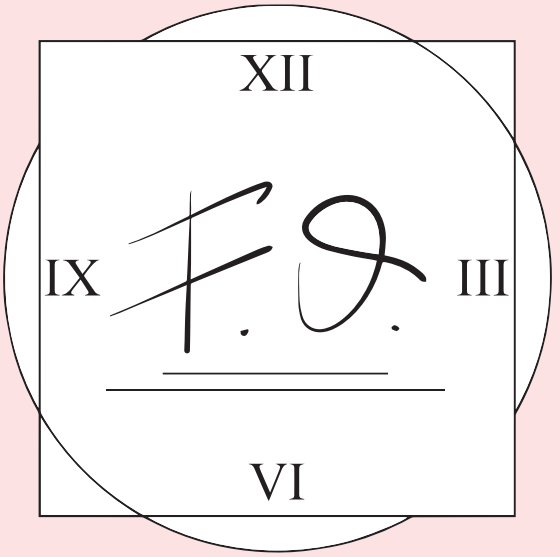
Fuori Orario

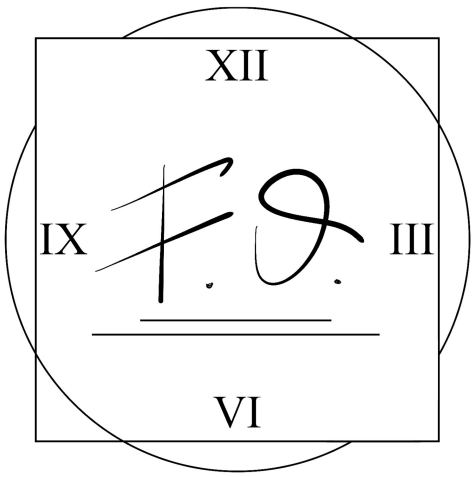
Resoconti di una giornata di seminari
15 Maggio 2021



Dipartimento di Matematica - Università degli Studi di Milano

FUORI ORARIO

Resoconti di una giornata di seminari
15 Maggio 2021



Fuori Orario
Resoconti di una giornata di seminari

15 Maggio 2021
Dipartimento di Matematica
Università degli Studi di Milano

Versione definitiva: novembre 2021
a cura di Samuele Gatti e Ivan Andreoni

INDICE

INTRODUZIONE

Caro lettore,

Il mio primo incontro con Fuori Orario è avvenuto alla fine del quinto anno di liceo, quando mi hanno regalato il libretto della terza edizione. Era stato un regalo apprezzato, l'ho sfogliato diverse volte con curiosità pur capendo solo una minima parte dei seminari raccolti, ma ad essere sincera, non ho pensato nemmeno per un attimo che potesse essere un'iniziativa a cui un giorno avrei partecipato.

Eppure, a marzo dell'anno dopo, in qualche modo, mi sono ritrovata ad organizzare la quarta edizione e poi, con non meno sorpresa, a tenere uno dei seminari di quello stesso anno. Sono state decisioni prese non so bene con quale motivazione: forse conoscere gente in un momento in cui questo era praticamente impossibile, forse andare contro la tendenza a tirarmi indietro che ogni tanto mi capita di avere. Ma sono state delle buone decisioni. Ho avuto l'occasione di mettermi in gioco, forse per la prima volta realmente, sotto diversi aspetti e alla fine mi sono rimasti l'entusiasmo che tutti ci avevamo messo e la soddisfazione per come era andata. Così mi sono sentita parte attiva di qualcosa che all'inizio sentivo lontano da me.

Naturalmente, Fuori Orario è nato ed è andato avanti indipendentemente da me e non è mia intenzione prendermi meriti o "appropriarmi" di nulla, ma è come se un pezzettino sia stato affidato a me, almeno per il momento. Questa è la sensazione che mi ha portato a dedicarmi con lo stesso entusiasmo all'organizzazione della quinta edizione: così come aveva significato tanto per me, avrebbe potuto essere un incontro importante anche per tanti altri.

Penso che da parte di tutti ci fosse la voglia di continuare a coinvolgere altre persone in quella che per noi era stata un'esperienza positiva e da qui, anche quest'anno, si è formato un nuovo team di organizzatori. È bello quando si riesce a lavorare insieme e vedi negli altri lo stesso desiderio di preparare nei dettagli un momento di condivisione e di comunità.

Certo, la speranza iniziale era quella di riuscire a riportare Fuori Orario nelle aule di via Saldini, ma purtroppo neanche quest'anno è stato possibile ritrovarsi tutti fisicamente in università e abbiamo dovuto optare per una seconda edizione "dentro casa". Dopo più di un anno di lezioni ed eventi online, credo che nessuno fosse contento di questa decisione, eppure alla fine c'è stata un'adesione ugualmente entusiasta da parte di tutti: hanno partecipato dodici speaker e, nell'arco della giornata, si sono collegati circa un centinaio di spettatori da diverse zone

dell'Italia e non solo. Ancora una volta, nonostante il forte desiderio di tornare alla normalità, questa possibilità di azzerare le distanze si è rivelata essere un aspetto positivo, che ha permesso di coinvolgere più o meno attivamente persone che altrimenti difficilmente avrebbero potuto partecipare.

Adesso penso che tu abbia voglia di dedicarti alla lettura di qualcuno dei resoconti dei seminari e io ho già raccontato parecchie cose, quindi lasciami solo aggiungere qualche parola per concludere.

Spero si sia colto da quel che ho scritto quanto credo che l'iniziativa sia, e possa continuare ad essere, significativa da diversi punti di vista e, indipendentemente dalla mia esperienza, il fatto che sia arrivata alla sua quinta edizione in questo modo ne è la prova. Sicuramente, da quando è stato organizzato per la prima volta, ci sono stati dei cambiamenti, e presumibilmente continueranno ad esserci, ma ognuno di questi è evidenza del fatto che Fuori Orario è "vivo", pronto ad adattarsi e ad evolvere. In tutto ciò, quel che rimane invariato è l'idea che sta alla base, che rende Fuori Orario quello che è: una giornata organizzata dagli studenti per altri studenti, un'occasione per scoprire che c'è di più oltre alla monotonia delle lezioni, un momento per condividere la propria passione per la matematica. Sono convinta che sia importante riuscire a trasmettere questo, cosicché coloro che si accostino all'iniziativa in ogni modo ne facciano esperienza.

Buona lettura,
Beatrice Ostorero Vinci

INSEGUIMENTI MATEMATICI: ACHILLE VS TARTARUGA, UOMO VS LEONE

FRANCESCO PAGLIARIN

1. INTRODUZIONE

Analizziamo due famosi problemi di natura molto diversa ma con un aspetto in comune. Entrambi riguardano una "sfida" di due "giocatori" in cui l'interesse dell'uno è opposto a quello dell'altro. Il primo venne partorito dalla mente del filosofo greco Zenone mentre il secondo è un modello semplificato di un classico problema introduttivo della Teoria dei giochi.

2. IL PARADOSSO DI ACHILLE E DELLA TARTARUGA

Questo problema in realtà nasce come un vero e proprio paradosso nella scuola eleatica del V secolo a.C.. L'allievo di Parmenide infatti si immagina una gara di corsa tra Achille "piè veloce" e una tartaruga, sicuramente più lenta dell'eroe omerico.

Per far sì che la gara non abbia esito banale già dall'inizio, si vuole dare un certo spazio di vantaggio x_0 alla tartaruga. Al via entrambi partono e Achille percorre in un tempo t_0 lo spazio di svantaggio x_0. Tuttavia, nel tempo t_0 la tartaruga è avanzata di uno spazio x_1 rimanendo perciò ancora in vantaggio su Achille. Ebbene, iterando questo ragionamento, Zenone afferma che Achille non riesca mai a raggiungere la tartaruga e quindi a vincere la gara; un'affermazione sicuramente sconcertante!

Vediamo come possa essere risolto il paradosso con qualche semplice strumento matematico.

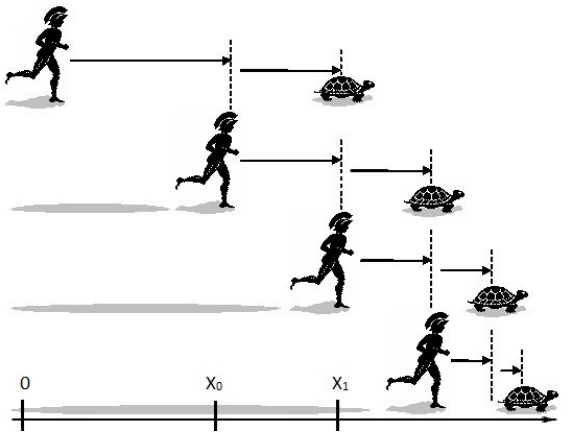
Assumiamo che entrambi si muovano di moto rettilineo uniforme con velocità v_A Achille, v_T la tartaruga e $v_A > v_T$ per quanto supposto in precedenza.
Sia P_1 Achille e P_2 la tartaruga.

Quando P_1 raggiunge x_0 al tempo t_0, P_2 è avanzato di x_1:

$$t_0 = \frac{x_0}{v_A} \quad , \quad x_1 = v_T t_0 = x_0 \frac{v_T}{v_A}$$

Quando P_1 ha percorso il tratto ulteriore x_1 nel tempo t_1, P_2 è avanzato di x_2:

$$t_1 = \frac{x_1}{v_A} = \frac{x_0}{v_A}\frac{v_T}{v_A} \quad , \quad x_2 = v_T t_1 = x_0 \left(\frac{v_T}{v_A}\right)^2$$



Induttivamente si dimostra che

$$x_n = x_0 \left(\frac{v_T}{v_A}\right)^n \quad , \quad t_n = \frac{x_0}{v_A}\left(\frac{v_T}{v_A}\right)^n$$

In conclusione, P_1 per raggiungere P_2 deve percorrere lo spazio:

$$x_{tot} = \sum_{n=0}^{+\infty} x_n = x_0 \sum_{n=0}^{+\infty} \left(\frac{v_T}{v_A}\right)^n$$

nel tempo:

$$t_{tot} = \sum_{n=0}^{+\infty} t_n = \frac{x_0}{v_A} \sum_{n=0}^{+\infty} \left(\frac{v_T}{v_A}\right)^n$$

Essendo entrambe due serie geometriche a termini positivi con ragione <1 (dalle ipotesi iniziali sulle velocità) convergono a:

$$x_{tot} = \frac{x_0 v_A}{v_A - v_T}, \quad t_{tot} = \frac{x_0}{v_A - v_T},$$

Ben diverse dall'essere due quantità infinite, come invece aveva concluso Zenone!

Il filosofo, a sua discolpa, non si immaginava come la somma di un numero infinito di termini potesse avere un limite finito; il calcolo infinitesimale infatti venne scoperto da Newton e Leibniz nel '700, più di 2000 anni dopo.
Possiamo dunque concludere che il Pelide raggiungerà la tartaruga e dichiarare risolto l'arguto paradosso.

3. UOMO E LEONE

Il seguente problema è un esempio molto famoso nell'ambito della teoria dei giochi e per questo motivo vi sono molte rivisitazioni dello stesso. Propongo una versione semplificata che recita così:
«Un uomo ed un leone sono chiusi in una gabbia circolare dalla quale non possono uscire ma in cui possono muoversi liberamente. Ipotizzando che entrambi non si stanchino e quindi possano correre per un tempo infinito, è possibile per l'uomo non farsi mai raggiungere dal felino?»
Cerchiamo di formalizzare il tutto.

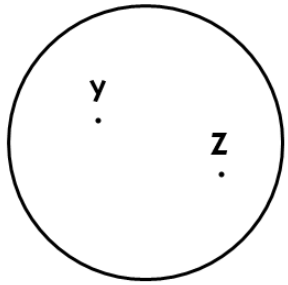
3.1. Impostazione del problema. Assumiamo che sia il leone sia l'uomo possano muoversi con uguale velocità massima di modulo $M > 0$. Siano $y(t) \in \mathbb{R}^2$ la posizione dell'uomo all'istante di tempo t e $z(t) \in \mathbb{R}^2$ la posizione del leone. Inoltre, l'uomo sceglie ad ogni istante la propria velocità $y'(t)$ nell'insieme di tutte le possibili velocità
$U = \{u \in \mathbb{R}^2, |u| \leq M\}$, così il leone sceglie la propria velocità $z'(t)$ nell'insieme $V = \{v \in \mathbb{R}^2, |v| \leq M\}$.

La dinamica del problema è:

$$y'(t) = u(t) \text{ con } u(t) \in U \text{ e } z'(t) = v(t) \text{ con } v(t) \in V.$$

Inoltre WLOG ipotizziamo che la gabbia sia rappresentata da una bolla di raggio R=1 centrata nell'origine. Si avranno dunque anche delle restrizioni sulle posizioni:

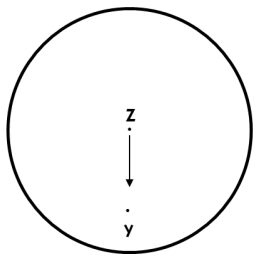
$$|y(t)| \leq R \text{ e } |z(t)| \leq R \quad \forall t \geq 0$$



Data la struttura del problema, risulta più comodo passare in coordinate polari, siano esse (ρ_M, θ_M) quelle dell'uomo e (ρ_L, θ_L) quelle del leone. Si ricava facilmente che la restrizione sul modulo della velocità diventa:

$$(\rho'_M)^2 + \rho_M^2(\theta'_M)^2 \leq M^2 \quad , \quad (\rho'_L)^2 + \rho_L^2(\theta'_L)^2 \leq M^2 \tag{1}$$

3.2. Strategia del leone. Diamo il via all'inseguimento.
Per semplificare i conti, assumiamo che il leone $z(t)$ parta nel centro della gabbia e mostriamo come sia in grado di far tendere a zero la distanza tra lui e l'uomo. La sua strategia è la seguente: muoversi il più velocemente possibile nella direzione dell'uomo, rimanendo sempre sul suo stesso raggio, ovvero in modo che $z(t)$ giaccia sul segmento $[0, y(t)]$ $\forall t$.



In coordinate polari ciò si traduce in: $\theta(t) := \theta_L(t) = \theta_M(t) \quad \forall t$. Dunque $\theta' := \theta'_L = \theta'_M$. Inoltre, il leone decide di massimizzare ρ'_L ottenendo (da (1)) :

$$\rho'_L = \left[M^2 - \rho_L^2(\theta')^2\right]^{\frac{1}{2}}.$$

Dimostriamo che la distanza tra lui e l'uomo tende a zero.

Dimostrazione. Se per assurdo non fosse così allora $\exists \epsilon > 0$ per cui:

$$\rho_L(t) + \epsilon \leq \rho_M(t) \qquad \forall t \geq 0.$$

Si ha:

$$(\rho_L(t) + \epsilon)|\theta'(t)| \leq \rho_M(t)|\theta'(t)| \leq M$$

Ottenendo:

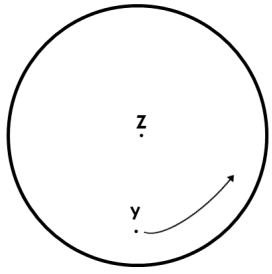
$$\rho'_L(t) = \left[M^2 - \rho_L^2(\theta')^2\right]^{\frac{1}{2}} \geq \left[M^2 - \frac{\rho_L^2 M^2}{(\epsilon + \rho_L)^2}\right]^{\frac{1}{2}} \geq \frac{M\epsilon}{1+\epsilon} > 0.$$

essendo $0 \leq \rho_L \leq 1$. Quest'ultima diseguaglianza tuttavia porta all'assurdo. Infatti, dal teorema dell'incremento finito, avendo una minorazione per ρ'_L data da una quantità strettamente positiva, si conclude che ρ_L tende a $+\infty$ contraddicendo l'ipotesi per cui $\rho_L \leq 1$. □

3.3. Strategia dell'uomo. Mostriamo ora la strategia adottata dall'uomo, che gli permette di stare lontano dal felino per più tempo possibile. Ipotizziamo WLOG che la posizione iniziale dell'uomo sia all'interno dell'arena, ovvero che $\rho_M(0) \in (0,1)$.

Egli allora, decide di "spiraleggiare" verso il bordo, avvicinandosi progressivamente ad esso. Più precisamente:

$$\theta'_M(=\theta') = M\left(\frac{2-\rho_M}{\rho_M}\right)^{\frac{1}{2}} \quad , \quad \rho'_M = (M^2 - (\rho_M\theta')^2)^{\frac{1}{2}}$$



Tali scelte per ρ'_M e θ' sono possibli in quanto, come prima da (1) l'uomo massimizza ρ'_M e il radicando risulta ≥ 0, infatti:

$$M^2 - (\rho_M\theta')^2 = M^2(1 - 2\rho_M + \rho_M^2) = M^2(1-\rho_M)^2 \geq 0.$$

che restituisce $\rho'_M = M(1-\rho_M)$. Risolvendo dunque l'equazione differenziale a variabili separabili si ottiene:

$$\forall t \geq 0, \quad \rho_M(t) = 1 - (1 - \rho_M(0))e^{-Mt} \tag{2}$$

Svolgendo ulteriori conti si ha:

$$\frac{d}{dt}|y(t)-z(t)| = \frac{d}{dt}(\rho_M(t)-\rho_L(t)) = \rho'_M(t)-\rho'_L(t)$$
$$= \left(M^2-(\rho_M\theta')^2\right)^{\frac{1}{2}} - \left(M^2-(\rho_L\theta')^2\right)^{\frac{1}{2}}$$

razionalizzando:

$$= -(\theta')^2(\rho_M^2-\rho_L^2)/[\rho'_M+\rho'_L]$$

essendo $\rho_M \geq \rho_L$, $\rho_L+\rho_M \leq 2$ e $\rho'_M \leq \rho'_L$:

$$\geq -2(\theta')^2(\rho_M-\rho_L)/[2\rho'_M]$$

e infine da (2)

$$= -(\theta')^2 e^{Mt}(\rho_M-\rho_L)/[(1-\rho_M(0))M]$$

Essendo $\rho_M(0) > \rho_L(0)$, si conclude dal Lemma di Gronwall che $\rho_M(t)$-$\rho_L(t)$>0 $\forall t \geq 0$.

Dunque, quasi sorprendentemente, benché il leone sia in grado di arrivare ad una qualsiasi distanza dall'uomo piccola a piacere, quest'ultimo riesce comunque a non farsi mai raggiungere.

Quindi, nel malaugurato caso in cui vi troviate faccia a faccia con un felino poco amichevole in una gabbia, ricordatevi la strategia da adottare. Confidando infatti nella vostra inesauribile resistenza, sarete così in grado di sfuggire al suo attacco con agilità (sperando che nel frattempo qualcuno dall'esterno vi faccia uscire).
N.B.: funziona anche per altre bestie feroci.

3.4. Lemma di Gronwall. Per concludere dimostriamo il Lemma di Gronwall.
Ne esistono diverse versioni, enunciamo tuttavia quella impiegata sopra.

Lemma (di Gronwall)**.** *Sia $u(t)$ derivabile su $I=[a,b)$ con $a<b\leq+\infty$. Se $u'(t)\geq \beta(t)u(t)$ per una certa $\beta(t)\in C^0(I)$, allora $u(t)\geq u(a)exp(\int_a^t \beta(s)ds) \quad \forall t\geq a$.*

Osservazione. Nella dimostrazione precedente, $I=[0,+\infty)$,

$$u(t)=\rho_M(t)-\rho_L(t) \text{ e } u(0)>0,$$

dunque

$$u(t)\geq u(0)\exp\left(\int_0^t \beta(s)ds\right) > 0 \quad \forall t\geq 0.$$

Dimostrazione. Sia

$$v(t)=exp(\int_a^t \beta(s)ds)$$

allora

$$v'(t)=\beta(t)v(t).$$

Si consideri la funzione $\dfrac{u(t)}{v(t)}$ e la si derivi:

$$\frac{d}{dt}\left(\frac{u(t)}{v(t)}\right) = \frac{u'v-uv'}{v^2} = \frac{u'v-uv\beta}{v^2} = \frac{u'-u\beta}{v} \geq 0.$$

Si conclude quindi che

$$\frac{u(t)}{v(t)} \geq \frac{u(a)}{v(a)} = u(a).$$

Quindi la tesi.

□

BIBLIOGRAFIA

- P.MAZZOLDI,M.NIGRO,C.VOCI, Fisica vol.1 (2000)
- P.CARDALIAGUET, Introduction to differential games (2010)

SASSO, CARTA, FORBICI: È UN GIOCO EQUILIBRATO?

URSULA D'ELIA

1. PRESENTAZIONE DEL DILEMMA DEL PRIGIONIERO

Partiamo subito da un esempio: il dilemma del prigioniero. Immaginiamo che due complici abbiano commesso un crimine, vengano arrestati e posti in due celle separate. I poliziotti interrogano ognuno di loro e gli pongono la seguente domanda: "l'altra persona che abbiamo arrestato è colpevole?". Poiché questo interrogatorio avviene in celle distinte, nessuno dei due giocatori può sapere cosa risponde l'altro. Le situazioni finali possibili sono le seguenti:

- nessuno denuncia: 1 anno di galera ciascuno
- entrambi denunciano: 5 anni di galera ciascuno
- uno denuncia e l'altro no: chi è rimasto in silenzio avrà 10 anni, l'altro sarà libero

Possiamo schematizzare le possibili situazioni con la seguente matrice:

	Denuncia	Non denuncia
Denuncia	5,5	0,10
Non denuncia	10,0	1,1

Giocatore 1 Giocatore 2

Ai fini di capire cosa risponderemmo noi se ci trovassimo al posto di uno dei complici, cerchiamo di comprendere a quale di queste situazioni conviene ambire. Sicuramente salta agli occhi che la scelta *collettivamente* giusta è che nessuno denunci. In questo caso in totale si ottengono due anni di prigione. Tuttavia ci troviamo a prendere una scelta nell'ignoranza di ciò che farà l'altro... vale la pena di ambire alla situazione "Non denuncia, Non denuncia"? Se noi scegliamo di non denunciare nella speranza che l'altro faccia lo stesso, stiamo rischiando di prendere ben 10 anni di galera dal momento che nessuno ci garantisce che anche l'altro farà la nostra medesima scelta. In realtà la scelta migliore per il singolo complice *non sapendo quella dell'altro* è denunciare. Infatti, se denuncio, quando scopro cosa l'altro ha scelto, denunciare resta la miglior scelta che potevo fare. Infatti, se vengo a scoprire che l'altro ha denunciato, ho fatto proprio la scelta giusta (se avessi scelto di non denunciare avrei preso 10 anni invece dei 5 che mi toccano avendo scelto di denunciare). Ma anche se vengo a scoprire che l'altro ha taciuto sono soddisfatto della mia scelta, non prendo nessun anno di galera, non ho nessun interesse a cambiare decisione, ho fatto la cosa migliore.

1.1. Formalizzazione di un "gioco" e dell'equilibrio di Nash. Il dilemma del prigioniero è un classico esempio di "gioco". La teoria dei giochi è una branca della matematica che riguarda i modelli di interazione strategica tra diversi agenti. In altre parole, descrive matematicamente tutte quelle situazioni in cui alcuni individui devono prendere delle decisioni e l'eventuale guadagno o perdita per il singolo agente non dipende solo dalla sua decisione individuale ma anche dalle decisioni che hanno preso gli altri. Ogni situazione fatta in questo modo è chiamata "gioco" ma non corrisponde necessariamente a un gioco nel senso tradizionale della parola. Alcuni esempi possono essere infatti: un investimento finanziario, una guerra o un appuntamento. Vediamo come possiamo formalizzare un "gioco" ai fini di capire matematicamente perché la scelta di denunciare è la migliore da fare.

DEFINIZIONE. Un **Gioco Strategico** o **Gioco in Forma Normale** è una terna

$$G = \{N, S, u\}$$

- $N = \{1, \dots, n\}$ numero di giocatori
- $S = S_1 \times \cdots \times S_n$ insieme di tutte le strategie
  - dove S_i è l'insieme di strategie possibili per il giocatore i-esimo
- $u = (u_1, \dots, u_n)$ è la **funzione di utilità**
  - ogni $u_i : S \to \mathbb{R}$ misura, dal punto di vista dell'i-esimo giocatore, la "qualità" della situazione in cui ogni giocatore ha preso la sua decisione
  - Più è alto il valore di u_i, più la situazione generale è favorevole per il giocatore i-esimo

Vediamo ora come possiamo formalizzare matematicamente il dilemma del prigioniero tramite la struttura appena introdotta.

- $N = \{1, 2\}$
- $S = \{\text{Denuncia, Non Denuncia}\} \times \{\text{Denuncia, Non Denuncia}\}$
  - in questo caso $S_1 = S_2$
- $u = (u_1, u_2)$
  - calcoliamo ad esempio $u_1 : S \to \mathbb{R}$

$u_1(\text{Denuncia , Denuncia}) = -5$
$u_1(\text{Non denuncia , Denuncia}) = -10$
$u_1(\text{Denuncia , Non denuncia}) = 0$
$u_1(\text{Non denuncia , Non Denuncia}) = -1$

n.b. il segno meno è una convenzione che fa sì che più alto sia il valore di u_i , più favorevole sia la situazione per il giocatore i-esimo.

Ora che abbiamo formalizzato il concetto di gioco possiamo introdurre la nozione rigorosa di equilibrio di Nash.

DEFINIZIONE. Un **equilibrio di Nash** è un profilo di strategie $x^* \in S$ tale che $\forall i$ la strategia x_i^* è la migliori risposta alla strategia x_{-i}^*

$$\forall i \in N \quad u_i\left(x_i^*, x_{-i}^*\right) \geq u_i\left(x_i, x_{-i}^*\right) \qquad \text{per ogni } x_i \in S_i$$

in cui abbiamo utilizzato la seguente notazione

- $x_{-i} = \left(x_j\right)_{j \neq i}$ "vettore (n-1) delle scelte" di tutti i giocatori eccetto l'i-esimo

- $S_{-i} = \prod_{j \neq i} S_j$ insieme di tutti i profili di strategie per tutti i giocatori tranne i

In altre parole, $x^* \in S$ ("vettore delle scelte prese") è un **Equilibrio di Nash** se tutti i giocatori, viste le scelte degli altri, scoprono che la loro scelta è la migliore che potevano fare.

Nel caso del dilemma del prigioniero, la situazione di equilibrio di Nash corrisponde a quella in cui entrambi i giocatori denunciano l'altro. Vediamolo nel dettaglio.

Il "vettore delle scelte" $x^* = (\text{Denuncia}, \text{Denuncia}) \in S$ è un equilibrio di Nash

	Denuncia	Non denuncia
Denuncia	5,5	0,10
Non denuncia	10,0	1,1

Infatti: fissiamo un giocatore, ad esempio giocatore 1. Per capire se è un' E.N. devo controllare che, tenendo fissa la scelta dell'avversario, g1 non ha interesse a cambiare la sua

$$-5 = u_1(\text{ D }, \text{D}) \geq u_1(\text{ ND }, \text{D}) = -10$$

Poiché anche per il giocatore 2 vale la stessa identica cosa, la condizione vale per *tutti i giocatori*, allora possiamo concludere che è un E.N.

1.2. Sasso carta forbici e le strategie miste. Abbiamo adesso tutti gli strumenti a disposizione per analizzare il gioco "Sasso carta forbici" tramite la teoria dei giochi. Possiamo innanzitutto schematizzarlo con la seguente tabella.

I/II	*carta*	*forbici*	*sasso*
carta	$(0,0)$	$(-1,1)$	$(1,-1)$
forbici	$(1,-1)$	$(0,0)$	$(-1,1)$
sasso	$(-1,1)$	$(1,-1)$	$(0,0)$

In questo gioco non c'è mai un equilibrio di Nash poichè,una volta scoperta la mossa dell'avversario, *almeno uno* dei due giocatori vorrà cambiare la sua.

Ad esempio: $x^* =$ (forbici, forbici) non è un equilibrio perché

$$0 = u_1(x_1^*, x_2^*) \quad < \quad u_1(\text{sasso}, x_2^*) = 1$$

Ma non è finita qui, in realtà se ampliamo la nostra visuale sui "giochi" possiamo essere in grado di trovare anche in "Sasso carta forbici" un equilibrio di Nash.

Vogliamo quindi generalizzare il concetto di gioco. Fin'ora abbiamo considerato come scelte solo decisioni "pure" come { carta } oppure { denuncia } Il modo in cui vogliamo ampliare la teoria dei giochi vista fin'ora consiste nel considerare come scelte anche strategie miste, ad esempio "con una probabilità del 90% denuncerà e con una del 10% non denuncerà" .

Prima di procedere con la formalizzazione precisa, ricordiamo la seguente definizione

DEFINIZIONE. Una **misura di probabilità** su un insieme X t. c. $|X| < \infty$ discreto è una funzione $\sigma : X \to [0,1]$ t.c. $\sum_{x \in X} \sigma(x) = 1$

Adesso possiamo formalizzare più specificatamente quelle strategie che comprendono in parte una scelta e in parte un'altra.

DEFINIZIONE. Una **strategia mista** per il giocatore i è una misura di probabilità sull'insieme di strategie pure S_i

In altre parole, una strategia mista σ_i assegna a ogni strategia pura $x_i \in S_i$ una probabilità che descrive come il singolo giocatore distribuisce le sue scelte.

Abbiamo quindi a che fare con un insieme molto più grande di strategie tra cui scegliere. Considereremo d'ora in poi non più l'insieme delle strategie pure S_i , ma l'insieme $\Delta(S_i)$ delle strategie miste (i cui elementi sono quindi misure di probabilità).

$$\Delta(S_i) = \left\{\sigma_i : S_i \to [0,1] : \textstyle\sum_{x_i \in S_i} \sigma_i(x_i) = 1\right\}$$

Un esempio di strategia mista nel gioco che vogliamo analizzare è la seguente. La misura $\sigma_i = (2/3, 1/3, 0)$ sull'insieme {Sasso, carta forbici} è un elemento di $\Delta(S_i)$ e rappresenta la decisione del giocatore i di giocare sasso con probabilità $2/3$, carta con $1/3$ e mai forbici.

Ora che abbiamo cambiato l'insieme di strategie, cambierà anche la funzione di utilità: sia $\sigma = (\sigma_1, \ldots, \sigma_n)$, la nuova funzione di utilità sarà

$$h_i(\sigma) = \sum_{x \in S} u_i(x_1, \ldots, x_n)\, \sigma_i(x_i)\, \sigma_{-i}(x_{-i})$$

$$\text{con } \sigma_{-i}(x_{-i}) = \prod_{j \neq i} \sigma_j(x_j)$$

Abbiamo tutti gli ingredienti a disposizione per formalizzare il nuovo gioco che abbiamo ottenuto a partire dal gioco classico.

DEFINIZIONE. Sia $G = \left(N, \{S_i\}_{i \in N}, \{u_i\}_{i \in N}\right)$ un gioco in forma normale. Allora il gioco

$$G_{me} = \left(N, \{\Delta(S_i)_i\}_{i \in N}, \{h_i\}_{i \in N}\right)$$

è chiamato **estensione** di G a strategie miste.

Ora siamo in grado di determinare i nuovi equilibri poiché gli equilibri di Nash per le strategie miste saranno gli equilibri di Nash per il gioco esteso. Vediamo la formulazione estesa di sasso carta forbici.

