# Rocnikovy Project

**Subfactorials to power**

Author:

Artsiom Shcherba

# Obsah

# 1 Anotacia

Bolo zavedené a preskúmané nový matematický pojem, ako je subfaktoriál na mocninu k (ďalej len $!^k n$). Počas výskumu bol odvodený vzorec na výpočet tejto hodnoty pre fixné sekvencie a odhadnutá horná hranica celkovej hodnoty, boli uvedené odhady pre k a predstavený algoritmus na zostavenie neusporiadaných permutácií pre viaceré sekvencie.

Výskum skúma a rozvíja oblasť kombinatorických úloh o neusporiadaných permutáciách. Bolo nájdené praktické využitie na riešenie matematických problémov, vrátane tých, ktoré sa používajú na matematických výskumných súťažiach, a zároveň bolo navrhnuté praktické uplatnenie, ktoré môže podporiť rozvoj oblasti kryptografie.

# 2 Úvod

Počas výskumu bude použitý vzorec inklúzií a exklúzií, ako aj vzorec pre počet neusporiadaných permutácií pre n čísel (alebo $!n$). Podrobnosti o nich nájdete v odkazoch na zdroje.

**Definícia:**

$!^k n$ - počet možností zostaviť k permutácií z n čísel tak, aby boli navzájom neusporiadané a zároveň neusporiadané vzhľadom na pôvodne fixovanú permutáciu $p_1$.

**Poznámka:**

V skutočnosti by formálnejšia a intuitívnejšia definícia bola nasledovná:

$!^k n'$ - počet možností zostaviť k+1 permutácií z n čísel tak, aby boli navzájom neusporiadané

Avšak aby klasický subfaktoriál bol špeciálnym prípadom pre $k = 1$, bolo zvolené také definovanie, kde jedna zo sekvencií je fixovaná (teda hľadáme počet možností usporiadať prvky k permutácií bez zmeny poradia prvkov prvej permutácie). To však nespôsobuje problémy, pretože vzorec na výpočet podľa tejto poznámky môžeme odvodiť nasledovne:

$n!*!^k n'$ (pretože zároveň zvažujeme všetky možné permutácie prvej sekvencie).

**Odporúčanie:**

V situácii, keď ste zabudli nejakú definíciu alebo si ju chcete podrobnejšie preštudovať na príklade, môžete sa obrátiť na bod 8, kde sú uvedené a rozobraté všetky definície.

# 3 Obmedzenia pre k

Formálnejšie možno tento bod chápať ako: hodnoty k, pri ktorých $!^k n > 0$. Na zodpovedanie tejto otázky zavedieme 2 vety.

**Veta 1**

Tvrdenie: $!^k n = 0$ pre $k \geq n$.

Dôkaz: Máme n pozícií pre čísla. Ak existuje $k+1$ ($k \geq n$) permutácia, potom podľa Dirichletovho princípu nejaké číslo $a$ bude umiestnené na jednej pozícii aspoň v 2 permutáciách, nech je to $p_i$ a $p_j$. Ale vtedy $p_i$ nie je neusporiadaním pre $p_j$, čo je v rozpore s definíciou.

**Veta 2**

Tvrdenie: $!^k n > 0$ pre $0 < k < n$.

Dôkaz: Všimnime si, že postupnosť získaná cyklickým posunom doprava o $h$ pôvodnej postupnosti je neusporiadaním voči pôvodnej (ak $h$ nie je väčšie ako počet prvkov v postupnosti). Tým môžeme získať k navzájom neusporiadaných permutácií cyklickým posunom pôvodnej postupnosti doprava o $1, 2, ..., k$.

# 4 Špeciálny prípad postupností

Zvážme prípad $k = 2$ a $n = 4$.

