Università di Torino

L'Assioma di Scelta

Andrea Gadotti

29 dicembre 2014

Indice

Introduzione **i**

Nozioni di base **1**
0.1 Logica del prim'ordine . . . 1
0.1.1 Connettivi . . . 1
0.1.2 Linguaggi . . . 2
0.1.3 Formule . . . 3
0.1.4 Strutture . . . 3
0.1.5 Teorie e modelli . . . 5
0.1.6 La Teoria degli Insiemi di Zermelo-Fraenkel . . . 6
0.2 Cardinalità e ordinali . . . 9

1 Assioma di Scelta e pratica matematica **11**
1.0.1 Formulazioni alternative . . . 12
1.1 Principali equivalenti . . . 13
1.2 C'è, ma non si vede . . . 15
1.3 C'è, ma non serve . . . 17

2 Disastri senza Scelta **19**
2.1 Finitezza . . . 19
2.2 Aritmetica cardinale . . . 25
2.3 Ordini . . . 28
2.4 Spazi vettoriali . . . 29
2.5 Spazi compatti . . . 31

3 Disastri con Scelta **33**
3.1 Decomposizioni paradossali . . . 33
3.1.1 Decomposizione paradossale della Sfera unitaria . . . 34
3.1.2 Gruppi indisciplinati . . . 36
3.1.3 Decomposizione paradossale della Palla unitaria . . . 39
3.1.4 Il paradosso di Banach-Tarski . . . 40

3.1.5 Di chi è la colpa 42

4 Assioma delle Scelte Dipendenti **43**
4.0.6 Il paradosso di Skolem 47

5 Cappelli e prigionieri **49**

Bibliografia **54**

Introduzione

L'Assioma di Scelta (brevemente AC) viene utilizzato per la prima volta, in modo implicito e del tutto inconsapevole, nella teoria dei numeri cardinali creata da Cantor. Infatti, nel tentativo di determinare la cardinalità del continuo, Cantor suppone che l'insieme dei numeri reali possa venire bene ordinato. La prima vera allusione si trova invece in uno scritto di equazioni differenziali ordinarie del 1890 ad opera di Giuseppe Peano il quale, consapevole di non poter applicare infinite volte una regola arbitraria che ad ogni classe associa un suo elemento, considera l'idea di affermare una regola precisa che permetta ciò[1]. Nel 1904 Zermelo[2] formula proprio questo principio, che prende il nome di Assioma di Scelta, e dimostra grazie ad esso che ogni insieme può essere bene ordinato e, in particolare, l'assunzione di Cantor. In altre parole Zermelo postula l'esistenza di una cosiddetta "funzione di scelta" su ogni famiglia di insiemi non vuoti, ma non dà nessuna idea sul come costruirla e per questo solleva le critiche dei matematici costruttivisti, per i quali il procedimento con cui si dimostra l'esistenza di un oggetto matematico deve permettere di esibire esplicitamente un testimone. La disputa sull'accettare o meno l'Assioma di Scelta ha fine verso la metà del Novecento con la dimostrazione, ad opera di Cohen (1963), della sua indipendenza dagli altri assiomi della teoria di Zermelo-Fraenkel (brevemente: ZF).

Nel Capitolo 1 introduciamo l'Assioma di Scelta e ne presentiamo alcune formulazioni alternative molto diffuse in letteratura. Dimostriamo poi l'equivalenza con alcuni principi matematici estremamente importanti, come il Lemma di Zorn e il Principio del buon ordinamento. Infine presentiamo un esempio di utilizzo "nascosto" di AC e due esempi di utilizzo superfluo.

Nel Capitolo 2 cerchiamo di fare matematica senza AC. Sarà da subito chiaro al lettore che questa scelta è davvero scomoda, dato che ci si trova di fronte a veri e propri *disastri*. Noi ne trattiamo alcuni riguardanti insiemi finiti, aritmetica cardinale, ordini, spazi vettoriali, spazi compatti.

Nel Capitolo 3 presentiamo un risultato affascinante e molto conosciuto: il Paradosso di Banach-Tarski, che essenzialmente afferma la possibilità di usare AC per

[1] [2]
[2] [3]

"duplicare" una palla in $\mathbb{R}^3$. Non entreremo nei dettagli tecnici del teorema; offriremo piuttosto una panoramica generale dell'idea che sta alla base del risultato, passando anche dal Paradosso di Hausdorff.

Nel Capitolo 4 introduciamo un assioma strettamente più debole di AC: l'Assioma delle Scelte Dipendenti. Mostriamo poi un risultato non molto conosciuto: il Teorema di Löwenheim-Skolem all'ingiù è equivalente all'Assioma delle Scelte Dipendenti. Accenniamo poi al Paradosso di Skolem.

Nel Capitolo 5 proponiamo un divertente puzzle che mostra un'altra conseguenza controintuitiva di AC relativamente alla Teoria della Probabilità.

Nozioni di base

Elenchiamo di seguito (senza dimostrazione) alcuni concetti che utilizzeremo nel corso del nostro lavoro. Purtroppo i prerequisiti necessari per una comprensione completa sarebbero troppi per includerli tutti. Per questo, l'elaborato è rivolto principalmente a coloro che conoscono già i concetti di base della Logica Matematica. Nonostante questo, crediamo che, dopo aver letto questa sezione, una grande parte dell'elaborato risulterà comprensibile a qualunque matematico.

0.1 Logica del prim'ordine

Vogliamo presentare alcuni concetti di base della logica del prim'ordine. Abbiamo scelto di includere questa rapida rassegna al fine di rendere più comprensibile la lettura di questo elaborato anche agli studenti di matematica che non hanno mai studiato la logica del prim'ordine. Da un punto di vista formale, lo sviluppo dei concetti basilari della logica del prim'ordine non è sempre immediato e richiede un po' di tempo. Fortunatamente però, le idee intuitive che ne stanno alla base sono quasi sempre piuttosto chiare. Per questo, considerato anche lo scopo puramente pragmatico di questa sezione, non saremo molto formali né precisi, e punteremo piuttosto a rendere i concetti quanto più chiari e accessibili possibile.

0.1.1 Connettivi

Sono ben noti a qualsiasi matematico i *connettivi logici*

$$\neg \quad \vee \quad \wedge \quad \Rightarrow \quad \Leftrightarrow$$

e i *quantificatori*

$$\exists \quad \forall$$

I connettivi e i quantificatori si dicono *costanti logiche*. L'espressione "$\exists x A$" significa "c'è un x tale che vale A", mentre "$\forall x A$" significa "per ogni x vale A". Quindi ad esempio

$$\exists x \neg A \Rightarrow \neg(\forall x A)$$

significa "se esiste un x tale che A non vale, allora non è vero che A vale per qualsiasi x".

0.1.2 Linguaggi

Un *linguaggio* L del prim'ordine consiste dei seguenti oggetti:

- la parentesi aperta (e la parentesi chiusa)
- i simboli $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow, \exists, \forall, =$;
- una lista infinita di simboli dette *variabili*

  $$v_0, v_1, v_2, ...$$

  Le lettere $x, y, z, ...$ indicano una generica variabile v_n;
- dei *simboli di costante* $c, d, e, ...$;
- dei *simboli di funzione* $g, g, h, ...$;
- dei *simboli di predicato* (o *di relazione*) $P, Q, R, ...$

Ad ogni simbolo di funzione e di predicato è associato un numero naturale detto *arietà* del simbolo, che indica il numero di parametri ai quali il simbolo deve essere applicato. I simboli di arietà 1, 2, 3 si dicono rispettivamente unari, binari, ternari. Spesso l'arietà si evince dal contesto.

Un esempio di predicato unario è $T(x)$, il predicato che dice "x è un triangolo rettangolo". Un esempio ben noto di predicato binario è il simbolo $<$ di "minore". Quindi $<(x, y)$ significa che x è minore di y. Un esempio di funzione binaria è il simbolo $+$ di somma. Quindi $+(x, y)$ è l'operazione somma applicata a x e y. Finora abbiamo utilizzato la notazione *prefissa*. Spesso i simboli binari vengono utilizzati con notazione *infissa*; scriveremo quindi $x < y$ e $x + y$ anziché $<(x, y)$ e $+(x, y)$.

I simboli di costante, funzione e predicato si dicono simboli non logici e caratterizzano il linguaggio in questione. Per i nostri scopi possiamo supporre per semplicità che siano sempre in numero finito. Con abuso di notazione definiremo un certo linguaggio L come $L = \{f_1, ..., f_n, R_1, ..., R_m, c_1, ..., c_k\}$ con $n, m, k \geq 0$ e f_i, R_i, c_i simboli di funzione, predicato e costante rispettivamente. Quindi ad esempio scriveremo $L = \{+, \cdot, <, 0, 1\}$.

0.1.3 Formule

Dato un linguaggio L possiamo costruire le L-formule, ovvero particolari espressioni scritte a partire dalle costanti logiche e dai simboli non logici di L. Facciamo qualche esempio:

- Sia $L_1 = \{\cdot, 0, 1\}$. Un esempio di L_1-formula è φ_1 data da

$$\forall x(x \neq 0 \Rightarrow \exists y(x \cdot y = 1)).$$

- Sia $L_2 = \{T, L, A\}$ con T, L, A predicati unari. Un esempio di L_2-formula è φ_2 data da

$$T(x) \Rightarrow (L(x) \Leftrightarrow A(x)).$$

  La formula φ_2 formalmente è solo una sequenza di simboli. Ma se immaginiamo $T(x)$ come la frase "x è un triangolo", $L(x)$ come "x è equilatero" e $A(x)$ come "x è equiangolo", allora possiamo vedere φ_2 come una *formalizzazione* della frase "se x è un triangolo, allora x è equilatero se e solo se è equiangolo".

- Sia $L_3 = \{<, \Pr\}$ con Pr predicato unario. Sia φ_3 la L_3-formula

$$\forall x \exists y(x < y \wedge \Pr(y)).$$

  Se immaginiamo $<$ come un ordine e $\Pr(x)$ come l'espressione "x è primo", allora φ_3 afferma che per ogni elemento esiste un elemento maggiore che è primo. Se interpretiamo questa formula nell'insieme $\mathbb{N}$ dei numeri naturali, otteniamo una formulazione del Teorema di Euclide sull'infinità dei numeri primi.

- Sia $L_4 = \{+, -, 0\}$. Un esempio di L_4-formula è φ_4 data da

$$\forall x(x + x = 0).$$

0.1.4 Strutture

Come abbiamo già accennato, le formule sono semplicemente stringhe di simboli. La loro utilità matematica risulta chiara quando esse vengono *interpretate* in qualche *struttura*.

Definizione 0.1.1. Sia $L = \{f_1, ..., f_n, R_1, ..., R_m, c_1, ..., c_k\}$ un linguaggio con $n, m, k \geq 0$ e f_i, R_i, c_i simboli di funzione, predicato e costante rispettivamente. Una L-struttura consiste di:

- un insieme non vuoto M detto *universo* della struttura;

- degli elementi privilegiati c_i^M di M per ogni $1 \leq i \leq k$;
- delle funzioni $f_i^M : M^{\mathrm{ar}(f_i)} \to M$ dove $\mathrm{ar}(f_i)$ è l'arietà associata a f_i nel linguaggio L in questione, per ogni $1 \leq i \leq n$;
- dei sottoinsiemi $R_i^M \subseteq M^{\mathrm{ar}(R_i)}$ dove $\mathrm{ar}(R_i)$ è l'arietà associata a R_i nel linguaggio L in questione, per ogni $1 \leq i \leq m$.

