Računovodsko pravilo 2

↓↓↓
Ivan Lisac

→ **Pred leti smo v Preseku [1] pisali o računovodskem pravilu, s katerim smo ugnali nekaj končnih vsot. Obudimo tokrat pravilo v nekaj novih primerih.**

Računovodsko pravilo

Naj bosta A in B končni množici ter R poljubna podmnožica kartezičnega produkta $A \times B$. Podmnožici R pravimo tudi *relacija*. Da sta elementa $a \in A$ ter $b \in B$ v relaciji R zapišemo $(a, b) \in R$ ali krajše aRb. Za dani $a \in A$ lahko zberemo vse $b \in B$, ki so v relaciji R z a v množico

- $R(a) = \{b \in B : aRb\}$.

Obratno lahko definiramo za dani b množico

- $R^{-1}(b) = \{a \in A : aRb\}$.

Moč končne množice X bomo označili z $|X|$. Potem računovodsko pravilo pravi:

- $$|R| = \sum_{a \in A} |R(a)| = \sum_{b \in B} |R^{-1}(b)|. \qquad (1)$$

Z znakom $\sum_{a \in A} |R(a)|$ smo označili vsoto števil $|R(a)|$, ko a preteče množico A, podobno pojasnimo znak $\sum$ v ostalih primerih. Zgornjo trditev (1) si najlažje predočimo ob spodnji tabeli za poseben primer relacije $R \subseteq \{a_1, a_2, a_3\} \times \{b_1, b_2, b_3, b_4\}$:

	b_1	b_2	b_3	b_4	$\sum$
a_1	0	0	1	1	2
a_2	1	1	0	1	3
a_3	1	0	0	0	1
$\sum$	2	1	1	2	6

Zapišimo elemente množice A v skrajni levi stolpec, elemente množice B pa v zgornjo vrstico. Če je aRb, zapišimo na križišče ustrezne vrstice in stolpca enico, sicer postavimo tja ničlo. Potem so tri števila iz enakosti (1) zaporedoma: skupno število enic, vsota enic, šteta po vrsticah, in vsota enic, šteta po stolpcih ($2 + 1 + 1 + 2 = 2 + 3 + 1 = 6$). Ta tri števila so enaka, zato enakost (1) velja. Sedaj si oglejmo nekaj primerov, kjer bomo izbirali množici A in B ter relacijo R, in tako našli ali vsaj preoblikovali nekaj končnih vsot.

Relacija 'deli' ($|$)

Označimo množico prvih n naravnih števil z znakom $\mathbb{N}_n = \{1, 2, \ldots, n\}$. Vzemimo $A = B = \mathbb{N}_n$ in $aRb \Leftrightarrow a|b$. Uvedimo še funkcijo *celi del*:

- $\lfloor x \rfloor = max(\{n \in \mathbb{Z} : n \leq x\})$.

Potem je

- $|R(a)| = \lfloor \frac{n}{a} \rfloor$,

saj a deli števila

- $a, 2a, \ldots, \lfloor \frac{n}{a} \rfloor a$,

množica $R^{-1}(b)$ pa vsebuje delitelje števila b, tako da dobimo

- $$\sum_{a=1}^{n} \lfloor \frac{n}{a} \rfloor = \sum_{b=1}^{n} \tau(b). \qquad (2)$$

Tu je τ funkcija, ki šteje delitelje argumenta. Za npr. $n = 4$ je leva stran

- $\lfloor \frac{4}{1} \rfloor + \lfloor \frac{4}{2} \rfloor + \lfloor \frac{4}{3} \rfloor + \lfloor \frac{4}{4} \rfloor = 4 + 2 + 1 + 1 = 8$,

desna pa

- $\tau(1) + \tau(2) + \tau(3) + \tau(4) = 1 + 2 + 2 + 3 = 8$.

Praštevilski kvocient

Vzemimo $A = B = \mathbb{N}_n$ in zahtevajmo za relacijo R še to, da je kvocient b/a praštevilo: $aRb \Leftrightarrow a|b \wedge b/a \in \mathbb{P}$. Potem je za dani a

- $|\{b \in B : pa = b, p \in \mathbb{P}\}| = |\{p \in \mathbb{P} : p \leq \lfloor \frac{n}{a} \rfloor\}|$.

Moč množice $R^{-1}(b)$ pa je

- $|R^{-1}(b)| = |\{p \in \mathbb{P} : p|b\}| = \omega(b)$,

kjer smo z $\omega(b)$ označili število praštevilskih deliteljev števila b. Uvedimo še funkcijo π, ki šteje praštevila do danega argumenta takole:

- $\pi(x) = |\{p \in \mathbb{P} : p \leq x\}|$,

pa že dobimo naslednjo enakost:

- $$\sum_{a=1}^{n} \pi(\lfloor \frac{n}{a} \rfloor) = \sum_{b=1}^{n} \omega(b). \qquad (3)$$

Primer.

