Matematyka dyskretna (L) - cheatsheet
Tomasz Woszczyński

1 Wariacje

Liczba wariacji z powtórzeniami

Dla zbiorów A, B o odpowiednio m, n elementach liczba funkcji ze zbioru A w B wynosi n^m, czyli $|\{f : A \to B\} = n^m|$.

Liczba wariacji bez powtórzeń

Dla zbiorów A, B o odpowiednio m, n elementach liczba funkcji różnowartościowych ze zbioru A w B wynosi $n(n-1)\dots(n-m+1) = \frac{n!}{(n-m)!}$.

Liczba podzbiorów

Zbiór A o n elementach ma $|\{B : B \subseteq A\} = 2^n|$ podzbiorów.

Para podzbiorów

Dla U będącego n-elementowym można wyznaczyć dwa jego podzbiory A, B takie, że $A \subseteq B$ na $|\{(A,B) : A \subseteq B \subseteq U\}| = |\{f : U \to \{0,1,2\}\}| = 3^n$ sposobów.

Liczba permutacji

Zbiór U o n elementach można spermutować na $n!$ sposobów.

Sufit, podłoga, część ułamkowa

Niech $x \in \mathbb{R}, n \in \mathbb{Z}$, wtedy:
$\lfloor x \rfloor = n \Leftrightarrow n \le x < n+1$
$\lceil x \rceil = n \Leftrightarrow n-1 < x \le n$
$\{x\} = x - \lfloor x \rfloor$

Własności sufitu i podłogi

Niech $x \in \mathbb{R}, n \in \mathbb{Z}$, wtedy:
$\lfloor x+n \rfloor = n + \lfloor x \rfloor$, ponieważ $\lfloor x \rfloor + n \le x + n < \lfloor x \rfloor + n + 1$.
Ponadto mamy:
$\lceil x+n \rceil = n + \lceil x \rceil$
$\lfloor -x \rfloor = -\lceil x \rceil$

Podzbiory k-elementowe

Niech $|U| = \{1, 2, \dots, n\}$ oraz $P_n^k = \{A \subseteq U : |A| = k\}$. Wtedy $\frac{n!}{(n-k)!} = k! \left|P_n^k\right|$, czyli $\left|P_n^k\right| = \frac{n!}{(n-k)!k!} = \binom{n}{k}$.

Symbol Newtona

Dla $k, n \in \mathbb{N}$ takich, że $0 \le k \le n$ zachodzi:
$\binom{n}{k} = \binom{n}{n-k}$
$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$

Kulki i szufladki

n kulek do k szuflad można wrzucić na tyle sposobów, ile jest ciągów złożonych z n zer i $k-1$ jedynek, czyli $\binom{n+k-1}{k-1}$.

Dwumian Newtona

Dla $n \in \mathbb{N}$ mamy $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$.

Zasada szufladkowa Dirichleta

Niech $k, s \in \mathbb{N}_+$. Jeśli wrzucimy k kulek do s szuflad (Dirichleta), a kulek jest więcej niż szuflad ($k > s$), to w którejś szufladzie będą przynajmniej dwie kulki. Innymi słowy, dla skończonych zbiorów A, B, jeśli $|A| > |B|$, to nie istnieje funkcja różnowartościowa z A w B. Dla $k > s \cdot i$ kulek oraz s szuflad będzie w jakiejś szufladzie $i+1$ kulek.

2 Asymptotyka

Niech $f, g : \mathbb{N} \to \mathbb{R} \ge 0$, wtedy możemy mówić o takich funkcjach asymptotycznych:

Notacja dużego O

Mamy $f(n) = O(g(n))$ wtw, gdy $\exists (c > 0)\ \exists (n_0 \in \mathbb{N})\ \forall (n \ge n_0)\ f(n) < cg(n)$.
Ponadto dla $C, a, \alpha, \beta \in \mathbb{R}$ zachodzą takie własności:
$\forall (\alpha, \beta)\ \alpha \le \beta \Rightarrow n^\alpha = O(n^\beta)$,
$\forall (\alpha > 1) n^C = O(a^n)$,
$\forall (\alpha > 0) (\ln n)^C = O(n^\alpha)$.
Przydatna może okazać się reguła de l'Hospitala, więc gdy $f(n)$ i $g(n)$ dążą do nieskończoności, to $\lim_{n\to\infty} \frac{f(n)}{g(n)} = \lim_{n\to\infty} \frac{f'(n)}{g'(n)}$.

