text{dla} \quad n \geq 0$$

$$P(n, 0) = 0 \quad \text{dla} \quad n > 0$$

Lemat

Dla $n \geq k \geq 0$ zachodzi zależność

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

Generowanie podziałów liczby n

```
podział[0] := n
k := 1
wypisz_podział(k)
while podział[0] > 1 do
    p := k - 1
    while podział[p] == 1 do
        p --
    podział[p] --
    s := k - p
    while s > 0 do
        if s >= podział[p] then
            podział[p + 1] := podział[p]
        else
            podział[p + 1] := s
        s := s - podział[p + 1]
        p ++
    k := p + 1
wypisz_podział(k)
```

Definicja

Liczbę Stirlinga pierwszego rodzaju oznaczamy symbolem $s(n, k)$ i definiujemy jako liczbę tych permutacji zbioru n -elementowego, które w rozkładzie na cykle posiadają k cykli.

Lemat

Dla liczb Stirlinga pierwszego rodzaju zachodzi zależność

$$s(n, k) = s(n - 1, k - 1) + (n - 1) \cdot s(n - 1, k) \quad \text{dla } 0 < k < n$$

$$s(n, n) = 1 \quad \text{dla } n \geq 0$$

$$s(n, 0) = 0 \quad \text{dla } n > 0$$

Definicja

Niech $h_0, h_1, \dots, h_n, \dots$ będzie nieskończonym ciągiem liczb. Mówimy, że spełnia on *liniowe równanie rekurencyjne stopnia k* jeśli istnieją współczynniki a_1, a_2, \dots, a_k, b ($a_k \neq 0$):

$$h_n = a_1 h_{n-1} + a_2 h_{n-2} + \dots + a_k h_{n-k} + b, \quad (n \geq k),$$

gdzie każdy ze współczynników a_1, a_2, \dots, a_k, b może zależeć od n .

Ciąg liczb $h_0, h_1, \dots, h_n, \dots$ spełniających powyższe równanie jest jednoznacznie wyznaczony przez liczby h_0, h_1, \dots, h_{k-1} nazywane *wartościami początkowymi*.

Liniowe równanie rekurencyjne jest *homogeniczne*, jeśli $b = 0$.

Liniowe równanie rekurencyjne ma *stałe współczynniki*, jeśli każdy ze współczynników a_1, a_2, \dots, a_k jest stałą.

Twierdzenie

Niech q będzie niezerową stałą.

Wówczas $h_n = q^n$ jest rozwiązaniem homogenicznego równania rekurencyjnego liniowego o stałych współczynnikach:

$$h_n - a_1 h_{n-1} - a_2 h_{n-2} - \dots - a_k h_{n-k} = 0, \quad (a_k \neq 0, n \geq k),$$

wtedy i tylko wtedy, gdy q jest pierwiastkiem wielomianu:

$$x^k - a_1 x^{k-1} - a_2 x^{k-2} \dots - a_k = 0.$$

Wielomian ten nazywany jest *wielomianem charakterystycznym*, a wszystkie jego pierwiastki *pierwiastkami charakterystycznymi*.

Jeśli wielomian charakterystyczny ma k różnych pierwiastków q_1, q_2, \dots, q_k , wtedy

$$h_n = c_1 q_1^n + c_2 q_2^n + \dots + c_k q_k^n$$

stanowi ogólną postać rozwiązania.

Dla każdego wyboru wartości początkowych h_0, h_1, \dots, h_{k-1} istnieją jednoznacznie określone stałe c_1, c_2, \dots, c_k .

Jeśli q_i jest pierwiastkiem s_i -krotnym wielomianu charakterystycznego, to wówczas każda z wartości $h_n = q_i^n, h_n = nq_i^n, h_n = n^2 q_i^n, \dots, h_n = n^{s_i-1} q_i^n$ jest rozwiązaniem równania, a stąd

$$h_n^{(i)} = c_1 q_i^n + c_2 n q_i^n + \dots + c_{s_i} n^{s_i-1} q_i^n$$

jest rozwiązaniem dla pierwiastka q_i ,
przy każdym wyborze współczynników c_1, c_2, \dots, c_{s_i} .

Niech q_1, q_2, \dots, q_t będą różnymi pierwiastkami, o krotnościach odpowiednio s_1, s_2, \dots, s_t .

Ogólna postać rozwiązania homogenicznego równania rekurencyjnego liniowego o stałych współczynnikach:

$$h_n = h_n^{(1)} + h_n^{(2)} + \dots + h_n^{(t)}.$$

W celu rozwiązania niehomogenicznego równania rekurencyjnego liniowego o stałych współczynnikach wykonujemy następujące kroki:

- (1) znajdujemy rozwiązanie ogólne odpowiedniego równania homogenicznego
- (2) znajdujemy rozwiązanie szczególne równania niehomogenicznego
- (3) łączymy oba rozwiązania z wykorzystaniem wartości początkowych.

