Seminar 1

Metode de numărare

1.1 Principii de numărare. Cardinalul mulţimii de funcţii între două mulţimi finite

Rezolvarea problemelor de teoria probabilităţilor implică calculul numărului de moduri în care se pot selecta (sub restricţii bine precizate) obiecte dintr-o mulţime. Pentru a putea raţiona corect în problemele de numărare repetăm sau definim câteva rezultate de aritmetica numărării. Metodele de numărare pe care le prezentăm se folosesc şi pentru a stabili complexitatea algoritmilor.

Reamintim:

Fie A, B două mulţimi nevide şi $f : A \to B$ o aplicaţie (funcţie) de la A la B, adică pentru orice element $a \in A$ din domeniu există un unic element $b \in B$ din codomeniu astfel încât $f(a) = b$.

- f este o **injecţie** (funcţie injectivă) dacă la două argumente diferite din A face să le corespundă două elemente diferite din B:

$$a_1 \neq a_2 \quad \Rightarrow \quad f(a_1) \neq f(a_2),$$

ceea ce este echivalent cu

$$f(a_1) = f(a_2) \quad \Rightarrow \quad a_1 = a_2.$$

- f este o **surjecţie** (funcţie surjectivă) dacă oricărui element b din codomeniu îi corespunde un element a din domeniu (nu neapărat unic) astfel încât $f(a) = b$, adică

$$\forall\, b \in B\ \exists a \in A \text{ astfel încât } f(a) = b.$$

- f este o **bijecţie** (funcţie bijectivă) dacă este atât injectivă, cât şi surjectivă.

Fie Ω o mulţime finită. Numărul elementelor acestei mulţimi, numit şi cardinalul mulţimii, se notează prin $|\Omega|$, $\text{card}(\Omega)$ sau $\#\Omega$.

Ideea de bază în deducerea numărului elementelor unei mulţimi finite este că **dacă două mulţimi finite sunt în corespondenţă bijectivă, atunci ele au acelaşi număr de elemente (acelaşi cardinal).**

Notăm cu $\mathcal{P}(\Omega)$ familia părţilor lui Ω, adică familia tuturor submulţimilor lui Ω.

Propoziţia 1.1.1 *Dacă mulţimea Ω are n elemente, atunci $\mathcal{P}(\Omega)$ are 2^n elemente.*

Demonstraţie: Dacă Ω nu are nici un element, adică $\Omega = \emptyset$, atunci $\mathcal{P}(\Omega) = \{\emptyset\}$ are un element. Dacă Ω are un element, de exemplu $\Omega = \{\omega_1\}$, atunci $\mathcal{P}(\Omega) = \{\emptyset, \{\omega_1\}\}$ are $2^1 = 2$ elemente. Demonstraţia se face în continuare prin inducţie matematică asupra numărului de elemente ale mulţimii Ω, $n \geq 1$.

Presupunem propoziţia adevărată pentru $\Omega' = \{\omega_1, \omega_2, \ldots, \omega_n\}$ şi să demonstrăm că familia părţilor lui $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n, \omega_{n+1}\}$ are 2^{n+1} elemente. $\mathcal{P}(\Omega)$ conţine două clase de submulţimi disjuncte ale lui Ω:

- submulţimi ce nu conţin elementul ω_{n+1};
- submulţimi ce conţin elementul ω_{n+1}.

Evident că familia submulţimilor din prima clasă coincide cu $\mathcal{P}(\Omega')$. A doua clasă de submulţimi este în corespondenţă bijectivă cu $\mathcal{P}(\Omega')$ prin bijecţia:

$$\mathcal{P}(\Omega') \ni A \mapsto A \cup \{\omega_{n+1}\}.$$

Deci, şi prima, şi cea de-a doua clasă conţin 2^n elemente, iar $\mathcal{P}(\Omega)$ are $2^n + 2^n = 2^{n+1}$ elemente. □

Definiţia 1.1.1 O mulţime Ω care este în corespondenţă bijectivă cu mulţimea numerelor naturale, notată în continuare cu $\mathbb{N}$, se numeşte *mulţime numărabilă*.

