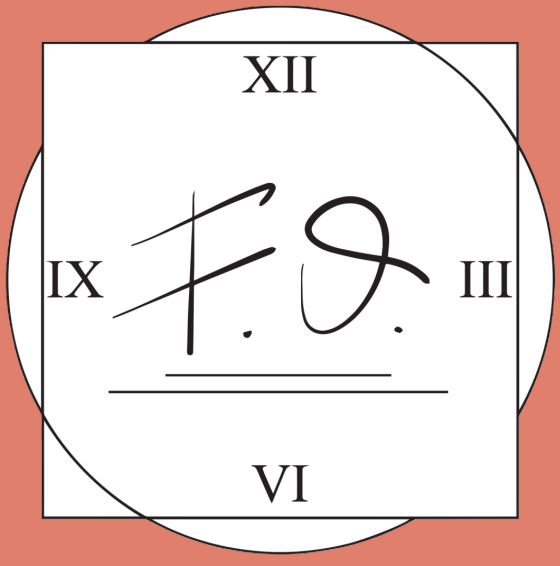
Fuori Orario

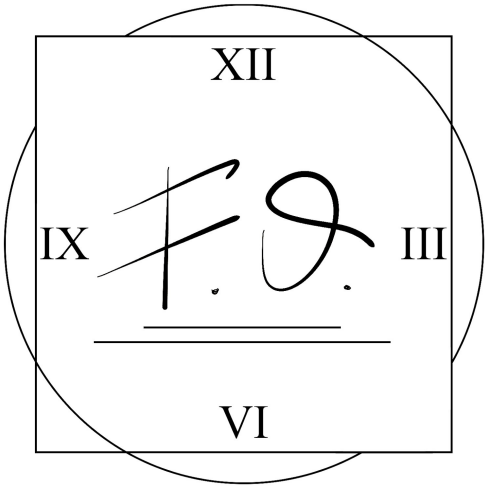
Resoconti di una giornata di seminari
30 Aprile 2026



Dipartimento di Matematica - Università degli Studi di Milano

FUORI ORARIO

Resoconti di una giornata di seminari
30 Aprile 2026



Fuori Orario
Resoconti di una giornata di seminari

30 Aprile 2026
Dipartimento di Matematica
Università degli Studi di Milano

Versione definitiva: Settembre 2026

Impaginazione in LaTeX e progetto grafico a cura di
Chiara Galimberti e Noemi Gennuso

INDICE

INTRODUZIONE 1

LA CONGETTURA DI KAKEYA *Damiano Bettega* 3

UNA RICETTA PER PARADOSSI *Elia Praderio* 5

HACKERIAMO UNA AI *Luca Simonelli* 13

DISCRETIZZIAMO UN IMPULSO ELETTRICO *Riccardo Donati, Chiara Galimberti* 17

L'IPOTESI DI RIEMANN SU CAMPI FINITI *Francesco Stoppa* 25

SULL'APPROSSIMAZIONE DIOFANTEA *Noemi Gennuso* 31

DAI TUMORI ALLE EPIDEMIE: COSA PUÒ DIRE LA MATEMATICA? *Kevin Arana* 35

INTRODUZIONE AI NUMERI P-ADICI *Sebastian Ocampo* 43

LA MECCANICA QUANTISTICA COME TEORIA STATISTICA *Lorenzo Silvidii, Matteo Razza* 59

GEOMETRIA DELLE TEORIE DI GAUGE *Mattia Belloni, Carlo Vittoli* 73

INTRODUZIONE

Caro lettore o cara lettrice,
sono lieta di vederti qui con in mano il libretto della decima edizione di Fuori Orario! In questa introduzione ci tengo a darti un assaggio dell'iniziativa, di cosa sta dietro e delle persone che ne rendono possibile la realizzazione. Anche quest'anno il nostro Dipartimento di Matematica in Via Saldini è rimasto chiuso, ergo non abbiamo potuto riprendere a frequentare il luogo cuore del percorso di ogni studente. Questo non ci ha fermati e Fuori Orario si è svolto mantenendosi saldo al suo scopo. Si tratta di una giornata di seminari organizzata dagli studenti per gli studenti, durante la quale hai la possibilità di immergerti, approfondendoli, in concetti matematici che alimentano la tua curiosità. Chi decide di ricoprire il ruolo di speaker si propone una sfida che porta soddisfazione e che incoraggia tutti al confronto. Partecipando ad organizzare, ma anche osservando come spettatore, entri in contatto con strumenti che incrementano le tue conoscenze e le tue competenze. Inoltre, le difficoltà diventano più leggere quando sei in un ambiente collaborativo che in questa iniziativa diventa realtà.

Sono una studentessa del corso di laurea triennale in matematica e da tempo faccio parte della famiglia di Fuori Orario, che da due anni coordino con Sara Donè. Dopo un cambio di corso, entrando nei nuovi luoghi, la lettura del libretto che mi è stato consegnato ha destato in me ispirazione e curiosità. Mi auguro che lo stesso succederà a te che stai leggendo! La matematica è un mondo immenso e permea quanto ci circonda, scegliere di studiarla è esplorazione così come ricerca.

Chi vorrà prendere parte al viaggio troverà un gruppo appassionato e accogliente. La giornata di quest'anno ha avuto 10 seminari che ci hanno trasportati in diverse aree della materia; ore in cui tanto si impara. Voglio riconoscere il lavoro di tutti coloro che già aiutano nell'impresa. Ringrazio gli organizzatori: Sara Donè, Eucantia Franzi, Alessandro Artoni, Stefano Barbaro, Alice Chen, Ines della Vedova, Chiara Galimberti, Noemi Gennuso, Giovanni Greco, Pietro Pellegrini, Francesco Stoppa. Ringrazio inoltre gli speaker e i professori che ci sostengono. Ogni singolo componente ha dato vita all'iniziativa. Fuori Orario lascia un messaggio importante che mi porto dietro e che arricchisce. Speriamo di rivederci con ancora più energia negli spazi del Dipartimento rinnovati.

È ora giunto il momento di salutarci e di lasciarti sfogliare le pagine che seguono, pronte ad accendere le tue idee.
Buon viaggio.

Eucantia Federica Franzi

LA CONGETTURA DI KAKEYA

DAMIANO BETTEGA

1. Introduzione

I dischi $D^n \subset \mathbb{R}^n$ possiedono diverse importanti proprietà, fra cui la seguente: contengono segmenti unitari orientati in tutte le direzioni dello spazio (ossia per ogni retta passante per l'origine, esiste un segmento di lunghezza 1 contenuto nel disco ad essa parallelo). Si scopre molto rapidamente che non sono gli unici insiemi a possedere la medesima proprietà: anche i seguenti (quadrato, triangolo deformato) la soddisfano!

Una caratteristica che accomuna tutti questi esempi, è che la dimensione di questi oggetti (intesa come la dimensione di Hausdorff) è esattamente pari a quella dello spazio ambiente: questo fatto ha intuitivamente senso, siccome la presenza di tutti i segmenti ruotati in ogni direzione ragionevolmente "ispessisce" il nostro insieme a sufficienza da massimizzare la dimensione. Ma quando si parla di matematica (ed in particoare teoria della misura, una branca ricca di patologie), questa intuizione non basta. Definiamo rigorosamente il protagonista e il problema ad esso connesso.

Definizione 1 (Insieme di Kakeya). Un insieme compatto $A \subset \mathbb{R}^n$ si dice **Kakeya** se per ogni retta dello spazio, esiste un segmento unitario in A parallelo ad essa.

Congettura 2 (di Kakeya). Un insieme di Kakeya in $\mathbb{R}^n$ ha dimensione di Hausdorff n.

Il caso 1-dimensionale è banale. Dimostreremo il caso nel piano, la cui prima dimostrazione è da attribuire a Davies [2]. Il caso 3-dimensionale è stato dimostrato recentemente da Hong Wang e Joshua Zahl ([4]). Il caso generale non è ancora stato dimostrato.
Questo problema è uno dei più vecchi della teoria geometrica della misura, ed affonda le sue radici nel lavoro di Besicovitch: egli, infatti, stava lavorando al seguente problema: trovare una funzione che fosse Riemann-integrabile in una regione del piano, ma non lungo alcuna retta per ogni direzione. Una possibile soluzione è data dalla funzione che vale 1 sui punti di coordinate razionali, zero altrimenti, definita su di un insieme di misura (2-dimensionale) di Lebesgue nulla, tale che però contiene un segmento in ogni direzione; tali insieme effettivamente si può costruire, e prende il nome di insieme di Besicovitch (che divenne il primo esempio di insieme di Kakeya non banale); una sua possibile costruzione è tramite il cosiddetto albero di Perron.

Successivamente, grazie anche al contributo di altri matematici, lo studio di questo genere di insiemi ha portato alla nascita della teoria geometrica della misura, con fruttuosi collegamenti all'analisi di Fourier.

2. Il teorema di Kakeya

Prima di iniziare, enunciamo un risultato chiave per la dimostrazione.

TEOREMA 3 (Teorema di proiezione di Marstrand). *Sia $A \subset \mathbb{R}^n$ un insieme di Borel, di dimensione di Hausdorff s. Se $s \leqslant 1$, allora la dimensione di Hausdorff della proiezione ortogonale di A su una retta passante per l'origine è s per Lebesgue-quasi ogni retta.*

Per la seguente dimostrazione, seguiamo Mattila [3] (pp. 144).

TEOREMA 4. *Per $n = 2$ la congettura di Kakeya è vera.*

Dimostrazione. Possiamo innanzitutto supporre che la misura del nostro insieme di Kakeya A sia zero, altrimenti la tesi è ovvia. Oltretutto, siccome ogni insieme è contenuto in un insieme di tipo G_δ della stessa misura, possiamo supporre che A sia G_δ. Per $a \in (0,1), b \in \mathbb{R}, q \in \mathbb{Q}$, denotiamo con $I(a,b,q)$ il segmento $\{(q+t, at+b) : 0 \leqslant t \leqslant 1/2\}$, di lunghezza minore di 1. Sia $C_q = \{(a,b) : I(a,b,q) \subset A\}$; osserviamo subito che è G_δ, dal momento che per ogni aperto B, l'insieme degli (a,b) tali che il segmento vi è contenuto è aperto. Indicata con π la proiezione sulla prima coordinata, per ipotesi di A insieme di Kakeya abbiamo che $\pi(C_q) = (0,1)$, perciò esiste un q tale che la misura di Hausdorff 1-dimensionale di C_q è positiva. Per il teorema di proiezione di Marstrand, significa che per Lebesgue-quasi ogni $t \in \mathbb{R}$, la dimensione di Haudorff di $\pi_t(\cup_{q\in\mathbb{Q}} C_q)$ è 1, dove $\pi_t(x,y) = tx + y$. Per $t \in [0, 1/2]$, abbiamo che $\{q+t\} \times \pi_t(C_q) = \{(q+t, at+b) : (a,b) \in C_q\} \subset A \cap \{(x,y) : x = q+t\}$; per un insieme di t di misura positiva, perciò, le sezioni verticali (dipendenti dal parametro) di A hanno dimensione 1. Per un risultato di teoria della misura questo implica che la dimensione di A è 2. □

Bibliografia

1 Falconer Kenneth, *Geometry of Fractals*, John Wiley & Sons, Terza Edizione, 2014.
2 Roy O. Davies, *Some remarks on the Kakeya problem*, Proc. Cambridge Phil. Soc. (1971), 69, 417-420.
3 Pertti Mattila, *Fourier Analysis and Hausdorff Dimension*, Cambridge studies in advanced mathematics, Cambridge University Press, 2015
4 Hong Wang e Joshua Zahl, *Sticky Kakeya sets and the sticky Kakeya conjecture*, Journal of American Mathematical Society (2026), 39.2, 515-585.

UNA RICETTA PER PARADOSSI

ELIA PRADERIO

Alice laughed.
"There's no use trying," she said: "one can't believe impossible things."
"I daresay you haven't had much practice," said the Queen. "When I was your age, I always did it for half-an-hour a day. Why, sometimes I've believed as many as six impossible things before breakfast."
- Lewis Carroll, *Through the Looking Glass*

1. Introduzione

In questo seminario voglio parlare più o meno nel dettaglio di paradossi, enunciati che sono contemporaneamente sia veri che falsi e di come siano tutti molto simili. Come spesso accade in matematica, ciò non è un caso e sono tutte diverse istanze di un procedimento comune, una vera e propria ricetta per paradossi.
Prima di partire direttamente con la matematica però, è bene fare un ripasso di grammatica. Un **aggettivo** è una parola che esprime proprietà di altre parole all'interno della frase. Per esempio nella frase

Il dipartimento è chiuso.

l'aggettivo *chiuso* esprime una proprietà del *dipartimento*. La cosa interessante è che gli aggettivi sono parole a loro volta e possiamo usare aggettivi per descrivere altri aggettivi. Per esempio:

La parola "italiana" è italiana.
La parola "francese" non è francese.
La parola "polisillabica" è polisillabica.
La parola "monosillabica" non è monosillabica.

DEFINIZIONE 1. Una parola è detta **eterologica** se **non** descrive sé stessa.

Domanda: la parola "eterologica" è eterologica oppure no?
Se non lo fosse allora descriverebbe sé stessa e quindi sarebbe eterologica e viceversa se lo fosse: è eterologica se e solo se non lo è, il che è paradossale.
A onor del vero sono obbligato a dire che dietro ad ogni paradosso c'è un trucco da prestigiatore, un'ipotesi falsa che il logico cerca di far passare come ovviamente vera gettando fumo negli occhi di chi ascolta. Per cercare di trovare il trucco, proviamo a tradurre questo paradosso in un linguaggio matematico, a noi più familiare.

Consideriamo l'insieme degli aggettivi Adj e l'insieme di valori di verità $\mathbf{2} = \{0, 1\}$. Il paradosso si può riassumere nel seguente diagramma commutativo:

$$\begin{array}{ccc} Adj \times Adj & \xrightarrow{\ g\ } & \mathbf{2} \\ {\scriptstyle\Delta}\uparrow & & \downarrow{\scriptstyle s} \\ Adj & \xrightarrow[\ f\ ]{} & \mathbf{2} \end{array}$$

Dove g è la funzione definita nel seguente modo

$$g(a_1,\, a_2) = \begin{cases} 1 & \text{se } a_2 \text{ descrive } a_1 \\ 0 & \text{altrimenti} \end{cases}$$

Prima di applicare la funzione g però ci precomponiamo un'altra funzione: la funzione diagonale Δ, definita come

$$\begin{aligned} \Delta :\ Adj &\longrightarrow Adj \times Adj \\ a &\longmapsto (a,\, a) \end{aligned}$$

La funzione $g \circ \Delta$ così ottenuta è la funzione caratteristica di tutti quegli aggettivi che descrivono sé stessi, ma dato che a noi interessano quelli che **non** descrivono sé stessi ci dobbiamo comporre una funzione che esprima questa negazione.

$$\begin{aligned} s :\ \mathbf{2} &\longrightarrow \mathbf{2} \\ 0 &\longmapsto 1 \\ 1 &\longmapsto 0 \end{aligned}$$

La funzione $f = s \circ g \circ \Delta$ identifica quindi tutti gli aggettivi eterologici. Questo diagramma, ed il teorema dietro ad esso, sono alla base di un'intera famiglia di paradossi detti argomenti diagonali a causa del loro legame con la funzione Δ. prima di poter enunciare il teorema però, dobbiamo parlare di funzioni e di prodotti.

2. Prodotti ed Esponenziali

Quando abbiamo una funzione che ha come dominio un prodotto, succede un fatto interessante che diamo sempre per scontato. Consideriamo la funzione

$$g : A \times B \longrightarrow C$$

Se fissiamo un elemento di B, diciamo $b \in B$, otteniamo immediatamente una nuova funzione

$$\begin{aligned} g_b :\ A &\longrightarrow C \\ a &\longmapsto g_b(a) = g(a, b) \end{aligned}$$

che siamo soliti chiamare funzione parametrica. La cosa interessante è che per ogni elemento di B questa costruzione fornisce univocamente una funzione g_b, e cioè stiamo implicitamente definendo un'altra funzione

$$\begin{aligned} \overline{g} : B &\longrightarrow C^A \\ b &\longmapsto g_b \end{aligned}$$

Tale funzione $\overline{g}$ è detta la **funzione compagna** di g, poiché ogni g determina univocamente una $\overline{g}$ e viceversa. A cosa serve tutto ciò? L'idea è che gli oggetti esponenziali come C^A sono abbastanza rari e complicati in matematica, mentre i prodotti sono oggetti molto più familiari. Ha dunque senso considerare solo funzioni della forma g anziché le loro compagne $\overline{g}$, dal momento che trasmettono le stesse identiche informazioni ma sono molto più facili da studiare.
Qual è il costo da pagare? Il costo è che - come suggerisce il nome - gli oggetti esponenziali sono più grandi dei prodotti e dunque non tutte le funzioni $f : A \to C$ sono della forma g_b. Quelle che invece lo sono, godono di proprietà speciali che valgono un nome proprio.

DEFINIZIONE 2. Una mappa $f : A \to C$ è detta **rappresentabile** da $g : A \times B \to C$ se esiste $b \in B$ tale che

$$f(-) = g(-, b)$$

Quando una certa g rappresenta *tutte* le funzioni f, succede qualcosa di bizzarro.

TEOREMA 3 (di punto fisso di Lawvere). *Siano A e C insiemi e $g : A \times A \to C$ tale che ogni $f : A \to C$ sia rappresentabile da g. Allora ogni endomorfismo $s : C \to C$ ammette un punto fisso, ovvero un elemento c tale che $s(c) = c$.*

Dimostrazione. Siano A, C, g ed s come nell'enunciato del teorema e costruiamo una f come nella sezione precedente.

$$\begin{array}{ccc} A \times A & \xrightarrow{\ g\ } & C \\ {\scriptstyle\Delta}\uparrow & & \downarrow{\scriptstyle s} \\ A & \xrightarrow[\ f\ ]{} & C \end{array}$$

Dato che - per ipotesi - tale f è rappresentata da g, esisterà un elemento $a \in A$ tale che

$$f(-) = g(-, a)$$

Ma quindi, valutando f in a otteniamo

$$g(a, a) = f(a) = sg\Delta(a) = sg(a, a)$$

Dunque $c = g(a, a)$ è punto fisso per s. □

Il risultato che interessa a noi però è il seguente

Corollario 4 (Contronominale). *Se C è un insieme ed esiste $s : C \to C$ senza alcun punto fisso, allora per ogni insieme A e per ogni funzione $g : A \times A \to C$ esiste una funzione $f : A \to C$ che non è rappresentabile da g e tale funzione è precisamente*

$$f = sg\Delta$$

3. Applicazioni del Corollario

Paradosso di Russell: Consideriamo l'insieme di tutti gli insiemi $Sets$ e la solita negazione $s : \mathbf{2} \to \mathbf{2}$. Inoltre consideriamo la funzione g data da

$$g(A, B) = \begin{cases} 1 & \text{se } A \in B \\ 0 & \text{se } A \notin B \end{cases}$$

e costruiamo il diagramma visto prima.

$$\begin{array}{ccc} Sets \times Sets & \xrightarrow{\ g\ } & \mathbf{2} \\ {\scriptstyle\Delta}\uparrow & & \downarrow{\scriptstyle s} \\ Sets & \xrightarrow[\ f\ ]{} & \mathbf{2} \end{array}$$

Dal momento che s non ammette punto fisso, il corollario ci assicura che f non può essere rappresentata da g. Ovvero per ogni insieme B

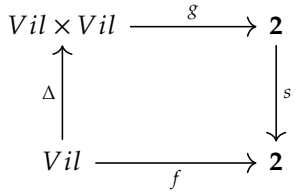
$$f(-) \neq g(-, B) = \chi_B$$

E cioè f non può essere una funzione caratteristica, ma ciò è assurdo perché f è una funzione che ha come codominio $\mathbf{2}$. Essere arrivati ad un assurdo implica l'essere partiti da un'ipotesi falsa e in questo caso è l'insieme di tutti gli insiemi: tale insieme non può esistere.
Dal punto di vista semantico, se f fosse davvero una funzione caratteristica, quale insieme caratterizzerebbe? Essa identifica l'insieme di tutti gli insiemi che non appartengono a sé stessi. Tale insieme appartiene a sé stesso oppure no?

Paradosso del Barbiere: In un villaggio Vil vive un barbiere che rade tutti gli abitanti del villaggio che non si radono da soli. Consideriamo la funzione g che esprima la relazione "b rade a"

$$g(a, b) = \begin{cases} 1 & \text{se } b \text{ rade } a \\ 0 & \text{altrimenti} \end{cases}$$

e costruiamo il solito diagramma.



La funzione f identifica tutte quelle persone che non si radono da sole, e che dunque vengono rasate dal barbiere. Tale gruppo di persone include il barbiere oppure no?

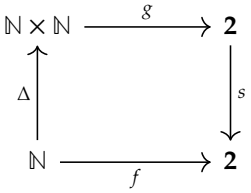
Teorema di Cantor: Non tutte le applicazioni del corollario sono paradossali, ma questo risultato sembrò tale a molti matematici dell'epoca.

TEOREMA 5. *La cardinalità di* $\mathbb{N}$ *è strettamente inferiore a quella di* $\mathscr{P}(\mathbb{N})$

Dimostrazione. Sia $S_0, \dots, S_n, \dots$ una possibile enumerazione di $\mathscr{P}(\mathbb{N})$, e consideriamo la funzione g data da

$$g : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbf{2}$$
$$(n, m) \longmapsto \begin{cases} 1 & \text{se } n \in S_m \\ 0 & \text{altrimenti} \end{cases}$$

E costruiamo il solito diagramma



Chiamiamo F l'insieme identificato dalla funzione f. Dal momento che s non ha punti fissi, il Corollario ci conferma che f non può essere rappresentata da g, ovvero che per ogni numero naturale m

$$\chi_F = f(-) \neq g(-, m) = \chi_{S_m}$$
$$\Longrightarrow F \neq S_m \quad \forall m \in \mathbb{N}$$

e dunque l'enumerazione proposta non può coprire tutto $\mathscr{P}(N)$. □

4. Applicazioni del Teorema

A onor del vero, non solo il corollario è utile a fornire risultati paradossali, ma anche il teorema vero e proprio ha svariate applicazioni, alcune delle quali sono pure molto famose.

Nota per il lettore: i teoremi famosi spesso richiedono strumenti avanzati, che possono creare confusione se non si ha già familiarità con essi. Pertanto vorremmo ricordare ai lettori - specie quelli all'inizio del loro percorso matematico - che questo è solo un

seminario divulgativo, e che non c'è bisogno di sbattere troppo la testa sui particolari delle dimostrazioni se questi risultano troppo oscuri.

Notazione:
- $B(x)$ identifica una **formula** nella variabile libera "x". Per esempio, assumendo di essere in un linguaggio che ci permetta di parlare di aritmetica, la formula $B(x)$ potrebbe identificare qualcosa del tipo "$x > 2$". Non è né vera né falsa a priori, ma dipende dal valore di x.
- $\ulcorner B(x) \urcorner$ identifica il **Gödeliano** della formula $B(x)$. Ovvero un numero naturale univocamente associato alla formula $B(x)$. L'idea è che se siamo in un linguaggio con un numero finito di simboli, abbiamo solo una quantità numerabile di stringhe finite costruite con questi simboli e cioè le formule.
- $D : \mathbb{N} \to \mathbb{N}$ identifica la funzione ricorsiva data da

$$\begin{aligned} D : \mathbb{N} &\longrightarrow \mathbb{N} \\ \ulcorner B(x) \urcorner &\longmapsto \ulcorner B(\ulcorner B(x) \urcorner) \urcorner \end{aligned}$$

- L^i identifica l'insieme* delle formule in i variabili libere quozientata sulla relazione di equivalenza $\sim$ data da

$$\varphi \sim \psi \quad \text{se e solo se} \quad \varphi \leftrightarrow \psi$$

Per esempio, le formule "$(x < 0) \wedge (x > 0)$" e "$x = 0$" sono tecnicamente due formule diverse ma semanticamente vogliono dire la stessa cosa, e quindi le identifichiamo con una sola classe di equivalenza.

TEOREMA 6 (Lemma di Diagonalizzazione). *Per ogni formula $E(x)$ esiste una formula chiusa C tale che*

$$C \longleftrightarrow E(\ulcorner C \urcorner)$$

Dimostrazione. Consideriamo le seguenti funzioni.

$$\begin{aligned} g : L^1 \times L^1 &\longrightarrow L^0 \\ (B(x),\, H(y)) &\longmapsto H(\ulcorner B(x) \urcorner) \end{aligned}$$

$$\begin{aligned} \Phi_E : L^0 &\longrightarrow L^0 \\ P &\longmapsto E(\ulcorner P \urcorner) \end{aligned}$$

Con queste possiamo costruire l'ormai familiare diagramma

$$\begin{array}{ccc} L^1 \times L^1 & \xrightarrow{\;g\;} & L^0 \\ {\scriptstyle\Delta}\uparrow & & \downarrow{\scriptstyle\Phi_E} \\ L^1 & \xrightarrow[\;f\;]{} & L^0 \end{array}$$

*In realtà è un'algebra, detta algebra di Lindenbaum-Tarski.

Il fatto interessante che contraddistingue questo caso dai precedenti è che f è effettivamente rappresentabile da g. Infatti, esplicitamente f è data da

$$\begin{aligned} f(B(x)) &= \Phi_E\, g(B(x), B(x)) \\ &= \Phi_E(B(\ulcorner B(x) \urcorner) \\ &= E(\ulcorner B(\ulcorner B(x) \urcorner) \urcorner) \end{aligned}$$

Consideriamo adesso la formula $F(x) = E(D(x))$. Vale che

$$\begin{aligned} f(B(x)) &= E(\ulcorner B(\ulcorner B(x) \urcorner) \urcorner) \\ &= E(D(\ulcorner B(x) \urcorner)) \\ &= F(\ulcorner B(x) \urcorner) \\ &= g(B(x), F(y)) \end{aligned}$$

Dunque f è rappresentabile da g e, per il Teorema di Lawvere, Φ_E presenta un punto fisso. Ovvero esiste una formula $C \in L^0$ tale che

$$C = \Phi_E(C) = E(\ulcorner C \urcorner)$$

e dunque

$$C \longleftrightarrow E(\ulcorner C \urcorner)$$

□

Il lemma di diagonalizzazione è centrale in svariati argomenti logici, in quanto codifica in termini matematici l'autoreferenzialità. Il più famoso teorema nell'ambito della logica matematica è uno di tali argomenti.