Wykonanie kroku (2) wymaga próby wykorzystania różnych form rozwiązania szczególnego h_n w zależności od postaci czynnika niehomogenicznego b . W szczególności:

- (i) gdy b jest wielomianem stopnia k to za testowane rozwiązanie szczególne h_n przyjmujemy również wielomian stopnia k ,
- (ii) gdy $b = sp^n$ to próbujemy wykorzystać $h_n = tp^n$.

Powodzenie w wykonaniu kroku (2) zależy od postaci wielomianu charakterystycznego.

Definicja

Nieskończonemu ciągowi a_0, a_1, a_2, \dots może zostać przypisany szereg formalny

$$A(x) = \sum_{i=0}^{\infty} a_i x^i.$$

Wówczas $A(x)$ oznacza *funkcję tworzącą* (zwyczajną) dla tego ciągu.

Jeśli $a_k = 0$ dla każdego $k > n$, to wtedy szereg utożsamiamy z wielomianem $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$.

Lemat

Każdy ciąg a_0, a_1, a_2, \dots wyznacza jednoznacznie funkcję tworzącą $A(x)$. Każda funkcja $A(x)$ określa jednoznacznie ciąg a_0, a_1, a_2, \dots .

Definicja

Funkcją tworzącą eksponencjalną nieskończonego ciągu a_0, a_1, a_2, \dots jest szereg formalny

$$B(x) = \sum_{i=0}^{\infty} a_i \frac{x^i}{i!}.$$

Lemat

Każdy ciąg a_0, a_1, a_2, \dots wyznacza jednoznacznie funkcję tworzącą eksponencjalną $B(x)$. Każda funkcja $B(x)$ określa jednoznacznie ciąg a_0, a_1, a_2, \dots

Twierdzenie

Niech $h_0, h_1, \dots, h_n, \dots$ będzie nieskończonym ciągiem liczb spełniającym homogeniczne równanie rekurencyjne liniowe stopnia k o stałych współczynnikach

$$h_n - a_1 h_{n-1} - a_2 h_{n-2} - \dots - a_k h_{n-k} = 0, \quad (a_k \neq 0, n \geq k).$$

Wówczas funkcja tworząca dla tego równania ma postać $H(x) = \frac{P(x)}{Q(x)}$, gdzie $Q(x)$ jest wielomianem stopnia k o niezerowym współczynniku stałym, natomiast $P(x)$ jest wielomianem stopnia mniejszego niż k .

Niech G będzie grupą permutacji zbioru $X = \{1, 2, \dots, n\}$.

Niech \mathcal{C} będzie zbiorem wszystkich pokolorowań zbioru X .

Niech $f \in G$ oraz $c \in \mathcal{C}$.

Niech f^* oznacza permutację indukowaną przez f , działającą na zbiorze kolorów.

Wtedy $f^*(c(x)) = c(f(x))$ dla każdego $x \in X$, czyli $f^* \circ c = c \circ f$.

Mówimy wówczas, że grupa G działa na zbiorze pokolorowań \mathcal{C} .

Definicja

Niech $c_1, c_2 \in \mathcal{C}$ będą dwoma różnymi pokolorowaniami. Mówimy, że $c_1 \sim c_2$ (są *równoważne*) jeśli $c_2 = c_1 \circ f = f^* \circ c_1$ dla pewnej permutacji $f \in G$.

Lemat

Relacja \sim jest relacją równoważności.

Niech $G(c) = \{f : f \in G, c \circ f = c\}$.

Niech $\mathcal{C}(f) = \{c : c \in \mathcal{C}, c \circ f = c\}$.

Definicja

Zbiór $G(c)$ nazywamy *stabilizatorem* kolorowania c .

Lemat

Dla każdego kolorowania $c \in \mathcal{C}$ stabilizator $G(c)$ tworzy grupę. Ponadto, dla dowolnych $f, g \in G$, $c \circ g = c \circ f$ wtedy i tylko wtedy, gdy $f^{-1} \circ g \in G(c)$.

Lemat

Niech $c \in \mathcal{C}$. Liczba $|\{c \circ f : f \in G\}|$ pokolorowań równoważnych do c jest równa

$$\frac{|G|}{|G(c)|}.$$

Twierdzenie

Niech G będzie grupą permutacji zbioru X , a \mathcal{C} zbiorem wszystkich takich pokolorowań, że $c \circ f \in \mathcal{C}$ dla każdego $f \in G$ oraz każdego $c \in \mathcal{C}$. Wówczas liczba $N(G, \mathcal{C})$ wszystkich nierównoważnych pokolorowań w \mathcal{C} jest dana wzorem

$$N(G, \mathcal{C}) = \frac{1}{|G|} \sum_{f \in G} |\mathcal{C}(f)|.$$

Niech $\lambda(f)$ oznacza liczbę cykli w rozkładzie permutacji f na cykle.

Twierdzenie

Niech $f \in G$ oraz niech k oznacza liczbę kolorów przypisanych elementom z X dla pewnego $c \in \mathcal{C}$. Wówczas $|C(f)| = k^{\lambda(f)}$.

Niech $f \in G$. Załóżmy, że f jest typu $(\lambda_1, \lambda_2, \dots, \lambda_n)$.