- $N = 2$ numero di giocatori
- $S = \{\Delta(S_1), \Delta(S_2)\}$
  - $\Delta(S_1) = \left\{p \in \mathbb{R}^3_+ : p_1 + p_2 + p_3 = 1\right\}$
  - $\Delta(S_2) = \left\{q \in \mathbb{R}^3_+ : q_1 + q_2 + q_3 = 1\right\}$
- $h_1 = u_1(\text{c}, \text{c})p_1q_1 + u_1(\text{c}, \text{f})p_1q_2 + u_1(\text{c}, \text{s})p_1q_3 + u_1(\text{f}, \text{c})p_2q_1 + u_1(\text{f}, \text{f})p_2q_2 + u_1(\text{f}, \text{s})p_2q_3 + u_1(\text{s}, \text{c})p_3q_1 + u_1(\text{s}, \text{f})p_3q_2 + u_1(\text{s}, \text{s})p_3q_3$ e sostituendo
- $h_1 = 0 - p_1q_2 + p_1q_3 + p_2q_1 + 0 - p_2q_3 - p_3q_1 + p_3q_2 + 0$

Vogliamo ora trovare un equilibrio, per farlo useremo anche noi una strategia, chiamata *strategia di sicurezza*. Ciò consiste nel valutare, per ogni singola scelta, qual è la peggiore delle cose che può capitare. Vediamo quindi per ogni nostra strategia il massimo valore della nostra perdita. A questo punto, per metterci appunto in sicurezza, scegliamo quella scelta che massimizza la perdita peggiore. Questa strategia è anche nota come "minmax", il cui termine è associato anche a uno dei più famosi teoremi di teoria dei giochi, cioè il teorema minmax di John Von Neumann (che però in questa trattazione non affrontiamo). La strategia di sicurezza può essere utile per trovare equilibri di Nash in alcuni casi, come nel nostro. Vediamo più precisamente quali sono i passaggi da seguire per mettere in atto tale strategia.

- Fissata la mia (g1) strategia p, qual è la cosa peggiore che può accadere?
  $\min\{h_1(p,q) : q \in \Delta(S_2)\} = w_1(p)$
- Tra tutte le mie strategie p, qual è quella per cui $w_1(p)$ è più alto? Scelgo quella e mi metto in *sicurezza*
  $\max\{w_1(p) : p \in \Delta(S_1)\}$
  $\text{argmax}\{w_1(p) : p \in \Delta(S_1)\} = p*$

Vediamo come applicare questa strategia per trovare un equilibrio in "sasso carta forbici"

Nel nostro caso

$$w_1(p) = \min\{h_1(p,q) =$$
$$= q_1(p_2 - p_3) + q_2(p_3 - p_1) + q_3(p_1 - p_2) : q \in \Delta(S_2)\}$$
$$= \min\{(p_2 - p_3), (p_3 - p_1), (p_1 - p_2)\}$$

oss. $w_1(p) \leq 0$ perché $(p_2 - p_3) + (p_3 - p_1) + (p_1 - p_2) = 0$

quindi la strategia di sicurezza che massimizza $w_1(p)$ è
$\text{argmax}\{(p_2 - p_3), (p_3 - p_1), (p_1 - p_2)\} = \{(1/3, 1/3, 1/3)\}$

Fact: In questo caso particolare (gioco a somma zero, gioco con valore) l'elemento di $\Delta(S)$ dato dalle strategie di sicurezza (p*, q*) è proprio un equilibrio di Nash $\rightarrow$ $(1/3, 1/3, 1/3)$, $(1/3, 1/3, 1/3)$ è un equilibrio di Nash. Quindi, in conclusione, anche il gioco sasso carta forbici ha un equilibrio di nash.

BIBLIOGRAFIA

- **TedEd: Why do competitors open their stores next to one another? - Jac de Haan** link.
- **BBC: The joy of winning - Hannah Fry** link
- **Sylvia Nasar - Il genio dei Numeri** link

CHI HA RUBATO LE CARTE DI DOBBLE?

MARCO CATTAZZO

1. INTRODUZIONE

Estate, vacanza, momento di riposo con gli amici sotto l'ombra dei boschi che coprono i colli toscani. Quale momento migliore per farsi tarlare la testa da un problema matematico?

Matteo estrae dallo zaino delle carte tonde e colorate, ciascuna con lo stesso numero di simpatici disegnini, e ci propone una partita a Dobble (o Spot-It, che dir si voglia). Ci spiega che è possibile giocare con questo particolare mazzo in diversi modi, ma la dinamica di gioco alla base di ogni modalità è sempre la stessa: riuscire a individuare, il più velocemente possibile, per ogni coppia di carte, il simbolo in comune.

Ma quindi ogni coppia di carte ha *almeno* un simbolo in comune? Guardo meglio. Ogni carta ha *uno e un solo simbolo in comune* con ciascuna altra! Febbrilmente mi metto a contarle: sono 55. Ma sono tutte? Siamo sicuri che non se ne possano aggiungere altre? Quante sono in tutto? Come si possono costruire altri mazzi di questo tipo?

Vorrei condividere con voi l'inaspettato tragitto che ho percorso per arrivare a rispondere a queste ed altre domande, che inevitabilmente passa attraverso l'inserimento del problema in un contesto assiomatico e rigoroso. Ciò che ai miei occhi rende degna di nota questa particolare formalizzazione, che scopriremo utilizzare un linguaggio estremamente comodo per parlare dell'oggetto in questione in modo efficace, è il suo essere anche una fonte di punti di vista innovativi e inaspettati sul problema. Del resto, il fatto che due concetti siano logicamente equivalenti non implica che tra questi sussista una equivalenza semantica!

2. IL MAZZO DI DOBBLE

2.1. Le regole del mazzo. Iniziamo dunque dicendo un po' più formalmente cosa è per noi un mazzo di carte di Dobble:

Definizione 1. Definiamo **mazzo di Dobble** una coppia $(\{simboli\}, \{carte\})$ che rispetti le seguenti proprietà:

FIGURA 1. Due diversi mazzi di Dobble, il primo nella sua versione classica, con 8 simboli per carta, il secondo in una versione ridotta con solo 5 simboli per carta.

D1. Ogni carta ha uno e un solo simbolo in comune con ogni altra carta
D2. Ogni carta ha lo stesso numero s di simboli
D3. Nessun simbolo appare più di una volta per ogni carta
D4. Non possono esistere due carte identiche nello stesso mazzo
D5. Ogni simbolo deve apparire su almeno una carta
D6. Non ci dev'essere uno stesso simbolo comune a ogni carta

Chiamiamo **cardinalità** di un mazzo di Dobble il numero delle sue carte.

Lasceremo per ora sottintesi nella presente formalizzazione alcuni dettagli squisitamente concreti di un mazzo di carte, quali la finitudine e il significato di appartenenza di un simbolo a una carta, così come anche eviteremo l'incombenza di considerare le eccezioni dovute ai casi "piccoli" (per esempio $|\{simboli\}| \leq 2$).

Soffermandoci ad analizzare il significato dei nostri *assiomi di mazzo di Dobble*, notiamo per esempio che D5 nel nostro caso funge un po' da rasoio di Occam [1], riducendo l'insieme dei simboli utilizzabili al minimo indispensabile, ovvero quelli realmente utilizzati. La condizione D6 è invece fondamentale per escludere la famiglia di mazzi banali rappresentata da quello della Figura 2, in cui tutte le carte hanno lo stesso simbolo in comune.

Se non avessimo D6, fissato $s \geq 2$, potremmo facilmente costruire mazzi di Dobble di cardinalità arbitraria, ma sarebbero tutti decisamente *noiosi*.

Per darsi ragione in modo un po' più preciso della selezione degli *assiomi* del mazzo di Dobble e dei problemi che si incorrono nei casi piccoli, è possibile consultare [MoTaG].

Ci si accorge ben presto però che queste condizioni, benchè siano sufficienti per generare un mazzo propriamente detto, non bastano a garantire che questo sia *divertente*. Consideriamo per esempio il caso rappresentato in Figura 3:

[1] del resto, «*frustra fit per plura quod potest fieri per pauciora*»

FIGURA 2. Insieme di carte che non è un mazzo, in quanto contraddice D6. Qui più che a *Spot It!* sembra di giocare a *Spot the Atom*.

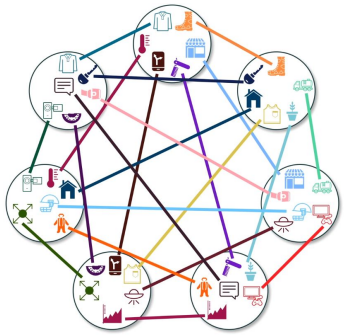


FIGURA 3. Mazzo di Dobble propriamente detto, ma non divertente!

In questa famiglia di mazzi, generati aggiungendo un nuovo simbolo per ogni coppia di carte distinte, un mazzo di n carte necessiterà di $n-1$ simboli per carta per essere realizzato, richiedendo dunque un totale di $\binom{n}{2}$ simboli diversi. Ciò significa che per eguagliare in dimensione il mazzo canonico di Dobble, composto da 55 carte, ogni carta dev'essere grande all'incirca come un lenzuolo, e servirà un plotone di grafici per realizzare tutti i $\binom{55}{2} = 1485$ simboli diversi necessari.

Ma è possibile realizzare un mazzo il più grande possibile, ma tale per cui ogni carta contenga (più o meno) il numero minimo di simboli sufficiente?

2.2. Le domande. Il mazzo canonico di Dobble, che troviamo a sinistra in Figura 1, è formato da 57 simboli e 55 carte, con 8 simboli per ogni carta. Ora che abbiamo definito con precisione l'ambiente dove lavoreremo, ci proponiamo come obiettivo quello di soddisfare la curiosità iniziale affrontando le seguenti domande:

- Il mazzo di Dobble di 55 carte è *completo*? Se non lo è, esiste un modo per *completarlo*? Se sì, quante carte dobbiamo aggiungere? Insomma, chi ha

rubato le carte di Dobble?
- Stuzzicati dalla curiosità e divertiti dal gioco, vogliamo giocare a Dobble coi nostri 20 amici, tutti insieme. Esiste un modo canonico per costruire un mazzo di Dobble *divertente* con un numero di carte arbitrario?

Lasciamo per ora che le definizioni di *completo* e *divertente* ci guidino solo a livello intuitivo: penseremo poi a formalizzarle, se necessario.

3. PIANI PROIETTIVI E GEOMETRIA D'INCIDENZA

Introduciamo le strutture formali che ci serviranno per modellizzare il nostro mazzo. Le prendiamo in prestito da una branca della matematica che giace all'intersezione tra la geometria di dimensione finita e il calcolo combinatorio: la geometria d'incidenza.

Andremo a definire alcuni particolari *sistemi di incidenza*, oggetti che, insieme ai sistemi di Steiner e ai multigrafi, sono fra i principali strumenti utilizzati dai matematici per studiare collegamenti e intersezioni tra collezioni di oggetti, a priori da qualsiasi topologia o operazione algebrica.

Definizione 2. Definiamo **Struttura (o sistema) di incidenza** una terna $(\mathfrak{P}, \mathfrak{L}, I)$ (anche abbreviata semplicemente $(\mathfrak{P}, \mathfrak{L})$ nei contesti in cui I è unica o nota), in cui $\mathfrak{P}$ e $\mathfrak{L}$ sono insiemi di elementi che chiamiamo rispettivamente **punti** e **rette**, mentre $I \subseteq \mathfrak{P} \times \mathfrak{L}$ è detta **relazione di incidenza**. Secondo una ovvia estensione terminologica, se la coppia (P, l) appartiene ad I, diremo che il punto **appartiene alla, o giace sulla** retta l, e che la retta l **contiene, o passa per** il punto P. Parleremo anche di **intersezione tra** e **unione di** rette come nel modo consueto.

Notiamo che un sistema di incidenza è tutto ciò che ci serve per formalizzare un mazzo di carte con simboli nella teoria degli insiemi. D'ora in avanti penseremo a un mazzo di Dobble come un sistema di incidenza definito nel seguente modo: sia $(\mathcal{S}, \mathcal{C})$ un mazzo di Dobble, dove $\mathcal{S}$ è l'insieme che ha per elementi i simboli del mazzo, mentre $\mathcal{C}$ le carte. Sia $\in \subseteq \mathcal{S} \times \mathcal{C}$ la relazione tale che, se s è un simbolo e c è una carta, allora (s, c) sta in $\in$ quando il simbolo appartiene alla carta. Si noti che in questo caso, per evidenti esigenze fisiche, avremo che $|\mathcal{S}|, |\mathcal{L}| \in \mathbb{N}$.

Viceversa, possiamo realizzare facilmente un mazzo di carte con simboli (non necessariamente di Dobble!) a partire da un sistema d'incidenza $(\mathfrak{P}, \mathfrak{L})$ tale che $|\mathfrak{P}|, |\mathfrak{L}| \in \mathbb{N}$: basta prendere tante carte quante sono le rette del sistema di incidenza, e su ciascuna carta rappresentare i punti che appartengono alla retta corrispondente.

Alla luce di questa osservazione, considereremo d'ora in avanti come equivalenti i termini retta-carta e i termini punto-simbolo, in modo da poterci focalizzare esclusivamente sulle proprietà che caratterizzano le strutture.

Definizione 3. Definiamo **Piano Proiettivo** un sistema di incidenza che rispetta le seguenti proprietà:

P1. Per ogni coppia di punti, esiste unica la retta che passa per entrambi
P2. Per ogni coppia di rette, esiste unico il punto che appartiene a entrambe
P3. Esistono quattro punti tali che nessuna terna di questi punti giaccia sulla stessa retta

Notiamo che i nomi e le proprietà date agli oggetti richiedono un ben definito sforzo semantico da parte di chi li usa: stimolano infatti una precisa e familiare visualizzazione dei collegamenti tra oggetti. Tuttavia, mentre facilmente riusciamo a figurarci le proprietà P1 e P2, un po' più ostica è la rappresentazione mentale di P3. Rafforziamo la nostra familiarità con l'oggetto tramite questo lemma, la cui dimostrazione è reperibile a pagina 52 di [Moorh].

Teorema 4. *Una struttura d'incidenza rispetta gli assiomi P1 e P2, ovvero è una* ***configurazione chiusa****, se e solo se è una delle seguenti:*

(1) $(\emptyset, \emptyset)$
(2) un singolo punto
(3) una singola retta
(4) una retta l e un punto P su di essa, con $m \geq 0$ rette passanti per P oltre a l, e $n \geq 0$ punti su l oltre a P
(5) una retta l e un punto $P \notin l$, con $m \geq 0$ rette passanti per P e i loro m punti di intersezione come punti di l
(6) un piano proiettivo

E vale che la configurazione chiusa è un piano proiettivo se e solo se vale P3.

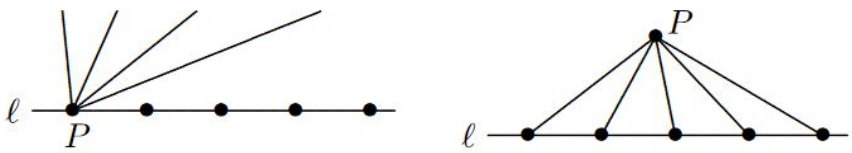


FIGURA 4. Rappresentazione tramite punti e rette in $\mathbb{R}^2$ del caso 4. e del caso 5.

Notiamo che $\mathbb{PR}^2$, l'usuale piano proiettivo reale, è un piano proiettivo secondo la geometria d'incidenza; tuttavia, per soddisfare le nostre curiosità riguardo al mazzo di Dobble, ci interesseremo esclusivamente di piani proiettivi generati a partire da campi finiti, la cui costruzione in forma generale è reperibile per esempio in [Sern].

Teorema 5. *I Piani proiettivi finiti* ***classici****, costruiti nel modo usuale a partire da un campo finito $\mathbb{F}_{p^n}$ e che denotiamo con $\mathbb{PG}^2(\mathbb{F}_{p^n})$, sono piani proiettivi finiti.*

La dimostrazione di questo fatto è facilmente deducibile con una adeguata mole di calcoli, che (come se ci fosse bisogno di dirlo!) ometteremo. Notiamo però sin d'ora alcune proprietà interessanti dei $\mathbb{PG}^2(\mathbb{F}_q)$, che ritroveremo in seguito: Siccome $\mathbb{F}_q^3$ è di dimensione 3 su $\mathbb{F}_q$, avrà $q^3 - 1$. Segue che, siccome ogni

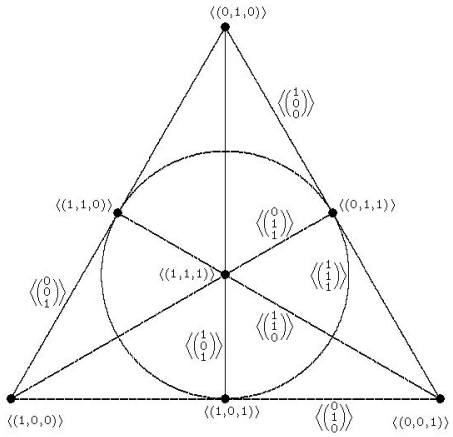


FIGURA 5. Il Piano di Fano, o $\mathbb{PG}^2(\mathbb{F}_2)$

sottospazio di dimensione 1 contiene $q-1$ vettori nonnulli, il numero di punti di $\mathbb{PG}^2(\mathbb{F}_q)$, che corrisponde al numero di sottospazi di dimensione 1, e nel nostro caso ai vettori riga omogenei di dimensione 3 a entrate in $\mathbb{F}_q$, è $\frac{q^3-1}{q-1} = q^2+q+1$. Osservando che le rette in un piano proiettivo così costruito sono tutti e soli i piani di $\mathbb{F}_q^3$ resi omogenei, ovvero sono i vettori omogenei colonna, deduciamo che anche le rette sono q^2+q+1.

Ci dimenticheremo tuttavia d'ora innanzi la struttura algebrica di questi piani proiettivi, mantenendo esclusivamente le proprietà di incidenza, posto che questa può essere parzialmente recuperata quando lo si desidera. A questo proposito si veda il capitolo 4 di [Sand].

4. DOBBLE E I PIANI PROIETTIVI - IL PERCORSO

Vogliamo indagare la relazione tra i piani proiettivi finiti e i mazzi di Dobble come strutture di incidenza, con l'obiettivo di arrivare ad utilizzare gli strumenti sviluppati dalla geometria d'incidenza a servizio dei nostri scopi. Procederemo in questo modo: dapprima dimostreremo che ogni piano proiettivo realizza un mazzo di Dobble. Definiremo poi alcune tipologie di mazzi detti *saturi*, degni di nota per la loro *efficienza* nell'utilizzo di simboli a parità di numero di carte ottenute. Dimostreremo che i mazzi generati dai piani proiettivi sono *saturi*. Noteremo che non vale il viceversa, ovvero non ogni mazzo di Dobble è un piano proiettivo, ma fortunatamente i nostri mazzi *saturi* si, individuando quindi un comodo campo comune all'interno del quale lavorare.

4.1. Tutti i piani proiettivi finiti sono mazzi di Dobble?

Teorema 6. *Ogni piano proiettivo finito è un mazzo di Dobble.*

Dimostrazione. Abbiamo già visto nelle osservazioni che seguono la definizione 2 che entrambi gli oggetti sono sistemi di incidenza con un numero finito di punti

e rette. Rimane dunque da dimostrare che gli assiomi di piano proiettivo sono più restrittivi di quelli di mazzo di Dobble.

P1. Per ogni coppia di punti, esiste unica la retta che passa per entrambi
P2. Per ogni coppia di rette, esiste unico il punto che appartiene a entrambe
P3. Esistono quattro punti tali che nessuna terna di questi punti giaccia sulla stessa retta

D1. Ogni carta ha uno e un solo simbolo in comune con ogni altra carta
D2. Ogni carta ha lo stesso numero s di simboli
D3. Nessun simbolo appare più di una volta per ogni carta
D4. Non possono esistere due carte identiche nello stesso mazzo
D5. Ogni simbolo deve apparire su almeno una carta
D6. Non ci dev'essere uno stesso simbolo comune a ogni carta

- P2 $\iff$ D1
- Piano proiettivo $\implies$ Sistema di incidenza $\implies$ D3
- P1 (unicità) $\implies$ D4, P1 (esistenza) $\implies$ D5

in modo ovvio, eseguite le dovute traduzioni.

- P1,P2,P3 $\implies$ D2

Lemma 7. *Sia $(\mathfrak{P}, \mathfrak{L})$ un piano proiettivo. Allora ogni retta contiene lo stesso numero di punti (**D2**), e questo numero coincide col numero di rette che passano per ogni punto. Se $n+1$ è il numero di punti per ogni retta, allora $|\mathfrak{P}| = |\mathfrak{L}| = n^2 + n + 1$.*

Dimostrazione. Sia $\lfloor P \rfloor$ l'insieme delle rette attraverso il punto P, e sia $\lfloor l \rfloor$ l'insieme dei punti appartenenti alla retta l. Se $P \notin l$, allora la bigezione ovvia consiste nell'associare a ogni punto Q di l la retta PQ che esiste ed è unica (P1). Viceversa, a ogni retta passante per P associo il suo punto di intersezione con l, che esiste ed è unico (P2). Siano ora l e m due rette distinte. Per (P3) esiste un punto $P \notin \lfloor l \rfloor \cup \lfloor r \rfloor$. Se così non fosse, infatti, avrei un assurdo (esercizio!). Vale allora che $||\lfloor l \rfloor|| = ||\lfloor P \rfloor|| = ||\lfloor r \rfloor||$. Dunque ogni coppia di rette ha la stessa cardinalità $n+1$. Chiamiamo n **ordine** del piano proiettivo. Sia ora P di nuovo un punto qualsiasi. So che ogni punto del piano giace su una retta che passa anche per P. Ognuna delle $n+1$ rette passanti per P contiene n punti oltre a P. Segue dunque che i punti, in totale, sono $(n+1)n+1$. Analogo ragionamento si può fare per le rette. □

- P3 $\implies$ D6

Iniziamo supponendo che tutte le (carte) rette abbiano uno stesso simbolo (punto) in comune, che chiameremo P. Siano poi altri 3 punti Q, R, S. Dimostro che Q, R, S sono collineari: Sia per assurdo $Q \notin RS$. Ma $P \in RS$ per ipotesi, dunque $RS \equiv PS$. Ma $P \in QS$, dunque $QS \equiv PS$. In conclusione $QS \equiv RS$, assurdo. Ho dimostrato che sotto l'ipotesi $\neg D6$ tutte le terne di punti sono collineari, negando $P3$.

□

Questo teorema ci fornisce un metodo per generare mazzi di Dobble arbitrariamente grandi, con dimensione che dipende dalla cardinalità del campo finito su cui li andiamo a costruire. Potresti obiettare che noi già possedevamo un metodo per farlo, per inefficiente che fosse, che è quello rappresentato dall'esempio in Figura 3. Sorge dunque una domanda: perchè tenersi particolarmente cara questa costruzione? è davvero più efficiente? La risposta è contenuta nella sezione seguente.

4.2. Tutti i piani proiettivi finiti sono mazzi di Dobble saturi? Vogliamo evidenziare una proprietà particolare dei piani proiettivi finiti: essi non sono dei mazzi di Dobble qualsiasi, ma condividono una particolare proprietà che li caratterizza.

Definizione 8. Chiamiamo un mazzo di Dobble $(\mathcal{S}, \mathcal{C})$ **completo** quando è massimale rispetto all'ordine parziale $(\mathcal{S}, \mathcal{C}) \subseteq (\mathcal{S}', \mathcal{C}') \overset{df}{\iff} \mathcal{S} \subseteq \mathcal{S}'$ e $\mathcal{C} \subseteq \mathcal{C}'$, dove con quest'ultima contenenza intendiamo anche che le carte mantengono gli stessi simboli.

Abbiamo qui definito dei mazzi di Dobble per noi di particolare interesse: possiamo considerare infatti un mazzo completo come un mazzo a cui non è più possibile aggiungere carte a meno di modificare tutte le altre, aggiungendo simboli.

Se le carte devono conservare il numero dei simboli, vediamo che la completezza dipende sia dal numero di simboli per carta, che da come i simboli sono disposti tra le carte.

Teorema 9. *In ogni mazzo di Dobble in cui ogni carta ha s simboli, ogni simbolo può comparire al massimo s volte.*

Dimostrazione. Supponiamo per assurdo che un simbolo P compaia in $s+1$ carte diverse. Se non esistessero altre carte, allora tutte le carte del mazzo avrebbero lo stesso simbolo, contraddicendo D6. Allora deve esistere un'altra carta r che abbia in comune uno e un solo simbolo con ogni carta precedente. Se questo simbolo fosse P, di nuovo D6 ci condurrebbe ad un assurdo. Ma siccome le carte, a meno di P, sono a due a due disgiunte, segue che r dovrebbe, per mantenere l'intersezione unica, contenere $s+1$ simboli. Assurdo. □

Alla luce di ciò, possiamo definire un'altra famiglia di mazzi secondo una condizione più restrittiva, dunque un'altra famiglia meno numerosa di quella appena definita.

Definizione 10. Chiamiamo un mazzo di Dobble con s simboli per carta **saturo** quando ogni simbolo compare su esattamente s carte diverse.

Corollario 11. *Condizione sufficiente perchè un mazzo di Dobble in cui ogni carta ha s simboli sia completo è che ogni simbolo compaia s volte sulle carte. In altre parole, ogni mazzo saturo è completo.*

Dimostrazione. Sia c una certa carta del mazzo. La carta c ha s simboli. Ma ciascuno di questi s simboli appare altre $s-1$ volte nel mazzo per ipotesi. Ogni carta in cui uno di questi simboli, diciamo †, appare, deve avere uno e un solo simbolo

comune con c, che sarà proprio †. Segue che nel mazzo dobbiamo individuare almeno altre $s(s-1)$ carte. Dimostriamo che nel mazzo non possono essercene (e non possono venirne aggiunte) altre. Supponiamo che ci sia (o che venga aggiunta) una certa carta k. Allora k deve avere un simbolo comune con ogni altra carta, quindi anche con c, sia esso ‡. Allora ‡ compare s volte nel mazzo, e una volta in k. Assurdo. □

Otteniamo come porisma che un mazzo saturo ha esattamente $s^2 - s + 1$ carte, e dunque $s^2 - s + 1$ simboli. Notiamo che l'esistenza di un mazzo saturo (non vuoto) non è garantita per ogni s! Vedremo in seguito che l'esistenza di questo mazzo è equivalente a uno dei «principali problemi aperti in geometria finita» [Moorh].

Corollario 12. *Ogni piano proiettivo di ordine n è un mazzo di Dobble in cui ogni carta ha $n+1$ simboli. Inoltre è saturo, dunque completo.*

Dimostrazione. Sappiamo che in ogni piano proiettivo di ordine n ci sono $n^2 + n + 1$ carte (rette), ciascuna con $n+1$ simboli (punti). Sappiamo inoltre per quanto visto all'inizio che esistono $n^2 + n + 1$ simboli (punti) differenti. Segue che ogni simbolo compare $n+1$ volte. □

Notiamo che un mazzo saturo è un mazzo *ottimale* nel senso che *fa il miglior uso possibile* di *ciascun* simbolo a sua disposizione, tra mazzi con lo stesso numero di simboli per carta. Siamo ben lontani dall'esempio in Figura 3, tramite il quale per realizzare n carte (necessariamente contenenti $n-1$ simboli ciascuna) servivano $\binom{n}{2}$ simboli. Per concretizzare l'esempio inserendo dei numeri, ricordo che per ottenere 55 carte erano necessari 1485 simboli, 54 per ogni carta. Utilizzando invece $\mathbb{P}\mathrm{G}^2(\mathbb{F}_7)$, con soli 57 simboli, 8 per carta, riesco a ottenere 57 carte, due in più delle 55 necessarie. Questi mazzi saranno il nostro oggetto di studio, sia in quanto sono i migliori mazzi di Dobble che speriamo di costruire, sia perchè, come già accennato e come esposto in seguito, caratterizzeranno, tra i mazzi di Dobble, i piani proiettivi.

Ma iniziamo a darci ragione del fatto che ci sia effettivamente bisogno di caratterizzarli.

4.3. Tutti i mazzi di Dobble sono piani proiettivi? No. Mi accorgo che prendendo un sottoinsieme di carte di un qualsiasi mazzo di Dobble completo con $n+1$ simboli per carta (ed eliminando dall'insieme dei simboli quelli che non compaiono più su nessuna carta per mantenere la proprietà D5), ottengo nuovamente un mazzo di Dobble. Questo mazzo, che è effettivamente un mazzo di Dobble, non potrà mai essere un piano proiettivo, in quanto non completo. Infatti il mazzo di partenza è "più grande" nel senso della Definizione 8.

4.4. Tutti i mazzi di Dobble saturi sono piani proiettivi?

Teorema 13. *Ogni mazzo di Dobble saturo è un piano proiettivo.*

Dimostrazione. Con le premesse del Teorema 6, mettiamo a confronto i due sistemi di assiomi.

D1. Ogni carta ha uno e un solo simbolo in comune con ogni altra carta
D2. Ogni carta ha lo stesso numero s di simboli
D3. Nessun simbolo appare più di una volta per ogni carta
D4. Non possono esistere due carte identiche nello stesso mazzo
S5. Ogni simbolo deve apparire su **esattamente** s **carte**
D6. Non ci dev'essere uno stesso simbolo comune a ogni carta

P1. Per ogni coppia di punti, esiste unica la retta che passa per entrambi
P2. Per ogni coppia di rette, esiste unico il punto che appartiene a entrambe
P3. Esistono quattro punti tali che nessuna terna di questi punti giaccia sulla stessa retta

- P2 $\iff$ D1 in modo ovvio
- P1 (unicità)

Siano S, T due simboli. Non è possibile che esistano due carte a, b tali che sia S che T appartengano a entrambe le carte, in quanto questo sarebbe in contraddizione con D1.

- P1 (esistenza)

Abbiamo visto col corollario 11 che, dato un mazzo saturo con s simboli per carta, abbiamo $s^2 - s + 1$ simboli e $s^2 - s + 1$ carte in totale. Sia ora $\odot$ un simbolo qualsiasi. So che $\odot$ appartiene a s carte, disgiunte a meno di $\odot$ stesso. Ho dunque che queste s carte coprono $s(s-1) = s^2 - s$ simboli, cioè tutti i simboli fatta eccezione per $\odot$.

- P3

Suppongo per assurdo che non esistano 4 punti tali che nessuna terna di questi punti giaccia sulla stessa retta. Dimostro che questa affermazione contraddice D2. Siano A, B, C, D quattro punti, assumiamo senza perdita di generalità che B, C, D siano quelli collineari. Siano r, s, t, u le quattro rette *distinte* come nella figura 6. Sia ora E un qualsiasi altro punto. Se dimostriamo che E può appartenere solo alla retta u, otteniamo che le rette non hanno tutte lo stesso numero di punti, che è assurdo per D2, completando la dimostrazione. Dimostro dunque che E non può stare su nessuna tra r, s e t. Assumiamo senza perdita di generalità che E stia su t. Ma allora la quaterna $EBDA$ contraddice l'ipotesi. Assurdo. □

5. OSSERVAZIONI

5.1. Collegamento tra le strutture. Abbiamo costruito una bigezione tra i mazzi di Dobble saturi e i piani proiettivi finiti. Così facendo abbiamo ottenuto una famiglia abbastanza ricca di mazzi di Dobble *divertenti* di cui conosciamo un buon numero di proprietà.