COROLLARIO 7 (Primo teorema d'incompletezza di Gödel). *Esistono formule impossibili da dimostrare e impossibili da confutare.*

Dimostrazione. Sia $Prov(y, x)$ l'enunciato

"*y è il Gödeliano di una dimostrazione di un enunciato il cui Gödeliano è x.*"

Ovvero essenzialmente dice "y è una dimostrazione per x". Sia ora

$$E(x) = \forall y \neg Prov(y, x)$$

Che essenzialmente dice "nessun y è una dimostrazione di x", ovvero "x è indimostrabile". Adesso, grazie al lemma di diagonalizzazione sappiamo che esiste una formula chiusa C tale che

$$C \longleftrightarrow E(\ulcorner C \urcorner)$$

E cioè C è equivalente all'enunciato

"*Questo enunciato è indimostrabile.*"

Tale enunciato è sia indimostrabile che inconfutabile. Infatti, se C fosse dimostrabile sarebbe vero, e - per quanto afferma C stesso - indimostrabile. Se invece fosse dimostrabile $\neg C$, avremmo che C è falso e cioè che C è dimostrabile. □

Bibliografia

[Lawvere] Lawvere F. William, "Diagonal Arguments and Cartesian Closed categories". Reprints in Theory and Applications of Categories, No. 15, 2006, pp. 1–13.

[Barreto] Barreto Joaquim Reizi, "A Survey on Lawvere's Fixed-Point Theorem". 2025, arXiv:2503.13536

[Gödel] Gödel Kurt, "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme, I". Monatshefte für Mathematik und Physik, v. 38 n. 1, 1931, pp. 173–198.

HACKERIAMO UNA AI

LUCA SIMONELLI

1. Introduzione alla Topological Data Analysis (TDA)

La **Topological Data Analysis (TDA)** si pone come ponte tra la topologia e la statistica, ponendosi l'obiettivo dello studio dei fondamenti geometrici dei dati statistici.

1.1. Simplessi e Complessi Simpliciali

Definizione 1.1 (Simplesso). Sia $k \geq 0$. Un *k-simplesso* σ in $\mathbb{R}^m$ è il più piccolo insieme convesso contenente un insieme P di $k+1$ punti affinementi indipendenti.

- 0-simplesso → punto / vertice
- 1-simplesso → edge / lato / segmento
- 2-simplesso → triangolo
- 3-simplesso → tetraedro

Definizione 1.2 (Faccia). Sia $0 \leq k' \leq k$. Una *k'-faccia* di σ è il k'-simplesso dato dal più piccolo convesso generato da un sottoinsieme di P di cardinalità $k'+1$.

Definizione 1.3 (Complesso Simpliciale). Un *complesso simpliciale* (o triangolazione) K è un insieme finito di simplessi tale che:

(1) K contiene tutte le facce di ogni suo simplesso;
(2) Per ogni $\sigma, \tau \in K$, l'intersezione $\sigma \cap \tau$ è vuota ($\varnothing$) oppure è una faccia comune di entrambi.

Definizione 1.4 (k-scheletro). Sia $k \geq 0$. Il *k-scheletro* di K, indicato con K^k, è il sottocomplesso formato da tutti i simplessi di dimensione al più k.

2. Catene, Bordo e Omologia

2.1. m-catene

Sia K un complesso simpliciale e $m \in \mathbb{N}$. Si dice *m-catena* una somma formale (o unione) di m-simplessi di K a coefficienti in $\mathbb{Z}_2$ (ossia modulo 2):

$$c = \sum_i a_i \sigma_i, \quad \sigma_i \in K \ (m\text{-simplessi}), \quad a_i \in \{0, 1\}.$$

2.2. Operatore di Bordo

Definizione 2.1 (Bordo di un simplesso e di una catena). Il bordo di un m-simplesso K, indicato con $\partial_m K$, è la somma delle sue facce di dimensione $m-1$. Di conseguenza, il bordo di una m-catena $c = \sum_i a_i \sigma_i$ è la $(m-1)$-catena definita da:

$$\partial_m c = \sum_i a_i \partial_m \sigma_i.$$

L'operatore di bordo mappa m-catene in $(m-1)$-catene riducendo la dimensione:

$$\dots \xrightarrow{\partial_{m+2}} C_{m+1} \xrightarrow{\partial_{m+1}} C_m \xrightarrow{\partial_m} C_{m-1} \xrightarrow{\partial_{m-1}} \dots$$

Definizione 2.2 (m-ciclo). Un' m-catena c è detta *m-ciclo* se ha bordo nullo:

$$\partial_m c = 0.$$

Teorema 2.1 (Proprietà fondamentale del bordo). Se d è una $(m+1)$-catena, allora il suo bordo è un m-ciclo, ossia:

$$\partial_m(\partial_{m+1} d) = 0 \quad (\text{ovvero } \partial^2 = 0).$$

Definizione 2.3 (Gruppo di Omologia). Due m-cicli c_1, c_2 appartengono allo stesso gruppo di omologia H_m se differiscono al più per il bordo di una $(m+1)$-catena (ossia $c_1 - c_2 = \partial d$).

3. Omologia Persistente

Sia K un complesso simpliciale e $f : K \to \mathbb{R}$ una funzione monotona non decrescente (cioè se σ è faccia di $\tau \in K \implies f(\sigma) \leq f(\tau)$).

Consideriamo l'insieme finito dei valori assunti da f: $a_0 \leq a_1 \leq a_2 \leq \dots \leq a_n$. Ponendo $a_0 = -\infty$, per ogni a_i definiamo il sottocomplesso:

$$K_i = K(a_i) = f^{-1}((-\infty, a_i]).$$

Si dice *filtrazione* la sequenza finita di sottocomplessi nidificati:

$$\varnothing \subseteq K_0 \subseteq K_1 \subseteq \dots \subseteq K_n = K.$$

L'omologia persistente caratterizza la struttura di K a dimensioni diverse ottenendo il **diagramma di persistenza**.

4. Persistence Landscapes e Teorema di Stabilità

Poiché i diagrammi di persistenza presentano un costo computazionale elevato per il calcolo diretto delle distanze, si introducono rappresentazioni funzionali alternative come i **Persistence Landscapes**.

Definizione 4.1 (Landscape). Un diagramma di persistenza trasforma la coppia di nascita-morte (b_i, d_i) nella funzione $f_{(b_i,d_i)}(t) = \max\{0, \min(t-b_i, d_i-t)\}$. Il landscape $L(k,t)$ nello spazio di Banach è definito come:

$$\lambda(k,t) = \text{il } k\text{-esimo valore più grande di } \{f_{(b_i,d_i)}(t)\}_i \quad \forall t.$$

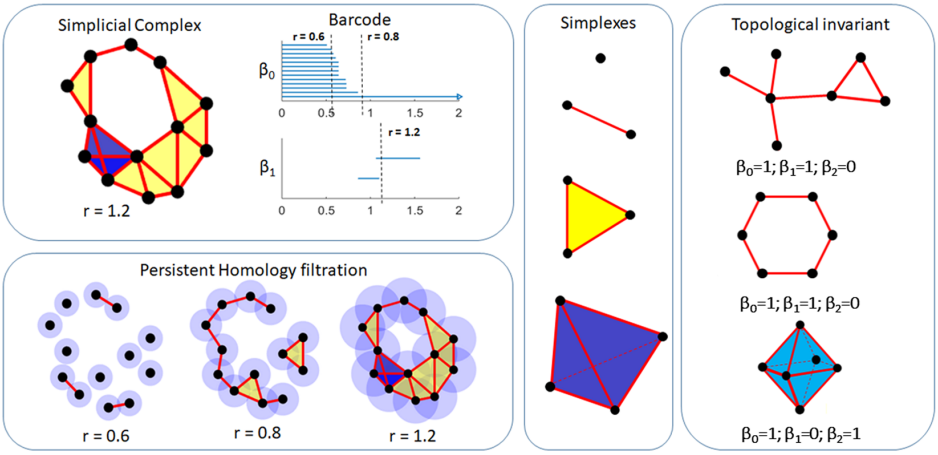


FIGURA 1. Panoramica sui concetti chiave della TDA: complesso simpliciale, filtrazione, barcode/diagrammi di persistenza, simplessi e invarianti topologici $(\beta_0, \beta_1, \beta_2)$.

In particolare, $\lambda(1, t)$ rappresenta il profilo delle caratteristiche più persistenti. Campionando la funzione λ si ottiene un vettore n-dimensionale, permettendo di calcolare facilmente medie, deviazioni standard e altre metriche statistiche.

4.0.1. *Distanze tra Diagrammi di Persistenza.* Siano D_1, D_2 due diagrammi di persistenza e $\gamma : D_1 \to D_2$ una bigezione tra i punti dei due diagrammi (inclusi i punti sulla diagonale).

DEFINIZIONE 4.2 (Distanza Bottleneck d_B). Rappresenta il costo dello spostamento del punto più distante tra i due diagrammi:

$$d_B(D_1, D_2) = \inf_{\gamma: D_1 \to D_2} \sup_{x \in D_1} \|x - \gamma(x)\|_\infty.$$

DEFINIZIONE 4.3 (Distanza Wasserstein d_W). Somma gli spostamenti di tutti i punti nel diagramma (solitamente con $p \approx 2$):

$$d_W(D_1, D_2) = \left(\inf_{\gamma: D_1 \to D_2} \sum_{x \in D_1} \|x - \gamma(x)\|_\infty^p \right)^{1/p}.$$

TEOREMA 4.1 (Teorema di Stabilità). Sia X uno spazio topologico (ad es. un grafo) e siano $f, g : X \to \mathbb{R}$ funzioni continue (che rappresentano funzioni di attivazione). Siano $D(f)$ e $D(g)$ i rispettivi diagrammi di persistenza. Allora vale la disuguaglianza:

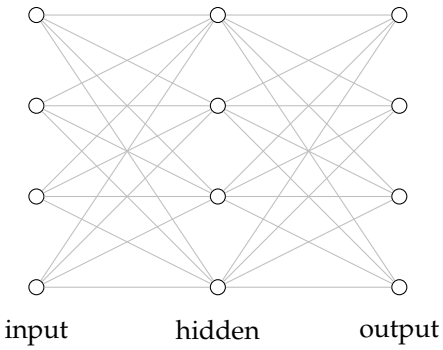
$$d_B(D(f), D(g)) \leq \|f - g\|_\infty,$$

dove d_B indica la distanza Bottleneck.

5. Applicazioni: Reti Neurali e Attacchi Adversarial

5.1. Rappresentazione di una Rete Neurale

Una rete neurale architetturale classica è composta da layer di Input, Hidden e Output:



5.2. Applicazione nel Deep Learning

Dati appartenenti alla stessa categoria avranno strutture topologiche analoghe. Un dato immesso nella rete genera un pattern di attivazioni nei vari layer. Se i neuroni di un livello si trovano in un'alta dimensione, l'attivazione genera una "nuvola di punti" di cui si studia l'omologia persistente.

5.3. Attacchi Adversarial

Un attacco adversarial modifica alcuni dati in modo da mantenerli invariati "visivamente", ma tali che li forzano ad occupare regioni dello spazio latente topologicamente incoerenti con l'originale manifold dei dati.

Controllo con la teoria:

(1) Per ogni livello della rete, si confronta il diagramma del dato corrente con un "diagramma medio" ottenuto durante la fase di training.
(2) Si utilizzano metriche come la distanza di **Bottleneck** (d_B) o di **Wasserstein** (d_W) imponendo una soglia di tolleranza.

DISCRETIZZIAMO UN IMPULSO ELETTRICO

RICCARDO DONATI, CHIARA GALIMBERTI

1. Problema

Si considera il seguente sistema Monodominio, con $\Omega = (0,1)^2$ e $x = (x,y) \in \Omega$, costituito da un'equazione parabolica di reazione-diffusione accoppiata con l'equazione differenziale ordinaria del modello di membrana di Roger McCulloch:

$$\begin{cases} c_m \frac{\partial v}{\partial t} - \operatorname{div}(D\nabla v) = -Gv\left(1 - \frac{v}{v_{th}}\right)\left(1 - \frac{v}{v_p}\right) - \eta_1 vw + I_{app} & (x,t) \in \Omega \times [0,T] \\ \frac{\partial w}{\partial t} = \eta_2\left(\frac{v}{v_p} - w\right) & (x,t) \in \Omega \times [0,T] \\ D\nabla v \cdot n = 0 & (x,t) \in \partial\Omega \times [0,T] \\ v(x,0) = 0 & x \in \Omega \\ w(x,0) = 0 & x \in \Omega \end{cases}$$

2. Descrizione fisica

Il modello descrive il comportamento di una membrana biologica quando viene stimolata da un impulso elettrico. In particolare, esso modella la generazione e la propagazione di un potenziale d'azione in un tessuto eccitabile, come il muscolo cardiaco o il tessuto nervoso. Questo modello rappresenta una generalizzazione dell'equazione di FitzHugh-Nagumo.

Il dominio Ω rappresenta una porzione di tessuto biologico. All'interno di questo dominio:

- La variabile v indica il potenziale di membrana.
- La variabile w rappresenta la variabile di recupero, ossia il meccanismo che riporta la membrana al suo stato di riposo.
- Lo stimolo elettrico esterno, indicato con I_{app}, è la corrente applicata alla membrana che dà origine alla propagazione dell'onda. Tale stimolo viene applicato all'istante iniziale per una durata breve, localizzato in un intorno circolare dell'origine.

I parametri del modello sono costanti fissate, con valori standard tratti dal contesto fisico del problema. Essi sono definiti come segue:

- c_m: capacità elettrica della membrana;
- D: coefficiente di diffusione della corrente elettrica (rappresentato da una matrice);

- v_{th}: potenziale soglia che deve essere superato per innescare la propagazione dell'onda;
- v_p: valore massimo raggiungibile dal potenziale v;
- η_2: velocità di recupero, che determina la rapidità con cui la membrana torna allo stato di riposo;
- η_1: parametro di accoppiamento tra v e w, che ne regola la relazione;
- G: fattore di scala che modula l'intensità della corrente applicata.

Affinché il sistema sia ben posto, il modello è completato da:

(1) Condizioni al contorno di Neumann omogenee: queste condizioni impongono che il tessuto sia isolato elettricamente, ovvero che nessuna corrente possa fluire attraverso i bordi del dominio Ω.
(2) Condizioni iniziali: all'istante $t = 0$, il tessuto si trova in uno stato di riposo, con valori iniziali di v e w che riflettono questa condizione.

3. Formulazione variazionale

Le equazioni presenti nel sistema sono soddisfatte puntualmente: per ogni x appartenente al dominio di definizione e per ogni istante temporale t. Nella formulazione variazionale invece le equazioni risultano soddisfatte per ogni funzione test (appartenente ad un opportuno spazio di funzioni) e per ogni istante t.

Per semplicità di notazione, si definisce la funzione:

$$G(v, w) = Gv\left(1 - \frac{v}{v_{th}}\right)\left(1 - \frac{v}{v_p}\right) + \eta_1 vw$$

dove le funzioni v, w, ed I_{app} sono definite da $\Omega \times [0, T]$ a valori in $\mathbb{R}$.

Si procede a modificare il sistema nella formulazione variazionale associata, moltiplicando ogni termine per una funzione ψ, detta funzione test, e integrando sul dominio Ω:

$$\begin{cases} \int_\Omega c_m \frac{\partial v}{\partial t}\psi - \int_\Omega \operatorname{div}(D\nabla v)\psi + \int_\Omega G(v, w)\psi = \int_\Omega I_{\text{app}}\psi \\ \int_\Omega \frac{\partial w}{\partial t}\psi = \int_\Omega \eta_2 \left(\frac{v}{v_p} - w\right)\psi \end{cases}$$

Il secondo addendo della prima equazione viene riformulato utilizzando l'integrazione per parti:

$$-\int_\Omega \operatorname{div}(D\nabla v)\psi = \int_\Omega D\nabla v \nabla\psi - \int_{\partial\Omega} D\nabla v \cdot n\psi$$

dove, grazie alle condizioni al contorno, l'integrale eseguito su $\partial\Omega$ risulta nullo.

Questa nuova formulazione è equivalente all'originale, a patto di utilizzare i giusti spazi funzionali, affinché risultino ben definiti gli integrali presenti e l'operazione di integrazione per parti sul bordo del dominio.

Considerando la mappa G come se fosse un termine lineare, per la buona definizione del sistema e delle operazioni svolte, le funzioni devono almeno appartenere ai seguenti spazi:

- $I_{app} \in L^2(0,T;L^2(\Omega))$: ad ogni istante temporale la funzione risulta quadrato integrabile.
- $v, w, \partial_t v, \partial_t w \in L^2(0,T;H^1(\Omega))$: ad ogni istante temporale le funzioni risultano quadrato integrabili con gradiente quadrato integrabile.
- $\psi \in H^1(\Omega)$.

Denotando il prodotto scalare in $L^2(\Omega)$ e la forma bilineare $a(\cdot,\cdot)$ come:

$$\langle f, g\rangle = \int_\Omega fg \qquad a(f,g) = \int_\Omega D\nabla f \nabla g$$

la scrittura definitiva della formulazione variazionale è quindi la seguente: per ogni $\psi \in H^1(\Omega)$ e ad ogni istante temporale t:

$$\begin{cases} c_m\langle \frac{\partial v(t)}{\partial t}, \psi\rangle + a(v(t),\psi) + < G(v(t),w(t)),\psi\rangle = \langle I_{\text{app}}(t),\psi\rangle & \forall \psi \in H^1(\Omega) \\ \langle \frac{\partial w(t)}{\partial t}, \psi\rangle = \langle \eta_2\left(\frac{v(t)}{v_p} - w(t)\right),\psi\rangle & \forall \psi \in H^1(\Omega) \end{cases}$$

Questo sistema, ad ogni istante temporale, è caratterizzato da un'infinità di condizioni, date dalle ψ che vivono nello spazio $H^1(\Omega)$ di dimensione infinita.

Si procede quindi con la discretizzazione del problema per raggiungere una quantità finita di condizioni, rappresentabili al calcolatore.
Per fare ciò esistono vari metodi. Di seguito si presenta l'idea del metodo agli elementi finiti $\mathbf{Q}^1$.

4. Discretizzazione in spazio

Si suddivide $\overline{\Omega} = [0,1]^2$ con una griglia cartesiana di quadratini E_j (detti elementi) di lato $h > 0$. Si denota con $\mathfrak{T}_h$ l'insieme di tali elementi, detto triangolazione. I vertici x_j degli elementi sono detti nodi di discretizzazione, e si suppone che il loro numero totale sia N.

Definizione 1 (Spazio $\mathbf{Q}^1$). Si definisce lo spazio agli elementi finiti $\mathbf{Q}^1$ come lo spazio di funzioni:

$$V_h = \{v_h \in C^0(\overline{\Omega}) \quad | \quad v_{h_{|E_j}} \in \mathbb{Q}^1\}$$

dove $\mathbb{Q}^1$ denota lo spazio dei polinomi bilineari in x ed y, cioè i polinomi della forma $p(x,y) = a + bx + cy + dxy$

Osservazione 2. Lo spazio V_h è caratterizzato da:

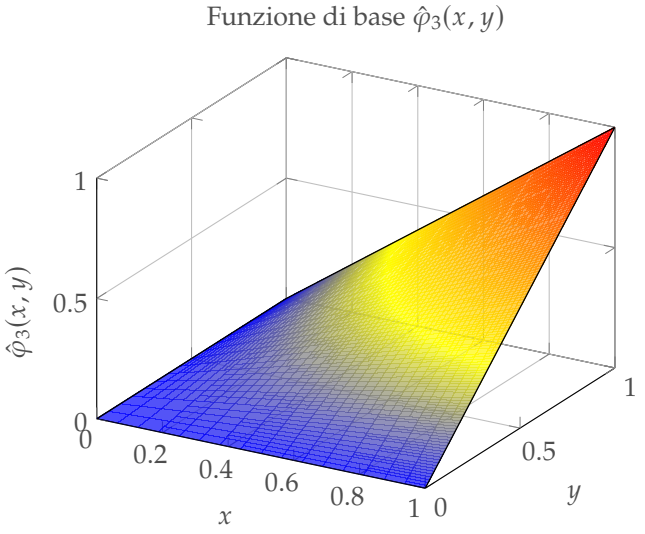
- $V_h \subset V = H^1(\Omega)$
- $\dim V_h = N$

Definizione 3 (Base nodale). Dato che V_h è uno spazio finito-dinensionale, si può considerare una sua base $\{\varphi_i\}_{i=1}^N$, detta base nodale, tale che $\varphi_i(x_j) = \delta_{ij}$, perciò su ogni elemento E_j vivono quattro funzioni di base.

Ad esempio, sul quadrato di riferimento $[0, h]^2$ le funzioni di base sono:

- $\hat{\varphi}_1(x, y) = 1 - \frac{x}{h} - \frac{y}{h} + \frac{xy}{h^2}$
- $\hat{\varphi}_2(x, y) = \frac{x}{h} - \frac{xy}{h^2}$
- $\hat{\varphi}_3(x, y) = \frac{y}{h} - \frac{xy}{h^2}$
- $\hat{\varphi}_4(x, y) = \frac{xy}{h^2}$

Il grafico sottostante rappresenta una delle funzioni di base, nel caso $h = 1$, per dare un'idea della costruzione:



Ora si può passare all'approssimazione spaziale sostituendo lo spazio originale $V = H^1(\Omega)$ con $V_h = \mathbf{Q}^1$, cioè si approssimano le funzioni:

$$
\begin{aligned}
V \ni v &\longleftrightarrow v_h \in V_h \\
V \ni w &\longleftrightarrow w_h \in V_h \\
V \ni \psi &\longleftrightarrow \psi_h \in V_h
\end{aligned}
$$

Allora il problema discreto diventa:

$$
\begin{cases}
c_m \left\langle \frac{\partial v_h}{\partial t}, \psi_h \right\rangle + a(v_h, \psi_h) + \langle G(v_h, w_h), \psi_h \rangle = \langle I_{\text{app}}, \psi_h \rangle & \forall \psi_h \in V_h \\
\left\langle \frac{\partial w_h}{\partial t}, \psi_h \right\rangle = \left\langle \eta_2 \left(\frac{v_h}{v_p} - w_h \right), \psi_h \right\rangle & \forall \psi_h \in V_h
\end{cases}
$$

Le funzioni approssimate appartengono ad uno spazio finito-dimensionale, quindi vengono espresse come espansione nella base di questo spazio:

$$
v_h = \sum_{j=1}^{N} V_j \varphi_j \qquad\qquad w_h = \sum_{j=1}^{N} W_j \varphi_j
$$

dove $V_j = V_j(t)$ e $W_j = W_j(t)$ sono funzioni che dipendono solo dal tempo, e non dallo spazio. Quindi il problema discreto diventa, $\forall \psi_h \in V_h$, cercare (V, W) tale che:

$$\begin{cases} c_m \left\langle \frac{\partial \sum_{j=1}^N V_j \varphi_j}{\partial t}, \psi_h \right\rangle + a(\sum_{j=1}^N V_j \varphi_j, \psi_h) + \langle G(\sum_{j=1}^N V_j \varphi_j, \sum_{j=1}^N W_j \varphi_j), \psi_h \rangle = \langle I_{\text{app}}, \psi_h \rangle \\ \left\langle \frac{\partial \sum_{j=1}^N W_j \varphi_j}{\partial t}, \psi_h \right\rangle = \left\langle \eta_2 \left(\frac{\sum_{j=1}^N V_j \varphi_j}{v_p} - \sum_{j=1}^N W_j \varphi_j \right), \psi_h \right\rangle \end{cases}$$

Dato che le funzioni $\{\varphi_i\}_{i=1}^N$ formano una base, e quindi generano tutto lo spazio, il problema semi-discreto è equivalente a sostituire ψ_h con $\varphi_i \quad \forall i = 1, \cdots N$:

$$\begin{cases} c_m \left\langle \frac{\partial \sum_{j=1}^N V_j \varphi_j}{\partial t}, \varphi_i \right\rangle + a(\sum_{j=1}^N V_j \varphi_j, \varphi_i) + \langle G(\sum_{j=1}^N V_j \varphi_j, \sum_{j=1}^N W_j \varphi_j), \varphi_i \rangle = \langle I_{\text{app}}, \varphi_i \rangle \\ \left\langle \frac{\partial \sum_{j=1}^N W_j \varphi_j}{\partial t}, \varphi_i \right\rangle = \left\langle \eta_2 \left(\frac{\sum_{j=1}^N V_j \varphi_j}{v_p} - \sum_{j=1}^N W_j \varphi_j \right), \varphi_i \right\rangle \end{cases}$$

Si utilizza ora la linearità del prodotto scalare e della forma bilineare a; inoltre si può considerare la mappa G come lineare (anche se è un polinomio di terzo grado) dato che in questa analisi viene approssimata con funzioni lineari, per cui l'errore commesso è dello stesso ordine dell'errore del metodo utilizzato.
Di conseguenza:

$$\begin{cases} c_m \sum_{j=1}^N V_j' \langle \varphi_j, \varphi_i \rangle + \sum_{j=1}^N V_j \; a(\varphi_j, \varphi_i) + \sum_{j=1}^N G(V_j, W_j) \langle \varphi_j, \varphi_i \rangle = \sum_{j=1}^N I_{\text{app}} \langle \varphi_j, \varphi_i \rangle \\ \sum_{j=1}^N W_j' \langle \varphi_j, \varphi_i \rangle = \eta_2 \left(\frac{1}{v_p} \sum_{j=1}^N V_j - \sum_{j=1}^N W_i \right) \langle \varphi_j, \varphi_i \rangle \end{cases}$$

Si considerano le matrici:

$$K = (K_{ij}) \quad \text{dove} \quad k_{ij} = a(\varphi_j, \varphi_i)$$

$$M = (M_{ij}) \quad \text{dove} \quad M_{ij} = \langle \varphi_j, \varphi_i \rangle$$

Allora si riscrive il sistema di N equazioni in forma matriciale come:

$$\begin{cases} c_m M V' + KV + MG(V, W) = M I_{\text{app}} \\ MW' = \eta_2 M \left(\frac{1}{v_p} V - W \right) \end{cases}$$

dove, si ricorda, le quantità V, W, I_{app} dipendono dal tempo.