Wówczas $\sum_{i=1}^n i\lambda_i = n$ oraz $\lambda(f) = \sum_{i=1}^n \lambda_i$.

Niech z_1, z_2, \dots, z_n będą niezmiennikami,
 z_i odpowiada cyklowi długości i .

Każdej permutacji f typu $(\lambda_1, \lambda_2, \dots, \lambda_n)$ przypisany jest monomial $\text{mon}(f) = z_1^{\lambda_1} z_2^{\lambda_2} \dots z_n^{\lambda_n}$, którego stopień wynosi $\lambda(f)$.

Wówczas

$$\sum_{f \in G} \text{mon}(f) = \sum_{f \in G} z_1^{\lambda_1} z_2^{\lambda_2} \dots z_n^{\lambda_n}$$

jest funkcją tworzącą typów permutacji w G .

Współczynnik przy danym $z_1^{\lambda_1} z_2^{\lambda_2} \dots z_n^{\lambda_n}$ oznacza liczbę permutacji typu $(\lambda_1, \lambda_2, \dots, \lambda_n)$.

Definicja

Cyklicznym indeksem grupy G nazywamy liczbę

$$P_G(z_1, z_2, \dots, z_n) = \frac{1}{|G|} \sum_{f \in G} z_1^{\lambda_1} z_2^{\lambda_2} \cdots z_n^{\lambda_n}.$$

Twierdzenie

Niech G będzie grupą permutacji n -elementowego zbioru X , a \mathcal{C} zbiorem wszystkich k^n pokolorowań elementów w X za pomocą k kolorów. Liczba $N(G, \mathcal{C})$ wszystkich nierównoważnych pokolorowań w \mathcal{C} jest równa

$$N(G, \mathcal{C}) = P_G(k, k, \dots, k).$$

Twierdzenie

Niech G będzie grupą permutacji n -elementowego zbioru X . Niech $U = \{u_1, u_2, \dots, u_k\}$ będzie zbiorem k kolorów, a \mathcal{C} zbiorem wszystkich pokolorowań elementów w X za pomocą kolorów z U . Wówczas funkcja tworząca dla liczby nierównoważnych pokolorowań w zależności od dystrybucji kolorów ma postać

$$P_G(u_1 + u_2 + \dots + u_k, u_1^2 + u_2^2 + \dots + u_k^2, \dots, u_1^n + u_2^n + \dots + u_k^n),$$

a współczynnik przy $u_1^{p_1} u_2^{p_2} \dots u_k^{p_k}$ oznacza liczbę nierównoważnych pokolorowań, w których p_i elementów zbioru X pokolorowanych jest kolorem u_i , dla każdego $i = 1, 2, \dots, k$.

Definicja

Grafem nazywamy parę $G = (V, E)$, w której V oznacza skończony zbiór *wierzchołków*, natomiast $E \subseteq \{\{u, v\} : u, v \in V\}$ jest zbiorem *krawędzi*.

Rzędem grafu $G = (V, E)$ jest liczba $n = |V|$, natomiast *rozmiarem* $m = |E|$.

Definicja

Grafem skierowanym (digrafem) nazywamy parę $G = (V, A)$, w której V oznacza skończony zbiór *wierzchołków*, natomiast $A \subseteq \{(u, v) : u, v \in V\}$ jest zbiorem *łuków*.

Definicja

Multigrafem nazywamy parę $G = (V, E)$, w której V oznacza skończony zbiór *wierzchołków*, natomiast $E \subseteq \{\{u, v\} : u, v \in V\}$ jest multizbiorem *krawędzi*.

Definicja

Hipergrafem nazywamy parę $G = (V, \mathcal{E})$, w której V oznacza skończony zbiór *wierzchołków*, natomiast $\mathcal{E} \subseteq \{e : e \subset V\}$ jest zbiorem *hiperkrawędzi*.

Definicja

Stopniem wierzchołka v w grafie $G = (V, E)$ nazywamy liczbę $d(v) = |\{\{v, u\} \in E : u \in V\}|$.

Stopniem maksymalnym w grafie $G = (V, E)$ (stopniem grafu) nazywamy liczbę $\Delta(G) = \max\{d(v) : v \in V\}$.

Stopniem minimalnym w $G = (V, E)$ jest liczba $\delta(G) = \min\{d(v) : v \in V\}$.

Lemat

Suma stopni wszystkich wierzchołków w grafie jest liczbą parzystą. Liczba wierzchołków stopnia nieparzystego w grafie jest parzysta.

Definicja

Spacerem w grafie $G = (V, E)$ nazywamy ciąg wierzchołków $\langle v_0, v_1, \dots, v_k \rangle$ o takiej własności, że dla każdego $1 \leq i \leq k$ $\{v_{i-1}, v_i\} \in E$.

Droga to spacer nie zawierający powtarzających się krawędzi.

Ścieżka to droga nie zawierająca powtarzających się wierzchołków.

Mówimy, że spacer jest *zamknięty* jeśli $\{v_k, v_0\} \in E$.

W przeciwnym przypadku spacer jest *otwarty*.

Zamkniętą ścieżkę nazywamy *cyklem*.

