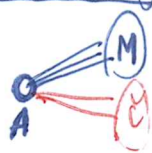


Intro: - co je DM, účel kursu, přednáška + cvičení, nahrávky + stream

- <https://uj.uow.ac.ukuka/dm>

Matfyzici v traumati: 6 lidí, telace "znat se" (symetrická) $\rightarrow \exists \Delta$ nebo $\triangle$ } vizualizace (graf)

Resem:



$$|M| + |C| = 5 \Rightarrow |M| \geq 3 \vee |C| \geq 3 \text{ (обучен)}$$

buď mezi M je $\Rightarrow \Delta$ s A symetrický
 nebo same $\Rightarrow \Delta$ unitární M

Souvislosti: Rannseyory věty, "neexistuje dokonalý chaos"

Nekonečně mnoho prvočísel (à la Euklides) - důkaz sporem

- kdyby jich bylo konečně mnoho, můžeme je vyjmenovat: $p_1 < p_2 < \dots < p_n$

- nymí máme $X = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$

- $x > p_n \Rightarrow x \neq p_i$ pro všechna $i \Rightarrow x$ není prvočíslo

- tedy $\exists i: p_i \mid x$... to ale není možné, protože $x \bmod p_i = 1$ $\downarrow$
 detektivní remota

Součet $S_n = 1 + 2 + \dots + n$ - značení: $S_n = \sum_{i=1}^n i$ ← aritmetická řada (spec. případ)
- okrajové případy: $S_0 = 0$, $S_1 = 1$ ← co je $\mathbb{N}$?

- okrajové případy: $S_0 = 0$, $S_1 = 1$

- přeuspořádání: $S_n = 1 + 2 + \dots + (n-1) + n$

$$S_n = n + (n-1) + \dots + 2 + 1$$

$$2S_n = (n+1) + \dots + (n+1) = \frac{n(n+1)}{2} = \frac{n^2 + n}{2}$$

- můžeme dokázat indukci ... obecný princip: $\varphi(0) \wedge (\forall n (\varphi(n) \Rightarrow \varphi(n+1))) \Rightarrow \forall n \varphi(n)$

$$- \varphi(n): \underbrace{1 + \dots + n}_{S_n} = \frac{n(n+1)}{2}$$

$$- \varphi(0): 0 = \frac{0.1}{2} \checkmark$$

- $n \rightarrow n+1$: viene $S_n = \frac{n(n+1)}{2}$

$$\text{Chceme } S_{n+1} = \frac{(n+1)(n+2)}{2}$$

$$S_{n+1} = S_n + (n+1) = \frac{n(n+1) + 2(n+1)}{2}$$

$$\frac{n(n-1)}{2} = \frac{(n-1)(n-2)}{2} \quad \text{Q.E.D.}$$

Součet $g_n = q^0 + q^1 + \dots + q^{n-1}$ ← geometrická řada

- fokus: $q=10$

$$\begin{array}{ccccccc} 10^0 & + & 10^1 & + & 10^2 & + & \dots + 10^{n-1} \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ 1 & & 10 & & 100 & & 10 \underbrace{\quad 0}_{n-1} \end{array} = \underbrace{1 \dots 1}_n = \frac{9 \dots 9}{9} = \frac{10^n - 1}{9}$$

- pro $q=3$ trojková soustava ... $\frac{3^n - 1}{2}$

- hipoteza: $g_n = \frac{q^n - 1}{q - 1}$... pokud $q \neq 1$... jinak $g_n = n$

- můžeme dokázat indukci:

• $g_0 = 0 = \frac{q^0 - 1}{q - 1} = 0 \checkmark$

• $n \rightarrow n+1: g_{n+1} = g_n + q^n = \frac{q^n - 1}{q - 1} + q^n = \frac{q^n - 1 + q^n(q - 1)}{q - 1} = \frac{q^{n+1} - 1}{q - 1} \checkmark$

jiný způsob:
 $g_n = q^0 + q^1 + \dots + q^{n-1}$
 $q \cdot g_n = q^1 + q^2 + \dots + q^n$
 $\Rightarrow (q-1)g_n = q^n - 1$

$q^{n+1} - q^n$

- trik: jelikož se jedná o rovnost polynomů, stačí, když platí pro dost různých q (my jich máme ∞)

Součet $\square_n = 1^2 + 2^2 + \dots + n^2$

- malé případy: $\square_0 = 0, \square_1 = 1, \square_2 = 5, \square_3 = 14 \dots$ pattern?