$p_q$ - jedna z permutácií.

| $p_1$ | $p_2$ | $p_3$ |
|---|---|---|
| 1234 | 2143 | 3421, 3412, 4321, 4312 |
| 1234 | 2341 | 3423, 4123 |
| 1234 | 2413 | 3142, 4321 |
| 1234 | 3412 | 2143, 2341, 4123, 4321 |
| 1234 | 3421 | 2143, 4312 |
| 1234 | 3142 | 2413, 4321 |
| 1234 | 4312 | 2143, 3421 |
| 1234 | 4321 | 2413, 2143 3412, 3142 |
| 1234 | 4123 | 2341, 3412 |

Pri zvažovaní tohto príkladu môžeme vidieť, že od predchádzajúcich postupností závisí počet možností na zostavenie aktuálnej. Napríklad prípady 1 a 2, kde v prvom prípade sú 4 možnosti na zostavenie $p_3$, zatiaľ čo v druhom prípade sú iba 2 možnosti. Tento dôsledok je zaujímavý a vytvára cieľ pochopiť, pri akej závislosti medzi permutáciami bude možné zostaviť určitý počet neusporiadaných permutácií.

# 5 Dovod dynamického počtu permutácií a riešiteľnosť

Pozrime sa bližšie na to, že pre permutácie 1234 a 2143 existujú 4 možnosti na zostavenie ďalšej, zatiaľ čo pre 1234 a 2341 len 2.
Je zrejmé, že na výber permutácie stačí vybrať pozíciu pre každý prvok, ktorých celkový počet (na dodržanie vlastnosti neusporiadaní) je $n - k$. Pre každý prvok a jeho pozíciu zapíšme do tabuľky hodnotu 1, ak môže byť tento prvok umiestnený na túto pozíciu, inak 0. Dostaneme tabuľky 1,2

Potom počet spôsobov, ako vybrať nasledujúcu permutáciu, je rovný počtu spôsobov, ako zvoliť $n$ jednotiek tak, aby v každom riadku a v každom stĺpci bola vybraná presne jedna jednotka (v prvom prípade 4 možnosti, v druhom 2). To je možné vypočítať napríklad pomocou dynamického programovania za $O(n^3)$. Tento prístup však neumožňuje odvodiť všeobecný vzorec (iba za exponenciálny čas). Preto sa ďalej budeme zaoberať odvodením vzorca pre fixné

| Elements | pos 1 | pos 2 | pos 3 | pos 4 |
|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 1 |
| 2 | 0 | 0 | 1 | 1 |
| 3 | 1 | 1 | 0 | 0 |
| 4 | 1 | 1 | 0 | 0 |

Tabuľka 1: $p_1 = 1234, p_2 = 2143$

| Elements | pos 1 | pos 2 | pos 3 | pos 4 |
|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 0 |
| 2 | 0 | 0 | 1 | 1 |
| 3 | 1 | 0 | 0 | 1 |
| 4 | 1 | 1 | 0 | 0 |

Tabuľka 2: $p_1 = 1234, p_2 = 2341$

postupnosti s cieľom jeho ďalšieho zovšeobecnenia na všeobecný vzorec.

# 6 Odvodenie vzorca pre fixné postupnosti

V tomto bode budeme hľadať počet možností, ako zostaviť jednu permutáciu z n čísel, ak máme k ďalších permutácií, ktoré sú navzájom neusporiadané, tak, aby bola neusporiadaním pre všetky z nich.

Inými slovami, fixujeme k postupností.

## 6.1 Myšlenka odvodenia vzorca pre fixné postupnosti

Zistíme, koľko je možné zostaviť neusporiadaní pre k fixných permutácií, ktoré sú navzájom neusporiadané, pomocou vzorca inklúzií a exklúzií. Počet bude:

$n! - a_2 * (n-1)! + a_3 * (n-2)! ... + (-1)^n * (n-n)!$

kde $a_i$ je počet spôsobov, ako vybrať i čísel a umiestniť ich na všetky možné pozície tak, že ak umiestnime číslo x na pozíciu j, potom v niektorej z predchádzajúcich postupností x už stojí na pozícii j. Pri tom pre akékoľvek 2 čísla nemôže byť vybraná jedna pozícia.

