q-Binomni koeficijenti

30. 10. 2025.

$\mathbb{F}_q$ = konačno polje reda q

Što znate o konačnim poljima?

- Što je uopće polje?
- Za koje redove $q \in \mathbb{N}$ postoje?

  Lako: za proste brojeve! $(\mathbb{Z}_p, +_p, \cdot_p)$

  Malo teže: za potencije prostih brojeva... $\mathbb{Z}_p[x]/(f(x))$
- Koliko polja istog reda postoji?
- Ako polje $\mathbb{F}_q$ ima potpolje $\mathbb{F}_{q'}$, što možete reći o q i q'? $q = p^t$, $q' = p^s$, $s \mid t$
- Kako dokazati da q mora biti prim potencija?

  char $\mathbb{F}_q = p$ $\mathbb{F}_q$ ima potpolje reda p i možemo ga promatrati kao vekt. prostor nad $\mathbb{F}_p$!

V = n-dim. vektorski prostor nad $\mathbb{F}_q$

Zad $|V| = q^n$

$W \leq V$, $\dim W = k$

Koliko ima takvih podprostora?

$\binom{n}{k}$ = # k-elemenih podskupova n-članog skupa

$\binom{n}{k}_2$ = # k-dim. podprostora n-dim. vekt. prostora nad $\mathbb{F}_2$

Zad Izvedite formulu za $\binom{n}{k}_2$!

Rj: Broj uređenih k-torki lin. nezavisnih vektora:

$$(2^n-1)(2^n-2)(2^n-2^2)\cdots(2^n-2^{k-1})$$

Linearna ljuska: k-dim podprostor W

Od koliko k-torki dolazimo istog podprostora W?

Koliko baza ima W?

$$(2^k-1)(2^k-2)(2^k-2^2)\cdots(2^k-2^{k-1})$$

Princip množenja:

$$\binom{n}{k}_2 = \frac{(2^n-1)(2^n-2)\cdots(2^n-2^{k-1})}{(2^k-1)(2^k-2)\cdots(2^k-2^{k-1})} = \frac{(2^n-1)(2^{n-1}-1)\cdots(2^{n-k+1}-1)}{(2^k-1)(2^{k-1}-1)\cdots(2-1)}$$

Možemo još napisati formulu koristeći faktorizaciju

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1)$$

(suma konačnog geometrijskog reda!)

Uvedimo kraticu $[n]_x = x^{n-1} + x^{n-2} + \dots + x^2 + x + 1$

$$\binom{n}{k}_x = \frac{\cancel{(x-1)^k}\ [n]_x\,[n-1]_x \cdots [n-k+1]_x}{\cancel{(x-1)^k}\ [k]_x\,[k-1]_x \cdots [1]_x}$$

Sada uvedemo x-faktorijele $[n]_x! = [n]_x \cdot [n-1]_x \cdots [1]_x$

i „proširimo" brojnik i nazivnik s $[n-k]_x!$

$$\binom{n}{k}_x = \frac{[n]_x!}{[k]_x!\,[n-k]_x!}$$

Kakva je to funkcija u varijabli x?

Računalo! Međutim, izračunamo nekoliko mjesta...

$$\binom{2}{0}_x = 1 \qquad \binom{2}{1}_x = x+1 \qquad \binom{2}{2}_x = 1$$

$$\binom{3}{0}_x = 1 \qquad \binom{3}{1}_x = x^2+x+1 = \binom{3}{2}_x \qquad \binom{3}{3}_x = 1$$

$$\binom{4}{0}_x = \binom{4}{4}_x = 1, \qquad \binom{4}{1}_x = \binom{4}{3}_x = x^3+x^2+x+1 = [4]_x \qquad \binom{4}{2}_x = 1+x+2x^2+x^3+x^4 = (1+x^2)(1+x+x^2)$$

Prop 1 $\begin{bmatrix} n \\ 0 \end{bmatrix}_2 = \begin{bmatrix} n \\ n \end{bmatrix}_2 = 1$

Dokaz V ima točno jedan 0-dim. potprostor $\{0\}$ i jedan n-dim. potprostor V

Prop 2 $\begin{bmatrix} n \\ 1 \end{bmatrix}_2 = \begin{bmatrix} n \\ n-1 \end{bmatrix}_2 = [n]_2$

Dokaz $\dfrac{2^n-1}{2-1} = 2^{n-1}+\dots+2+1 = [n]_2$ (za 1-dim)

Zrcale li nekim bijekcija između 1-dim. i (n-1)-dim. ?