Definicja

Liczbę krawędzi w spacerze $\langle v_0, v_1, \dots, v_k \rangle$ (otwartym lub zamkniętym) nazywamy jego *długością*.

Definicja

Mówimy, że graf $G = (V, E)$ jest *spójny*, jeśli dla każdej pary wierzchołków $u, v \in V$ istnieje ścieżka o wierzchołkach końcowych u i v .

W przeciwnym przypadku graf jest *niespójny*.

Definicja

Odległością $d(u, v)$ wierzchołków u i v w grafie $G = (V, E)$ nazywamy minimalną długość ścieżki z u do v .

Średnica grafu $G = (V, E)$ to liczba $\text{diam}(G) = \max\{d(u, v) : u, v \in V\}$.

Lemat

Niech $\delta(G) \geq \lfloor \frac{n}{2} \rfloor$.

Wówczas G jest grafem spójnym.

Definicja

Graf $G' = (V', E')$ nazywamy *podgrafem* grafu $G = (V, E)$, jeśli $V' \subset V$ oraz $E' \subset E$.

Jeśli G' zawiera każdą krawędź grafu G , której oba wierzchołki końcowe są w V' , to G' jest podgrafem *indukowanym* przez V' .

Jeśli $V' = V$ to G' jest podgrafem *spinającym*.

Lemat

W każdym grafie $G = (V, E)$ zbiór V jest jednoznacznie rozkładalny na takie podzbiory V_1, V_2, \dots, V_k

($V_1 \cup V_2 \cup \dots \cup V_k = V$, $V_i \cap V_j = \emptyset$ jeśli $i \neq j$), że każdy podgraf indukowany przez V_i jest spójny oraz, dla każdego $i \neq j$, $u \in V_i$, $v \in V_j$, nie istnieje ścieżka o końcach u i v , $i, j \in \{1, 2, \dots, k\}$.

Definicja

Podgrafy indukowane przez V_1, V_2, \dots, V_k nazywamy *spójnymi składowymi* grafu G .

Definicja

Mówimy, że grafy $G = (V, E)$ oraz $G' = (V', E')$ są *izomorficzne*, jeśli istnieje taka bijekcja $\varphi : V \mapsto V'$, że

$$\{x, y\} \in E \Leftrightarrow \{\varphi(x), \varphi(y)\} \in E'.$$

| n | grafy poetykietowane | grafy nieizomorficzne |
|-----|------------------------|-----------------------|
| 2 | 2 | 2 |
| 3 | 8 | 4 |
| 4 | 64 | 11 |
| 5 | 1 024 | 34 |
| 6 | 32 768 | 156 |
| 7 | 2 097 152 | 1 044 |
| 8 | 268 435 456 | 12 346 |
| 9 | 68 719 476 736 | 274 668 |
| 10 | 35 184 372 088 832 | 12 005 168 |
| 11 | 36 028 797 018 963 968 | 1 018 997 864 |

Definicja

Dopełnieniem grafu $G = (V, E)$ jest graf $\bar{G} = (V, \bar{E})$, w którym $E \cap \bar{E} = \emptyset$ oraz $E \cup \bar{E} = E(K_n)$.

Definicja

Graf izomorficzny ze swoim dopełnieniem nazywamy *samodopełniającym*.

Definicja

Drogą Eulera (zamkniętą) w spójnym multigrafie $G = (V, E)$ nazywamy drogę zamkniętą zawierającą każdą krawędź ze zbioru E .

Twierdzenie

Multigraf spójny $G = (V, E)$ posiada zamkniętą drogę Eulera wtedy i tylko wtedy, gdy stopień każdego wierzchołka w G jest parzysty.

Znajdowanie drogi Eulera

$D := \emptyset$

$v = v_0$

for każda krawędź $\{v, u\}$ w G **do**

 odwiedzona $\{\{v, u\}\} := 0$

do

if istnieje nieodwiedzona krawędź $\{v, u\}$ incydentna do v **then**

 połóż_na_stos($\{v, u\}$)

 odwiedzona $\{\{v, u\}\} := 1$

else

$\{v, u\} := \text{zdejmij_ze_stosu}()$

$D := D \cup \{v, u\}$

$v := u$

while stos_niepusty()

return D

Definicja

Otwartą drogą Eulera w spójnym multigrafie $G = (V, E)$ nazywamy drogę otwartą zawierającą każdą krawędź ze zbioru E .

Twierdzenie

Multigraf spójny $G = (V, E)$ posiada otwartą drogę Eulera wtedy i tylko wtedy, gdy dokładnie dwa wierzchołki w G mają stopnie nieparzyste.

Problem chińskiego listonosza

Wejście: Graf spójny $G = (V, E)$ oraz funkcja kosztu $w : E \mapsto \mathbb{R}^+$.

Wyjście: Zamknięty spacer D o minimalnej wadze $w(D)$ zawierający każdą krawędź z E .

Definicja

Graf $G = (V, E)$ jest *dwudzielny*, jeśli istnieje taki podział (X, Y) zbioru V ($X \cup Y = V$, $X \cap Y = \emptyset$), że każda krawędź w G ma jeden wierzchołek końcowy w X a drugi w Y .