Notacja małego o

$f(n) = o(g(n))$ wtw, gdy $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$.

Notacja duże Omega (Ω)

$f(n) = \Omega(g(n))$ wtw, gdy $\exists (c > 0) \exists (n_0 \in \mathbb{N}) \forall (n \ge n_0) f(n) \ge cg(n)$.

Notacja Theta (Θ)

$f(n) = \Theta(g(n))$ wtw, gdy $f(n) = \Omega(g(n)) \wedge f(n) = O(g(n))$.

Notacja małe Omega (ω)

$f(n) = \omega(g(n))$ wtw, gdy $\lim_{n\to\infty} = \frac{f(n)}{g(n)} = \infty$.

3 Arytmetyka modularna

Funkcja modulo

Niech $n, d \in \mathbb{Z}$ i $d \ne 0$. Wtedy:
$n \bmod d = n - \left\lfloor \frac{n}{d} \right\rfloor \cdot d$.

$n \bmod d = r$ wtw, gdy $0 \le r < d \ \wedge\ \exists (k \in \mathbb{Z})\ n = kd + r$

Przystawanie modulo

$a \equiv_n b$ wtw, gdy $a \bmod n = b \bmod n$

Własności funkcji modulo

$a + b \equiv_n a \bmod n + b \bmod n$
$a \cdot b \equiv_n (a \bmod n) \cdot (b \bmod n)$

Podzielność

Niech $n, d \in \mathbb{Z}$ i $d \ne 0$. Wtedy:
$d|n$ wtw, gdy $\exists (k \in \mathbb{Z})\ n = kd$
$d|n$ wtw, gdy $n \bmod d = 0$
$d|n$ wtw, gdy $n \equiv_d 0$
$d|n_1 \wedge d|n_2$ to $d|(n_1 + n_2)$

Największy wspólny dzielnik (NWD, gcd)

Niech $a, b \in \mathbb{N}$, wtedy
$\gcd(a,b) = \max\{d \in \mathbb{N} : d|a \wedge d|b\}$

Algorytm Euklidesa

Dla $a \ge b > 0$ korzystamy z własności: $\gcd(a,b) = \gcd(b, a \bmod b)$ oraz $\gcd(a, 0) = a$.

```
gcd(a, b):
    while b != 0:
        c = a mod b
        a = b
        b = c
    return a
```

Rozszerzony algorytm Euklidesa

Dla $a \ge b > 0$:
$\exists (x, y \in \mathbb{Z})\ xa + yb = \gcd(a,b)$

```
gcd(a, b):
    x = 1, y = 0, r = 0, s = 1
    while b != 0:
        c = a mod b
        q = a div b
        a = b
        b = c

        r' = r
        s' = s
        r = x - q * r
        s = y - q * s
        x = r'
        y = s'

    return a, x, y
```

Liczby względnie pierwsze

Niech $a, b \in \mathbb{Z}$, wtedy te liczby są względnie pierwsze, gdy $\gcd(a,b) = 1$.

4 Wzór włączeń i wyłączeń

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I \subseteq \{1,\dots,n\}} \left| \bigcap_{i \in I} A_i \right|$$

5 Rekurencja, zależności rekurencyjne

Liczby Fibonacciego

Niech $F_0 = 0, F_1 = 1$, wtedy $F_n = F_{n-1} + F_{n-2}$ dla $n > 1$.

Operator przesunięcia $\mathbf{E}$

Mamy ciąg $\langle a_n \rangle = \langle a_0, a_1, \dots, a_n, \dots \rangle$.
Wtedy $\mathbf{E} \langle a_n \rangle = \langle a_{n+1} \rangle = \langle a_1, \dots, a_n, \dots \rangle$.