Nota. Ribadiamo che gli f_i, R_i, c_i sono solamente dei simboli (eventualmente con un'arietà associata). Diversamente, gli f_i^M, R_i^M, c_i^M sono rispettivamente funzioni, relazioni ed elementi di M.

Esempio 0.1.2. Consideriamo L_1, L_3 e L_4 come sopra.

- $(\mathbb{N}, \cdot^{\mathbb{N}}, 0^{\mathbb{N}}, 1^{\mathbb{N}}), (\mathbb{R}, \cdot^{\mathbb{R}}, 0^{\mathbb{R}}, 1^{\mathbb{R}}), (\mathcal{M}_3, \cdot^{\mathcal{M}_3}, 0^{\mathcal{M}_3}, 1^{\mathcal{M}_3})$, con $\mathcal{M}_3$ l'insieme delle matrici 3×3 su $\mathbb{R}$, sono tutte L_1-strutture se interpretiamo i vari $\cdot^M$ come il prodotto standard sull'universo in questione e le costanti $0^M, 1^M$ in modo ovvio. Per alleggerire la notazione, d'ora in poi ometteremo gli apici nelle funzioni, relazioni e costanti delle strutture.
- $(\mathbb{N}, <, \mathrm{Pr})$ è una L_3-struttura se interpretiamo $<$ come l'ordine standard su $\mathbb{N}$ e Pr come l'insieme dei numeri naturali primi;
- $(\mathbb{Z}, +, -, 0)$ e $(\mathbb{Z}/2\,\mathbb{Z}, +, -, 0)$ sono L_4 strutture, se interpretiamo le operazioni e lo 0 nel modo standard rispetto alla struttura considerata.

Definizione 0.1.3. Sia φ una formula di qualche linguaggio. Una variabile che compare in φ si dice *libera* se non è quantificata in φ, altrimenti si dice vincolata. Una formula in cui tutte le variabili sono vincolate si dice *formula chiusa* o *enunciato*. Se φ è una formula con $x_1, ..., x_n$ variabili libere, scriveremo spesso $\varphi(x_1, ..., x_n)$.

Esempio 0.1.4. φ_1 è una formula chiusa, come anche φ_3 e φ_4. Al contrario, φ_2 non è chiusa perché la variabile x non è vincolata. Quindi $\varphi_2 = \varphi_2(x)$.

Definizione 0.1.5. Sia L un linguaggio, M una L-struttura e σ un L-enunciato. Diciamo che M *soddisfa* σ, in simboli $M \models \sigma$, se σ vale in M (rispetto all'interpretazione dei simboli di L in M che abbiamo scelto).[3]

Esempio 0.1.6.

[3] La definizione è volutamente "confusa", dato che non abbiamo definito cosa significa che un enunciato "vale" in una struttura. In effetti una definizione rigorosa della nozione di "soddisfazione" richiede un po' di lavoro. Tuttavia riteniamo che il concetto intuitivo sia chiaro e chiediamo quindi al lettore di accontentarsi di questa "definizione", osservando anche gli esempi che seguono.

- $(\mathbb{R}, \cdot, 0, 1)$ soddisfa φ_1, dato che $\mathbb{R}$ è un campo. Al contrario, $(\mathbb{N}, \cdot, 0, 1) \not\models \varphi_1$, dato che l'enunciato non è vero, ad esempio, per $x = 2$. Lo stesso vale per $(\mathcal{M}_3, \cdot, 0, 1)$, dato che esistono matrici non invertibili. Si osservi comunque che interpretando invece il simbolo $\cdot$ come l'operazione somma $+$ di $\mathcal{M}_3$, l'enunciato diventa vero. Tuttavia, nella pratica la scelta "tipografica" dei simboli del linguaggio rispecchia l'uso che vogliamo farne poi interpretandoli nelle strutture. Quindi difficilmente si troverà un simbolo come $\cdot$ interpretato come una qualche "somma".

- $(\mathbb{N}, <, \mathrm{Pr})$ soddisfa ovviamente φ_3 (come già detto, è il Teorema di Euclide sui numeri primi).

- $(\mathbb{Z}/2\,\mathbb{Z}, +, -, 0)$ soddisfa φ_4, che infatti nel nostro caso afferma che ogni elemento di $\mathbb{Z}/2\,\mathbb{Z}$ ha ordine ≤ 2. Ovviamente $(\mathbb{Z}, +, -, 0)$ non soddisfa φ_4.

0.1.5 Teorie e modelli

Definizione 0.1.7. Sia L un linguaggio. Una *L-teoria* (del prim'ordine) è un insieme di L-enunciati. Se abbiamo una teoria T, spesso chiamiamo *assiomi* gli enunciati di T.

Definizione 0.1.8. Sia L un linguaggio e sia T una L-teoria. Una L-struttura si dice *modello* per T se soddisfa tutti gli assiomi di T. Con un leggero abuso di notazione, in questo caso scriveremo $M \models T$.

Esempio 0.1.9. Sia $L = \{+, -, \cdot, 0, 1\}$, con $+, \cdot$ operazioni binarie, $-$ operazione unaria e $0, 1$ costanti. La *teoria dei campi* è la L-teoria data dai seguenti assiomi:

1. $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$
2. $\forall x \forall y (x + y = y + x)$
3. $\forall x (x + 0 = x \wedge 0 + x = x)$
4. $\forall x (x + (-x) = 0 \wedge (-x) + x = 0)$
5. $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
6. $\forall x (x \cdot 1 = x \wedge 1 \cdot x = x)$
7. $\forall x \forall y \forall z ((x + y) \cdot z = (x \cdot z) + (y \cdot z)$
8. $\forall x \forall y (x \cdot y = y \cdot x)$
9. $0 \neq 1$

10. $\forall x(x \neq 0 \Rightarrow \exists y(x \cdot y = 1))$

Ovviamente, una generica L-struttura non sarà necessariamente un campo. Ma se richiediamo che una L-struttura soddisfi tutti gli enunciati della teoria dei campi, allora sarà un campo. Ad esempio, $(\mathbb{R}, +, -, \cdot, 0, 1)$ è un campo se interpretiamo $+, -, \cdot, 0, 1$ nel modo ovvio.

Definizione 0.1.10. Siano L un linguaggio e T una L-teoria. Sia σ un L-enunciato. Diciamo che T *dimostra* σ se ogni modello di T soddisfa σ, in simboli:

$$M \models T \;\Rightarrow\; M \models \sigma$$

per ogni L-struttura M. In questo caso, scriviamo $T \vdash \sigma$.

Definizione 0.1.11. Una L-teoria T si dice *coerente* (o *consistente*) se $T \nvdash \sigma \wedge \neg\sigma$ per ogni L-enunciato σ. Inoltre T si dice *completa* se è coerente e

$$T \vdash \sigma \text{ oppure } T \vdash \neg\sigma$$

per ogni σ enunciato di L.

Concludiamo con un'importante proprietà della logica del prim'ordine:

Teorema 0.1.12. Una teoria è coerente se e solo se ammette un modello.

0.1.6 La Teoria degli Insiemi di Zermelo-Fraenkel

In matematica, e in particolare in logica matematica, la teoria degli insiemi di Zermelo-Fraenkel comprende gli assiomi standard della teoria assiomatica degli insiemi su cui si basa gran parte della matematica ordinaria secondo formulazioni moderne (insieme all'Assioma di Scelta).

Gli assiomi sono il risultato del lavoro di Thoralf Skolem del 1922, basato su lavori precedenti di Abraham Fraenkel nello stesso anno, che si basa sul sistema assiomatico sviluppato da Ernst Zermelo nel 1908 (teoria degli insiemi di Zermelo).

Il linguaggio della teoria degli insiemi contiene un unico simbolo di relazione binaria: $L = \{\in\}$.

Per rendere più agevole la lettura degli assiomi, introduciamo nuovi simboli così definiti:

$$\text{inclusione: } x \subseteq y \Leftrightarrow \forall z(z \in x \Rightarrow z \in y),$$
$$\text{successore: } y = S(x) \Leftrightarrow \forall z(z \in y \Leftrightarrow z \in x \vee z = x),$$
$$\text{intersezione: } y = v \cap w \Leftrightarrow \forall x(x \in y \Leftrightarrow x \in v \wedge x \in w),$$
$$\text{singoletto: } \mathrm{SING}(x) \Leftrightarrow \exists y \in x \forall z \in x(z = y)^4.$$

[4] Quella usata è una forma abbreviata di scrittura. La versione estesa sarebbe $\exists y(y \in x \wedge \forall z(z \in x \Rightarrow z = y))$.

- ***Estensionalità***

$$\forall x \forall y (x \subseteq y \wedge y \subseteq x \Rightarrow x = y)$$

- ***Schema di separazione***

$$\forall w_1, ..., w_n (\forall v \exists y \forall x (x \in y \Leftrightarrow x \in v \wedge \varphi(x, w_1, ..., w_n, v))),$$

per ogni L-formula $\varphi(x, w_1, ..., w_n, v)$. Questo è uno *schema* di assiomi: ogni L-formula φ dà un assioma diverso.

- ***Insieme vuoto***

$$\exists x \forall y (y \notin x)$$

Denotiamo con $\emptyset$ l'unico[5] insieme che soddisfa questo assioma.

- ***Fondazione***

$$\forall x (x \neq \emptyset \Rightarrow \exists y (y \in x \wedge \neg \exists z (z \in x \wedge z \in y)))$$

- ***Coppia***

$$\forall x \forall y (\exists z (x \in z \wedge y \in z))$$

- ***Unione***

$$\forall f (\exists a \forall y \forall x (x \in y \wedge y \in f \Rightarrow x \in a))$$

- ***Schema di rimpiazzamento***

$$\forall w_1, ..., w_n \forall A (\forall x \in A \exists! y \varphi(x, y, w_1, ..., w_n, A) \Rightarrow \exists B \forall x \in A \exists y \in B \varphi(x, y, w_1, ..., w_n, A)),$$

per ogni L-formula $\varphi(x, y, w_1, ..., w_n, A)$.

- ***Infinito***

$$\exists x (\emptyset \in x \wedge \forall y \in x (S(y) \in x))$$

- ***Potenza***

$$\forall x (\exists y \forall z (z \subseteq x \Rightarrow z \in y))$$

Per completezza, includiamo anche l'Assioma di Scelta in una delle sue formulazioni al prim'ordine:

- ***Assioma di Scelta***

$$\forall F (\emptyset \notin F \wedge \forall x \in F \forall y \in F (x \neq y \Rightarrow x \cap y = \emptyset) \Rightarrow \exists C \forall x \in F (\mathrm{SING}(C \cap x)))$$

Gli assiomi appena dati costituiscono la teoria ZFC, indicata anche con $\mathsf{ZF} + \mathsf{AC}$. ZF denota la teoria data da ZFC senza l'Assioma di Scelta.

[5] L'unicità segue immediatamente da Estensionalità.

NOTA: In tutto l'elaborato lavoriamo, salvo indicazione contraria, in ZF.

0.2 Cardinalità e ordinali

Elenchiamo adesso alcune nozioni che ritroveremo spesso nel corso dell'elaborato. È probabile che il lettore conosca già una buona parte di quanto scritto, ma lo invitiamo comunque a leggere questa breve sezione il cui scopo è anche quello di fissare la notazione.

Definizione 0.2.1. Siano A, B due insiemi. Diciamo che A *domina* B e scriviamo $B \preceq A$ se esiste una funzione iniettiva da B in A. Diciamo che A e B sono *equipotenti* e scriviamo $A \approx B$ se esiste una biezione da A in B.

È chiaro che la relazione di equipotenza è una relazione di equivalenza. Il seguente importante teorema assicura che la relazione di dominazione si comporta in modo simile a un ordine:

Teorema 0.2.2 (Schröder-Bernstein)**.** Siano A, B insiemi. Se $A \preceq B$ e $B \preceq A$ allora $A \approx B$.