Lemat

Graf G jest dwudzielny wtedy i tylko wtedy, gdy każdy cykl w G ma parzystą długość.

Definicja

Drzewem nazywamy graf spójny acykliczny.

Lasem nazywamy graf acykliczny.

Liść w lesie to wierzchołek stopnia 1.

Lemat

Rozmiar drzewa rzędu n wynosi $n - 1$.

Lemat

Liczba liści l w drzewie rzędu n spełnia $0 \leq l \leq n$. Liczba liści l w drzewie rzędu $n \geq 3$ spełnia $2 \leq l \leq n - 1$.

Lemat

W drzewie każda para wierzchołków połączona jest dokładnie jedną ścieżką.

Definicja

Cykl zawierający każdy wierzchołek grafu $G = (V, E)$ nazywamy *cyklem Hamiltona*.

Graf G posiadający cykl Hamiltona jest *grafem hamiltonowskim*.

Definicja

Ścieżkę zawierającą każdy wierzchołek grafu $G = (V, E)$ nazywamy *ścieżką Hamiltona*.

Graf G posiadający ścieżkę Hamiltona jest *trasowalny*.

Twierdzenie

Niech $n \geq 3$. Jeśli $\delta(G) \geq \frac{n}{2}$ to G jest hamiltonowski.

Twierdzenie

Niech G będzie grafem, w którym, dla każdej pary niesąsiednich wierzchołków u i v , zachodzi warunek $d(u) + d(v) \geq n$.
Wtedy G jest hamiltonowski.

Problem komiwojżera

Wejście: Graf pełny $K_n = (V, E)$ oraz funkcja kosztu $w : E \mapsto \mathbb{R}^+$.

Wyjście: Cykl Hamiltona o minimalnej wadze.

Definicja

Skojarzeniem w grafie $G = (V, E)$ nazywamy podzbiór $M \subset E$ wierzchołkowo rozłącznych krawędzi.

Licznością skojarzenia M jest liczba $|M|$.

Skojarzenie M w grafie $G = (V, E)$ nazywamy *pełnym* jeśli $|M| = \frac{n}{2}$, a *niemal pełnym* jeśli $|M| = \frac{n-1}{2}$.

Lemat

Graf $G = (V, E)$ o parzystym rzędzie, w którym $\delta(G) \geq \frac{n}{2}$, posiada pełne skojarzenie.

Twierdzenie

Graf G posiada pełne skojarzenie wtedy i tylko wtedy, gdy $|S| \geq c$ dla każdego podzbioru $S \subset V$, gdzie c oznacza liczbę spójnych składowych o nieparzystym rzędzie w grafie $G[V \setminus S]$.

Twierdzenie

Graf dwudzielny $G(X, Y; E)$ zawiera skojarzenie rozmiaru $|X|$ wtedy i tylko wtedy, gdy dla każdego $S \subset X$ zachodzi $|S| \leq |N(S)|$.

Mówimy, że M jest *najliczniejszym* skojarzeniem w G jeśli $|M| = \max\{|M'| : M' \text{ jest skojarzeniem w } G\}$. Wówczas liczbę $\mu(G) = |M|$ nazywamy *liczbą skojarzeniową* grafu G .

Ścieżka $P = \langle v_0, v_1, \dots, v_k \rangle$ o nieparzystej długości k jest *ścieżką powiększającą* względem skojarzenia M w grafie G jeśli dla każdego l spełniającego $1 \leq l \leq \frac{k-1}{2}$ zachodzi $\{v_{2l-1}, v_{2l}\} \in M$, a wierzchołki v_0 oraz v_k są *wolne* (czyli nie są incydentne z żadną krawędzią skojarzenia M).

Twierdzenie

M jest najliczniejszym skojarzeniem w grafie G wtedy i tylko wtedy, gdy G nie zawiera ścieżki powiększającej względem M .

Definicja

Przez *płaską reprezentację* grafu $G = (V, E)$ rozumiemy takie rozmieszczenie wierzchołków zbioru V na płaszczyźnie (sferze), że jedyny punkt przecięcia dowolnych dwóch krawędzi to ewentualnie ich wspólny koniec.

Definicja

Graf nazywamy *planarnym* jeśli posiada płaską reprezentację.

Definicja

Reprezentacja płaska grafu rozdziela jednoznacznie powierzchnię sfery na regiony zwane *ścianami*.

Lemat

Niech f oznacza liczbę ścian w płaskiej reprezentacji spójnego grafu $G = (V, E)$. Wówczas $n - m + f = 2$.

Lemat

W każdym grafie planarnym $G = (V, E)$ rzędu $n \geq 3$ zachodzi zależność $m \leq 3n - 6$.

Lemat

Każdy graf planarny $G = (V, E)$ zawiera wierzchołek stopnia co najwyżej 5.

Definicja

Rozdzieleniem krawędzi $\{u, v\}$ w grafie $G = (V, E)$ nazywamy dodanie nowego wierzchołka w oraz zastąpienie tej krawędzi przez dwie krawędzie $\{u, w\}$ i $\{w, v\}$.