Złożenie operatora przesunięcia

$\mathbf{E}^2 \langle a_n \rangle = \mathbf{E}(\mathbf{E}\langle a_n \rangle) = \langle a_2, \dots, a_n, \dots \rangle$

Operatory działające na ciągi

$\langle a_n \rangle + \langle b_n \rangle = \langle a_n + b_n \rangle = \langle a_0 + b_0, \dots \rangle$
$c\langle a_n \rangle = \langle ca_n \rangle = \langle ca_0, ca_1, \dots \rangle$

Co anihiluje dane ciągi?

$\langle \alpha \rangle$ anihiluje $\mathbf{E} - 1$.
$\left\langle \alpha a^i \right\rangle$ anihiluje $\mathbf{E} - a$.
$\left\langle \alpha a^i + \beta b^i \right\rangle$ anihiluje $(\mathbf{E} - a)(\mathbf{E} - b)$.
$\left\langle \sum_{k=0}^{n} \alpha_k a_k^i \right\rangle$ anihiluje $\prod_{k=0}^{n} (\mathbf{E} - a_k)$.
$\langle \alpha i + \beta \rangle$ anihiluje $(\mathbf{E} - 1)^2$.
$\left\langle (\alpha i + \beta) a^i \right\rangle$ anihiluje $(\mathbf{E} - a)^2$.
$\left\langle (\alpha i + \beta) a_i + \gamma b^i \right\rangle$ anihiluje $(\mathbf{E} - a)^2 (\mathbf{E} - b)$.
$\left\langle \sum_{k=0}^{n-1} \alpha_k i^k \right\rangle a^i$ anihiluje $(\mathbf{E} - a)^n$.

Dodatkowe własności anihilatorów

Jeśli $\mathbf{E}_A$ anihiluje $\langle a_i \rangle$, to ten sam anihilator anihiluje również ciąg $c\langle a_n \rangle$ dla dowolnej stałej c.
Jeśli $\mathbf{E}_A$ anihiluje $\langle a_i \rangle$ i $\mathbf{E}_B$ anihiluje $\langle b_i \rangle$, to $\mathbf{E}_A \mathbf{E}_B$ anihiluje $\langle a_i \rangle \pm \langle b_i \rangle$.

Liczby Catalana

C_n oznacza n-tą liczbę Catalana, wyraża się przez $C_n = \sum_{i=1}^{n} C_{i-1} C_{n-i}$ dla $C_0 = 0$.
Można je również przedstawić wzorami $C_n = \frac{1}{n+1} \binom{2n}{n} = \frac{(2n)!}{(n+1)!n!}$. Spełniają one zależność $C_n = \binom{2n}{n} - \binom{2n}{n+1}$.
Liczby Catalana posiadają różne interpretacje kombinatoryczne, takie jak liczba poprawnych rozmieszczeń nawiasów, liczba dróg w układzie współrzędnych w I ćwiartce, liczba drzew binarnych, liczba podziałów wielokąta wypukłego na trójkąty.

Funkcje tworzące (OGF)

Dla ciągu $\langle a_n \rangle$ można utworzyć funkcję $\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \ldots = A(x)$, która jest funkcją tworzącą tego ciągu. Poniżej kilka typowych funkcji tworzących dla ciągów:
$\frac{1}{1-x}$ dla ciągu $\langle 1 \rangle$, czyli $\frac{n}{1-x}$ dla $\langle n \rangle$.
$\frac{1}{1-2x}$ dla ciągu $\langle 2^n \rangle$.
$\frac{1}{(1-x)^2}$ dla ciągu $\langle 1, 2, 3, \dots \rangle$.
$\frac{1}{1-x^2}$ dla ciągu $\langle 0, 1, 0, 1, \dots \rangle$.

Przerwy pomiędzy wyrazami

Funkcją tworzącą takiego ciągu $\langle a_0, 0, a_1, 0, a_2, 0, \dots \rangle$ jest $\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x^2 + a_2 x^4 + \ldots = A(x^2)$. Dla ciągu o wyrazach co 3 miejsca byłoby to $A(x^3)$, dla 4 to $A(x^4)$, dla n więc $A(x^n)$.