Se due insiemi A e B sono equipotenti, diremo spesso che hanno la medesima *cardinalità* (o *numero cardinale)*, e scriveremo $|A| = |B|$. Se $A \preceq B$ scriveremo anche $|A| \leq |B|$. Quindi $\leq$ è una relazione d'ordine[6] sulle cardinalità.

Teorema 0.2.3 (Cantor)**.** Sia A un insieme. Allora $A \preceq \mathcal{P}(A)$ ma $A \not\approx \mathcal{P}(A)$.

Definizione 0.2.4. Si definisce una somma sulle cardinalità: se A e B sono insiemi, $|A| + |B| = |A \times \{0\} \cup B \times \{1\}|$.

Definizione 0.2.5. Un insieme X si dice *transitivo* se $x \in X \Rightarrow x \subseteq X$. Un *ordinale* è un insieme transitivo tale che ogni suo elemento è transitivo. La collezione[7] di tutti gli ordinali si indica con Ord.

Gli ordinali si indicano di solito con lettere greche minuscole come $\alpha, \beta, ...$ Si vede subito che ogni elemento di un ordinale è a sua volta un ordinale. Inoltre si dimostra che l'appartenenza insiemistica $\in$ è un ordine lineare sulla famiglia degli ordinali, ed è anche un buon ordine; talvolta scriveremo infatti $\alpha < \beta$ anziché $\alpha \in \beta$. È immediato allora che dato un qualsiasi ordinale α si ha $\alpha = \{\beta \mid \beta < \alpha\}$. È chiaro che se un insieme è in biezione con un ordinale è bene ordinabile; si dimostra che vale anche il viceversa e che due ordinali distinti non sono isomorfi. Quindi possiamo vedere gli ordinali anche come rappresentanti canonici di buoni ordini a meno di isomorfismo.

[6] Con "ordine" intendiamo *ordine parziale.* In un ordine parziale, a differenza degli *ordini lineari* (o *totali*), possono esistere a e b tali che non vale né $a \leq b$ né $b \leq a$.

[7] Usiamo un termine un po' confuso come "collezione" perché stiamo in realtà parlando di una classe propria, non di un insieme.

Si dimostra che ogni $n \in \mathbb{N}$ è un ordinale, così come $\mathbb{N}$ stesso. Inoltre è il più piccolo[8] ordinale infinito. In logica spesso si usa la lettera greca ω per indicare $\mathbb{N}$ e $\aleph_0$ per indicare $|\mathbb{N}|$. Si dimostra che $\aleph_0$ è il più piccolo numero cardinale infinito, nel senso che, per ogni X insieme, $|X| < \aleph_0 \Rightarrow X$ finito. Si dimostra che $|\mathbb{R}| = |2^\omega| = 2^{\aleph_0} > \aleph_0$.

Definizione 0.2.6. Un insieme X si dice *numerabile* se è finito o in biezione con ω, ovvero se $X \preceq \omega$.

Nota. Talvolta useremo il termine "numerabile" per dire proprio $X \approx \omega$, senza renderlo esplicito. Questi casi risulteranno evidenti dal contesto.

Uno strumento particolarmente utile è il seguente:

Definizione 0.2.7. Il *numero di Hartogs* di un insieme X, indicato con $\mathrm{Hrtg}(X)$, è il più piccolo ordinale che non si inietta in X.

Si dimostra che $\mathrm{Hrtg}(X)$ esiste per ogni insieme X. Inoltre, se α è un ordinale, solitamente $\mathrm{Hrtg}(\alpha)$ si denota con α^+.

L'induzione sui numeri naturali è ben nota ad ogni matematico. In realtà si può fare induzione su qualsiasi buon ordine. Di seguito enunciamo l'*induzione transfinita* su Ord.

Teorema 0.2.8. Sia $\Omega = \mathrm{Ord}$ oppure $\Omega \in \mathrm{Ord}$. Sia $I \subseteq \Omega$. Supponiamo che

$$\big(\forall \beta \in \Omega\,(\beta < \alpha \Rightarrow \beta \in I)\big) \Rightarrow \alpha \in I,$$

per ogni $\alpha \in \Omega$. Allora $I = \Omega$.

[8] rispetto all'ordine dato dall'appartenenza.

Capitolo 1

Assioma di Scelta e pratica matematica

Iniziamo col dare la definizione di *funzione di scelta* e *prodotto cartesiano generalizzato*.

Definizione 1.0.9. Sia I un insieme e sia $\mathcal{A} := \{A_i \mid i \in I\}$ una famiglia di insiemi. Diciamo che $f : I \to \bigcup \mathcal{A}$ è una funzione di scelta di I su $\mathcal{A}$ se $f(i) \in A_i$ per ogni $i \in I$.

Definizione 1.0.10. Sia I un insieme e sia $\mathcal{A} := \{A_i \mid i \in I\}$ una famiglia di insiemi. Il prodotto cartesiano generalizzato degli A_i è

$$\times_{i \in I} A_i := \{f \mid f : I \to \bigcup \mathcal{A} \text{ è una funzione di scelta di } I \text{ su } \mathcal{A}\}$$

Possiamo ora formulare l'Assioma di Scelta.

Definizione 1.0.11 (AC)**.** L'Assioma di Scelta asserisce che per ogni insieme I e per ogni famiglia $\mathcal{A} := \{A_i \mid i \in I\}$ tale che $A_i \neq \emptyset$ per ogni $i \in I$, vale

$$\times_{i \in I} A_i \neq \emptyset$$

ovvero, esiste una funzione di scelta di I su $\mathcal{A}$.

Osservazione 1.0.12. Quando scriviamo "$\mathcal{A} = \{A_i \mid i \in I\}$", stiamo di fatto affermando che esiste una biezione tra $\mathcal{A}$ e I. Questo si può sempre fare, dato che come insieme I di indici possiamo prendere $\mathcal{A}$ stesso. In questo caso, una funzione di scelta di $\mathcal{A}$ su $\mathcal{A}$ è una $f : \mathcal{A} \to \bigcup \mathcal{A}$ tale che $f(A) \in A$ per ogni $A \in \mathcal{A}$. Per questo motivo, parleremo semplicemente di funzione di scelta su $\mathcal{A}$. Quindi, AC può essere riformulato così: se $\mathcal{A}$ è un insieme tale che $\forall A \in \mathcal{A}\,(A \neq \emptyset)$, allora esiste una funzione di scelta su $\mathcal{A}$.

1.0.1 Formulazioni alternative

Come vedremo, l'Assioma di Scelta è equivalente (in ZF) a moltissimi altri enunciati. Tuttavia, in questa sezione vogliamo elencare alcune formulazioni alternative molto diffuse in letteratura.

Proposizione 1.0.13. Sono equivalenti:

(i) AC;

(ii) L'Assioma di Scelta per famiglie di insiemi disgiunti: se $\mathcal{A}$ è un insieme tale che $\forall A \in \mathcal{A}(A \neq \emptyset)$ e $\forall A, B \in \mathcal{A}\ (A \neq B \Rightarrow A \cap B = \emptyset)$, allora esiste una funzione di scelta su $\mathcal{A}$;

(iii) se $\mathcal{A}$ è un insieme tale che $\forall A \in \mathcal{A}\ (A \neq \emptyset)$ e $\forall A, B \in \mathcal{A}\ (A \neq B \Rightarrow A \cap B = \emptyset)$, allora
$$\exists T \subseteq \bigcup \mathcal{A} \text{ tale che } \forall A \in \mathcal{A}\,(A \cap T \text{ è un singoletto});$$

(iv) Per ogni insieme X, esiste una funzione di scelta su $\mathcal{P}(X) \setminus \{\emptyset\}$.

Dimostrazione. Immediato. □

Se consideriamo insiemi di indici *finiti*, allora l'esistenza di una funzione di scelta non richiede AC. Lo stesso vale se la famiglia di insiemi è formata da un solo elemento (anche se l'insieme di indici è infinito). Più precisamente:

Proposizione 1.0.14. Le seguenti valgono in ZF:

1. Se $A_i = A$ per ogni $i \in I$, allora $\times_{i \in I} A_i = A^I$, ovvero è non vuoto se $A \neq \emptyset$.

2. Se $I = \{0, ..., n\}$ per qualche $n \in \mathbb{N}$, allora $\times_{i \in I} A_i$ può essere identificato (i.e. è in biezione) con il prodotto cartesiano $A_0 \times ... \times A_n$. Quindi, se $A_i \neq \emptyset$ per ogni $i \in I$, allora $\times_{i \in I} A_i \neq \emptyset$.

Dimostrazione. Per il primo punto basta considerare una qualsiasi funzione costante $i \mapsto a$ con $a \in A$. Per il secondo punto è sufficiente procedere con una semplice induzione su $\mathbb{N}$ (che *non* usa AC). □

Osservazione 1.0.15. La proposizione appena dimostrata *non* afferma che se A_i è finito per ogni $i \in I$, allora $\times_{i \in I} A_i \neq \emptyset$. Infatti, si dimostra che in ZF questo non è necessariamente vero nemmeno se tutti gli A_i sono formati da soli due elementi (distinti).

1.1 Principali equivalenti

Proposizione 1.1.1. Sono equivalenti

(1) AC

(2) Se $f : X \to Y$ è suriettiva, allora ammette un'inversa destra. Ovvero, esiste $g : Y \to X$ tale che $f(g(y)) = y$ per ogni $y \in Y$.

Dimostrazione.
(1) $\implies$ (2): Basta scegliere, grazie a AC, un elemento dall'insieme $f^{-1}(y)$ per ogni $y \in Y$.
(2) $\implies$ (1): Sia $\mathcal{A}$ una famiglia di insiemi non vuoti. Grazie alla Proposizione 1.0.13, possiamo assumere senza perdita di generalità che gli insiemi siano mutualmente disgiunti. Definiamo allora una funzione che manda ogni $a \in \bigcup \mathcal{A}$ nell'unico $A \in \mathcal{A}$ tale che $a \in A$. Questa funzione è chiaramente suriettiva, e una qualsiasi sua inversa destra (che esiste per ipotesi) è una funzione di scelta su $\mathcal{A}$. □

Si osservi che la proposizione appena mostrata mette in luce come AC sia talvolta necessario per provare anche risultati di base e intuitivamente evidenti.

Il prossimo risultato è un esempio in qualche modo opposto: il fatto che ogni insieme sia bene ordinabile appare qualcosa di poco chiaro, e forse addirittura in contrasto con la nostra intuizione matematica[1]. Questa sensazione di "disorientamento" si può riassumere in una paradossale citazione di J.L. Bona: *"The Axiom of Choice is obviously true, the Well–Ordering Principle is obviously false; and who can tell about Zorn's Lemma"*[2].

Teorema 1.1.2. Sono equivalenti:

(1) AC

(2) Ogni insieme è in biezione con un ordinale.