- $$\pi\left(\lfloor \frac{4}{1} \rfloor\right) + \pi\left(\lfloor \frac{4}{2} \rfloor\right) + \pi\left(\lfloor \frac{4}{3} \rfloor\right) + \pi\left(\lfloor \frac{4}{4} \rfloor\right) = 2 + 1 + 0 + 0 = 3$$

in

- $\omega(1) + \omega(2) + \omega(3) + \omega(4) = 0 + 1 + 1 + 1 = 3$.

Koreni

Vzemimo $A = B = \mathbb{N}_n$ in $aRb \Leftrightarrow a^2 \leq b$. Potem so v $R(a)$ števila

- $a^2, a^2 + 1, \ldots, n$,

ki jih je natanko $(n - a^2 + 1)$, če je le $a^2 \leq n$, ter 0 sicer. V množici $R^{-1}(b)$ pa so števila

$$1, 2, \ldots, \lfloor \sqrt{b} \rfloor.$$

Prvo vsoto zapišimo samo do tistega največjega m, pri katerem je $n + 1 - m^2 \geq 0$, tj. $m = \lfloor \sqrt{n+1} \rfloor$, potem je

- $$\sum_{a=1}^{m} (n + 1 - a^2) = \sum_{b=1}^{n} \lfloor \sqrt{b} \rfloor = m(n+1) - m(m+1)(2m+1)/6. \qquad (4)$$

Pri tem smo uporabili znano formulo za vsoto prvih m kvadratov

- $1^2 + 2^2 + \cdots + m^2 = m(m+1)(2m+1)/6$.

Za npr. $n = 10$ imamo $m = 3$ in

- $$\sum_{b=1}^{10} \lfloor \sqrt{b} \rfloor = 3 \cdot 11 - 3 \cdot 4 \cdot 7/6 = 33 - 14 = 19.$$

Negibne točke

Vzemimo $A = \mathbb{N}_n$ in $B = A^A$ množico preslikav f iz množice A vase. *Negibna točka* $a \in A$ funkcije f zadošča enakosti $f(a) = a$. Postavimo $aRf \Leftrightarrow f(a) = a$ in preštejmo negibne točke teh preslikav. Najprej je

- $|R(a)| = |\{f \in B : f(a) = a\}| = n^{n-1}$,

saj preslikavi f predpišemo negibno točko a, iz ostalih $n - 1$ vrednosti izberemo poljubno iz množice A. Množica $R^{-1}(f)$ pa je množica negibnih točk preslikave f. Sledi

- $$\sum_{a \in A} n^{n-1} = n^n = \sum_{f \in B} |R^{-1}(f)|, \qquad (5)$$

kar pomeni, da ima naključno izbrana preslikava v povprečju eno samo negibno točko. Podoben premislek lahko naredimo za množico bijektivnih preslikav množice A vase in dobimo enak rezultat: naključno izbrana permutacija ima v povprečju eno samo negibno točko.

Potence dvojke

Vzemimo $A = \mathbb{N}_n$ in potenčno množico $\mathcal{B} = P(A)$. Postavimo še $aRB \Leftrightarrow a = \min(B)$ za $B \neq \emptyset$. Potem je leva stran

- $$\sum_{a \in A} |R(a)| = \sum_{a=1}^{n} 2^{n-a} = \sum_{a=0}^{n-1} 2^a,$$

saj dobimo množice B z minimumom a tako, da izberemo ali opustimo elemente iz množice $\{a+1, a+2, \ldots, n\}$ moči $(n-a)$, kar da skupaj 2^{n-a} možnosti. Desna stran pa je

- $$\sum_{B \in \mathcal{B}} |R^{-1}(B)| = \sum_{B \in \mathcal{B} \setminus \{\emptyset\}} 1 = 2^n - 1, \qquad (6)$$

saj ima neprazna množica B natanko en minimum. To je še en način seštevanja geometrijske vrste s koeficientom 2.

Dvojke ponovno

Vzemimo $A = \{(m, M) : 1 \le m < M \le n\}$ in potenčno množico $\mathcal{B} = P(\mathbb{N}_n)$. Postavimo tokrat

- $(m, M)RB \Leftrightarrow m = \min(B) \wedge M = \max(B)$.