- hypotéza: je to kubický polynom, tedy $\square_n = ax^3 + bx^2 + cx + d$ pro nějaké a, b, c, d

- pak: $\square_0 = 0 \Rightarrow d = 0$

$\square_1 = 1 \Rightarrow a + b + c = 1$

$\square_2 = 5 \Rightarrow 8a + 4b + 2c = 5$

$\square_3 = 14 \Rightarrow 27a + 9b + 3c = 14$

$c = \frac{1}{6}$

$b = \frac{1}{2}$

$6a + 2b = 3$

$6a = 2 \rightarrow a = \frac{1}{3}$

$24a + 6b = 11$

- mělo by tedy být $\square_n = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = \frac{n(n+1)(n+2)}{6}$

- ověříme indukci (D.č.)

Platíme pomocí 3Kč a 5Kč - které částky jdou zaplatit?

"indukce s prefixem"

0 ✓	8 ✓
1 ✗	9 ✓
2 ✗	10 ✓
3 ✓	11 ✓
4 ✗	12 ✓
5 ✓	13 ✓
6 ✓	14 ✓
7 ✗	15 ✓

odd.
od 11 dál můžeme
indukovat

Princip: $\varphi(n_0) \& (\forall n \geq n_0: \varphi(n) \Rightarrow \varphi(n+1))$

$\Rightarrow \forall n \geq n_0 \varphi(n)$

• $\varphi(n)$ = "pro 8 Kč n to jde"
 $n_0 = 10$

Existence zápisů ve dvojkové soustavě - každé $n \geq 0$ jde zaplat jako součet různých mocnin dvojky

Silná indukce: $\varphi(0) \& (\forall n (\forall k < n \varphi(k)) \Rightarrow \varphi(n)) \Rightarrow \forall n \varphi(n)$

• $\varphi(n)$ = "n lze zaplat"

• $\varphi(0) \checkmark$ (prázdný součet)

• n : nechť 2^i je nejvyšší mocnina 2 menší rovná n

$n' = n - 2^i \dots n' < n \Rightarrow \varphi(n')$ platí ... vezmeme zápis n' a přičteme 2^i

• zesílení úvahy: zápis existuje právě jeden (ať na pořadí sčítanců)

- každý zápis n musí obsahovat 2^i ,
 neboť $2^0 + \dots + 2^{i-1} = 2^i - 1 < n$

- stačí využít jednoznačnost zápisu $n' \in \mathbb{N}$

nemůže ale obsahovat 2^i ?
 kdyby ano, pak $n' \geq 2^i$
 a tedy $n \geq 2^i + 2^i = 2^{i+1}$
 $\Rightarrow 2^i$ nebyla největší

Dělitelnost

$a \mid b \equiv \exists c: b = ac$ ☺ 1|b pro všechna b
 $a \mid 0$ pro všechna a (0|0 platí)
-3|6 ... obecně funguje pro $\mathbb{Z}$

(3)

$$a \mid b \Leftrightarrow a \bmod b = 0$$

Kongruence $a \equiv b \pmod{n} \Leftrightarrow n \mid a - b \Leftrightarrow a \bmod n = b \bmod n$

"chová se jako rovnost" - $a \equiv a$, $a \equiv b \Leftrightarrow b \equiv a$, $a \equiv b \& b \equiv c \Rightarrow a \equiv c$ (R, S, T)