Dimostrazione.
(2) $\implies$ (1): Per ipotesi ogni insieme è bene ordinabile. Allora, preso qualsiasi X possiamo scegliere un buon ordine $\lhd_X$ su X (*senza* usare AC, dato che stiamo scegliendo un buon ordine per un singolo insieme X). La funzione definita da $f(A) = \lhd_X\text{-min } A$ è una funzione di scelta su $\mathcal{P}(X) \setminus \{\emptyset\}$.
(1) $\implies$ (2): Sia X un insieme. Se $X = \emptyset$, allora X è banalmente bene ordinabile. Supponiamo quindi X non vuoto e fissiamo una funzione di scelta C su $\mathcal{P}(X) \setminus \{\emptyset\}$. Sia x_0 un elemento di X, per esempio $x_0 = C(X)$ e supponiamo di avere costruito

[1] Si provi a immaginare un buon ordine su $\mathbb{R}$.
[2] [4], p. 145

tramite induzione transfinita $x_0, x_1, ..., x_\beta, ...$ elementi distinti di X per tutti i $\beta < \alpha$ per qualche ordinale α. Se $X = \{x_\beta \mid \beta < \alpha\}$, allora $\alpha \to X$, $\beta \mapsto x_\beta$ è la biezione cercata. Altrimenti scegliamo un nuovo elemento $x_\alpha \in X$ distinto dai precedenti, per esempio $x_\alpha = C(X \setminus \{x_\beta \mid \beta < \alpha\})$. Se la funzione $\alpha \mapsto x_\alpha$ fosse definita per tutti gli $\alpha < \mathrm{Hrtg}(X)$, allora avremmo un'iniezione $\mathrm{Hrtg}(X) \to X$, contro la definizione di numero di Hartogs. Quindi esiste un $\overline{\alpha} < \mathrm{Hrtg}(X)$ tale che $X = \{x_\beta \mid \beta < \overline{\alpha}\}$. □

Nota. La dimostrazione appena presentata non è del tutto rigorosa, in quanto la funzione $\mathrm{Ord} \to X$, $\alpha \mapsto x_\alpha$ è definita per ricorsione, e in particolare tramite *ricorsione transfinita*. Il fatto che una tale funzione esista e sia ben definita non è garantito a priori, ma è una conseguenza del Teorema di Ricorsione Transfinita. Tuttavia, la nostra dimostrazione del Teorema 1.1.2 ci sembra intuitivamente chiara, quindi non tratteremo qui il Teorema di Ricorsione Transfinita[3].

Mostreremo adesso che AC è equivalente ad altri due principi frequentemente utilizzati nella pratica matematica: il principio di massimalità di Hausdorff e il Lemma di Zorn.

Teorema 1.1.3. Sono equivalenti:

(1) AC;

(2) **Principio di massimalità di Hausdorff:** Ogni insieme non vuoto parzialmente ordinato contiene una catena[4] massimale;

(3) **Lemma di Zorn:** Ogni insieme non vuoto parzialmente ordinato in cui ogni catena ha un maggiorante, contiene un elemento massimale.

Dimostrazione.
(1) $\implies$ (2): Sia X un insieme. Per assurdo, sia $\leq$ un ordine parziale su X privo di catene massimali. Quindi, se $C \subseteq X$ è una catena, l'insieme

$$K(C) = \{x \in X \setminus C \mid C \cup \{x\} \text{ è una catena}\}$$

è non vuoto. Fissiamo una funzione di scelta $F : \mathcal{P}(X) \setminus \{\emptyset\} \to X$. La funzione $g : \mathrm{Hrtg}(X) \to X$ definita da

$$g(\alpha) = F(K(\{g(\beta) \mid \beta < \alpha\}))$$

è iniettiva, contro la definizione di numero di Hartogs.
(2) $\implies$ (3): Sia X un insieme. Sia $\leq$ un ordine parziale su X in cui ogni catena

[3] si veda eventualmente [5], p. 48.

[4] In un insieme parzialmente ordinato X, un sottoinsieme $C \subseteq X$ si dice *catena* se è linearmente ordinato, i.e. se $\forall x, y \in C \ (x \leq y \vee y \leq x)$.

ha un maggiorante. Se $C \subseteq X$ è una catena massimale, allora il maggiorante di C deve appartenere a C e quindi è un elemento massimale di X.
(3) $\implies$ (1): Se $X = \emptyset$ l'enunciato vale banalmente prendendo la funzione vuota. Sia allora $X \neq \emptyset$. Sia

$$\mathcal{F} := \{f \mid f \text{ è una funzione}, \mathrm{dom}(f) \subseteq \mathcal{P}(X) \setminus \{\emptyset\} \text{ e } \forall A \in \mathrm{dom}(f)\ (f(A) \in A)\}$$

$\mathcal{F}$ è chiaramente non vuoto, dato che sicuramente esistono $A \in \mathcal{P}(X) \setminus \{\emptyset\}$ e $a \in A$, perciò la funzione $A \mapsto a$ sta in $\mathcal{F}$. Inoltre, $\mathcal{F}$ è parzialmente ordinato da $\subseteq$[5]. Sia $\mathcal{G} \subseteq \mathcal{F}$ una catena. Sia $g := \bigcup \mathcal{G}$. Affermiamo che $g \in \mathcal{F}$. L'unica cosa da controllare è che g è davvero una funzione, il che segue banalmente dall'ipotesi che $\mathcal{G}$ è un insieme di funzioni totalmente ordinato dall'inclusione, quindi ogni funzione è estensione di quelle che la precedono. Inoltre, è chiaro che g è un maggiorante per $\mathcal{G}$. Quindi le ipotesi del Lemma di Zorn sono soddisfatte, e perciò esiste un elemento massimale $G \in \mathcal{F}$. Per concludere basta mostrare che G è definita su tutto $\mathcal{P}(X) \setminus \{\emptyset\}$. Supponiamo per assurdo che esista $\emptyset \neq S \subseteq X$ tale che G non è definita su S. Sia $s \in S$. Allora definiamo

$$G'(A) := \begin{cases} G(A) & \text{se } A \in \mathrm{dom}(G) \\ s & \text{se } A = S \end{cases}$$

Si ha che $G' \in \mathcal{F}$ e $G' \supsetneq G$, assurdo. □

1.2 C'è, ma non si vede

Spesso non è immediato individuare un eventuale ricorso dell'Assioma di Scelta all'interno di una dimostrazione. Talvolta, persino lo stesso autore della dimostrazione non è consapevole di averlo usato. A prova di questo fatto, citiamo ad esempio Borel, il quale, pur rifiutando AC per famiglie non numerabili di insiemi[6], lo utilizzò applicandolo proprio a una famiglia di cardinalità $2^{\aleph_0}$ per dimostrare che esistono funzioni continue reali di variabile reale che non possono essere rappresentate come serie doppie di polinomi. Lo stesso accadde a Lebesgue: nonostante si dichiarasse esplicitamente critico nei confronti di AC, lo usò per dimostrare che l'unione numerabile di sottoinsiemi misurabili di $\mathbb{R}$ è misurabile.

[5] Ricordiamo che una funzione è un insieme di coppie ordinate.

[6] *"The last concept* [AC] *seems to me to be entirely devoid of sense. As regards a denumerable infinity of choices, they cannot, of course, all be performed, but we can at least indicate such a procedure that, if we establish it beforehand, we may be sure that each choice will be made within a finite period of time; therefore, if two given systems of choice are different, we are sure to notice this after a finite number of operations. When an infinite number of choices is not denumerable, it is impossible to imagine a way of defining it, i.e., distinguishing it from an analogous infinite number of choices; thus it is impossible to regard it as a mathematical creation which can be introduced in arguments."* E. Borel, [6]

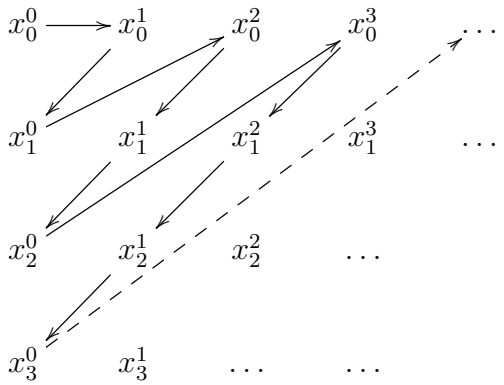
Vediamo allora un esempio alquanto istruttivo di una dimostrazione che appare costruttiva, ma che in realtà non lo è.

Proposizione 1.2.1. Unione numerabile di insiemi numerabili è numerabile

Dimostrazione. Sia $X = \bigcup_{n\in\mathbb{N}} X_n$ unione numerabile di insiemi numerabili X_n. Assumiamo senza perdita di generalità che gli X_n siano a due a due disgiunti. X_n è numerabile, quindi può essere scritto nella forma

$$X_n = \{x_n^i \mid i \in \mathbb{N}\} = \{x_n^0, x_n^1, x_n^2, ...\}$$

Definiamo allora una biezione $f : \mathbb{N} \to X$ come nella seguente figura:



ovvero,

$$f(0) = x_0^0, \quad f(1) = x_0^1, \quad f(2) = x_1^0, \quad f(3) = x_0^2, \quad f(4) = x_1^1,$$
$$f(5) = x_2^0, \quad f(6) = x_0^3, ...$$

Possiamo anche considerare la sua inversa $f^{-1} : X \to \mathbb{N}$, data dalla formula esplicita:

$$f^{-1}(x_i^k) = (i+1) + \sum_{\nu=1}^{i+k} \nu = (i+1) + \frac{(i+k)\cdot(i+k+1)}{2}$$

Quindi X è numerabile. □

Osservazione 1.2.2. La dimostrazione appena presentata sembra fornire una biezione esplicita tra $\mathbb{N}$ e X, ma in realtà non è così. In effetti, una volta che tutti gli X_n sono stati espressi nella forma $X_n = \{x_n^i \mid i \in \mathbb{N}\}$, il resto della dimostrazione è davvero costruttiva. Il problema è che per scrivere *tutti* gli X_n in quella forma, stiamo in realtà utilizzando AC. Cerchiamo di capire perché: un insieme si dice numerabile se *esiste* una biezione con $\mathbb{N}$. Ma le possibili biezioni sono molteplici! Quindi per scegliere una biezione per ogni X_n dobbiamo effettuare una quantità infinita (numerabile) di scelte, ricorrendo perciò ad AC.

Per completezza, segnaliamo che l'enunciato in questione è davvero indipendente da ZF (ma è più debole di AC)[7].

1.3 C'è, ma non serve

Nella sezione precedente abbiamo visto come l'utilizzo di AC sia talvolta "nascosto". Vogliamo adesso presentare qualche esempio di situazione opposta: enunciati dimostrati utilizzando AC, che possono però essere dimostrati anche senza ricorrervi.

Può accadere che la dimostrazione senza AC richieda un totale stravolgimento della dimostrazione iniziale, ma talvolta è sufficiente un piccolo aggiustamento. È il caso del seguente.

Proposizione 1.3.1. Ogni sottoinsieme chiuso di uno spazio compatto è compatto.

Dimostrazione. Sia X un sottoinsieme chiuso di uno spazio compatto Y, e sia $\mathcal{B}$ un ricoprimento aperto di X, sul quale consideriamo ovviamente la topologia indotta da Y. Per ogni $B \in \mathcal{B}$, scegliamo un aperto $A(B)$ di Y tale che $B = X \cap A(B)$. Definiamo $\mathcal{A} = \{A(B) \mid B \in \mathcal{B}\}$. Allora $\mathcal{A} \cup \{Y \setminus X\}$ è un ricoprimento aperto di Y, e quindi ammette un sottoricoprimento finito $\mathcal{F}$. Perciò, $\mathcal{G} = \{X \cap F \mid F \in \mathcal{F} \cap \mathcal{A}\}$ è un ricoprimento finito di X con $\mathcal{G} \subseteq \mathcal{B}$. □

Osservazione 1.3.2. In questa dimostrazione abbiamo fatto uso di AC per scegliere gli $A(B)$. Ma in realtà l'utilizzo di AC può essere evitato definendo diversamente $\mathcal{A}$:

$$\mathcal{A} = \{A \mid A \text{ è un aperto di } Y \text{ e } X \cap A \in \mathcal{B}\}.$$

In questo modo, il nuovo $\mathcal{A}$ potrebbe essere molto più grosso rispetto a quello originale, ma la dimostrazione funziona comunque senza modificare nient'altro.