Proprietate. *Dacă mulţimea Ω este numărabilă, atunci familia părţilor sale, $\mathcal{P}(\Omega)$, este infinită, dar nenumărabilă* (este în corespondenţă bijectivă cu mulţimea numerelor reale, care nu este numărabilă).

Dăm în continuare regulile de numărare a unor mulţimi de obiecte selectate şi a unor funcţii particulare între mulţimi finite.

Principiul sumei
Dacă $A_1, A_2, \ldots, A_m$ sunt m mulţimi finite, disjuncte două câte două, atunci cardinalul reuniunii lor este suma cardinalelor mulţimilor $A_1, A_2, \ldots, A_m$:

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = |A_1| + |A_2| + \cdots + |A_m|.$$

Exemplul 1. Coordonatele unui vector din $\mathbb{R}^n$, $v[0], v[1], \ldots, v[n-1]$, sunt sortate crescător. Deduceţi care este numărul comparaţiilor din pseudocodul de mai jos:

```
for(i=0; i<n-1;i++)
    for(j=i+1; j<n;j++){
       if(v[i]>v[j]) interschimba v[i] cu v[j];
       else {...}
       };
```

Rezolvare:

Notăm cu A mulţimea comparaţiilor ce se fac în secvenţa de pseudocod. De asemenea, notăm:

A_0 – mulţimea comparaţiilor de forma `v[0]>v[j]`, $j = 1, 2, \ldots, n-1$;

A_1 – mulţimea comparaţiilor de forma `v[1]>v[j]`, $j = 2, 3, \ldots, n-1$;

...

A_{n-2} – mulţimea comparaţiilor de forma `v[n-2]>v[j]`, $j = n-1$.

Este evident că $A = A_0 \cup A_1 \cup \ldots \cup A_{n-2}$. Mulţimile $A_0, A_1, \ldots, A_{n-2}$ sunt disjuncte două câte două şi $|A_0| = n-1$, $|A_1| = n-2, \ldots, |A_{n-2}| = 1$. Prin urmare, mulţimea A are cardinalul:

$$|A| = (n-1) + (n-2) + \cdots + 1 = \frac{(n-1)n}{2},$$

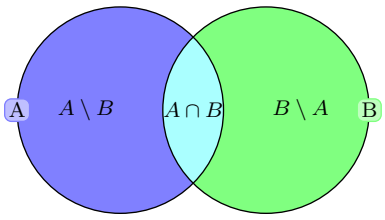
deci în secvenţa de pseudocod se fac $n(n-1)/2$ comparaţii.

□

Principiul includerii-excluderii

Dacă A, B sunt două mulţimi finite cu intersecţia nevidă, atunci

$$|A \cup B| = |A| + |B| - |A \cap B|.$$



Mai general, dacă A_1, A_2, A_3 sunt trei mulţimi finite, atunci are loc:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

Formula de mai sus poate fi generalizată pentru un număr oarecare de mulţimi: dacă $A_1, A_2, \ldots, A_n$ sunt mulţimi finite, atunci are loc

$$\begin{aligned}\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| &- \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| \\ &+ \cdots + (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| \\ &+ \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|.\end{aligned}$$

Principiul diferenţei

Cardinalul diferenţei a două mulţimi finite A şi B este $|A \setminus B| = |A| - |A \cap B|$.

Principiul produsului

Fie A şi B două mulţimi nevide finite. $A \times B = \{(x, y) \mid x \in A, y \in B\}$ este produsul lor cartezian, iar $B^A = \{f : A \to B\}$ este mulţimea funcţiilor definite pe A cu valori în B.