Co drugi wyraz ciągu (pochodne)

Funkcją tworzącą $\langle a_0, 0, a_2, 0, a_4, 0, \dots \rangle$ jest $\frac{A(x)+A(-x)}{2}$, dla $\langle 0, a_1, 0, a_3, \dots \rangle$ mamy $\frac{A(x)-A(-x)}{2}$.

Funkcją tworzącą takiego ciągu $\langle 0, a_1, 2a_2, 3a_3, 4a_4, \dots, ia_i, \dots \rangle$ jest pochodna funkcji $A(x)$ przesunięta o jedno miejsce w prawo, a więc $xA'(x)$.

Wykorzystanie całek w OGF

Aby odnaleźć funkcję tworzącą ciągu $\left\langle 0, \frac{a_1}{1}, \frac{a_2}{2}, \dots, \frac{a_i}{i}, \dots \right\rangle$ należy scałkować funkcję tworzącą $A(x)$ i przesunąć ją w lewo: $\int_0^1 \frac{A(x)-a_0}{x} dx = \sum_{i=0}^{\infty} \frac{a_i}{i} x^i$.

Liczba podziałów liczby n

Dowolne składniki: $\prod_{i=1}^{\infty} \frac{1}{1-x^i}$

Różne składniki: $\prod_{i=1}^{\infty} (1 + x^i)$

Nieparzyste składniki: $\prod_{i=1}^{\infty} (1 + x^{2i-1})$

Składniki mniejsze od m: $\prod_{i=1}^{m-1} \frac{1}{1-x^i}$

Różne potęgi 2: $\prod_{i=1}^{\infty} (1 + x^{2^i})$

Rekursja uniwersalna

Niech a, b, c będą dodatnimi stałymi, rozwiązaniem równania rekurencyjnego

$$T(n) = \begin{cases} b & \text{dla } n = 1 \\ aT\left(\frac{n}{c}\right) + bn & \text{dla } n > 1 \end{cases}$$

dla n będących potęgą liczby c jest

$$T(n) = \begin{cases} O(n) & \text{dla } a < c \\ O(n \log n) & \text{dla } a = c \\ O\left(n^{\log_c a}\right) & \text{dla } a > c \end{cases}$$

6 Teoria grafów

Graf nieskierowany

Graf nieskierowany to para zbiorów (V, E), gdzie $E = \{\{u, v\} : u, v \in V\}$. V to zbiór wierzchołków, E to zbiór krawędzi.

"Patologie"w grafach

Pętla to krawędź postaci $\{v, v\}$, a krawędzie równoległe to dwie lub więcej krawędzi łączących te same wierzchołki u, v (dla $u \ne v$).

Graf prosty

Graf $G = (V, E)$ jest prosty, jeśli nie zawiera pętli ani krawędzi równoległych.

Graf skierowany

Graf nieskierowany to para zbiorów (V, E), gdzie $E = \{(u, v) : u, v \in V\}$. V to zbiór wierzchołków, E to zbiór krawędzi skierowanych lub łuków.

Krawędź incydentna

Krawędź e jest incydentna do wierzchołka u, jeśli jeden z końców e to u.

Stopień wierzchołka

Stopień wierzchołka u oznaczany przez $\deg(u)$ to liczba krawędzi incydentnych do u. Każda pętla incydentna do u dokłada się do stopnia u liczbą 2.

Lemat o uściskach dłoni

Niech $G = (V, E)$ będzie nieskierowanym grafem. Wtedy $\sum_{v \in V} \deg(v) = 2|E|$.

Matematyka dyskretna (L) - cheatsheet
Tomasz Woszczyński

Reprezentacje grafów

Graf można reprezentować za pomocą list sąsiadów, macierzy sąsiedztwa lub macierzy incydencji.

Izomorfizm grafów

Dwa grafy nieskierowane proste $G = (V, E)$ i $H = (V', E')$ są izomorficzne wtw, gdy istnieje bijekcja $f : V \to V'$ taka, że $\forall (u, v \in V)\ \{u, v\} \in E \Leftrightarrow \{f(u), f(v)\} \in E'$.

Marszruta, ścieżka, droga, cykl

Marszruta o długości k to ciąg $\langle v_0, v_1, \ldots, v_k \rangle$ taki, że $\forall (0 \leq i < k)\ \{v_i, v_{i+1}\} \in E$.
Droga to marszruta, w której żadna krawędź nie występuje dwukrotnie.