$a \equiv a'$, $b \equiv b' \Leftrightarrow a + b \equiv a' + b'$... sečteme kongruence nebo vynásobíme výraz
za kongruentní

$$\Leftrightarrow a - b \equiv a' - b'$$

$$\Rightarrow ab \equiv a'b' \text{ --- ale pozor, tedy } \Leftarrow \text{ obecně neplatí!}$$

modulo 4: $2 \cdot 2 \equiv 2 \cdot 4$, ale $2 \not\equiv 4$

↓
představa
ciferníku hodin

Skoumáme $n^2 \bmod 4$

n	n^2	$n^2 \bmod 4$	$\bmod 8$
0	0	0	0
1	1	1	1
2	4	0	4
3	9	1	1
4	16	0	0
5	25	1	1
6	36	0	4
7	49	1	1

→ pro n sudé je $4 \mid n^2$

pro n liché je $n^2 \bmod 4 = 1$... tedy $n^2 \equiv 1 \pmod{4}$

• lze indukovat

• nebo také $(2n)^2 \equiv 4n^2 \equiv 0 \cdot n^2 \equiv 0$

$$(2n+1)^2 \equiv 4n^2 + 4n + 1 \equiv 0 + 0 + 1 \equiv 1$$

• co mod 8? $(2n+1)^2 \equiv 4n^2 + 4n + 1 \equiv 0 + 1$
 $\underbrace{4n(n+1)}_{\text{sudé}}$

Celočíslné kořeny polynomů

uvažujme $f(x) = 4x^5 - 12x^4 - 5x^3 + 15x^2 + x - 3$... jaké má kořeny?

... to je obecně těžké (Galoisova věta), ale celočíslné jsou najít snadno

Obecně: uvažujme $f(x) = \sum_{i=0}^n a_i x^i$ je polynom s celočíslnými koeficienty $a_0 - a_n$

Pokud x je kořen: $\sum_{i=0}^n a_i x^i = 0$... uvažme mod $|x|$

$x \neq 0$ } $x=0$
se pozná
snadno ($a_0=0$)

$$\hookrightarrow \underbrace{a_0 x^0 + a_1 x^1 + \dots + a_n x^n}_{\text{jsou dělitelné } x, \text{ tedy } \equiv 0} \equiv a_0$$

Z toho $a_0 \equiv 0 \pmod{x}$

Jinými slovy $x \mid a_0$

... takže stačí prozkoumat konečně mnoho dělitelů a_0

V našem případě $a_0 = -3$... kandidáti jsou

+1	✓	$4 - 12 - 5 + 15 + 1 - 3 = 0$
-1	✓	$-4 - 12 + 5 + 15 - 1 - 3 = 0$
+3	✓	
-3	✗	

Vylepšení: racionální kořeny (pro celočíselné koeficienty)

(4)

Nechť $\sum_i a_i \left(\frac{p}{q}\right)^i = 0$... vynásobíme obe strany $q^n \rightarrow \sum_i a_i p^i q^{n-i} = 0$

Nyní mod p : $p \nmid a_0$
 mod q : $q \nmid a_n$ } konečně mnoho kandidátů
 V našem případě: $p \in \{\pm 1, \pm 3\}$, $q \in \{\pm 1, \pm 2, \pm 4\}$
 Funguje $1/2$ a $-1/2$... a to už je 5 kořenů
 $\Rightarrow$ jsou všechny reálné

Jedničková čísla (a.k.a. repunits)

$J_n = \underbrace{1 \dots 1}_n$... Platí pro nějaké n : $2017 \mid J_n$?

• zobecníme pro dělitelnost jakýmkoliv m

• malé případy:

m	J_n
1	1
2	x
3	111
4	x
5	x

m	J_n
6	x
7	111 111 = 111 · 1001
8	x
9	111 111 111
10	x

7 · 11 · 13

m	J_n
11	11
13	111 111
17	?

číslo je m dělitelné 2 nebo 5, evidentně to nejde

• hypotéza: pro všechna ostatní n to jde

• uvažujeme všechna $J_n \bmod m$... konečně mnoho zbytků $\Rightarrow$ princip holubníku

takže $\exists i > j: J_i \equiv J_j \pmod{m}$

$\Rightarrow J_i - J_j \equiv 0 \pmod{m}$

číslo tvaru $\underbrace{1 \dots 1}_{i-j} \underbrace{0 \dots 0}_j = J_{i-j} \cdot 10^j$