Un primo esempio interessante di proprietà deducibile è la non unicità di struttura di un mazzo saturo di cardinalità fissata. Come al solito, per valutare la struttura sottogiacente a un oggetto dobbiamo essere in grado di raccogliere in

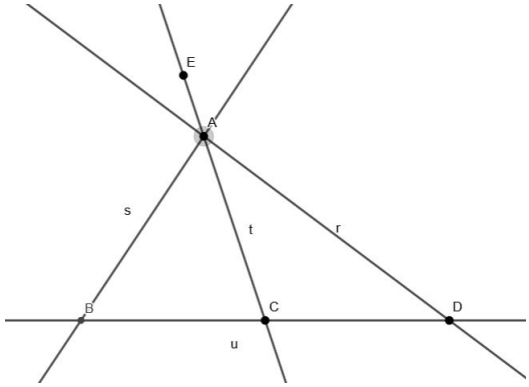


FIGURA 6. visualizzazione mediante punti e rette in $\mathbb{R}^2$ della struttura di incidenza

classi equivalenti oggetti che per noi si assomigliano, in particolare lo facciamo considerando le classi di strutture di incidenza a meno di isomorfismo.

Definizione 14. Chiamiamo **omomorfismo** tra due piani proiettivi $(\mathfrak{P}, \mathfrak{L}, I)$ e $(\mathfrak{Q}, \mathfrak{M}, J)$ una funzione $\sigma\colon \mathfrak{P} \cup \mathfrak{L} \longrightarrow \mathfrak{Q} \cup \mathfrak{M}$ tale che $\sigma(\mathfrak{P}) \subseteq \mathfrak{Q}$, $\sigma(\mathfrak{L}) \subseteq \mathfrak{M}$ e $\forall P \in \mathfrak{P}, \forall l \in \mathfrak{L}, (P,l) \in I \implies (\sigma(P), \sigma(l)) \in J$. Chiamiamo **isomorfismo** di piani proiettivi un omomorfismo tale per cui σ sia bigezione tra $\mathfrak{P}$ e $\mathfrak{Q}$ e tra $\mathfrak{L}$ e $\mathfrak{M}$, e inoltre $\forall P \in \mathfrak{P}, \forall l \in \mathfrak{L}, (P,l) \in I \iff (\sigma(P), \sigma(l)) \in J$.

Una volta fatto ciò, troviamo in [Moorh] che la struttura di piano proiettivo non è unica, neanche fissato l'ordine del piano. Infatti

Teorema 15. *Esistono 4 diversi piani proiettivi di ordine 9 a meno di isomorfismo*

Posso quindi costruire 4 diversi mazzi di Dobble completi con 91 carte. Inoltre

Teorema 16. *Non esistono piani proiettivi di ordine 10*

dunque non è possibile costruire un mazzo di Dobble con 111 carte tale che su ogni carta ci siano 11 simboli,

Sempre in [Moorh] troviamo la tavola dei piani proiettivi di ordine piccolo, accompagnate da due interessanti domande tutt'ora senza risposta: Esistono piani proiettivi finiti con ordine diverso dalla potenza di un primo? Esistono piani proiettivi di ordine primo diversi da quelli classici? Ecco che ci riconduciamo alla domanda senza risposta del paragrafo che segue il corollario 11.

Troviamo inoltre nel bagaglio della geometria d'incidenza un'altra proprietà molto interessante:

Teorema 17. *Se $(\mathfrak{P}, \mathfrak{L})$ è un piano proiettivo, anche il suo duale $(\mathfrak{L}, \mathfrak{P})$ lo è. Inoltre Ogni $\mathbb{PG}^2(\mathbb{F}_{p^n})$ è **isomorfo** al suo duale.*

Alla luce di questo fatto, ci accorgiamo che possiamo dare ai mazzi di Dobble completi una doppia interpretazione come piani proiettivi: possiamo vedere i simboli come punti e le carte come rette, e viceversa possiamo vedere le carte come punti e i simboli che le *attraversano* come rette. Se il piano non è classico,

otteniamo addirittura due diverse strutture. Ecco presentato tramite la dualità, che possiamo considerare una equivalenza logica, un quasi completo ribaltamento semantico!

Siamo ora pronti a rispondere alle domande che ci eravamo posti come obiettivo.

6. CONCLUSIONE

Tramite l'accostamento dei mazzi di Dobble ai piani proiettivi abbiamo risposto alle domande iniziali:

- Il mazzo è completo? Se non lo è, esiste un modo per completarlo? Se sì, quante carte dobbiamo aggiungere?

Risp: Il mazzo di Dobble iniziale non è completo, ma si verifica in modo sperimentale che, in quanto sottostruttura di $\mathbb{PG}^2(\mathbb{F}_7)$, può essere completato aggiungendo le 2 carte mancanti per arrivare a $57 = 7^2 + 7 + 1$.

Il lettore attento noterà che abbiamo un po' sviato nella risposta. Ci si sarebbe infatti ragionevolmente aspettati, a questo punto, la descrizione di un algoritmo di completamento di qualche sorta. La questione dei piani di estensione (pag. 66) generati da mazzi di Dobble non saturi (in quanto *piani parziali*, pag. 6), alquanto delicata, è presentata nel capitolo I, sezione 2.5 di [Stev]. Penso sia rilevante notare che, ai fini del nostro utilizzo, l'algoritmo di completamento si rivela poco utile, sia perchè non preserva in alcun modo l'ordine, sia perchè non è sempre garantita la finitudine del piano proiettivo ottenuto. Alcuni casi particolari riguardo agli algoritmi di completamento sono tutt'ora oggetto di ricerca, come si evince per esempio da [Embed].

Di più facile risposta è invece la seconda domanda.

- Esiste un modo elegante per costruire un mazzo di Dobble *divertente* di cardinalità arbitraria?

Risp: Posso estrarre un mazzo di cardinalità arbitraria dal mazzo di Dobble completo la cui struttura rispecchia quella del $\mathbb{PG}^2(\mathbb{F}_{p^n})$ di cardinalità maggiore più vicina.

7. BIBLIOGRAFIA

[Stev] F.W.Stevenson (1972), Polygonal Publishing House, *Projective Planes*.

[Sandl] A.Albert,R.Sandler (1968), Holt,Rinehart and Winston, *An Introduction to Finite Projective Planes*.

[Sern] E.Sernesi (2000), Bollati Borlinghieri, *Geometria 1 - Seconda edizione riveduta e ampliata*.

[Moorh] E.Moorhouse (2007), *Incidence Geometry*, Si trova online a questo link.

[IntGame] B. Polster, *The intersection Game*, Si trova online a questo link.

[MoTaG] P.Collingridge, *The Matematics of Toys and Games*, Si trova online a questo link.

[HdDW] M.Parker, *How does Dobble (Spot It) work?* Si trova online a questo link.

[Embed] E. Moorhouse, *Embedding finite partial linear spaces in finite translation nets*, Si trova online a questo link.

TOE TAC TIC

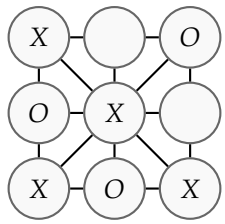
BEATRICE OSTORERO VINCI

Tutti, almeno una volta, hanno giocato a Tris e i più esperti hanno perfino la propria strategia vincente. Ma se vi dicessero di giocare per perdere, sapreste trovare un modo per vincere?

LE REGOLE DEL GIOCO

Cosa significa esattamente "giocare per perdere"? Se nel gioco usuale l'obiettivo di ciascun giocatore è quello di mettere tre simboli in sequenza, in *Tris al contrario* questa situazione corrisponde alla vittoria dell'avversario.

Nel dettaglio, i due giocatori si accordano su una griglia finita di punti e linee e cominciano a giocare a Tris nel modo usuale, apponendo alternativamente il proprio simbolo su un nodo della griglia. Il gioco termina nel momento in cui uno dei due mette tre simboli in fila, oppure non vi sono più nodi disponibili.



Inoltre notiamo che, a seconda del modo in cui si gioca, i possibili esiti della partita risultano essere:

- *Tris normale*: il primo giocatore ha una strategia vincente, oppure entrambi forzano la patta.
- *Tris al contrario*: entrambi i giocatori possono avere una strategia vincente o forzare la patta.

In particolare, in questo secondo caso, quale tra il primo e il secondo giocatore abbia una strategia vincente, dipende dalle proprietà della griglia scelta.

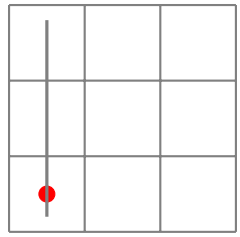
COSTRUZIONE DELLA GRIGLIA

Volendo ora descrivere la griglia su cui ipotizzeremo di giocare, introduciamo alcune definizioni:

Definizione 1. Si definisce *Sistema Triplo di Steiner* di dimensione n, $STS(n)$, una collezione $\mathcal{P}$ di n oggetti, detti punti, e un insieme $\mathcal{L}$ di sottoinsiemi, dette linee, tali che:

- ogni linea è costituita da tre punti
- ogni coppia di punti è contenuta in esattamente una linea.

Si osservi che quel che è stato appena definito ha proprio le caratteristiche della classica scacchiera 3×3 su cui generalmente si gioca. Infatti, si può considerare come "punto" ognuno dei nove quadrati e le "linee" in questo caso sono le righe, le colonne e le diagonali principali.



Definizione 2. Definiamo *Sistema Triplo di Steiner Proiettivo Binario* di dimensione n, $PBSTS(n)$, un sistema Triplo di Steiner di n punti con:

- $n = 2^k - 1$
- $\mathcal{P} = \mathbb{F}_2^k \setminus \{\vec{0}\}$
- $\mathcal{L} = \{\{a, b, c\} : a, b, c \in \mathcal{P},\ a + b + c \equiv 0 \mod 2\}$

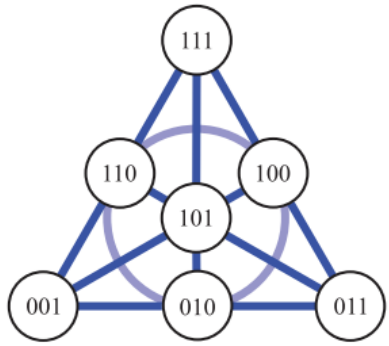
Potrebbe sembrare, dalle proprietà appena elencate, che questa definizione sia ben lontana da quelle che si associano generalmente agli spazi proiettivi, siano essi discreti o meno. Tuttavia, anche se non è stato definito come tale, si tratta effettivamente di uno spazio proiettivo discreto su $\mathbb{F}_2^k$; infatti, sfruttando la costruzione usuale, si andrebbe a considerare il quoziente $\frac{\mathbb{F}_2^k \setminus \{\vec{0}\}}{\{1\}}$, che coincide con tutto $\mathbb{F}_2^k \setminus \{\vec{0}\}$.

Un esempio di $PBSTS(n)$ con $n = 7$ è dato da:

- Punti:
  $\mathcal{P} = \{001, 010, 011, 100, 110, 101, 111\}$
- Linee:

$$\begin{array}{lll} \{001, 010, 011\}, & \{010, 100, 110\}, & \{011, 101, 110\}, \\ \{001, 100, 101\}, & \{010, 101, 111\}, & \{011, 100, 111\}, \\ \{001, 110, 111\}. & & \end{array}$$

Che a livello grafico può essere rappresentato nel seguente modo:



Da questo esempio, osservando la linea $\{010, 100, 110\}$, risulta evidente che l'unica condizione che una linea deve soddisfare è che i tre punti che la costituiscono sommati diano $000 \mod 2$, e non è quindi necessario che questa sia una retta.

Una proprietà importante. Ora che è stata introdotta una griglia finita, siamo interessati ad alcune sue proprietà.

Definizione 3. Si definisce *cap* un sottoinsieme di punti di un STS che non contiene alcuna linea. Inoltre, se tale cap ha la massima dimensione possibile, diremo che è *massimale*.

L'importanza di quest'ultima sottostruttura della griglia sta nel fatto che la sua dimensione limita la durata del gioco e questo risulta particolarmente rilevante alla luce del seguente risultato:

Proposizione. *La massima dimensione di un cap in un* $PBSTS(2^k - 1)$ *è* 2^{k-1} *e un tale cap esiste.*

Nell'esempio precedente si può considerare $\{100, 101, 110, 111\}$, che è un cap, in quanto prendendo 3 punti qualsiasi tra i 4 questi non costituiscono una linea, e, avendo dimensione $2^{3-1} = 4$, è massimale.

In generale, è sempre possibile individuare un cap massimale in un $PBSTS(n)$ scegliendo tra i punti della griglia quelli che hanno la coordinata più a sinistra pari a 1. Infatti, prendendo tre qualsiasi di questi punti e facendone la somma, per la prima coordinata si ottiene $1 + 1 + 1 \equiv 1 \mod 2$; conseguentemente non potranno mai dare una linea. Se poi contiamo quanti punti hanno la coordinata più a sinistra pari a 1, questi risultano essere esattamente 2^{k-1}.

Il fatto che un cap massimale esista in tutte le griglie della tipologia scelta ci garantisce quindi che la durata del gioco sia limitata. Questo non è un grande risultato se inteso semplicemente nel senso che la partita termina in un numero finito di mosse, in quanto i punti a disposizione sono comunque finiti; tuttavia, sfruttando l'esistenza di tale cap, il gioco ha durata limitata e termina con la vittoria di uno dei due giocatori.

GIOCHIAMO!

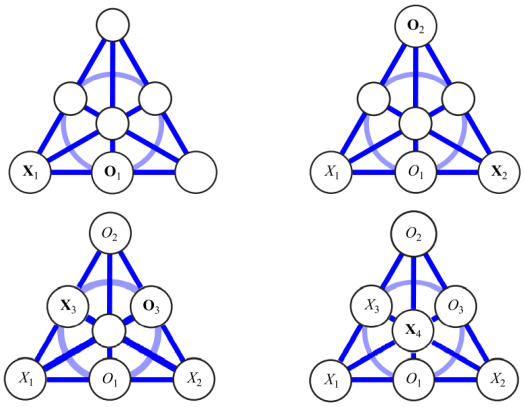
Una strategia sul piano di Fano. Quello che fino a questo momento è stato indicato con $PBSTS(7)$ è il più piccolo STS non banale ed è noto anche come

piano di Fano. Inoltre, risulta essere la griglia più semplice su cui giocare a *Tris al contrario*.

Supponiamo quindi che due giocatori, Xavier e Olivia, si sfidino su tale griglia. Indichiamo con X_i, con O_i le rispettive mosse al turno i, $i \geq 1$: un turno conseguentemente sarà una coppia di mosse (X_i, O_i).

Un esempio di partita può essere il seguente:

- Turno 1: Xavier sceglie il punto X_1 arbitrariamente e lo stesso fa Olivia con O_1.
- Turno 2: Xavier sceglie come sua seconda mossa X_2 l'unico punto che completa la linea su cui stanno X_1 e O_1. Per Olivia, qualunque punto tra i rimanenti forma una linea diversa con ciascuno dei tre già scelti, quindi sceglie O_2 arbitrariamente.
- Turno 3: Xavier sceglie il punto X_3 tra quelli che completano le linee contenenti un punto di Olivia, essendo in questo modo certo di non perdere. A questo punto, Olivia ha due possibili scelte, una delle quali la farebbe perdere: chiamiamo quindi O_3 l'altro punto.
- Turno 4: Xavier non può che scegliere il punto centrale, che forma una linea con X_2, X_3, e in questo modo perde.



Da questo esempio si può intuire che il giocatore per il quale è possibile trovare una strategia vincente sulla griglia scelta è il secondo, ed effettivamente questo è confermato dal seguente risultato.

Teorema. *Il secondo giocatore, Olivia, vince a Tris al contrario seguendo questa strategia:*

(1) Le prime due mosse di Olivia sono arbitrarie.
(2) La terza mossa di Olivia è uno qualunque dei punti che non è $O_1 + O_2$.

Dimostrazione. Olivia gioca per seconda, quindi può arrivare a prendere al massimo 3 punti. Pertanto, può perdere solo se questi formano una linea.

O_1 e O_2 definiscono un'unica linea: $\{O_1, O_2, O_1 + O_2\}$. C'è quindi un unico punto che la può far perdere.

Al momento della terza mossa, Olivia può scegliere tra due punti, di cui al più uno è $O_1 + O_2$. Ne segue che Olivia può sempre scegliere un punto che non la faccia perdere.

Inoltre, se si dividono i punti in due insiemi da 4 e 3 elementi, uno di questi deve contenere una linea, quindi non è possibile che il gioco finisca pari.

Olivia non pareggia, nè perde, quindi vince. □

Giocare su griglie più grandi. Si supponga ora di voler giocare su un $PBSTS$ di dimensione n generica: anche in questo caso è possibile trovare una strategia vincente per Olivia, abbiamo però bisogno di qualche elemento in più.

Definizione 4. Si definisce *sottosistema* di un $PBSTS(2^k - 1)$ un sottoinsieme di punti e linee che costituisca un $PBSTS(2^j - 1)$, $j \leq k$.

Se la dimensione del sottosistema è $2^{k-1} - 1$, si parla di *iperpiano*.

Vale inoltre il seguente risultato:

Proposizione. *Per ogni cap massimale M di un $PBSTS$ con insieme di punti $\mathcal{P}$, $\mathcal{P} \setminus M$ è un iperpiano.*

Come già fatto sul piano di Fano, descriviamo ora una situazione che garantisce la vittoria di Olivia.

Lemma. *Se Olivia riesce a possedere i $\frac{3}{4}$ dei punti di un cap massimale, allora Xavier perde al turno successivo.*

Dimostrazione. Un cap massimale M ha 2^{k-1} punti, quindi i $\frac{3}{4}$ di questi sono $2^{k-2} + 2^{k-3}$. Olivia non può formare una linea con questi punti, perché stanno in un cap.

Contiamo ora i punti che possono essere occupati da Xavier:

- In M può avere al massimo 2^{k-3} punti.
- I punti al di fuori di M costituiscono un iperpiano H.
- In H, un cap massimale ha 2^{k-2} punti. Pertanto, questo è il numero massimo di punti che Xavier può scegliere in H per non perdere.

Quindi sia Xavier che Olivia possiedono $2^{k-2} + 2^{k-3}$ punti e con la successiva mossa, Xavier sceglierà sicuramente un punto che completa una linea, perdendo. □

Valgono una serie di risultati che garantiscono che una situazione del genere possa effettivamente essere raggiunta con un'opportuna sequenza di mosse. E conseguentemente si può concludere che:

Teorema. *Olivia ha una strategia vincente per Tris al contrario giocato su un qualsiasi STS.*

BIBLIOGRAFIA

- David Clark, Sophia Mancini & Jacob Van Hook (2020) Misère Tic-Tac-Toe on Projective Binary Steiner Triple Systems, The American Mathematical Monthly, 127:5, 411-426, DOI: 10.1080/00029890.2020.1715706

COLLANE ROTOLANTI E TRIANGOLI INTERI

IVAN ANDREONI

In queste pagine vedremo come un teorema di teoria dei gruppi (il teorema di Cauchy-Frobenius, trattato nella prima sezione) può essere usato per affrontare problemi di combinatoria.

1. IL TEOREMA DI CAUCHY-FROBENIUS

Consideriamo l'azione di un gruppo G su un insieme X; tratteremo sempre di gruppi e insiemi finiti. Ricordiamo che ad ogni elemento dell'insieme x si associano il suo *stabilizzatore*

$$G_x = \{g \in G : gx = x\}$$

e la sua *orbita*

$$O_x = \{gx : g \in G\}.$$

Indichiamo con X/G l'insieme delle orbite (le orbite partiscono X, così che la notazione è coerente col fatto che questo è a tutti gli effetti un "insieme quoziente"). Ricordiamo inoltre che

$$O_{gx} = O_x, \quad G_{gx} = gG_xg^{-1}.$$

Un noto risultato afferma che la cardinalità di ogni orbita è uguale all'indice dello stabilizzatore di un suo elemento, ovvero

$$|G| = |O_x||G_x|.$$

Definiamo il *carattere di permutazione* associato ad una azione come la quantità, definita per ogni $g \in G$,

$$\chi(g) = |\{x \in X : gx = x\}|,$$

ovvero ad ogni elemento del gruppo è associato il numero di elementi da esso fissati. Osserviamo prima di tutto che questa funzione è invariante sulle classi di coniugio: infatti, dati $g, h \in G$, un $x \in X$ è fissato da g se e solo se hx è fissato da hgh^{-1}, il che dà una biezione tra gli insiemi contati da $\chi(g)$ e $\chi(hgh^{-1})$.

Teorema 1 (Cauchy-Frobenius)**.** *Il numero di orbite è pari alla media del carattere di permutazione, ovvero*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

Dimostrazione. Consideriamo l'insieme

$$\{(g, x) : gx = x\} \subseteq G \times X.$$

La cardinalità di questo insieme può essere contata "per righe" o "per colonne", il che dà l'uguaglianza delle due quantità

$$\sum_{x \in X} |G_x| = \sum_{g \in G} \chi(g).$$

Raccogliendo in orbite la somma a sinistra si ha che

$$\sum_{g \in G} \chi(g) = \sum_{O \in X/G} \sum_{x \in O} |G_x| = \sum_{O_x \in X/G} |O_x||G_x| = \sum_{O_x \in X/G} |G| = |X/G||G|$$

e la tesi segue. □

Vedremo come questo teorema ha delle interessanti applicazioni in combinatoria: se ne fa uso quando bisogna contare delle classi di equivalenza che si riescono ad esprimere come indotte da una azione di gruppo.

2. COLLANE ROTOLANTI

Fissimao due numeri n e k. Una *collana* è data da n perline di k colori diversi, disposte su un filo chiuso. Matematicamente, potremmo dire che una collana è una funzione

$$\{1, \dots n\} \to \{1, \dots k\}$$

che alla m-sima perlina associa un certo colore. Questa definizione ci dà una descrizione "facile" dell'insieme delle collane (che, in particolare, avrà quindi cardinalità k^n) ma c'è un problema: vengono considerate diverse collane che in realtà sono uguali: per esempio, due collane da tre perline "bianco-nero-bianco" e "nero-bianco-bianco" sono in verità la stessa collana, una volta che questa viene chiusa e le perline possono girare liberamente sul filo. Quindi la domanda interessante è: *quante classi di equivalenza di collane di n perline di k colori ci sono?*

Sull'insieme delle collane agisce in modo naturale il gruppo ciclico di ordine n $\mathbb{Z}_n$ (che consideriamo come gruppo additivo); si tratta proprio dell'azione di "far girare" la collana. Più formalmente, alla collana-funzione f e ad $a \in \mathbb{Z}_n$ si associa

$$af : m \mapsto f(m + a)$$

con $m + a$ considerato modulo n. Questa è proprio l'azione di cui abbiamo bisogno: le orbite raccolgono insieme le collane equivalenti. Per rispondere alla nostra domanda, possiamo perciò utilizzare il teorema di Cauchy-Frobenius, calcolando il carattere di permutazione degli elementi di $\mathbb{Z}_n$.

Cominciamo dall'elemento neutro 0. Tutte le collane sono fissate da esso, e perciò

$$\chi(0) = k^n.$$

Consideriamo ora il generatore del gruppo ciclico 1. Una collana fissata da 1 è una collana che rimane invariata se le perline vengono ruotate di 1: un fatto che può accadere solo se le perline sono tutte dello stesso colore. Le collane di questo tipo sono tante quante i colori, e

$$\chi(1) = k.$$

Consideriamo ora un m che divide n, e una collana fissata da m. Possiamo immaginare di dividerla in m/n sezioni, ognuna lunga m perline. Applicando una rotazione di m, queste sezioni ruotano una sull'altra. Perciò, perché la collana sia fissata, possiamo immaginare di colorare a piacere la prima sezione, e colorare di conseguenza le altre, ripetendo gli stessi colori. Questo significa fare m scelte di colore, e si ha che

$$\chi(m) = k^m.$$

Si noti che in questo caso ricadono coerentemente i due considerati prima (considerando che $0 = n$).

Per considerare il caso generico, facciamo una osservazione che riguarda la generica azione di un gruppo G su un insieme X, dalla dimostrazione immediata.

Osservazione 2. Un $x \in X$ è fissato da $g \in G$ se e solo se è fissato da ogni $g^n \in \langle g \rangle$.

Il corollario, immediato ma interessante, è che il carattere di permutazione $\chi(g)$ dipende solo dal gruppo ciclico generato da g, e può essere calcolato scegliendo un altro generatore.

Nel nostro caso, dato $m \in \mathbb{Z}_n$, sfruttiamo il seguente fatto.

Lemma 3. *Il gruppo ciclico generato da $m \in \mathbb{Z}_n$ è lo stesso generato da (m, n).*

Dimostrazione. Dal fatto che m è multiplo di (m, n) segue una inclusione. Per l'altra, consideriamo l'identità di Bezout per scrivere (con a, b interi)

$$(m, n) = am + bn \equiv am \pmod{n},$$

da cui segue che (m, n) è nel gruppo generato da m. □

Per i ragionamenti fatti sopra, possiamo perciò concludere che, per un generico $m \in \mathbb{Z}_n$

$$\chi(m) = \chi((m, n)) = k^{(m,n)}.$$

Abbiamo perciò tutti gli ingredienti necessari per applicare la formula di Cauchy-Frobenius, ottenendo la formula

$$\text{numero di collane } = \frac{1}{n} \sum_{m=1}^{n} k^{(m,n)}.$$

Questa espressione si può migliorare; la cosa da fare è raccogliere insieme gli elementi con lo stesso MCD, e reindicizzare la formula sui divisori di n, ottenendo

$$\frac{1}{n} \sum_{d|n} \left[k^d \sum_{m:\,(m,n)=d} 1 \right].$$

l'insieme contato dalla somma interna ammette una espressione esplicita: infatti, i numeri interi $1 \leq m \leq n$ con $(m, n) = d$ sono in corrispondenza (dividendo per d) con gli $1 \leq m' \leq n/d$ con $(m', n/d) = 1$. Questi sono perciò $\varphi(n/d)$, con φ la funzione di Eulero. Si ha perciò

$$\text{numero di collane} = \frac{1}{n} \sum_{d|n} k^d \varphi(n/d).$$

Val la pena riflettere un attimino su ciò che abbiamo fatto. Quello che abbiamo sfruttato in maniera importante è il fatto che $\mathbb{Z}_n$ sia un gruppo ciclico: il che ha

reso l'applicazione dell'osservazione particolarmente fruttuosa, dato che i sottogruppi ciclici di $\mathbb{Z}_n$ e le cosine connesse sono ben note. Questo ci ha permesso di ricondurci a calcolare $\chi(d)$ solo per i divisori di n, semplificandoci notevolmente la vita. Vale in effetti in generale che, nell'azione di $\mathbb{Z}_n$ su un insieme,

$$\text{numero di orbite} = \frac{1}{n}\sum_{d|n}\chi(d)\varphi(n/d).$$

Noi ci fermiamo qui, ma va detto che la stessa formula si poteva ottenere per altre vie, e che non si limita a risolvere il nostro problemino di combinatoria, ma ha dei legami con la "matematica vera" (l'autore ha sentito raccontare queste cose in un seminario nella seconda edizione di Fuori Orario...). Per chi fosse interessata ad approfondire, una buona parola chiave da cui iniziare sono i "polinomi di Moreau".

3. TRIANGOLI INTERI

La domanda a cui vogliamo rispondere in questa sezione è *quanti sono i triangoli di lati interi e dato perimetro?*

Ancora una volta, partiamo da un insieme "facile" che opportunamente quozientiamo. Chiamiamo

$$T_n = \{a_1, a_2, a_3 \in \mathbb{N} : 1 \leq a_i < n/2, a_1 + a_2 + a_3 = n\}.$$

Questo insieme raccoglie le triple di numeri che si chiudono in un triangolo di perimetro n: ancora una volta, il problema è che permutando i lati si ottiene "lo stesso triangolo", e per rispondere alla nostra domanda ciò che dobbiamo contare è la cardinalità dell'insieme quoziente: in questo caso, rispetto alla azione di S_3. Qui calcoleremo solo il caso di perimetro pari: il caso dispari è analogo (rimandiamo alla bibliografia per la sua trattazione)

Teorema 4. *I triangoli interi di perimetro $2k$ sono pari al numero intero più vicino a $k^2/12$.*

Il primo passo è calcolare la cardinalità di T_n. Da qui in avanti, supponiamo di avere $n = 2k$ pari.

Lemma 5. *Se $n = 2k$ è pari, $|T_n| = \binom{k-1}{2}$.*

Dimostrazione. Definiamo gli insiemi (per $i = 1, 2, 3$)

$$T'_h = \{a_1, a_2, a_3 \in \mathbb{N} : a_1 + a_2 + a_3 = h\},$$
$$T^i_n = \{a_1, a_2, a_3 \in \mathbb{N} : a_1 + a_2 + a_3 = n, a_i \geq n/2\}$$

e constatiamo che

$$|T_n| = |T'_n| - 3|T^1_n|.$$

La cardinalità di T'_h si calcola con un facile argomento di "stars and bars", ottenendo

$$|T'_h| = \binom{h-1}{2}.$$

Considerando una tripla in T^i_{2k}, la sostituzione $a_i \mapsto a_i - k + 1$ dà una biezione tra T^i_{2k} e T'_{k+1}, da cui

$$|T^i_{2k}| = |T'_{k+1}| = \binom{k}{2}.$$

Da ciò si ottiene

$$|T_n| = \binom{2k-1}{2} - 3\binom{k}{2} = \binom{k-1}{2}$$

(svolgendo i dovuti calcolini...), ovvero la tesi. □

Tutto questo insieme è fissato dall'identità, e abbiamo perciò calcolato $\chi(1)$. Per gli altri calcoli, sfruttiamo il fatto che χ sia costante sulle classi di coniugio: lavorando su S_3, le classi di coniugio coincidono con le possibili strutture cicliche, e ci basta calcolare $\chi((1\,2))$ e $\chi((1\,2\,3))$. Quest'ultimo è il più facile: un triangolo rimane invariante sotto l'azione di un 3-ciclo se e solo se i tre lati sono uguali: il che ammonta ad un caso solo (la tripla $(n/3, n/3, n/3)$) che è presente se e solo se n è divisibile per tre. Scriviamo

$$\chi(1\,2\,3) = [0/1]$$

per indicare un numero che potrebbe essere zero o uno a seconda dei casi.

Per calcolare $\chi(1\,2)$, consideriamo un triangolo fissato da questo scambio, ovvero con $a_1 = a_2$. Si ha perciò

$$1 \leq a_3 = 2k - 2a_1 \leq k - 1,$$

da cui

$$\frac{k+1}{2} \leq a_1 \leq k - 1.$$

Questo significa avere

$$\frac{k - [1/2]}{2}$$

scelte per a_1, e altrettanti triangoli (ancora, $[1/2]$ indica un numero che potrebbe essere 1 oppure 2).

Mettendo insieme tutto ciò, si ottiene che il numero di orbite nel caso $n = 2k$ è pari a

$$\begin{aligned}\frac{1}{6}[\chi(1) + 3\chi(1\,2) + 2\chi(1\,2\,3)] &= \frac{1}{6}\left(\frac{k^2 - 3k + 2}{2} + 3\frac{k - [1/2]}{2} + 2[0/1]\right) \\ &= \frac{k^2}{12} + \frac{1}{6} - \frac{1}{4}[1/2] + \frac{1}{3}[0/1].\end{aligned}$$

La quantità che oscilla a seconda dei casi (data i termini con le parentesi quadre) varia fra $-1/2$ e $1/12$, e si ha

$$\frac{k^2}{12} - \frac{1}{3} \leq \text{n. orbite} \leq \frac{k^2}{12} + \frac{1}{4}.$$

In questo intervallo di incertezza c'è al più un numero intero, che risulterà essere il numero intero più vicino a $k^2/12$. Questo dimostra il teorema.