$A = \langle a \rangle$, $a = (a_1, \dots, a_n) \in \mathbb{F}_2^n$, $a \neq 0$

$A^\perp = \{ (x_1, \dots, x_n) \in \mathbb{F}_2^n \mid a_1x_1 + \dots + a_nx_n = 0 \}$

Uvedemo „skalarni produkt" na $\mathbb{F}_2^n$:

$x \cdot y = x_1y_1 + \dots + x_ny_n \in \mathbb{F}_2$

To je simetrična bilinearna funkcional

Ne možemo garantirati o pozitivnosti, a nedegeneriranost treba definirati drugačije nego u $\mathbb{R}^n / \mathbb{C}^n$!

Može se dogoditi $x \cdot x = 0$, $x \neq 0$

Ali: $x \cdot y = 0, \forall y \in \mathbb{F}_2^n \Rightarrow x = 0$

Sada lako dokazemo simetricnost!

Prop. 3 $\binom{n}{k}_\Sigma = \binom{n}{n-k}_\Sigma$

Dokaz $W \longmapsto W^\perp$ je bijekcija između k-dim. i $(n-k)$-dim. potprostora od V

Alternativno, slijedi direktno iz zapisa

$$\binom{n}{k}_\Sigma = \frac{[n]_\Sigma!}{[k]_\Sigma! \, [n-k]_\Sigma!}$$

Pogledajmo još primjere...

$$\binom{5}{2}_\Sigma = \binom{5}{3}_\Sigma = \Sigma^6 + \Sigma^5 + 2\Sigma^4 + 2\Sigma^3 + 2\Sigma^2 + \Sigma + 1$$
$$= (1+\Sigma^2)(1+\Sigma+\Sigma^2+\Sigma^3+\Sigma^4)$$

$$\binom{6}{2}_\Sigma = \binom{6}{4}_\Sigma = \Sigma^8 + \Sigma^7 + 2\Sigma^6 + 2\Sigma^5 + 3\Sigma^4 + 2\Sigma^3 + 2\Sigma^2 + \Sigma + 1$$
$$= (1+\Sigma^2+\Sigma^4)(1+\Sigma^2+\Sigma^3+\Sigma^4)$$

$$\binom{6}{3}_\Sigma = \Sigma^9 + \Sigma^8 + 2\Sigma^7 + 3\Sigma^6 + 3\Sigma^5 + 3\Sigma^4 + 3\Sigma^3 + 2\Sigma^2 + \Sigma + 1$$
$$= (1+\Sigma^2)(1+\Sigma^3)(1+\Sigma+\Sigma^2+\Sigma^3+\Sigma^4)$$

Izgleda da su to polinomi, a ne racionalne funkcije!

Ako pogledate u to, kojeg bi bili stupnja?

$$\binom{n}{k}_\Sigma = \frac{(\Sigma^n-1)(\Sigma^{n-1}-1)\cdots(\Sigma^{n-k+1}-1)}{(\Sigma^k-1)(\Sigma^{k-1}-1)\cdots(\Sigma-1)}$$

$\longrightarrow$ Stupnja $\sum_{i=0}^{k-1}(n-i) = kn - \frac{k(k-1)}{2}$

$\longrightarrow$ Stupnja $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$

$$\deg \binom{n}{k}_2 = kn - \frac{k(k-1)}{2} - \frac{k(k+1)}{2} =$$

$$= kn - \frac{k^2 - k + k^2 + k}{2} = kn - k^2 = k(n-k)$$

Kako znamo da će pri dijeljenju brojnika s nazivnikom ostatak biti 0?

Tm. 4 (2-Pascalova rekurzija)

$$\binom{n}{k}_2 = 2^{n-k}\binom{n-1}{k-1}_2 + \binom{n-1}{k}_2$$

Dokaz Fiksiramo „hyperravninu", tj. $(n-1)$-dim. potprostor $H \leq V$. Kod prebrojavanja k-dim. potprostora W imamo dvije mogućnosti:

1.) $W \leq H$ Takvih ima $\binom{n-1}{k}_2$ po def.

2.) $W \not\leq H$ Tada je $\dim(W \cap H) = k-1$

Prvo izaberemo potprostor $W' = W \cap H$ na $\binom{n-1}{k-1}_2$ načina a zatim vektor $x \in V \setminus H$ t.d. je $W = \langle W' \cup \{x\} \rangle$

N.K.N. možemo izabrati x t.d. dodajemo razbijte W?

$$\frac{2^n - 2^{n-1}}{2^k - 2^{k-1}} = \frac{2^{n-1}(2-1)}{2^{k-1}(2-1)} = 2^{n-k}$$

Alternativna Σ-Pascalova rekurzija dobijamo iz simetrije:

$$\binom{n}{k}_\Sigma = \binom{n}{n-k}_\Sigma = \Sigma^{n-(n-k)} \binom{n-1}{n-k-1}_\Sigma + \binom{n-1}{n-k}_\Sigma$$

$$= \Sigma^{k} \binom{n-1}{k}_\Sigma + \binom{n-1}{k-1-k+k}_\Sigma =$$

$$= \binom{n-1}{k-1}_\Sigma + \Sigma^{k} \binom{n-1}{k}_\Sigma$$

Kombinatorni / linearnoalgebarski dokaz ???