Ścieżka to marszruta, w której żaden wierzchołek nie występuje dwukrotnie.
Cykl to marszruta, w której pierwszy wierzchołek jest taki sam jak ostatni, a poza tym, żaden wierzchołek nie występuje dwukrotnie.
$u - v$-marszruta to marszruta taka, że $v_0 = u$ i $v_k = v$, analogicznie definiujemy $u - v$-drogę i $u - v$-ścieżkę.
Marszruta/droga jest zamknięta, gdy $v_0 = v_k$. Zamknięta ścieżka to cykl.

Graf spójny

Nieskierowany graf $G = (V, E)$ jest spójny, jeśli z każdego wierzchołka da się dojść do innego, tzn. dla każdego wierzchołka $u, v \in V$ istnieje $u - v$-ścieżka.

Podgraf

Podgrafem grafu $G = (V, E)$ jest dowolny graf $H = (V', E')$ taki, że $V' \subseteq V$ i $E' \subseteq E$. Podgraf jest właściwy, jeśli $G \neq H$.

Spójna składowa

Spójna składowa grafu G to dowolny podgraf spójny $H = (V', E')$ grafu G, który jest maksymalny ze względu na zawieranie, tzn. taki, że nie istnieje podgraf spójny H', którego podgrafem właściwym jest H.

Drzewo i las

Graf $G = (V, E)$ jest acykliczny, jeśli nie zawiera żadnego cyklu. Las jest acyklicznym grafem, a drzewo acyklicznym grafem spójnym. Drzewa są spójnymi składowymi lasu, a więc las składa się z drzew.
Drzewo jest najmniejszym grafem spójnym, a więc jeśli chcemy zbudować graf spójny G na zbiorze wierzchołków V, to G musi być drzewem.

Liść

Liść to wierzchołek o stopniu 1. Dowolne drzewo o $n \geq 2$ wierzchołkach zawiera przynajmniej 2 liście.

Most

Most to krawędź, której usunięcie zwiększa liczbę spójnych składowych grafu, ponadto żaden most nie leży na cyklu.

Charakteryzacja drzewa

Niech $G = (V, E)$ będzie n-wierzchołkowym grafem nieskierowanym ($n \geq 1$). Wtedy wszystkie następujące stwierdzenia są równoważne:
1. G jest spójny i acykliczny (G jest drzewem).
2. G jest spójny i ma $n - 1$ krawędzi.
3. G jest acykliczny i ma $n - 1$ krawędzi.
4. Dla każdego $u, v \in V$ w G jest tylko jedna $u - v$-ścieżka.
5. G jest spójny i każda krawędź jest mostem.
6. G nie ma cykli, ale dołożenie jakiejkolwiek krawędzi tworzy cykl.

Graf dwudzielny

Graf $G = (V, E)$ jest dwudzielny wtw, gdy istnieje podział zbioru V na zbiory A i B taki, że dla każdej krawędzi $e \in E$ jeden koniec e należy do zbioru A, a drugi do zbioru B. Podział wierzchołków nie zawsze jest jednoznaczny!
Graf G jest dwudzielny wtw, gdy nie zawiera cyklu o nieparzystej długości.

Lemat o zamkniętej marszrucie

Każda zamknięta marszruta o nieparzystej długości zawiera cykl o nieparzystej długości.

Graf o minimalnym stopniu k

Niech G będzie grafem prostym, w którym każdy wierzchołek ma stopień przynajmniej k. Wówczas G zawiera ścieżkę o długości k. Jeśli $k \geq 2$, to G zawiera cykl o długości przynajmniej $k + 1$.

Drzewo rozpinające

Niech $G = (V, E)$ będzie grafem spójnym. Drzewo rozpinające grafu G to podgraf $T = (V, E')$, który jest drzewem. T zawiera wszystkie wierzchołki grafu G.

Las rozpinający

Niech $G = (V, E)$ będzie grafem niekoniecznie spójnym. Las rozpinający grafu G to podgraf $F = (V, E')$, który jest lasem, którego liczba spójnych składowych jest taka sama jak liczba spójnych składowych grafu G.