5. Discretizzazione in tempo

Per risolvere il sistema di ODE ottenuto, se si utilizzasse un metodo esplicito, ad ogni passo temporale si dovrebbe risolvere un sistema lineare, ma risulterebbe necessario usare un passo temporale "piccolo" per sperare di avere convergenza. Viceversa, se si utilizzasse un metodo implicito, non si avrebbero restrizioni sul passo, ma per via del termine non lineare G andrebbe risolto un sistema non lineare (molto più costoso).
Di conseguenza, si opta per una terza via: un metodo semi-implicito, cioè si trattano i

termini lineari mediante un metodo implicito, ed i termini non lineari mediante un metodo esplicito. Così facendo, si arriva alla seguente discretizzazione temporale:

$$\begin{cases} c_m M \frac{V^{n+1}-V^n}{\tau} + KV^{n+1} + MG(V^n, W^{n+1}) = MI_{\text{app}}^{n+1} \\ M \frac{W^{n+1}-W^n}{\tau} = \eta_2 M \left(\frac{1}{v_p} V^n - W^{n+1} \right) \end{cases}$$

che porta alla seguente soluzione:

$$\begin{cases} W^{n+1} \left(\frac{1}{\tau} + \eta_2 \right) = \frac{1}{\tau} W^n + \frac{\eta_2}{v_p} V^n \\ \left(\frac{c_m}{\tau} M + K \right) V^{n+1} = \frac{c_m}{\tau} M V^n - MG(V^n, W^{n+1}) + MI_{\text{app}}^{n+1} \end{cases}$$

per cui, ad ogni iterazione, va risolto un sistema lineare.

6. Risultati numerici

Tramite MATLAB, discretizziamo il problema con $N = 10.000$ passi spaziali, 100 per ogni lato del quadrato, ed $L = 5.000$ passi temporali.

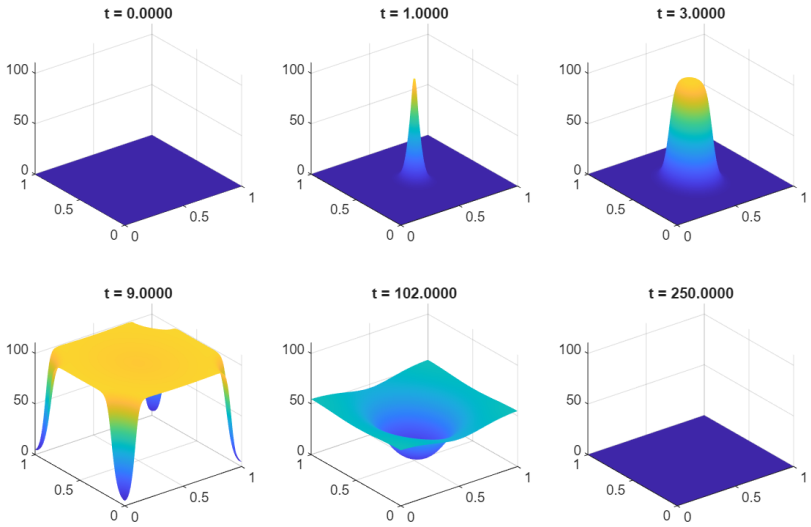


FIGURA 1. Istantanea della soluzione a sei istanti temporali.

Tramite questa immagine, notiamo delle fasi temporali distinte:

- Stimolo iniziale: all'inizio il tessuto è a riposo, ed una volta applicato l'impulso elettrico si eccita velocemente raggiungendo il suo picco massimo.
- Propagazione del fronte d'onda: il potenziale inizia a propagarsi radialmente fino ai bordi del dominio, e il fronde d'onda forma un ellisse perché la matrice D non è un multiplo dell'identità. Infatti, poiché la diffusività lungo l'asse x è maggiore, l'impulso viaggia più velocemente in quella direzione rispetto all'asse y.

- Fase di recupero: il potenziale scende, per tonare progressivamente (non istantaneamente) allo stato di riposo $v = 0$.

Infine, studiamo il potenziale d'azione, cioè l'andamento temporale del potenziale v valutato in un singolo punto specifico della griglia. In questo caso studiamo i potenziali d'azione di tre punti distinti.

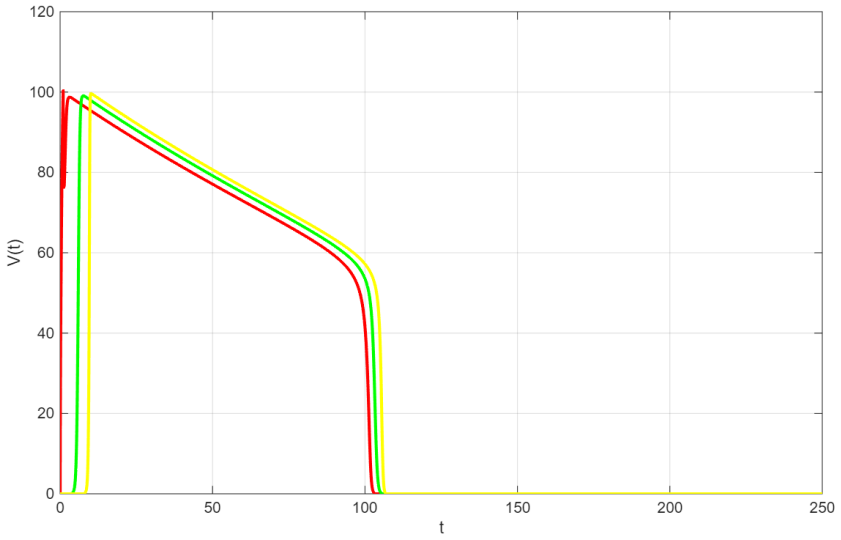


FIGURA 2. Potenziale d'azione dell'origine (rosso), di un punto interno al dominio (verde), e di un punto sul bordo del dominio (giallo).

Tramite questo grafico, concludiamo le stesse proprietà ricavate dal grafico precedente. Inoltre notiamo che, al variare dei punti, la forma dei potenziali d'azione rimane uguale a meno di traslazione.

L'IPOTESI DI RIEMANN SU CAMPI FINITI

FRANCESCO STOPPA

1. Introduzione

Consideriamo la seguente serie a variabile complessa: $\zeta(s) := \sum_{n \geqslant 1} \frac{1}{n^s}$. Questa serie è nota come "Funzione zeta di Riemann". Questa funzione a priori è definita solo per quei numeri complessi $s \in \mathbb{C}$ tali che $\mathfrak{Re}(s) > 1$, tuttavia, si può estendere a praticamente tutti i valori complessi, tranne $s = 1$, tramite un processo chiamato continuazione analitica. È possibile dimostrare che $\zeta(-2n) = 0$ per ogni numero naturale positivo $n \in \mathbb{N}$. Una domanda naturale è se questi siano tutti e soli gli zeri, la risposta è no! Inoltre, questi sembrano avere tutti una caratteristica in comune, la loro parte reale vale sempre $\frac{1}{2}$; la congettura per cui questo fatto non sia una semplice coincidenza, ma che sia una caratteristica di tutti gli zeri rimanenti, è nota come ipotesi di Riemann.

Sorprendentemente, questa funzione è collegato ad un problema di natura apparentemente molto differente: contare il numero di soluzioni di equazioni su campi finiti.

Lo scopo del seminario è di illustrare come i due probemi siano molto vicini e di mostrare come questi risultati possano applicarsi ad altri problemi, come l'ultimo teorema di Fermat.

2. Punti razionali

Sia $p \in \mathbb{Z}$ un numero primo e sia $q = p^n$ una sua potenza con $n > 0$ naturale. Allora denotiamo con $\mathbb{F}_q$ il campo finito con q elementi e fissiamo $R = \mathbb{F}_q[T_0, \ldots, T_n]/(f_1, \ldots, f_m)$, con $f_i \in \mathbb{F}_q[T_0, \ldots, T_n]$ polinomi omogenei.

Osservazione 1. A priori l'esistenza di un campo finito con questo numero di elementi non è scontata. L'idea è che i campi finiti possono avere solo cardinalità che siano potenze di primi. Per mostrare che ognuna di queste cardinalità è possibile considerare il più piccolo campo finito che contiene le radici di $f(x) = x^{p^n} - x$.

Definizione 2. Definiamo $Spec(R) = \{\mathfrak{p} \subset R \text{ ideale primo}\}$ e $Proj(R) = \{\mathfrak{p} \in Spec(R)$ tale che i generatori siano polinomi omogenei$\}$. Chiamiamo il primo tipo di oggetti "varietà affini" e il secondo tipo di oggetti "varietà proiettive".

D'ora in avanti indicheremo con X una varietà (affine o proiettiva) associata ad un anello R della forma $\mathbb{F}_q[T_0, \dots, T_n]/(f_1, \dots, f_m)$. Inoltre, se $x \in X$ rappresenta un ideale massimale, allora lo chiameremo "punto chiuso".

DEFINIZIONE 3. Sia X una varietà associata all'anello $R = \mathbb{F}_q[T_0, \dots, T_n]/(f_1, \dots, f_m)$, dove m il numero minimo di generatori per l'ideale $(f_1, \dots f_m)$. Se X è affine, allora $dim(X) = n - m$, se X è proiettiva, allora $dim(X) = n - m - 1$.

OSSERVAZIONE 4. Questa definizione collima la con la classica definizione di dimensione, che dovrebbe essere numero di dimensioni, dato dalle variabili, meno numero di equazioni indipendenti.

Abbiamo anche le seguenti notazioni:

- Dato $x \in X$, definiamo $\kappa(x) = Frac(R/x)$ e lo chiamiamo campo residuo in x
- dato $x \in X$ punto chiuso, definiamo $deg(x) = dim_{\mathbb{F}_q}(\kappa(x))$
- Infine, definiamo $X(\mathbb{F}_{q^m}) = \{x \in X |\ \kappa(x) \subseteq \mathbb{F}_{q^m}\}$ e lo chiamiamo insieme dei punti $\mathbb{F}_{q^m}$ razionali.

OSSERVAZIONE 5. Osserviamo che il campo residuo in ogni punto chiuso deve essere un campo finito. L'idea è che ogni variabile viene sostituita con un elemento che è soluzione di qualche polinomio a coefficienti in $\mathbb{F}_q$, quindi può avere solo un numero di potenze differenti.

Osserviamo che l'insieme dei punti razionali ha un'interpretazione classica:

LEMMA 6. *Abbiamo le seguenti biezioni:*

- *Se X è una varietà affine di dimensione d, allora $V(\mathbb{F}_{q^m}, f_1, \dots, f_d) = \{\underline{x} \in \mathbb{F}_{q^m}^{n+1} | f(\underline{x}) = \cdots = f_d(\underline{x}) = 0\} \cong X(\mathbb{F}_{q^m})$*
- *Se X è una varietà proiettiva di dimensione d, allora abbiamo che $X(\mathbb{F}_{q^m}) \cong V_+(\mathbb{F}_{q^m}, f_1, \dots, f_d) := V(\mathbb{F}_{q^m}, f_1, \dots, f_d)^{\neq 0}/(x \sim \lambda x)$, con $\lambda \in \mathbb{F}_{q^m}^{\times}$.*

Dimostrazione. Ci soffermeremo solo sul primo caso. Prima di tutto osserviamo che se $x \in X(\mathbb{F}_{q^m})$, allora è un punto chiuso, infatti $\kappa(x) = Frac(R/x)$ è un campo finito, ma allora anche R/x deve essere finito, in quanto sottoanello di $\kappa(x)$, ma, dal momento che x corrisponde ad un ideale primo, allora R/x è un dominio finito, quindi è un campo.

Consideriamo la mappa $ev_x : \mathbb{F}_q[T_0, \dots, T_n] \to R \to R/x \hookrightarrow \mathbb{F}_{q^m}$ e definiamo $\underline{x} \in \mathbb{F}_q^{n+1}$ il punto tale che $\underline{x}_i = ev_x(T_i)$. Dal momento che ev_x fattorizza su R, abbiamo che $f_i(\underline{x}) = ev_x(f) = 0$, per ogni $i \leqslant dim(X)$, quindi abbiamo prodotto una mappa $X(\mathbb{F}_{q^m}) \to V(\mathbb{F}_{q^m}, f)$.

Per mostrare che è biettiva troviamone un'inversa. Consideriamo quindi un punto $\underline{x} \in V(\mathbb{F}_{q^m}, f_1, \dots, f_d)$ e definiamo la seguente mappa $v_{\underline{x}} : \mathbb{F}_q[T_0, \dots, T_n \to \mathbb{F}_{q^m}$ tale che $v_{\underline{x}}(T_i) = \underline{x}_i$. Osserviamo che $v_{\underline{x}}(f_i) = f_i(\underline{x}) = 0$, per ogni $i \leqslant d$, quindi la mappa fattorizza attraverso R, fornendoci una mappa $\bar{v}_{\underline{x}} : R \to \mathbb{F}_{q^m}$. L'immagine di questa mappa è un dominio finito, quindi è un campo contenuto in $\mathbb{F}_{q^m}$, quindi il suo kernel $x = Ker(\bar{v}_{\underline{x}})$ è un ideale massimale con campo residuo in $\mathbb{F}_{q^m}$. Perciò, otteniamo una mappa ben definita nella direzione opposta.

È immediato mostrare che le due mappe definite sono l'una l'inversa dell'altra. □

Riportiamo qui un risultato tecnico che non andiamo a dimostrare:

LEMMA 7. *Sia X varietà, allora $\sharp X(\mathbb{F}_{q^m}) = \sum_{d|m} d \cdot n_d$, dove $n_d = \sharp\{x \in X(\mathbb{F}_{q^m}) | \ deg(x) = d\}$.*

3. La funzione Zeta di una verietà

Ora che abbiamo visto come possiamo algebrizzare il problema di studiare soluzioni di equazioni su campi finiti, spostandoci da un problema su un insieme, allo studio di un anello, vediamo come possiamo interpretare analiticamente il problema.

L'idea è che andremo a definire una funzione in grado di esprimere al meglio molte proprietà geometriche "interessanti" della varietà che consideriamo. In particolare, valutando questa funzione in punti speciali, potremo ricavare il numero di soluzioni in un particolare campo finito.

DEFINIZIONE 8. Sia X una varietà e definiamo $v_m = \sharp X(\mathbb{F}_{q^m})$. La funzione Zeta associata ad X è $Z(X,T) = exp(\sum_{n>0} v_n \frac{T^n}{n})$.

OSSERVAZIONE 9. Nella definizione precedente, con $exp(T)$ intendiamo la serie formale $\sum_{n\geqslant 0} \frac{T^n}{n!}$.

Nonostante questa definizione sembri complicata e completamente separata da quella della funzione zeta di Riemann, sono in realtà molto correlate: consideriamo $log(Z(X,T)) = \sum v_n \frac{T^n}{n} = \sum_n \sum_{d|n} n_d \cdot d \frac{T^{\ell\cdot d}}{\ell\cdot d} = \sum_{d\geqslant 1} n_d \sum_{\ell\geqslant 1} \frac{T^{\ell\cdot d}}{\ell} = \sum_d n_d log(\frac{1}{1-T^d}) = \sum_{x\in X^c} log(\frac{1}{1-T^{deg(x)}}) = log(\prod_{x\in X} \frac{1}{1-T^{deg(x)}})$. Deduciamo quindi l'uguaglianza formale $Z(X,T) = \prod_{x\in X^c} \frac{1}{1-T^{deg(x)}}$. Dove con X^c denotiamo l'insieme dei punti chiusi di X.

Poniamo ora $T = q^{-s}$, allora otteniamo che $Z(X,T) = \prod_{x\in X^c} \frac{1}{1-(q^{deg(x)})^{-s}} = \prod_{x\in X^c} \frac{1}{1-\sharp\kappa(x)^{-s}}$.

Prendendo questa come definizione della funzione Zeta, possiamo considerare $Z(Spec(\mathbb{Z}),T) = \prod_{p \text{ primo}} \frac{1}{1-\sharp(\mathbb{Z}/p\mathbb{Z})^{-s}} = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}} = \zeta(s)$. Dove il prodotto avviene sui primi poichè un ideale massimale di $\mathbb{Z}$ è un numero primo e viceversa.

Vediamo quindi che studiare la funzione Zeta ci permette anche di capire qualcosa in più sulla natura della zeta di Riemann.

OSSERVAZIONE 10. La conoscenza della funzione Zeta di una varietà ci permette di rispondere al problema iniziale, conoscere v_n. Infatti, $\frac{d}{dT} log(Z(X,T))_{|T=0} = v_1 = \sharp X(\mathbb{F}_q)$.

ESEMPIO 11. Abbiamo capito che la funzione Zeta è importante, tuttavia sembra molto difficile da comprendere, quindi cerchiamo di vedere qualche esempio per familiarizzarci.

- Sia $X = Spec(\mathbb{F}_q[T_1,\dots,T_n]) =: \mathbb{A}^n_{\mathbb{F}_q}$. In questo caso, $v_m = \sharp\mathbb{A}^n_{\mathbb{F}_q}(\mathbb{F}_{q^m}) = \sharp(\mathbb{F}_{q^m})^n = q^{n\cdot m}$, quindi $log(Z(X,T)) = \sum_m \frac{(q^nT)^m}{m} = log(\frac{1}{1-q^nT})$, quindi $Z(X,T) = \frac{1}{1-q^nT}$.

- Sia $S \subseteq X$ una sottovarietà di una varietà tale che anche $U = X \setminus S$ si possa vedere come varietà, allora abbiamo $Z(X,T) = Z(S,T)Z(U,T)$.
- Si può mostrare che $\mathbb{P}^n_{\mathbb{F}_q} = \mathbb{A}^n_{\mathbb{F}_q} \amalg \mathbb{P}^{n-1}_{\mathbb{F}_q}$, da cui si deduce $Z(\mathbb{P}^n_{\mathbb{F}_q}, T) = Z(\mathbb{A}^n_{\mathbb{F}_q}, T)Z(\mathbb{P}^{n-1}_{\mathbb{F}_q}, T)$. Per ricorsione deduciamo che $Z(\mathbb{P}^n_{\mathbb{F}_q}, T) = \prod_{i \leqslant n} \frac{1}{1-q^i T}$. Quindi $v_m = \sum_{i \leqslant n} (q^i)^m$. Questo ultimo esempio ci mostra come possiamo contare il numero di punti dello spazio proiettivo su campi finiti usando la funzione Zeta.
- Come ultimo esempio consideriamo una curva ellittica $E : y^2 = x^3 + Ax + B$, si può mostare che $Z(E,T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$, dove $a = \gamma_1 + \gamma_2$ con $\gamma_1 = \bar{\gamma}_2 \in \mathbb{C}$ tali che $|\gamma_1| = |\gamma_2| = q^{1/2}$

Andiamo ora a enunciare il teorema principale che riguarda la teoria della funzione Zeta e delle varietà sui campi finiti. Più nello specifico, andremo a enunciarne solo una parte, in particolare enunceremo la parti che applicheremo nel prossimo esempio.

Teorema 12. *Sia X una varietà proiettiva, allora valgono le seguenti:*

- *La funzione $Z(X,T)$ è una funzione razionale a coefficienti in $\mathbb{Q}$, ovvero è il rapporto di due polinomi a coefficienti interi.*
- *Poniamo $Z(X,T) = \frac{P(T)}{Q(T)}$, con $P(T), Q(T) \in \mathbb{Z}[T]$, allora abbiamo che $P(T) = \prod_{i \leqslant 2d-1} \prod_j (1 - \alpha_{ij} T)$, con $|\alpha_{ij}| = q^{i/2}$ e $\alpha_i \in \mathbb{C}$.*

Questo risultato è noto come "congetture di Weil", anche se sono un teorema. La loro importanza risiede nel fatto che nel loro complesso ci descrivono perfettamente la struttura della funzione Zeta, e forniscono anche informazioni su come ricavare i gradi dei polinomi in gioco nella scrittura di questa funzione.

Inoltre, la seconda affermazione è nota come ipotesi di Riemann su campi finiti. La ragione di questo nome è la seguente: gli zeri della funzione Zeta sono $T = \frac{1}{\alpha_{ij}}$. Se ora consideriamo la sostituzione $T = q^{-s}$, otteniamo $q^s = \alpha_{ij}$, ovvero $|q^s| = q^{i/2}$, ovvero che $Re(s) = \frac{i}{2}$. Quindi, nel caso in cui X sia una curva, scopriamo che gli zeri della funzione Zeta hanno tutti parte reale $1/2$, nella variabile s, come predetto dall'ipotesi di Riemann nel caso di $Spec(\mathbb{Z})$. Il fatto è che nella teoria generale della geometria algebrica $Spec(\mathbb{Z})$ si percepisce come un oggetto di dimensione uno, quindi questa funzione davvero generalizza l'ipotesi di Riemann ad un contesto geometrico più vasto.

4. Applicazioni all'ultimo teorema di Fermat

In questa sezione apprezzeremo maggiormente la complessità dell'ultimo teorema di Fermat:

Teorema 13. *L'equazione $X^d + Y^d = Z^d$ non ha soluzioni razioali banali per ogni $d > 2$. Dove una soluzione è banale se possiede almeno una coordinata nulla.*

Osservazione 14. Il caso $d = 2$ è il classico caso delle terne pitagoriche, che si conosce essere infinite.

Un approccio al problema potrebbe essere il seguente: se riuscissimo a trovare un primo p, tale per cui l'equazione non ha soluzioni modulo p, allora avremmo finito. Infatti, se per assurdo ci fosse una soluzione razionale (x, y, z), dal momento che il polinomio è omogeneo, potremmo assumerla intera. Ma allora, riducendo modulo p, questa dovrebbe essere una soluzione su $\mathbb{F}_p$, assurdo.

La falla in questo semplicissimo argomento è che questo primo p, non è così difficile da trovare, dal momento che sono infiniti:

PROPOSIZIONE 15. *Sia* $X_{p,d} = Proj(\mathbb{F}_p[X;Y,Z]/(X^d + Y^d - Z^d)$. *Per ogni* $d > 2$, *esiste* $N \in \mathbb{N}$, *tale che* $\forall p > N\ X_{d,p}(\mathbb{F}_p) \neq \emptyset$.

Dimostrazione. Usando le congetture di Weil e osservando che $\dim(X_{p,d}) = 1$, si può dimostrare che $Z(X,T) = \frac{P(T)}{(1-T)(1-pT)}$, con $g = \frac{(d-1)(d-2)}{2}$ e $P(T) = \prod_{j=1}^{2g}(1 - \alpha_j T)$ e $|\alpha_j| = p^{1/2}$.

Mostriamo ora che le soluzion in cui una coordinata è nulla sono al più $3d$. Poniamo $Z = 0$, e osserviamo che $A_Z = V_+(\mathbb{F}_p, X^d + Y^d) = V_+((X/Y)^d + 1)$. Dato che però un polinomio di gardo d ha al più d soluzioni, ne deduciamo che $\sharp A_Z \leqslant d$. Dato che la situazione è simmetrica nelle tre variabili, deduciamo l'obbiettivo.

Dalla descrizione precedente della funzione Zeta, deduciamo che $log(Z(X,T)) = log(P(T)) - log(1-T) - log(1-pT)$ e quindi $\frac{d}{dt}(log(Z(X,T))_{|T=0} = \frac{P'(0)}{P(0)} + p + 1$, ovvero $a_p = |\sharp X_{d,p}(\mathbb{F}_p)| = |1 + p + \sum_{i=1}^{2g} \alpha_i| \leqslant 1 + p + \sum |\alpha_i| = 1 + p + 2g\sqrt{p} = 1 + p + \sqrt{p}(d^2 - 3d + 2)$. Si osserva immediatamente che per $p \gg 0$ abbiamo $a_p > 3d$, quindi esiste almeno una soluzione non banale. □

SULL'APPROSSIMAZIONE DIOFANTEA

NOEMI GENNUSO

1. Introduzione

Sappiamo che i numeri razionali sono densi in $\mathbb{R}$, ma è possibile approssimare bene ogni numero irrazionale? Quali informazioni può dare l'errore commesso nell'approssimazione sulla natura del numero considerato? Durante questo seminario, risponderemo a queste domande e vedremo come siano state storicamente applicate alla costruzione di numeri trascendenti e a risultati sulle soluzioni di equazioni diofantee. Come notazione, scrivendo un numero razionale, ad esempio come p/q, intenderemo automaticamente che il rappresentante scritto soddisfa p e q interi coprimi e $q > 0$. Inoltre, dato $r \in \mathbb{R}$, $\lfloor r \rfloor \in \mathbb{Z}$ è la parte intera di r (ovvero il minimo intero minore o uguale a r) e $\{r\} := r - \lfloor r \rfloor \in [0, 1)$ è la parte razionale di r.

2. Il teorema di Dirichelet

Innanzitutto, vorremmo definire cosa significa approssimare bene. Infatti, dato $\alpha \in \mathbb{R}$, dalla densità di $\mathbb{Q}$ in $\mathbb{R}$, per ogni scelta di $\varepsilon \in \mathbb{R}_{>0}$ esiste $p/q \in \mathbb{Q}$ tale che $|\alpha - p/q| < \varepsilon$, ma vorremmo fare in modo che la disuguaglianza sia valida senza che p e q siano arbitrariamente grandi. In questo senso, il seguente teorema fornisce una caratterizzazione dei numeri irrazionali.