Rozdzieleniem grafu G nazywamy graf G' powstały z G poprzez wykonanie kolejnych rozdzieleni krawędzi.

Twierdzenie Kuratowskiego

Graf G jest planarny wtedy i tylko wtedy, gdy nie zawiera podgrafu będącego rozdzieleniem grafu K_5 lub $K_{3,3}$.

Zwinięciem krawędzi $\{u, v\}$ w grafie $G = (V, E)$ nazywamy operację złączenia wierzchołków u oraz v wraz z usunięciem powstałej pętli oraz zastąpienia potencjalnych równoległych krawędzi przez pojedynczą krawędź.

Minorem grafu G nazywamy graf G' powstały z G poprzez wykonanie kolejnych operacji usuwania wierzchołków, usuwania krawędzi oraz/lub zwijania krawędzi.

Twierdzenie Wagnera

Graf G jest planarny wtedy i tylko wtedy, gdy nie posiada minorów będących K_5 lub $K_{3,3}$.

Definicja

Zbiorem *niezależnym* w grafie $G = (V, E)$ nazywamy taki podzbiór $I \subset V$, że żadne dwa wierzchołki w I nie są sąsiednie.

Mówimy, że zbiór niezależny I w grafie G jest *najliczniejszy*, jeśli nie istnieje inny zbiór niezależny w G o rzędzie większym niż $|I|$. Wówczas $\alpha(G) = |I|$ nazywamy *liczbą niezależności* grafu G .

Definicja

Kliką w grafie $G = (V, E)$ nazywamy taki podzbiór $Q \subset V$, że każde dwa wierzchołki w Q są sąsiednie.

Mówimy, że klika Q w grafie G jest *najliczniejsza*, jeśli nie istnieje klika w G rzędu większego niż $|Q|$.

Wówczas $\omega(G) = |Q|$ nazywamy *liczbą klikową* grafu G .

Lemat

W każdym grafie G zachodzi $\alpha(G) = \omega(\overline{G})$.

Definicja

Kolorowaniem (wierzchołkowym) grafu $G = (V, E)$ nazywamy odwzorowanie $c : V \mapsto C$, gdzie C oznacza zbiór kolorów.

Jeśli dla każdego dwóch sąsiednich wierzchołków v, u zachodzi $c(v) \neq c(u)$, to kolorowanie nazywamy *właściwym*.

Jeśli $|C| = k$ to mówimy o *k-kolorowaniu*.

Minimalną liczbę k , dla której istnieje *k-kolorowanie* właściwe wierzchołków grafu G nazywamy *liczbą chromatyczną* grafu G i oznaczamy $\chi(G)$.

Zbiór wierzchołków pokolorowanych tym samym kolorem nazywamy *klasą kolorową*.

Każda klasa kolorowa jest zbiorem niezależnym.

Lemat

Dla każdego grafu G zachodzi $1 \leq \chi(G) \leq n$.

Lemat

Niech G będzie grafem, w którym $\Delta(G) \geq 1$. Wówczas $\chi(G) = 2$ wtedy i tylko wtedy, gdy G jest grafem dwudzielnym.

Lemat

W każdym grafie G zachodzą zależności:

$$\chi(G) \geq \omega(G)$$

$$\chi(G) \geq \lceil \frac{n}{\alpha(G)} \rceil$$

$$\chi(G) \leq \Delta(G) + 1$$

Twierdzenie Brooks'a

Dla każdego grafu G zachodzi

$$\chi(G) \begin{cases} = \Delta(G) + 1 & \text{gdy } G = K_n \text{ lub } G = C_{2p+1} \\ \leq \Delta(G) & \text{wpp} \end{cases}$$

Twierdzenie

Jeśli G jest grafem planarnym, to $\chi(G) \leq 4$.

Twierdzenie

Jeśli G jest grafem planarnym nie zawierającym trójkątów, to $\chi(G) \leq 3$.

Definicja

Graf $G = (V, E)$ jest r -cyrkularnie kolorowalny jeśli istnieje takie odwzorowanie $c' : V \mapsto [0, r)$, że

$$\forall \{x, y\} \in E : 1 \leq |c'(x) - c'(y)| \leq r - 1.$$

Cyrkularna liczbą chromatyczna grafu G , oznaczona $\chi_c(G)$, wynosi:
 $\chi_c(G) = \inf\{r : G \text{ jest } r\text{-cyrkularnie kolorowalny}\}.$

Twierdzenie

Dla każdego grafu G zachodzi $\chi(G) - 1 < \chi_c(G) \leq \chi(G).$

Definicja

Krawędziowym k -kolorowaniem (właściwym) grafu $G = (V, E)$ nazywamy takie odwzorowanie $c : E \mapsto C$, gdzie C oznacza zbiór kolorów oraz $|C| = k$, że dla każdych dwóch incydentnych krawędzi e_1, e_2 zachodzi $c(e_1) \neq c(e_2)$.

Minimalną liczbę k , dla której istnieje właściwe k -kolorowanie krawędzi grafu G nazywamy *indeksem chromatycznym* grafu G i oznaczamy $\chi'(G)$.