Anche in questo caso, val la pena notare come per semplificare i calcoli si è sfruttata la struttura del gruppo. In questo caso, la proprietà che si è sfruttata è

coincidenza fra classi di coniugio e possibili strutture cicliche, tipica proprietà dei gruppi simmetrici (i gruppi di permutazione S_n).

BIBLIOGRAFIA

- I.M. Isaacs, *Algebra, a graduate course*, American Math. Soc. (2009)
- J. East & R. Niles, *Integer Triangles of Given Perimeter: A New Approach via Group Theory*, The American Mathematical Monthly, 126:8 (2019), 735-739

QUANDO LA PROBABILITÀ INCONTRA L'ALGEBRA ASTRATTA

FILIPPO BERETTA

1. INTRODUZIONE

Nell'ambito dei gruppi finiti si può essere spesso tentati di studiare la probabilità che alcuni elementi commutino, o ancora siano preservati da automorfismi. Questo approccio fornisce risultati soddisfacenti che, come si vedrà, permettono di rispondere a domande non banali in teoria dei gruppi.

2. PRELIMINARI E DEFINIZIONI

In tutta la trattazione si assume che G sia un gruppo finito. Per prima cosa si ricordano alcuni concetti relativi al coniugio. In particolare alcune definizioni.

Definizione 1. Due elementi $x, y \in G$ si dicono coniugati se $\exists g \in G$ tale che $y = g^{-1}xg$. Viene detto automorfismo interno indotto da g la mappa $T_g : x \to g^{-1}xg$. In ultimo, si dice classe di coniugio dell'elemento x

$$Cl(x) = \{\alpha(x) | \alpha \in Inn(G)\}$$

Dove $Inn(G)$ è l'insieme degli automorfismi interni. Si indice con $k(G)$ il numero di classi di coniugio di G.

Definizione 2. Si dice centro di G, indicato con $Z(G)$, il sottogruppo di G

$$Z(G) = \{x \in G | \, yx = xy \ \ \forall y \in G\}$$

Ovviamente, $x \in Z(G) \iff Cl(x) = \{x\}$.

Definizione 3. Si dice grado di commutatività di G, denotato $P(G)$, la probabilità che due elementi scelti a caso e con rimpiazzo, in un gruppo finito, commutino. Fissato $D = \{(x, y) \in G \times G | \, yx = xy\}$, allora

$$P(G) = \frac{|D|}{|G|^2}$$

In modo del tutto analogo a quanto fatto finora, si può discutere della presenza di automorfismi che fissino un dato elemento. In particolare

Definizione 4. Dato $x \in G$, si definisce classe di fusione di x l'insieme $F(x) = \{\alpha(x) | \alpha \in Aut(G)\}$. Si indica con $f(G)$ il numero di classi di fusione di G.

Definizione 5. Si dice centro assoluto di G, indicato con $L(G)$, il sottogruppo di G

$$L(G) = \{x \in G | \alpha(x) = x \ \ \forall \alpha \in Aut(G)\}$$

Ovviamente, $x \in L(G) \iff F(x) = \{x\}$.

Definizione 6. Si dice grado di autocommutatività di G, denotato $P_A(G)$, la probabilità che, scelti a caso un elemento di G ed un automorfismo, l'automorfismo fissi l'elemento. Preso $E = \{(x, \alpha) \in G \times Aut(G) | \alpha(x) = x\}$, allora

$$P_A(G) = \frac{|E|}{|G||Aut(G)|}$$

Osservazione 7. La definizione di $P(G)$ è del tutto analoga a quella di $P_A(G)$ sostituendo $Imm(G)$ ad $Aut(G)$.

3. ELEMENTI FISSATI DAL CONIUGIO

La definizione data precedentemente di $P(G)$ è certo intuitiva, ma poco pratica nei calcoli. Vale tuttavia la seguente proposizione

Proposizione 8.

$$P(G) = \frac{|D|}{|G|^2} = \frac{k(G)}{|G|}$$

Dimostrazione. Per prima cosa, si osservi che

$$|D| = \sum_{x \in G} |C_G(x)|$$

Dove $C_G(x) = \{a \in G | \, ax = xa\}$ è il centralizzante di x, semplicemente spezzando sui singoli elementi. Ora, se x, y sono coniugati, si trovano nella stessa orbita rispetto all'azione di coniugio, per cui gli stabilizzatori $C_G(x)$ e $C_G(y)$ sono coniugati. Allora $|C_G(x)| = |C_G(y)|$. Vale quindi che se due elementi sono coniugati, i loro centralizzanti hanno la stessa cardinalità. Ricordando che $|Cl(x) = |G|/|C_G(x)|$, segue allora che

$$|D| = \sum_{t=1}^{k(G)} |Cl(x)||C_G(x)| = \sum_{t=1}^{k(G)} |G| = k(G)|G|$$

Da cui la tesi. □

Si noti che quanto appena dimostrato è in realtà una applicazione del Teorema di Cauchy-Frobenius. Possiamo allora enunciare il primo risultato notevole di questa discussione.

Teorema 9. *Per un gruppo G finito non abeliano, $P(G) \leq \frac{5}{8}$*

Dimostrazione. Si fa uso dell'equazione delle classi: si ha che

$$|G| = |Z| + |C_1| + ... + |C_t|$$

Dove $\{C_j\}_{j=1}^t$ sono classi di coniugio non banali, e t un indice fissato. Ciò vale poiché l'azione di coniugio divide G in orbite distinte. Segue quindi che $k(G) =$

$t + |Z|$ è il numero di classi di coniugio, dal momento che ogni elemento nel centro costituisce una classe di coniugio a sé. Poiché $\forall j\ |C_j| \geq 2$,

$$t \leq \frac{|G| - |Z|}{2}$$

Da cui $k(G) \leq |G|/2 + |Z|/2$. Ora, poiché G non è abeliano, G/Z non è ciclico. Questa affermazione, di carattere generale, si può verificare facilmente per contronominale (e viene lasciata per esercizio al lettore).
Usando ciò, si può affermare che $|G/Z| \geq 4$, da cui $|Z| \leq |G|/4$, per cui in ultimo

$$k(G) \leq \frac{|G|}{2} + \frac{|G|}{8} = \frac{5}{8}|G|$$

□

Osservazione 10. Il bound è stretto, ovvero esistono degli insiemi tali per cui $P(G) = 5/8$. In particolare, preso Q_8 il gruppo dei quaternioni, vale che $P(Q_8) = 5/8$.

Dimostrazione. Si ricordi che i quaternioni possono essere scritti come $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, in modo che $i * i = -1$ e così pure per j e k. Inoltre, $i * j = k, j * k = i, k * i = j$. Una verifica diretta mostra che $Z(Q_8) = \{1, -1\}$, mentre $Cl(i) = \{i, -i\}$, $Cl(j) = \{j, -j\}$, ... Si conclude che $|G| = 8$, $k(G) = 5$, da cui la tesi. □

In effetti Q_8 è un caso particolare di un risultato più generale, ovvero che

Proposizione 11. *Sia dato un gruppo G finito non abeliano. Se $|G/Z(G)| = 4$, allora $P_G = 5/8$.*

Dimostrazione. Si prendano 2 elementi $a_1, a_2 \in G$ tali che $a_1 a_2 \neq a_2 a_1$. Allora vale che $G/Z(G) = \{Z(G), a_1 Z(G), a_2 Z(G), a_3 Z(G)\}$, dove $a_3 = a_1 a_2$ (perché questi elementi sono certamente in classi diverse). Si ha allora che

$$|D| = |\{(x, y) \in G \times G | yx = xy\} = |\{(x, y) | x \in Z(G), y \in G\}| +$$
$$+ \sum_{i=1}^{3} |\{(x, y) | x \in a_i Z(G), y \in Z(G)\}| + \sum_{i=1}^{3} |\{(x, y) | x \in a_i Z(G), y \in a_i Z(G)\}|$$
$$= |G||Z(G)| + 6|Z(G)|^2 = |G|^2/4 + 6|G|^2/16 = 5|G|^2/8$$

Da cui la tesi. □

4. ELEMENTI FISSATI DA AUTOMORFISMI

In analogia con il caso precedente, è possibile provare che

Proposizione 12. *Dato G un gruppo finito, vale che*

$$P_A(G) = \frac{|E|}{|G||Aut(G)|} = \frac{f(G)}{|G|}$$

Si veda [3] per una referenza dettagliata. Segue allora che

Corollario 13. *Se G è un gruppo non abeliano, $P_A(G) \leq 5/8$*

Dimostrazione. E' sufficiente osservare che $f(G) \leq k(G)$, poiché gli autormorfismi interni sono particolari automorfismi, ed applicare le osservazioni precedenti. □

E' tuttavia possibile generalizzare questo risultato, come viene espresso nel prossimo teorema.

Teorema 14. *Sia G un gruppo finito non ciclico. Allora* $P_A(G) \leq 5/8$.

Dimostrazione. La dimostrazione è analoga a quella del **Teorema 9**, sostituendo $L(G)$ a $Z(G)$ e $f(G)$ a $k(G)$. La sola differenza nasce dal fatto che G non ciclico non implica G/Z non ciclico (al contrario del caso abeliano). Vale tuttavia il seguente lemma

Lemma 15. *Sia G un gruppo finito. Allora G è ciclico se e solo se* $G/L(G)$ *è ciclico. Più in generale, se* $G/L(G) \simeq C_n$, *allora* $G \simeq C_{2n}$ *se n pari, mentre* $G \simeq C_{2n}$ *o* $G \simeq C_n$ *se n dispari.*

Utilizzando il lemma, la dimostrazione segue in modo analogo al **Teorema 9**. Per una dimostrazione del lemma, si veda [4], (Th 2.2). □

Viene ora naturale domandarsi cosa succeda nel caso di un gruppo G ciclico. Vale in particolare questo risultato.

Teorema 16. *Sia* $G \simeq C_n$. *Allora* $P_A(G) \geq 5/8$ *se e solo se* $G \simeq C_2$,C_3,C_4 *o* C_6.

Dimostrazione. Per prima cosa, si studiano i casi particolari: se $G \simeq C_2$, allora vi è un solo automorfismo di gruppo, l'identità, per cui $f(G) = 2$, e $P_A(G) = 1$. Se poi $G \simeq C_3$, una verifica diretta mostra che $f(C_3) = 2$, da cui $P_A(C_3) = 2/3$. Per quanto riguarda C_4, si ricordi che $Aut(C_4, *) \simeq (U_4, \cdot) \simeq C_2$, dove $(U_n, \cdot)$ è il gruppo moltiplicativo di $(Z_n, +, \cdot)$. Segue allora $P_A(C_4) = 3/4$. In modo analogo, si mostra che $P_A(C_6) = 2/3$. Per l'implicazione inversa, si scriva $n = p_1^{a_1}...p_r^{a_r}$, dove $p_1 < p_2 < ... < p_r$ sono primi distinti e a_i interi positivi. Allora $G \simeq G_1 \times ... \times G_r$, dove i G_i sono dei p_i-sottogruppi di Sylow ciclici. Come riportato in [3] (p.262-263), è possibile mostrare che $P_A(G) = P_{A_1}(G_1)...P_{A_r}(G_r)$, dove A_i è il gruppo degli automorfismi di G_i. Sempre da [3] segue che

$$P_A(G) = \frac{a_1 + 1}{p_1^{a_1}} \ ... \ \frac{a_r + 1}{p_r^{a_r}}$$

Per induzione si verifica facilmente che per ogni n naturale,

$$\frac{n+1}{p^n} \leq \frac{2}{p}$$

Per quanto appena visto, se $r \geq 3$,

$$P_A(G) \leq \frac{2^r}{p_1 p_2 ... p_r} \leq \frac{2 \cdot 2 \cdot 2}{2 \cdot 3 \cdot 5} < \frac{5}{8}$$

Se poi $r = 2$, $P_A(G) \geq 5/8$ implica che

$$\frac{a_1 + 1}{p_1^{a_1}} \frac{a_2 + 1}{p_2^{a_2}} \geq \frac{5}{8}$$

Questa disuguaglianza è verificata se e solo se $a_1 = a_2 = 1$, $p_1 = 1$, $p_2 = 3$. Allora $G \simeq C_2 \times C_3 \simeq C_6$. In ultimo, se $r = 1$, la disuguaglianza $\frac{a_1+1}{p_1^{a_1}} \geq \frac{5}{8}$ è verificata se e solo se $G \simeq C_2$, C_3 o C_4. □

Da quanto visto seguono alcuni ovvi corollari.

Corollario 17. *Per ogni gruppo G finito, $P_A(G) = 3/4$ se e solo se $G \simeq C_4$.*

Corollario 18. *Per ogni gruppo G finito, $P_A(G) = 2/3$ se e solo se $G \simeq C_3$ o $G \simeq C_6$.*

5. $\nexists$ G TALE CHE $P_A(G) = 5/8$

Per mostrare questo risultato notevole, si farà uso del seguente lemma. La dimostrazione è presentata in [4] (Th. 3.1).

Lemma 19. *Sia G un gruppo finito tale che $G/L(G) \simeq C_2 \times C_2$. Allora G è isomorfo ad uno dei seguenti gruppi: $C_2 \times C_2$, $C_4 \times C_2$, il diedrale D_8 di ordine 8, Q_8 o il gruppo $G_1 = \langle x, y | x^4 = y^4 = 1, y^{-1}xy = x^{-1} \rangle$*

E' ora possibile procedere nella dimostrazione. Per prima cosa, un lemma

Lemma 20. *Se G è un gruppo finito con $P_A(G) = 5/8$, allora $|G/L(G)| \leq 4$.*

Dimostrazione. Se per assurdo si avesse $|G/L(G)| > 4$, allora

$$\frac{5}{8} = P_A(G) = \frac{f(G)}{|G|} = \frac{|L(G)|}{|G|} + \frac{f(G) - |L(G)|}{|G|} < \frac{1}{4} + \frac{f(G) - |L(G)|}{|G|}$$

Da cui

$$|L(G)| < f(G) - \frac{3}{8}|G|$$

Inoltre, dall'equazione delle classi (di fusione), segue che

$$\frac{|G| - |L(G)|}{2} \geq r = f(G) - |L(G)|$$

Dove r è il numero di classi di fusione non banali. Si ottiene quindi che $2f(G) - |G| \leq |L(G)|$. Combinando le relazioni, si ottiene che $2f(G) - |G| < f(G) - \frac{3}{8}|G|$. Quindi $P_A(G) = f(G)/|G| < 5/8$, il che è assurdo. □

Teorema 21. *Non esiste un gruppo finito G per cui $P_A(G) = 5/8$.*

Dimostrazione. Sia G con $P_A(G) = 5/8$. Allora $|G/L(G)| \leq 4$. Se $|G/L(G)| \leq 3$, allora per il **Lemma 15**, G è isomorfo ad un gruppo ciclico di ordine 2,3,4,6. Tutti questi casi sono stati studiati precedentemente, e per nessuno di essi $P_A(G) = 5/8$. Sia allora $|G/L(G)| = 4$, per cui $G/L(G) \simeq C_4$ o a $C_2 \times C_2$. Se $G/L(G) \simeq C_4$, allora $G \simeq C_8$. Studiandolo come in precedenza, si prova che $f(C_8) = 4$, da cui $P_A(C_8) = 1/2$. Se $G/L(G) \simeq C_2 \times C_2$, si applica il **Lemma 20**, per cui G deve essere isomorfo ad uno tra $C_2 \times C_2$, $C_4 \times C_2$, D_8, Q_8 o $G_1 = \langle x, y | x^4 = y^4 = 1, y^{-1}xy = x^{-1} \rangle$. Tutti questi casi vengono analizzati singolarmente in [1], e si conclude che per nessuno di essi vale che $P_A(G) = 5/8$. □

6. CONSEGUENZE, APPROFONDIMENTI

Utilizzando i risultati precedenti, è facile dimostrare che

Teorema 22. *Sia G un gruppo finito. Allora sono equivalenti:*
(1) $Aut(G) = Aut_c(G)$
(2) $P_A(G) = P(G)$
(3) $k(G) = f(G)$
Dove $Aut_c(G)$ è il sottogruppo degli automorfismi che preservano le classi di coniugio. Ovviamente $Inn(G)$ è contenuto in $Aut_c(G)$.

Dimostrazione. L'equivalenza tra (2) e (3) è ovvia per quanto già visto. Resta da provare quella tra (1) e (3). Si supponga prima che $k(G) = f(G)$. Se esistesse un $x \in G$ per cui $Cl(x) \neq F(x)$, allora esiste un $y \in F(x)/Cl(x)$. Ma allora si avrebbe che $F(x)$ è unione di più classi di coniugio, per cui $f(x) < k(x)$, assurdo. Allora per ogni x, $Cl(x) = F(x)$. Sia $\alpha \in Aut(G)$. Allora $\alpha(x) \in F(x) = Cl(x)$. Quindi, $\alpha \in Aut_c(G)$, da cui si conclude questa implicazione.
Sia invece $Aut(G) = Aut_c(G)$. Per un certo x, si prenda $y \in F(x)$. Allora esiste $\alpha \in Aut(G)$ per cui $\alpha(x) = y$. Poiché α preserva le classi, $y \in Cl(x)$, da cui $F(x) = Cl(x)$. Da ciò, segue la tesi. □

Questo teorema è molto maneggevole, e permette di ottenere alcuni risultati interessanti in teoria dei gruppi. Si noti per esempio il seguente corollario.

Corollario 23. *Sia G un gruppo finito per cui $G/Z(G) \simeq C_2 \times C_2$. Allora $Aut(G) \neq Aut_c(G)$.*

Dimostrazione. Per la **Proposizione 11**, $P(G) = 5/8$. Tuttavia, per il **Teorema 21**, non esiste G per cui $P_A(G) = 5/8$. Allora dal teorema appena dimostrato segue che $Aut(G) \neq Aut_c(G)$. □

Lo studio di gruppi dove siano presenti automorfismi che non preservano le classi di coniugio gode di un certo interesse in teoria dei gruppi ed è spesso non banale, motivo per cui questo approccio può risultare molto efficace.

BIBLIOGRAFIA

- A. Goyal, H. Kalra, D. Gumber. *On the probability that an automorphism fixes a group element*. Amer. Math. Monthly, 126(8):748-753.
- W. H. Gustafson. *What is the probability that two elements commute?*. Amer. Math. Monthly, 80(9):1031-1034.
- G. J. Sherman. *What is the probability that two group elements commute?* Amer. Math. Monthly, 82(3):261-264.
- M. Chaboksavar, M. Farrokhi, F. Saeedi. *Finite groups with a given absolute central factor group* Arch. Math, 102(5):401-409.

L'ULTIMO TEOREMA DI FERMAT...NEI CAMPI FINITI

PAOLO SOMMARUGA

1. PRIME CONSIDERAZIONI

Ricordiamo innanzitutto l'ultimo teorema di Fermat nella sua versione originale:

Teorema 1 (Ultimo Teorema di Fermat)**.** *Non esistono soluzioni intere positive all'equazione* $a^n + b^n = c^n \ \forall n > 2$

L'attuale dimostrazione di Wiles comprende tecniche talmente avanzate che pochi matematici sono in grado di comprenderla; quello che faremo qui è invece di chiederci cosa succede nei campi di p elementi, con p primo.

Bastano in realtà semplici considerazioni per vedere che l'ultimo teorema di Fermat non vale per i campi finiti:

Esempio 2. Poniamo per esempio $a = b = 1$, ci servono allora $c \in \mathbb{F}_p$ (per qualche p primo) ed $n \in \mathbb{N}$ tali che $c^n = 2$. Ad esempio scegliamo $c = 2$, fissiamo poi p e guardiamo 2 in $\mathbb{F}_p$. Se chiamiamo k il suo periodo rispetto alla moltiplicazione, allora per $n = mk + 1$ con $m \in \mathbb{N}$ l'equazione è banalmente soddisfatta perchè appunto $2^{mk+1} = 2$ per come è stato scelto k.

Esempio 3. Sempre fissando un p primo, sappiamo che l'elevamento alla p (o automorfismo di Frobenius) è un automorfismo di campi, e così tutte le sue iterate (ovvero elevamenti a p^n). Dunque $\forall x, y, z \in \mathbb{F}_p$ tali che $x + y = z$ e $\forall n \in \mathbb{N} - \{0\}$ vale $x^{p^n} + y^{p^n} = z^{p^n}$ (infatti vale che $\forall x, y \in \mathbb{F}_p \ (x + y)^{p^n} = x^{p^n} + y^{p^n}$, come facile applicazione della formula del binomio di Newton).

In realtà per queste prime considerazioni sparse non occorre neanche porsi un $\mathbb{F}_p$, ma si possono fare considerazioni anche in $\mathbb{Z}/n\mathbb{Z}$ per qualsiasi n:

Esempio 4. Il primo esempio non ha niente a che vedere con i primi e dunque vale in qualsiasi $\mathbb{Z}/n\mathbb{Z}$.

Esempio 5. Più in generale presi $a, b, c, n \in \mathbb{N}$ qualsiasi, detto $z := a^n + b^n - c^n$ ed m un divisore di z tale che non divida nè a, nè b, nè c, allora chiaramente $z \equiv 0 \mod m$ e dunque $a^n + b^n = c^n$ in $\mathbb{Z}/m\mathbb{Z}$.

Vogliamo ora però fornire un risultato un po' più elegante, che si basa sulla teoria dei grafi (in particolare la teoria di Ramsey), ottenuto da Shur nel 1916.

2. TEOREMA DI RAMSEY

Il teorema di Ramsey afferma che in ogni grafo completo abbastanza grande e con colorazioni sui lati è possibile trovare un sottografo completo monocromatico di grandezza fissata.

Definizione 6. Un grafo è una coppia di insiemi V ed E rispettivamente di vertici e lati fra di essi (che vengono indicati con coppie di vertici). Considereremo qui grafi non orientati (ovvero coppie non ordinate). Un grafo è detto completo se per ogni coppia di vertici c'è un lato che li connette.

Dato un grafo su n vertici, si dice colorazione del grafo con c colori una funzione $f : E \longrightarrow \{1, ..., c\}$, dove E è l'insieme dei lati del grafo.

Teorema 7 (Ramsey)**.** *Per ogni $k \in \mathbb{N}$ e per ogni c numero di colori, esiste $n \in \mathbb{N}$ tale che, per ogni colorazione dei lati di un grafo completo di n vertici con c colori, esiste un sottografo completo di k vertici i cui lati sono colorati tutti nello stesso modo. Chiameremo $r_c(k)$ il minimo n per cui ciò accade.*

Dimostrazione. La dimostrazione è per induzione sul numero di colori c:

Per $c = 1$ è ovvio, infatti $r_1(k) = k$ (Il grafo stesso è un sottografo completo monocromatico). Ci serve dimostrare anche il caso con $c = 2$, infatti il caso generale si baserà su quello.

Per $c = 2$ procedo per induzione su k. Il passo base è ovvio: un grafo con 1 verice non ha lati e un grafo completo su 2 vertici è composto da un lato, che deve avere un certo colore e dunque è esso stesso il sottografo cercato. Mostro quindi che $r_2(k) \leq 2r_2(k-1)$ (il membro di destra è ben definito per ipotesi induttiva).

Etichetto i due colori con a e b. Preso un grafo G con $2r_2(k-1)$ vertici, e mostro che esso ha al suo interno un sottografo completo di k vertici monocromatico.

Considero un vertice v e divido l'insieme dei vertici di G (escluso v) in due insiemi A e B, con A l'insieme dei w tali che il lato $\{v, w\}$ è colorato con a e B l'insieme dei vertici w tali che il lato $\{v, w\}$ è colorato con b. Si ha dunque che $|A| + |B| + 1 = 2r_2(k-1)$ (infatti poichè il grafo è completo, ogni vertice diverso da v ha un lato che lo connette a v e dunque deve stare in A o in B), da cui segue banalmente che vale uno tra $r_2(k-1) \leq |A|$ e $r_2(k-1) \leq |B|$.

Supponendo che valga la prima, allora nel sottografo indotto da A (ovvero il grafo che ha per vertici gli elementi di A e per lati tutti i lati di G con estremi in A) c'è un sottografo completo di k-1 vertici e con lati tutti colorati con a. Tutti questi vertici di A sono collegati a v con lati colorati con a (per definizione di A), cioè il grafo di partenza ha un sottografo monocromatico su k vertici (Si conclude ugualmente nel caso $r_2(k-1) \leq |B|$).

Infine facciamo induzione su c per il caso generale: supponiamo che l'asserto valga per c colori e mostriamo che vale per $c+1$. In particolare mostriamo che $r_{c+1}(k) \leq r_2(r_c(k))$.

Prendo un grafo G con $r_2(r_c(k))$ vertici (posso farlo perchè $r_c(k)$ è ben definito per ipotesi induttiva e ugualmente $r_2(r_c(k))$). Etichetto i colori con i numeri naturali 1,.....,c. Considero una colorazione ausiliaria: coloro con a i lati di G che erano colorati con il colore 1; coloro con b i lati di G che erano colorati con un qualsiasi

altro colore. Per come ho scelto il numero di vertici so che c'è un sottografo completo di $r_c(k)$ vertici colorato con a oppure con b (infatti avevo scelto un grafo con $r_2(r_c(k))$ vertici, che ho poi colorato con 2 colori). Nel primo caso ho dunque un sottografo completo su $r_c(k)$ vertici colorato con a, che coincide con il colore 1; ma $k \leq r_c(k)\ \forall c$ e sono a posto. Nel secondo caso ho un grafo colorato con b, cioè con i colori da 2 a c, e con $r_c(k)$ vertici e dunque per definizione di $r_c(k)$ posso trovare un sottografo completo monocromatico di k vertici.

□

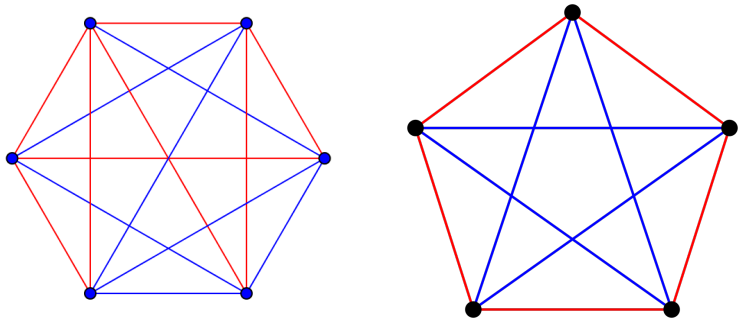
Esempio 8. Date le notazioni del precedente teorema si ha che $r_2(3) = 6$.

Questo esempio è anche conosciuto come il "teorema" degli amici e degli sconosciuti.

Dimostrazione. Prendo un grafo completo di 6 vertici e lo coloro con rosso e blu. Fisso un vertice v. Da ogni vertice (quindi anche da v) escono 5 lati e dunque almeno tre di essi sono dello stesso colore, supponiamo rosso. Siano v_1, v_2, v_3 gli estremi dei lati rossi che escono da v. Se almeno un lato di quelli che li collegano è rosso ho (almeno) un triangolo rosso, altrimenti sono tutti blu e quindi in tal caso ho un triangolo blu. In entrambi i casi ho trovato un triangolo monocromatico.

Serve ora osservare che per $n = 5$ esiste un grafo senza triangoli monocromatici (basta colorare il perimetro di un pentagono di un colore e le diagonali dell'altro colore).

Ho mostrato cioè che $5 < r_2(3) \leq 6$. □



Curiosità sul teorema di Ramsey:

Esiste una versione un po' più generale del teorema, che afferma che sono ben definiti i numeri $r(n_1, ..., n_s)$, che indicano il numero minimo di vertici che deve avere un grafo completo colorato con s colori, in modo tale che esista un sottografo completo di n_1 vertici colorato con il colore 1, oppure un sottografo completo di n_2 vertici colorato con il colore 2 e così via per ogni colore. Tale numero viene chiamato numero di Ramsey.

Con queste nuove notazioni l'esempio di prima afferma che $r(3,3) = 6$ e in generale il numero che avevamo indicato con $r_c(k)$ si riscrive come $r(k, k, ..., k)$ con c argomenti.

La dimostrazione è quasi analoga a quella già fatta e occorre semplicemente modificare di poco la prova per induzione.

Per calcolare i numeri di Ramsey di solito si procede come si è fatto sopra: si trova una stima dall'alto del numero di vertici necessario e si mostra che è la migliore possibile, cioè che esiste un grafo con un vertice in meno che non ha alcun sottografo monocromatico e completo con il numero di vertici desiderato.

Già solamente restringendosi al caso di due colori distinti si conoscono solo pochissimi numeri di Ramsey (a patto che n_1 ed n_2 siano entrambi maggiori di 2, altrimenti è banale), ma in generale si conoscono solo stime per difetto e per eccesso.

3. TEOREMI DI SHUR

Utilizziamo ora la teoria di Ramsey per ottenere il risultato che ci serve sui campi finiti.

Premettiamo però un lemma:

Lemma 9 (Shur)**.** *Per ogni numero di colori c, esiste $n \in \mathbb{N}$ t.c. per ogni colorazione di $\{1, 2, ..., n\}$ esistono $a, b, c \in \mathbb{N}$ $(a, b, c \leq n)$ tali che a, b, c hanno la stessa colorazione e $a + b = c$.*

Dimostrazione. Una colorazione è come prima una funzione F: $\{1, 2, ..., n\} \longrightarrow \{1, 2, ..., c\}$.

Diversamente da prima l'enunciato parla di colorazione di elementi di un insieme, non di lati di un grafo come fatto fin qui. Tuttavia la dimostrazione si basa sulla costruzione di un grafo colorato e sul teorema precedente:

sia $n := r_c(3)$; si costruisca un grafo completo sui vertici $\{1, 2, ..., n\}$, colorando il lato $\{a, b\}$ con $F(|a - b|)$. (Cioè abbiamo colorato i lati del grafo in base alla colorazione dei suoi estremi).

Per come abbiamo scelto n, esiste un sottografo completo su tre vertici (cioè un triangolo) tutto colorato nello stesso modo. Siano x, y, z i vertici di tale triangolo con $x > y > z$. Siano $a := x - y$, $b := y - z$ e $c := x - z$. Allora ricordando che il triangolo è monocroamtico e che il colore del lato è il colore del modulo della differenza dei vertci, si ottiene che i vertci a, b, c sono colorati nello stesso modo (perchè i loro colori coincidono con quelli dei lati del triangolo monocromatico) e vale $a + b = c$ per come sono definiti (Infatti $x - y + y - z = x - z$). □

Definizione 10. Il minimo numero che soddisfa il lemma è chiamato numero di Shur ed è indicato con $s(c)$. In dettaglio: dati c colori, $s(c)$ è il minimo numero tale che per ogni colorazione di $\{1, ..., s(c)\}$ si trovano $a, b, c \in \mathbb{N}$ $(a, b, c \leq s(c))$ tali che a, b, c hanno la stessa colorazione e $a + b = c$.

Dalla definizione segue subito che $s(c) \leq r_c(3) - 1$. (Il -1 discende dal fatto che nella dimostrazione del lemma, per colorare il grafo mi bastano i colori da 1 ad $n - 1$; il colore di n non iterviene mai.

Esempio 11. Si ha che s(2) = 5

Dimostrazione. Abbiamo appena notato che $s(2) \leq r_2(3) - 1 = 6 - 1 = 5$.