Najprv predpokladáme, že $a_i = C_n^i * k^i$, pretože vyberáme i čísel a pre každé vyberáme ľubovoľnú z k pozícií. Tento vzorec však môžeme ľahko vyvrátiť. Na to zvážme príklad:

$k = 2, p1 = 1, 2, 3, p2 = 3, 1, 2$. Zvážme dvojicu 1 a 2. Keďže počítame všetky možnosti, zahrnieme aj prípady, keď 2 je na pozícii 2 a 1 je tiež na pozícii 2, avšak nemôžeme umiestniť 2 čísla na jednu pozíciu. Preto musíme odvodiť vzorec na výpočet $a_i$. Začneme s $i = 2$.

## 6.2 Odvodenie vzorca pre $a_2$

**Definícia**

i-prienik pre množinu B je i čísel z množiny B, ktoré sa nachádzajú na rovnakej pozícii vo svojej permutácii.

$h_i$ je počet všetkých i-prienikov pre vybranú množinu. Zvážme príklad:

$n = 4, k = 3, p_1 = 1, 2, 3, 4, p_2 = 2, 1, 4, 3, p_3 = 3, 4, 1, 2$. Potom pre trojicu čísel 1,2,3 bude 2-prienikom napríklad 1 na pozícii 3 a 3 na pozícii 3. 3-prienikom bude 1,2,3 na pozícii 1. $h_2 = 6$ (1,2 na prvej pozícii; 1,3 na prvej pozícii; 2,3 na prvej pozícii; 1,2 na druhej pozícii; 1,3 na tretej pozícii; 2,3 na štvrtej pozícii), a $h_3 = 1$.

Všimnime si, že pre každé číslo existuje k pozícií. Potom pre každú dvojicu čísel bude $k^2$ možností výberu pozícií. Ak však pre túto dvojicu existuje 2-prienik, tieto pozície nemôžeme vybrať, pretože by potom dve čísla stáli na jednej pozícii. Preto pre každú dvojicu čísel musíme odpočítať počet 2-prienikov. Vzorec pre ľubovoľnú dvojicu bude $k^2 - h_2$

Môžeme nájsť súčet $h_2$ pre všetky možné dvojice čísel, pretože akékoľvek 2 rôzne čísla, ktoré sa nachádzajú v jednom stĺpci (označme ich x a y), budú 2-prienikom pre množinu $x, y$. A keďže podľa definície sú akékoľvek 2 čísla v stĺpci rôzne, počet 2-prienikov pre ľubovoľnú množinu bude $n * C_k^2$.

Teda:

$a_2 = C_n^2 * k^2 - n * C_k^2$

## 6.3 Odvodenie vzorca pre $a_3$

Všimnime si, že ak pre nejakú množinu platí $h_2 = 0$, bude existovať $k^3$ spôsobov, ako zvoliť pozície pre čísla tejto trojice. Zvážme, ako sa počet spôsobov mení so zvyšujúcou sa hodnotou $h_2$. Uveďme to na príklade: Nech máme množinu 1, 2, 3. Pre 2-prienik čísel 1 a 2 bude k spôsobov, ako umiestniť číslo 3. To znamená, že za každý 2-prienik musíme odpočítať k možností. Avšak môže nastať prípad, keď existuje 3-prienik. V takom prípade spočítame možnosť, že všetky 3 čísla stoja na pozícii 3-prieniku $C_3^2$-krát, keď by sme ich mali spočítať len raz. Preto musíme za každý 3-prienik pripočítať $C_3^2 - 1$. Teraz vypočítajme súčet $h_2$ a $h_3$. Pre $h_2$ môžeme na začiatku zvoliť $C_k^2 * n$ možností 2-prienikov. A pre každú takúto možnosť bude $C_{n-2}^{3-2}$ možností zvoliť tretie číslo pre množinu obsahujúcu tento 2-prienik. Pre 3-prieniky bude existovať $C_k^3 * n$ možností 3-prienikov. Tým získame konečný vzorec:

$a_3 = C_n^3 * k^3 - k * n * C_k^2 * C_{n-2}^{3-2} + n * C_k^3 * (C_3^2 - 1)$

## 6.4 Odvodenie vzorca pre $a_4$

Základné vzorce a dôsledky boli rozpracované v predchádzajúcich dvoch bodoch, preto sa tu budeme zaoberať iba špecifikami, ktoré sú vlastné pre $a_i$ pri $i \geq 4$.

