Probabilità dell'indipendenza lineare di vettori appartenenti a spazi vettoriali su campi finiti

Giulio Ticli

14 novembre 2023

Sia $\mathbb{K}$ un campo finito con p elementi, n un numero naturale strettamente positivo e $V = \mathbb{K}^n$ uno spazio vettoriale su $\mathbb{K}$.

Si vuole risolvere il seguente quesito: qual è la probabilità che, scelti n vettori di V, essi siano tra loro linearmente indipendenti?

Sia c_i il numero di vettori $\mathbf{v}_i \in V$ tali che, se $S_{i-1} = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1})$ è una $(i-1)$-upla ordinata di vettori di V tra loro linearmente indipendenti, allora $S_i = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_i)$ è una i-upla ordinata di vettori linearmente indipendenti.

È chiaro che lo spazio vettoriale V è costituito da p^n vettori, in quanto per ognuna delle n componenti di un suo vettore esistono p possibili scelte. Ne segue che $c_1 = p^n - 1$, infatti ogni vettore diverso dal vettore nullo può essere scelto come primo vettore.

$c_2 = p^n - p$. Infatti ogni vettore $\mathbf{v}_2$ diverso da un multiplo di $\mathbf{v}_1$, eventualmente anche nullo, è una valida scelta. I multipli di $\mathbf{v}_1$ sono tutti quei vettori che si possono scrivere come $\lambda\mathbf{v}_1$ per qualche $\lambda \in \mathbb{K}$; esistono p scelte di λ, perciò esistono p multipli di $\mathbf{v}_1$.

In generale $c_i = p^n - p^{i-1}$. Infatti S_{i-1} è una $(i-1)$-upla di vettori linearmente indipendenti, perciò tutti e soli i vettori $\mathbf{u}_i$ che non si possono scegliere come i-esimo vettore $\mathbf{v}_i$ sono della forma

$$\mathbf{u}_i = \lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_{i-1}\mathbf{v}_{i-1} = \sum_{k=1}^{i-1} \lambda_k \mathbf{v}_k$$

per una opportuna scelta di λ_k. Poiché per ipotesi S_{i-1} forma una base di $\mathrm{Span}(S_{i-1})$, la scelta dei coefficienti λ_k è unica. Allora il numero di vettori $\mathbf{u}_i$ non validi è semplicemente il numero delle scelte di λ_k, ossia p^{i-1}.

Possiamo dunque concludere che, detto N il numero di n-uple S_n tali che i vettori contenuti in S_n siano linearmente indipendenti, vale

$$N = \prod_{i=1}^{n} c_i = \prod_{i=1}^{n} p^n - p^{i-1} = (p^n - 1)(p^n - p)(p^n - p^2)\ldots(p^n - p^{n-1})$$

Il numero totale T di possibili n-uple ordinate di vettori in V, incluse quelle che contengono vettori linearmente dipendenti, è semplicemente

$$T = (p^n)^n = p^{n^2} = \prod_{i=1}^{n} p^n$$

Perciò la probabilità $\mathcal{P}$ cercata è:

$$\mathcal{P}(p,n) = \frac{N(p,n)}{T(p,n)} = \prod_{i=1}^{n} \frac{p^n - p^{i-1}}{p^n} = \prod_{i=1}^{n} 1 - p^{i-1-n}$$

che, operando il cambio di indici $j = n + 1 - i$, diventa più semplicemente

$$\mathcal{P}(p,n) = \prod_{j=1}^{n} 1 - p^{-j}$$

È evidente che questa funzione $\mathcal{P}(p,n)$ è decrescente a parità di p al variare di n, infatti ciascun termine della produttoria è strettamente compreso tra 0 e 1 per costruzione (essendo $p \geq 2$, tutti i p^{-j}, da p^{-1} fino a p^{-n}, saranno numeri razionali positivi minori di 1).

È intuitivo inoltre che $\mathcal{P}(p,n)$ sia una funzione crescente a parità di n al variare di p. Anche questa dimostrazione non è difficile: sia $q \in \mathbb{N} \mid q > p$. Allora $\forall r \in \mathbb{R}^- \quad q^r < p^r$. Di conseguenza ogni termine della produttoria

$$\prod_{j=1}^{n} 1 - q^{-j}$$

sarà maggiore del corrispondente termine della produttoria

$$\prod_{j=1}^{n} 1 - p^{-j}$$

(si ricorda che gli esponenti $-j$ sono tutti negativi). Allora necessariamente $\mathcal{P}(q,n) > \mathcal{P}(p,n)$.

Si riporta una tabella dei valori di $\mathcal{P}(p,n)$ per $p \in \{2,3,5\}$ e $n \in \{1,2,3,4,5,6\}$.

n	$\mathcal{P}(2,n)$	$\mathcal{P}(3,n)$	$\mathcal{P}(5,n)$
1	$1/2 = 0.5$	$2/3 \approx 0.667$	$4/5 = 0.8$
2	$3/8 = 0.375$	$16/27 \approx 0.593$	$96/125 = 0.768$
3	≈ 0.328	≈ 0.571	≈ 0.7618
4	≈ 0.308	≈ 0.564	≈ 0.7606
5	≈ 0.298	≈ 0.5613	≈ 0.7604
6	≈ 0.293	≈ 0.5605	≈ 0.7603