} jelikož m není dělitelné 2 ani 5, máme $m \mid J_{i-j}$ $\square$

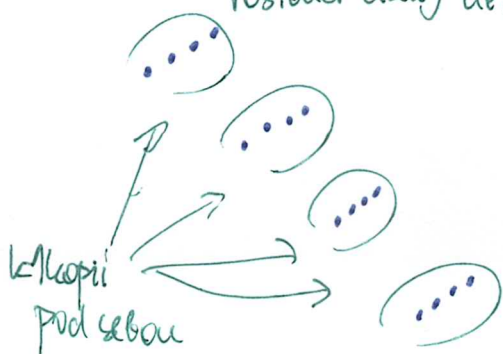
Monotónní ^{pod}postupnosti

Dostaneme postupnost $x_1 \sim x_n \in \mathbb{R}$ různých čísel

Jak dlouhá rostoucí/klesající vybraná podpostupnost v ní musí být?

Pokus o konstrukci dlouhé posl. bez dlouhých monotónních pp.:

rostoucí úseky délky $r-1$



- neobsahuje rostoucí pp. délky r
- ani klesající pp. délky k
- má celkem $n = (r-1)(k-1) + 1$ prvků

Ukažme, že je nejdelší možná.

Věta (Erdősöva - Szekeresöva): Postoupnost dölky (alespon) $(r-1)(k-1)+1$ obsahuje rostoucí pp. dölky r nebo klesající pp. dölky k

(5)

Dle: pro $x_1 \dots x_n$

def. (a_i, b_i) , kde $a_i :=$ dölka nejdelší rostoucí pp. končící prvkem x_i
 $b_i :=$ — " — klesající — " —

Sporem: pokud $\exists$ dost dlouhá pp., je vždy $1 \leq a_i \leq r-1$, $1 \leq b_i \leq k-1$
 $\Rightarrow (r-1)(k-1)$ možných hodnot dvojice, ale $n > (r-1)(k-1)$

Tedy podle principu holubůvku $\exists i, j$: $i < j$, $(a_i, b_i) = (a_j, b_j)$

To ale není možné: Buď $x_i < x_j$, ale pak $a_j \geq a_i + 1$
 nebo $x_i > x_j$, — " — $b_j \geq b_i + 1$ $\searrow$

Přidávky

- Neexistují dvě množiny 2 lišící se jen pořadím cifer.
- Wilsonova věta: n je prvočíslo $\Leftrightarrow (n-1)! + 1$ je dělitelné n
- Čínská zbytková věta (díky holubůvku)
- 3 doměty a 3 studny

KOMBINATORIKA

- KOLIK JE OBJEKTŮ DANÉHO DRUHŮ?

Přklady:

① # slov o 8 písmenech z $\{a-z\} = 26^8 \leftarrow$ 26 znaků angl. abecedy 2 písmenka: 26^2  pak pokračujeme indukcí

② ... všechna písmena různá: $26 \cdot 25 \cdot 24 \cdot \dots \cdot 19 = 26^{\underline{8}}$
 8 členů

③ # přesmyček slova KRUTOVLADCE = $11^{\underline{11}} = 11!$ $\leftarrow$ jiný lepší příklad: ZPRACHNIVĚLOST ^{27 znaků}
 či ZUBOLEKARSTVI

④ # přesmyček slova JEZEVEC ... nejdrůve JEZEVEC = $7!$ (nejdelší rozumná bez opakování)
 • $3! = 6$ způsobů, jak E-čka očíslovat $\Rightarrow$ #přesmyček $\cdot 3! = 7!$
 $\Rightarrow$ #přesmyček = $\frac{7!}{3!}$

$\hookrightarrow$ technika počítání dvěma způsoby

př. ⑤ # rozestavení 8 věží na šachovnici 8×12 , aby se neohrožovaly. ⑥
 ... v každém sloupci právě 1 věž: posloupnost $r_1 - r_8 \in \{1-12\}$
 (vlastně slovo nad 12-znakovou abecedou)
 a všechna r_i jsou navzájem různá $\rightarrow 12^8$ možností

Díjný pohled: hledám funkce, které přiručují sloupcům řádky: $f: \{1-8\} \rightarrow \{1-12\}$
 neboli zobrazení

⑥ co kdyby věží bylo jen 5?