Teorema 1. *(Dirichelet) Dato $\alpha \in \mathbb{R}$, α è irrazionale se e solo se esistono infiniti $p/q \in \mathbb{Q}$ tali che $|\alpha - p/q| \leqslant 1/q^2$.*

Dimostrazione. L'implicazione da destra a sinistra è immediata poiché se α fosse razionale, $\alpha = p'/q'$ e $1/q' \leqslant |qp' - pq'| \leqslant 1/q$, da cui $q \leqslant q'$. Inoltre, $|p| \leqslant |q\alpha - p| \leqslant 1/q + |q\alpha|$, ovvero, esistono finite possibilità per p e q, contraddicendo l'assunzione. Per quanto riguarda l'altra implicazione, dimostriamo l'esistenza di tali p/q. Sia Q un intero positivo. L'insieme

$$F_Q := \big\{\{q\alpha\} \in [0, 1] : q \in \{0, 1, \dots, Q\}\big\}$$

è costituito da $Q + 1$ punti nell'intervallo unitario, pertanto, per il principio dei cassetti applicato alla partizione dell'intervallo unitario in Q intervalli di ampiezza $1/Q$, esistono $q_1, q_2 \in \{0, 1, \dots, Q\}$ con $q_1 > q_2$, tali per cui $|\{q_1\alpha\} - \{q_2\alpha\}| \leqslant 1/Q$.

Riscrivendo,

$$|(q_1 - q_2)\alpha - \lfloor q_1\alpha \rfloor + \lfloor q_2\alpha \rfloor| \leqslant \frac{1}{Q},$$

da cui risulta immediato definire p/q come il rappresentante definito nell'introduzione di $\frac{\lfloor q_1\alpha \rfloor - \lfloor q_2\alpha \rfloor}{q_1 - q_2}$ e, in particolare, $q \leqslant q_1 - q_2 \leqslant Q$. Pertanto, dato un intero positivo Q, il numero razionale p/q appena definito, soddisfa

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{Qq} \leqslant \frac{1}{q^2}.$$

Notiamo che, essendo F_Q un insieme finito, le possibili scelte di q_1, q_2 che portano alla costruzione di p/q sono in numero finito. Per dimostrare che esistono infiniti razionali che soddisfano la condizione richiesta, consideriamo, per un intero positivo Q fissato, il numero razionale u/v definito come il minimo dei p/q appena costruiti, al variare delle scelte possibili di q_1 e q_2. Consideriamo ora un altro intero positivo Q' tale che $Q' > |\alpha - u/v|^{-1}$. Tale Q' porterà alla costruzione di un certo u'/v' minimale nel senso appena descritto nel caso di Q, che soddisfa $|\alpha - u'/v'| \leqslant 1/Q'v' < |\alpha - u'/v'|$. Ovvero, u'/v' è diverso da u/v, pertanto l'infinità dei razionali che soddisfano la condizione richiesta è dimostrata. □

3. Il teorema di Liouville

Aggiungendo ipotesi su α, il seguente teorema fornisce un lower-bound dell'errore commesso nell'approssimazione e permette dunque di dedurre una condizione sufficiente per la trascendenza. Sia quindi $\alpha \in \mathbb{R}$, algebrico su $\mathbb{Q}$ di grado $d := [\mathbb{Q}[\alpha] : \mathbb{Q}]$ (i.e. α è radice di un polinomio irriducibile a coefficienti razionali di grado d).

Teorema 2. *(Liouville) Con una tale scelta di α, esiste una costante $C_\alpha \in \mathbb{R}_{>0}$ tale che per ogni $p/q \in \mathbb{Q}$ vale*

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{C_\alpha}{q^d}.$$

Dimostrazione. Sia $f(T) \in \mathbb{Z}[T]$ il polinomio minimo di α. Possiamo considerare $f \in C^\infty(\mathbb{R})$ e porre $\tilde{c} := \max\{f'(t) : t \in [\alpha - 1, \alpha + 1]\}$. Quindi, per ogni $p/q \in [\alpha - 1, \alpha + 1]$, otteniamo $|f(\alpha) - f(p/q)| = |f(p/q)| \leqslant \tilde{c}|\alpha - p/q|$. Pulendo i denominatori, $q^d f(p/q)$ è un intero maggiore o uguale a 1. Quindi, per ogni $p/q \in [\alpha - 1, \alpha + 1]$,

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{1}{\tilde{c}\, q^d}.$$

Notiamo che per $\alpha \notin [\alpha - 1, \alpha + 1]$ si ha la stima banale $|\alpha - p/q| > 1 \geqslant 1/q^d$, pertanto la tesi segue ponendo $C_\alpha = \min\{1, 1/\tilde{c}\}$. □

Nonostante la dimostrazione sia decisamente elementare, questo teorema è stato storicamente importante per costruire numeri trascendenti nel 1844. L'esistenza di tali numeri era già chiara, in quanto i numeri algebrici sono numerabili in $\mathbb{R}$, ma mancavano esempi espliciti di numeri trascendenti. Infatti, la trascendenza di e fu dimostrata solo nel 1873 da Hermite e quella di π nel 1882 da Von Lindemann,

sfruttando idee simili a quelle di Hermite.

Vediamo dunque come definire un numero di Liouville e come il teorema lo renda automaticamente trascendente. Sia

$$\alpha := \sum_{n=1}^{\infty} 2^{-n!}$$

e sia α_N la serie troncata al termine N-esimo, in particolare, $\alpha_N \in \mathbb{Q}$. Calcoliamo l'errore commesso nell'approssimazione:

$$|\alpha - \alpha_N| = \sum_{n=N+1}^{\infty} 2^{-n!} = 2^{-(N+1)!}\left(1 + 2^{-(N+2)} + \dots\right) \leqslant 2 \cdot 2^{-(N+1)!}$$

D'altra parte, se α fosse algebrico di grado d, dovrebbe soddisfare

$$|\alpha - \alpha_N| \geqslant \frac{C_\alpha}{2^{N! \cdot d}}.$$

Tuttavia, per $N >> d$, si ha

$$2 \cdot 2^{-(N+1)!} < \frac{C_\alpha}{2^{N! \cdot d}},$$

che dimostra la trascendenza di α.

4. Applicazioni

I teoremi precedenti forniscono, per un dato numero algebrico α, upperbound e lowerbound per ogni approssimazione diofantea tramite razionali $p/q \in \mathbb{Q}$. In particolare, nel caso quadratico, q ha esponente 2 ovvero l'approssimazione è ottimale nel senso esplicitato dal seguente corollario (si dice che α ha esponente di approssimazione 2).

Corollario 3. *Sia $\alpha \in \mathbb{R}$ algebrico di grado 2. Allora, esiste una costante $\omega_\alpha \in (0,1)$ tale per cui*

$$|\alpha - p/q| \leqslant \omega_\alpha / q^2$$

è valida per infiniti $p/q \in \mathbb{Q}$, ottimale nel senso che $|\alpha - p/q| \leqslant k/q^2$ è valida per un numero finito di $p/q \in \mathbb{Q}$ se $k < \omega_\alpha$.

Dimostrazione. Sia

$$D(\alpha) := \{x > 0 : |\alpha - p/q| \leqslant x/q^2 \text{ è valida per finiti } p/q\}.$$

Per il teorema di Liouville, $D(\alpha)$ non è vuoto e, per il teorema di Dirichelet, $D(\alpha)$ è limitato in $[0,1]$. Pertanto, si conclude ponendo $\omega_\alpha := \max D(\alpha)$. □

Possiamo notare che il teorema di Liouville permette di calcolare esplicitamente la costante C_α, mentre il corollario fornisce solo l'esistenza di una costante di ottimalità ω_α. Ad esempio, nel caso elementare in cui $\alpha = \sqrt{2}$, possiamo stimare $\omega_{\sqrt{2}} \in (C_{\sqrt{2}}, 1)$,

dove $C_{\sqrt{2}} = \min\left\{1, \frac{1}{\max\{(T^2-2)'\}}\right\} = \frac{1}{2\sqrt{2}+2}$ (per questo caso è possibile calcolare esplicitamente $\omega_{\sqrt{2}} = 1/2\sqrt{2}$, si veda [M]).

Per quanto riguarda il caso α non quadratico, possiamo chiederci se l'esponente d sia ottimale nel lowerbound del teorema di Liouville, ovvero, se d sia l'esponente di approssimazione per α. Il risultato migliore e ottimale è del 1955 da parte di Roth e afferma che 2 è l'esponente di approssimazione anche nel caso di α non quadratico (per un'idea della dimostrazione si veda [S]).

5. Equazioni diofantee

Il teorema di Roth permette di collegare teoremi sull'approssimazione diofantea a risultati sulle soluzioni di equazioni diofantee. Un esempio è dato dall'equazione

$$x^3 - 2y^3 = m$$

dove $m \in \mathbb{Z}$ fissato. Le soluzioni con $y = 0$ sono al più una. Nel caso in cui $y \neq 0$, detta $\zeta_3 \neq 1$ una radice cubica dell'unità, possiamo riscrivere l'equazione come

$$\prod_{i=0}^{2}\left(\frac{x}{y} - \sqrt[3]{2}\zeta_3^i\right) = \frac{m}{y^3}.$$

Notiamo che per $i = 1, 2$, si ha $\left|x/y - \sqrt[3]{2}\zeta_3^i\right| \geqslant \left|\mathrm{Im}\left(x/y - \sqrt[3]{2}\zeta_3^i\right)\right| > 0$, quindi esiste una costante $K_1 > 0$ tale per cui

$$\left|\frac{x}{y} - \sqrt[3]{2}\right| \leqslant \frac{K_1}{y^3}.$$

D'altra parte, il teorema di Roth fornisce l'esistenza (in modo non effettivo) di una costante $K_2 > 0$ tale per cui, per infiniti $x/y \in \mathbb{Q}$, vale

$$\left|\frac{x}{y} - \sqrt[3]{2}\right| \geqslant \frac{K_2}{y^2}.$$

Pertanto, l'equazione diofantea $x^3 - 2y^3 = m$ ammette un numero finito di soluzioni $(x, y) \in \mathbb{Z}^2$. Più esplicitamente, consideriamo $m = 1$. Si verifica facilmente che $(1, 0)$ e $(-1, -1)$ sono soluzioni. Tuttavia, è importante notare che con questo metodo, non conoscendo la costante K_2, non si può concludere che queste sono anche le uniche soluzioni e diventa quindi necessario sviluppare un'altra strategia (si veda [C]).

Bibliografia

[C] K. Conrad. *Integral solutions of* $x^3 - 2y^3 = 1$.
[M] G. Molteni. *Advanced Topics in Analytic Number Theory: Transcendental numbers*.
[S] J.H. Silverman. *The Arithmetic of Elliptic Curves*.

DAI TUMORI ALLE EPIDEMIE: COSA PUÒ DIRE LA MATEMATICA?

KEVIN ARANA

In queste note raccogliamo i tre modelli differenziali principali trattati nel libro di M. Braun [1]. L'idea è vedere come equazioni differenziali ordinarie del primo e del secondo ordine permettano di estrarre informazioni quantitative e qualitative cruciali in ambito biologico e medico.

1. Dinamica della Crescita dei Tumori Solidi

1.1. Introduzione e Crescita Esponenziale delle Cellule Libere

Come discusso da M. Braun [1], lo studio delle equazioni differenziali del primo ordine trova applicazioni straordinarie ed estremamente utili in biologia e medicina. Tra queste, la prima applicazione fondamentale riguarda proprio la dinamica di crescita dei tumori solidi, affiancata storicamente da problemi di miscuglio (compartment analysis) e dalla ricerca di traiettorie ortogonali.

Osservando sperimentalmente il comportamento delle cellule libere in divisione, come ad esempio i batteri, si nota che esse crescono a una velocità direttamente proporzionale al volume delle cellule presenti in quel dato momento. Denotando con $V(t)$ il volume delle cellule in divisione al tempo t, l'equazione differenziale che governa il processo è:

$$\frac{\mathrm{d}V}{\mathrm{d}t} = \lambda V, \tag{1}$$

per una certa costante positiva λ. La soluzione generale di tale equazione è:

$$V(t) = V_0 e^{\lambda(t-t_0)}, \tag{2}$$

dove V_0 rappresenta il volume iniziale delle cellule all'istante t_0. Da ciò si deduce che le cellule libere in divisione crescono in modo **esponenziale** nel tempo. Una conseguenza fondamentale di questa legge è che il volume delle cellule raddoppia costantemente in ogni intervallo di tempo di lunghezza fissa pari a $\ln 2/\lambda$.

1.2. La Legge di Gompertz per i Tumori Solidi

Tuttavia, la realtà clinica e sperimentale dei **tumori solidi** differisce radicalmente da questo modello ideale: i tumori solidi non crescono in modo esponenziale. Con

l'aumentare delle dimensioni del tumore, il tempo necessario per raddoppiare il volume totale aumenta continuamente. Svariati ricercatori hanno dimostrato che i dati empirici relativi a moltissimi tumori solidi si adattano straordinariamente bene, coprendo un fattore di crescita quasi millesimo del volume tumorale, alla relazione di Gompertz:

$$V(t) = V_0 \exp\left(\frac{\lambda}{\alpha}\left(1 - e^{-\alpha t}\right)\right), \quad \lambda, \alpha > 0. \tag{3}$$

Questa relazione indica che il tumore cresce sempre più lentamente con il passare del tempo, approssimandosi asintoticamente al volume massimo limite $V_\infty = V_0 e^{\lambda/\alpha}$.

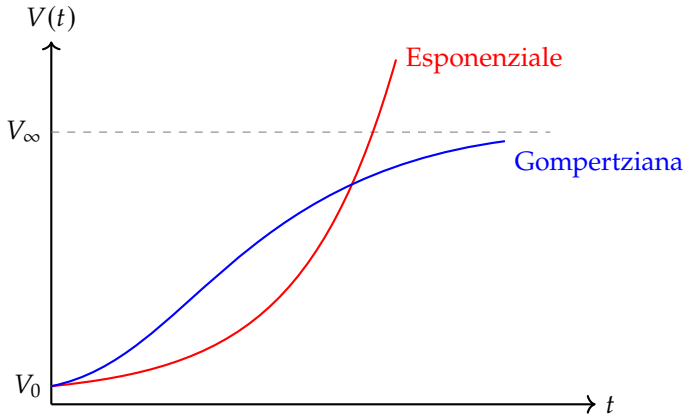


FIGURA 1. Confronto qualitativo tra la crescita esponenziale illimitata e la crescita gompertziana tipica dei tumori solidi.

1.3. Derivazione del Modello e le Due Teorie Conflittuali

Per comprendere a fondo le ragioni di questa deviazione dalla crescita esponenziale semplice, si analizza l'equazione differenziale soddisfatta da $V(t)$. Derivando la (3) rispetto al tempo t si ottiene:

$$\begin{aligned} \frac{\mathrm{d}V}{\mathrm{d}t} &= V_0 \lambda e^{-\alpha t} \exp\left(\frac{\lambda}{\alpha}\left(1 - e^{-\alpha t}\right)\right) \\ &= \lambda e^{-\alpha t} V(t). \end{aligned} \tag{4}$$

A livello biologico e meccanicistico, sono state avanzate due teorie differenti per spiegare la dinamica sottostante a questa equazione, riconducibili a due diverse interpretazioni algebriche della derivata:

$$\frac{\mathrm{d}V}{\mathrm{d}t} = \left(\lambda e^{-\alpha t}\right) V \tag{5}$$

$$\frac{\mathrm{d}V}{\mathrm{d}t} = \lambda \left(e^{-\alpha t} V\right) \tag{6}$$

(1) **Prima Teoria (Invecchiamento Cellulare - eq. (5))**: L'effetto di rallentamento della crescita tumorale è attribuito a un aumento graduale del tempo medio di generazione delle cellule, senza alcuna variazione nella proporzione di cellule capaci di riprodursi. Con il passare del tempo le cellule riproduttive maturano, invecchiano e di conseguenza si dividono sempre più lentamente.
(2) **Seconda Teoria (Necrosi Centrale e Core Necrotico - eq. (6))**: Il tempo medio di generazione delle cellule in divisione rimane costante, mentre il rallentamento della crescita è causato da una perdita progressiva di cellule riproduttive all'interno della massa tumorale. Una spiegazione fondamentale legata a questa ipotesi è lo sviluppo di una *regione necrotica* al centro del tumore. Tale necrosi compare quando il tumore raggiunge una dimensione critica per un dato tipo di tessuto; successivamente, il "core" necrotico cresce rapidamente man mano che aumenta la massa totale del tumore. Ciò accade perché in molti tumori solidi l'apporto sanguigno — e quindi l'approvvigionamento di ossigeno e nutrienti essenziali — è quasi interamente limitato alla superficie esterna e a un breve strato sottostante. Con l'espandersi del tumore, la diffusione verso il nucleo centrale diviene sempre più difficoltosa, determinando la morte cellulare e la formazione del nucleo necrotico.

2. Diagnosi del Diabete: Il Modello di Ackerman

2.1. Il Contesto Clinico e il Test di Tolleranza al Glucosio (GTT)

Il diabete mellito è una patologia metabolica caratterizzata da un eccesso di zucchero nel sangue e nelle urine, causata dall'incapacità dell'organismo di metabolizzare adeguatamente i carboidrati per un apporto insufficiente di insulina. La diagnosi clinica si avvale solitamente del **Test di Tolleranza al Glucosio (GTT)**: il paziente si presenta in ospedale dopo un digiuno notturno e riceve una dose massiccia di glucosio, monitorandone la concentrazione ematica per le successive 3-5 ore.

La criticità clinica risiede nel fatto che non esiste un criterio universale e condiviso per interpretare i risultati del GTT: interpretazioni di medici diversi possono condurre a diagnosi diametralmente opposte (ad esempio, diabete conclamato, normalità o persino un tumore all'ipofisi) a partire dai medesimi dati empirici.

2.2. Il Sistema Ormonale di Regolazione

I livelli di glucosio ematico sono sottoposti a un rigido controllo autoregolatorio mediato da diversi ormoni:

(1) **Insulina**: Secreta dalle cellule β del pancreas. Stimolata dall'assunzione di carboidrati e dai livelli di glucosio stesso, facilita l'ingresso del glucosio attraverso le membrane cellulari.
(2) **Glucagone**: Secreto dalle cellule α del pancreas, stimola la conversione del glicogeno epatico in glucosio in condizioni di ipoglicemia o digiuno.

(3) **Epinefrina (Adrenalina)**: Secreta in condizioni di emergenza da stress o ipoglicemia severa, inibisce l'azione dell'insulina e stimola la produzione rapida di glucosio.
(4) **Glucocorticoidi (es. cortisolo)**, **Tiroxin** e **Ormone della Crescita (Somatotropina)**: Intervengono sul metabolismo dei carboidrati e concorrono a modulare o ridurre la sensibilità periferica all'insulina.

2.3. Il Modello Matematico a Parametri Concentrati

A metà degli anni '60, Ackerman e collaboratori svilupparono un modello per descrivere il sistema durante un GTT, focalizzandosi su due sole variabili macroscopiche:

- $G(t)$: la concentrazione ematica di glucosio.
- $H(t)$: la concentrazione ormonale netta (effetto cumulativo dell'insulina e degli ormoni antagonisti).

Il sistema di equazioni differenziali non lineari che governa le variazioni è:

$$\frac{\mathrm{d}G}{\mathrm{d}t} = F_1(G, H) + J(t) \tag{7}$$

$$\frac{\mathrm{d}H}{\mathrm{d}t} = F_2(G, H) \tag{8}$$

dove $J(t)$ rappresenta il tasso di infusione esterna del glucosio. Supponendo che a digiuno il paziente si trovi nei valori ottimali di equilibrio (G_0, H_0), tali che $F_1(G_0, H_0) = 0$ e $F_2(G_0, H_0) = 0$, introduciamo le deviazioni:

$$g = G - G_0, \quad h = H - H_0.$$

Linearizzando il sistema tramite lo sviluppo in serie di Taylor nell'intorno dell'equilibrio, si ottiene un sistema lineare del secondo ordine per la deviazione del glucosio $g(t)$, riconducibile all'equazione dell'oscillatore smorzato:

$$\frac{\mathrm{d}^2 g}{\mathrm{d}t^2} + 2\alpha \frac{\mathrm{d}g}{\mathrm{d}t} + \omega_0^2 g = 0$$

2.4. Il Ruolo dell'Epinefrina e il Grafico di Recupero

Il criterio diagnostico di Ackerman sfrutta il periodo naturale delle oscillazioni per discriminare i soggetti sani dai lievi diabetici. Un aspetto cruciale si osserva quando $\alpha^2 - \omega_0^2 > 0$: in questo caso, la risposta del glucosio $g(t)$ sperimenta un crollo repentino al di sotto dei livelli di digiuno, attivando la secrezione d'emergenza di epinefrina.

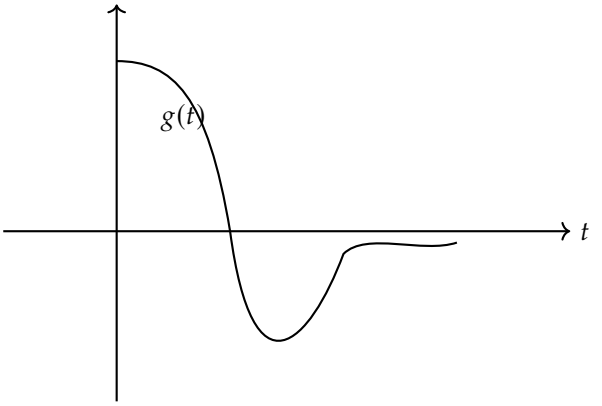


FIGURA 2. Grafico di $g(t)$ per $\alpha^2 - \omega_0^2 > 0$. Si noti il rapido calo a un valore negativo, che induce il corpo a secernere massicce quantità di epinefrina scambiandolo per un'emergenza estrema.

3. Modello Epidemico SIR e Teorema Soglia

3.1. Assunzioni e Formulazione del Modello SIR

Consideriamo la situazione in cui un piccolo gruppo di persone infette viene inserito in una vasta popolazione in grado di contrarre la malattia. Vogliamo capire se la malattia si estinguerà rapidamente o se si verificherà un'epidemia. Assumiamo che la malattia conferisca immunità permanente a chi guarisce e che il periodo di incubazione sia trascurabilmente breve.

La popolazione N viene divisa in tre classi: Suscettibili (S), Infetti (I) e Rimossi (R). La diffusione è governata dalle seguenti regole:

(1) **Regola 1**: La popolazione resta a un livello fisso N, trascurando nascite, morti (per altre cause), immigrazione ed emigrazione.
(2) **Regola 2**: Il tasso di variazione dei suscettibili è proporzionale al prodotto tra il numero di suscettibili (S) e di infetti (I).
(3) **Regola 3**: Gli individui vengono rimossi dalla classe infettiva a un tasso proporzionale alla dimensione di I.

Questo si traduce nel sistema di equazioni differenziali:

$$\begin{aligned} \frac{\mathrm{d}S}{\mathrm{d}t} &= -rSI \\ \frac{\mathrm{d}I}{\mathrm{d}t} &= rSI - \gamma I \\ \frac{\mathrm{d}R}{\mathrm{d}t} &= \gamma I \end{aligned} \tag{9}$$

dove $r > 0$ è il tasso di infezione e $\gamma > 0$ è il tasso di rimozione. Essendo $S + I + R = N$, è sufficiente studiare le prime due equazioni.

3.2. Analisi delle Orbite e Valore Soglia

Le orbite del sistema nel piano (S, I) si trovano integrando l'equazione del primo ordine $\frac{dI}{dS} = -1 + \frac{\rho}{S}$, dove $\rho = \frac{\gamma}{r}$ è il **valore soglia**. L'integrazione fornisce:

$$I(S) = I_0 + S_0 - S + \rho \ln\left(\frac{S}{S_0}\right)$$

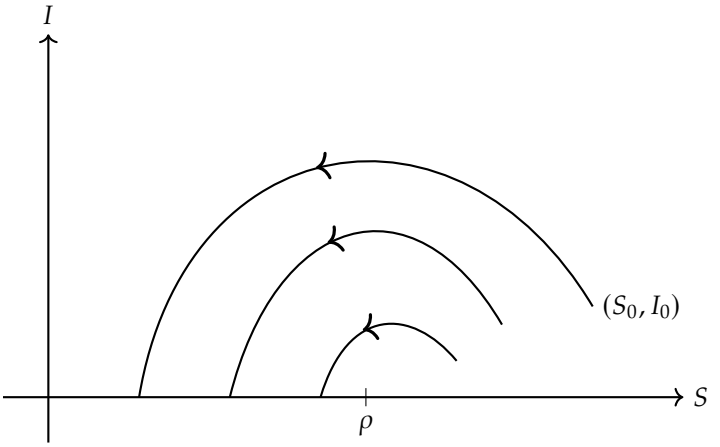


FIGURA 3. Le orbite del sistema SIR nel piano delle fasi. Il picco degli infetti si verifica quando la popolazione suscettibile scende esattamente al valore soglia ρ.

Da questa analisi si traggono due conclusioni fondamentali per l'epidemiologia:

- **Conclusione 1**: Un'epidemia si verificherà *solo se* il numero di suscettibili S_0 supera il valore soglia ρ.
- **Conclusione 2**: La diffusione della malattia non si ferma per mancanza di suscettibili, ma per mancanza di infetti. Alcuni individui sfuggiranno del tutto alla malattia.

3.3. Il Teorema Soglia di Kermack-McKendrick e la Curva Epidemica

Se S_0 è maggiore, ma vicino alla soglia ρ, possiamo stimare quanti contrarranno l'infezione.