Propoziţia 1.1.2 1) *Dacă A are m elemente şi B are n elemente, atunci produsul cartezian $A \times B$ are $m \cdot n$ elemente, adică cardinalul produsului cartezian este produsul cardinalelor lui A şi B:*

$$|A \times B| = |A| \cdot |B|. \tag{1.1}$$

Mai general, dacă $B_1, B_2, \ldots, B_n$ sunt mulţimi nevide finite, atunci

$$|B_1 \times B_2 \times \cdots \times B_n| = |B_1| \cdot |B_2| \cdots |B_n|. \tag{1.2}$$

2) *Numărul funcţiilor de la A la B este egal cu cardinalul lui B ridicat la puterea cardinalul lui A:*

$$|B^A| = |B|^{|A|}. \tag{1.3}$$

Demonstraţie: 2) Dacă A are m elemente, atunci mulţimea funcţiilor de la A la B este în corespondenţă bijectivă cu produsul cartezian $\underbrace{B \times B \times \cdots \times B}_{m \text{ ori}}$:

$$f \equiv \begin{pmatrix} a_1 & a_2 & \ldots & a_m \\ \downarrow & \downarrow & \ldots & \downarrow \\ b_1 & b_2 & & b_m \end{pmatrix} \leftrightarrow (b_1, b_2, \ldots, b_m) \in \underbrace{B \times B \times \cdots \times B}_{m \text{ ori}}. \tag{1.4}$$

Cu alte cuvinte, o aplicaţie de la A la B se identifică cu m–uplul valorilor sale. Deci, există atâtea aplicaţii câte m–upluri $(b_1, b_2, \ldots, b_m)$ cu elemente din B există.

Datorită acestei corespondenţe, B^A are acelaşi număr de elemente ca şi produsul cartezian $\underbrace{B \times B \times \cdots \times B}_{m \text{ ori}}$, adică are $\underbrace{|B| \cdot |B| \cdot \ldots \cdot |B|}_{m \text{ ori}} = |B|^m = |B|^{|A|}$ elemente. □

1.2 k–liste generale

Definiţia 1.2.1 Fie A o mulţime nevidă finită cu n elemente (obiecte). O *k–listă cu elemente din A* este un element al produsului cartezian $\underbrace{A \times A \times \cdots \times A}_{k \text{ ori}}$, adică un k–uplu $(a_1, a_2, \ldots, a_k)$ cu elemente din A.

Remarcăm că:

• o k–listă este o selecţie **ordonată** de k obiecte. De exemplu, 5-listele $(7, 1, 2, 8, 9)$, $(8, 7, 9, 2, 1)$, selectate din mulţimea $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, sunt distincte, pentru că, deşi conţin aceleaşi elemente, ordinea diferă;

• dacă o k–listă se obţine prin extragerea succesivă a elementelor sale dintr-o mulţime, urmată de returnarea în mulţimea iniţială, atunci există posibilitatea existenţei repetiţiilor unui obiect într-o k-listă, de exemplu $(4, 0, 0, 1, 7)$.

Propoziţia 1.2.1 *Numărul k–listelor ce se pot forma din elementele unei mulţimi A, de cardinal n, este n^k.*

Demonstraţie: O k–listă $(a_1, a_2, \ldots, a_k)$ este definită de o aplicaţie

$$L : \{1, 2, \ldots, k\} \to A,\ L(i) = a_i,$$

care indexează elementele ei, deci mulţimea k–listelor cu elemente din A coincide cu mulţimea $\mathcal{L} = \{L : \{1, 2, \ldots, k\} \to A\}$, ce are cardinalul $|A|^k = n^k$. □

Exemplul 2. Fie A mulţimea literelor mici din alfabetul limbii engleze:

$$A = \{a, b, c, d, \ldots, x, y, z\}.$$

Câte password-uri de 8 litere din mulţimea A se pot forma?
Rezolvare: Cardinalul lui A este 26. Mulţimea password–urilor de 8 litere este, de fapt, mulţimea aplicaţiilor Pass : $\{1, 2, 3, 4, 5, 6, 7, 8\} \to A$ care asociază fiecărui număr $i = 1, 2, \ldots, 8$ a i-a literă din password–ul $\ell_1\ell_2 \ldots \ell_8$. Astfel, se pot forma 26^8 password–uri de câte 8 caractere din cele 26 de litere ale alfabetului A.