Potem je $|R((m, M))| = 2^{M-m-1}$, saj so za dana minimum m in maksimum M v množici B prosti elementi za izbiro le še tisti vmes ($M - m - 1$ jih je). Ko m in M tečeta po množici A, zavzame izraz $M - m$ vrednosti od 1 do $n - 1$. Vrednost 1 zavzame $(n - 1)$-krat, vrednost 2 zavzame $(n - 2)$-krat, ... in vrednost $(n - 1)$ enkrat tako, da velja

- $$\sum_{(m,M)\in A} 2^{M-m-1} = \sum_{v=1}^{n-1} (n - v)2^{v-1}.$$

Po drugi strani pa za vsako množico B z vsaj dvema elementoma dobimo natanko en tak par $(m, M) \in A$, da je $m = \min(B)$ in $M = \max(B)$, zato je

- $$\sum_{v=1}^{n-1} (n - v)2^{v-1} = \sum_{B\in\mathcal{B}'} 1 = 2^n - n - 1. \qquad (7)$$

V enakosti (7) smo se v drugi vsoti izognili enkrat prazni množici in n-krat enoelementnim množicam. Za npr. $n = 6$ dobimo

- $5 \cdot 2^0 + 4 \cdot 2^1 + 3 \cdot 2^2 + 2 \cdot 2^3 + 1 \cdot 2^4 =$
  $= 5 + 8 + 12 + 16 + 16 = 57 = 2^6 - 6 - 1.$

Ciklične grupe

Oglejmo si še najbolj zahteven primer v tem članku. Definirajmo množico $\mathbb{Z}_n$ ostankov pri deljenju z n. Operacija na njej sešteva ostanke po *modulu* n in iz nje napravi *grupo*. Vzemimo za primer grupo $\mathbb{Z}_{12} = \{1, 2, \ldots, 12\}$. Podobna je vsakdanjemu gledanju na uro, kjer lahko seštevamo ure preko poldneva, npr. $10 + 4 = 2(+12)$. Ostanek 12 je tu nevtralni element. Vsakega od ostankov lahko dobimo že zgolj s seštevanjem samih enic. Učeno pravimo, da ostanek 1 *generira* grupo $\mathbb{Z}_{12}$. Ni pa edini: družbo mu delajo še taki ostanki m, da števila $m, m + m, m + m + m, \ldots, 12m$ zasedejo vseh 12 ostankov, za kar zadošča, da za nek naravni k ostanek km zasede tudi enico oz. velja $km \equiv 1 \pmod{12}$ oz. je m tuj modulu 12. Generatorji $\mathbb{Z}_{12}$ so tako še ostanki 5, 7 in 11.

Grupe, ki jih generira že en sam generator, so *ciklične*. Podmnožicam grupe, ki so zaprte za dano operacijo (in njen inverz), pravimo *podgrupe*. Naštejmo vse podgrupe grupe $\mathbb{Z}_{12}$:

- $\{\underline{1}, 2, 3, 4, \underline{5}, 6, \underline{7}, 8, 9, 10, \underline{11}, 12\}$,
  $\{\underline{2}, 4, 6, 8, \underline{10}, 12\}, \{\underline{3}, 6, \underline{9}, 12\}$,
  $\{\underline{4}, \underline{8}, 12\}, \{\underline{6}, 12\}, \{\underline{12}\}$.

Tu smo generatorje podgrup podčrtali. Iz teorije grup si sedaj brez dokaza izposodimo tele trditve:

- Podgrupe ciklične grupe so ciklične.
- Za vsak delitelj d števila n obstaja natanko ena podgrupa moči n/d z generatorjem d.
- Vseh podgrup $\mathbb{Z}_n$ je kot deliteljev števila n, tj. $\tau(n)$.
- $\mathbb{Z}_n$ ima $\phi(n)$ generatorjev: to so ostanki, ki so tuji n.

Tu je $\phi(n)$ *Eulerjeva funkcija*, ki vrača število proti n tujih števil iz $\mathbb{Z}_n$. Sedaj vzemimo $A = \mathbb{Z}_n$ in $B = \{b \in \mathbb{Z}_n : b|n\}$ ter aRb, če a in b generirata isto podgrupo. Potem je $|R(a)| = 1$, saj obstaja natanko en tak generator $b \in B$, da je podgrupa generirana z a enaka podgrupi generirani z b. Obratno pa dani b generira ciklično podgrupo moči n/b, ki ima $\phi(n/b)$ generatorjev. Zato dobimo

- $$\sum_{a\in A} 1 = n = \sum_{b|n} \phi(n/b) = \sum_{b|n} \phi(b). \qquad (8)$$

V enakosti (8) smo pri tretjem enačaju elemente n/b samo našteli v obratnem vrstnem redu. Še primer: za $n = 12$ imamo

- $\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) =$
  $= 1 + 1 + 2 + 2 + 2 + 4 = 12.$

Literatura

[1] I. Lisac, *O računovodskem pravilu*, Presek **24** (1997), 6, 346–351.

×××