TEOREMA (Teorema Soglia di Kermack-McKendrick, 1927). *Sia $S_0 = \rho + \nu$ e assumiamo che $\frac{\nu}{\rho}$ sia molto piccolo rispetto a 1. Assumendo inoltre un numero iniziale di infetti I_0 molto piccolo, il numero di individui che alla fine contrarranno la malattia è approssimativamente 2ν. Ovvero, il livello dei suscettibili viene ridotto a un punto tanto al di sotto della soglia quanto originariamente ne era al di sopra.*

Per confrontare il modello con i dati reali, poiché le statistiche riportano i nuovi rimossi e non i nuovi infetti giornalieri, si calcola $\frac{dR}{dt}$. Con opportune approssimazioni

di Taylor, si ottiene:

$$\frac{\mathrm{d}R}{\mathrm{d}t} = \frac{\gamma\alpha^2\rho^2}{2S_0}\mathrm{sech}^2\left(\frac{1}{2}\alpha\gamma t - \phi\right) \tag{10}$$

Questa equazione definisce una curva a campana simmetrica, chiamata **curva epidemica**.

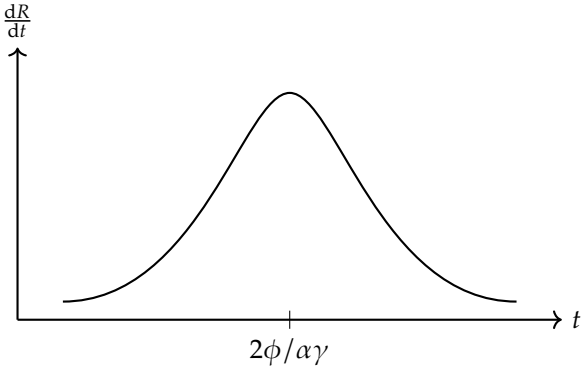


FIGURA 4. La curva epidemica teorica della malattia nel piano $t - \frac{\mathrm{d}R}{\mathrm{d}t}$, che mostra il tipico andamento a campana.

Kermack e McKendrick paragonarono i valori previsti da questa funzione con i dati effettivi della peste di Bombay del 1905-1906, ponendo $\frac{\mathrm{d}R}{\mathrm{d}t} = 890\mathrm{sech}^2(0.2t - 3.4)$. Come si evince dalla sovrapposizione grafica, l'accordo tra il modello differenziale e i decessi reali è eccellente, confermando la solidità del modello SIR.

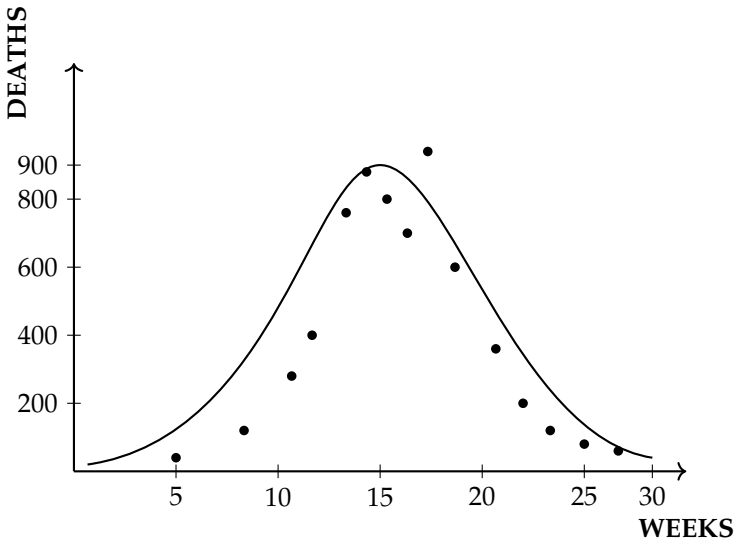


FIGURA 5. Confronto tra i valori reali dei decessi settimanali per la peste di Bombay (•) e la curva prevista dall'equazione del modello SIR.

Bibliografia

[1] Braun, M., *Differential Equations and Their Applications: An Introduction to Applied Mathematics*, 4th ed., Springer-Verlag, New York, 1993.

[2] Bailey, N. T. J., *The mathematical theory of epidemics*, New York, 1957.

[3] Kermack, W. O. e McKendrick, A. G., *Contributions to the mathematical theory of epidemics*, Proceedings Roy. Stat. Soc., A, 115, 700-721, 1927.

[4] Waltman, P., *Deterministic threshold models in the theory of epidemics*, Springer-Verlag, New York, 1974.

INTRODUZIONE AI NUMERI P-ADICI

SEBASTIAN OCAMPO

1. Valutazioni e valori assoluti

DEFINIZIONE 1 (Valore assoluto). Sia K un campo. Un *valore assoluto* su K è una mappa

$$|\cdot| : K \longrightarrow \mathbb{R}_{\geqslant 0} \tag{1}$$

soddisfacente:

(AV1) $\forall x \in K : \ |x| = 0 \iff x = 0$
(AV2) $\forall x, y \in K : \ |xy| = |x| \cdot |y|$
(AV3) $\forall x, y \in K : \ |x + y| \leqslant |x| + |y|$

La coppia $(K, |\cdot|)$ è detta *campo normato*.

ESERCIZIO 2 (Assioma di non-degenerazione). Verificare (AV1) per il valore assoluto usuale su $\mathbb{Q}$ con $x = \frac{2}{3}$ e con $x = 0$.

Soluzione.

$$\begin{aligned} &\left|\tfrac{2}{3}\right| = \tfrac{2}{3} \neq 0 \quad [\tfrac{2}{3} \neq 0] \\ &|0| = 0 \quad [\text{secondo caso}] \\ &|x| = 0 \iff x = 0 \quad \checkmark \quad [\text{(AV1)}] \end{aligned}$$

□

DEFINIZIONE 3 (Non-archimedeo / ultrametrico). $|\cdot|$ è detto *non-archimedeo* (o *ultrametrico*) sse

$$\forall x, y \in K : \quad |x + y| \leqslant \max\big(|x|, |y|\big). \tag{2}$$

Altrimenti $|\cdot|$ è detto *archimedeo*.

ESERCIZIO 4 (Il modulo usuale non è ultrametrico). Stabilire se il valore assoluto usuale su $\mathbb{Q}$ soddisfa (2), provando con $x = y = 1$.

Soluzione.

$$\begin{aligned} &|x + y| = |1 + 1| = 2 \\ &\max(|x|, |y|) = \max(1, 1) = 1 \\ &|x + y| = 2 > 1 = \max(|x|, |y|) \quad [\text{viola (2)}] \\ &\Rightarrow \ |\cdot| \text{ è archimedeo} \quad \checkmark \end{aligned}$$

□

PROPOSIZIONE 5 (Proprietà elementari). $\forall (K, |\cdot|)$ *campo normato:*

$$|1_K| = 1 \tag{3}$$
$$\forall x \in K: \quad |-x| = |x| \tag{4}$$
$$\forall x \in K^\times: \quad |x^{-1}| = |x|^{-1} \tag{5}$$
$$\forall x, y \in K: \quad \big||x| - |y|\big| \leqslant |x - y| \tag{6}$$

ESERCIZIO 6 (Invarianza per segno). Verificare (4) per $x = \frac{3}{4}$ con il valore assoluto usuale su $\mathbb{Q}$.

Soluzione.

$$\begin{aligned} -x &= -\tfrac{3}{4} \\ |-x| &= \left|-\tfrac{3}{4}\right| = \tfrac{3}{4} \\ |x| &= \left|\tfrac{3}{4}\right| = \tfrac{3}{4} \\ |-x| &= \tfrac{3}{4} = |x| \quad \checkmark \quad [(4)] \end{aligned}$$

□

DEFINIZIONE 7 (Valutazione). Sia K un campo. Una *valutazione* su K è una mappa

$$v : K \longrightarrow \mathbb{R} \cup \{+\infty\} \tag{7}$$

soddisfacente:

(V1) $\forall x \in K: \ v(x) = +\infty \iff x = 0$
(V2) $\forall x, y \in K: \ v(xy) = v(x) + v(y)$
(V3) $\forall x, y \in K: \ v(x + y) \geqslant \min\big(v(x), v(y)\big)$

v è detta *discreta* sse $v(K^\times) \subseteq \mathbb{Z}$.

ESERCIZIO 8 (Additività della valutazione). Sia v una valutazione con $v(x) = 2$ e $v(y) = 5$. Calcolare $v(xy)$.

Soluzione.

$$\begin{aligned} v(xy) &= v(x) + v(y) \quad [(V2)] \\ &= 2 + 5 \\ &= 7 \end{aligned}$$

□

PROPOSIZIONE 9 (Disuguaglianza ultrametrica forte). $(K, |\cdot|)$ *ultrametrico per 3. Allora*

$$\forall x, y \in K: \quad |x| \neq |y| \implies |x + y| = \max\big(|x|, |y|\big). \tag{8}$$

ESERCIZIO 10 (Somma con moduli distinti). Sia $|\cdot|$ ultrametrico con $|x| = 8$ e $|y| = 2$. Calcolare $|x + y|$.

Soluzione.

$$\begin{aligned}
&|x| = 8 \neq 2 = |y| \quad \text{[moduli distinti]}\\
&|x+y| = \max(|x|,|y|) \quad [(8)]\\
&= \max(8,2)\\
&= 8
\end{aligned}$$

□

2. La valutazione p-adica su $\mathbb{Q}$

Fissiamo $p \in \mathbb{Z}$ primo, $p \geqslant 2$.

Definizione 11 (Valutazione p-adica su $\mathbb{Z}$). $\forall n \in \mathbb{Z} \setminus \{0\}$:

$$v_p(n) \coloneqq \max\{k \in \mathbb{N} : p^k \mid n\}, \qquad v_p(0) \coloneqq +\infty. \tag{9}$$

Esercizio 12 (Valutazione di un intero). Calcolare $v_2(24)$.

Soluzione.

$$\begin{aligned}
&24 = 2^3 \cdot 3\\
&2^3 = 8 \mid 24 \quad [24 = 8 \cdot 3]\\
&2^4 = 16 \nmid 24 \quad [24/16 \notin \mathbb{Z}]\\
&v_2(24) \overset{(9)}{=} \max\{k : 2^k \mid 24\} = 3
\end{aligned}$$

□

Definizione-Proposizione 13 (Estensione a $\mathbb{Q}$). $\forall x \in \mathbb{Q}^\times$, scritto $x = a/b$ con $a, b \in \mathbb{Z}$, $b \neq 0$:

$$v_p(x) \coloneqq v_p(a) - v_p(b) \tag{10}$$

è ben definita (indipendente dalla rappresentazione a/b). La mappa $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ è una valutazione discreta nel senso di 7.

Esercizio 14 (Valutazione di un razionale). Calcolare $v_2\left(\dfrac{12}{5}\right)$.

Soluzione.

$$\begin{aligned}
&12 = 2^2 \cdot 3, \qquad 5 = 5\\
&v_2(12) \overset{(9)}{=} 2 \quad [2^2 \mid 12,\ 2^3 \nmid 12]\\
&v_2(5) \overset{(9)}{=} 0 \quad [\gcd(5,2) = 1]\\
&v_2\left(\tfrac{12}{5}\right) \overset{(10)}{=} v_2(12) - v_2(5) = 2 - 0 = 2
\end{aligned}$$

□

Definizione 15 (Valore assoluto p-adico). $\forall x \in \mathbb{Q}$:

$$|x|_p := \begin{cases} p^{-v_p(x)} & x \neq 0 \\ 0 & x = 0 \end{cases} \tag{11}$$

Esercizio 16 (Valore assoluto di un intero). Calcolare $|48|_2$.

Soluzione.

$$\begin{aligned} &48 = 2^4 \cdot 3 \\ &v_2(48) \overset{(9)}{=} 4 \quad [2^4 \mid 48,\ 2^5 \nmid 48] \\ &|48|_2 \overset{(11)}{=} 2^{-4} = \tfrac{1}{16} \end{aligned}$$

□

Proposizione 17 ($|\cdot|_p$ è valore assoluto non-archimedeo). $|\cdot|_p$ *definito in* (11) *soddisfa* (AV1), (AV2), (AV3) *e* (2).

Esercizio 18 (Verifica della moltiplicatività). Verificare $|2 \cdot 6|_2 = |2|_2 \, |6|_2$.

Soluzione.

$$\begin{aligned} &|2|_2 \overset{(11)}{=} 2^{-1} = \tfrac{1}{2} \quad [v_2(2) = 1] \\ &|6|_2 \overset{(11)}{=} 2^{-1} = \tfrac{1}{2} \quad [6 = 2 \cdot 3,\ v_2(6) = 1] \\ &2 \cdot 6 = 12 = 2^2 \cdot 3 \\ &|2 \cdot 6|_2 \overset{(11)}{=} 2^{-2} = \tfrac{1}{4} \quad [v_2(12) = 2] \\ &\tfrac{1}{4} = \tfrac{1}{2} \cdot \tfrac{1}{2} = |2|_2 \, |6|_2 \quad [\text{conferma (AV2)}] \end{aligned}$$

□

Teorema 19 (Ostrowski). *Ogni valore assoluto non triviale su $\mathbb{Q}$ è equivalente o al valore assoluto archimedeo standard $|\cdot|_\infty$ o a $|\cdot|_p$ per qualche primo p (cfr. 15).*

Esercizio 20 (Valori p-adici di un intero). Per $x = 24$ calcolare $|24|_2$ e $|24|_3$.

Soluzione.

$$\begin{aligned} &24 = 2^3 \cdot 3 \\ &|24|_2 \overset{(11)}{=} 2^{-3} = \tfrac{1}{8} \quad [v_2(24) = 3] \\ &|24|_3 \overset{(11)}{=} 3^{-1} = \tfrac{1}{3} \quad [v_3(24) = 1] \\ &|24|_p \overset{(11)}{=} p^0 = 1 \quad [p \nmid 24,\ p \neq 2, 3] \end{aligned}$$

□

Proposizione 21 (Formula del prodotto). $\forall x \in \mathbb{Q}^\times$:

$$|x|_\infty \cdot \prod_{p \text{ primo}} |x|_p = 1. \tag{12}$$

Esercizio 22 (Formula del prodotto su un intero). Verificare (12) per $x = 6$.

Soluzione.

$$
\begin{aligned}
&6 = 2 \cdot 3 \\
&|6|_\infty = 6 \\
&|6|_2 \overset{(11)}{=} 2^{-1} = \tfrac{1}{2}, \qquad |6|_3 \overset{(11)}{=} 3^{-1} = \tfrac{1}{3} \\
&|6|_p \overset{(11)}{=} 1 \quad [p \nmid 6,\ p \neq 2, 3] \\
&|6|_\infty \cdot \prod_p |6|_p = 6 \cdot \tfrac{1}{2} \cdot \tfrac{1}{3} \overset{(12)}{=} 1
\end{aligned}
$$

□

3. Spazi ultrametrici

Definizione 23 (Spazio ultrametrico). Uno spazio metrico (X, d) è *ultrametrico* sse

$$\forall x, y, z \in X: \quad d(x, z) \leqslant \max\big(d(x, y), d(y, z)\big). \tag{13}$$

Esercizio 24 (Verifica della disuguaglianza ultrametrica). In $(\mathbb{Q}, d)$ con $d(x, y) = |x - y|_2$, verificare (13) per $x = 0$, $y = 2$, $z = 4$.

Soluzione.

$$
\begin{aligned}
&d(x, z) = |0 - 4|_2 = |-4|_2 \overset{(11)}{=} 2^{-2} = \tfrac{1}{4} \\
&d(x, y) = |0 - 2|_2 = |-2|_2 \overset{(11)}{=} 2^{-1} = \tfrac{1}{2} \\
&d(y, z) = |2 - 4|_2 = |-2|_2 \overset{(11)}{=} 2^{-1} = \tfrac{1}{2} \\
&d(x, z) = \tfrac{1}{4} \leqslant \tfrac{1}{2} = \max\big(d(x, y), d(y, z)\big) \quad \checkmark \quad [(13)]
\end{aligned}
$$

□

Definizione 25 (Palle). $\forall a \in X, \forall r > 0$:

$$B(a, r) := \{x \in X : d(x, a) < r\} \tag{14}$$

$$\overline{B}(a, r) := \{x \in X : d(x, a) \leqslant r\} \tag{15}$$

Esercizio 26 (Appartenenza a una palla aperta). In $(\mathbb{Q}, d)$ con $d(x, y) = |x - y|_3$, stabilire se $6 \in B(0, 1)$.

Soluzione.

$$
\begin{aligned}
&d(6, 0) = |6|_3 \overset{(11)}{=} 3^{-v_3(6)} = 3^{-1} = \tfrac{1}{3} \\
&\tfrac{1}{3} < 1 \quad [d(6, 0) < 1] \\
&\Rightarrow\ 6 \in B(0, 1) \quad \checkmark \quad [(14)]
\end{aligned}
$$

□

Proposizione 27 (Ogni punto è centro). *(X, d) ultrametrico per 23. $\forall a \in X$, $\forall r > 0$, $\forall b \in B(a, r)$:*

$$B(a, r) = B(b, r). \tag{16}$$

Analogamente per $\overline{B}$.

Esercizio 28 (Ricentrare una palla). In $(\mathbb{Q}, d)$ con $d(x, y) = |x - y|_2$, verificare che $2 \in B(0, 1)$ e che $0 \in B(2, 1)$, coerentemente con (16).

Soluzione.

$$d(2, 0) = |2|_2 \overset{(11)}{=} 2^{-1} = \tfrac{1}{2} < 1 \quad [2 \in B(0, 1)]$$
$$d(0, 2) = |-2|_2 \overset{(11)}{=} 2^{-1} = \tfrac{1}{2} < 1 \quad [0 \in B(2, 1)]$$
$$\Rightarrow B(0, 1) = B(2, 1) \quad \checkmark \quad [(16)]$$

□

Proposizione 29 (Palle aperte sono chiuse e viceversa). *(X, d) ultrametrico. $\forall a \in X$, $\forall r > 0$: $B(a, r)$ è chiusa e $\overline{B}(a, r)$ è aperta nella topologia di d.*

Esercizio 30 (Una palla aperta è anche chiusa). In $(\mathbb{Q}, d)$ con $d(x, y) = |x - y|_2$, mostrare che $B(0, 1) = \overline{B}(0, \frac{1}{2})$.

Soluzione.

$$|x|_2 \in \{2^k : k \in \mathbb{Z}\} \cup \{0\} \quad [(11)]$$
$$|x|_2 < 1 \iff |x|_2 \leqslant \tfrac{1}{2} \quad [\text{nessun valore in } (\tfrac{1}{2}, 1)]$$
$$B(0, 1) \overset{(14)}{=} \{x : |x|_2 \leqslant \tfrac{1}{2}\} \overset{(15)}{=} \overline{B}(0, \tfrac{1}{2})$$
$$\Rightarrow B(0, 1) \text{ è chiusa} \quad \checkmark \quad [29]$$

□

Proposizione 31 (Triangoli isosceli). *(X, d) ultrametrico. $\forall x, y, z \in X$, almeno due fra $d(x, y), d(y, z), d(x, z)$ coincidono e sono $\geqslant$ del terzo.*

Esercizio 32 (Triangolo isoscele 2-adico). In $(\mathbb{Q}, d)$ con $d(x, y) = |x - y|_2$, calcolare le tre distanze fra $0, 1, 2$ e verificare 31.

Soluzione.

$$d(0, 1) = |-1|_2 \overset{(11)}{=} 2^0 = 1$$
$$d(1, 2) = |-1|_2 \overset{(11)}{=} 2^0 = 1$$
$$d(0, 2) = |-2|_2 \overset{(11)}{=} 2^{-1} = \tfrac{1}{2}$$
$$d(0, 1) = d(1, 2) = 1 \geqslant \tfrac{1}{2} = d(0, 2) \quad \checkmark \quad [31]$$

□

Proposizione 33 (Sconnessione totale). *(X, d) ultrametrico $\implies$ (X, d) è totalmente sconnesso.*

Esercizio 34 (Separazione di due punti). In $(\mathbb{Q}, d)$ con $d(x, y) = |x - y|_2$, separare 0 e 1 con due palle disgiunte.

Soluzione.

$$
\begin{aligned}
&d(0,1) = |-1|_2 \overset{(11)}{=} 2^0 = 1 \\
&0 \in B(0,1), \quad d(1,0) = 1 \not< 1 \Rightarrow 1 \notin B(0,1) \\
&1 \in B(1,1), \quad B(0,1) \cap B(1,1) = \varnothing \quad \text{[palle clopen disgiunte]} \\
&\Rightarrow (\mathbb{Q}, d) \text{ è totalmente sconnesso} \quad \checkmark \quad [33]
\end{aligned}
$$

□

Definizione 35 (Successione di Cauchy). $(x_n)_{n\in\mathbb{N}} \subseteq X$ è di *Cauchy* sse

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall m, n \geqslant N :\ d(x_m, x_n) < \varepsilon. \tag{17}$$

Esercizio 36 (Successione costante è di Cauchy). In $(\mathbb{Q}, d)$ con $d(x, y) = |x - y|_5$, mostrare che $x_n = 3$ (costante) è di Cauchy.

Soluzione.

$$
\begin{aligned}
&d(x_m, x_n) = |3 - 3|_5 = |0|_5 = 0 \\
&\forall \varepsilon > 0 :\ 0 < \varepsilon \quad [\text{con } N = 0] \\
&\Rightarrow (x_n) \text{ è di Cauchy} \quad \checkmark \quad [(17)]
\end{aligned}
$$

□

Proposizione 37 (Caratterizzazione Cauchy nel caso ultrametrico). (X, d) *ultrametrico.* $(x_n) \subseteq X$ *è di Cauchy* (17) *sse*

$$\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geqslant N :\ d(x_{n+1}, x_n) < \varepsilon. \tag{18}$$

Esercizio 38 (Cauchy via differenze consecutive). In $(\mathbb{Q}, d)$ con $d(x, y) = |x - y|_3$, usare (18) per mostrare che $x_n = 3^n$ è di Cauchy.

Soluzione.

$$
\begin{aligned}
&x_{n+1} - x_n = 3^{n+1} - 3^n = 3^n \cdot 2 \\
&v_3(3^n \cdot 2) \overset{(9)}{=} n \quad [v_3(2) = 0] \\
&d(x_{n+1}, x_n) \overset{(11)}{=} 3^{-n} \xrightarrow{n\to\infty} 0 \\
&\Rightarrow (x_n) \text{ è di Cauchy} \quad \checkmark \quad [(18)]
\end{aligned}
$$

□

Proposizione 39 (Convergenza delle serie). $(K, |\cdot|)$ *campo ultrametrico completo.* $\forall (a_n)_{n\in\mathbb{N}} \subseteq K$*:*

$$\sum_{n=0}^{\infty} a_n \text{ converge} \iff |a_n| \xrightarrow{n\to\infty} 0. \tag{19}$$

Esercizio 40 (Convergenza di una serie 5-adica). Stabilire se $\sum_{n=0}^{\infty} 5^n$ converge in un campo ultrametrico completo, tramite (19).

Soluzione.

$$
\begin{aligned}
&v_5(5^n) \overset{(9)}{=} n \\
&|5^n|_5 \overset{(11)}{=} 5^{-n} \\
&\lim_{n\to\infty} |5^n|_5 = 0 \\
&\Rightarrow \sum_{n=0}^{\infty} 5^n \text{ converge} \quad \checkmark \quad [(19)]
\end{aligned}
$$

□

4. Il campo $\mathbb{Q}_p$

Definizione 41 (Il campo $\mathbb{Q}_p$). Il campo dei *numeri p-adici* $\mathbb{Q}_p$ è il *completamento* di $\mathbb{Q}$ rispetto alla metrica p-adica $d_p(x,y) := |x-y|_p$:

$$\mathbb{Q}_p := \widehat{\mathbb{Q}}^{|\cdot|_p}, \tag{20}$$

ossia l'unico spazio metrico completo, a meno di isometria, in cui $\mathbb{Q}$ si immerge come sottospazio denso.

Esercizio 42 (Successioni con lo stesso limite). In $\mathbb{Q}_5$, mostrare che le successioni razionali $(3)_{n\geq 0}$ e $(3+5^n)_{n\geq 0}$ hanno lo stesso limite.

Soluzione.

$$
\begin{aligned}
&(3+5^n) - 3 = 5^n \\
&|(3+5^n)-3|_5 = |5^n|_5 \overset{(11)}{=} 5^{-n} \xrightarrow{n\to\infty} 0 \\
&\Rightarrow\ 3+5^n \xrightarrow{n\to\infty} 3 \text{ in } \mathbb{Q}_5 \quad \checkmark \quad [(20)]
\end{aligned}
$$

□

Proposizione 43 ($\mathbb{Q}_p$ è un campo). *Le operazioni di somma e prodotto di $\mathbb{Q}$ si estendono per continuità a $\mathbb{Q}_p$, che risulta così un campo contenente $\mathbb{Q}$ come sottocampo denso.*

Esercizio 44 (Inverso in $\mathbb{Q}_p$). In $\mathbb{Q}_5$, calcolare l'inverso di $3 \in \mathbb{Q} \subseteq \mathbb{Q}_5$.

Soluzione.

$$
\begin{aligned}
&3 \in \mathbb{Q} \subseteq \mathbb{Q}_5 \quad [\mathbb{Q} \text{ sottocampo denso}] \\
&3 \cdot \tfrac{1}{3} = 1, \quad \tfrac{1}{3} \in \mathbb{Q} \subseteq \mathbb{Q}_5 \\
&\Rightarrow\ 3^{-1} = \tfrac{1}{3} \text{ in } \mathbb{Q}_5 \quad \checkmark \quad [43]
\end{aligned}
$$

□

Definizione-Proposizione 45 (Estensione di $|\cdot|_p$ a $\mathbb{Q}_p$). Il valore assoluto $|\cdot|_p$ si estende in modo unico per continuità a $\mathbb{Q}_p$: se $\xi = \lim_{n\to\infty} x_n$ con $x_n \in \mathbb{Q}$, allora

$$|\xi|_p = \lim_{n\to\infty} |x_n|_p \tag{21}$$

(limite esistente e indipendente dalla successione approssimante). La mappa $|\cdot|_p : \mathbb{Q}_p \to \mathbb{R}_{\geqslant 0}$ è un valore assoluto non-archimedeo (3) che estende $|\cdot|_p$ su $\mathbb{Q}$ (15).