Najprv zvážme, ako výsledok ovplyvňuje 4-prieniky. Všimnime si, že keď budeme k výsledku pridávať možnosti spočítané viackrát za každé 3-prieniky (teda možnosti, keď 3 čísla z množiny stoja na jednej pozícii), spočítame možnosť, keď 4 čísla stoja na jednej pozícii, $C_4^3$-krát (za každé 3-prieniky), hoci táto možnosť by mala byť spočítaná iba raz. Znamená to, že za každý 4-prienik musíme od výsledku odpočítať $C_4^3 - 1$.

Teraz si všimnime, že existuje ďalší faktor, ktorý ovplyvňuje výsledok: Ak máme 2 rôzne 2-prieniky, ktorých zjednotenie prvkov je podmnožinou danej množiny, možnosť zvoliť prvky

týchto 2-prienikov na týchto pozíciách bude spočítaná dvakrát namiesto raz.

Pre názornosť zvážme dva príklady z nami preštudovaného špeciálneho prípadu.

| $p_1$ | $p_2$ | $p_3$ |
|---|---|---|
| 1234 | 2143 | 3421, 3412, 4321, 4312 |
| 1234 | 2341 | 3423, 4123 |

Zvážme prvý prípad: Vezmime množinu $1, 2, 3, 4$. Potom možnosť, že 1 je na pozícii 1, 2 na pozícii 1, 3 na pozícii 3, a 4 na pozícii 3, bude spočítaná 2-krát (za 2-prienik na pozícii 1 a za 2-prienik na pozícii 3), hoci by mala byť spočítaná iba raz. Okrem tohto prípadu existujú aj takéto možnosti:

1,2 na pozícii 1; 3,4 na pozícii 4

1,2 na pozícii 2; 3,4 na pozícii 3
1,2 na pozícii 2; 3,4 na pozícii 4

To znamená, že od výsledku bude potrebné odpočítať ešte 4.

Zvážme druhý prípad: Tu bude 2 možnosti zvoliť také 2-prieniky:

1,2 na pozícii 1; 3,4 na pozícii 3

2,3 na pozícii 2; 1,4 na pozícii 4

To znamená, že od výsledku bude potrebné odpočítať ešte 2.

Týmto sme odpovedali na otázku položenú počas rozboru špeciálnych prípadov: Počet možností na zostavenie aktuálnej postupnosti bude závisieť od počtu spôsobov, ako zvoliť takéto 2-prieniky.

Označme také pozície pre danú množinu, kde existuje aspoň i stĺpcov, v ktorých sú zvolené aspoň 2 pozície, ako $t_i$.

Označme $num(t_i)$ ako počet všetkých možných $t_i$.

Potom môžeme odvodiť vzorec pre $a_4$:

$$a_4 = C_n^4 * k^4 - k^2 * n * C_k^2 * C_{n-2}^{4-2} + n * k * C_k^3 * C_{n-3}^{4-3} * (C_3^2 - 1) - n * C_k^4 * (C_4^3 - 1) + num(t_2)$$

## 6.5 Použitie $num(t_i)$ pre všeobecný vzorec fixných postupností

Na začiatok si všimnime, že každé $t_x$ bude spočítané a odpočítané od výsledku presne x-krát (za každý stĺpec), namiesto jedného razu. Ak teda pripočítame k výsledku $num(t_i)$ pre každé $2 \leq i \leq x$, spočítame $t_x$ presne x-1-krát. Tým dosiahneme, že bude odpočítané od výsledku iba raz, čo je požadované. Aby sme teda získali konečný vzorec, musíme k výsledku pripočítať $\sum_{b=2}^{n}(num(t_b))$.