Definiamo una colorazione di $\{1, 2, 3, 4\}$ che non soddisfi la proprietà richiesta. Useremo i colori blu e rosso per fissare le idee:

- coloro 1 di rosso
- poichè 1+1 = 2, il 2 deve essere blu

- poichè 2+2=4 e il due è blu allora il 4 deve essere rosso
- il 3 deve essere blu poichè altrimenti 1+3=4 e 1,3,4 rossi

Dunque le terne $\{1,1,2\}, \{1,2,3\}, \{1,3,4\}, \{2,2,4\}$ sono composte da numeri di colori diversi e sono le uniche possibili (perchè 2+3 e 3+3 e le somme con addendo 4 non stanno in $\{1,2,3,4\}$). Questo prova che $s(2) > 4$. □

Dimostriamo finalemente "l'ultimo teorema di Fermat moudulo p", che afferma che per ogni k, pur di scegliere un primo p abbastanza grande (quanto "grande" dipende da k...), l'equazione $x^k + y^k = z^k$ ammette delle soluzioni.

Teorema 12. *$\forall k \in \mathbb{N}$ $\exists n \in \mathbb{N}$ tale che $\forall p \geq n$ (p primo) $\exists x, y, z \in \mathbb{F}_p$ tali che $x^k + y^k = z^k$.*

Dimostrazione. La dimostrazione si basa sul fatto che l'insieme $\{1, ..., p-1\}$ (gruppo degli elementi con inverso moltiplicativo in $\mathbb{F}_p$) formano un gruppo rispetto alla moltiplicazione e che tale gruppo è ciclico (è qui che si usa che p deve essere primo!).

Sia k fissato. Sia n dato dal lemma precedente e sia $p \geq n$. Sia g un generatore del gruppo degli invertibili di $\mathbb{F}_p$. Per ogni $a \in \mathbb{F}_p$ posso scrivere $a = g^{\alpha}$ per la ciclicità. Divido α per k e ottengo $a = g^{kq_a + r_a}$. Coloro gli elementi di $\{1, ..., p-1\}$ in base a r_a. Dunque per il lemma posso trovare tre di questi con uguale colorazione di cui uno è la somma degli altri due, cioè esistono r, q_1, q_2, q_3 tali che $g^{kq_1+r} + g^{kq_2+r} = g^{kq_3+r}$. Moltiplicando per l'inverso di g^r si ottiene $g^{kq_1} + g^{kq_2} = g^{kq_3}$ e infine ponendo $x := g^{q_1}$, $y := g^{q_2}$, $z := g^{q_3}$ si ha la tesi. □

4. BIBLIOGRAFIA

- Schur, I., "Über die Kongruenz $x^m + y^m \equiv z^m$(mod p)", Jahresber. Deutschen Math. Verein. 25 (1916), 114–117.
- Ramsey, F. P., "On a problem of formal logic", Proceedings of the London Mathematical Society, 30 (1930): 264–270,
- Kisner, S. L.. "Schur's Theorem and Related Topics in Ramsey Theory." (2013).

L'AUREUM THEOREMA

FRANCESCO ALESSIO ZUCCON

1. L'EQUAZIONE MODULARE QUADRATICA

Introduzione al problema

Tra le varie finalità per le quali nacque questa "gemma dell'aritmetica", spicca in particolar modo la risoluzione teorica dell'equazione quadratica modulare:

$$ax^2 + bx + c \equiv_n 0 \tag{1}$$

Ciò che va a falsificare la classica formula risolutiva è l'anomalo funzionamento della cancellazione in $\mathbb{Z}/n\mathbb{Z}$, il cui anello dei polinomi, non essendo in generale un dominio, non potrà nemmeno controllare il numero di radici con il grado. Procedendo per passi, questo problema verrà ricondotto all'enunciato della legge di reciprocità quadratica, a cui si aggiungeranno due complementi di simile natura. Prima di addentrarsi nella trattazione, sembra dovuta un'avvertenza al lettore sul carattere puramente teorico di tale indagine: l'obiettivo non è risolvere un'equazione quadratica a livello computazionale, bensì di stabilire se o meno essa risulti risolvibile a priori dalla ricerca di eventuali soluzioni.

Riduzione dell'equazione

Tramite il classico metodo per ricondursi al quadrato, con dovute osservazioni sulla legge di cancellazione e sulla risolubilità delle equazioni lineari modulari, è immediata la seguente equivalenza:

$$ax^2 + bx + c \equiv_n 0 \iff y^2 \equiv_m b^2 - 4ac \ \wedge \ MCD(2a; n) \mid y - b$$
$$\text{ove } y \equiv_m 2ax + b \wedge m = MCD(4a; n) \cdot n$$

Si è, pertanto, semplificato il problema ad un'equazione pura, ma grazie al Teorema Cinese dei Resti la questione si trasporta soltanto sulla seguente forma:

$$x^2 \equiv_{p^a} d \ \text{ per } a \in \mathbb{N}^+$$

Osservazione 1. Qualora l'ambiente sia $\mathbb{Z}/p\mathbb{Z}$, l'equazione quadratica generica è equivalente alla forma pura in quanto ci si trova in un campo, ove non necessitano condizioni di divisibilità. Si noti che da ora in avanti p andrà ad indicare un generico numero primo dispari (positivo).

Prima di addentrarsi nello studio della reciprocità, si presenta un'ultima osservazione, unica sulla natura del calcolo e che, in ogni caso, risulta poco agevole nella ricerca di soluzioni esplicite (di poco migliore rispetto ai semplici tentativi!).

Proposizione 2. *Per risolvere l'equazione:* $x^2 \equiv_{p^a} d$ *è necessario e sufficiente risolvere la forma ridotta:* $x^2 \equiv_p d$

Dimostrazione. Il fatto che sia necessario è ovvio, per mostrare che è anche sufficiente si procede in modo ricorsivo. Sia x_0 t.c.:

$$x_0{}^2 \equiv_p d$$

Allora le eventuali soluzioni dell'equazione generica hanno forma $\pm x_0 + kp^t$ (può vedersi come applicazione del Teorema di Corrispondenza), ove si può supporre $1 \leq t < a$ (se $t = 0$, allora si avrebbe $k = 0$ e si verifica manualmente se o meno le soluzioni $\pm x_0$ soddisfino anche l'equazione generica), mentre kp^t è la nuova incognita. Sostituendo nell'equazione generica si ottiene:

$$(\pm x_0 + kp^t)^2 \equiv_{p^a} d$$

Manipolando algebricamente:

$$\pm 2x_0 kp^t + (kp^t)^2 \equiv_{p^a} -(x_0{}^2 - d)$$

Ma si osserva che tanto il primo membro quanto il secondo (per la definizione iniziale di x_0) sono divisibili per p, dunque, tramite cancellazione si giunge ad una coppia di equazioni quadratiche di incognita $y = kp^{t-1}$, nella quale però il modulo ha esponente inferiore di uno come segue:

$$\pm 2x_0 y + py^2 \equiv_{p^{a-1}} c \text{ ove } -(x_0{}^2 - d) \equiv_{p^a} pc$$

da cui la tesi applicando tale procedimento altre $a - 2$ volte. □

Osservazione 3. si è ridotta la difficoltà di verifica sulla risolubilità dell'equazione da p^a tentativi a 2^{a-1} verifiche con le soluzioni dell'equazione ridotta.

2. IL SIMBOLO DI LEGENDRE

Definizione 4. d è un n-residuo quadratico $\iff$ esiste un elemento x t.c.

$$x^2 \equiv_n d \not\equiv_p 0 \tag{2}$$

Caratterizzazione dei p-residui.
d è un p-residuo quadratico $\iff d \in \{1^2, 2^2, ..., [(p-1)/2]^2\}$

Dimostrazione. Innanzitutto si considera il caso p primo dispari poichè per il primo 2 l'unico residuo è banalmente l'unità. Risulta poi ovvio che i numeri dell'insieme a sinistra siano residui, ma d'altra parte, supponendo che d sia un n-residuo quadratico, per definizione esiste un elemento x t.c. soddisfa (2), ma al contempo $-x \equiv_p (p - x)$ soddisfa l'equazione e uno dei due necessariamente è minore di $p/2$ da cui la tesi. □

Proposizione 5.

i) a, b n-residui $\implies$ *ab n-residuo*

ii) a p-residuo, b non p-residuo $\implies$ *ab non p-residuo*

iii) a, b non p-residui $\implies$ *ab p-residuo*

Dimostrazione. *i*) ovvia. *ii*) Si consideri a un p-residuo e sia ϕ_a la permutazione regolare destra indotta su $\mathbb{Z}/p\mathbb{Z}^*$ da tale elemento. Per la caratterizzazione, nell'immagine della permutazione vi saranno $(p-1)/2$ p-residui, ma da *i*) è noto che il sottoinsieme di residui è ϕ_a-invariante, da cui i restanti, che sono i prodotti ab con b non p-residuo, non potranno che essere non p-residui.
iii) Con la medesima permutazione in cui si pone a non p-residuo, per *ii*) si ha che le permutazioni dei p-residui saranno non p-residui, dunque i restanti, che sono i prodotti ab con a, b non p-residui, dovranno essere p-residui. □

Osservazione 6. in *ii*) e *iii*) è essenziale che si tratti di p-residui poichè nel generico anello $\mathbb{Z}/n\mathbb{Z}$ tali proprietà cadono come suggerito dai seguenti esempi:

Esempio 7. In $\mathbb{Z}/6\mathbb{Z}$ si ha che 3 è un 6-residuo, 5 non lo è, ma $15 \equiv_6 3$, quindi è falso che prodotti tra residuo e non residuo dia un non residuo.

Esempio 8. In $\mathbb{Z}/12\mathbb{Z}$ si ha che 2 e 5 non sono 12-residui, e nemmeno il loro prodotto lo è, falsificando la terza proprietà che si ha nel caso dei primi.

Definizione 9. Si definisce il Simbolo di Legendre come una funzione che distingue i p-residui:

$$\chi_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}\,, \quad \chi_p(a) := \begin{cases} 1 & \text{se } a \text{ è } p\text{-residuo} \\ 0 & \text{se } a \equiv_p 0 \\ -1 & \text{altrimenti} \end{cases} \tag{3}$$

Nota Storica. Quest'ultima notazione, dovuta al fatto che tale funzione è un carattere di Dirichlet, è più recente rispetto a quella usata ad inizio Ottocento di seguito riportata:

$$\left(\frac{a}{p}\right)$$

Proposizione 10. *La funzione χ_p è ben definita, ossia vale $\chi_p(a+kp) = \chi_p(a)$*

Dimostrazione. Supponendo $\chi_p(a+kp) = -1$, allora se valesse $\chi_p(a) = 1 \implies \exists x : x^2 \equiv_p a \equiv_p a + kp$ assurdo, se invece valesse $\chi_p(a) = 0 \implies 0 \equiv_p a \equiv_p a + kp$ assurdo. Supponendo $\chi_p(a+kp) = 0 : a + kp \equiv_p 0 \equiv_p a \implies \chi_p(a+kp) = 0$. Infine, $\chi_p(a+kp) = 1 \iff \exists x \; t.c. \; x^2 \equiv_p a + kp \equiv_p a \iff \chi_p(a) = 1$ □

Proposizione 11. *La funzione χ_p è totalmente moltiplicativa, ossia $\forall a, b \in \mathbb{Z}$ vale $\chi_p(ab) = \chi_p(a)\chi_p(b)$*

Dimostrazione. Segue dalla Prop. 2.2, con ovvie osservazioni qualora $a = 0$. □

Osservazione 12. Lo zero può sempre considerarsi un residuo, ma, per preservare la totale moltiplicatività di χ_p, tale funzione è ivi definita nulla. Inoltre, si osservi che la totale moltiplicatività non richiede la coprimità tra i due fattori, a differenza per esempio della sola moltiplicatività del toziente di Eulero.

3. UNA DIMOSTRAZIONE ELEMENTARE

3.1. Il Criterio di Eulero.

Teorema 13.

$$\chi_p(a) \equiv_p a^{(p-1)/2} \tag{4}$$

Dimostrazione. Per $a \equiv_p 0$ ovvio. Si supponga che $\chi_p(a) = 1 \iff \exists x : x^2 \equiv_p a$, allora segue $a^{(p-1)/2} \equiv_p x^{(p-1)} \equiv_p 1$ per il Piccolo Teorema di Fermat. Se, invece, vale $\chi_p(a) = -1$, allora per le proprietà di gruppo (moltiplicativo) si ottiene che $\forall i \in \mathbb{Z}/p\mathbb{Z}^* \exists! j \in \mathbb{Z}/p\mathbb{Z}^*$ *t.c.* : $i \cdot j \equiv_p a$, ove però si avrà $i \neq j$ poiché altrimenti a sarebbe un p-residuo. Allora si considerino tutte le possibili $i \in \mathbb{Z}/p\mathbb{Z}^*$ a cui associare la rispettiva j, ottenendo $(p-1)$ coppie che, dunque, saranno tutte ripetute due volte. Pertanto, si considerino le $(p-1)/2$ coppie distinte moltiplicate tra loro, da cui per il Teorema di Wilson si otterrà:

$$a^{(p-1)/2} \equiv_p (i_1 \cdot j_1)(i_2 \cdot j_2)...(i_{(p-1)/2} \cdot j_{(p-1)/2}) \equiv_p (p-1)! \equiv_p -1$$

□

Corollario 14. $p = a^2 + b^2 \iff p \equiv_4 1 \vee p = 2$

Dimostrazione. Si consulti l'Appendice (Teorema di "Natale"). □

Corollario 15.

$$n = \prod_{i=1}^{k} p_i^{q_i}$$

$$n = a^2 + b^2 \iff \forall i : p_i \equiv_4 1 \vee p_i = 2 \vee p_i \equiv_4 3 \wedge q_i \equiv_2 0$$

3.2. Lemma di Gauss. Un'importante applicazione del Criterio di Eulero è una semplice dimostrazione del Lemma con cui Gauss operò una delle prime dimostrazione della reciprocità.

Teorema 16.

$$a \not\equiv_p 0, s(p) := \{n \in \mathbb{N}^+ : n < p\},$$
$$s_a := |\{i \in s(p) : i < p/2 \ \wedge \ \exists k : p/2 < ai + kp < p\}|$$
$$\implies \chi_p(a) = (-1)^{s_a}$$

Dimostrazione. Siano $w_i := ai$ t.c.: $0 < i < p/2 \ \wedge \ \exists k_i : p/2 < ai + k_i p < p$ e siano $v_j := aj$ t.c.: $0 < j < p/2 \wedge \ \exists k_j : 0 < aj + k_j p < p/2$. Si osserva $0 < (1-k_i)p - w_i < p/2$, e se si avesse $(1-k_i)p - w_i = v_j \implies 0 \equiv_p w_i + v_j = a(i+j)$, allora da $a \not\equiv_p 0$, si avrebbe $i + j = tp$ con $t \geq 1$, ma ciò è assurdo in quanto $0 < i, j < p/2$. Pertanto, si ottiene l'uguaglianza insiemistica $\{(1-k_i)p - w_i, v_j\}_{i,j} = \{1, 2, ..., (p-1)/2\}$, moltiplicando:

$$[(p-1)/2]! = \prod_i (1-k_i)p - w_i \prod_j v_j \equiv_p (-1)^{s_a} \prod_i w_i \prod_j v_j =$$
$$= (-1)^{s_a} \prod_i ai \prod_j aj = (-1)^{s_a} a^{(p-1)/2} \prod_i i \prod_j j =$$
$$= (-1)^{s_a} a^{(p-1)/2} [(p-1)/2]! \implies (-1)^{s_a} \equiv_p a^{(p-1)/2}$$

da cui la tesi per il Criterio di Eulero. □

Corollario 17. $\chi_p(2) = (-1)^{(p^2-1)/8}$

Dimostrazione. Per il lemma di Gauss si ha che $\chi_p(2) = (-1)^{s_2}$, ricordando che $s_2 := |\{i \in s(p) : i < p/2 \ \wedge \ \exists k_i : p/2 < 2i + k_i p < p\}$. Allora si ha l'equivalenza: $0 < 2i + k_i p < p/2 \iff 0 < i \leq [p/4]$, da cui $s_2 = (p-1)/2 - [p/4]$ (le quadre indicano la parte intera). Dunque, basta mostrare $(n-1)/2 - [n/4] \equiv_2 (n^2-1)/8$ per n dispari, ma si mostra che se vale per n allora vale per $n + 8t$, infatti:

$$(n+8t-1)/2 - [(n+8t)/4] \equiv_2 (n-1)/2 - [n/4] \overset{Hp}{\equiv}_2 (n^2-1)/8$$
$$((n+8t)^2 - 1)/8 = (n^2-1)/8 + 2nt + +8t^2 \equiv_2 (n^2-1)/8$$

da cui la tesi verificando per $\{1, 3, 5, 7\}$. □

Osservazione 18. Come accennato dall'inizio la legge di reciprocità quadratica esaurisce quasi interamente il problema dei p-residui, ma a completare l'opera sono necessari i risultati ottenuti in Cor.3.2 e in Cor.3.5.

3.3. La Dimostrazione Geometrica di Eisenstein. Fu il matematico Eisenstein a sfruttare i parziali risultati precedentemente presentati per ottenere una dimostrazione tra le più elementari in assoluto, che consiste in combinatoria di base applicata alla geometria della retta, breve rispetto al procedimento delle somme di Gauss.

Lemma 19.

$$a \not\equiv_2 0, S(a,p) := \sum_{i=1}^{(p-1)/2} [ka/p] \implies \chi_p(a) = (-1)^{S(a,p)}$$

Dimostrazione. Tramite il Lemma di Gauss basta mostrare $S(a,p) \equiv_2 s_a$. Sia allora per l'algoritmo di Euclide $ka = p[ka/p] + r_k$. Si osserva poi che $i \neq j \implies r_i \neq r_j$ poiché $r_i \equiv_p ai \not\equiv_p aj \equiv_p r_j$. Allora riprendendo le definizioni date per il Lemma di Gauss seguirà che $\forall k : r_k = w_i \vee r_k = v_j$. Pertanto si ottiene:

$$a \sum_{k=1}^{(p-1)/2} k = p \sum_{k=1}^{(p-1)/2} [ka/p] + \sum_{k=1}^{(p-1)/2} r_k = pS(a,p) + \sum_i w_i + \sum_j v_j$$

Ma ricordando (si considerano w_i, v_j ridotti al rappresentante principale):

$$\sum_{k=1}^{(p-1)/2} k = \sum_i p - w_i + \sum_j v_j = ps_a - \sum_i w_i + \sum_j v_j$$

Si otterrà immediatamente sottraendo:

$$(a-1) \sum_{k=1}^{(p-1)/2} k = p(S(a,p) - s_a) + 2\sum_i w_i$$

Ma poiché $a \equiv_2 p \equiv_2 1$ si ottiene la tesi. □

Osservazione 20. Pronti, infine, tutti gli strumenti necessari alla dimostrazione della Legge di reciprocità quadratica, è bene focalizzarsi sul suo significato più concreto (7) come può dedursi dall'enunciato formale tramite il simbolo di Legendre (6) appena di seguito (p, q indicano primi dispari distinti):

Teorema 21.

$$\chi_p(q) \cdot \chi_q(p) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \tag{5}$$

$$\begin{aligned} p \equiv_4 1 : x^2 \equiv_p q \text{ è risolvibile} &\iff x^2 \equiv_q p \text{ è risolvibile} \\ p \equiv_4 q \equiv_4 3 : x^2 \equiv_p q \text{ risolvibile} &x^2 \equiv_q p \text{ non è risolvibile} \end{aligned} \tag{6}$$

Dimostrazione. Si consideri la retta $r : py = qx$ e si definisca un sottoinsieme del piano $L := \{(x, y) \in \mathbb{Z}^2 : 1 \leq x \leq (p-1)/2 \ \wedge \ 1 \leq y \leq (q-1)/2\}$. Si osserva $L \cap r = \emptyset$ poiché $py = qx \implies p|qx \implies p|x$ assurdo se $(x, y) \in L$ per $1 \leq x \leq (p-1)/2$. Allora si attua una partizione di $L = L_1 \cup L_2$ ove:

$$L_1 := \{(x, y) \in L : py > qx\} \wedge L_2 := \{(x, y) \in L : py < qx\}$$

è inoltre evidente che: $\frac{p-1}{2} \cdot \frac{q-1}{2} = |L| = |L_1| + |L_2|$. Si mostrerà che $|L_1| = S(p, q)$ e $|L_2| = S(q, p)$ da cui per il Lemma di Eisenstein (19) la tesi sarà dimostrata. Infatti, $(x, y) \in L_1 \iff 1 \leq x \leq [yp/q]$, allora fissato y vi saranno un numero di x che soddisfano l'appartenenza ad L_1 pari a $[yp/q]$, ma si sa che $1 \leq y \leq (q-1)/2 \implies |L_1| = \sum_{y=1}^{(q-1)/2} [yp/q] = S(p, q)$. Analogo per $|L_2| = S(q, p)$. In conclusione:

$$\begin{cases} \chi_p(q) = (-1)^{S(q,p)} \\ \chi_q(p) = (-1)^{S(p,q)} \end{cases} \implies \chi_p(q) \cdot \chi_q(p) = (-1)^{S(q,p)+S(p,q)} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

□

4. APPLICAZIONE ALLE FORME QUADRATICHE

Obiettivo di questa breve sezione è mostrare come la reciprocità quadratica possa essere sfruttata per valutare e caratterizzare la presenza di numeri primi in forme quadratiche (solitamente definite positive a coefficienti in $\mathbb{Z}$). Verrà, infatti, presentato un teorema (4.2) già noto a Fermat che è composto di tre proposizioni di identica dimostrazione. Tuttavia, è bene sottolineare che superando i più piccoli numeri primi si perde la possibilità di dimostrare l'implicazione che sfrutta il Lemma di Thue, infatti in generale vale soltanto:

Proposizione 22. $p = nx^2 + my^2 \implies \chi_p(-n \cdot m^{-1}) = 1$

Dimostrazione. Triviale dalla definizione di residuo quadratico. □

Lemma di Thue 1. $\forall a : p \nmid a \implies \exists x, y : ax \equiv_p y \wedge 0 < |x|, |y| < \sqrt{p}$

Dimostrazione. Si considerino i valori $k \equiv_p x - ay$ generati dalle coppie nell'insieme $S := \{(x, y) \in \mathbb{Z}^2 : 0 \leq x, y \leq [\sqrt{p}]\}$, allora poiché $|S| = ([\sqrt{p}] + 1)^2 \geq p + 1$ esistono due coppie distinte di x, y che genereranno lo stesso $k \equiv_p x_1 - ay_1 \equiv_p x_2 - ay_2 \implies x_1 - x_2 \equiv_p a(y_1 - y_2)$. Ma per definizione $0 \leq x_i, y_i \leq$

$\sqrt{p} \implies 0 \leq |x_1 - x_2|, |y_1 - y_2| \leq \sqrt{p}$ da cui i valori desiderati osservando $x_1 \neq x_2$ altrimenti le coppie non sarebbero distinte, quindi anche $y_1 \neq y_2$. □

Teorema 23.

$$i)\ \exists x, y : p = x^2 + 2y^2 \iff p = 2 \vee p \equiv_8 x : x \in \{1, 3\}$$
$$ii)\ \exists x, y : p = x^2 + 3y^2 \iff p = 3 \vee p \equiv_3 1$$
$$iii)\ \exists x, y : p = x^2 + 5y^2 \implies p = 5 \vee p \equiv_{20} x : x \in \{1, 3, 7, 9\}$$
$$iv)\ p = 5 \vee p \equiv_2 0x : x \in \{1, 9\} \implies \exists x, y : p = x^2 + 5y^2$$

Dimostrazione. Si prova $i)$ a titolo di esempio, le altre sono simili. Se vale $p = x^2 + 2y^2 \implies x^2 \equiv_p -2y^2 \implies \chi_p(-2) = 1$ per $p \neq 2$, altrimenti è ovvia. Ma in virtù della totale moltiplicatività, del Teor.3.1 e del Cor.3.5 si ha:

$$\chi_p(-2) = \chi_p(-1) \cdot \chi_p(2) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}}$$

sia allora $p \equiv_4 1 \implies p \equiv_8 x : x \in \{1, 5\}$ ma per $x = 5$ non si avrebbe un residuo, al contrario del caso in cui $x = 1$. Se $p \equiv_4 3 \implies p \equiv_8 x : x \in \{3, 7\}$, e -2 risulta un residuo solo quando $x = 3$.
Viceversa se $p \equiv_8 x : x \in \{1, 3\} \iff \chi_p(-2) = 1$ (equivalenza vista nell'implicazione precedente), allora $\exists a : a^2 \equiv_p -2$ e per il Lemma di Thue $\exists x, y : ax \equiv_p y \wedge 0 < |x|, |y| < [\sqrt{p}] \implies 2x^2 + y^2 \equiv_p 0 \implies 0 < 2x^2 + y^2 = kp < 3p$. Ora se fosse $k = 2$ allora si avrebbe necessariamente che y è pari:$y = 2n \implies 2x^2 + 4n^2 = 2p \implies x^2 + 2n^2 = p$, quindi in ogni caso si può considerare $k = 1$ che è la tesi. □

5. APPENDICE

Dim. di Cor 3.2 (Teorema di "Natale") 1. $p = a^2 + b^2 \iff p \equiv_4 1 \ \vee \ p = 2$

Dimostrazione. Se p è dispari e $p = a^2 + b^2$, allora si può supporre a dispari e b pari, da cui $p \equiv_4 a^2 \equiv_4 1$, dato che $a \equiv_4 \pm 1$, altrimenti segue $p = 2$. Viceversa se $p = 2 = 1^2 + 1^2$, se invece $p \equiv_4 1$ allora per il criterio di Eulero si ottiene $\exists a : a^2 \equiv_p -1$. Inoltre, per il Lemma di Thue $\exists x, y : ax \equiv_p y \wedge 0 < |x|, |y| < \sqrt{p}$, da cui elevando a potenza:$-x^2 \equiv_p y^2 \implies 0 < x^2 + y^2 = kp < 2p \implies k = 1$ □

Teorema dei due quadrati di Fermat (Cor 3.3) 1.

$$n = \prod_{i=1}^{k} p_i^{q_i}$$
$$n = a^2 + b^2 \iff p_i \equiv_4 1 \vee p_i = 2 \vee p_i \equiv_4 3 \wedge q_i \equiv_2 0$$

Esercizio 24. Dimostrare Cor. 3.3 (Sugg.: sfruttare Cor. 3.2 e l'identità di Diofanto: $(a^2 + b^2) \cdot (c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$ di ovvia verifica algebrica).

5.1. La Generalizzazione con il Simbolo di Jacobi.

Definizione 25. Si definisce il Simbolo di Jacobi come una funzione che estende in senso lato il Simbolo di Legendre:

$$n = \prod_{i=1}^{k} p_i^{q_i}$$

$$\chi_n(a) := \prod_{i=1}^{k} (\chi_{p_i}(a))^{q_i}$$

Osservazione 26. Il Simbolo di Jacobi non ha lo stesso significato del Simbolo di Legendre, in quanto non va ad individuare i più generali n-residui. Infatti, tale estensione viene formulata per fini puramente computazionali in modo da poter sfruttare la Legge di reciprocità quadratica senza dipendere dalla fattorizzazione in primi, ma sfruttando più semplicemente l'algoritmo di divisione euclidea, come mostrato in seguito (5.5). Inoltre, si tratta di un'estensione conservativa:

Teorema 27.

$$\begin{aligned}
&i)\ (a,n) = (b,n) = 1 \implies \chi_n(ab) = \chi_n(a) \cdot \chi_n(b)\\
&ii)(a,n) = (b,n) = 1 \wedge a \equiv_n b \implies \chi_n(a) = \chi_n(b)\\
&iii)\ \chi_n(-1) = (-1)^{(n-1)/2}\\
&iv)\ \chi_n(2) = (-1)^{(n^2-1)/8}\\
&v)(n,m) = 1 \implies \chi_n(m)\chi_m(n) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}
\end{aligned}$$

Dimostrazione. Esercizio lasciato al lettore (bastano i risultati precedenti!). □

Algoritmo di Jacobi

Teorema 28. *sia $a > b \wedge (a,b) = 1$, si ponga per comodità $a = R_0, b = R_1$, si usi l'algoritmo di Euclide separando nei resti la massima potenza di due:*

$$\begin{cases}
R_0 = R_1 \cdot q_1 + 2^{s_1} \cdot R_2\\
R_1 = R_2 \cdot q_2 + 2^{s_2} \cdot R_3\\
\quad\quad : : :\\
R_{n-2} = R_{n-1} \cdot q_{n-1} + 2^{s_{n-1}} \cdot R_n\\
R_n = 1 \wedge s_n = 0\\
\forall i \leq n : (R_i, R_{i+1}) = 1 \wedge 2 \nmid R_i
\end{cases} \implies \chi_b(a) = (-1)^{\delta}$$

$$ove\ \ \delta = \sum_{1}^{n-1} \left(s_i \cdot \frac{{R_i}^2 - 1}{8} + \frac{R_i - 1}{2} \cdot \frac{R_{i+1} - 1}{2} \right)$$

Dimostrazione. Si procede ricorsivamente:

$$\chi_b(a) = \chi_{R_1}(R_0) = \chi_{R_1}(2^{s_1}R_2) = [\chi_{R_1}(2)]^{s_1}\chi_{R_1}(R_2) =$$

$$= (-1)^{s_1 \cdot \frac{{R_1}^2-1}{8}}\chi_{R_1}(R_2) = (-1)^{\left(s_1 \cdot \frac{{R_1}^2-1}{8} + \frac{R_1-1}{2}\cdot\frac{R_2-1}{2}\right)}\chi_{R_2}(R_1)$$

In generale: $\chi_{R_{k+1}}(R_k) = (-1)^{\left(s_1 \cdot \frac{R_{k+1}{}^2-1}{8} + \frac{R_{k+1}-1}{2} \cdot \frac{R_{k+2}-1}{2}\right)} \chi_{R_{k+1}}(R_{k+2})$, da cui si ha la tesi procedendo fino a $\chi_{R_{n-1}(R_n)=1}$. □

BIBLIOGRAFIA

1. S. J. Wright. *Quadratic residues and non-residues*.
2. D. M. Burton. *Elementary Numer Theory*.
3. G.H. Hardy, E.M. Wright. *An Introduction to the Theory of Numbers*.

IL TEOREMA DI VAN-KAMPEN SECONDO GROTHENDIECK

LORENZO ABATE

1. INTRODUZIONE

Il teorema di Seifert−Van-Kampen[1] è uno strumento di notevole importanza nella topologia algebrica: infatti è uno degli strumenti principali per il calcolo del gruppo fondamentale di un dato spazio topologico X. Consideriamo infatti due aperti non vuoti connessi $A, B \subseteq X$ tali che $X = A \cup B$. Allora:

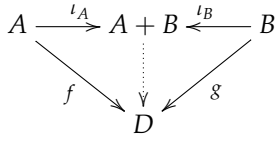
Teorema (Van-Kampen)**.** *Fissato un punto $x_0 \in X$, nelle ipotesi precedenti, si ha che il gruppo fondamentale $\pi_1(X, x_0)$ è isomorfo al prodotto amalgamato $\pi_1(A, x_0) *_{\pi_1(A\cap B, x_0)} \pi_1(B, x_0)$.*

Una dimostrazione di questo teorema può essere facilmente reperita in quasi ogni testo di topologia algebrica (tra i quali Algebraic Topology di A. Hatcher). Dato che l'enunciato del teorema coinvolge i gruppi fondamentali, che sono classi di equivalenza di cappi, non dovrebbe sorprendere che anche la dimostrazione di questo teorema si basa sullo studio dei cappi in $A \cup B$. Tuttavia noi forniremo un'altra dimostrazione di questo teorema, raffornzando le ipotesi e applicando le proprietà dei rivestimenti topologici e dell'azione di monodromia. Ricordiamo brevemente qualche definizione prima di procedere con la dimostrazione.