Minimalne drzewo rozpinające (MST)

Niech $G = (V, E)$ będzie grafem spójnym o nieujemnych wagach na krawędziach, a graf $T = (V, E')$ jego drzewem rozpinającym.
Wagę definiuje funkcja $c : E \to \mathbb{R}_+$. Wtedy wagą drzewa rozpinającego $c(T) = \sum_{e \in E'} c(e)$. Minimalnym drzewem rozpinającym (MST) grafu G jest drzewo rozpinające T o minimalnej wadze.

Algorytmy na znajdowanie MST

Algorytm Kruskala polega na dodawaniu kolejnych krawędzi w taki sposób, aby nie stworzyły one żadnego cyklu.

```
KRUSKAL:
sort(E) wzgledem wagi
T = {}
for i in [1, m]:
    if (T + {e(i)} nie tworzy
        zadnego cyklu):
        T = T + {e(i)}
```

Algorytm Prima polega na dobieraniu najlżejszych krawędzi do grafu T.

```
PRIM:
T = {}
U = {1} (dowolny wierzcholek G)
while (U != V):
    e = najlzejsza krawedz (u, v),
        taka ze u jest z U,
        a v jest z V-U
    T = T + {(u, v)}
    U = U + {v}
```

Algorytm Boruvki polega na dodawaniu najlżejszych krawędzi do T, łączeniu ich w superwierzchołki i wykonywaniu algorytmu od początku.

```
BORUVKA:
T = V
while (T != MST):
    wybierz najmniejsza krawedz
    z najmniejsza waga i dodaj
    ja do zbioru E'

    gdy jest wiecej niz jedna
    spojna skladowa, polacz
    wszystkie wierzcholki w
    superwierzcholki i wykonaj
    algorytm od poczatku
```

Skojarzenie (matching)

Niech $G = (V, E)$ będzie grafem spójnym. Skojarzenie grafu G to dowolny pozdbiór krawędzi $M \subseteq E$ taki, że żadne dwie krawędzie z M nie mają wspólnego końca.

Największe skojarzenie

Skojarzenie największe grafu G to skojarzenie o maksymalnej liczbie krawędzi.

Wierzchołki skojarzone, wolne

Niech $G = (V, E)$ będzie grafem spójnym, a M jakimś skojarzeniem w G. Wierzchołek $v \in V$ jest skojarzony w M, jeśli jest końcem jakiejś krawędzi z M. Wierzchołek $v \in V$ jest wolny/nieskojarzony, jeśli żadna krawędź z M nie jest z nim incydentna.

Ścieżka alternująca

Ścieżka P w grafie G jest alternująca (względem M) jeśli krawędzie na P na przemian należą i nie należą do M.

Ścieżka powiększająca

Ścieżka P w grafie G jest powiększająca (względem M), jeśli jest alternująca względem M i jej końce są nieskojarzone (w M).

Skojarzenie doskonałe/pełne

Skojarzenie doskonałe/pełne grafu G to skojarzenie, w którym każdy wierzchołek z V jest skojarzony.

Cykl alternujący

Cykl C w grafie G jest alternujący względem M jeśli krawędzie na C na przemian należą i nie należą do M.

Twierdzenie Berge'a

Skojarzenie M grafu G jest największe wtw, gdy G nie zawiera ścieżki powiększającej względem M.

Sąsiedztwo wierzchołków

Niech $G = (V, E)$ będzie grafem a $W \subseteq V$ podzbiorem wierzchołków. Sąsiedztwo W oznaczane jako $N(W)$ definiujemy jako zbiór $\{v \in V : \exists (w \in W)\ \{v, w\} \in E\}$.

Warunek Halla

Niech graf $G = (A \cup B, E)$ będzie grafem dwudzielnym.
Dla każdego $A' \subseteq A$ zachodzi $|N(A')| \geq |A'|$ oraz dla każdego $B' \subseteq B$ zachodzi $|N(B')| \geq |B'|$.

Skojarzenie doskonałe w grafie dwudzielnym

Graf dwudzielny G zwiera skojarzenie doskonałe wtw, gdy spełniony jest w nim warunek Halla.