Zbiór krawędzi pokolorowanych tym samym kolorem nazywamy *klasą kolorową*.
Każda klasa kolorowa jest skojarzeniem.

Lemat

Dla każdego grafu G spełniona jest zależność $\chi'(G) \leq 2\Delta(G) - 1$.

Twierdzenie

Jeśli G jest grafem dwudzielnym, to $\chi'(G) = \Delta(G)$.

Twierdzenie

W dowolnym grafie G zachodzi $\chi'(G) \leq \lfloor \frac{3}{2}\Delta(G) \rfloor$.

Twierdzenie

Dla każdego grafu G zachodzi $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$.

Definicja

Dekompozycją grafu $G = (V, E)$ nazywamy rodzinę jego krawędziowo rozłącznych podgrafów G_1, G_2, \dots, G_t o takiej własności, że każda krawędź grafu G jest zawarta w dokładnie jednym z tych podgrafów.

Jeśli każdy G_i , $i = 1, 2, \dots, t$, jest izomorficzny z grafem H , to mówimy wówczas o *H-dekompozycji* grafu G .

Lemat

Jeśli istnieje *H-dekompozycja* grafu G , to $|E(G)|$ jest podzielne przez $|E(H)|$.

Twierdzenie

Graf pełny K_n posiada M_k -dekompozycję na skojarzenia rozmiaru k wtedy i tylko wtedy, gdy $1 \leq k \leq \lfloor \frac{n}{2} \rfloor$ oraz $k \mid \binom{n}{2}$.

Twierdzenie

Graf pełny K_n posiada P_{k+1} -dekompozycję na ścieżki długości k wtedy i tylko wtedy, gdy $1 \leq k \leq n - 1$ oraz $k \mid \binom{n}{2}$.

Twierdzenie

Graf pełny K_n posiada C_k -dekompozycję na cykle długości k wtedy i tylko wtedy, gdy $3 \leq k \leq n$, $k \mid \binom{n}{2}$ oraz n jest nieparzyste.

Hipoteza

Graf pełny K_{2n+1} posiada T_{n+1} -dekompozycję dla każdego drzewa T_{n+1} rzędu $n + 1$.

Definicja

Kwadratem łacińskim rzędu n (o boku n) nazywamy tablicę rozmiaru $n \times n$, w której każda komórka zawiera element ze zbioru S rzędu n w taki sposób, że każdy symbol z S występuje dokładnie raz w każdym wierszu i dokładnie raz w każdej kolumnie kwadratu.

Definicja

Dwa kwadraty łacińskie, L i L' , rzędu n są *ortogonalne*, jeśli wszystkie spośród n^2 par $(L(i, j), L'(i, j))$ są parami różne.

Twierdzenie

Dla każdego $n \geq 1$, $n \neq 2, 6$, istnieje para ortogonalnych kwadratów łacińskich rzędu n .

Definicja

Mówimy, że w zbiorze L_1, L_2, \dots, L_m kwadraty łacińskie rzędu n są *wzajemnie ortogonalne* (ozn. $\text{MOLS}(n)$), jeśli dla każdego $1 \leq i < j \leq m$, L_i oraz L_j są ortogonalne. Niech $N(n)$ oznacza maksymalną liczbę kwadratów w zbiorze $\text{MOLS}(n)$.

Lemat

Dla każdego n zachodzi $1 \leq N(n) \leq n - 1$.

Twierdzenie

Jeśli $q = p^k$ jest potęgą liczby pierwszej, wówczas $N(q) = q - 1$.

Definicja

Częściowym kwadratem łacińskim rzędu n nazywamy tablicę rozmiaru $n \times n$, w której każda komórka jest albo pusta albo zawiera element ze zbioru S w taki sposób, że każdy symbol z S występuje co najwyżej raz w każdym wierszu i co najwyżej raz w każdej kolumnie.

Twierdzenie

Częściowy kwadrat łaciński rzędu n , w którym co najwyżej $n - 1$ komórek jest niepustych, może zostać uzupełniony do kwadratu łacińskiego rzędu n .

Definicja

Niech a , b i n będą liczbami naturalnymi spełniającymi zależność $a \times b = n$. Wówczas tablica rozmiaru $n \times n$ może zostać podzielona na rozłączne *bloki*, każdy z nich będący podtablicą rozmiaru $a \times b$. (a, b) -kwadratem *Sudoku* nazywamy kwadrat łaciński nad zbiorem symboli $\{1, 2, \dots, n\}$, w którym każdy blok zawiera wszystkie symbole z S .

Definicja

(a, b) -zbiorem *krytycznym Sudoku* nazywamy częściowy kwadrat łaciński P , który może zostać uzupełniony w sposób jednoznaczny do (a, b) -kwadratu *Sudoku*, a ponadto usunięcie jakiegokolwiek niepustej komórki z P zaburza jednoznaczność tego uzupełnienia.