### 6.6 Odvodenie všeobecného vzorca pre fixné postupnosti

Najprv odvodíme vzorec pre $a_i$:
Zvážme a zovšeobecníme všetky údaje, ktoré boli získané v bodoch pre $a_2$, $a_3$, $a_4$:

- Ak $h_2 = 0$, $a_i = C_n^i k^i$
- Za každé 2-prieniky odpočítame od výsledku $k^{i-2}$ (počet spôsobov, ako rozmiestniť ostatné čísla, pričom tieto 2 sú fixované).
- Celkovo bude $C_k^j n$ prienikov ($C_k^j$ v jednom stĺpci, za každý z n stĺpcov).
- Každý j-prienik bude spočítaný $C_{n-j}^{i-j}$-krát (počet spôsobov výberu zostávajúcich prvkov).
- Pre každý j-prienik, ktorý je obsiahnutý v $(j+1)$-prieniku ($j+1 \leq k$), všetky možnosti výberu pozícií prvkov množiny obsahujúcej tento $(j+1)$-prienik budú spočítané $C_{j+1}^j$-krát namiesto raz. Celkový počet výberov pozícií obsahujúcich tento $(j+1)$-prienik bude $k^{i-(j+1)}$. Všimnime si, že najprv pridávame nadbytočne spočítané možnosti a potom ich vylúčime. To znamená, že môžeme použiť vzorec inklúzií a exklúzií.
- Každá množina pozícií $t_i$ bude spočítaná za každý z i stĺpcov, v ktorých sa nachádzajú aspoň 2 pozície. To znamená, že takáto množina bude spočítaná i-krát.

So zohľadnením všetkých prejednaných bodov získame:
$a_i = C_n^i * k^i + \sum_{j=2}^{i}((-1)^{j+1} * n * C_k^j * C_{n-j}^{i-j} * k^{i-j} * (C_j^{j-1} - 1) - \sum_{b=2}^{j} num(t_b))$

Dosadíme získané hodnoty do vzorca.

$n! - a_1 * (n-1)! + a_2 * (n-2)! ... + (-1)^n * (n-n)!$

A získame vzorec pre pevné postupnosti.

$n! - k*n! + \sum_{i=2}^{n}(-1)^i * (C_n^i * k^i + \sum_{j=2}^{i}((-1)^{j+1} * n * C_k^j * C_{n-j}^{i-j} * k^{i-j} * (C_j^{j-1} - 1) - \sum_{b=2}^{j}(num(t_b))) * (n-i)!)$

# 7 Odvodenie všeobecného vzorca

## 7.1 Myšlenka odvodenia všeobecného vzorca

Na odvodenie všeobecného vzorca budeme rekurzívne určovať počet spôsobov, ako zostaviť $l$ sekvencií, a potom pomocou nami odvodeného vzorca určíme počet spôsobov, ako zostaviť sekvenciu pre všetky možné varianty zostavenia predchádzajúcich $l$ sekvencií. Avšak výpočet $num(t_i)$ pre všetky sady týchto $l$ sekvencií spôsobuje príliš veľké komplikácie. Z tohto dôvodu toto hodnotenie vyjmeme zo súčtu a analyzujeme jeho správanie za predpokladu, že zvažujeme všetky možné varianty predchádzajúcich $l$ permutácií. Získame:

$\prod_{k=1}^{n}(n! - k * n! + \sum_{i=2}^{n}((-1)^i * C_n^i * k^i) * (n-i)! + \sum_{i=2}^{n}(\sum_{j=2}^{i}((-1)^{j+1} * n * C_k^j * C_{n-j}^{i-2} * k^{i-j} * (C_j^{j-1} - 1)) * (n-i)! - (\sum_{m=2}^{n}(\sum_{b=2}^{n}(C_m^{2b} * C_n^b * C_k^2 * k^{m-2b} * (m-2b) * k!)) * (n-i)!)$

### 7.2 Myšlenka výpočtu vzorca pre $num(t_i)$

V skutočnosti nám stačí vyjadriť súčet $num(t_i)$ pre všetky možné permutácie predchádzajúcich sekvencií. Potom môžeme uvažovať o akejkoľvek konfigurácii pozícií pre množinu čísel tak, aby neboli porušené podmienky neusporiadanosti. Pretože na to, aby takáto konfigurácia bola $t_i$, je potrebné, aby existovalo aspoň i stĺpcov, v ktorých sú aspoň 2 čísla z množiny, tieto čísla najprv vyberieme a potom nájdeme počet možností, ako zvoliť stĺpce pre ostatné čísla. Na začiatku je preto potrebné vybrať $2 * i$ čísel a rozmiestniť ich na možné pozície tak, aby bolo i 2-priesečníkov, a následne rozmiestniť všetky ostatné čísla z množiny.