Nejprve si je očíslováme: 8^5 možností, jak vybrat sloupce
 12^5 možností, jak nezávisle vybrat řádky } $8^5 \cdot 12^5$ rozestavení
 A pak vydělíme $5!$ na konkrétních, prvcích nezávislých

Zobecníme: # k -znakových slov z n -znakové abecedy = n^k
 ... bez opakování = $n^{\underline{k}}$ co se stane pro $k=0, n=0$,
 # pořadí abecedy (permutací) = $n! = n^{\underline{n}}$ připadne $k > n$?
 # neuspořádaných k -tic vybraných z n prvků = $\frac{n^{\underline{k}}}{k!}$
 # funkcí z $\{1-k\}$ do $\{1-n\}$
 # prostých funkcí
 # bijekcí z $\{1-n\}$ do $\{1-n\}$
 ↑ také se jim říká permutace

Princip kódování: Kolik podmnožin má množina $1 \dots n$? (malý případ: $n=2, n=3$)

Podmnožinu popíše charakteristickou posloupností $c_1 - c_n \in \{0,1\}$
 $\uparrow A \subseteq \{1-n\}$ $\uparrow c_i = \begin{cases} 0 & \text{if } i \notin A \\ 1 & \text{if } i \in A \end{cases}$

podmnožin = # posloupností = 2^n Příklad pro $n=2$: $00 \rightarrow \emptyset, 01 \rightarrow \{1\}, 10 \rightarrow \{2\}, 11 \rightarrow \{1,2\}$
 znáčení: $2^X = \mathcal{P}(X)$
 vlastně mám bijekci mezi podmnožinami a posloupnostmi $\Rightarrow$ je jich stejně

Díjný pohled: charakt. funkce $\{1-n\} \rightarrow \{0,1\}$

Argument bijekci: Necht $\mathcal{Y} := \{A \subseteq \{1-n\} \mid |A| \text{ je sudý}\}$ notace: $[n] = \{1-n\}$
 a $\mathcal{X} := \{A \subseteq \{1-n\} \mid |A| \text{ je lichý}\}$ "Sudé a liché podmnožiny"

Ukažeme bijekci mezi $\mathcal{Y}$ a $\mathcal{X} \Rightarrow |\mathcal{Y}| = |\mathcal{X}| \Rightarrow$ jelikož $|\mathcal{Y}| + |\mathcal{X}| = 2^n$, musí být obě 2^{n-1}

zvolíme $a \in [n]$, množině X přiřadíme $X \Delta \{a\} = \begin{cases} X \cup \{a\} & \text{pokud } a \notin X \\ X \setminus \{a\} & \text{pokud } a \in X \end{cases}$
 ↑ symetrický rozdíl

Pro liché n funguje jako bijekce doplněk. Ale co pro sudé n ?

→ sudé množině přiřadím lichou a naopak
 invenzi sama k sobě $\Rightarrow$ je to bijekce mezi $\mathcal{Y}$ a $\mathcal{X}$

Počítáme k -prvkové podmnožiny $[n]$ - to jsou vlastně neuspořádané k -tice z $[n]$

$\Rightarrow$ je jich $\frac{n^{\underline{k}}}{k!}$ ← takže značíme $\binom{n}{k}$ " n nad k " - kombinační číslo
 též značíme jako $\frac{n!}{k!(n-k)!}$ což je totéž neboli binomický koeficient
 (ale pozor na případ $k > n$)

V char. posloupnostech: posl. 0/1 délky n , v nichž je právě k jedniček
 to by také šlo počítat jako přesný slova $\underbrace{1-1}_k \underbrace{0-0}_{n-k}$
 což je toto

Vlastnosti kombinačních čísel

$$\binom{n}{0} = 1 \quad \binom{n}{1} = n \quad \binom{n}{2} = \frac{n(n-1)}{2} \quad \binom{n}{n} = 1 \quad \binom{n}{n-1} = n \rightarrow \text{obecně } \binom{n}{n-k} = \binom{n}{k}$$

$$\sum_{k=0}^n \binom{n}{k} = 2^n \quad \text{rozepisujeme (pod) množiny podle \# prvků}$$