Esercizio 46 (Valore assoluto di un razionale in $\mathbb{Q}_p$). In $\mathbb{Q}_5$, calcolare $|\xi|_5$ dove $\xi = 3 \in \mathbb{Q} \subseteq \mathbb{Q}_5$.

Soluzione.

$$\begin{aligned}
&\xi = \lim_{n\to\infty} 3 \quad \text{[successione costante]}\\
&|3|_5 \overset{(11)}{=} 5^0 = 1\\
&|\xi|_5 \overset{(21)}{=} \lim_{n\to\infty} |3|_5 = 1 \quad \checkmark
\end{aligned}$$

□

Proposizione 47 ($|\mathbb{Q}_p^\times|_p = p^{\mathbb{Z}}$).

$$\left\{|\xi|_p : \xi \in \mathbb{Q}_p^\times\right\} = \left\{p^n : n \in \mathbb{Z}\right\}. \tag{22}$$

Esercizio 48 (Un valore ammissibile). Verificare che $|\xi|_5 = \frac{1}{25}$ appartiene al gruppo dei valori $\{5^n : n \in \mathbb{Z}\}$.

Soluzione.

$$\begin{aligned}
&\tfrac{1}{25} = 5^{-2}\\
&-2 \in \mathbb{Z} \Rightarrow 5^{-2} \in \{5^n : n \in \mathbb{Z}\}\\
&\Rightarrow \tfrac{1}{25} \in |\mathbb{Q}_5^\times|_5 \quad \checkmark \quad [(22)]
\end{aligned}$$

□

Definizione-Proposizione 49 (Estensione di v_p a $\mathbb{Q}_p$). $\forall \xi \in \mathbb{Q}_p$:

$$v_p(\xi) := -\log_p |\xi|_p \quad (v_p(0) := +\infty) \tag{23}$$

è una valutazione discreta (7) su $\mathbb{Q}_p$ che estende v_p su $\mathbb{Q}$ (13), e $v_p(\mathbb{Q}_p^\times) = \mathbb{Z}$.

Esercizio 50 (Valutazione da valore assoluto). Dato $\xi \in \mathbb{Q}_5$ con $|\xi|_5 = \frac{1}{25}$, calcolare $v_5(\xi)$.

Soluzione.

$$\begin{aligned}
&|\xi|_5 = \tfrac{1}{25} = 5^{-2}\\
&v_5(\xi) \overset{(23)}{=} -\log_5 |\xi|_5 = -\log_5 5^{-2}\\
&= -(-2) = 2\\
&\Rightarrow v_5(\xi) = 2 \quad \checkmark
\end{aligned}$$

□

5. L'anello $\mathbb{Z}_p$

DEFINIZIONE 51 (Interi p-adici).

$$\mathbb{Z}_p \coloneqq \{\xi \in \mathbb{Q}_p : |\xi|_p \leqslant 1\} = \{\xi \in \mathbb{Q}_p : v_p(\xi) \geqslant 0\}. \tag{24}$$

ESERCIZIO 52 (Appartenenza a $\mathbb{Z}_2$). Stabilire se $\frac{3}{4} \in \mathbb{Z}_2$.

Soluzione.

$$4 = 2^2 \implies v_2(4) \overset{(9)}{=} 2, \quad v_2(3) = 0 \ [\gcd(3,2) = 1]$$
$$v_2\left(\tfrac{3}{4}\right) \overset{(10)}{=} 0 - 2 = -2$$
$$\left|\tfrac{3}{4}\right|_2 \overset{(11)}{=} 2^2 = 4 > 1 \overset{(24)}{\implies} \tfrac{3}{4} \notin \mathbb{Z}_2$$

□

PROPOSIZIONE 53 ($\mathbb{Z}_p$ è sottoanello). *$\mathbb{Z}_p$ è un sottoanello di $\mathbb{Q}_p$ contenente $\mathbb{Z}$.*

ESERCIZIO 54 (Chiusura per somma in $\mathbb{Z}_5$). Verificare che $\frac{1}{3}, \frac{1}{2} \in \mathbb{Z}_5$ e che $\frac{1}{3} + \frac{1}{2} \in \mathbb{Z}_5$.

Soluzione.

$$v_5\left(\tfrac{1}{3}\right) \overset{(10)}{=} 0, \quad v_5\left(\tfrac{1}{2}\right) \overset{(10)}{=} 0 \implies \tfrac{1}{3}, \tfrac{1}{2} \in \mathbb{Z}_5$$
$$\tfrac{1}{3} + \tfrac{1}{2} = \tfrac{5}{6}, \quad v_5\left(\tfrac{5}{6}\right) \overset{(10)}{=} 1 - 0 = 1 \geq 0$$
$$\implies \tfrac{5}{6} \in \mathbb{Z}_5 \text{ [stabile per somma]}$$

□

PROPOSIZIONE 55 (Caratterizzazione delle unità).

$$\mathbb{Z}_p^\times = \{\xi \in \mathbb{Z}_p : |\xi|_p = 1\} = \{\xi \in \mathbb{Z}_p : v_p(\xi) = 0\}. \tag{25}$$

ESERCIZIO 56 (Unità di $\mathbb{Z}_5$). Stabilire se $\frac{3}{7} \in \mathbb{Z}_5^\times$.

Soluzione.

$$v_5(3) = 0, \quad v_5(7) = 0 \implies v_5\left(\tfrac{3}{7}\right) \overset{(10)}{=} 0$$
$$\left|\tfrac{3}{7}\right|_5 \overset{(11)}{=} 5^0 = 1$$
$$\implies \tfrac{3}{7} \in \mathbb{Z}_5^\times \text{ [per (25)]}$$

□

PROPOSIZIONE 57 ($\mathbb{Z}_p$ è anello locale). *$\mathbb{Z}_p$ è un anello locale con unico ideale massimale*

$$\mathfrak{m} \coloneqq p\mathbb{Z}_p = \{\xi \in \mathbb{Z}_p : |\xi|_p < 1\} = \{\xi \in \mathbb{Z}_p : v_p(\xi) \geqslant 1\}. \tag{26}$$

ESERCIZIO 58 (Appartenenza al massimale). Stabilire se $\frac{6}{5} \in 3\mathbb{Z}_3$.

Soluzione.

$$6 = 2 \cdot 3 \;\Rightarrow\; v_3(6) \overset{(9)}{=} 1, \quad v_3(5) = 0$$
$$v_3\left(\tfrac{6}{5}\right) \overset{(10)}{=} 1 - 0 = 1 \geq 1$$
$$\Rightarrow\; \tfrac{6}{5} \in 3\mathbb{Z}_3 \text{ [per (26)]}$$

□

Proposizione 59 (Campo residuo).

$$\mathbb{Z}_p \big/ p\mathbb{Z}_p \cong \mathbb{F}_p. \tag{27}$$

Esercizio 60 (Riduzione in $\mathbb{F}_5$). Calcolare l'immagine di 7 in $\mathbb{Z}_5 \big/ 5\mathbb{Z}_5 \cong \mathbb{F}_5$.

Soluzione.

$$v_5(7) = 0 \;\Rightarrow\; 7 \in \mathbb{Z}_5$$
$$7 = 1 \cdot 5 + 2 \;\Rightarrow\; 7 \equiv 2\,(5)$$
$$\Rightarrow\; \overline{7} = \overline{2} \in \mathbb{F}_5 \text{ [per (27)]}$$

□

Proposizione 61 ($\mathbb{Q}_p$ come campo dei quozienti).

$$\mathbb{Q}_p = \mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Z}_p\left[\tfrac{1}{p}\right]. \tag{28}$$

Esercizio 62 (Scrittura in $\mathbb{Z}_3[\frac{1}{3}]$). Scrivere $\frac{7}{9} \in \mathbb{Q}_3$ come $u \cdot 3^k$ con $u \in \mathbb{Z}_3^\times$.

Soluzione.

$$9 = 3^2 \;\Rightarrow\; v_3\left(\tfrac{7}{9}\right) \overset{(10)}{=} 0 - 2 = -2$$
$$\tfrac{7}{9} = 7 \cdot 3^{-2}, \quad v_3(7) = 0 \;\Rightarrow\; u = 7 \in \mathbb{Z}_3^\times$$
$$\Rightarrow\; \tfrac{7}{9} \in \mathbb{Z}_3\left[\tfrac{1}{3}\right] \text{ [per (28)]}$$

□

Teorema 63 (Compattezza). *$\mathbb{Z}_p$ è compatto e $\mathbb{Q}_p$ è localmente compatto.*

Esercizio 64 (Ricoprimento finito di $\mathbb{Z}_5$). Esibire un ricoprimento di $\mathbb{Z}_5$ con 5 palle di raggio $\frac{1}{5}$.

Soluzione.

$$\mathbb{Z}_5 = \bigsqcup_{a=0}^{4} (a + 5\mathbb{Z}_5) \text{ [classi mod 5]}$$
$$a + 5\mathbb{Z}_5 = \left\{\xi : |\xi - a|_5 \overset{(11)}{\leq} 5^{-1}\right\} \text{ [palla raggio } \tfrac{1}{5}\text{]}$$
$$\Rightarrow\; 5 \text{ palle ricoprono } \mathbb{Z}_5 \text{ [totale limitatezza]}$$

□

Teorema 65 ($\mathbb{Z}_p$ è chiusura di $\mathbb{Z}$). *$\mathbb{Z}_p$ è la chiusura di $\mathbb{Z}$ in $\mathbb{Q}_p$.*

Esercizio 66 (Interi che approssimano -1). Mostrare che gli interi $x_k = 3^k - 1$ tendono a -1 in $\mathbb{Z}_3$.

Soluzione.

$$\begin{aligned} &-1 - x_k = -1 - (3^k - 1) = -3^k \\ &|-1 - x_k|_3 \overset{(11)}{=} 3^{-k} \longrightarrow 0 \, [k \to \infty] \\ &\Rightarrow \; x_k \longrightarrow -1 \; \Rightarrow \; -1 \in \overline{\mathbb{Z}} = \mathbb{Z}_3 \end{aligned}$$

□

6. Sviluppo p-adico

Definizione 67 (Cifre). $\mathscr{D} \coloneqq \{0, 1, \dots, p-1\} \subseteq \mathbb{Z}$.

Esercizio 68 (Insieme delle cifre per $p = 3$). Elencare $\mathscr{D}$ per $p = 3$ e dire quante cifre ci sono.

Soluzione.

$$\begin{aligned} &\mathscr{D} = \{0, 1, \dots, p-1\} \; \Rightarrow \; \mathscr{D} = \{0, 1, 2\} \, [p = 3] \\ &|\mathscr{D}| = p = 3 \\ &\Rightarrow \text{ ogni cifra } a_n \in \{0, 1, 2\} \quad \checkmark \end{aligned}$$

□

Teorema 69 (Sviluppo p-adico in $\mathbb{Z}_p$). *$\forall \xi \in \mathbb{Z}_p$, $\exists!\, (a_n)_{n \geqslant 0} \subseteq \mathscr{D}$ tale che*

$$\xi = \sum_{n=0}^{\infty} a_n p^n \tag{29}$$

(serie convergente in $\mathbb{Z}_p$ per 39).

Esercizio 70 (Sviluppo 5-adico di un intero). Scrivere lo sviluppo 5-adico di 12.

Soluzione.

$$\begin{aligned} &12 = 2 \cdot 5 + 2 \; \Rightarrow \; a_0 = 2, \quad \xi_1 = 2 \\ &2 = 0 \cdot 5 + 2 \; \Rightarrow \; a_1 = 2, \quad \xi_2 = 0 \\ &12 \overset{(29)}{=} 2 + 2 \cdot 5 = 2 + 10 \quad \checkmark \end{aligned}$$

□

Teorema 71 (Sviluppo p-adico in $\mathbb{Q}_p$). *$\forall \xi \in \mathbb{Q}_p^{\times}$, posto $n_0 \coloneqq v_p(\xi) \in \mathbb{Z}$, $\exists!\, (a_n)_{n \geqslant n_0} \subseteq \mathscr{D}$ con $a_{n_0} \neq 0$ tale che*

$$\xi = \sum_{n=n_0}^{\infty} a_n p^n. \tag{30}$$

Esercizio 72 (Prima cifra 3-adica di $\frac{1}{2}$). Calcolare la cifra a_0 nello sviluppo 3-adico di $\frac{1}{2}$.

Soluzione.

$$v_3\left(\tfrac{1}{2}\right) \overset{(10)}{=} 0 \;\Rightarrow\; n_0 = 0,\ \tfrac{1}{2} \in \mathbb{Z}_3$$
$$2\,a_0 \equiv 1\ (3) \;\Rightarrow\; 2 \cdot 2 = 4 \equiv 1\ (3)$$
$$\Rightarrow\; a_0 = 2 \quad \checkmark$$

□

Corollario 73 (Cardinalità). $|\mathbb{Z}_p| = |\mathbb{Q}_p| = 2^{\aleph_0}$.

Esercizio 74 (Conteggio delle cifre iniziali). Contare le successioni di 3 cifre iniziali (a_0, a_1, a_2) in $\mathbb{Z}_5$.

Soluzione.

$$a_i \in \mathscr{D} = \{0, \dots, 4\} \;\Rightarrow\; 5 \text{ scelte per ciascuna}$$
$$\#\{(a_0, a_1, a_2)\} = 5 \cdot 5 \cdot 5 = 5^3 = 125$$
$$\Rightarrow\; p^k = 5^3 \text{ successioni} \quad \checkmark$$

□

7. Ideali e quozienti di $\mathbb{Z}_p$

Proposizione 75 (Caratterizzazione di $p^n\mathbb{Z}_p$). $\forall n \in \mathbb{N}$:

$$p^n\mathbb{Z}_p = \left\{\xi \in \mathbb{Z}_p : |\xi|_p \leqslant p^{-n}\right\} = \left\{\xi \in \mathbb{Z}_p : v_p(\xi) \geqslant n\right\}. \tag{31}$$

Esercizio 76 (Appartenenza agli ideali $3^n\mathbb{Z}_3$). Dire a quali $3^n\mathbb{Z}_3$ appartiene $\xi = 45$.

Soluzione.

$$45 = 3^2 \cdot 5 \;\Rightarrow\; v_3(45) \overset{(9)}{=} 2$$
$$45 \in 3^n\mathbb{Z}_3 \overset{(31)}{\iff} v_3(45) \geq n \iff n \leq 2$$
$$\Rightarrow\; 45 \in \mathbb{Z}_3,\ 3\mathbb{Z}_3,\ 9\mathbb{Z}_3; \quad 45 \notin 27\mathbb{Z}_3 \quad \checkmark$$

□

Teorema 77 (Classificazione degli ideali). *Gli ideali di $\mathbb{Z}_p$ sono esattamente*

$$\{0\} \quad e \quad p^n\mathbb{Z}_p,\ n \in \mathbb{N}. \tag{32}$$

In particolare $\mathbb{Z}_p$ è un dominio a ideali principali.

Esercizio 78 (Ideale generato da 12). Identificare l'ideale $12\mathbb{Z}_3$ nella lista (32).

Soluzione.

$$12 = 3 \cdot 4, \quad v_3(4) = 0 \;\Rightarrow\; 4 \in \mathbb{Z}_3^\times$$
$$12\mathbb{Z}_3 = 3 \cdot 4\,\mathbb{Z}_3 = 3\mathbb{Z}_3 \text{ [unità assorbita]}$$
$$\Rightarrow\; 12\mathbb{Z}_3 = 3^1\mathbb{Z}_3 \text{ [per 77]} \quad \checkmark$$

□

Corollario 79 (Proprietà algebriche di $\mathbb{Z}_p$). *$\mathbb{Z}_p$ è:*

(1) *dominio d'integrità;*
(2) *locale, con massimale $p\mathbb{Z}_p$;*
(3) *noetheriano;*
(4) *a ideali principali;*
(5) *anello di valutazione discreta;*
(6) *dominio di Dedekind con un unico primo.*

Esercizio 80 (Ideale a due generatori è principale). Mostrare che $(9, 27) \subseteq \mathbb{Z}_3$ è principale.

Soluzione.

$$\begin{aligned} &v_3(9) = 2, \quad v_3(27) = 3 \implies \min\{2,3\} = 2 \\ &27 = 9 \cdot 3 \implies 27 \in 9\mathbb{Z}_3 \implies (9,27) = 9\mathbb{Z}_3 \\ &\implies \text{principale } [77 : \ \mathbb{Z}_3 \text{ è PID}] \quad \checkmark \end{aligned}$$

□

Teorema 81 (Quozienti finiti). *$\forall n \in \mathbb{N}$, $n \geqslant 1$:*

$$\mathbb{Z}_p \big/ p^n\mathbb{Z}_p \cong \mathbb{Z} \big/ p^n\mathbb{Z} \tag{33}$$

come anelli.

Esercizio 82 (Riduzione di -1 modulo 25). Calcolare $\pi_2(-1)$ in $\mathbb{Z}_5 \big/ 25\mathbb{Z}_5 \cong \mathbb{Z} \big/ 25\mathbb{Z}$.

Soluzione.

$$\begin{aligned} &\mathbb{Z}_5 \big/ 5^2\mathbb{Z}_5 \overset{(33)}{\cong} \mathbb{Z} \big/ 25\mathbb{Z} \\ &-1 \equiv 24 \ (25) \ [-1 + 25 = 24] \\ &\implies \pi_2(-1) = \overline{24} \quad \checkmark \end{aligned}$$

□

Corollario 83 (Cardinalità dei quozienti). *$\forall n \in \mathbb{N}$, $n \geqslant 1$: $|\mathbb{Z}_p / p^n\mathbb{Z}_p| = p^n$.*

Esercizio 84 (Cardinalità di un quoziente). Calcolare $\left|\mathbb{Z}_5 \big/ 25\mathbb{Z}_5\right|$.

Soluzione.

$$\begin{aligned} &\mathbb{Z}_5 \big/ 25\mathbb{Z}_5 \overset{(33)}{\cong} \mathbb{Z} \big/ 25\mathbb{Z} \\ &\left|\mathbb{Z} \big/ 25\mathbb{Z}\right| = 25 = 5^2 \\ &\implies \left|\mathbb{Z}_5 \big/ 25\mathbb{Z}_5\right| = 5^2 = 25 \quad \checkmark \end{aligned}$$

□

Proposizione 85 (Compatibilità delle proiezioni). *$\forall n \in \mathbb{N}$, sia*

$$\pi_n : \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}_p \big/ p^n\mathbb{Z}_p \cong \mathbb{Z} \big/ p^n\mathbb{Z} \tag{34}$$

la proiezione canonica. $\forall m \geqslant n \geqslant 1$, $\exists!$ *omomorfismo* $\varphi_{m,n} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ *tale che*

$$\varphi_{m,n} \circ \pi_m = \pi_n. \tag{35}$$

Esercizio 86 (Compatibilità delle riduzioni). Verificare $\varphi_{2,1}(\pi_2(-1)) = \pi_1(-1)$ in $\mathbb{Z}_5$.

Soluzione.

$$\pi_2(-1) = \overline{24} \in \mathbb{Z}/25\mathbb{Z}\ [-1 \equiv 24\ (25)]$$
$$\varphi_{2,1}(\overline{24}) = 24 \bmod 5 = \overline{4}\ [24 = 4 \cdot 5 + 4]$$
$$\pi_1(-1) = -1 \bmod 5 = \overline{4} \implies \text{uguali} \quad \checkmark$$

□

Teorema 87 (Iniettività della famiglia (π_n)).

$$\bigcap_{n\geqslant 1} p^n\mathbb{Z}_p = \{0\}, \tag{36}$$

ovvero la famiglia $(\pi_n)_{n\geqslant 1}$ *separa i punti di* $\mathbb{Z}_p$.

Esercizio 88 (Un elemento non nullo esce dall'intersezione). Mostrare che $5 \notin \bigcap_{n\geq 1} 5^n\mathbb{Z}_5$.

Soluzione.

$$v_5(5) \overset{(9)}{=} 1$$
$$5 \in 5^n\mathbb{Z}_5 \overset{(31)}{\iff} 1 \geq n \implies 5 \notin 5^2\mathbb{Z}_5$$
$$\implies 5 \notin \bigcap_{n\geq 1} 5^n\mathbb{Z}_5 \overset{(36)}{=} \{0\} \quad \checkmark$$

□

LA MECCANICA QUANTISTICA COME TEORIA STATISTICA

LORENZO SILVIDII, MATTEO RAZZA

In questo intervento presenteremo la definizione assiomatica di teoria statistica secondo l'approccio di Holevo e mostreremo come tale formalismo generale si specializzi nel caso classico e in quello quantistico, evidenziandone le differenze.

Infatti, nonostante l'efficacia predittiva della meccanica quantistica, la sua formulazione standard risulta talvolta inadeguata. Inquadrare la meccanica quantistica come teoria statistica nel linguaggio di Holevo non solo ne dà un formalismo più chiaro e profondo, ma la rende anche adeguata a una trattazione nell'ambito dell'informazione quantistica e dei sistemi quantistici aperti.

1. Definizione di teoria statistica

Quando parliamo di teoria statistica intendiamo una teoria in cui l'oggetto principe è la probabilità e il modo in cui all'interno della nostra teoria questa sia definita. Una volta caratterizzata la probabilità è poi possibile ottenere tutte le altre quantità statistiche di interesse, come medie e varianze.

Nel seguito enunceremo gli assiomi di Holevo che danno la definizione matematica di teoria statistica.

1.1. Stati, Misurazioni e Probabilità

Essendo interessati alla statistica di un dato esperimento, per prima cosa lo possiamo suddividere in tre parti:

- preparazione: si segue una procedura in modo da portare il sistema preso in esame in una data configurazione. Diamo a questa configurazione il nome di stato;
- misurazione: facciamo interagire il nostro sistema con un apparato di misura esterno e otteniamo dei risultati in seguito a questa interazione;
- probabilità: categorizziamo i risultati della misurazione e ricostruiamo la distribuzione di probabilità in base alla frequenza con cui si realizza ogni risultato.

Stiamo quindi implicitamente supponendo di poter ripetere il nostro esperimento infinite volte e che ogni ripetizione sia indipendente dalle altre.

Come esempio semplice di questa suddivisione, possiamo pensare al lancio di un dado: scuotere il dado e lanciarlo corrisponde alla preparazione, leggere il numero

della faccia superiore corrisponde alla misurazione e ripetendo tante volte questa procedura si accumula statistica e si ottiene la distribuzione di probabilità associata al dado, così da poter controllare se sia bilanciato o truccato.

A questo punto, siamo pronti a entrare nel vivo del formalismo.

Chiameremo S gli stati e $\mathscr{C}$ il loro insieme. Chiameremo M le misurazioni e $\mathscr{M}$ il loro insieme. Ad ogni misurazione è associato uno spazio misurabile $(X, \mathscr{F}(X))$, composto da uno spazio campionario X, lo spazio dei possibili risultati della misura, e una σ-algebra $\mathscr{F}(X)$ su di esso definita. Ricordiamo che la σ-algebra $\mathscr{F}(X)$ è una collezione di sottoinsiemi di X in cui:

- X e $\varnothing$ appartengono a $\mathscr{F}(X)$;
- dato un sottoinsieme A, il suo complementare $A^c \in \mathscr{F}(X)$;
- dati $A, B \in \mathscr{F}(X)$, la loro unione $A \cup B \in \mathscr{F}(X)$.

Indicheremo con $P_S^M(B)$ la probabilità che, preparando il sistema nello stato S e facendo la misurazione M sul sistema, si ottenga un risultato di misura $x \in B$.

Ricordiamo che, dato uno spazio misurabile $(X, \mathscr{F}(X))$, una distribuzione di probabilità su questo spazio è una funzione $P : \mathscr{F}(X) \to [0, 1]$ con le seguenti proprietà:

- positività: $P(A) \geqslant 0 \quad \forall A \in \mathscr{F}(X)$;
- normalizzazione: $P(X) = 1$;
- σ-additività: dati $A, B \in \mathscr{F}(X)$, con $A \cap B = \varnothing$, allora $P(A \cup B) = P(A) + P(B)$.

Chiameremo $\mathscr{D}(X)$ l'insieme delle distribuzioni di probabilità riferite all'insieme $(X, \mathscr{F}(X))$.

Quanto detto finora può essere formalizzato nel primo assioma.

Assioma 1. Gli stati sono elementi S di un insieme $\mathscr{C}$.
Le misurazioni sono elementi M di un insieme $\mathscr{M}$; ad ogni misurazione è associato uno spazio misurabile $(X, \mathscr{F}(X))$.
Alla coppia (S, M) associamo una distribuzione di probabilità $P_S^M \in \mathscr{D}(X)$.

I prossimi assiomi ci daranno delle condizioni che lo spazio degli stati e quello delle misurazioni devono rispettare.

1.2. La miscela statistica

In generale, la procedura di preparazione dello stato non sarà perfetta e potremmo non avere sempre a disposizione lo stato S desiderato, ma potremmo generare degli stati S_j ognuno con probabilità p_j. Chiamiamo la famiglia $\{S_j, p_j\}_{j=1}^n$ miscela statistica.

Nel caso del dado, potremmo ad esempio pensare di scuoterlo in maniera diversa in ogni lancio, o di gettarlo su una superficie diversa.

Facciamo dunque richiesta che esista, all'interno della nostra teoria, uno stato associato alla statistica della miscela.