2. PRELIMINARI DI TEORIA DELLE CATEGORIE

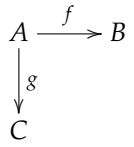
Fissiamo inizialmente una categoria $\mathcal{C}$ generica.

Definizione 1. Siano A, B due oggetti nella categoria $\mathcal{C}$. Il coprodotto è un oggetto $A + B$ con le frecce (dette iniezioni) $\iota_A : A \to A + B$, $\iota_B : B \to A + B$ tale che per ogni oggetto D e per ogni coppia di frecce $f : A \to D$ e $g : B \to D$, si ha che esiste un'unica freccia $A + B \to D$ tale che il seguente diagramma commuta:

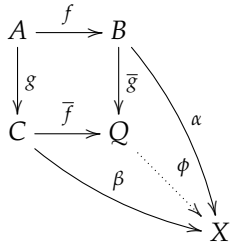


[1]Herbert Seifert, nato a Bernstadt auf dem Eigen il 27 maggio 1907 e mort ad Heidelberg il 1 ottobre 1996 è stato un matematico tedesco.
Egbert van Kampen, nato a Berchem il 28 maggio 1908 e morto a Baltimora l'11 febbraio 1942 è stato un matematico olandese.

Definizione 2. Date due frecce $f : A \to B$ e $g : A \to C$ in $\mathcal{C}$, un pushout di f e g è un colimite per il diagramma

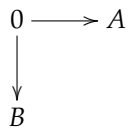


Esplicitamente, il pushout è dato da un oggetto Q con due frecce $\overline{f} : C \to Q$ e $\overline{g} : B \to Q$ tale che, per ogni oggetto X e coppia di frecce $\alpha : B \to X$ e $\beta : C \to X$, esiste un'unica $\phi : Q \to X$, tale che il seguente diagramma commuta:

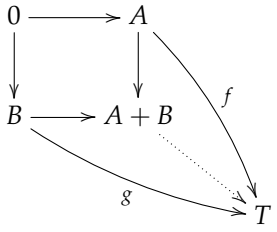


Nella categoria dei gruppi Grp, il coprodotto di due gruppi G, H è dato dal prodotto libero $G * H$.
Nelle categorie con un oggetto iniziale, possiamo caratterizzare il coprodotto come un certo pushout.

Proposizione 3. *Sia $\mathcal{C}$ una categorie con un oggetto iniziale 0 e siano $A, B \in Ob(\mathcal{C})$, allora il coprodotto $A + B$, se esiste, è dato dal pushout del seguente diagramma:*



Dimostrazione. È sufficiente verificare la proprietà universale del coprodotto: infatti, per ogni $T \in Ob(\mathcal{C})$ $f : A \to T$ e $g : B \to T$



□

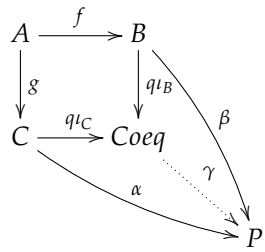
Nella categoria Grp, l'oggetto iniziale è il gruppo banale 0.
Osserviamo che, in modo duale, vale una proprietà simile anche per i pullback e i prodotti di categorie. I dettagli sono ovvi e sono lasciati al lettore interessato.

Proposizione 4. *Sia $\mathcal{C}$ una categorie con coprodotti (almeno binari) e coeqeualizzatori. Allora $\mathcal{C}$ ammette anche i pushout.*

Dimostrazione. Consideriamo $A, B, C \in Ob(\mathcal{C})$ e due frecce $f : A \to B$ e $g : A \to C$. Costruiamo il coprodotto $B + C$ e otteniamo il seguente diagramma (in generale non commutativo).

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \iota_B} \\ C & \xrightarrow{\iota_C} & B + C \end{array}$$

Costruiamo ora il coequalizzatore delle frecce $\iota_B f$ e $\iota_C g$, che denotiamo con $Coeq$ e $q : B + C \to Coeq$.
Consideriamo ora un qualunque oggetto P con due frecce $\alpha : C \to P$ e $\beta : B \to P$ tali che $\alpha g = \beta f$. Dalla proprietà universale del coprodotto, deduciamo che esiste un'unica freccia $h : B + C \to P$ tale che $\alpha = h\iota_C$ e $\beta = h\iota_B$. Infine, applichiamo la proprietà universale del coequalizzatore alla freccia h: infatti $h\iota_C g = \alpha g = \beta f = h\iota_B f$. Da ciò, deduciamo che esiste un'unica freccia $\gamma : Coeq \to P$ tale che $h = \gamma q$. Abbiamo quindi mostrato che $Coeq$ è il pushout del diagramma di partenza, infatti:



Inoltre $\gamma q \iota_B = h\iota_B = \beta$ e $\gamma q \iota_C = h\iota_C = \alpha$. □

3. PRELIMINARI GEOMETRICI

Definizione 5. Un rivestimento topologico su uno spazio topologico X è il dato di uno spazio topologico E, detto spazio totale del rivestimento e di una mappa continua $p : E \to X$, tali che, per ogni $x \in X$ esiste un aperto V_x di x detto intorno banalizzante tale che

$$p^{-1}(V_x) = \bigsqcup_{\alpha \in A} U_\alpha$$

dove A è un insieme non vuoto di indici e ciascun U_α è un aperto di E tale che $p_{|U_\alpha} : U_\alpha \to V_x$ sia un omeomorfismo.

Definizione 6. Siano X uno spazio topologico localmente connesso per archi, $x \in X$ un punto fissato e $p : E \to X$ un rivestimento. Si definisce l'azione destra di monodromia del gruppo fondamentale l'azione gruppale di $\pi_1(X, x)$ su $p^{-1}(x)$ definita da

$$p^{-1}(x) \times \pi_1(X, x_0) \to p^{-1}(x_0) \quad (e, [\alpha]) \longmapsto e \cdot [\alpha] \stackrel{def}{=} \alpha_e(1)$$

dove α_e è il sollevamento del cammino α, ossia è una mappa continua $\alpha_e : [0,1] \to E$ tale che $p\alpha_e = \alpha$ e $\alpha_e(0) = e$.

Prima di enunciare e dimostrare il teorema principale, premetto i seguenti due risultati sull'azione di monodromia, che ci serviranno per dimostrare il teorema principale.

Proposizione 7. *Dati due gruppi G, H, un insieme T, un'azione sinistra libera e transitiva di G su T ed un'azione destra di H su T compatibile con l'azione di G. Per ogni $e \in T$ definiamo la seguente applicazione $\theta_e : H \to G$ ponendo $\theta_e(h)$ come l'unico $g \in G$ tale che $g \cdot e = e \cdot h$. Allora θ_e è un omomorfismo di gruppi e l'insieme $\{h \in H | e \cdot h = e\}$ è un sottogruppo normale di H.*

Proposizione 8. *Sia X uno spazio topologico connesso, localmente connesso per archi e semilocalmente semplicemente connesso. Per ogni insieme non vuoto T e per ogni azione destra $T \times \pi_1(X,x) \to T$ esiste un rivestimento $p : E \to X$ ed una bigezione $\phi : T \to p^{-1}(x)$ tale che $\phi(t \bullet a) = \phi(t) \cdot a$ per ogni $t \in T$ e per ogni $a \in \pi_1(X,x)$. Inoltre la coppia (p, ϕ) è unica a meno di isomorfismi.*

4. LA DIMOSTRAZIONE DI GROTHENDIECK

Consideriamo uno spazio topologico X e due aperti connessi per archi $A, B \subseteq X$ tali che $A \cup B = X$. Fissiamo un punto $x_0 \in A \cap B$. Osserviamo che le inclusioni $A \subseteq X$, $B \subseteq X$, $A \cap B \subseteq A$ e $A \cap B \subseteq B$ inducono il seguete diagramma commutativo di omomorfismi di gruppi:

$$\begin{array}{ccc} \pi_1(A \cap B, x_0) & \xrightarrow{\alpha_*} & \pi_1(A, x_0) \\ \downarrow{\scriptstyle \beta_*} & & \downarrow{\scriptstyle f_*} \\ \pi_1(B, x_0) & \xrightarrow{g_*} & \pi_1(X, x_0) \end{array}$$

Consideriamo il prodotto libero (i.e. coprodotto in Grp) di $\pi_1(A, x_0)$ e $\pi_1(B, x_0)$ e applichiamo la proprietà universale del coprodotto con $\pi_1(X, x_0)$.

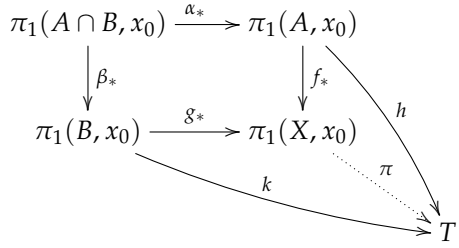
$$\begin{array}{ccccc} \pi_1(A, x_0) & \longrightarrow & \pi_1(A, x_0) * \pi_1(B, x_0) & \longleftarrow & \pi_1(B, x_0) \\ & {\scriptstyle f_*} \searrow & \downarrow {\scriptstyle \exists! h} & \swarrow {\scriptstyle g_*} & \\ & & \pi_1(X, x_0) & & \end{array}$$

Dato che l'immagine del morfismo h è il sottogruppo di $\pi_1(X, x_0)$ generato dalle immagini f_* e g_*, possiamo dedurre, lasciando i dettagli per il lettore, che h è surgettivo. Tuttavia, h non è iniettivo in generale, quindi il gruppo fondamentale di X con punto base x_0 non è isomorfo al prodotto libero di $\pi_1(A, x_0)$ e $\pi_1(B, x_0)$, ma ad un suo quoziente. Parleremo meglio di questi aspetti nella sezione successiva.

Ora siamo finalmente pronti per fornire una dimostrazione del teorema di Van-Kampen che sfrutta i risultati sull'azione di monodromia. Tale dimostrazione è attribuita ad Alexander Grothendieck[2].

[2]Alexander Grothendieck, nato a Berlino il 28 marzo 1928 e morto a Saint-Girons il 13 novembre 2014, è stato un matematico apolide naturalizzato francese.

Teorema (Van-Kampen secondo Grothendieck)**.** *Usando le notazioni precedenti supponiamo che X possieda un sistema fondamentale di intorni semplicemente connessi. Allora, per ogni gruppo T ed ogni coppia di omomorfismi $h : \pi_1(A, x_0) \to T$ e $k : \pi_1(B, x_0) \to T$ tali che $h\alpha_* = k\beta_*$, esiste un unico omomorfismo di gruppi $\pi : \pi_1(X, x_0) \to T$, che rende commutativo il seguente diagramma:*



Dimostrazione. Come nella dimostrazione orginale del teorema di Van Kampen, notiamo che $\pi_1(X, x_0)$ è generato dalle immagini di f_* e g_*. Pertanto, supponendone l'esistenza, deduciamo l'unicità di π.
Mostriamo ora che π esiste.
Gli omomorfismi h e k permettono di definire le seguenti azioni destre di gruppi:

$$T \times \pi_1(A, x_0) \to T, \quad (t, a) \longmapsto t \bullet a = th(a)$$
$$T \times \pi_1(B, x_0) \to T, \quad (t, b) \longmapsto t \bullet b = tk(b)$$

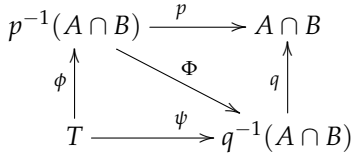
Tali azioni sono compatibili con l'azione di sinistra data dal prodotto $T \times T \to T$. Pertanto, in virtù della proposizione 8 esistono due rivestimenti topologici $p : E \to A$ e $q : F \to B$ e due bigezioni $\phi : T \to p^{-1}(x_0)$ e $\psi : T \to q^{-1}(x_0)$ le cui azioni di monodromia sono date dalle due precedenti azioni. Consideriamo ora l'azione di monodromia associata al rivestimento $p : p^{-1}(A \cap B) \to A \cap B$. Per ogni $a \in \pi_1(A \cap B, x_0)$ e $t \in T$ si ha

$$\phi(t) \cdot a = \phi(t \bullet \alpha_*(a)) = \phi(th(\alpha_*(a)))$$

Analogamente, se consideriamo l'azione di monodromia del rivestimento $q : q^{-1}(A \cap B) \to A \cap B$, deduciamo che

$$\psi(t) \cdot a = \psi(t \bullet \beta_*(a)) = \psi(tk(\beta_*(a)))$$

Sappiamo, per ipotesi, che $h\alpha_* = k\beta_*$, dunque concludiamo che le due azioni appena descritte sono isomorfe. Grazie alla proposizione 8 abbiamo un omeomorfismo $\Phi : p^{-1}(A \cap B) \to q^{-1}(A \cap B)$, tale che il seguente diagramma commuta:



Incollando i rivestimenti topologici E ed F tramite la funzione Φ otteniamo un rivestimento $E \cup_\Phi F \to X$, tale che la fibra su x_0 è isomorfa a T: quindi otteniamo un'azione di monodromia $T \times \pi_1(X, x_0) \to T$. Definiamo ora la funzione $\pi : \pi_1(X, x_0) \to T$ con $\pi(a) = 1 \cdot a$ dove 1 è l'elemento neutro di T. Osserviamo che, se $a \in \pi_1(A, x_0)$, allora $1 \cdot f_*(a) = 1 \bullet a = h(a)$. Analogamente, se

$a \in \pi_1(B, x_0)$, vale che $1 \cdot g_*(a) = 1 \bullet a = k(a)$.
L'azione di moltiplicazione $T \times T \to T$ è compatibile con la restrizione della monodromia ai gruppi $f_*\pi_1(A, x_0)$ e $g_*\pi_1(B, x_0)$. Dato che tali gruppi generano $\pi_1(X, x_0)$ segue che l'azione di monodromia $T \times \pi_1(X, x_0) \to T$ è compatibile con la moltiplicazione $T \times T \to T$. Pertanto, l'applicazione π è un omomorfismo di gruppi in virtù della proposizione 7. Concludiamo così la dimostrazione. □

5. IMPLICAZIONI ED OSSERVAZIONI FINALI

Notiamo che il gruppo fondamentale di X è il pushout del seguente diagramma

$$\begin{array}{ccc} \pi_1(A \cap B, x_0) & \xrightarrow{\alpha_*} & \pi_1(A, x_0) \\ \downarrow{\scriptstyle \beta_*} & & \\ \pi_1(B, x_0) & & \end{array}$$

Infatti il limite per quest'ultimo diagramma soddisfa la proprietà universale dei pushout.
Ora possiamo quindi dedurre che, nel caso in cui il gruppo fondamentale $\pi_1(A \cap B, x_0)$ sia iniziale in Grp (i.e. $A \cap B$ è semplicemente connesso), allora il gruppo fondamentale $\pi_1(X, x_0)$ coincide con il coprodotto (i.e. prodotto libero) di $\pi_1(A, x_0)$ e $\pi_1(B, x_0)$ in virtù di una proposizione mostrata precedentemente. Abbiamo quindi mostrato, sfruttando la teoria delle categorie, un noto risultato molto utile nello studio della topologia algebrica.

Corollario 9. *Usando le notazioni precedenti, se $A \cap B$ è semplicamente connesso, allora $\pi_1(X, x_0) \cong \pi_1(A, x_0) * \pi_1(B, x_0)$.*

Invece, nel caso in cui $A \cap B$ non è semplicemente connesso, allora la questione si complica e costruire il gruppo fondamentale di X richiede più impegno. Ma, nella sezione di preliminari di teoria delle categoria abbiamo mostrato che, in una categoria con coprodotti ed equalizzatori, sappiamo costruire il pushout di un diagramma. La categoria dei gruppi Grp soddisfa queste ipotesi: infatti possiede sia i coprodotti binari (i.e. prodotti liberi) che i coequalizzatori.

Questi ultimi, possono essere espressi nel modo seguente: dati due gruppi G, H e due morfismi di gruppi $f, g : G \to H$, allora il coequalizzatore di f e g è dato dal gruppo quoziente di H per la chiusura normale dell'insieme $S \stackrel{def}{=} \{f(x)g(x)^{-1} | x \in G\}$.

Ora dovrebbe essere immediato oservare che, nel caso generale, $\pi_1(X, x_0)$ è isomorfo al gruppo quoziente $(\pi_1(A, x_0) * \pi_1(B, x_0))/Y$ dove $Y = < \alpha_*(\gamma)\beta_*(\gamma) | \gamma \in \pi_1(A \cap B, x_0) >$ che coincide con il prodotto amalgamato. Abbiamo quindi mostrato la relazione tra il teorema di Van-Kampen formulato tramite prodotto amalgamato e il teorema di Van-Kampen enunciato da Grothendieck.

Veniamo infine alle ultime considerazioni sull'importanza della dimostrazione di Grothendieck del teorema di Van-Kampen: infatti Grothendieck ha dimostrato una versione più debole del teorema rispetto a Van-Kampen. Come mai diamo così tanta importanza alla tecnica dimostrativa di Grothendieck?
La risposta risiede nel fatto che la dimostrazione di Grothendieck può essere estesa facilmente ad altri contesti algebrici, tra cui il gruppo fondamentale étale per le varietà e gli schemi. In quest'ultima branca della geometria algebrica, il concetto di cammino o di cappio non è più utile, mentre la nozione di ricoprimento assume un ruolo fondamentale.

Osseriviamo inoltre che, nella dimostrazione di Grothendieck, siamo partiti da due rivestimenti sugli aperti A e B e abbiamo costruito un rivestimento sullo spazio X. In alternativa avremmo potuto procedere senza costruire questo rivestimento, lavorando con una famiglia di rivestimenti di Galois. Quest'ultimo modo di ragionare è tipico della teoria di Galois di Grothendieck che studia in modo astratto la teoria di Galois dei campi per ottenere informazioni sui gruppi fondamentali nella topologia algebrica. Quest'ultima teoria, tra le varie possibili applicazioni, viene utilizzata per definire il gruppo fondamentale étale.

BIBLIOGRAFIA

- Marco Manetti. *Topologia*. Springer, 2014.
- Saunders Mac Lane. *Categories for the Working Mathematician*. Springer, 1997.
- James S. Milne. *Lectures on Étale Cohomology* (2013). Si trova online a questo link.

NAVIER-STOKES: UN TURBOLENTO PROBLEMA DEL MILLENNIO

DOMENICO CAFIERO

1. INTRODUZIONE ALLE EQUAZIONI DI NAVIER-STOKES

Le equazioni di Navier-Stokes costituiscono uno dei 7 Problemi del Millennio. La soluzione di queste equazioni permette di descrivere rigorosamente il moto di un qualsiasi fluido. Nonostante siano passati alcuni secoli dalla loro formulazione, per le equazioni di Navier-Stokes in 3 dimensioni non c'è ancora una dimostrazione rigorosa che permette di dare informazioni sul problema di esistenza e unicità delle soluzioni.
Ricordiamo due date fondamentali nella formulazione di questo problema:

- 1755: Eulero formula le equazioni per fluidi non viscosi
- 1822-1830: Viene generalizzata l'equazione di Eulero a fluidi viscosi in maniera indipendente da Navier, Stokes, Poisson e Saint-Venant

Prima dare la formulazione completa delle equazioni, introduciamo un po' di terminologia fisica utile nel contesto della fluidodinamica e la relativa "traduzione" matematica.

Definizione 1. Un fluido è una sostanza che si deforma illimitamente se sottoposta a uno sforzo di taglio costante, anche molto piccolo.

Le idee fondamentali per la deduzione delle equazioni sono le seguenti:

- secondo principio della dinamica
- mezzo continuo
- pressione
- forza viscosa

Come per ogni sistema fisico si parte dalle equazioni del moto: le equazioni di Navier-Stokes descrivono il moto di un fluido Newtoniano incomprimibile. Immaginiamo che il fluido sia composto N molecole e applichiamo la seconda legge di Newton. Per $j = 1, \dots, N$ la dinamica della $j-$esima molecola è descritta da:

$$\ddot{x}_j(t) = F(x_1, \dots, x_N) \tag{1}$$

L'evoluzione del sistema di N equazioni determina completamente il moto del fluido. Sorge però un problema:

Osservazione 2. In generale il numero N di particelle in un fluido è molto grande. Quindi la seconda legge di Newton considerata per ogni singola molecola di fluido diventa complicata da gestire. É fondamentale l'ipotesi del mezzo continuo, cioè il fluido occupa completamente una parte di spazio.

2. LA FORMULAZIONE DELLE EQUAZIONI DI NAVIER-STOKES

2.1. Definizioni preliminari.

Definizione 3. Definiamo un corpo continuo tridimensionale ogni terna $(\mathcal{C}, \mathcal{A}, m)$, dove:

- $\mathcal{C}$ è uno spazio topologico dotato di una famiglia Φ di omeomorfismi del tipo $\varphi : \mathcal{C} \to S_\varphi$, con S_φ chiusura di un aperto dello spazio geometrico;
- $\mathcal{A}$ è la $\sigma-$algebra di Borel dello spazio topologico $\mathcal{C}$.
- m è una misura che prende il nome di distribuzione di massa

Definizione 4. Preso un sottoinsieme A di $\mathcal{A}$ definiamo $m(A)$ la massa di A e, in particolare, $m(\mathcal{C})$ la massa del corpo continuo.

In quello che segue ci concentreremo su sottoinsiemi $\Omega \subset \mathbb{R}^3$ dotato della misura di Lebesgue.
Avendo definito il fluido come un continuo bisogna imporre la conservazione di alcune quantità fisiche .

2.2. Conservazione della massa. Imponiamo, innanzitutto, la coservazione della massa.
Sia $u(x,t) \in \mathbb{R}^d$ $(d = 2, 3)$ il campo di velocità del fluido in una data posizione $x \in \mathbb{R}^d$ al dato tempo $t \in \mathbb{R}$. Indichiamo con $\rho(x,t) \in \mathbb{R}$ la densità del fluido e con $p(x,t) \in \mathbb{R}$ la pressione. Consideriamo un elemento di volume $\Omega \subset \mathbb{R}^3$ del fluido con superficie $\partial\Omega$. La variazione sarà data dall'equazione seguente

$$\frac{\mathrm{d}}{\mathrm{d}t} \int_\Omega \rho(x,t)\, \mathrm{d}x = - \int_{\partial\Omega} \rho u \cdot n \, \mathrm{d}S, \tag{2}$$

dove $\mathrm{d}S$ è l'elemento di superficie, e $n(x) = (n_1(x), \ldots, n_d(x))$ è la normale esterna alla superficie. Richiamiamo un teorema (in versione più "semplice") che ci servirà a trattare meglio il secondo termine:

Teorema 5 (della divergenza)**.** *Sia $\Omega \subset \mathbb{R}^3$ un insieme compatto delimitato da una superficie liscia $\partial\Omega$. Sia $f = (f_1, f_2, f_3) : \mathbb{R}^3 \to \mathbb{R}^3$ di classe $\mathcal{C}^1$, allora vale*

$$\int_\Omega \mathrm{div}(f)\, \mathrm{d}x = \int_{\partial\Omega} f \cdot n \, \mathrm{d}S, \tag{3}$$

dove $\mathrm{div}(f) = \sum_{i=1}^3 \partial_{x_i} f_i$ e $n(x) = (n_1(x), \ldots, n_3(x))$ è la normale esterna alla superficie.

Applichiamo questo teorema al secondo membro dell'equazione (2). Risulta:

$$- \int_{\partial\Omega} \rho u \cdot n \, \mathrm{d}S = - \int_\Omega \mathrm{div}(\rho u)\, \mathrm{d}x \tag{4}$$

Riassumendo troviamo che

$$\frac{\mathrm{d}}{\mathrm{d}t} \int_\Omega \rho \, \mathrm{d}x = \int_\Omega \frac{\partial \rho}{\partial_t} \, \mathrm{d}x = - \int_\Omega \mathrm{div}(\rho u)\, \mathrm{d}x \tag{5}$$

Dall'arbitrarietà di Ω si ottiene

$$\partial_t \rho + \operatorname{div}(\rho u) = 0. \tag{6}$$

2.3. Conservazione della quantità di moto. La quantità di moto di un dato volume di fluido Ω cambia sotto l'azione del flusso attraverso la superficie e sotto l'azione delle forze sulla superficie del volume stesso. Per modellizzare le forze, assumiamo l'esistenza di una matrice $\sigma = (\sigma_{ij})_{i,j=1,\dots,d}$ che collega la direzione della normale alla superficie alla direzione e intensità della forza:

$$f_i = \sum_{j=1}^{d} \sigma_{ij} n_j \tag{7}$$

Ragionando come nella conservazione della massa possiamo impostare l'equazione seguente

$$\frac{\mathrm{d}}{\mathrm{d}t} \int_\Omega \rho u_i \mathrm{d}x = - \int_{\partial\Omega} \sum_{j=1}^{d} (\rho u_i) u_j n_j \, \mathrm{d}S + \int_{\partial\Omega} \sum_{j=1}^{d} \sigma_{ij} n_j \, \mathrm{d}S \tag{8}$$

Dall'arbitrarietà di Ω e usando il teorema della divergenza

$$\partial_t(\rho u_i) + \operatorname{div}(\rho u_i u) = \operatorname{div}(\sigma_{i\cdot}) \tag{9}$$

Dalla conservazione della massa e della quantità di moto abbiamo ricavato

$$\begin{aligned} &\partial_t \rho + \operatorname{div}(\rho u) = 0 \\ &\partial_t(\rho u_i) + \operatorname{div}(\rho u_i u) = \operatorname{div}(\sigma_{i\cdot}) \end{aligned}$$

Inseriamo ora l'equazione di continuità nell'equazione di conservazione del momento e ricaviamo

$$\rho \left[\partial_t u_i + \sum_{j=1}^{d} (u_j \cdot \partial_{x_j}) u_i \right] = \sum_{j=1}^{d} \partial_{x_j} \sigma_{ij} \tag{10}$$

o, equivalentemente,

$$\rho[\partial_t u_i + (u \cdot \nabla) u_i] = \nabla \cdot \sigma_{i\cdot}. \tag{11}$$

L'equazione (11) collega la densità del fluido, la velocità e il tensore degli sforzi. Ma queste non sono le quantità di interesse che c'eravamo prefissati: pressione e forze. Vogliamo, in ciò che segue, esprimere tutto in funzione di pressione e forza.

2.4. Leggi costitutive. Vogliamo quindi capire meglio come è fatto il tensore degli sforzi. Distinguiamo due tipi di fluidi: i **fluidi viscosi** e i **fluidi non viscosi**. I fluidi non viscosi sono fluidi senza frizione interna. Le froze di superficie sono dovute solo alla pressione. Sono quindi parallele alla normale esterna e l'intensità non dipende dalla direzione.

$$f_i = \sum_{j=1}^{d} \sigma_{ij} n_j = - \sum_{j=1}^{d} p \delta_{ij} n_j = -p n_i \tag{12}$$

Da qui ricaviamo la legge costitutiva

$$\sigma_{ij} = -p \delta_{ij} \tag{13}$$

Inserendo questa legge nell'equazione (11) otteniamo

$$\partial_t u + (u \cdot \nabla)u = -\frac{1}{\rho}\nabla p \tag{14}$$

L'ultimo passaggio è collegare p con ρ e u. Una scelta tipica è la sequente: $p = c\rho^\gamma$ per qualche costante $c > 0$ e $\gamma \geq 1$. Per fluidi incomprimibili si ha $\rho = cost.$ e si ottengono le equazioni di Eulero

$$\begin{cases} \partial_t u + (u \cdot \nabla)u = -\frac{1}{\rho}\nabla p \\ \nabla \cdot u = 0 \end{cases} \tag{15}$$

Per un fluido viscoso la relazione costitutiva è.

$$\sigma_{ij} = -p\delta_{ij} + \tau_{ij} \tag{16}$$

dove τ_{ij} modellizza la frizione interna. Possiamo immaginare che le forze agiscano sulla superficie superiore e inferiore del nostro volume, e che siano proporzionali alla differenza delle due velocità. Per un elemento infinitesimo di volume f sarà proporzionale allo sforzo $\partial_{x_2} u_1$. Le forze sono perpendicolari alla superficie superiore. Perciò troviamo

$$\tau_{12} = \mu \partial_{x_2} u_1 \tag{17}$$

dove $\mu > 0$ è la costante di viscosità dinamica. Il fluido è isotropo, quindi σ dev'essere simmetrico, da cui

$$\tau_{ij} = 2\mu\dot{\varepsilon}_{ij} + \lambda \sum_{k=1}^{d} \dot{\varepsilon}_{kk}\delta_{ij} \tag{18}$$

con

$$\dot{\varepsilon}_{ij} = \frac{1}{2}(\partial_{x_j} u_i + \partial_{x_i} u_j) \tag{19}$$

2.5. Le equazioni di Navier-Stokes. La forma funzionale di ρ dipende dal tipo di fluido che stiamo considerando: per l'aria la proprietà di comprimibilità è molto importante, mentre per fluidi come l'acqua possiamo considerare ρ come costante, quindi $\partial_t \rho = 0$. L'equazione di continuità diventa:

$$\mathrm{div} u = 0 \tag{20}$$

Da $\sum_{k=1}^{d} \dot{\varepsilon}_{kk} = \sum_{k=1}^{d} \partial_{x_k} u_k = 0$ si trova che $\tau_{ij} = 2\mu\dot{\varepsilon}_i j$. Inoltre

$$\sum_{j=1}^{d} \partial_{x_j}\tau_{ij} = \sum_{j=1}^{d} \partial_{x_j}(\partial_{x_j} u_i + \partial_{x_i} u_j) = \sum_{j=1}^{d} \partial_{x_j}^2 u_i + \partial_{x_i}\left(\sum_{j=1}^{d} \partial_{x_j} u_j\right) = \sum_{j=1}^{d} \partial_{x_j}^2 u_i \tag{21}$$

da cui

$$\partial_t u + (u \cdot \nabla)u = -\frac{1}{\rho}\nabla p + \frac{\mu}{\rho}\Delta u \tag{22}$$

Siamo arrivati quindi alla forma delle equazioni di Navier-Stokes

$$\begin{cases} \partial_t u + (u \cdot \nabla)u = -\frac{1}{\rho}\nabla p + \frac{\mu}{\rho}\Delta u \\ \nabla \cdot u = 0 \end{cases} \tag{23}$$

Le equazioni scritte coinvolgono grandezze fisiche che possiedono una loro dimensione. Vogliamo ora eliminarle, cioè procediamo con l'adimensionalizzazione delle equazioni. Definiamo:

$$u = Uu^*, \qquad x = lx^*, \qquad p = \rho U^2 p^*, \qquad t = lt^*/U \tag{24}$$

dove U e l sono rispettivamente la velocità tipca e la lunghezza tipica del flusso. Sostituendo ed eliminando gli asterischi, si ottengolo le equazioni di Navier-Stokes in forma adimensionale

$$\begin{cases} \partial_t u + (u \cdot \nabla)u = -\nabla p + \frac{1}{\mathcal{R}}\Delta u \\ \nabla \cdot u = 0 \end{cases} \tag{25}$$

dove $\mathcal{R} = Ul\mu/\rho$ è un parametro fisico detto numero di Reynold. Più grande è $\mathcal{R}$ più complesso è il fluido. A livello puramente matematico consideriamo $\mathcal{R} = 1$.