□

1.3 k–liste de elemente distincte

Mulţimea k-listelor cu elemente distincte dintr-o mulţime A, de cardinal n, $1 \leq k \leq n$, poate fi identificată cu mulţimea aplicaţiilor injective definite pe $\{1, 2, \ldots, k\}$ cu valori în A şi anume: o injecţie $f : \{1, 2, \ldots, k\} \to A$ asociază fiecărui număr $i \in \{1, 2, \ldots, k\}$ un element $a_i \in A$ şi pentru orice $i \neq j$, $a_i \neq a_j$. Astfel, injecţia este reprezentată de mulţimea valorilor sale, k-lista de elemente distincte $(a_1, a_2, \ldots, a_k) \in \underbrace{A \times A \times \cdots \times A}_{k\ ori}$.

a_1 poate fi $1, 2, \ldots, n$. O dată fixat a_1, a_2 poate lua oricare din cele $n-1$ valori rămase, pentru a_3 sunt $n-2$ variante, $\cdots$, a_k poate lua $n-(k-1)$ valori rămase din cele n. Deci, avem în total $n(n-1)\cdots(n-k+1)$ posibilităţi. În concluzie, *cu elementele unei mulţimi de cardinal n se pot forma aranjamente de n luate câte k,*

$$A_n^k = n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!},$$

k–liste de elemente distincte sau, echivalent, există aranjamente de n luate câte k injecţii de la o mulţime cu k elemente la o mulţime cu n elemente, $1 \leq k \leq n$.

În cazul particular, $k = n$, o n–listă cu elemente distincte ale lui A, $|A| = n$, este o permutare a lui A. Mulţimea permutărilor lui A coincide cu mulţimea funcţiilor bijective $\sigma : A \to A$. Particularizând rezultatul de mai sus, există $A_n^n = n(n-1)\cdots(n-n+1) = n!$ permutări ale mulţimii A sau $n!$ funcţii bijective de la A la A.

1.4 k–combinări

Fie A o mulţime finită cu n elemente şi k un număr natural astfel încât $0 \leq k \leq n$. Orice submulţime formată din k elemente ale lui A se numeşte k–combinare (combinare de n elemente luate câte k). Notăm cu $\mathcal{P}_k(A)$ mulţimea părţilor lui A ce au k elemente. De exemplu, dacă $A = \{1, 2, 3, 4\}$, atunci $\mathcal{P}_3(A) = \{\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}\}$.

Propoziţia 1.4.1 *Mulţimea părţilor lui A ce conţin k elemente, $\mathcal{P}_k(A)$, are cardinalul egal cu combinări de n luate câte k:*

$$C_n^k = \frac{n!}{(n-k)!\,k!} = \frac{n(n-1)\cdots(n-k+1)}{k!}. \tag{1.5}$$

Demonstraţie: Pentru $k = 0$, $\mathcal{P}_0(A)$ este mulţimea părţilor lui A ce conţin 0 elemente, adică $\mathcal{P}_0(A)$ constă doar din mulţimea vidă, deci cardinalul său este $1 = C_n^0$. Pentru $k = n$, $\mathcal{P}_n(A)$ conţine doar mulţimea A, deci are cardinalul $1 = C_n^n$. Fixăm $k > 0$ şi demonstrăm relaţia prin inducţie asupra lui n, $n \geq k$.

Presupunem că pentru A' de cardinal n, cardinulul mulţimii părţilor de k elemente este $|\mathcal{P}_k(A')| = C_n^k$ şi demonstrăm că dacă A are $n+1$ elemente, atunci $|\mathcal{P}_k(A)| = C_{n+1}^k$.

Fie $A = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$ şi $A' = \{a_1, a_2, \ldots, a_n\}$. Mulţimea $\mathcal{P}_k(A)$ se descompune în două clase disjuncte, $\mathcal{P}_k(A) = \mathcal{C}_1 \cup \mathcal{C}_2$:

- $\mathcal{C}_1$ conţine toate părţile lui A ce **nu** îl conţin pe a_{n+1};
- $\mathcal{C}_2$ conţine toate părţile lui A ce conţin elementul a_{n+1}.