### 7.3 Problém takéhoto výpočtu:

Zložitosť spočíva v tom, že nemôžeme umiestniť do jedného stĺpca viac ako k čísel, a preto hodnota súčtu $num(t_i)$ nebude úplne presná. Na opravu tohto problému je potrebné zaviesť obmedzenia na rozdelenie čísel. Tiež je potrebné nájsť všetky možné umiestnenia čísel v stĺpci, avšak nevieme, koľko pozícií bude vybraných v každom stĺpci. Toto je možné urobiť pomocou rekurentného vzorca, ale výpočet by bol príliš komplikovaný. V súčasnosti hľadáme iné spôsoby riešenia tohto problému. Avšak, keďže v takomto prípade počet možností presahuje odpoveď, skutočný vzorec v bode 8.1 predstavuje pomerne presnú hornú hranicu.

## 8 Definicii a priklady

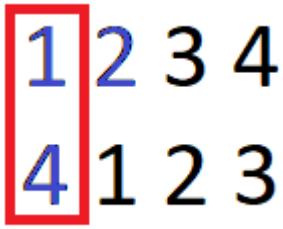
### 8.1 $a_i$

$a_i$ – počet spôsobov, ako vybrať i čísel a rozmiestniť ich na všetky možné pozície tak, že ak číslo $x$ umiestnime na pozíciu $j$, potom v niektorej z predchádzajúcich sekvencií už číslo $x$ bolo na pozícii $j$. Zároveň pre ľubovoľné 2 čísla nemôže byť vybraná tá istá pozícia.

**Príklad:**

Ukážeme, ktoré množiny pozícií budú započítané v $a_i$, a ktoré nebudú. Uveďme príklad: $p_1 = 1, 2, 3, 4$, $p_2 = 4, 1, 2, 3$. Teraz zvážme množinu čísel $1, 2, 4$, pre ktorú budú v $a_3$ započítané nasledujúce varianty:


To znamená, že pre tieto 3 čísla budú 4 možnosti, ako vybrať takéto pozície. Na druhej strane, nasledujúci variant nebude započítaný:



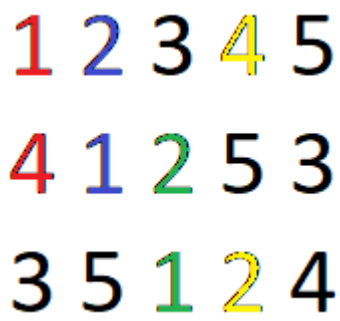
pretože v tomto prípade majú čísla 1 a 4 vybranú tú istú pozíciu, čo je v rozpore s definíciou. Tým pádom $a_3$ bude počtom spôsobov, ako vybrať takéto pozície pre každú trojicu čísel.

## 8.2 i-priesečníky a $h_i$

i-priesečník pre množinu $B$ je i čísel z množiny $B$, ktoré sa nachádzajú na tej istej pozícii vo svojej permutácii.
$h_i$ – počet všetkých i-priesečníkov pre vybranú množinu.

**Priklad:**

Rozoberme permutácie $p_1 = 1, 2, 3, 4, 5$, $p_2 = 4, 1, 2, 5, 3$, $p_3 = 3, 5, 1, 2, 4$. Zvážme množinu $1, 2, 4$ a nájdime pre ňu všetky 2-priesečníky:



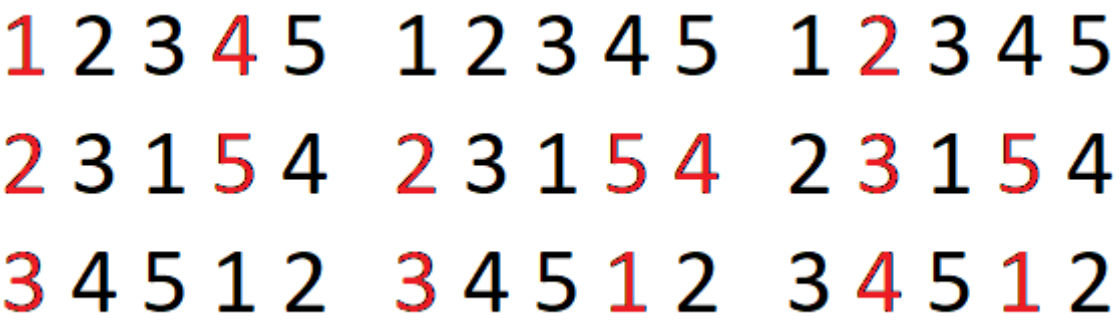

Tu sú číslami označenými rovnakou farbou znázornené prvky, ktoré patria do jedného 2-priesečníka. Pre túto množinu je teda $h_2 = 4$.

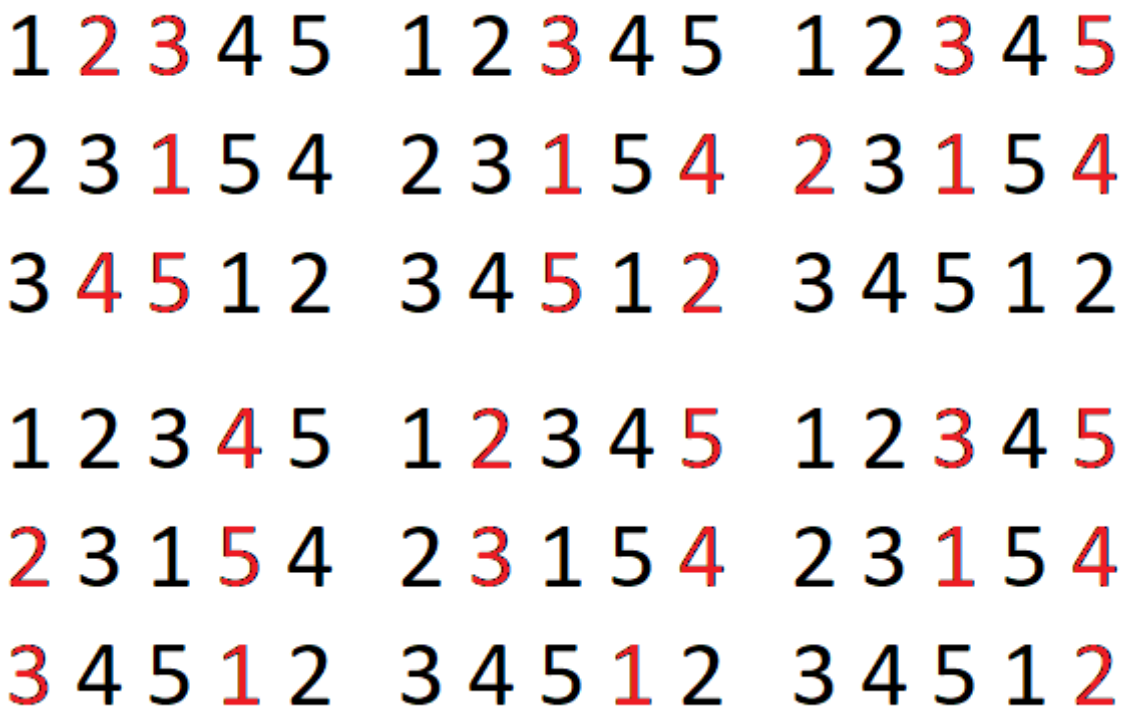
## 8.3 $t_i$ a $num(t_i)$

$t_i(B)$ – pozície pre danú množinu $B$, také, že existuje aspoň $i$ stĺpcov, v ktorých sa nachádzajú aspoň 2 prvky z $B$.
$num(t_i)$ – počet $t_i$ pre všetky množiny.