Assioma 2. Alla miscela statistica $\{S_j, p_j\}_{j=1}^n$ dove $S_j \in \mathscr{C}\ \forall j, p_j \geqslant 0\ \forall j, \sum_{j=1}^n p_j = 1$, è sempre associabile uno stato $\bar{S} \in \mathscr{C}$ tale che:

$$P_{\bar{S}}^M(B) = \sum_{j=1}^n p_j P_{S_j}^M(B) \qquad \forall M \in \mathscr{M}, \forall B \in \mathscr{F}(X). \tag{1}$$

Conseguenza di questo assioma è il fatto che l'insieme degli stati $\mathscr{C}$ è in corrispondenza diretta con un insieme convesso.

Negli esempi che faremo nel seguito, $\mathscr{C}$ sarà direttamente un insieme convesso. Questo significa che dati $S_1, S_2 \in \mathscr{C}$, allora la combinazione convessa dei due $S = pS_1 + (1-p)S_2$, $0 \leqslant p \leqslant 1$, appartiene a $\mathscr{C}$.

Nel caso in cui nella decomposizione di S valga che $p = 0, p = 1$ o $S_1 = S_2 = S$, cioè S non è scrivibile come combinazione convessa di altri stati, i.e., S è punto estremo dell'insieme, chiameremo S stato puro; in caso alternativo parleremo di stato misto.

1.3. Subordinazione e compatibilità

Per introdurre il terzo assioma, legato all'insieme delle misurazioni, diamo prima la definizione di misurazione subordinata.

Definizione 1. Siano date due misurazioni $M_1, M_2 \in \mathscr{M}$, riferite ai rispettivi spazi misurabili $(X_1, \mathscr{F}(X_1))$ e $(X_2, \mathscr{F}(X_2))$. Se esiste una funzione $f : X_1 \to X_2$ misurabile tale per cui

$$P_S^{M_2}(B) = P_S^{M_1}(f^{-1}(B)) \quad \forall S \in \mathscr{C},\ \forall B \in \mathscr{F}(X_2), \tag{2}$$

allora la misurazione M_2 è detta subordinata alla misurazione M_1.

La subordinazione di una misura corrisponde a una sistematica perdita di informazione dovuta al raggruppamento dei possibili esiti. Ad esempio, rispetto a un apparato capace di identificare le singole lettere dell'alfabeto, una misurazione subordinata si limiterebbe a distinguere tra due sole macro-categorie, come vocali e consonanti.

Possiamo ora introdurre il terzo assioma, che riguarda le misurazioni e le loro subordinazioni.

Assioma 3. Data una misurazione $M \in \mathscr{M}$, tutte le misurazioni subordinate a M appartengono a $\mathscr{M}$.

Grazie alla subordinazione, possiamo anche dare la definizione di compatibilità tra due misurazioni.

Definizione 2. Due misurazioni M_1 e $M_2 \in \mathscr{M}$ sono dette compatibili se esiste una misurazione $M \in \mathscr{M}$ rispetto alla quale sono entrambe subordinate.

Questa definizione è molto importante in quanto la compatibilità tra misurazioni è una delle differenze cardine tra la meccanica classica e quella quantistica.

1.4. Separabilità

Introduciamo ora un ultimo assioma, che rappresenta una richiesta di consistenza formale della nostra teoria statistica.

Assioma 4. Dati due stati $S_1, S_2 \in \mathscr{C}$, se $P^M_{S_1}(B) = P^M_{S_2}(B)\ \forall M \in \mathscr{M}$ e $\forall B \in \mathscr{F}(X)$, allora $S_1 = S_2$.
Date due misurazioni $M_1, M_2 \in \mathscr{M}$, se $P^{M_1}_S(B) = P^{M_2}_S(B)\ \forall S \in \mathscr{C}$ e $\forall B \in \mathscr{F}(X)$, allora $M_1 = M_2$.

Questo assioma ci dice che, siccome siamo interessati alla statistica, se due stati (misurazioni) restituiscono la stessa statistica, e cioè non sono distinguibili statisticamente, allora sono lo stesso stato (la stessa misurazione). Un modello statistico in qui sia valido questo assioma è detto separabile.

Se un modello statistico non soddisfa questo assioma, si possono definire delle classi di equivalenza di stati (misurazioni) tali che, dati due stati (misurazioni) che restituiscono la stessa statistica, questi appartengono alla stessa classe di equivalenza. Se ora prendiamo come spazio degli stati (delle misurazioni) l'insieme delle classi di equivalenza, l'assioma è soddisfatto e il modello è separabile.

1.5. Gli assiomi di Holevo

Per chiarezza, riscriviamo qui i quattro assiomi che abbiamo introdotto nelle sezioni precedenti.

Assioma 1. Gli stati sono elementi S di un insieme $\mathscr{C}$.
Le misurazioni sono elementi M di un insieme $\mathscr{M}$; ad ogni misurazione è associato uno spazio misurabile $(X, \mathscr{F}(X))$.
Alla coppia (S, M) associamo una distribuzione di probabilità $P^M_S \in \mathscr{D}(X)$.

Assioma 2. Alla miscela statistica $\{S_j, p_j\}_{j=1}^n$ dove $S_j \in \mathscr{C}\ \forall j, p_j \geqslant 0\ \forall j, \sum_{j=1}^n p_j = 1$, è sempre associabile uno stato $\bar{S} \in \mathscr{C}$ tale che:

$$P^M_{\bar{S}}(B) = \sum_{j=1}^n p_j P^M_{S_j}(B) \qquad \forall M \in \mathscr{M}, \forall B \in \mathscr{F}(X).$$

Assioma 3. Data una misurazione $M \in \mathscr{M}$, tutte le misurazioni subordinate a M appartengono a $\mathscr{M}$.

Assioma 4. Dati due stati $S_1, S_2 \in \mathscr{C}$, se $P^M_{S_1}(B) = P^M_{S_2}(B)\ \forall M \in \mathscr{M}$ e $\forall B \in \mathscr{F}(X)$, allora $S_1 = S_2$.
Date due misurazioni $M_1, M_2 \in \mathscr{M}$, se $P^{M_1}_S(B) = P^{M_2}_S(B)\ \forall S \in \mathscr{C}$ e $\forall B \in \mathscr{F}(X)$, allora $M_1 = M_2$.

Possiamo anche riformulare leggermente l'assioma 1, definendo prima lo spazio degli stati $\mathscr{C}$ e scegliendo come misurazioni le mappe da $\mathscr{C}$ allo spazio delle distribuzioni di probabilità.

Assioma I. Gli stati sono elementi S di un insieme $\mathscr{C}$, le misurazioni $M \in \mathscr{M}$ sono mappe dallo spazio degli stati alle distribuzioni di probabilità su uno spazio misurabile $(X, \mathscr{F}(X))$, i.e.,

$$\begin{aligned} M\colon \mathscr{C} &\to \mathscr{D}(X) \\ S &\mapsto M[S] = P_S^M. \end{aligned} \tag{3}$$

L'assioma può anche essere riformulato definendo prima lo spazio delle misurazioni e prendendo gli stati come mappe dallo spazio delle misurazioni alle distribuzioni di probabilità.

2. Teoria statistica classica

Come esempio di applicazione della formulazione assiomatica di una teoria statistica, prendiamo in esame quella che chiamiamo teoria statistica classica. Per teoria statistica classica intendiamo una teoria statistica in cui:

- dato un insieme misurabile $(\Omega, \mathscr{F}(\Omega))$, dove Ω viene anche chiamato spazio delle fasi, lo spazio degli stati è l'insieme $\mathscr{D}(\Omega)$ delle distribuzioni di probabilità sullo spazio misurabile;
- lo spazio delle misurazioni è lo spazio di tutte le mappe affini $M : \mathscr{D}(\Omega) \to \mathscr{D}(X)$, con $(X, \mathscr{F}(X))$ lo spazio misurabile associato a M.

Daremo ora una descrizione più dettagliata dei due insiemi.

2.1. Lo spazio degli stati classico

Per semplicità prenderemo lo spazio delle fasi come un insieme finito, cioè consideriamo $\Omega = \{\omega_1, \dots, \omega_n\}$. Preso un elemento $\mu \in \mathscr{D}(\Omega)$, possiamo identificarlo con un vettore $\boldsymbol{\mu}$ secondo la relazione:

$$\boldsymbol{\mu} = (\mu_1 = \mu(\omega_1), ..., \mu_n = \mu(\omega_n)). \tag{4}$$

Gli estremi dello spazio degli stati sono i vettori in cui un solo elemento vale 1 mentre tutti gli altri sono zero:

$$\boldsymbol{e_i} = (0, ..., 0, \mu_i = 1, 0, ..., 0). \tag{5}$$

Tali vettori sono a loro volta associati a una distribuzione di probabilità tramite la relazione:

$$e_i(\omega_j) = \delta_{i,j}, \tag{6}$$

dove $i, j = 1, ..., n$ e $\delta_{i,j}$ è la delta di Kronecker. Vi è quindi una corrispondenza uno a uno tra uno stato puro e_i e l'elemento ω_i con lo stesso indice.

Un generico stato può quindi essere scritto come:

$$\mu = \sum_{i=1}^{n} \mu_i e_i. \tag{7}$$

Una particolarità dello spazio degli stati classico, che costituisce anche una differenza con quello quantistico, è che lo spazio degli stati classico è un simplesso, perciò la decomposizione di un generico stato misto in termini di stati puri è univoca.

2.2. Lo spazio delle misurazioni classico

Passiamo ora allo spazio delle misurazioni classico. Per fare ciò, introduciamo le variabili aleatorie: una variabile aleatoria è una funzione misurabile

$$\begin{aligned} \chi : \Omega &\to X \\ \omega &\mapsto x = \chi(\omega). \end{aligned} \tag{8}$$

La probabilità che, preparato un generico stato μ, facendo una misurazione M si ottenga un risultato $x \in B$, $B \in \mathscr{F}(X)$, è data da:

$$P_\mu^M(B) = \mu(\chi^{-1}(B)). \tag{9}$$

Assumiamo che, oltre allo spazio delle fasi, anche l'insieme degli esiti sia finito: $X = \{x_1, ..., x_m\}$.

Come prima osservazione, notiamo che, essendo mappe affini, l'azione di M su un generico stato μ si può scrivere come:

$$M[\mu] = M\left[\sum_{i=1}^{n} \mu_i e_i\right] = \sum_{i=1}^{n} \mu_i M[e_i], \tag{10}$$

per cui è sufficiente specificare l'azione delle mappe sugli stati puri.

Possiamo ora definire quelle che chiamiamo misurazioni deterministiche nel seguente modo:

$$P_{e_i}^M(x) = e_i(\chi^{-1}(x)) = \begin{cases} 1 & \text{se } x = \chi(\omega_i) \\ 0 & \text{altrimenti} \end{cases}. \tag{11}$$

Stiamo definendo delle misurazioni che descrivono la situazione in cui, se il sistema è preparato in uno stato puro e_i, il risultato della misurazione assume un valore ben definito $\chi(\omega_i)$ con probabilità 1.

Così come per la preparazione, anche la misurazione potrebbe non essere sempre una misurazione deterministica, ma potremmo realizzare delle misurazioni deterministiche M_k ognuna con frequenza p_k. Possiamo descrivere questa situazione con una misurazione $M = \sum_k p_k M_k$, che è ancora una mappa affine. Alle misurazioni che sono scrivibili come combinazione convessa di misurazioni deterministiche diamo il nome di misurazioni *fuzzy*.

L'insieme delle misurazioni deterministiche e delle misurazioni *fuzzy* rappresenta tutte le possibili misurazioni definibili in una teoria statistica classica; l'insieme delle misurazioni è quindi un insieme convesso i cui punti estremi sono le misurazioni deterministiche.

2.3. Compatibilità tra misurazioni

Come già accennato, preso un generico stato $\mu \in \mathscr{D}(X)$ la probabilità che una misurazione $M \in \mathscr{M}$ restituisca un risultato in $B \in \mathscr{F}(X)$ è data dalla Eq. (9). Nulla ci vieta di prendere una misurazione che abbia come spazio degli esiti proprio lo spazio delle fasi, cioè $X = \Omega$, e come variabile aleatoria l'identità, cosicché:

$$P_\mu^M(B) = \mu(B). \tag{12}$$

Possiamo chiamare questa misurazione come misurazione dello stato.

Confrontando Eq. (9) e Eq. (12) con la definizione di subordinazione che abbiamo dato in Eq. (2), si vede che la generica misurazione è subordinata alla misurazione dello stato. Ma, siccome tutte le misurazioni sono subordinate alla misurazione dello stato, allora in un modello classico le misurazioni sono tutte compatibili tra di loro.

Come esempio, prendiamo due misurazioni M_1 e M_2, con i rispettivi insiemi degli esiti X_1 e X_2 e variabili aleatorie χ_1 e χ_2. Sappiamo che, facendo parte di un modello statistico classico, tali misurazioni sono compatibili tra di loro. Possiamo dunque definire una misurazione congiunta M^c, definita su $X_1 \times X_2$ per cui valga:

$$P_\mu^{M^c}(B_1 \times B_2) = \mu\left(\chi_1^{-1}(B_1) \cap \chi_2^{-1}(B_2)\right), \tag{13}$$

da cui si possono ottenere le distribuzioni delle singole misurazioni tramite marginalizzazione:

$$\begin{aligned} P_\mu^{M^c}(B_1 \times X_2) &= \mu(\chi_1^{-1}(B_1) \cap \chi_2^{-1}(X_2)) = \mu(\chi_1^{-1}(B_1)) = P_\mu^{M_1}(B_1), \\ P_\mu^{M^c}(X_1 \times B_2) &= \mu(\chi_1^{-1}(X_1) \cap \chi_2^{-1}(B_2)) = \mu(\chi_2^{-1}(B_2)) = P_\mu^{M_2}(B_2). \end{aligned} \tag{14}$$

Ciò è sempre possibile dato un modello classico. Perciò, dato una collezione di misurazioni, è sempre possibile definire una misurazione congiunta, che al più corrisponde alla misurazione dello stato, da cui ottenere tutte le altre misurazioni tramite subordinazione.

É vero anche il viceversa, e ciò è possibile per il teorema di estensione di Kolmogorov, che enunciamo nel seguente modo.

Teorema 3 (Kolmogorov). *Sia μ_n una distribuzione di probabilità sullo spazio misurabile $(\mathbb{R}^n, \mathfrak{B}(\mathbb{R}^n))$, dove $\mathfrak{B}(\mathbb{R}^n)$ indica la σ–algebra di Borel.*
Se esiste una distribuzione di probabilità μ_{n+k} su $(\mathbb{R}^{n+k}, \mathfrak{B}(\mathbb{R}^{n+k}))$ tale per cui

$$\mu_{n+k}(X \times \mathbb{R}^k) = \mu_n(X) \qquad \forall k \in \mathbb{N}, \forall X \in \mathscr{F}(X), \tag{15}$$

allora esiste un'unica distribuzione μ_∞ su $(\mathbb{R}^\infty, \mathfrak{B}(\mathbb{R}^\infty))$ tale per cui

$$\mu_\infty(X \times \mathbb{R} \times \mathbb{R} \times \dots) = \mu_n(X) \qquad \forall X \in \mathscr{F}(X). \tag{16}$$

Dunque, partendo da una collezione di distribuzioni di probabilità che soddisfano le condizioni di consistenza di Kolmogorov in Eq. (15), si può sempre costruire un modello classico in cui la misurazione dello stato corrisponde alla misurazione massimale, da cui tutte le altre misurazioni possono essere ottenute tramite marginalizzazione.

3. Formulazione Standard della Meccanica Quantistica

Prima di presentare la teoria statistica della Meccanica Quantistica (MQ) vale forse la pena ricordare quali sono i postulati della sua formulazione standard alla Dirac-Von Neumann.

- *Postulato 1: gli stati.* Lo stato di un sistema quantistico è associato ad un (raggio) vettore in uno spazio in cui vale il principio di sovrapposizione ed è definito un prodotto scalare con le consuete proprietà (hermitianità, positività, linearità) ovvero uno spazio di Hilbert $\mathscr{H}$. Un tale stato si indica con $|\psi\rangle$ e viene comunemente

chiamato "*ket*" mentre il suo aggiunto, detto "*bra*", si indica con $\langle\psi|$ in modo tale che il prodotto scalare tra due stati $|\psi\rangle$ e $|\phi\rangle$ ("*braket*") sia $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$. Inoltre, i vettori di stato sono scelti normalizzati, in modo tale che $\langle\psi|\psi\rangle = 1$.

- *Postulato 2: le osservabili.* Risultati possibili di misure sul sistema sono associati a stati esclusivi ed esaustivi che costituiscono una base ortonormale. Questo postulato viene a volte formulato, equivalentemente, dicendo che ad ogni osservabile è associato un operatore hermitiano $\hat{A}$ la cui decomposizione spettrale è data in termini di proiettori ortogonali $\hat{P}_i$ secondo $\hat{A} = \sum_i a_i \hat{P}_i$.
- *Postulato 3: regola di Born e collasso.* La misura di un sistema che si trova in uno stato $|\psi\rangle$ restituisce uno degli autovalori a_i associati all'osservabile, con probabilità data dalla regola di Born $p_i = \langle\psi|\hat{P}_i|\psi\rangle \overset{\star}{=} \mathrm{Tr}\left(|\psi\rangle\langle\psi|\hat{P}_i\right)$. Dopo la misura il sistema si trova ("collassa") nello stato $\frac{\hat{P}_i|\psi\rangle}{\sqrt{p_i}}$ corrispondente al valore misurato.
- *Postulato 4: evoluzione unitaria.* Esiste un operatore hermitiano $\hat{H}(t)$ che genera l'evoluzione temporale dei sistemi quantistici, cioè tale per cui l'operatore di evoluzione temporale infinitesima ha la forma $S(t+\epsilon, t) = \mathbb{I} - \frac{i\epsilon}{\hbar}\hat{H}(t)$.

Questi postulati sono sufficienti per una formulazione completa della fisica quantistica, tuttavia hanno delle criticità. Ci limitiamo qui a mettere in evidenza alcuni aspetti che riteniamo rilevanti.

Innanzitutto notiamo subito che il primo postulato non contempla la possibilità di una miscela statistica, la cui necessità è stata già ampiamente discussa nella descrizione dell'Assioma 2 di Holevo. Infatti, se prendiamo la miscela statistica $\{\lambda_j, |\psi_j\rangle\}_{j=1}^n$ (con la condizione $\sum_j \lambda_j = 1$) ci aspettiamo che per una misura dell'osservabile $\hat{A} = \sum_i a_i \hat{P}_i$ la probabilità di ottenere come risultato l'autovalore a_i associato a $\hat{P}_i$ sia data dalla somma delle probabilità ottenute con la regola di Born pesate dai λ_j della distribuzione statistica, ovvero

$$p_i = \sum_{j=1}^n \lambda_j \langle\psi_j|\hat{P}_i|\psi_j\rangle = \sum_{j=1}^n \lambda_j \,\mathrm{Tr}\left(|\psi_j\rangle\langle\psi_j|\hat{P}_i\right) \tag{17}$$

$$= \mathrm{Tr}\left\{\left(\sum_{j=1}^n \lambda_j |\psi_j\rangle\langle\psi_j|\right)\hat{P}_i\right\} = \mathrm{Tr}\left(\rho\hat{P}_i\right), \tag{18}$$

dove abbiamo definito l'operatore statistico (a volte detto "matrice densità" dal momento che il prodotto esterno ket–bra restituisce di fatto una matrice)

$$\rho \equiv \sum_{j=1}^n \lambda_j |\psi_j\rangle\langle\psi_j|, \tag{19}$$

piccolo spoiler di quello che vedremo in seguito quando parleremo di spazio degli stati. Se ci fossimo affidati alla linearità dello spazio di Hilbert $\mathscr{H}$ e avessimo definito

⋆ Ricordiamo che $\mathrm{Tr}\,\hat{O} = \sum_n \langle\varphi_n|\hat{O}|\varphi_n\rangle$ dove $\{\varphi_n\}$ è un sistema ortonormale completo di $\mathscr{H}$.

$|\phi\rangle \equiv \sum_j \lambda_j |\psi_j\rangle$, la regola di Born non avrebbe restituito la p_i di cui sopra, com'è facile dimostrare calcolando $\mathrm{Tr}\left(|\phi\rangle\langle\phi|\hat{P}_i\right)$.

Inoltre, è evidente che questi postulati descrivono solo sistemi chiusi: lo stato $|\psi\rangle$ racchiude in sé tutte le informazioni sul sistema e la sua evoluzione, essendo unitaria, ne preserva la norma e le probabilità dei risultati di misura calcolate con la regola di Born. Per questo motivo già solo fare una misura risulta abbastanza controverso, dal momento che si tratta di accoppiare il sistema con i gradi di libertà (esterni) di un apparato. Quello che succede dopo la misura, noto come "problema del collasso", è per forza di cose qualcosa di poco chiaro e in effetti è necessario postularlo. Con il linguaggio della teoria statistica, la misura viene descritta come un'operazione di *selezione* degli stati determinata dai risultati della misura: si tratta quindi di probabilità condizionate e stati a posteriori ed è possibile presentare una trattazione del collasso meno oscura.

Sempre nell'ottica dei sistemi quantistici aperti, il fatto che l'evoluzione sia unitaria non permette di descrivere fenomeni di dissipazione o decoerenza.

Infine, che significato ha la regola di Born? Perché è così fondamentale da dover essere postulata? Si potrebbe forse fare una scelta diversa?

Purtroppo non sarà possibile rispondere a tutte queste provocazioni in questo contesto ma crediamo sia interessante accorgersi della duplice valenza della formulazione standard della MQ: da un lato questi postulati, "regole del gioco" relativamente semplici, hanno permesso per decenni di raggiungere risultati straordinari e rivoluzionari della fisica, dall'altro (come ci ricordano la teoria dei sistemi quantistici aperti e la teoria quantistica dell'informazione) è importante anche dedicare la giusta attenzione ai fondamenti e alla struttura profonda di una teoria così controintuitiva, ma potente, come la MQ.

4. Teoria Statistica Quantistica

A questo punto, vediamo in che modo si esplicitano gli assiomi di Holevo nel caso quantistico.

4.1. Spazio degli Stati

Lo spazio degli stati è inteso come rappresentazione matematica della classe di equivalenza delle procedure di preparazione ed è definito dall'insieme degli operatori statistici:

$$\mathscr{S}(\mathscr{H}) = \{\rho \in \mathscr{T}(\mathscr{H}) : \rho \geq 0, \rho = \rho^\dagger, \mathrm{Tr}(\rho) = 1\}, \tag{20}$$

dove $\mathscr{T}(\mathscr{H})$ è lo spazio degli operatori di classe traccia ovvero

$$\mathscr{T}(\mathscr{H}) = \{\hat{T} \in \mathscr{B}(\mathscr{H}) : \mathrm{Tr}|\hat{T}| < \infty\}, \tag{21}$$

dove $\mathscr{B}(\mathscr{H})$ è lo spazio degli operatori limitati su $\mathscr{H}$ e $|\hat{T}| = \sqrt{\hat{T}^\dagger \hat{T}}$. Si può dimostrare che $\mathrm{Tr}|\hat{T}|$ è una norma rispetto alla quale $\mathscr{T}(\mathscr{H})$ è spazio di Banach. L'aspetto veramente interessante, però, è che si può dimostrare la seguente catena di inclusioni

$$\mathscr{T}(\mathscr{H}) \subseteq \mathscr{C}(\mathscr{H}) \subseteq \mathscr{B}(\mathscr{H}) \tag{22}$$

dove $\mathscr{C}(\mathscr{H})$ è lo spazio degli operatori compatti (chiusura dell'insieme degli operatori degeneri ovvero degli operatori che possono essere scritti come $\hat{A} = \sum_i |u_i\rangle \langle v_i|$, $\{u_i\}$ e $\{v_i\}$ famiglie di vettori linearmente indipendenti). Questo ci è utile in luce del fatto che

Teorema 4. *Sia $\hat{O} \in \mathscr{B}(\mathscr{H})$ autoaggiunto e compatto. Allora esiste un sistema ortonormale e completo $\{\varphi_n\}$ di autovettori di $\hat{O}$ con corrispondenti autovalori $\{o_n\}$, $o_n \in \mathbb{R}$ tale che $\hat{O}$ ammette rappresentazione spettrale*

$$\hat{O} = \sum_n o_n \left|\varphi_n\right\rangle \left\langle\varphi_n\right|, \tag{23}$$

e si verifica che $\lim_{n\to\infty} o_n = 0$. Se, in particolare, $\hat{O} \in \mathscr{T}(\mathscr{H})$ allora

$$\mathrm{Tr}\,|\hat{O}| = \mathrm{Tr}\left(\sqrt{\hat{O}^\dagger \hat{O}}\right) = \sum_n |o_n|. \tag{24}$$

Insomma, considerare come traccia la somma dei moduli degli autovalori ha senso anche nel caso ∞–dimensionale a patto che $\hat{O}$ sia compatto e autoaggiunto (cosa che si verifica nel caso di $\rho \in \mathscr{S}(\mathscr{H})$ dal momento che $\rho = \rho^\dagger$ e $\rho \in \mathscr{T}(\mathscr{H}) \subseteq \mathscr{C}(\mathscr{H})$).

Le richieste $\rho \geq 0, \mathrm{Tr}(\rho) = 1$ sono giustificate dal fatto che richiediamo che le probabilità siano positive e sommino a 1, come forse si può meglio intuire dalla riflessione che ha portato all'Eq. (19). $\rho = \rho^\dagger$, invece, corrisponde a richiedere che i risultati di una misura siano numeri reali, come in effetti ci aspettiamo accada in laboratorio.