In casi particolarmente fortunati, una semplice analisi più attenta rivela che una dimostrazione apparentemente in ZFC deriva in realtà anche solo da ZF senza cambiare nulla. Vediamo un esempio.

Proposizione 1.3.3. L'unione disgiunta di un numero finito di spazi compatti è compatta.

Dimostrazione. Sia X l'unione disgiunta di spazi compatti $X_1, ..., X_n$, e sia $\mathcal{B}$ un ricoprimento aperto di X. Per ogni $i = 1, ..., n$ l'insieme $\mathcal{B}_i = \{B \cap X_i \mid B \in \mathcal{B}\}$ è un ricoprimento aperto di X_i. Per compattezza, ogni $\mathcal{B}_i$ contiene un ricoprimento finito $\mathcal{F}_i$ di X_i. Per ogni $F \in \mathcal{F}_i$ scegliamo un elemento $B(F)$ in $\mathcal{B}$ tale che $F = B(F) \cap X_i$. Allora l'insieme $\mathcal{F} = \{B(F) \mid i \in \{1, ..., n\} \text{ e } F \in \mathcal{F}_i\}$ è un ricoprimento finito di X con $\mathcal{F} \subseteq \mathcal{B}$. □

[7] Si veda: `http://mathoverflow.net/questions/74743/countable-unions-and-the-axiom-of-countable-choice`

Osservazione 1.3.4. Nella dimostrazione abbiamo usato AC per scegliere i $B(F)$. Ma osservando bene la situazione, si poteva anche farne a meno. Infatti, gli X_i sono in numero finito e, per costruzione, ogni $\mathcal{F}_i$ è una famiglia finita. Quindi dobbiamo effettuare solo un numero finito di scelte, ovvero possiamo evitare l'utilizzo di AC.

Capitolo 2

Disastri senza Scelta

2.1 Finitezza

Solitamente la definizione di *insieme finito* viene data in termini di numeri naturali: un insieme si dice finito se è in biezione con un numero naturale[1]. Tuttavia, una tale definizione può risultare poco soddisfacente se si ritiene che il concetto di finitezza sia più "primitivo" e "basilare" di quello di numero naturale. Questa era proprio la posizione di Frege e Dedekind, per citarne alcuni. Storicamente infatti, la prima definizione alternativa si deve proprio a quest'ultimo (1888):

Definizione 2.1.1. [2] Un insieme X si dice *Dedekind-infinito* o *D-infinito* se esiste un suo sottoinsieme proprio $Y \subsetneq X$ tale che $|X| = |Y|$. X si dice *D-finito* se non è D-infinito.

Lo scopo di questa sezione è mettere a confronto alcune diverse definizioni di insieme finito. Come vedremo, le definizioni "dialogano" davvero male in assenza di AC. Iniziamo facendo vedere che ZF è comunque in grado di dimostrare che gli insiemi D-finiti godono di alcune proprietà intuitivamente corrette.

Proposizione 2.1.2. Sono equivalenti (in ZF):

(1) X è D-infinito.

(2) $|X| = |X| + 1$.[3]

(3) $\aleph_0 \leq |X|$, i.e. esiste una funzione iniettiva $\mathbb{N} \to X$.

[1] Ricordiamo che $n = \{0, ..., n-1\}$ per ogni $n \in \mathbb{N}$.
[2] [21]
[3] Qui 1 è inteso come la cardinalità degli insiemi con un solo elemento.

Dimostrazione.
(3) $\implies$ (2): Sia $f : \mathbb{N} \to X$ una funzione iniettiva. Sia ∞ un elemento non contenuto in X[4]. Allora la mappa $g : X \to X \cup \{\infty\}$ definita da

$$g(x) = \begin{cases} \infty & \text{se } x = f(0) \\ f(n) & \text{se } x = f(n+1) \\ x & \text{altrimenti} \end{cases}$$

è una biezione.
(2) $\implies$ (1): Sia ∞ un elemento non contenuto in X e sia $f : X \to X \cup \{\infty\}$ una biezione. Allora f^{-1} ristretta a X è iniettiva e ha come immagine il suo sottoinsieme proprio $X \setminus \{f^{-1}(\infty)\}$.
(1) $\implies$ (3): Sia $f : X \to X$ iniettiva. Supponiamo che l'immagine di f sia un sottoinsieme proprio di X. Sia allora $y \in X \setminus f[X]$ e definiamo ricorsivamente[5] $g : \mathbb{N} \to X$ data da $g(0) = y$ e $g(n+1) = f(g(n))$. Allora g è iniettiva. □

Purtroppo, ZF non è abbastanza potente per dimostrare alcune proprietà che vorremmo decisamente fossero soddisfatte da ogni insieme "finito".

Proposizione 2.1.3. In alcuni modelli di ZF possono essere soddisfatte le seguenti:

1. Esiste un'unione D-finita di insiemi D-finiti che è D-infinita.
2. Esiste un insieme D-finito il cui insieme delle parti è D-infinito.
3. Esiste un insieme D-infinito che è immagine di un insieme D-finito.

Dimostrazione. Consideriamo un modello di ZF con la seguente proprietà:

> Esiste una sequenza $(X_n)_{n\in\mathbb{N}}$ di insiemi mutualmente disgiunti formati da due elementi, i.e. $X_n = \{x_n, y_n\}$, tale che $X = \bigcup_{n\in\mathbb{N}} X_n$ è D-finito.

Si dimostra che un tale modello esiste[6] (e non soddisfa AC). Mostriamo ora che questo modello soddisfa tutti gli enunciati in questione:

1. Per ogni $z \in X$, consideriamo l'insieme $Y_z = \{z, n\}$, dove $n \in \mathbb{N}$ è l'unico naturale tale che $z \in X_n$. Allora $Y = \bigcup_{z\in X} Y_z$ è unione D-finita di insiemi D-finiti. Ma $Y = \mathbb{N} \cup \bigcup_n X_n$ è D-infinito, dato che la funzione $f : \mathbb{N} \to Y$ definita da $f(n) = n$ è ovviamente iniettiva.

[4]Si dimostra facilmente che gli assiomi di ZF ci permettono sempre di trovare un elemento che non appartiene a un certo insieme.

[5]Il Teorema di Ricorsione sui naturali non usa AC.

[6]Ad esempio il modello N2(2) in [9]. È chiaro che in tale modello non può esistere una funzione di scelta C di $\mathbb{N}$ su $\{X_n \mid n \in \mathbb{N}\}$, perché altrimenti $f : \mathbb{N} \to X$, $n \mapsto C(X_n)$ sarebbe una funzione iniettiva, ovvero X sarebbe D-infinito per la Proposizione 2.1.2.

2. Nonostante X sia D-finito, il suo insieme delle parti $\mathcal{P}(X)$ è D-infinito. Infatti la funzione $f : \mathbb{N} \to \mathcal{P}(X)$ definita da $f(n) = \bigcup_{m \leq n} X_m$ è iniettiva.

3. Nonostante X sia D-finito, la funzione $f : X \to \mathbb{N}$ che manda ogni $x \in X$ nell'unico $n \in \mathbb{N}$ tale che $x \in X_n$, è suriettiva.

□

La Proposizione 2.1.3 mostra che la definizione di insieme finito secondo Dedekind si comporta estremamente male in assenza di AC. Vedremo tra poco che tutti i problemi scompaiono in presenza di AC. Nel frattempo, introduciamo una terza (e ultima) definizione di insieme finito dovuta a Tarski (1924).

Definizione 2.1.4. [7] Un insieme X si dice *Tarski-finito* se ogni sottoinsieme non vuoto di $\mathcal{P}(X)$ contiene un elemento minimale rispetto all'ordine dato dall'inclusione. Un insieme si dice *Tarski-infinito* se non è Tarski-finito.

Proposizione 2.1.5. Sono equivalenti (in ZF):

(1) X è Tarski-finito.

(2) Se $\mathfrak{U} \subseteq \mathcal{P}(X)$ soddisfa

   a) $\emptyset \in \mathfrak{U}$, e

   b) se $A \in \mathfrak{U}$ e $x \in X$, allora $A \cup \{x\} \in \mathfrak{U}$,

   allora $X \in \mathfrak{U}$.

Dimostrazione.
(1) $\implies$ (2): Sia $\mathfrak{U}$ come in (2). La collezione $\mathcal{B} = \{X \setminus A \mid A \in \mathfrak{U}\}$ è non vuota e quindi per ipotesi ha un elemento minimale, diciamo B. Quindi $\mathfrak{U}$ ha un elemento massimale $A = X \setminus B$. La condizione (b) implica banalmente $A = X$.
(2) $\implies$ (1): Sia $\mathfrak{U}$ la famiglia di tutti i sottoinsiemi Tarski-finiti di X. Poiché $\mathfrak{U}$ soddisfa (a) e (b)[8], abbiamo che per ipotesi vale $X \in \mathfrak{U}$. Ovvero X è Tarski-finito. □

Corollario 2.1.6. Ogni insieme è finito se e solo se è Tarski-finito.

Dimostrazione. Supponiamo X finito, ovvero $|X| = n$ per qualche $n \in \mathbb{N}$. Allora $|\mathcal{P}(X)| = 2^n$, ovvero anche $\mathcal{P}(X)$ è finito[9]. Perciò un suo qualsiasi sottoinsieme è finito, e ogni insieme finito parzialmente ordinato contiene banalmente un elemento

[7] Tarski, [7].
[8] La verifica è immediata.
[9] La dimostrazione di questo fatto è ben nota, procede per induzione e vale in ZF.

minimale. Viceversa, supponiamo X infinito. Sia $\mathfrak{U} = \{F \subseteq X \mid F \text{ è finito}\} \subseteq \mathcal{P}(X)$. Allora ovviamente $\mathfrak{U}$ soddisfa le condizioni (a) e (b) della Proposizione 2.1.5. Se per assurdo X fosse Tarski-finito, allora avremmo che $X \in \mathfrak{U}$, ovvero X è finito, contraddizione. □

Osservazione 2.1.7. Alla luce del corollario appena mostrato, è chiaro che gli insiemi Tarski-finiti non soddisfano nessuna delle spiacevoli proprietà degli insiemi D-finiti descritte nella Proposizione 2.1.3. Quest'ultima affermazione si può dimostrare piuttosto facilmente usando semplicemente la definizione di insieme Tarski-finito, ma data la totale equivalenza con la definizione tradizionale di insieme finito, preferiamo non annoiare il lettore[10]. Inoltre, per lo stesso motivo, d'ora in poi scriveremo semplicemente "finito" anziché "Tarski-finito".

Vogliamo concludere questa sezione occupandoci del rapporto tra finitezza in senso tradizionale e finitezza secondo Dedekind.

Proposizione 2.1.8. Ogni insieme finito è D-finito.

Dimostrazione. Supponiamo che X sia D-infinito. Allora esiste $f : \mathbb{N} \to X$ iniettiva. Quindi il sottoinsieme di $\mathcal{P}(X)$ dato da $\mathfrak{U} = \{\{f(m) \mid m \geq n\} \mid n \in \mathbb{N}\}$ è non vuoto, ma ovviamente non contiene nessun elemento minimale (rispetto all'inclusione). Quindi X è infinito. □

L'implicazione inversa non vale in ZF. Infatti, si possono trovare modelli di ZF nei quali esistono insiemi infiniti che sono D-finiti (ad esempio X della dimostrazione di 2.1.3, che è banalmente infinito). Si osservi che questo, unito alla caratterizzazione (3) della Proposizione 2.1.2, significa che in qualche modello di ZF esistono insiemi infiniti che non contengono una "copia" di $\mathbb{N}$, nel senso che $\mathbb{N}$ non si inietta in essi.