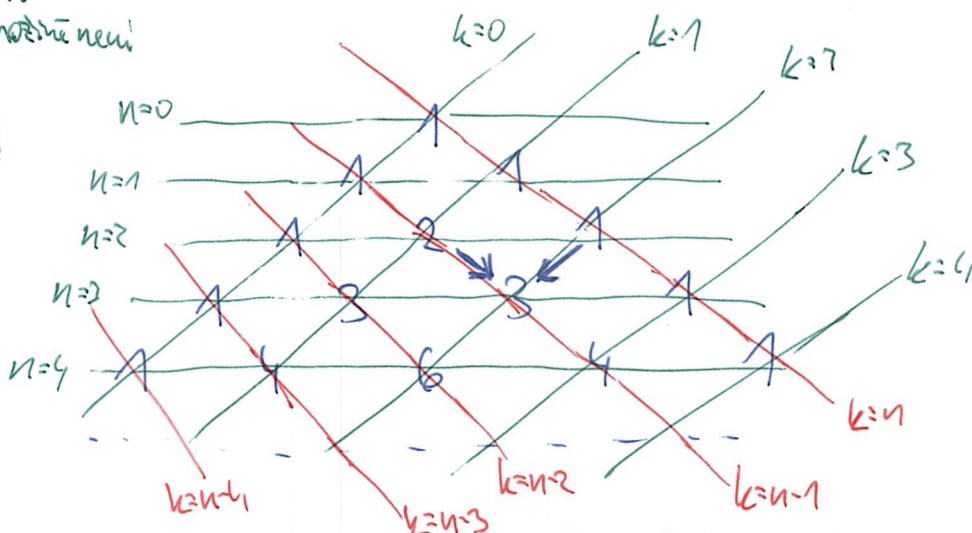
počítáme prvky, co nejsou v množině

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

prvek n v podmnožině není je tam

kombinatorický argument (šloby též upočítat z definice)

Pascalův Δ (tabulka $\binom{n}{k}$)



Vše je vidět zde

Binomická věta: $\forall x, y \in \mathbb{R} \quad \forall n \in \mathbb{N}: (x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k$ } také můžeme chápat jako rovnost polynomů ve 2 proměnných

Důkaz: Roznásobujeme $(x+y)(x+y) \dots (x+y) = \underbrace{xxx \dots x + xx \dots xy + \dots + y \dots y}_{n \text{ závorek}}$
 $\forall$ člen si z $\forall$ závorek vybere x nebo y $\Rightarrow 2^n$ členů, ale všechny jsou tvaru $x^{n-k} y^k$

Kolik členů je tvaru $x^{n-k} y^k$? Máme z n závorek k-krát vybrat y $\rightarrow \binom{n}{k}$.

Otázka: Jak vypadá multinomial věta? Treba $(x+y+z)^n$?

Příklady: $2^n = (1+1)^n = \sum_{k=0}^n \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^n \binom{n}{k}$... už známe

$$0 = (1-1)^n = \sum_{k=0}^n \binom{n}{k} 1^{n-k} (-1)^k = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \dots + (-1)^n \binom{n}{n}$$

pro n > 0 sudých a lichých podmnožin je stejné

Další zajímavá číselní?

Rozklady na součet: kolika způsoby lze n zapsat jako $x_1 + x_2 + \dots + x_k$ ($\forall x_i \in \mathbb{N}$)
 na pořadí nám záleží

$$5 = \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \quad | \quad \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \quad | \quad \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \quad | \quad \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \quad | \quad \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet} \overset{1}{\bullet}$$

$$5 = 2 + 0 + 1 + 2 + 0$$

Umísťujeme n nerozlišitelných kuliček

do k rozlišitelných (očíslovaných) přihrádek.

kódování: posloupnost $\bullet$ a $|$ (krajní nepočítám) $\Rightarrow n+k-1$ pozic, k z nich je $|$
 $\Rightarrow$ lze vybrat $\binom{n+k-1}{k-1}$ způsobů.