Iz Pascalovih rekurzija indukcijom slijedi da je $\binom{n}{k}_\Sigma$ polinom stupnja $k(n-k)$

$$\binom{n}{k}_\Sigma = \binom{n-1}{k-1}_\Sigma + \Sigma^{k} \binom{n-1}{k}_\Sigma$$

$\nearrow$ $\qquad$ $\uparrow$

deg $(k-1)(n-1-k+1)$ $\qquad$ deg $k + k(n-1-k)$

$(k-1)(n-k)$ $\qquad$ $k(n-k)$

ne može poništiti vodeći član!

$$\binom{n}{k}_\Sigma = \Sigma^{n-k} \binom{n-1}{k-1}_\Sigma + \binom{n-1}{k}_2$$

$n-k + (k-1)(n-k) \qquad k(n-1-k)$

$k(n-k)$ ✓

Dakle,

$$\binom{n}{k}_2 = \sum_{i=0}^{k(n-k)} c(n,k,i)\, 2^i$$

Još jedna pravilnost: koeficijenti su simetrični po i!

$$c(n,k,i) = c(n,k,N-i), \quad i = 0,\dots,N$$

$$N = k(n-k)$$

Kako „okrenemo" koeficijente polinoma

$$p(x) = a_0 + a_1 x + \dots + a_n x^n ?$$

$$x^n p\left(\tfrac{1}{x}\right) = x^n\left(a_0 + a_1 x^{-1} + \dots + a_n x^{-n}\right) = a_n + a_{n-1} x + \dots + a_0 x^n$$

Dakle, koeficijenti su simetrični akko vrijedi identitet

$$p(x) = x^n p\left(\tfrac{1}{x}\right), \quad \forall x$$

Lako pokažemo

$$\binom{n}{k}_{1/2} = \frac{1}{2^{k(n-k)}} \binom{n}{k}_2$$

$$\binom{n}{k}_{\frac{1}{2}} = \frac{\left(\frac{1}{2}^n - 1\right)\left(\frac{1}{2}^{n-1} - 1\right)\cdots\left(\frac{1}{2}^{n-k+1} - 1\right)}{\left(\frac{1}{2}^k - 1\right)\left(\frac{1}{2}^{k-1} - 1\right)\cdots\left(\frac{1}{2} - 1\right)} \cdot \frac{2^n \cdot 2^{n-1} \cdots 2^{n-k+1}}{1} =$$

$$= \frac{(1-q^n)(1-q^{n-1})\cdots(1-q^{n-k+1})}{(1-q^k)(1-q^{k-1})\cdots(1-q)} \underbrace{\frac{1}{q^{(n-k)(n-1-(k-1))\cdots}}}_{k(n-k)} = \frac{1}{q^{k(n-k)}} \begin{bmatrix} n \\ k \end{bmatrix}_q$$

Sylvester je pokazao da je ruz koeficijenata od $\begin{bmatrix} n \\ k \end{bmatrix}_q$ unimodalan hipotezi teorija invarijanata. Može se pokazati kombinatorno, ali je gadno. Ovo je komb. interpret. koeficijenata:

$c(n,k,i)$ = broj rastućih šetnji u jediničnoj mreži od $(0,0)$ do $(k, n-k)$ takvih da je površina ispod šetnje točno i.

Tm (q-Binomni teorem)

$$\prod_{i=1}^{n} (1+q^i x) = \sum_{S \subseteq \{1,\dots,n\}} q^{\text{sum}(S)} x^{|S|} = \sum_{k=0}^{n} q^{\frac{k(k+1)}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q x^k$$

Pritom je $\text{sum}\, S = \sum_{i \in S} i$

Dakle, $\sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S|=k}} q^{\text{sum}(S)} = q^{\frac{k(k+1)}{2}} \begin{bmatrix} n \\ k \end{bmatrix}_q$

To je alternativna komb. interpretacija q-binomnih koef.!

Ima još interpretaciju:

$$\sum_{P \in L(m,n)} q^{par(P)} = \binom{m+n}{m}_q = \binom{m+n}{n}_q$$

$L(m,n)$ = skup svih najkraćih puteva od $(0,0)$ do (m,n)

$par(P)$ = površina između puta P i x-osi

$$\sum_{\pi \in S_n} q^{inv(\pi)} = [n]_q!$$

$inv(\pi)$ = broj inverzija permutacije π