Prima clasă coincide cu $\mathcal{P}_k(A')$, deci are, conform ipotezei inducţiei, C_n^k elemente, iar cea de-a doua clasă este în corespondenţă bijectivă cu $\mathcal{P}_{k-1}(A')$:

$$E = \{e_1, e_2, \ldots, e_{k-1}, a_{n+1}\} \leftrightarrow \{e_1, e_2, \ldots, e_{k-1}\} \in \mathcal{P}_{k-1}(A').$$

Conform ipotezei inducţiei, $|\mathcal{P}_{k-1}(A')| = C_n^{k-1}$. Astfel, din principiul sumei, rezultă că

$$|\mathcal{P}_k(A)| = |\mathcal{C}_1| + |\mathcal{C}_2| = C_n^k + C_n^{k-1} = C_{n+1}^k.$$

□

Formula

$$C_{n+1}^k = C_n^k + C_n^{k-1},$$

valabilă pentru orice $n \in \mathbb{N}^*$ şi $k = 1, 2, \ldots, n$, generează **triunghiul lui Pascal**:

`http://en.wikipedia.org/wiki/Pascal's_triangle`.

Exemplul 3. Fie A mulţimea stringurilor de n biţi, $s = b_1 b_2 \ldots b_n$, $b_i \in \{0, 1\}$. Să se determine câte stringuri au suma biţilor egală cu k.

Rezolvare: Un string s are suma biţilor k dacă acesta conţine k de 1. Aceşti biţi 1 pot fi plasaţi în poziţiile de indici $i_1, i_2, \ldots, i_k$ cu $1 \leq i_1 < i_2 < \ldots < i_k \leq n$. Cum există C_n^k

submulţimi de k indici din mulţimea de n simboluri, $\{1, 2, \ldots, n\}$, rezultă că există C_n^k stringuri de biţi a căror sumă este k.

□

Exemplul 4. Codul zecimal exprimat în binar atribuie fiecărei cifre $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ un cod din 4 biţi:

0	1	2	3	4	5	6	7	7	9
0000	0001	0010	0011	0100	0101	0110	0111	1000	1001

a) Care este numărul m al codurilor de patru biţi ce se pot forma? Câte din cele m coduri au rămas nefolosite după alegerea codurilor pentru cifrele în baza 10?

b) În câte moduri pot fi codificate cifrele zecimale prin coduri de 4 biţi?

c) Presupunem că în definirea unui cod arbitrar (nu neapărat cel dat) pentru cifrele zecimale se specifică în prealabil care sunt codurile de 4 biţi neutilizate în codificare. Câte posibilităţi de codificare pe 4 biţi a cifrelor $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ există în această etapă a codificării?

Rezolvare: a) Un cod de 4 biţi este o 4–listă cu elemente din mulţimea $A = \{0, 1\}$. Deci, există în total $2^4 = 16$ coduri pe 4 biţi. Cum în tabelul de mai sus avem 10 coduri, 6 sunt neutilizate din cele 16 posibile.

b) În criptografie mulţimea aplicaţiilor $s : \{1, 2, \ldots, n\} \to \{0, 1\}$ se notează prin $\{0, 1\}^n$. Cu această notaţie, mulţimea codurilor pe 4 biţi este mulţimea $\{0, 1\}^4$.

Codificarea cifrelor $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ printr-un cod de 4 biţi se realizează printr-o aplicaţie injectivă:

$$C : \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \to \{0, 1\}^4.$$

Mulţimea aplicaţiilor injective între cele două mulţimi are cardinalul A_{16}^{10}, unde 16 este cardinalul lui $\{0, 1\}^4$, iar 10 este cardinalul mulţimii cifrelor zecimale.

c) Dacă înainte de codificare se aleg cele 6 coduri din cele 16 posibile pe 4 biţi ce nu vor fi folosite, avem 10! posibilităţi de codificare a cifrelor, adică numărul bijecţiilor între $\{0, 1, 2, \ldots, 9\}$ şi cele 10 coduri pe patru biţi rămase.