Possiamo chiederci: quando i due concetti di finitezza coincidono? Il prossimo teorema mostrerà che condizione (ovviamente necessaria, ma anche) sufficiente è che uno qualsiasi dei disastri della Proposizione 2.1.3 non si avveri. Abbiamo prima bisogno di un lemma:

Lemma 2.1.9. Sono equivalenti:

(1) $\aleph_0 \leq^* |X|$, ovvero esiste una suriezione $X \to \mathbb{N}$.

(2) $\mathcal{P}(X)$ è D-infinito, ovvero esiste un'iniezione $\mathbb{N} \to \mathcal{P}(X)$.

Dimostrazione.
(1) $\implies$ (2): Sia $f : X \to \mathbb{N}$ suriettiva. Allora la funzione $g : \mathbb{N} \to \mathcal{P}(X)$ definita da $g(n) = f^{-1}(n)$ è iniettiva.
(2) $\implies$ (1): Sia $f : \mathbb{N} \to \mathcal{P}(X)$ iniettiva. Vogliamo riuscire a definire ricorsivamente

[10] Si veda eventualmente p. 46, [1].

una funzione $g : \mathbb{N} \to \mathcal{P}(X)$ tale che tutti i $g(n)$ sono non vuoti e mutualmente disgiunti. Infatti, una volta che disponiamo di una tale g, la mappa $h : X \to \mathbb{N}$ definita da

$$h(x) = \begin{cases} n & \text{se } x \in g(n) \\ 0 & \text{se } x \notin \bigcup_{n\in\mathbb{N}} g(n) \end{cases}$$

è suriettiva.
Cerchiamo allora di costruire g come descritto. Sia $n \in \mathbb{N}$. Supponiamo ora di aver definito $g(m)$ per tutti gli $m < n$ in modo che

$$\text{l'insieme } \{f(k) \setminus \bigcup_{m<n} g(m) \mid k \geq n\} \text{ è finito.} \qquad (*)$$

Osserviamo che la condizione $(*)$ implica banalmente che $f(k) \setminus \bigcup_{m<n} g(m) \neq \emptyset$ per una quantità infinita di k. Di conseguenza, di nuovo grazie a $(*)$, per almeno uno di questi k si avrà anche che $f(k) \cup \bigcup_{m<n} g(m) \neq X$. Perciò, siamo autorizzati a definire

$$n^* = \min \left\{ k \;\middle|\; k \geq n \text{ e } f(k) \setminus \bigcup_{m<n} g(m) \neq \emptyset \neq X \setminus \left(f(k) \cup \bigcup_{m<n} g(m) \right) \right\}.$$

Consideriamo ora due casi: supponiamo che $\{f(k) \setminus [f(n^*) \cup \bigcup_{m<n} g(m)] \mid k > n^*\}$ sia

- infinito. Allora definiamo $g(n) = f(n^*) \setminus \bigcup_{m<n} g(m)$.
- finito. Allora definiamo $g(n) = X \setminus \big(f(n^*) \cup \bigcup_{m<n} g(m)\big)$.

Per costruzione di n^*, è chiaro che in entrambi i casi $g(n) \neq \emptyset$ e che $g(n)$ è disgiunto da tutti i $g(m)$ precedenti. Resta da verificare che la condizione $(*)$ è soddisfatta (sostituendo $n + 1$ a n). Nel primo dei due casi, questo è immediato. Nel secondo caso, deriva in modo semplice (ma noioso da verificare) da $(*)$ e dall'ipotesi di f iniettiva. □

Teorema 2.1.10. Sono equivalenti:

(1) Finito = D-finito.

(2) Unione D-finita di insiemi D-finiti è D-finita.

(3) Le immagini di insiemi D-finiti sono D-finite.

(4) L'insieme delle parti di un insieme D-finito è D-finito.

(5) Ogni insieme X è confrontabile con $\aleph_0$, i.e. vale $\aleph_0 \leq |X|$ oppure $|X| \leq \aleph_0$.

Dimostrazione.
(1) $\Longrightarrow$ (2): Segue banalmente dall'Osservazione 2.1.7.
(2) $\Longrightarrow$ (3): Sia X D-finito e sia $f : X \to Y$ suriettiva. Allora $Y = \bigcup_{x \in X} \{f(x)\}$ è unione D-finita di insiemi D-finiti, quindi D-finita.
(3) $\Longrightarrow$ (4): Supponiamo $\mathcal{P}(X)$ D-infinito. Allora, grazie al lemma precedente esiste $f : X \to \mathbb{N}$ suriettiva. Poiché $\mathbb{N}$ è D-infinito, per ipotesi abbiamo che X è D-infinito.
(4) $\Longrightarrow$ (1): È sufficiente mostrare che ogni insieme infinito è D-infinito. Sia allora X infinito. La funzione $f : \mathbb{N} \to \mathcal{P}(\mathcal{P}(X))$ definita da $f(n) = \{A \subseteq X \mid |A| = n\}$ è iniettiva. Quindi $\mathcal{P}(\mathcal{P}(X))$ è D-infinito. Per ipotesi, otteniamo che $\mathcal{P}(X)$ è D-infinito. Di nuovo per ipotesi, anche X è D-infinito.
(1) $\Longleftrightarrow$ (5): Se ogni insieme infinito è D-infinito, allora per ogni insieme infinito X vale $\aleph_0 \leq |X|$, mentre ovviamente $|X| \leq \aleph_0$ se X è finito. Viceversa, se X è un insieme infinito, allora si ha necessariamente $\aleph_0 \leq |X|$, dato che $|A| < \aleph_0 \Rightarrow A$ finito, per ogni insieme A. □

Osserviamo che gli insiemi D-finiti possono essere piuttosto "grossi". Se X è D-finito e $\mathcal{P}(X)$ è D-infinito, allora per il Lemma 2.1.9 si ha $\aleph_0 \leq^* |X|$. Ancora peggio: si può dimostrare[11] che è consistente con ZF assumere che per $\aleph_\alpha$ arbitrariamente grandi esistono insiemi D-finiti X tali che $\aleph_\alpha \leq^* |X|$.

La dimostrazione dell'ultimo teorema mette in luce un fatto interessante: nonostante la classe di tutti gli insiemi finiti e la classe di tutti gli insiemi D-finiti non coincidano, la prima è completamente determinata dalla seconda. Per chiarezza ripetiamo la dimostrazione.

Proposizione 2.1.11. Sono equivalenti:

(1) X è finito.

(2) $\mathcal{P}(\mathcal{P}(X))$ è D-finito.

Dimostrazione.
(1) $\Longrightarrow$ (2): Immediato per la Proposizione 2.1.8.
(2) $\Longrightarrow$ (1): Supponiamo X infinito. La funzione $f : \mathbb{N} \to \mathcal{P}(\mathcal{P}(X))$ definita da $f(n) = \{A \subseteq X \mid |A| = n\}$ è iniettiva. Quindi $\mathcal{P}(\mathcal{P}(X))$ è D-infinito. □

L'ultimo risultato della sezione ci restituisce finalmente un po' di serenità:

Proposizione 2.1.12. Se vale AC, finito = D-finito.

[11] Monro, [8].

Dimostrazione. È sufficiente mostrare che ogni insieme infinito X è D-infinito. Se X è infinito allora, per ogni $n \in \mathbb{N}$, l'insieme X_n di tutte le n-uple iniettive $\overrightarrow{t_n} = (x_1, ..., x_n)$ di X è non vuoto[12]. Allora per AC esiste una sequenza di tuple

$$\left(\overrightarrow{t_n}\right)_{n\in\mathbb{N}} \in \times_{n\in\mathbb{N}} X_n.$$

La concatenazione di tutte le $\overrightarrow{t_n}$ definisce una successione $(s_n)_{n\in\mathbb{N}}$ in X che ha immagine infinita (più precisamente: se $\overrightarrow{t_n} = (x_1^n, ..., x_n^n)$, allora $s_{n\frac{(n+1)}{2}+k} = x_k^{n+1}$ con $n \in \mathbb{N}$ e $k \in \{1, ..., n+1\}$).
La successione $(s'_n)_{n\in\mathbb{N}}$ ottenuta "cancellando" tutti i termini ripetuti di s_n è ovviamente una funzione iniettiva $\mathbb{N} \to X$ (più precisamente: $s'_n = s_{\min\{k|s_k \notin \{s'_m|m<n\}\}}$).
Quindi X è D-infinito. □

Il converso non vale. Infatti, esistono modelli di ZF che soddisfano l'enunciato "finito = D-finito", ma non soddisfano AC[13].

2.2 Aritmetica cardinale

Verso la fine del XIX secolo, Georg Cantor diede inizio allo studio della Teoria degli Insiemi come la conosciamo ora. In particolare, fondò i suoi lavori sull'idea di confrontare le "dimensioni" di due insiemi in termini di funzioni iniettive.

È chiaro che, affinché una definizione di *dimensione* di un insieme ci soddisfi appieno, vorremmo che, applicando una medesima operazione insiemistica ad insiemi di uguale *dimensione*, i due insiemi risultanti avessero la stessa *dimensione*. Inoltre, ci piacerebbe che due qualsiasi insiemi fossero sempre confrontabili. Purtroppo, in assenza di AC, queste due condizioni (insieme a molte altre) non sono necessariamente soddisfatte, se con *dimensione* intendiamo *cardinalità*.

Abbiamo già osservato questo fatto relativamente a $\aleph_0$ nella precedente sezione con il Teorema 2.1.10. Vogliamo ora presentare qualche risultato che descrive in modo più preciso l'aritmetica cardinale in assenza di AC.

Definizione 2.2.1. Sia I un insieme e sia $\{A_i \mid i \in I\}$ una successione di insiemi. L'*unione disgiunta* degli A_i è

$$\biguplus_{i\in I} A_i = \bigcup_{i\in I} A_i \times \{i\}$$

[12]La dimostrazione è immediata per induzione: supponiamo di aver definito $f : \{1, ..., n\} \to X$ iniettiva. Se $X \setminus \mathrm{ran}(f) \neq \emptyset$, allora estendiamo f mandando $n+1$ in un qualsiasi elemento che non sta nell'immagine. Se per assurdo $X \setminus \mathrm{ran}(f) = \emptyset$, allora f è una biezione, contro l'ipotesi di X infinito.

[13]Ad esempio il modello di Sageev (M6 in [9]).

Definizione 2.2.2. Definiamo la somma e il prodotto numerabile di cardinali in questo modo: sia $\{X_n \mid n \in \mathbb{N}\}$ una famiglia di insiemi. Allora

- $\sum_{n\in\mathbb{N}} |X_n| := |\biguplus_{n\in\mathbb{N}} X_n|$,
- $\prod_{n\in\mathbb{N}} |X_n| := |\times_{n\in\mathbb{N}} X_n|$,

dove $\times$ indica il prodotto cartesiano generalizzato (Definizione 1.0.10).

Il seguente mostra che in ZF, quella appena data non è una buona definizione.

Proposizione 2.2.3. In alcuni modelli di ZF esistono successioni di insiemi $(A_n)_{n\in\mathbb{N}}$ e $(B_n)_{n\in\mathbb{N}}$ tali che $|A_n| = |B_n|$ per ogni $n \in \mathbb{N}$, ma $\sum_{n\in\mathbb{N}} |A_n| \neq \sum_{n\in\mathbb{N}} |B_n|$ e $\prod_{n\in\mathbb{N}} |A_n| \neq \prod_{n\in\mathbb{N}} |B_n|$.