2.6. La formulazione vorticosa. Le equazioni (25) vedono come incognita il campo di velocità del fluido. Si possono formulare in un altro modo, coinvolgendo quella che è la vorticità del fluido. Consideriamo la vorticità, cioè la densità superficiale di circolazione, così definita

$$\omega = \nabla \times u = \begin{pmatrix} \partial_{x_2} u_3 - \partial_{x_3} u_2 \\ \partial_{x_3} u_1 - \partial_{x_1} u_3 \\ \partial_{x_1} u_2 - \partial_{x_2} u_1 \end{pmatrix} \tag{26}$$

nel caso 3-dimensionale. Nel caso 2-dimensionale definiamo

$$\omega = \partial_{x_1} u_2 - \partial_{x_2} u_1 \tag{27}$$

Applichiamo l'operatore $\nabla\times$ alle equazioni di Navier-Stokes e otteniamo l'equazione per la vorticità. In 3D si ottiene

$$\partial_t \omega = \nu\Delta\omega - (u \cdot \nabla)\omega + (\omega \cdot \nabla)u \tag{28}$$

In 2D si ottiene

$$\partial_t \omega = \nu\Delta\omega + (\omega \cdot \nabla)u \tag{29}$$

Inoltre se consideriamo l'equazione 3D e siamo in $\Omega = \mathbb{R}^3$ possiamo ricostruire u partendo da ω attraverso la legge di Biot-Savart

$$u(x) = \int_{\mathbb{R}^3} \frac{1}{4\pi|x-y|} \mathrm{rot}\omega(y)\mathrm{d}y \tag{30}$$

Osservazione 6.

- Osserviamo che l'equazione (29) è un'equazione del trasporto per la vorticità
- L'equazione (28), oltre ai termini di diffusione e di trasporto, contiene anche il termine di produzione $(u \cdot \nabla)\omega$.
- Le differenze nell'approccio all'esistenza globale e unicità tra il caso 2D e 3D non sono puramente matematiche: a livello fisico, si mostra tramite esperimenti che nel caso 3D si creano vortici sempre più piccoli, mentre nel caso 2D i vortici più piccoli svaniscono perché "mangiati" da quelli grandi.

- In $\mathbb{R}^d$ o $\mathbb{T}^d$, $\omega = 0$ è una soluzione all'equazione della vorticità: la vorticità si conserva. La conservazione della vorticità insieme all'incomprimibilità del fluido ci permettono di costruire delle soluzioni. Dal fatto che $\omega = \nabla \times u = 0$ si ha l'esistenza di un potenziale $\Phi : \mathbb{R}^d \to \mathbb{R}$ con $u = \nabla\Phi$ e tale che $\Delta\Phi = 0$. Questo è detto flusso potenziale.

2.7. Un esempio di soluzione in 2D. Diamo l'esempio dei così detti flussi di deformazione irrotazionale. Questi flussi sono dati da

$$u(x,t) = \gamma \begin{pmatrix} -x_1 \\ x_2 \end{pmatrix}, \qquad p(x,t) = p_0 - \frac{\gamma^2}{2}(x_1^2 + x_2^2) \tag{31}$$

I vortici sono dati da

$$\omega(x,t) = \omega_0 \begin{pmatrix} -x_1 \\ x_2 \end{pmatrix}, \qquad p(x,t) = p_0 + \frac{\omega_0^2}{2}(x_1^2 + x_2^2) \tag{32}$$

3. IL PROBLEMA DI ESISTENZA E UNICITÀ E LO STATEMENT DEL MILLENIUM PRIZE

Avendo a che fare con un'equazione differenziale alle derivate parziali, affinché si possa pensare a problemi di esistenza e unicità bisogna dare delle condizioni ulteriori. Noi prendiamo il seguente problema di Cauchy

$$\begin{cases} \partial_t u + (u \cdot \nabla)u + \nabla p = \nu\Delta u + f_i(x,t) \\ \nabla \cdot u = 0 \qquad\qquad\qquad\qquad\qquad\qquad x \in \mathbb{R}^3, t \geq 0 \\ u(x,0) = u_0(x) \end{cases} \tag{33}$$

dove $\nu > 0$ è la viscosità e $f_i(x,t)$ è una componente di forze esterne (gravità per esempio). Richiediamo inoltre che $u_0(x)$ sia un campo $\mathcal{C}^\infty$ a divergenza nulla. Imponiamo ora alcune condizioni ulteriori, che seguono la descrizione fisica del teorema:

- Vogliamo che $u(x,t)$ non cresca molto per $|x| \to \infty$.
- Chiediamo $|\partial_x^\alpha u_0(x)| \leq C(\alpha, K)(1+|x|)^{-K}$ su $\mathbb{R}^3$ per ogni α, K.
- Chiediamo $|\partial_x^\alpha \partial_t^m f_i(xnt)| \leq C(\alpha, m, K)(1+|x|+t)^{-K}$ su $\mathbb{R}^3 \times [0,\infty)$ per ogni α, m, K.
- Inoltre, per essere fisicamente accettabili, si richiede che le soluzioni siano tali che

$$u, p \in \mathcal{C}^\infty(\mathbb{R}^3 \times [0,\infty)) \tag{34}$$

$$\int_{\mathbb{R}^3} |u(x,t)|^2 \mathrm{d}x < C \qquad \text{per ogni } t \geq 0 \tag{35}$$

Statement del millenium prize: sia $\nu > 0$. Sia $u_0(x)$ un qualsiasi campo smooth a divergenza nulla tale che $|\partial_x^\alpha u_0(x)| \leq C(\alpha, K)(1+|x|)^{-K}$ su $\mathbb{R}^3$ per ogni α, K. Sia $f(x,t)$ identicamente nulla. Allora esistono delle funzioni smooth $p(x,t)$, $u_i(x,t)$ su $\mathbb{R}^3 \times [0,\infty)$ che soddisfano (33), (34), (35).

Osservazione 7. Riportiamo di seguito alcune considerazioni finali sui risultati fino a ora ottenuti.

- In due dimensioni i risultati sono già noti.
- In tre dimensioni, il termine di produzione complica le cose.

- In tre dimensioni lo statement è vero per dati iniziali $u_0(x)$ di taglia piccola oppure localmente, cioè se si sostituisce $[0, \infty)$ con un piccolo intervallo $[0, T)$, dove T dipende dal dato iniziale.
- Il massimo T possibile viene detto "blow-up time".
- Accadono cose spiacevoli vicino ai tempi di blow-up: già per l'equazione di Eulero, se $T < \infty$ si ha che

$$\int_0^T \left\{ \sup_{x \in \mathbb{R}^3} |\omega(x,t)| \right\} \mathrm{d}t = \infty$$

  cioè la vorticità esplode rapidamente.
- Si sono provati metodi standard nella teoria moderna delle PDE: studio di soluzioni deboli prima, e passaggio a soluzioni smooth poi.
- C'è stato un paziale successo: non è nota per esempio l'unicità.
- Uno dei più bei teoremi su Navier-Stokes è dovuto a Caffarelli-Kohn-Nieremberg e riguarda una parziale regolarità delle soluzioni.
- Il problema è ancora irrisolto. Servono probabilmente idee "nuove e profonde".

BIBLIOGRAFIA

- G. Schneider, H. Uecker, *Nonlinear PDEs A Dynamical Systems Approach*, Graduate Studies in Mathematics, AMS (2017)
- M. Bramanti, C. D. Pagani, S. Salsa, *Analisi Matematica 2*, Zanichelli (2008)

L'ILLUSIONE DELLA SCELTA

GABRIELE CASSESE

1. INTRODUZIONE

In varie occasioni si sente dire che un risultato "dipende dall'assioma della scelta"; In che senso "dipende"? Cosa succede se rimuoviamo, o indeboliamo, l'assioma della scelta? Un mondo in cui tutti gli insiemi in $\mathbb{R}$ sono misurabili sarebbe senza dubbio interessante, ma ne vale la pena? Il nostro obbiettivo è cercare di esporre alcune relazioni dell'assioma della scelta con risultati più propriamente appartenenti alla matematica di tutti i giorni, con l'idea di dare alcuni strumenti per rispondere alla domanda: vale la pena di tenere l'assioma della scelta? Ai posteri l'ardua sentenza. Prima di cominciare, una precisazione: tutti i risultati per i quali non citeremo una esplicita referenza sono dimostrati in [1].

2. RIPASSO INSIEMISTICO

Dove non diversamente specificato, ci muoviamo in ZF, la teoria degli insiemi di Zermelo-Fraenkel, di cui assumiamo la consistenza. Cominciamo col ricordare le seguenti equivalenze:

Teorema 1. *Sono equivalenti i seguenti enunciati:*

(1) Data una collezione indicizzata di insiemi $\{A_i\}_{i\in I}$ non vuoti, esiste $f : I \to \cup A_i : f(i) \in A_i$, detta funzione di scelta
(2) (Lemma di Zorn) Sia X un poset. Se ogni catena ha un upper bound, X ammette un elemento massimale
(3) (Principio del buon ordinamento) Sia X un insieme. Esiste una relazione $\leq$ tale che $(X, \leq)$ è un insieme ben ordinato.

Dimostrazione. Cominciamo col dimostrare le direzioni più semplici: innanzitutto $(2) \to (3)$. Difatti, sia[1]

$$\mathcal{O} = \{(S, R) : S \subset X, R \subset S^2 : R \text{ è un buon ordine su } S\}$$

Su di esso poniamo la seguente relazione d'ordine: $(A, R_1) \preccurlyeq (B, R_2)$ se $A \subset B$ e $R_2 \cap A^2 = R_1$, con l'ulteriore condizione che tutti gli elementi di $B - A$ siano maggiori di tutti gli elementi di A (rispetto a R_2). È evidente che ogni catena (A_i, R_i) in tale insieme ha un upper bound $(\cup A_i, \cup R_i)$. Per Zorn esiste dunque (A, R) massimale in $(\mathcal{O}, \preccurlyeq)$. Per assurdo, sia $x \in X - A$; è facile definire R' come

[1] che questo sia un insieme segue dagli assiomi di ZF, poiché la proprietà di essere un buon ordine può essere esplicitata mediante una formula

estensione di R in cui x è maggiore di ogni elemento di A, ma questo implica $(A, R) \preccurlyeq (A \cup \{x\}, R')$, assurdo. Dimostriamo ora $(3) \to (1)$: se $\leq$ un buon ordine su $\cup A_i$, $f(i) := \min_{\leq} A_i$ dà una funzione di scelta. L'implicazione più difficile è senza dubbio $(1) \to (2)$. Per ottenerla, ci avvaliamo del seguente lemma

Lemma 2 (Hartogs)**.** *Sia X un insieme. Esiste un ordinale minimo ω che non può essere iniettato in X. Esso è detto numero di Hartogs di X*

Dimostrazione. Definiamo innanzitutto l'insieme $\mathcal{O}$ definito come precedentemente. Ogni suo elemento può essere mappato nel suo tipo d'ordine, ottenendo così una funzione $f : \mathcal{O} \to \text{Ord}$. Poichè, in ZF, l'immagine mediante una funzione di un insieme è un insieme, otteniamo che $f(\mathcal{O})$ è un insieme in Ord. È evidente che $f(\mathcal{O})$ è un insieme transitivo di ordinali ed è quindi lui stesso un ordinale (chiamiamolo ω) ed è facile vedere che soddisfa i requisiti richiesti: se, per assurdo, esistesse una iniezione da ω in X, allora $\omega \in f(\mathcal{O}) = \omega$, ovvero $\omega \in \omega$, assurdo; inoltre, se $\alpha < \omega$, $\alpha \in \omega$ e quindi esiste una iniezione da α in X. □

Supponiamo ora per assurdo che esista un controesempio al lemma di Zorn, sia esso $(X, <)$ (ovviamente $X \neq \emptyset$). Ciò implica che, data una catena $S \subset X$, esiste $x \in X - S : x > S$. Sia quindi $\mathcal{F} := \{X - S : S \text{ è una catena}\}$, sia $f : S \to \cup(X - S)$ una funzione di scelta e sia ω il numero di Hartogs di X. Definiamo per induzione transfinita $h : \omega \to X$ come segue: $h(0) = x_0$ arbitrario, $h(\alpha) = f(\{x_\lambda\}_{\lambda<\alpha})$. È evidente che questa è un'iniezione, il che ci dà un assurdo. □

Ricordiamo le seguenti formulazioni equivalenti dell'assioma della scelta, che si ottengono rapidamente da quelle appena viste

(1) Data una collezione $\{X_i\}$ di insiemi non vuoti, $\prod_{i\in I} X_i \neq \emptyset$
(2) Dati due insiemi A, B, esiste necessariamente o una iniezione o una suriezione da A in B (in altri termini leggermente impropri, la relazione di cardinalità è un ordine totale)
(3) Ogni funzione suriettiva ha un'inversa destra.

Ricordiamo inoltre le seguenti formulazioni, più deboli, dell'assioma della scelta:

Definizione 3. (1) Assioma della scelta dipendente (DC): sia X un insieme non vuoto e sia R una relazione binaria su X tale che per ogni $a \in X$ esiste $b \in X$ per cui aRb. Per ogni $x_0 \in X$ esiste una successione $\{x_n\}_{n\in\mathbb{N}}$ tale che per ogni n $x_n R x_{n+1}$
(2) Assioma della scelta numerabile (CC): l'assioma della scelta vale con la condizione $|I| \leq \aleph_0$
(3) Lemma dell'ultrafiltro (UL): dato un insieme X, ogni filtro su X è contenuto in un ultrafiltro

Evidentemente $(AC) \to (DC) \to (CC); (AC) \to (UL)$.

Osservazione 4. Si può dimostrare (assumendo la coerenza di ZF) che nessuna delle implicazioni appena evidenziate è reversibile e non vi sono altre implicazioni (ovvero (DC) e (UL) sono indipendenti così come $(CC), (UL)$). Per coloro interessati di logica, Löwenheim-Skolem è equivalente a (DC), il teorema di completezza di Gödel è equivalente a (UL).

3. L'ASSIOMA DELLA SCELTA IN TOPOLOGIA

Sia (TT) il teorema di Tychonov, (TTH) il teorema di Tychonov per spazi di Hausdorff e (BT) il teorema di categoria di Baire per spazi metrici. Prima di cominciare, una parola di cautela: molte delle definizioni date in topologia, sono equivalenti tra loro solamente assumendo l'assioma della scelta in una qualche forma (ad esempio, la compattezza per ultrafiltri diventa banale se non esistono ultrafiltri non principali[2]). Tuttavia, l'insidia non si limita a questo: svariate dimostrazioni presentate nei corsi di topologia (specialmente in quelli iniziali), utilizzano inutilmente l'assioma della scelta, ovvero lo utilizzano quando non è necessario. Ne diamo un esempio: poniamo di volter dimostrare l'asserto "un insieme $A \subset X$ è aperto se per ogni $a \in A$ esiste un intorno aperto totalmente contenuto in A". Una delle usuali dimostrazioni è

Dimostrazione. Per ogni $x \in A$, esiste un intorno I_x totalmente contenuto in A, quindi $A = \cup I_x$ è unione di aperti quindi aperto □

Questa dimostrazione utilizza l'assioma della scelta per definire la funzione I, ma ciò non è necessario: è sufficiente definire $I_x = \cup_{s \in S_x} s$, dove S_x è l'insieme di intorni di x contenuti in A. L'errore può sembrare innoquo, ma ci sono situazioni in cui è più insidioso: si consideri ad esempio una rete $x_\lambda \in \prod X_i$ tale che la sua proiezione su ogni fattore converge. Se lo spazio non è di Hausdorff, la proiezione può convergere a più valori per ogni i, siano essi C_i. È evidente che x_λ converge a z sse $z \in \prod C_i$, ma questo potrebbe essere vuoto senza AC. Perciò, l'asserto "una rete converge nel prodotto $\prod X_i$ sse la sua proiezione su ogni fattore converge", richiede la piena forza dell'assioma della scelta per essere dimostrato, anche se nella dimostrazione il suo utilizzo sembra innocuo.

Teorema 5. (TT) *è equivalente a* (AC)

Dimostrazione. Una direzione è l'usuale dimostrazione di TT, che ricordiamo brevemente: poichè uno spazio è compatto sse ogni rete ha una sottorete convergente, è sufficiente dimostrare che una rete $\{z_\lambda\} \subset \prod X_i$ ammette una sottorete convergente. (UL) implica l'esistenza di una sottorete universale, sia essa h_v. Poiché la sua proiezione su ogni fattore converge (per compattezza di ciascuno dei fattori), l'assioma della scelta implica che essa converge. L'altra direzione è leggermente più laboriosa, ed è stata dimostrata per la prima volta da Kelley: Sia $\{A_i\}$ una collezione di insiemi non vuoti, che topologizziamo con la topologia cofinita. Sia X_i definito come l'unione disgiunta di A_i e $\{i\}$: $X := \prod X_i$ è compatto per (TT). Poiché A_i è chiuso in X_i, $\pi_i^{-1}(A_i)$ (dove π_i indica la proiezione sul fattore i) è chiuso in X. Ora, la famiglia $\{\pi_i^{-1}(A_i)\}$ ha la FIP, poiché $\cap_{i_1=1}^{i_n} \pi_{i_j}^{-1}(A_{i_j})$ contiene il punto x tale che per $i \notin \{i_j\}$, $x_i = i$, altrimenti $x_i \in A_i$ (questo è possibile poiché una funzione di scelta esiste per famiglie finite in ZF). Per compattezza, $\prod A_i = \cap \pi_i^{-1}(A_i) \neq \emptyset$ e il risultato è dimostrato. □

Teorema 6. (TTH) *è equivalente a* (UL)

[2] S. Feferman ha dimostrato che è coerente con ZF che $\mathbb{N}$ non ammetta ultrafiltri non principali, A. Blass ha esteso questo risultato dimostrando che è coerente che non esistano ultrafiltri non principali

Dimostrazione. La dimostrazione dell'implicazione $(UL) \to (TTH)$ è sostanzialmente equivalente a quella esposta nel teorema precedente per $(AC) \to (TT)$, col solo accorgimento che, essendo lo spazio di Hausdorff, non è necessario utilizzare l'assioma della scelta per garantire la convergenza della sottorete universale. Per l'altra direzione, osserviamo innanzitutto che (TTH) implica l'esistenza della compattificazione di Stone-Cech per spazi $T_{3+\frac{1}{2}}$: difatti, dato uno spazio X, esso si embedda in $[0,1]^{\mathcal{C}^0(X,[0,1])}$ e la chiusura dell'immagine di tale embedding è la compattificazione cercata. Sia ora X un insieme e $\mathcal{F} = \{F_i\}$ un filtro su tale insieme. Mettiamo su X la metrica discreta e consideriamo ora $\mathcal{G} = \bar{\mathcal{F}} = \{\bar{F}_i\}_i$, dove la chiusura è da intendersi in βX. Per proprietà di filtro, $\mathcal{G}$ ha la proprietà dell'intersezione finita e quindi (essendo una famiglia di insiemi chiusi in un compatto) ha intersezione non vuota e sia x un elemento di tale intersezione. Sia $\mathcal{H} := \{A \subset X : \bar{A} \ni x\}$. Affermiamo innanzitutto che si tratta di un ultrafiltro: l'unica proprietà non ovvia è la proprietà di intersezione finita. Dati quindi $A_1, A_2 \in \mathcal{H}$, supponiamo per assurdo che $\overline{A_1 \cap A_2}$ non contenga x. In particolare, $\hat{A}_2 := A_2 - (A_1 \cap A_2), A_1$, sono due insiemi disgiunti in X le cui rispettive chiusure in βX contengono uno stesso elemento. Perciò esiste $f : X \to [0,1]$ tale che $f(A_1) = 1, f(\hat{A}_2) = 0$; per proprietà di βX esse ammettono un estensione e ciò è assurdo poiché tale estensione dovrebbe soddisfare $f(x) = 0, f(x) = 1$ in contemporanea. $\mathcal{H}$ è dunque un ultrafiltro e ovviamente estende $\mathcal{F}$, dando (UL) □

Osservazione 7. Abbiamo difatti dimostrato di più, ovvero che (TTH) è equivalente anche all'esistenza della compattificazione di Stone Cech per spazi $T_{3+\frac{1}{2}}$.

Teorema 8. *(DC) è equivalente a (BT).*

Dimostrazione. $(DC) \to (BT)$ si dimostra come usualmente. Per l'altra direzione, sia X un insieme con una relazione R binaria intera e sia $x_0 \in X$. Mettiamo su $\{f \in X^{\mathbb{N}} : f(0) = x_0\}$ la seguente metrica: $d(f,g) = 2^{-\min\{n : f(n) \neq g(n)\}}$. È facile vedere che si tratta di uno spazio metrico completo. Definiamo $D_n := \cup_{m>n}\{f : f(n)Rf(m)\}$; si vede facilmente che esso è aperto e denso. Ora, $\cap D_n$ è denso per Baire ; sia f un suo elemento. Esiste quindi $n_1 : f(0)Rf(n_1)$. Possiamo quindi definire per induzione g tale che $g(0) = x_0$ e $g(n+1) := f(\min\{k : g(n)Rf(k))$ e questa definisce la successione richiesta. □

Se lo spazio metrico è separabile, BT si può dimostrare in ZF:

Dimostrazione. Sia U_n una famiglia di insiemi aperti densi. A meno di considerare $\cap_{i=1}^{n} U_i$, possiamo supporre che gli insiemi siano innestati. Rimane da dimostrare che $U = \cap_i U_i$ è denso, ovvero che per ogni x, ogni bolla $B(x,r)$ con $r > 0$ interseca U. Sia ora $\{e_k\}_{k\in\mathbb{N}}$ l'insieme numerabile denso nello spazio. Per costruzione, esiste k_1 minimale tale che $e_{k_1} \in B(x, r/2) \cap U_1$. Procedendo per induzione, definiamo $k_{n+1} = \min\{k : e_k \in B(e_{k_n}, r/2^n)\}$. La successione e_{k_n} è dunque una successione di Cauchy di elementi contenuta in U e in $B(x,r)$, dando il risultato. □

In particolare, BT vale in ZF per $L^p(\mathbb{R})$ con $p \in [1, +\infty)$ e similmente per ℓ^p.

4. L'ASSIOMA DELLA SCELTA IN ANALISI

Moltissime cose si potrebbero dire e dimostrare sull'utilizzo dell'assioma della scelta in analisi. In particolare, sarebbe interessante soffermarsi sull'utilizzo in analisi funzionale e in questioni di misurabilità. Per problemi di tempo e spazio, analizzeremo la prima delle due, mentre per la seconda ci limitiamo a enunciare una serie di risultati:

Teorema 9. *È compatibile con ZF che $\mathbb{R}$ sia l'unione di un'infinità numerabile di insiemi numerabili e quindi che $\mathcal{B}(\mathbb{R}) = \mathcal{P}(\mathbb{R})$. È compatibile con $ZF + (DC)$ (se si assume l'ipotesi dell'esistenza di un cardinale inaccessibile, vedasi [6]) che $\mathcal{L}(\mathbb{R}) = \mathcal{P}(\mathbb{R})$[3]. Infine, osserviamo che il teorema di Hahn-Banach (in ZF) è sufficiente a costruire il paradosso di Banach- Tarski ([7])*

Osservazione 10. Spesso, nei corsi introduttivi di teoria della misura, viene evidenziato che il fatto che l'inclusione $\mathcal{L}(\mathbb{R}) \subset \mathcal{P}(\mathbb{R})$ sia propria richiede l'assioma della scelta, mentre non viene detto niente riguardo l'inclusione $\mathcal{B}(\mathbb{R}) \subsetneq \mathcal{L}(\mathbb{R})$. Difatti, l'usuale dimostrazione mediante induzione transfinita non sembra utilizzare la scelta in alcun modo a un primo sguardo, ma analizzandola più attentamente scopriamo un utilizzo di (CC) nell'utilizzo dell'asserzione "unione numerabile di numerabili è numerabile". Di conseguenza, anche il fatto che questa ultima inclusione sia propria richiede scelta, seppur una forma $((CC))$ più debole in un certo senso.

Teorema 11. *In ZF, (UL) e il teorema di Banach-Alaoglu per spazi di Banach sono equivalenti*

Dimostrazione. Come abbiamo visto nella sezione dedicata alla topologia, (UL) implica (TTH), da cui la dimostrazione di Banach-Alaoglu prosegue come classicamente. Per l'altra direzione, sia X un insieme e sia $\mathcal{F}$ un filtro su tale insieme. $Y = l_\infty(S)$ è uno spazio di Banach. Sia Y^* il suo duale e B la bolla unitaria di questo. Per ogni $h \in Y^*$, definiamo una misura finitamente addittiva come $\mu_h(A) = \mu(\chi_A)$. L'insieme

$$H := \{h \in Y^* : \mu_h(X) = 1, \forall A \in \mathcal{P}(X)\ \mu_h(A) \in \{0,1\}\}$$

è evidentemente un sottoinsieme $*-$chiuso di B e quindi, per B-A, è compatto. Definiamo per ogni $x \in X$ il funzionale φ_x di valutazione in x; evidentemente se prendiamo un elemento f del filtro e definiamo $D_f := \overline{\{\varphi_x : x \in f\}}^*$ otteniamo una famiglia $\{D_f\}$ che ha la FIP e quindi la cui intersezione contiene un elemento, sia esso $g.\mu_g$ evidentemente assume valore 1 su ogni elemento di $\mathcal{F}$ e quindi la famiglia di insiemi su cui vale 1 è l'ultrafiltro cercato. □

Teorema 12. *In ZF, (AC) è equivalente a Krein-Milman+Banach-Alaoglu*

Dimostrazione. Dimostriamo in realtà un asserto leggermente più forte, ovvero che AC è equivalente all'asserto che la bolla B unitaria del duale di uno spazio di Banach ha un punto estremante. Per vederlo, sia $\{A_i\}$ una famiglia di insiemi non

[3]La teoria costruita con tale sistema di assiomi è nota come *dream mathematics*, in quanto in essa abbiamo ancora *DC*, che consente molte costruzioni che richiedono la scelta, ma ogni insieme è misurabile. Essa ha vari inconvenienti, primo dei quali il fatto che Hahn-Banach fallisce

vuoti (che possiamo supporre senza perdita di generalità disgiunti). Sia $A = \cup A_i$ e definiamo lo spazio di Banach

$$X := \left\{ x : A \to \mathbb{R} : \forall \varepsilon > 0 \, \#\{t \in A : |x(t)| > \varepsilon\} < +\infty; \sum_i \sup_{t \in A_i} |x(t)| < +\infty \right\}$$

È facile vedere che esso è uno spazio di Banach se equipaggiato della norma $\sum_i \sup_{t \in A_i} |x(t)|$. Il suo duale può essere identificato con lo spazio

$$X' := \left\{ x : A \to \mathbb{R} : \sup_i \sum_{t \in A_i} |x(t)| < +\infty \right\}$$

dotato di norma $\|x\|_* = \sup_i \sum_{t \in A_i} |x(t)|$. Sia B la bolla di X'. Per assunto, essa ha un punto estremante e; se riusciamo a dimostrare che per ogni i esiste un unico $t : e(t) \neq 0$, il risultato è dimostrato. Dimostriamo innanzitutto che per ogni i esiste almeno un tale t. Se così non fosse per i_0, definiamo $x, y \in X'$ nel seguente modo: preso arbitrario $v \in A_{i_0}$, $x(v) = 1, y(v) = -1$ e per tutti gli altri valori $x = y = e$, contraddicendo l'estremalità di e. Supponiamo ora che per i_0 esistano $s, t : e(s), e(t) \neq 0$. Nuovamente, definiamo x, y in maniera da ottenere un assurdo. Per farlo è sufficiente richiedere che $x(s) = e(s)(1 + |e(t)|), x(t) = e(t)(1 - |e(s)|)$ e allo stesso modo coi più e meno scambiati per y, mentre per tutti gli altri valori imponiamo $x = y = e$. Si verifica facilmente che questo contraddice l'assunto di estremalità di e. □

Osserviamo infine il seguente risultato, di cui omettiamo la dimostrazione:

Teorema 13. *$ZF + (UL)$ implica il teorema di Hahn Banach.*

D'altro canto, Hahn Banach con l'ipotesi aggiuntiva di separabilità dello spazio di Banach si può dimostrare in ZF:

Teorema 14. *Sia X uno spazio di Banach separabile, Y un suo sottospazio e f un funzionale lineare su Y tale che $f(x) \leq c\|x\|_X$ per un qualche $c < +\infty$. Esiste un funzionale lineare g su X tale che $\|g\| \leq c$ e $g_Y = f$.*

Dimostrazione. Senza perdita di generalità, supponiamo $c = 1$. Sia $\{e_n\}$ un sottoinsieme numerabile di X. Per induzione, definiamo $Y_n = \text{span}(Y_{n-1} \cup \{x_n\})$. Vogliamo dimostrare che è possibile estendere canonicamente f a Y_n, per induzione. È sufficiente dunque dimostre che esiste una estensione canonica di f da Y_n a Y_{n+1}. Per farlo, siano $x, y \in Y_n$. Per linearità abbiamo che

$$-\| - e_n - x\| - f(x) \leq \|e_n + y\| + f(y)$$

Di conseguenza definendo a_n come il sup del termine sinistro rispetto a $x \in Y_n$ e b_n come l'inf del termine destro rispetto a $y \in Y_n$ abbiamo $a_n \leq b_n$. Estendiamo f ponendo $f(e_n) = a_n$. Affermiamo che tale estensione soddisfa $f \leq \|\cdot\|$: per dimostrarlo, sia $r > 0$. Allora, poiché $ra_n \leq p(y + re_n) - f(y)$, abbiamo che $f(y + re_n) \leq p(y + re_n)$. La stessa conclusione si ottiene facilmente con $r < 0$. Otteniamo quindi per induzione l'estensione di f a $\cup Y_n$, un sottospazio denso di X. Estendendo f per continuità a X il risultato è dimostrato (è lasciato al lettore il facile compito di costruire una estensione di f senza utilizzare forme di assiomi di scelta) □

Osservazione 15. In un certo senso quindi, per fare analisi funzionale, è necessario AC. Tuttavia, per risultati più elementari questo non è necessario: per dimostrare il teorema della mappa aperta, del grafo chiuso e il teorema di Banach-Steinhaus è sufficiente $ZF + (CC)$ (vedasi [8]). Vediamo inoltre, qui come nella sezione dedicata alla topologia, che l'utilizzo di forme di scelta può essere evitato nel momento in cui si abbiano ipotesi più stringenti sulla struttura dell'oggetto in questione.

Osservazione 16. Vediamo ora che in un mondo in cui $\mathcal{L}(\mathbb{R}) = \mathcal{P}(\mathbb{R})$ si ha che sia il teorema di Hahn-Banach che quello di Banach-Alaoglu falliscono. Analisi funzionale si rivela quindi sostanzialmente impossibile, almeno per spazi generali, nel framework della *dream mathematics*. Tuttavia, in tale sistema assiomatico valgono ancora (in quanto deducibili da $ZF + (BT)$) i principi basilari, ovvero Banach-Steinhaus, grafo chiuso e mappa aperta.