□

Exemplul 5. Să se determine numărul stringurilor de 8 biţi care fie încep cu bitul 1, fie se termină cu 2 biţi 0.

Rezolvare: Notăm cu A mulţimea stringurilor de biţi de forma $1b_2b_3 \ldots b_8$, respectiv cu B mulţimea stringurilor de biţi de forma $b_1b_2 \ldots b_600$. Se cere să determinăm cardinalul lui $A \cup B$. Pentru aceasta calculăm $|A|$, $|B|$ şi $|A \cap B|$. Mulţimea $A \cap B$ este mulţimea stringurilor de biţi de forma $1b_2b_3 \ldots b_600$.

În A există atâtea stringuri câte substringuri $b_2b_3 \ldots b_8$ de 7 biţi există. Interpretând un astfel de substring ca o 7-listă, avem că $|A|$ este egal cu numărul de 7-liste cu elemente din $\{0, 1\}$, adică $|A| = 2^7$. Analog, $|B| = 2^6$ şi $|A \cap B| = 2^5$.

Prin urmare, $|A \cup B| = 2^7 + 2^6 - 2^5 = 2^5(4 + 2 - 1) = 32 \cdot 5 = 160$.

□

Temă

1. Să se determine câte password-uri de 8 caractere din mulţimea

$$C = \{a, b, c, \ldots, x, y, z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

se pot forma astfel încât fiecare password conţine cel puţin o cifră şi se termină cu o literă.

2. O magistrală a plăcii de bază este un circuit specializat ce comunică cuvinte. În cazul de faţă un cuvânt este un string binar de 8 biţi.

a) Câte cuvinte distincte poate comunica magistrala?

b) În modul de lucru redus cel mult 6 biţi dintr-un cuvânt pot fi setaţi simultan pe 1. Câte cuvinte diferite poate să comunice magistrala în modul redus?

3. Există 128 caractere ASCII. Câte din stringurile de 5 caractere ASCII conţin caracterul `@`?

4. Un sistem de parolare a încuietorii la geamantan foloseşte cifrele $0, 1, 2, \ldots, 9$. Câte combinaţii distincte se pot forma din 4 cifre ce nu se repetă?

5. Oricărui device ce se conectează la internet (calculator, telefon mobil, imprimantă în reţea etc) i se atribuie o adresă de identificare. Pentru IPv4 (Internet Protocol versiunea 4) o adresă este reprezentată pe 32 de biţi. Aceasta începe cu un număr numit *netid* (identificatorul reţelei), ce este apoi urmat de *hostid* (identificatorul locaţiei device-lui în reţea).

Se folosesc 3 tipuri de adrese cu număr diferit de biţi alocaţi pentru *netid* şi *hostid*:

• Clasa A de adrese se foloseşte pentru reţele foarte mari, iar o astfel de adresă începe cu 0, urmat de 7 biţi pentru *netid* şi 24 pentru *hostid*;

• Clasa B de adrese se foloseşte pentru reţele de mărime medie. Adresa începe cu biţii 10, apoi 14 biţi pentru *netid* şi 16 biţi pentru *hostid*;

• Clasa C conţine adrese pentru reţele mici. O adresă începe cu biţii 110, urmaţi de 21 biţi pentru *netid* şi 8 biţi pentru *hostid*.

Există şi câteva restricţii pentru adrese:

• pentru clasa A nu se admite 01111111 ca *netid*;

• nu se permite pentru nici o reţea un *hostid* care să aibă toţi biţii 0 sau toţi 1;

• un device conectat la net primeşte fie adresă de clasă A, fie de clasă B, fie de clasă C.

Câte adrese IPv4 diferite sunt disponibile pentru device-uri unice conectate la internet?