Dimostrazione. Supponiamo di lavorare in un modello di ZF in cui esiste una successione $(A_n)_{n\in\mathbb{N}}$ tale che ogni A_n contiene esattamente due elementi e $\times_{n\in\mathbb{N}} A_n = \emptyset$[14]. Sia $B_n = \{0, 1\}$ per ogni $n \in \mathbb{N}$. Quindi $|A_n| = 2 = |B_n|$ per ogni $n \in \mathbb{N}$. Si ha però che:

1. Ovviamente $|\times_{n\in\mathbb{N}} A_n| = 0$. Inoltre $\times_{n\in\mathbb{N}} B_n = 2^{\mathbb{N}}$. Quindi otteniamo $\prod_{n\in\mathbb{N}} |B_n| = 2^{\aleph_0} \neq \prod_{n\in\mathbb{N}} |A_n|$.
2. È chiaro che $\biguplus_{n\in\mathbb{N}} B_n$ è in biezione con $\mathbb{N}\times\{0, 1\}$. Vogliamo mostrare che $\prod_{n\in\mathbb{N}} |A_n| \neq \aleph_0 = \prod_{n\in\mathbb{N}} |B_n|$. L'uguaglianza segue subito da questo risultato elementare[15]: $|\mathbb{N}\times\{0, 1\}| = |\mathbb{N}|$. Per verificare la disuguaglianza procediamo per assurdo[16]. Se per assurdo esistesse una biezione

$$f : \mathbb{N} \to \bigcup_{n\in\mathbb{N}} A_n \times \{n\}$$

[14] Ad esempio N2(2) in [9].

[15] Per l'iniezione non banale, si consideri la mappa $(n, 0) \mapsto 2n$, $(n, 1) \mapsto 2n + 1$ e si applichi Schröder-Bernstein.

[16] La dimostrazione formale che segue risulta un po' macchinosa, ma il concetto è semplice: se abbiamo una biezione da $\mathbb{N}$ in un'unione disgiunta di insiemi, allora abbiamo un buon ordine su quell'unione: il buon ordine indotto dall'ordine canonico di $\mathbb{N}$. Quindi posso utilizzare questo buon ordine per scegliere un elemento da ogni A_n.

allora potremmo definire $F \in \times_{n\in\mathbb{N}} A_n$ così:

$$F(n) = \pi_1\Big(f\big(\min\big\{f^{-1}[A_n \times \{n\}]\big\}\big)\Big)$$

dove π_1 è la proiezione sulla prima componente. Quindi $\times_{n\in\mathbb{N}} A_n$ sarebbe non vuoto, contraddizione.

□

Lo spiacevole risultato appena presentato fu descritto da Russel in termini di due sequenze (infinite): una formata da paia di calzini e l'altra formata da paia di scarpe. Le due sequenze rappresentano rispettivamente $(A_n)_{n\in\mathbb{N}}$ e $(B_n)_{n\in\mathbb{N}}$ della proposizione. In ogni paio, la scarpa destra e quella sinistra sono distinguibili una dall'altra, mentre ciò non avviene con le paia di calzini. Quindi, "*non possiamo scegliere un calzino da un numero infinito di paia, a meno che non disponiamo di una qualche* ***regola*** *per scegliere, e in questo caso non possiamo trovare nessuna regola.*", [10].

Il prossimo teorema mostra che possiamo incontrare situazioni scomode anche solo limitandoci a un numero finito di cardinali.

Definizione 2.2.4. Due numeri cardinali a e b si dicono *confrontabili* rispetto a $\leq$ (risp. rispetto a $\leq^*$) se $a \leq b$ o $b \leq a$ (risp. $a \leq^* b$ o $b \leq^* a$).

Proposizione 2.2.5. Può succedere che:

(1) Esistono cardinali a e b tali che $a \leq^* b$ e $a \not\leq b$.

(2) Esistono cardinali a e b tali che non sono confrontabili rispetto a $\leq$.

(3) Esistono cardinali a e b tali che non sono confrontabili rispetto a $\leq^*$.

Dimostrazione.

(1) Supponiamo di lavorare in un modello di ZF in cui esiste un insieme infinito X che è D-finito. Allora esiste un cardinale a tale che $\aleph_0 \leq^* a$ e $\aleph_0 \not\leq a$. Infatti, grazie Lemma 2.1.9, se $\mathcal{P}(X)$ è D-infinito basta prendere $a = |X|$. Se invece $\mathcal{P}(X)$ è D-finito, allora poniamo $a = |\,\mathcal{P}(X)|$. Anche in questo caso la richiesta è soddisfatta, dato che $\mathcal{P}(\mathcal{P}(X))$ è D-infinito per la Proposizione 2.1.11, e si conclude di nuovo per il Lemma 2.1.9.

(2) Sia X un insieme che non è bene ordinabile. Sia $\mathrm{Hrtg}(X)$ il suo numero di Hartogs. Allora $|\,\mathrm{Hrtg}(X)| \not\leq |X|$ per definizione. Ma vale anche $|X| \not\leq |\,\mathrm{Hrtg}(X)|$, perché altrimenti X sarebbe bene ordinabile, dato che $\mathrm{Hrtg}(X)$ è un ordinale.

(3) Si veda il prossimo teorema.

□

Teorema 2.2.6. Sono equivalenti:

(1) Presi due cardinali qualsiasi, questi sono confrontabili rispetto a $\leq$.

(2) Presi due cardinali qualsiasi, questi sono confrontabili rispetto a $\leq^*$.

(3) AC.

Dimostrazione.
(1) $\implies$ (2): Segue subito dal fatto (banale) che ogni funzione iniettiva ammette un'inversa sinistra.
(2) $\implies$ (3): Sia X un insieme. Allora, per qualsiasi insieme Y, $|Y| \leq^* |X|$ implica $|Y| \leq |\mathcal{P}(X)|$ [17]. Quindi necessariamente $|\operatorname{Hrtg}(\mathcal{P}(X))| \not\leq^* |X|$. Per ipotesi abbiamo $|X| \leq^* |\operatorname{Hrtg}(\mathcal{P}(X))|$, i.e. (per $X \neq \emptyset$) esiste $f : \operatorname{Hrtg}(\mathcal{P}(X)) \to X$ suriettiva. Sia $g : X \to \operatorname{Hrtg}(\mathcal{P}(X))$ definita da $g(x) = \min f^{-1}(x)$. Ovviamente g è iniettiva. Quindi X è bene ordinabile. Per arbitrarietà di X otteniamo AC.
(3) $\implies$ (1): Siano X e Y insiemi arbitrari. Per il Teorema 1.1.2, X e Y sono bene ordinabili. È un risultato ben noto che due qualsiasi insiemi bene ordinati sono isomorfi oppure uno è isomorfo a un segmento iniziale dell'altro[18]. Perciò $|X| = |Y|$ oppure $|X| \leq |Y|$ oppure $|Y| \leq |X|$. □

2.3 Ordini

In questa sezione trattiamo solamente un risultato, sufficiente però a mostrare come in assenza di AC anche gli ordini lineari possono verificare proprietà molto strane.

Definizione 2.3.1. Sia $(X, \leq)$ un insieme ordinato. Chiamiamo *successione decrescente* (risp. *crescente*) una successione $(x_n)_{n\in\mathbb{N}}$ in X tale che $x_{n+1} < x_n$ (risp. $x_n < x_{n+1}$) per ogni $n \in \mathbb{N}$.

Proposizione 2.3.2. I seguenti fatti possono essere validi in qualche insieme $(X, \leq)$ linearmente ordinato, persino prendendo $X \subseteq \mathbb{R}$:

(1) $(X, \leq)$ non contiene nessuna successione decrescente, ma non è un buon ordine.

(2) $(X, \leq)$ è infinito, ma non contiene successioni né crescenti né decrescenti.

[17] Se $s : X \to Y$ è suriettiva allora $i : Y \to \mathcal{P}(X)$, $y \mapsto s^{-1}(y)$ è iniettiva.
[18] Remark 4 in `http://terrytao.wordpress.com/2009/01/28/245b-notes-7-well-ordered-sets-ordinals-and-zorns-lemma-optional/`

(3) $(X, \leq)$ è non vuoto e non ha un elemento massimo, ma non contiene successioni crescenti.

Dimostrazione. Sia $X \subseteq \mathbb{R}$ infinito e D-finito[19]. Consideriamo su X l'ordine indotto dall'ordine standard di $\mathbb{R}$.

(1) e (2) Allora X non contiene nessuna sequenza crescente o decrescente, dato che questa sarebbe anche una funzione iniettiva $\mathbb{N} \to X$. Inoltre, X non è un buon ordine, perché altrimenti potremmo definire una successione crescente $(x_n)_{n\in\mathbb{N}}$ tramite ricorsione in questo modo:

$$x_n = \min(X \setminus \{x_m \mid m < n\}).$$

(3) Consideriamo lo stesso insieme X di prima. Se X non ammette massimo, allora grazie alla dimostrazione di (2) basta prendere come testimone X stesso. Se invece X ha un massimo, allora esiste $F \subseteq X$ finito tale che $Y = X \setminus F$ è infinito, D-finito e privo di massimo, dato che altrimenti potremmo definire una successione decrescente $(x_n)_{n\in\mathbb{N}}$ in X tramite ricorsione in questo modo:

$$x_n = \max(X \setminus \{x_m \mid m < n\}).$$

Quindi possiamo ripetere per Y la dimostrazione di (2) in modo esattamente uguale per provare che Y non contiene successioni crescenti. Quindi Y soddisfa la richiesta di (3).

□

2.4 Spazi vettoriali

Nelle sezioni precedenti abbiamo visto come l'Assioma di Scelta sia fondamentale per assicurare che alcune strutture matematiche (insiemi finiti, cardinali, ordini,...) si comportino in modo simile alla nostra intuizione. Finora però la nostra analisi si è concentrata principalmente su argomenti inerenti, o comunque vicini, alla Logica Matematica.

Lo scopo di questa sezione e della prossima sarà illustrare due celebri risultati che mostrano l'importanza di AC anche in altre aree della matematica. In particolare, ci occuperemo di Algebra Lineare e di Topologia.

Ricordiamo prima la definizione di base per uno spazio vettoriale.

Definizione 2.4.1. Sia F un campo e sia V uno spazio vettoriale su F. Sia $B \subseteq V$. Diciamo che B è una *base* per V se valgono entrambe le condizioni:

[19] Esistono modelli di ZF che contengono un tale insieme, ad esempio il modello di Cohen M1 in [9].

- Per ogni sottoinsieme finito $B_0 \subseteq B$, i vettori di B_0 sono linearmente indipendenti.
- Ogni elemento di V si può scrivere come combinazione lineare di un numero finito di vettori di B.

Si dimostra che tale scrittura è unica.

Nel prossimo teorema dimostreremo che AC è equivalente all'affermazione che ogni spazio vettoriale ha una base. In realtà formalmente mostreremo l'equivalenza con un principio apparentemente più debole: l'Assioma di Scelta Multipla (AMC):

Definizione 2.4.2 (AMC)**.** Per ogni famiglia $(X_i)_{i\in I}$ di insiemi non vuoti e mutualmente disgiunti esiste una famiglia $(F_i)_{i\in I}$ di insiemi finiti non vuoti tali che $F_i \subseteq X_i$ per ogni $i \in I$.

È immediato che AC $\Rightarrow$ AMC. In realtà vale anche l'implicazione opposta. La dimostrazione di questo fatto non è immediata e utilizza alcuni concetti piuttosto tecnici di teoria degli insiemi (e.g. la gerarchia di von Neumann). Decidiamo pertanto di non riportarla in questo elaborato, rimandando il lettore interessato al Teorema 2.4 di pag. 11 in [1][20].