L'insieme $\mathscr{S}(\mathscr{H})$ ha la proprietà di essere convesso, ovvero, dati due operatori statistici, una loro combinazione lineare convessa appartiene ancora all'insieme:

$$\rho_1, \rho_2 \in \mathscr{S}(\mathscr{H}) \implies \lambda\rho_1 + (1-\lambda)\rho_2 \in \mathscr{S}(\mathscr{H}) \quad \text{con } 0 \leq \lambda \leq 1. \tag{25}$$

Gli estremi di questo spazio convesso sono i proiettori di rango 1 che possono essere individuati tramite la purezza. La purezza di uno stato quantistico è definita come:

$$\mathscr{P}(\rho) = \mathrm{Tr}(\rho^2). \tag{26}$$

La purezza è convessa ($\mathscr{P}(\lambda\rho_1 + (1-\lambda)\rho_2) = \lambda\mathscr{P}(\rho_1) + (1-\lambda)\mathscr{P}(\rho_2)$, $0 \leqslant \lambda \leqslant 1$), invariante per trasformazioni unitarie ed è limitata ($0 < \mathscr{P}(\rho) \leq 1$). In particolare $\mathscr{P}(\rho) = 1$ iff $\rho = |\psi\rangle\langle\psi|$, ed è proprio questo il motivo per cui diciamo che la purezza è in grado di individuare gli estremi.

Similmente uno stato puro può essere individuato dall'entropia di Von Neumann:

$$S(\rho) = -\,\mathrm{Tr}(\rho \log \rho). \tag{27}$$

L'entropia di Von Neumann è concava ($S(\lambda\rho_1 + (1-\lambda)\rho_2) \geq \lambda S(\rho_1) + (1-\lambda)S(\rho_2)$, $0 \leqslant \lambda \leqslant 1$), è invariante per trasformazioni unitarie e anch'essa ordina rispetto agli estremi. In particolare $S(\rho) = 0$ iff $\rho = |\psi\rangle\langle\psi|$ ovvero ρ puro. Infine, per uno

stato massimamente misto in uno spazio di dimensione N, l'entropia è massima: $S(\rho) = \log N$.

4.2. Effetti

Gli effetti sono intesi come rappresentazione matematica della classe di equivalenza delle procedure di registrazione dei risultati di una misura. Chiamiamo questi oggetti "effetti" perché in un certo senso rappresentano l'effetto dell'apparato sullo stato. Consideriamo per il momento la misura corrispondente all'evento più semplice possibile ovvero l'apparato risponde sì–no a domande precise, del tipo: la misura di una certa quantità restituisce *quel* valore? Identifichiamo un evento così semplice con una mappa che associa ad ogni risultato la probabilità di avere risposta positiva a tale domanda.

$$\begin{aligned} E\colon \mathscr{S}(\mathscr{H}) &\to [0,1] \\ \rho &\mapsto E[\rho] \end{aligned} \tag{28}$$

Siccome lo spazio degli stati è convesso allora richiediamo che la mappa E sia affine:

$$E(\lambda\rho_1 + (1-\lambda)\rho_2) = \lambda E(\rho_1) + (1-\lambda)E(\rho_2). \tag{29}$$

Siccome si può dimostrare che $\mathscr{B}(\mathscr{H}) = \mathscr{T}'(\mathscr{H})$ (tramite la traccia), i.e., lo spazio degli operatori limitati coincide con il duale degli operatori di classe traccia, allora identifichiamo lo spazio degli effetti come

$$\mathscr{E}(\mathscr{H}) = \{\hat{E} \in \mathscr{B}(\mathscr{H}) : 0 \leqslant \hat{E} \leqslant \mathbb{I}\}. \tag{30}$$

La richiesta $0 \leqslant \hat{E} \leqslant \mathbb{I}$ si giustifica con la regola di Born: ci aspettiamo, infatti, che $0 \leqslant \mathrm{Tr}\{\rho\hat{E}\} \leqslant 1$. Lo spazio degli effetti è convesso e inoltre, indicando con $\mathscr{P}(\mathscr{H})$ lo spazio dei proiettori, vale che $\mathscr{P}(\mathscr{H}) \subseteq \mathscr{E}(\mathscr{H}) \subseteq \mathscr{B}(\mathscr{H})$. In particolare, i proiettori ortogonali sono gli estremi di $\mathscr{E}(\mathscr{H})$. In effetti, l'idempotenza implica che gli autovalori di un proiettore siano $0, 1$ che corrisponde al verificarsi o meno di un evento elementare.

4.3. La Regola di Born

Un risultato molto importante in questa formulazione della MQ è che la regola di Born non è più postulata ma è una conseguenza della relazione di dualità che, come dicevamo, è mediata dalla traccia. Enunciamo, quindi, il seguente

Teorema 5 (Regola di Born). *Data una mappa affine*

$$\begin{aligned} E\colon \mathscr{S}(\mathscr{H}) &\to [0,1] \\ \rho &\mapsto E[\rho] \end{aligned} \tag{31}$$

esiste un operatore $\hat{E}$ limitato e autoaggiunto tale che vale la rappresentazione

$$E[\rho] = \mathrm{Tr}\,(\rho\hat{E}), \quad 0 \leqslant \hat{E} \leqslant \mathbb{I}. \tag{32}$$

4.4. Il Teorema di Gleason

Gli effetti sono l'insieme di osservabili più generale. Ora proviamo a fare il procedimento inverso cioè partiamo dall'insieme degli effetti e cerchiamo di capire che risultati si possono ricavare sullo spazio degli stati. Per fare ciò passiamo attraverso il concetto di misura di probabilità generalizzata ovvero una mappa

$$\begin{aligned} \nu\colon \mathscr{E}(\mathscr{H}) &\to [0,1] \\ \hat{E} &\mapsto \nu[\hat{E}] \end{aligned} \tag{33}$$

tale che

(1) $0 \leqslant \nu(\hat{E}) \leqslant 1$;
(2) $\nu(\mathbb{I}) = 1$;
(3) $\nu(\sum_{i=1}^n \hat{E}_i) = \sum_{i=1}^n \nu(\hat{E}_i)$, $\sum_{i=1}^n \hat{E}_i \leqslant \mathbb{I}$.

Un risultato importante è che una misura di probabilità generalizzata può essere identificata (sempre grazie alle relazioni di dualità) con un operatore statistico. Si tratta del

Teorema 6 (Busch). *Sia ν una misura di probabilità generalizzata sullo spazio degli effetti $\mathscr{E}(\mathscr{H})$. Allora esiste un operatore statistico $\rho \in \mathscr{S}(\mathscr{H})$ tale che*

$$\nu(\hat{E}) = \mathrm{Tr}\,(\rho\hat{E}) \quad \forall \hat{E} \in \mathscr{E}(\mathscr{H}), \tag{34}$$

con ρ univocamente identificato.

Restringendo l'insieme degli effetti ai proiettori ortogonali, come accade nel caso della formulazione standard della MQ, lo spazio degli stati che troviamo è più generale? La risposta è, ovviamente, negativa ed è quello che è contenuto nel

Teorema 7 (Gleason). *Sia $\mu : \mathscr{P}(\mathscr{H}) \to [0,1]$ una misura di probabilità generalizzata sull'insieme dei proiettori $\mathscr{P}(\mathscr{H})$. Se* $\dim \mathscr{H} \geqslant 3$, *allora esiste un unico operatore statistico $\rho \in \mathscr{S}(\mathscr{H})$ tale che:*

$$\mu(\hat{P}) = \mathrm{Tr}\Big(\rho\hat{P}\Big) \quad \forall \hat{P} \in \mathscr{P}(\mathscr{H}). \tag{35}$$

Vale la pena evidenziare che μ su $\mathscr{P}(\mathscr{H})$ soddisfa le stesse proprietà che soddisfano le misure di probabilità generalizzate su $\mathscr{E}(\mathscr{H})$, a patto di modificare leggermente il punto 3 scrivendo che $\mu\left(\sum_{i=1}^n \hat{P}_i\right) = \sum_{i=1}^n \mu(\hat{P}_i)$ vale per ogni famiglia di proiettori ortogonali, i.e., $\hat{P}_i\hat{P}_j = 0\ \forall i \neq j$, cosicché abbiamo la garanzia che $\sum_{i=1}^n \hat{P}_i$ sia ancora un proiettore.

Questo teorema è importante perché si può inquadrare in un approccio alla teoria statistica quantistica basato sull'assioma di Holevo 1 (invece che sull'Assioma I) cioè delinea un contesto in cui si definiscono prima gli oggetti matematici associati alle misurazioni. Dopodiché, se valgono le ipotesi del teorema (se ci limitiamo a $\mathscr{P}(\mathscr{H})$ bisogna fare riferimento al Teorema di Gleason (7)), allora lo spazio degli stati risulta essere proprio $\mathscr{S}(\mathscr{H})$ e le probabilità sono date dalla legge di Born.

In questo senso, allora, possiamo dire che il Teorema di Gleason (7) (o più in generale il Teorema di Busch (6)) mostra l'equivalenza tra definire prima lo spazio degli stati e poi quello delle misurazioni (tutte le mappe affini sullo spazio degli stati)

e l'approccio in cui si definisce prima lo spazio delle misurazioni e si inferiscono gli stati a partire dalle richieste che costituiscono le ipotesi del teorema.

A livello classico questo secondo approccio è quello descritto dal Teorema di estensione di Kolmogorov (3): definendo le misurazioni tramite le corrispondenti distribuzioni di probabilità, se queste soddisfano le condizioni di consistenza in Eq. (15), allora lo spazio degli stati è costituito dallo spazio delle distribuzioni di probabilità $\mathscr{D}(X)$ e vale che $P_\mu^M(B) = \mu(\chi^{-1}(B))$.

4.5. POVM

Concludiamo ora la nostra trattazione con un ultimo step di complessità. Vogliamo ora costruire la più generale nozione di osservabile con un arbitrario spazio misurabile $(\Omega, \mathscr{F}(\Omega))$ dove $\mathscr{F}(\Omega)$ è la σ–algebra sullo spazio campionario Ω. Definiamo come POVM ("positive operator-value measure") la mappa

$$\begin{aligned} F\colon \mathscr{F}(\Omega) &\to \mathscr{E}(\mathscr{H}) \\ M &\mapsto F[M] \end{aligned} \tag{36}$$

tale che

(1) $0 \leqslant F(M) \leqslant \mathbb{I} \quad \forall M \in \mathscr{F}(\Omega)$;
(2) $F(\varnothing) = 0, \quad F(\Omega) = \mathbb{I}$;
(3) $F(\bigcup_i M_i) = \sum_i F(M_i)$ convergenza in senso debole $\forall M_i \cap M_j = \varnothing$, $i \neq j$.

Data una POVM possiamo ricostruire la distribuzione di probabilità sugli esiti come

$$\mu_\rho^F(M) = \mathrm{Tr}\big(\rho F(M)\big), \tag{37}$$

che rappresenta la probabilità che una misura per l'osservabile F dello stato ρ restituisca un risultato nell'intervallo M. La mappa $F(\cdot)$ rimane una POVM fintantoché $\mathrm{Tr}\big(\rho F(M)\big)$ è una misura di probabilità sullo spazio misurabile $(\Omega, \mathscr{F}(\Omega))$.

Siamo certi di aver finalmente raggiunto la descrizione più generale e che ogni osservabile compatibile con l'interpretazione statistica della MQ possa essere identificata con una POVM grazie al seguente

Teorema 8. *Data una POVM $F(\cdot)$ sullo spazio misurabile $(\Omega, \mathscr{F}(\Omega))$, la mappa*

$$\begin{aligned} \Phi_F\colon \mathscr{S}(\mathscr{H}) &\to \mathscr{D}(\Omega) \\ \rho &\mapsto \Phi_F[\rho] = \mathrm{Tr}\big(\rho F(\cdot)\big) \end{aligned} \tag{38}$$

è una mappa affine dall'insieme convesso degli stati quantistici all'insieme convesso delle distribuzioni di probabilità su $(\Omega, \mathscr{F}(\Omega))$. Viceversa, ogni mappa affine può essere realizzata come Φ_F per una qualche POVM $F(\cdot)$.

Bibliografia

- B. Vacchini, *Open Quantum Systems: Foundations and Theory*, Graduate Texts in Physics, Springer Cham, 2024. DOI: 10.1007/978-3-031-58218-9.

- A. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, Publications of the Scuola Normale Superiore, Edizioni della Normale Pisa, DOI: 10.1007/978-88-7642-378-9

GEOMETRIA DELLE TEORIE DI GAUGE

MATTIA BELLONI, CARLO VITTOLI

1. Fibrati

1.1. Fibrati generali

Definizione 0.1. Siano E, M, F varietà lisce e sia $\pi : E \to M$ una mappa liscia suriettiva. Allora (E, F, M) è un fibrato se per ogni $x \in M$ esiste un aperto $U \subseteq M$ tale che esista un diffeomorfismo

$$\phi_U : E_U = \pi^{-1}(U) \to U \times F \tag{1}$$

per cui

$$\mathrm{pr}_1 \circ \phi = \pi. \tag{2}$$

In tal caso chiamiamo:

- E spazio totale,
- M base,
- F fibra,
- π proiezione,
- (U, ϕ_U) trivializzazione locale.

Definizione 0.2. Siano (E, F, M) e (E', F', M) fibrati su M. Un **morfismo di fibrati** è una mappa liscia $H : E \to E'$ tale che

$$\pi' \circ H = \pi. \tag{3}$$

Se H è un diffeomorfismo, allora è un **isomorfismo di fibrati**.

Esempio 0.3. Siano M e F varietà arbitrarie e si definisca $E = M \times F$. Allora la proiezione pr_1 definisce un fibrato $(M \times F, F, M)$, detto **fibrato banale** su M.

Definizione 0.4. Un fibrato isomorfo al fibrato banale è anch'esso detto **fibrato banale**.

Osservazione 0.5. Per definizione, ogni fibrato è localmente isomorfo al fibrato banale, ma non globalmente.

Esiste un criterio per stabilire quando un fibrato è banale.

Proposizione 0.1. *Sia (E, F, M) un fibrato. Esso è banale se e solo se esiste una mappa liscia $\tau : E \to F$ tale che*

$$\tau|_{E_x} : E_x \to F \tag{4}$$

sia un diffeomorfismo per ogni $x \in M$.

1.2. Fibrati principali

Definizione 0.6. Un fibrato (P, G, M), dove G è un gruppo di Lie, è detto **G-fibrato principale** se:

(1) l'azione del gruppo preserva le fibre ed è semplicemente transitiva su di esse: l'azione si restringe a $P_x \times G \to P_x$ e la mappa $G \to P_x,\ g \mapsto pg$ è biiettiva per ogni $x \in M$ e per ogni $p \in P_x$;
(2) esiste un atlante di trivializzazioni G-equivarianti $\phi_i : P_{U_i} \to U_i \times G$, cioè tali che $\phi_i(pg) = \phi_i(p)g$, dove l'azione di destra sul prodotto diretto è quella banale sulla prima componente.

1.3. Fibrati vettoriali

Definizione 0.7. Un fibrato (E, V, M) è detto **fibrato vettoriale** di rango m se:

(1) la fibra tipica V è uno spazio vettoriale di dimensione m;
(2) esiste un atlante di trivializzazioni $\{U_i, \phi_i\}$ per E tale che le mappe indotte $\phi_{ix} : E_x \to V$ siano isomorfismi vettoriali per ogni $x \in U_i$.

Definizione 0.8. Se (P, G, M) è un G-fibrato principale, V è uno spazio vettoriale e $\rho : G \to \mathrm{Aut}(V)$ è una rappresentazione di G, allora

$$E = P \times_\rho V = (P \times V)/G \tag{5}$$

è il **fibrato vettoriale associato** al fibrato principale P e alla rappresentazione ρ su V.

2. Connessioni e Curvatura

Definizione 0.9. Una **1-forma di connessione** su un G-fibrato principale (P, G, M) è una 1-forma twistata $A \in \Omega^1(P, \mathfrak{g})$ tale che:

- $r_g^* A = \mathrm{Ad}_{g^{-1}} \circ A$;
- $A(\tilde{X}) = X$ per ogni $X \in \mathfrak{g}$, dove $\tilde{X}$ è il corrispondente campo vettoriale fondamentale.

Questa è anche chiamata **campo di gauge** su P.

2.1. Espressioni locali della connessione e della curvatura

Per le applicazioni fisiche è utile scrivere la connessione e la curvatura in coordinate locali. Sia $\{U\}$ un aperto di trivializzazione con una sezione locale $s : U \to P$. Allora la 1-forma di connessione $A \in \Omega^1(P, \mathfrak{g})$ si rappresenta come una 1-forma a valori nell'algebra di Lie su U:

$$A^U = s^* A \ \in\ \Omega^1(U, \mathfrak{g}).$$

In coordinate locali x^μ su U, possiamo scrivere

$$A^U = A_\mu(x)\, \mathrm{d}x^\mu, \qquad A_\mu \in \mathfrak{g}. \tag{6}$$

Le funzioni A_μ sono dette **potenziali di gauge** (o componenti della connessione).

La corrispondente **curvatura** (o campo di gauge) $F \in \Omega^2(P, \mathfrak{g})$ si pull-back a

$$F^U = s^* F \ \in \ \Omega^2(U, \mathfrak{g}),$$

e in coordinate si scrive

$$F^U = \frac{1}{2} F_{\mu\nu} \, \mathrm{d}x^\mu \wedge \mathrm{d}x^\nu, \tag{7}$$

con

$$F_{\mu\nu} = \partial_\mu A_\nu - \partial_\nu A_\mu + [A_\mu, A_\nu]. \tag{8}$$

2.2. Trasformazioni di gauge locali

Sia $u : U \to G$ una trasformazione di gauge locale (cioè una mappa liscia che definisce un automorfismo sulla trivializzazione). Il potenziale di gauge si trasforma come

$$A'_\mu = u^{-1} A_\mu \, u + u^{-1} \, \partial_\mu u, \tag{9}$$

che è la versione in coordinate della formula generale $A' = u^{-1} A \, u + u^{-1} \mathrm{d}u$.

Per la curvatura, invece, si ha la trasformazione covariante

$$F'_{\mu\nu} = u^{-1} F_{\mu\nu} \, u, \tag{10}$$

o, equivalentemente, $F' = u^{-1} F \, u$. Questa proprietà è fondamentale perché garantisce che l'azione di Yang–Mills sia invariante di gauge.

Osservazione 0.10. La legge di trasformazione per la connessione (9) non è omogenea a causa del termine $u^{-1}\partial_\mu u$; ciò riflette il fatto che la connessione non è un tensore. Al contrario, la curvatura trasforma in modo omogeneo, il che la rende una quantità fisica (osservabile) a livello classico.

3. Descrizione Locale, Trasformazioni di Gauge e Azione di Yang–Mills

3.1. 1-forme di connessione locali

Sia $s : U \to P$ una sezione locale del G-fibrato principale (P, G, M). La **1-forma di connessione locale** (o potenziale di gauge) è il pull-back della connessione $A \in \Omega^1(P, \mathfrak{g})$ mediante s:

$$A^U \ := \ s^* A \ \in \ \Omega^1(U, \mathfrak{g}). \tag{11}$$

Quando non c'è rischio di confusione scriviamo semplicemente A per la forma locale.

Se s_i, s_j sono due sezioni locali con funzione di transizione $g_{ij} : U_i \cap U_j \to G$ definita da $s_j(x) = s_i(x) g_{ij}(x)$, le corrispondenti forme di connessione locali soddisfano

$$A_j \ = \ g_{ij}^{-1} A_i \, g_{ij} + g_{ij}^{-1} \, \mathrm{d}g_{ij}. \tag{12}$$

3.2. Trasformazioni di gauge

Definizione 0.11. Una **trasformazione di gauge** è un automorfismo di fibrati $\Phi : P \to P$ che copre l'identità su M, cioè $\pi \circ \Phi = \pi$ e $\Phi(pg) = \Phi(p)g$.

Su una sezione locale s, una trasformazione di gauge è descritta da una mappa liscia $u : U \to G$ mediante $\Phi(s(x)) = s(x)u(x)$. L'azione sul potenziale di gauge locale è

$$A' \;=\; u^{-1}A\,u + u^{-1}\mathrm{d}u. \tag{13}$$

L'insieme di tutte le trasformazioni di gauge forma il **gruppo di gauge** $\mathscr{G}(P)$.

3.3. Il gruppo di gauge come spazio di mappe

Proposizione 0.2. *Per un G-fibrato principale (P, G, M), il gruppo di gauge $\mathscr{G}(P)$ è canonicamente isomorfo allo spazio delle sezioni globali del **fibrato aggiunto** $\mathrm{Ad}(P) = P \times_G G$, dove G agisce su sé stesso per coniugio. In simboli,*

$$\mathscr{G}(P) \;\cong\; \Gamma\big(M, \mathrm{Ad}(P)\big).$$

In particolare, se il fibrato è banale ($P \cong M \times G$), allora

$$\mathscr{G}(P) \;\cong\; C^\infty(M, G),$$

dove l'operazione di gruppo è la moltiplicazione puntuale.

Dimostrazione. **[Cenni all'identificazione]** Una trasformazione di gauge $\Phi : P \to P$ è G-equivariante e copre l'identità. In una trivializzazione $P \cong M \times G$, ogni tale Φ si scrive univocamente come $\Phi(x, g) = (x, u(x)g)$ per una mappa liscia $u : M \to G$. Viceversa, ogni $u : M \to G$ liscia definisce un automorfismo mediante moltiplicazione a destra per $u(x)$ sulla fibra. Nel caso generale (non banale), gli automorfismi corrispondono alle sezioni del fibrato associato $\mathrm{Ad}(P)$. □

Osservazione 0.12. Sotto questa identificazione, la legge di trasformazione di gauge locale $A' = u^{-1}A\,u + u^{-1}\mathrm{d}u$ dalla (13) è esattamente il pull-back dell'automorfismo globale Φ sulla trivializzazione locale U.

3.4. 2-forma di curvatura

Definizione 0.13. La **curvatura** di una connessione A è la 2-forma a valori in $\mathfrak{g}$ su P

$$F \;=\; \mathrm{d}A + \tfrac{1}{2}[A \wedge A] \;\in\; \Omega^2(P, \mathfrak{g}). \tag{14}$$

Il suo pull-back mediante una sezione locale dà il **tensore di campo** $F^U = s^*F$.

In coordinate locali si scrive $A = A_\mu\,\mathrm{d}x^\mu$ e

$$F_{\mu\nu} \;=\; \partial_\mu A_\nu - \partial_\nu A_\mu + [A_\mu, A_\nu]. \tag{15}$$

La curvatura trasforma in modo covariante sotto trasformazioni di gauge:

$$F \;\longmapsto\; u^{-1}F\,u. \tag{16}$$

3.5. Lagrangiana di Yang–Mills

Supponiamo che la varietà di base M sia dotata di una metrica (pseudo-) riemanniana g e che $\mathfrak{g}$ sia munito di un prodotto interno Ad-invariante $\langle \cdot, \cdot \rangle$ (per le algebre di matrici si prende solitamente $\langle X, Y \rangle = -\mathrm{Tr}(XY)$).

Definizione 0.14. La **Lagrangiana di Yang–Mills** (densità) è la 4-forma (o forma di grado massimo)

$$\mathscr{L}_{\mathrm{YM}} \;=\; \langle F \wedge \star F \rangle, \tag{17}$$

dove $\star$ è l'operatore di Hodge indotto da g. Nello spaziotempo lorentziano quadridimensionale si scrive

$$\mathscr{L}_{\mathrm{YM}} \;=\; -\frac{1}{2}\,\mathrm{Tr}\big(F_{\mu\nu}F^{\mu\nu}\big)\,\sqrt{|g|}\,\mathrm{d}^4x. \tag{18}$$

L'**azione di Yang–Mills** è l'integrale

$$S_{\mathrm{YM}}[A] \;=\; \int_M \langle F \wedge \star F \rangle. \tag{19}$$

L'invarianza di gauge segue dalla covarianza $F \mapsto u^{-1}Fu$ e dall'invarianza del prodotto interno.

Osservazione 0.15. Variando l'azione rispetto ad A si ottengono le **equazioni di Yang–Mills**

$$\mathrm{d}_A \star F = 0, \tag{20}$$

dove $\mathrm{d}_A = \mathrm{d} + [A \wedge \cdot]$ è la derivata esterna covariante. Insieme all'identità di Bianchi $\mathrm{d}_A F = 0$, esse descrivono la dinamica dei campi di gauge classici.

3.6. Fissaggio del gauge e gauge fisici

Per estrarre previsioni fisiche dall'azione classica o per effettuare la quantizzazione tramite integrale di cammino, è necessario eliminare i gradi di libertà di gauge ridondanti. Questa procedura è nota come **fissaggio del gauge**.

Definizione 0.16 (Scelta del gauge / Condizione di gauge). Una **scelta del gauge** (o **fissaggio del gauge**) è una selezione liscia di un rappresentante per ogni orbita di gauge. Equivalentemente, è la specificazione di una sezione locale $s : U \to P$ del fibrato principale. In termini del potenziale di gauge $A \in \Omega^1(U, \mathfrak{g})$, ciò equivale a imporre un vincolo funzionale

$$\mathscr{F}(A) = 0,$$

che rimuove localmente la libertà di applicare trasformazioni arbitrarie $u : U \to G$.

Osservazione 0.17 (Libertà di gauge residua). Una condizione di gauge non sempre fissa il gauge completamente. Se una trasformazione di gauge u soddisfa $\mathscr{F}(A') = \mathscr{F}(A)$ per $A' = u^{-1}Au + u^{-1}\mathrm{d}u$, essa è detta **simmetria di gauge residua**. Ad esempio, nel gauge di Lorenz $\partial_\mu A^\mu = 0$ (caso abeliano), le trasformazioni residue sono date da u tali che $\Box u = 0$. Queste simmetrie residue devono spesso essere fissate ulteriormente per ottenere un rappresentante unico.

Fuori Orario è una giornata di seminari *per studenti da studenti*, giunta quest'anno alla sua decima edizione, organizzata dai giovani del Dipartimento di Matematica dell'Università degli Studi di Milano. Nata per condividere specifici argomenti di notevole bellezza che non trovano spazio all'interno delle lezioni ordinarie, questa iniziativa permette a noi studenti di via Saldini di metterci in gioco. Siamo così stati in grado di condividere le nostre idee e confrontarci dal vivo con grande passione.

Stampato con il contributo dell'Università derivante dai fondi previsti per le attività culturali e sociali.