Lemat

Dla każdego k , $17 \leq k \leq 35$, istnieje $(3,3)$ -zbiór krytyczny *Sudoku* posiadający k niepustych komórek.

| typ | liczba kwadratów Sudoku |
|--------|-------------------------------|
| (1, 1) | 1 |
| (2, 2) | 288 |
| (3, 3) | 6 670 903 752 021 072 936 960 |

Definicja

Systemem trójek Steinerja, $STS(v)$, rzędu v nazywamy taką parę (V, \mathcal{B}) , w której V jest skończonym zbiorem punktów, $|V| = v$, oraz \mathcal{B} jest rodziną 3-elementowych podzbiorów zbioru V nazywanych *trójkami* o takiej własności, że każdy 2-elementowy podzbiór zbioru V jest zawarty w dokładnie jednej trójce.

Warunek konieczny na istnienie $STS(v)$: $v \equiv 1, 3 \pmod{6}$.

Twierdzenie

System trójek Steinerja rzędu v istnieje wtedy i tylko wtedy, gdy $v \equiv 1, 3 \pmod{6}$.

Definicja

Dwa systemy trójek Steinera, (V_1, \mathcal{B}_1) and (V_2, \mathcal{B}_2) , są *izomorficzne* jeśli istnieje taka bijekcja $\alpha : V_1 \mapsto V_2$, że dla dowolnej trójki $B_1 \in \mathcal{B}_1$ istnieje trójka $B_2 \in \mathcal{B}_2$, która spełnia $B_2 = \{\alpha(x_i) : x_i \in B_1\}$.

| v | liczba nieizomorficznych STS(v) |
|-----|-------------------------------------|
| 7 | 1 |
| 9 | 1 |
| 13 | 2 |
| 15 | 80 |
| 19 | 11 084 874 829 |
| 21 | 14 796 207 517 873 771 |

Definicja

Automorfizm systemu trójek to izomorfizm w samego siebie. Zbiór wszystkich automorfizmów tworzy grupę automorfizmów systemu trójek.

Definicja

$STS(v)$ jest *cykliczny* jeśli posiada automorfizm składający się z jednego cyklu długości v .

Definicja

Uporządkowany 3-elementowy podzbiór (a, b, c) zbioru $\{1, 2, \dots, (v-1)/2\}$ nazywamy *trójką różnicową* wtedy, gdy $a + b = c$ lub $a + b + c = v$.

Problem różnicowy Hefftera

- (1) Niech $v = 6k + 1$. Czy istnieje podział zbioru $\{1, 2, \dots, 3k\}$ na k trójek różnicowych?
- (2) Niech $v = 6k + 3$. Czy istnieje podział zbioru $\{1, 2, \dots, 3k + 1\} \setminus \{2k + 1\}$ na k trójek różnicowych?

Twierdzenie

Problem różnicowy Hefftera posiada rozwiązanie dla każdego $v \geq 3$ z wyjątkiem $v = 9$.

Dla zadanego rozwiązania problemu Hefftera:

(1) każda trójka różnicowa (a, b, c) wyznacza bazową trójkę $\{0, a, a + b\}$ cyklicznego STS($6k + 1$)

(1) każda trójka różnicowa (a, b, c) wyznacza bazową trójkę $\{0, a, a + b\}$ cyklicznego STS($6k + 3$); ponadto $\{0, 2k + 1, 4k + 2\}$ jest bazową trójką dla *krótkiej orbity*.

Definicja

Konfiguracją kombinatoryczną typu BIBD nazywamy taką parę (V, \mathcal{B}) , w której $|V| = v$ oraz \mathcal{B} jest rodziną składającą się z b bloków, każdy będącym k -elementowym podzbiorem zbioru V o takiej własności, że każdy element z V jest zawarty w dokładnie r blokach i ponadto każdy 2-elementowy podzbiór zbioru V jest zawarty w dokładnie λ blokach. Liczby v , b , r , k oraz λ nazywane są *parametrami* konfiguracji BIBD.

Warunki konieczne na istnienie konfiguracji BIBD(v, b, r, k, λ):

- (1) $\lambda(v-1) \equiv 0 \pmod{k-1}$,
- (2) $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$.

$$r = \frac{\lambda(v-1)}{k-1} \quad b = \frac{vr}{k}$$

Twierdzenie

Dla $k \leq 6$, konfiguracja $(v, k, 1)$ – BIBD istnieje gdy:

$k = 2$ wtedy i tylko wtedy, gdy $v \geq 2$

$k = 3$ wtedy i tylko wtedy, gdy $v \equiv 1, 3 \pmod{6}$

$k = 4$ wtedy i tylko wtedy, gdy $v \equiv 1, 4 \pmod{12}$

$k = 5$ wtedy i tylko wtedy, gdy $v \equiv 1, 5 \pmod{20}$

$k = 6$ wtedy i tylko wtedy, gdy $v \equiv 1, 6 \pmod{15}$

oraz $v \neq 16, 21, 36, 46; 51, 61, 81, 166, 226, 231, 256, 261, 286,$
 $316, 321, 346, 351, 376, 406, 411, 436, 441, 471, 501, 561, 591, 616,$
 $646, 651, 676, 771, 796, 801$