**Priklad:**

Zvážme permutácie $p_1 = 1, 2, 3, 4, 5$, $p_2 = 2, 3, 1, 5, 4$, $p_3 = 3, 4, 5, 1, 2$. Vezmime množinu čísel $1, 2, 3, 4, 5$, nižšie sú uvedené niektoré $t_2$ pre túto množinu:






## 9 Vytváranie takýchto permutácií

V prílohách je uvedený kód, ktorý pre dané hodnoty $k$, $n$ a $k-1$ párových neusporiadaností generuje všetky možné neusporiadanosti v exponenciálnom čase. Tento kód bol použitý napríklad v bode 4, ako aj na validáciu niektorých výsledkov v bode 6. Je zrejmé, že je použiteľný iba pre malé hodnoty.

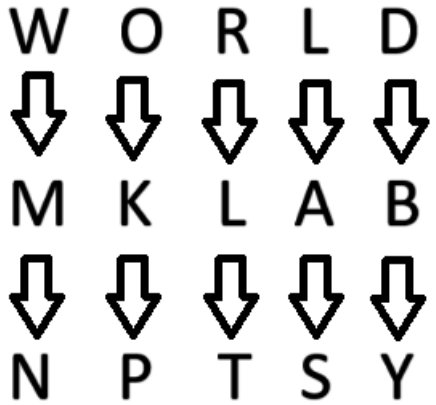
Zdrojový kód programu napísaného v jazyku C++ sa nachádza v prílohách.

## 10 Použitie na riešenie úloh

Zvážme príklad z bodu 5 úloh TYM 2021.
Zadanie:
B) Koľkými spôsobmi je možné natrieť dosku veľkosti $n \times n$ v $n$ farbách tak, aby v každom riadku a každom stĺpci bola presne jedna bunka každej farby?
Nie je ťažké si všimnúť, že toto číslo bude rovné $!^n n * n!$, čo možno vypočítať pomocou vzorcov pre hodnotu subfaktoriálu umocneného na daný stupeň.

## 11 Praktické využitie

Ďalší výskum môže priniesť veľa užitočných aplikácií v kryptografii. Zvážme napríklad, aké výsledky by mohol priniesť pri dešifrovaní šifrovacieho stroja „Enigma“. (Ďalšie úvahy vychádzajú z princípu fungovania Enigmy, s ktorým sa môžete podrobnejšie oboznámiť v tomto článku: `https://www.cryptomuseum.com/crypto/enigma/working.htm`).
Mechanizmus fungovania bol založený na tom, že pri každej iterácii prešla písmena do iného, v závislosti od polohy rotora. Pozoruhodnou vlastnosťou však bolo, že písmeno nikdy nemohlo zostať rovnaké ani po ľubovoľnom počte iterácií. Napríklad:




Z toho, že písmeno sa nikdy nevracia samo na seba, vyplýva, že slová v každej iterácii sú párové neusporiadanosti. To znamená, že tento výskum môže byť použitý napríklad na odhad počtu šifier alebo na výber najpravdepodobnejšej postupnosti (na základe vzorcov pre fixované postupnosti).

# 12 Prilohy

```
#include <bits/stdc++.h>

using namespace std;

signed main(){
    int k,n;
    cin>>k>>n;
    vector<vector<int> > permutations(k,vector<int> (n));
    for(int i=0;i<k-1;i++){
        for(int j=0;j<n;j++)
            cin>>permutations[i][j];
    }
    for(int i=0;i<n;i++)
        permutations[k-1][i] = i+1;

    do{
        bool valid = true;
        for(int j=0;j<n;j++){
            for(int i=0;i<k-1;i++)
                if(permutations[i][j]==permutations[k-1][j]){
                    valid = false;
                    break;
                }
            if(!valid)
                break;
        }
        if(valid){
            for(int i=0;i<n;i++){
                cout<<permutations[k-1][i]<<" ";
            }
            cout<<endl;
        }
```

```
    }while(next_permutation(permutations[k-1].begin(),permutations[k-1].end()));
}
```

# 13 Zdroje

https://en.wikipedia.org/wiki/Derangement

https://www.cryptomuseum.com/crypto/enigma/working.htm

https://www.statisticshowto.com/subfactorial/