5. CONCLUSIONE

Si potrebbe dire molto di più sulle implicazioni che ha l'assioma della scelta, anche volendo continuare a restringerci all'ambito topologico e dell'analisi funzionale. In particolare citiamo i seguenti risultati:

(1) È consistente con $ZF + (CC)$ che il lemma di Urysohn sia falso ([4]) ma esso segue da $ZF + (DC)$
(2) Il teorema di metrizzazione di Nagata-Smirnov-Bing è equivalente (su ZF) al teorema di Stone sulla paracompattezza dei metrici, che non è un teorema in ZF ([5])
(3) È consistente con ZF che esistano varietà lisce[4] paracompatte non metrizzabili
(4) L'ipotesi del continuo generalizzata ($2^{\aleph_\alpha} = \aleph_{\alpha+1}$) implica l'assioma della scelta
(5) È consistente con ZF che $(\ell^\infty)^* = \ell^1$
(6) È consistente con ZF che vi siano spazi metrici non compatti ma sequenzialmente compatti

Per chi fosse interessato a proseguire nello scoprire gli orrori della matematica senza scelta, la letteratura per proseguire è estremamente vasta. Suggeriamo in particolare [2] e l'enciclopedico [3].

BIBLIOGRAFIA

1. T. J. Jech *The axiom of choice* Dover publications
2. C. Good, I. J. Tree *Continuing horrors of topology without choice*. Topology Appl, 63(1):79-90.
3. P. Howard, J. E. Rubin *Consequences of the axiom of choice* Math. Surv., 59.
4. E. Tachtis *The Urysohn Lemma is independent of ZF + Countable Choice* Proc. Amer. Math. Soc. 147 (2019): 4029-4038.

[4] qui non supposte secondo-numerabili

5. P. Howard, K. Keremedis, J. E. Rubin, A. Stanley *Paracompactness of Metric Spaces and the Axiom of Multiple Choice* MLQ 46: 219-232.
6. R. Solovay *A model of set-theory in which every set of reals is Lebesgue measurable* Ann. Math. 92 (1): 1-56.
7. J. Pawlikowski *The Hahn-Banach Theorem implies the Banach-Tarski Paradox* Fund. Math. 138 (1): 21-22
8. A.F.D. Fellhauer *On the relation of three theorems of analysis to the axiom of choice* J. Log. Anal 9 (2017) : 1-23

L'ASSIOMA DELLA SCELTA... NELLE CATEGORIE

MATTEO DE BERARDINIS

1. L'ASSIOMA DELLA SCELTA

Dal primo anno di matematica, sappiamo che l'assioma della scelta (AC) è indipendente dagli altri assiomi della teoria degli insiemi di Zermelo-Frænkel (ZF). Per dimostrare ciò, è necessario fornire un modello di (ZF) in cui vale (AC) e un modello di (ZF) in cui vale ($\neg$AC). Il nostro obiettivo è di utilizzare la teoria dei topoi per fornire un modello di (ZF)+($\neg$AC).

2. RICHIAMI SUI TOPOI

2.1. Topoi elementari.

Ricordiamo la definizione di topos elementare:

Definizione 1. Sia $\mathcal{C}$ categoria con prodotti finiti; c'è un endofuntore

$$X \times - : \mathcal{C} \to \mathcal{C}$$

per ogni $X \in \mathcal{C}$.
Se, per ogni $X \in \mathcal{C}$, il funtore $X \times -$ ha aggiunto destro

$$(-)^X : \mathcal{C} \to \mathcal{C}$$

(ovvero c'è un isomorfismo $\mathrm{Hom}_{\mathcal{C}}(Y \times X, Z) \cong \mathrm{Hom}_{\mathcal{C}}(Y, Z^X)$ naturale), la categoria $\mathcal{C}$ si dice *cartesiana chiusa*.

Osservazione.

- Nel caso di $\mathcal{C} = \mathbf{Set}$, $Z^X := \{\text{funzioni } f : X \to Z\}$ è aggiunto destro di $X \times -$
- In generale, Z^X è una sorta di *hom-set* ($\mathrm{Hom}_{\mathcal{C}}(X, Z)$) *interno* alla categoria $\mathcal{C}$

Ricorda.

- $m : U \rightarrowtail X$ è *monomorfismo* (*mono*) se

$$m \circ f = m \circ g \implies f = g$$

- $e : Y \twoheadrightarrow X$ è *epimorfismo* (*epi*) se

$$f \circ e = g \circ e \implies f = g$$

Definizione 2. Un *classificatore di sottoggetti* per $\mathcal{C}$ (categoria con limiti finiti) è un monomorfismo $\mathrm{true} : 1 \rightarrowtail \Omega$ (dove 1 è oggetto terminale di $\mathcal{C}$) tale che, per ogni

monomorfismo $U \rightarrowtail X$ in $\mathcal{C}$, esiste un unico morfismo (*morfismo caratteristico*) $\chi_U : X \to \Omega$ che renda il seguente diagramma un pullback

$$\begin{array}{ccc} U & \xrightarrow{\exists!} & 1 \\ \downarrow & \lrcorner & \downarrow{\scriptstyle \text{true}} \\ X & \xrightarrow[\chi_U]{} & \Omega \end{array}$$

Definizione 3. Un *topos elementare* $\mathcal{E}$ è una categoria che

- ha limiti finiti
- è cartesiana chiusa
- ha classificatore di sottoggetti

Esempio.

- **Set**, con
  - $X^Y := \mathrm{Hom}_{\mathbf{Set}}(Y, X)$
  - true : $\{*\} \rightarrowtail \{0, 1\}$ che seleziona 1
- $\mathbf{Set}^{\mathbf{A}^{op}}$, con
  - $X^Y(a) := \mathrm{Hom}_{\mathbf{Set}^{\mathbf{A}^{op}}}(\mathrm{Hom}_{\mathbf{A}}(-, a) \times Y, X)$
  - $\mathrm{true}_a : 1(a) = \{*\} \rightarrowtail \Omega(a) = \{\text{crivelli su } a\}$ che seleziona il crivello massimale

2.2. Alcune proprietà. In un topos elementare $\mathcal{E}$ posso considerare, per ogni oggetto X, l'insieme *sottoggetti di X*

$$\mathrm{Sub}_{\mathcal{E}}(X) := \{U \rightarrowtail X \text{ mono}\} / \sim$$

con $(m : U \rightarrowtail X) \sim (m' : U' \rightarrowtail X)$ sse esiste $\varphi : U \to U'$ iso t.c. il seguente diagramma

$$\begin{array}{ccc} U & \xrightarrow{\varphi} & U' \\ & {\scriptstyle m}\searrow \quad \swarrow{\scriptstyle m'} & \\ & X & \end{array}$$

sia commutativo ($\sim$ è relazione di equivalenza).

Tale costruzione è funtoriale: al morfismo $Y \xrightarrow{f} X$ in $\mathcal{E}$ associo la funzione di insiemi $\mathrm{Sub}_{\mathcal{E}}(X) \xrightarrow{f^{-1}} \mathrm{Sub}_{\mathcal{E}}(Y)$ che, alla classe $[(m : U \rightarrowtail X)] \in \mathrm{Sub}_{\mathcal{E}}(X)$, associa la classe di $(f^{-1}(U) \rightarrowtail Y)$ in $\mathrm{Sub}_{\mathcal{E}}(Y)$, costruito tramite il seguente pullback

$$\begin{array}{ccc} f^{-1}(U) & \longrightarrow & U \\ \downarrow & \lrcorner & \downarrow{\scriptstyle m} \\ Y & \xrightarrow[f]{} & X \end{array}$$

Osservazione. Grazie alla proprietà del classificatore di sottoggetti, c'è un isomorfismo naturale tra i funtori $\mathrm{Sub}_{\mathcal{E}}(X)$ e $\mathrm{Hom}_{\mathcal{E}}(X, \Omega)$.

Osservazione. Queste prime costruzioni generalizzano costruzioni tipiche della categoria degli insiemi:

- I sottoggetti di un oggetto $X \in \mathcal{E}$ generalizzano la nozione di sottoinsiemi di un insieme nella categoria **Set**.
- Il classificatore di sottoggetti Ω generalizza l'insieme $\{0, 1\}$ nella categoria **Set**; i morfismi caratteristici corrispondono alle funzioni caratteristiche.
- L'isomorfismo naturale $\mathrm{Sub}_{\mathcal{E}}(X) \cong \mathrm{Hom}_{\mathcal{E}}(X, \Omega)$ corrisponde alla bieezione tra sottoinsiemi di un insieme e funzioni caratteristiche.

Fatto. Si possono dimostrare le seguenti proprietà:

- Un topos $\mathcal{E}$ ha tutti i colimiti finiti; in particolare, ha oggetto iniziale 0. Inoltre, ogni morfismo $X \to 0$ è un iso e ogni morfismo $0 \to Y$ è un mono.
- Ogni morfismo $f : Y \to X$ in $\mathcal{E}$ ammette una fattorizzazione, unica a meno di isomorfismo, $f = m \circ e$, con $e : Y \twoheadrightarrow f(Y)$ epi e $m : f(Y) \rightarrowtail X$ mono. $f(Y) \rightarrowtail X$ è un sottoggetto di X ed è detto *immagine* di f.

Un'altra proprietà fondamentale di un topos $\mathcal{E}$ è che, per ogni oggetto $X \in \mathcal{E}$, $\mathrm{Sub}_{\mathcal{E}}(X)$ è un'*algebra di Heyting*. Infatti, dati U, V sottoggetti di X (cioè $U \rightarrowtail X$, $V \rightarrowtail X$ in $\mathrm{Sub}_{\mathcal{E}}(X)$),

- $V \leq U$ sse $V \rightarrowtail X$ fattorizza attraverso $U \rightarrowtail X$
- 0 (*bottom*) è dato da $0 \rightarrowtail X$
- 1 (*top*) è dato da $X \xrightarrow{\mathrm{id}_X} X$
- $V \wedge U$ (*meet*) è dato dal pullback

$$\begin{array}{ccc} V \wedge U & \rightarrowtail & U \\ \downarrow & \lrcorner & \downarrow \\ V & \rightarrowtail & X \end{array}$$

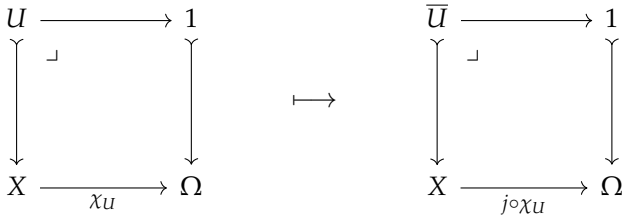
- $V \vee U$ (*join*) è dato dall'immagine $V + U \twoheadrightarrow V \vee U \rightarrowtail X$
- $V \Rightarrow U$ (*implication*) è dato da $U^V \rightarrowtail X$ (si può dimostrare che U^V è sottoggetto)

Osservazione. In ogni algebra di Heyting, si può definire $\neg x := x \Rightarrow 0$ (*negation*). Con questa definizione, vale $\neg 0 = 1$, $\neg 1 = 0$, ma, in generale, non vale $\neg\neg x = x$; un'algebra di Heyting è un'algebra di Boole sse $\neg\neg x = x$ per ogni elemento x.

2.3. Topologia su un topos elementare. Sia $\mathcal{E}$ un topos e $\mathrm{true} : 1 \rightarrowtail \Omega$ il suo classificatore di sottoggetti.

Dare un morfismo $j : \Omega \to \Omega$, equivale a dare, per ogni $X \in \mathcal{E}$, un operatore $\mathrm{Sub}_{\mathcal{E}}(X) \to \mathrm{Sub}_{\mathcal{E}}(X)$, naturale in X: al sottoggetto U (con funzione caratteristica

χ_U), associo il sottoggetto $\overline{U}$ (con funzione caratteristica $\chi_{\overline{U}} := j \circ \chi_U$)



Definizione 4. Un morfismo $j : \Omega \to \Omega$ si dice *topologia* (*Lawvere-Tierney topology*) su $\mathcal{E}$ se l'operatore ad esso associato soddisfa le seguenti condizioni:

- $U \leq \overline{U}$
- $\overline{\overline{U}} = \overline{U}$
- $\overline{V \wedge U} = \overline{V} \wedge \overline{U}$

Definizione 5. Un sottoggetto U di X si dice *denso* se $\overline{U} = X$; si dice invece *chiuso* se $\overline{U} = U$.

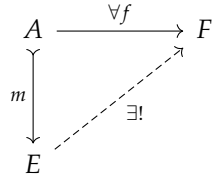
Fatto. $\neg\neg : \mathrm{Sub}_{\mathcal{E}}(X) \to \mathrm{Sub}_{\mathcal{E}}(X)$, con $U \mapsto \overline{U} := \neg\neg U$, è naturale in X e soddisfa le tre proprietà della definizione di topologia (*double negation topology*).

2.4. Fasci per una topologia. Sia ora $\mathcal{E}$ un topos con una topologia fissata $j : \Omega \to \Omega$.

Definizione 6. $F \in \mathcal{E}$ si dice fascio per la topologia j se ogni monomorfismo denso $m : A \rightarrowtail E$ (cioè $\overline{A} = E$) induce una biiezione

$$m^* : \mathrm{Hom}_{\mathcal{E}}(E, F) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{E}}(A, F)$$

ovvero ogni $f : A \to F$ si estende in modo unico a E



Lemma 7 (Fascificazione)**.** *Sia $Sh_j\mathcal{E} \hookrightarrow \mathcal{E}$ la sottocategoria piena dei fasci per una topologia fissata j su un topos $\mathcal{E}$.*

Allora $Sh_j\mathcal{E}$ è a sua volta un topos elementare e il funtore di inclusione ha un aggiunto sinistro $a : \mathcal{E} \to Sh_j\mathcal{E}$ che è esatto a sinistra (cioè preserva i limiti finiti).

Osservazione. Nel caso in cui $\mathcal{E} = \mathbf{Set}^{\mathbf{A}^{op}}$ categoria di prefasci, dare una topologia come nella **Definizione 4** corrisponde a dare una *topologia di Grothendieck* su $\mathbf{A}$ (attraverso la nozione di ricoprimento aperto); la nozione di fascio risulterà essere la medesima, così come l'operazione di fascificazione.

3. COSTRUZIONI DALLA TEORIA DEGLI INSIEMI

3.1. Assioma dell'infinito: natural number object. Questa costruzione generalizza l'insieme dei numeri naturali.

Definizione 8. Un *natural number object* (*n.n.o.*) per un topos $\mathcal{E}$ è un oggetto $\mathbf{N}$ con delle frecce

$$1 \xrightarrow{0} \mathbf{N} \xrightarrow{s} \mathbf{N}$$

tali che, per ogni diagramma

$$1 \xrightarrow{x} X \xrightarrow{f} X$$

esiste un'unica $h : \mathbf{N} \to X$ che faccia commutare il seguente diagramma

$$\begin{array}{ccccc} 1 & \xrightarrow{0} & \mathbf{N} & \xrightarrow{s} & \mathbf{N} \\ \| & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h} \\ 1 & \xrightarrow[x]{} & X & \xrightarrow[f]{} & X \end{array}$$

Fatto. Ogni topos di Grothendieck $\mathcal{G}$ (cioè una categoria di fasci per una topologia di Grothendieck) ha n.n.o, dato da $\mathbf{N} = a\Delta(\mathbb{N})$ (dove $\Delta(\mathbb{N})$ è il prefascio costante sull'insieme dei numeri naturali $\mathbb{N} \in \mathbf{Set}$ e a è il funtore fascificazione). Inoltre, $\mathbf{N} = a\Delta(\mathbb{N}) \cong \coprod_{n\in\mathbb{N}} 1$ (coprodotto in $\mathcal{G}$ dell'oggetto terminale, indicizzato sull'insieme dei numeri naturali).

3.2. L'assioma della scelta... nelle categorie. Una delle versioni equivalenti dell'assioma della scelta, afferma che il prodotto $\prod_i X_i$ di una famiglia di insiemi non vuoti X_i è un insieme non vuoto.
Un'altra formulazione afferma che ogni funzione suriettiva $p : X \twoheadrightarrow I$ ammette una sezione $s : I \to X$ (ovvero t.c. $p \circ s = \mathrm{id}_I$).

Un topos $\mathcal{E}$ soddisfa l'assioma della scelta (AC) se ogni epi $p : X \twoheadrightarrow I$ ammette una sezione $s : I \to X$.
Equivalentemente se, dato $p : X \twoheadrightarrow I$ epi,

$$\mathrm{Hom}_{\mathcal{E}}(E, X) \xrightarrow{p_*} \mathrm{Hom}_{\mathcal{E}}(E, I)$$

è suriettiva per ogni $E \in \mathcal{E}$ (la preimmagine sarà data da $s \circ \varphi \overset{p_*}{\longmapsto} \varphi$ per ogni $\varphi \in \mathrm{Hom}_{\mathcal{E}}(E, I)$).

Per dare una nozione interna dell'assioma della scelta, sostituiamo gli *hom-set* $\mathrm{Hom}_{\mathcal{E}}(E, -)$ con le loro versioni interne $(-)^E$: un topos $\mathcal{E}$ soddisfa la versione interna dell'assioma della scelta (IAC) se, dato $p : X \twoheadrightarrow I$ epi, la mappa indotta

$$X^E \xrightarrow{p^E} I^E$$

è un epi per ogni oggetto $E \in \mathcal{E}$.
Equivalentemente se, per ogni $E \in \mathcal{E}$, il funtore

$$(-)^E : \mathcal{E} \to \mathcal{E}$$

preserva gli epi.

Osservazione. (IAC) è più debole di (AC): se un epi $p : X \twoheadrightarrow I$ in $\mathcal{E}$ ammette una sezione $s : I \to X$, allora, per ogni $E \in \mathcal{E}$, la mappa $p^E : X^E \to I^E$ ha come sezione $s^E : I^E \to X^E$, dunque p^E risulta essere un epi.

4. UN TOPOS IN CUI FALLISCE (IAC)

Teorema. *Esiste un two-valued Boolean Grothendieck topos $\mathcal{F}$, con n.n.o.* $\mathbf{N}$*, con una sequenza di oggetti $F_0, F_1, F_2, \dots$ tali che*

(i) per ogni n, l'unica mappa $F_n \to 1$ è un epi,
(ii) il prodotto $\prod_m F_m$ esiste ed è l'oggetto iniziale 0,
(iii) ogni F_n è sottoggetto di $P(\mathbf{N}) := \Omega^{\mathbf{N}}$, con Ω classificatore di sottoggetti.

Alcune precisazioni.

- $\mathcal{F}$ è un topos di Grothendieck, cioè la categoria dei fasci (contenuta in $\mathbf{Set}^{\mathbf{A}^{op}}$) per una topologia di Grothendieck su $\mathbf{A}$. Abbiamo già osservato che dare una topologia di Grothendieck su $\mathbf{A}$, equivale a dare una topologia (Lawvere-Tierney topology) sul topos $\mathbf{Set}^{\mathbf{A}^{op}}$. Abbiamo inoltre osservato che $\mathcal{F}$ ammette n.n.o., dato da $\mathbf{N} = a\Delta(\mathbb{N}) \cong \coprod_{m\in\mathbb{N}} 1$.
- Un topos $\mathcal{E}$ si dice *two-valued* se gli unici sottoggetti dell'oggetto terminale 1 sono $0 \rightarrowtail 1$ e $1 \xrightarrow{\mathrm{id}_1} 1$.
- Un *Boolean topos* $\mathcal{E}$ è un topos in cui $\mathrm{Sub}_{\mathcal{E}}(X)$ è un'algebra di Boole per ogni $X \in \mathcal{E}$ (ricordiamo che sull'algebra di Heyting $\mathrm{Sub}_{\mathcal{E}}(X)$ possiamo definire una negazione $\neg U := U \Rightarrow 0$ e che $\mathrm{Sub}_{\mathcal{E}}(X)$ risulta essere un'alebra di Boole sse $\neg\neg U = U$ per ogni U in $\mathrm{Sub}_{\mathcal{E}}(X)$).
- Il punto (iii), che non dimostreremo, risulta importante affinchè gli oggetti F_n siano "piccoli" e vivano all'interno della "gerarchia cumulativa", da costruirsi in $\mathcal{F}$, in modo che $\mathcal{F}$ risulti essere un modello della teoria degli insiemi di Zermelo-Frænkel.

Prima di costruire $\mathcal{F}$ come nel teorema, verifichiamo che (IAC) fallisce in $\mathcal{F}$:

Consideriamo le mappe $F_m \twoheadrightarrow 1$ (sono epi per il punto (i)) e la mappa indotta dalla proprietà universale del coprodotto

$$p : \coprod_{m\in\mathbb{N}} F_m \twoheadrightarrow \coprod_{m\in\mathbb{N}} 1 \cong \mathbf{N}$$

Si osserva facilmente che p è epi.

Costruiamo il pullback P

$$\begin{array}{ccc} P & \xrightarrow{k} & (\coprod_m F_m)^{\mathbf{N}} \\ \downarrow & \lrcorner & \downarrow{\scriptstyle p^{\mathbf{N}}} \\ 1 & \xrightarrow[\widetilde{\mathrm{id}}]{} & \mathbf{N}^{\mathbf{N}} \end{array}$$

dove $\widetilde{\mathrm{id}}$ è la trasposta dell'identità $\mathbf{N} \to \mathbf{N}$ via l'aggiunzione $\mathbf{N} \times - \dashv (-)^{\mathbf{N}}$

Fissato $X \in \mathcal{F}$, la proprietà universale per P e l'aggiunzione $\mathbf{N} \times - \dashv (-)^{\mathbf{N}}$ ci dicono che, dare una mappa $f : X \to P$, corrisponde a dare una mappa

$$g : \mathbf{N} \times X \to \coprod_{m \in \mathbb{N}} F_m$$

tale che $p \circ g = \pi_1 : \mathbf{N} \times X \to \mathbf{N}$ (proiezione sulla prima componente).
Ma

$$\mathbf{N} \times X \cong (\coprod_{m \in \mathbb{N}} 1) \times X \cong \coprod_{m \in \mathbb{N}} (1 \times X) \cong \coprod_{m \in \mathbb{N}} X$$

dunque g è data da una famiglia di mappe $g_m : X \to \coprod_{m \in \mathbb{N}} F_m$ tali che g_m fattorizza attraverso $F_m \to \coprod_{m \in \mathbb{N}} F_m$ (questa condizione corrisponde all'identità $p \circ g = \pi_1$), cioè è data da una famiglia di mappe $g'_m : X \to F_m$. Questo significa che $f : X \to P$ corrisponde ad una mappa $g' : X \to \prod_{m \in \mathbb{N}} F_m$.
Ricapitolando, abbiamo un isomorfismo (naturale in X)

$$\mathrm{Hom}_{\mathcal{F}}(X, P) \cong \mathrm{Hom}_{\mathcal{F}}(X, \prod_{m \in \mathbb{N}} F_m)$$

Per Yoneda, vale $P \cong \prod_{m \in \mathbb{N}} F_m$, quindi, per il punto (ii), $P = 0$.
Abbiamo dunque trovato un epi, $p : \coprod_{m \in \mathbb{N}} F_m \twoheadrightarrow \coprod_{m \in \mathbb{N}} 1 \cong \mathbf{N}$ tale per cui $p^{\mathbf{N}} : (\coprod_m F_m)^{\mathbf{N}} \to \mathbf{N}^{\mathbf{N}}$ non è epi: se lo fosse, infatti, anche il suo pullback lungo $\widetilde{\mathrm{id}}$

$$\begin{array}{ccc} 0 & \xrightarrow{k} & (\coprod_m F_m)^{\mathbf{N}} \\ \downarrow & \lrcorner & \downarrow{\scriptstyle p^{\mathbf{N}}} \\ 1 & \xrightarrow[\widetilde{\mathrm{id}}]{} & \mathbf{N}^{\mathbf{N}} \end{array}$$

dovrebbe esserlo, ma $0 \to 1$ non lo è.

4.1. Costruzione di $\mathcal{F}$. Sia $\mathbf{A}$ la categoria con

- oggetti: gli insiemi finiti $n = \{0, 1, \ldots, n\}$,
- frecce: $f : n \to m$ funzioni da $\{0, 1, \ldots, n\}$ a $\{0, 1, \ldots, m\}$, con $n \geq m$ e $f(i) = i$ per ogni $i \leq m$.

Definiamo $\mathcal{F} := Sh_{\neg\neg}(\mathbf{A})$, ovvero i fasci per la topologia $\neg\neg$ (double negation topology) su $\mathbf{Set}^{\mathbf{A}^{op}}$.

La categoria $\mathbf{A}$ soddisfa le seguenti proprietà (ci torneranno utili in seguito):

1) $\mathrm{Hom}_{\mathbf{A}}(m, n) \neq \emptyset$ se e solo se $m \geq n$;
2) se c'è un quadrato commutativo

$$\begin{array}{ccc} p & \longrightarrow & m \\ \downarrow & & \downarrow{\scriptstyle g} \\ m & \xrightarrow[f]{} & n \end{array}$$

allora $f = g$.

Fatto. $\mathcal{F}$ è Boolean (ovvero $\mathrm{Sub}_{\mathcal{F}}(X)$ è un'algebra di Boole per ogni $X \in \mathcal{F}$), perchè è la categoria dei fasci per la topologia $\neg\neg$ su $\mathbf{Set}^{\mathbf{A}^{op}}$.

Per mostrare che è two-valued (ovvero che $|\mathrm{Sub}_{\mathcal{F}}(1)| = 2$), consideriamo i sottoggetti di 1 nel topos $\mathbf{Set}^{\mathbf{A}^{op}}$ (contenente $\mathcal{F}$ come sottocategoria piena); essi sono prefasci

$$X : \mathbf{A}^{op} \longrightarrow \mathbf{Set}$$

il cui valore $X(n)$ sul generico oggetto n in $\mathbf{A}$ è l'insieme vuoto $\emptyset$, oppure il singoletto 1.

Per la proprietà 1), se un tale funtore X è non vuoto in un certo n, allora deve necessariamente essere non vuoto in ogni $m \geq n$ (poichè, per funtorialità, la freccia $m \to n$ induce una funzione $X(n) \to X(m)$).

Dunque, i sottoggetti di 1 in $\mathbf{Set}^{\mathbf{A}^{op}}$ sono tutti e soli i funtori della forma

- $\emptyset$ (il prefascio vuoto)
- $U_n(m) = \begin{cases} \emptyset & \text{se } m < n \\ 1 & \text{se } m \geq n \end{cases}$

Osservazione. $U_0 = 1$ funtore costante sul singoletto.

Fatto. In un'algebra di Heyting si ha $\neg\neg x = 1$ se e solo se $x \wedge y \neq 0$ per ogni $y \neq 0$.

Ora, siccome

$$U_n \cap U_m \supseteq U_{n+m} \neq \emptyset$$

si ha, per il fatto precedente, che $\neg\neg U_n = 1$ per ogni n. Questo significa che ogni U_n è sottoggetto denso di 1 per la topologia $\neg\neg$ su $\mathbf{Set}^{\mathbf{A}^{op}}$.

Inoltre, dato che 1 è un fascio, (si può mostrare che) i suoi sottoggetti che sono fasci sono tutti e soli i suoi sottoggetti chiusi.

Dunque, gli unici sottoggetti di 1 in $\mathcal{F} = Sh_{\neg\neg}(\mathbf{A})$ sono $\emptyset$ (in quanto $\neg\neg\emptyset = \emptyset$) e 1, cioè $\mathcal{F}$ è two-valued.

Osservazione. Il prefascio vuoto $\emptyset$ (oggetto iniziale di $\mathbf{Set}^{\mathbf{A}^{op}}$), risulta essere un fascio per la topologia $\neg\neg$ (dunque è oggetto iniziale anche in $\mathcal{F}$).

4.2. Costruzione degli F_n. Consideriamo ora i funtori rappresentabili

$$H_n := \mathrm{Hom}_{\mathbf{A}}(-, n) \in \mathbf{Set}^{\mathbf{A}^{op}}$$

Sia

$$F_n := a(H_n) \in \mathcal{F}$$

la loro fascificazione.

4.3. Dimostrazione di (i). Vogliamo mostrare che $F_n \to 1$ è epi.

Abbiamo $F_n \neq 0$, in quanto ho un (mono)morfismo (denso) $H_n \rightarrowtail F_n$ (morfismo di fascificazione) e $H_n \neq \emptyset$ (per l'Osservazione precedente, l'oggetto iniziale di $\mathcal{F}$ coincide con il prefascio vuoto).

Per lo stesso motivo, se considero la fattorizzazione epi-mono in $\mathcal{F}$ dell'unico morfismo $F_n \to 1$,

$$F_n \twoheadrightarrow V_n \rightarrowtail 1$$

l'immagine V_n non può essere 0 (essendo, per quanto detto prima, $F_n \neq 0$).

Dato che $\mathcal{F}$ è two-valued e V_n è un sottoggetto di 1, necessariamente $V_n = 1$, dunque $F_n \to 1$ è un epi.

4.4. Dimostrazione di (ii). Mostriamo che $X := \prod_m F_m$ è 0.

Se non lo fosse, esisterebbe un certo n per cui $X(n) \neq \emptyset$. L'esistenza delle proiezioni $X = \prod_m F_m \to F_m$, implica dunque che $F_m(n) \neq \emptyset$ per ogni m.

Mostriamo, al contrario, che, per ogni n, $F_{n+1}(n) = \emptyset$.

Se, per assurdo, $F_{n+1}(n) \neq \emptyset$, per il lemma di Yoneda, esisterebbe una trasformazione naturale $u : H_n \to F_{n+1}$.

Consideriamo ora il monomorfismo denso di fascificazione $H_{n+1} \rightarrowtail F_{n+1}$ e prendiamone il pullback lungo u

$$\begin{array}{ccc} Q & \xrightarrow{u'} & \mathrm{Hom}(-, n+1) \\ \downarrow & \lrcorner & \downarrow \\ \mathrm{Hom}(-, n) & \xrightarrow[u]{} & F_{n+1} \end{array}$$

ottenendo un sottoggetto denso Q di $\mathrm{Hom}(-, n)$ (questo implica che $Q \neq \emptyset$, in quanto $\emptyset$ non è sottoggetto denso di H_n).

Siccome $Q \neq \emptyset$, esiste un certo m e una $g \in Q(m) \subseteq \mathrm{Hom}(m, n)$.

Consideriamo l'immagine $h := u'(g) \in \mathrm{Hom}(m, n+1)$ (dunque deve valere $m \geq n+1$).

Consideriamo le mappe in **A**

$$f, f' : m+1 \to m$$

definite da $f(m+1) = n+1$ e $f'(m+1) = g(n+1) \leq n$ (sugli altri valori non ho scelta, per come è stata costruita la categoria **A**).

Si verifica facilmente che $g \circ f = g \circ f'$. Quindi, per quanto appena detto e per la naturalità di u',

$$h \circ f = u'(g) \circ f = u'(g \circ f) = u'(g \circ f') = u'(g) \circ f' = h \circ f'$$

Ma $h(f(m+1)) = h(n+1) = n+1$, mentre $h(f'(m+1)) = h(g(n+1)) = g(n+1) \leq n$ (assurdo).

Fuori Orario è una giornata di seminari *per studenti da studenti*, giunta quest'anno alla sua quinta edizione, organizzata dagli studenti 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. Quest'anno l'evento si è svolto online, vista l'impossibilità di svolgerlo in completa sicurezza: passione e condivisione hanno riunito–nonostante la distanza–la nostra comunità.

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