Teorema 2.4.3. Sono equivalenti:

(1) Ogni spazio vettoriale ha una base.

(2) AC.

Dimostrazione.
(1) $\implies$ (2): Vogliamo mostrare che vale AMC. Sia allora $(X_i)_{i\in I}$ una famiglia di insiemi non vuoti e mutualmente disgiunti. Sia k un campo arbitrario e sia $k(X)$ il campo delle funzioni razionali su k nelle variabili $x \in X = \bigcup_{i\in I} X_i$. Consideriamo i monomi di $k(X)$, ovvero gli elementi della forma $p = c \cdot x_1^{n_1} \cdot x_2^{n_2} \cdot \ldots \cdot x_m^{n_m}$. Per ogni $i \in I$, se p è un monomio definiamo l'i-grado di p come

$$d_i(p) = \sum_{x_k \in X_i} n_k.$$

Dato un elemento generico α di $k(X)$, $\alpha = \frac{p_1+\ldots+p_n}{q_1+\ldots+q_m}$ con p_k e q_k monomi, diremo che α è i-omogeneo di grado d se tutti i q_k hanno lo stesso i-grado, diciamo d_1, e tutti i p_k hanno lo stesso i-grado $d_2 = d_1 + d$. Allora

$$K = \{a \in k(X) \mid a \text{ è } i\text{-omogeneo di grado 0 per ogni } i \in I\}$$

[20]Per una dimostrazione più completa si veda `http://caicedoteaching.wordpress.com/2009/11/11/502-equivalents-of-the-axiom-of-choice/`.

è un sottocampo di $k(X)$. Quindi $k(X)$ è uno spazio vettoriale su K. Per ipotesi, $k(X)$ ha una base B. Per ogni $x \in X$ il monomio x si scrive in modo unico come

$$x = \sum_{b \in B(x)} a_b(x) \cdot b,$$

dove $B(x)$ è un sottoinsieme finito di B e $a_b(x) \in K \setminus \{0\}$.

Siano x e y elementi dello stesso X_i. Allora

$$\sum_{b \in B(y)} a_b(y) \cdot b = y = \frac{y}{x} \cdot x = \sum_{b' \in B(x)} \frac{y}{x} \cdot a_{b'}(x) \cdot b'.$$

Poiché $\frac{y}{x} \in K$, questo implica $B(x) = B(y)$ e $\frac{a_b(y)}{y} = \frac{a_b(x)}{x}$ per ogni $b \in B(x)$. Perciò gli insiemi $B(x)$ e gli elementi $\frac{a_b(x)}{x}$ dipendono solo da i e non dal particolare $x \in X_i$. Scriviamo allora $B_i = B(x)$ e $\alpha(b, i) = \frac{a_b(x)}{x}$. Poiché gli $a_b(x)$ sono i-omogenei di grado 0, gli $\alpha(b, i)$ sono i-omogenei di grado -1. Quindi se scriviamo $\alpha(b, i)$ come quoziente di polinomi in forma ridotta, al denominatore deve necessariamente comparire qualche $x \in X_i$. Chiamiamo F_i l'insieme di tutti gli $x \in X_i$ che compaiono nel denominatore di $\alpha(b, i)$ nella sua forma ridotta per qualche $b \in B_i$. Per ogni $i \in I$, l'insieme F_i è un sottoinsieme finito e non vuoto di X_i. La dimostrazione è conclusa.
(2) $\Longrightarrow$ (1): La dimostrazione è ben nota e usa il Lemma di Zorn. □

2.5 Spazi compatti

Il teorema di Tychonoff (i.e. *Il prodotto di compatti è compatto*) viene comunemente considerato uno dei risultati più importanti di Topologia generale.

> *The theorem just proved* [the Tychonoff Theorem] *can lay good claim to being the most important theorem in general (nongeometric) topology.*
>
> (S. Willard, [20])

Osservando le dimostrazioni più comuni di questo teorema si nota che esse fanno uso di AC. Ma è davvero necessario? La risposta è affermativa.

Definizione 2.5.1. Sia $\mathcal{A} = \{A_i \mid i \in I\}$ una famiglia di insiemi. Diciamo che $\mathcal{A}$ ha la *proprietà dell'intersezione finita* se per ogni sottoinsieme finito $I_0 \subseteq I$ vale

$$\bigcap_{i \in I_0} A_i \neq \emptyset.$$

Proposizione 2.5.2. Uno spazio topologico è compatto se e solo se ogni famiglia di chiusi che ha la proprietà dell'intersezione finita ha intersezione non vuota.

Dimostrazione. La dimostrazione è semplice e ben nota[21]. □

Definizione 2.5.3. Sia $(X_i, \tau_i)_{i\in I}$ una famiglia di spazi topologici. Lo *spazio topologico prodotto* degli (X_i, τ_i) è (X, τ) dove $X = \times_{i\in I} X_i$ e τ è la topologia meno fine che rende continue le proiezioni $\pi_i : X \to X_i$.

Teorema 2.5.4. Sono equivalenti:

(1) Il teorema di Tychonoff: Il prodotto di spazi compatti è compatto.

(2) AC.

Dimostrazione.
(1) $\implies$ (2): Sia $(X_i)_{i\in I}$ una famiglia di insiemi non vuoti e sia ∞ un elemento che non appartiene a nessun X_i. Definiamo degli spazi topologici (Y_i, τ_i) con $Y_i = X_i \cup \{\infty\}$ e $\tau_i = \big\{\emptyset, Y_i, \{\infty\}\big\}$. Gli (Y_i, τ_i) sono banalmente compatti. Per ipotesi, lo spazio topologico $P = \prod_{i\in I}(Y_i, \tau_i)$ è compatto. Sia $\pi_i : P \to Y_i$ la proiezione sulla i-esima componente, che è continua per definizione di topologia prodotto. Inoltre ovviamente $X_i = Y_i \setminus \{\infty\}$ è chiuso in Y_i. Allora, per ogni $i \in I$ l'insieme $A_i = \pi_i^{-1}(X_i)$ è un sottoinsieme chiuso e non-vuoto di P. La famiglia $\mathfrak{U} = \{A_i \mid i \in I\}$ ha la proprietà dell'intersezione finita. Infatti, se $I_0 = \{i_1, ..., i_n\} \subseteq I$, allora scegliamo $x_{i_1} \in X_{i_1}, x_{i_2} \in X_{i_2}, ..., x_{i_n} \in X_{i_n}$. Definiamo poi $f : I \to \bigcup_{i\in I} Y_i$ così:

$$f(i) = \begin{cases} x_i & \text{se } i \in I_0, \\ \infty & \text{altrimenti.} \end{cases}$$

È chiaro che $f \in P$ e che $\pi_i(f) \in X_i$ per ogni $i \in I_0$, ovvero $f \in \bigcap_{i\in I_0} A_i$.

Quindi per compattezza di P abbiamo $\bigcap_{i\in I} A_i \neq \emptyset$. Poiché $\bigcap_{i\in I} A_i = \times_{i\in I} X_i$, per arbitrarietà di $(X_i)_{i\in I}$ segue AC.
(2) $\implies$ (1): Si veda qualsiasi libro di topologia generale. □

[21] Si veda eventualmente
`http://planetmath.org/aspaceiscompactiffanyfamilyofclosedsetshavingfiphasnonemptyintersection`

Capitolo 3

Disastri con Scelta

Nel capitolo precedente abbiamo presentato una serie di risultati che mostrano come rinunciare ad AC porti a situazioni molto spiacevoli. Ma allora qual è il motivo di tutta questa attenzione attorno all'Assioma di Scelta? Sappiamo che, supponendo ZF consistente, ZFC è consistente. Quindi da un punto di vista puramente formale, aggiungere AC agli altri assiomi di ZF non porta a nessuna contraddizione. Ma allora cosa ci trattiene dal lavorare senza alcuna preoccupazione in ZFC?

NOTA: In questa sezione lavoriamo, salvo indicazione contraria, in ZFC.

3.1 Decomposizioni paradossali

L'intuizione è una guida importante per i matematici. Purtroppo, l'intuizione non sempre è affidabile. Esistono risultati matematici che sono controintuitivi. E nella maggior parte di essi, il principale "colpevole" è sempre lo stesso: l'Assioma di Scelta. Ovvero: molti risultati paradossali sono dimostrabili in ZFC, ma non in ZF. Quello forse più stupefacente (e preoccupante) di tutti è il famoso *Paradosso di Banach-Tarski*, che stabilisce l'esistenza di decomposizioni davvero strane della palla unitaria e non solo.

In particolare, il Paradosso di Banach-Tarski dimostra (con una buona dose di spettacolarità) che in ZFC non esiste una misura su $\mathbb{R}^3$ che sia allo stesso tempo finitamente additiva e invariante per isometrie, e che misuri tutti i sottoinsiemi dello spazio. Purtroppo, almeno le prime due richieste sono irrinunciabili se vogliamo modellizzare la nostra idea intuitiva di *volume*, dato che la nostra esperienza ci dice che spostando uno stesso oggetto da una posizione ad un'altra, le sue dimensioni non cambiano.

In realtà lo stesso risultato era già stato ottenuto da Hausdorff, ma, come vedremo, in modo meno elegante.

La dimostrazione completa e dettagliata di questi risultati è composta di molti lemmi estremamente tecnici, la cui trattazione è al di fuori degli scopi di questo lavoro. Vogliamo però descrivere le idee principali che stanno alla base di questi paradossi così affascinanti e così importanti, anche storicamente. Per i dettagli tecnici rimandiamo a [11].

Definizione 3.1.1. Sia (X, d) uno spazio metrico. Una *isometria* di X è una funzione $f : X \to X$ biettiva tale che per ogni $x, y \in X$ vale $d(f(x), f(y)) = d(x, y)$. Due sottoinsiemi $A, B \subseteq X$ si dicono *congruenti* e si scrive $A \approx B$ se esiste un'isometria f di X tale che $f[A] = B$.

Ricordiamo che R^n è uno spazio metrico con la distanza indotta dal prodotto scalare standard.

Definizione 3.1.2. Per ogni $n \in \mathbb{N}^+$, una *misura $n-$dimensionale* è una funzione $\mu_n : \mathcal{P}_b(\mathbb{R}^n) \to \mathbb{R}^+$, definita sull'insieme $\mathcal{P}_b(\mathbb{R}^n)$ dei sottoinsiemi limitati di $\mathbb{R}^n$, che soddisfa le seguenti condizioni:

(M1) μ_n è additiva, ovvero $\mu(A \cup B) = \mu(A) + \mu(B)$ per ogni $A, B \in \mathcal{P}_b(\mathbb{R}^n)$ disgiunti.

(M2) μ_n è invariante, ovvero $A \approx B$ implica $\mu_n(A) = \mu_n(B)$.

(M3) $\mu_n([0, 1]^n) = 1$.

3.1.1 Decomposizione paradossale della Sfera unitaria

Hausdorff fu il primo a dimostrare che non esiste nessuna misura $3-$dimensionale (e di conseguenza neppure $n-$dimensionale per ogni $n \geq 3$ [1]). Ottenne questo risultato esibendo una decomposizione paradossale della sfera:

3.1.3. Teorema di Hausdorff sulla decomposizione della sfera unitaria[2] Esiste una partizione $\{A, B, C, D\}$ della sfera unitaria $\mathcal{S}^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$ tale che:

1. $A \approx B \approx C$.
2. $A \approx (B \cup C)$.

[1] Se per assurdo μ_n fosse una misura $n-$dimensionale con $n \geq 3$, allora $\mu_3 : S \mapsto \mu_n(S \times [0, 1]^{n-3})$ sarebbe una misura $3-$dimensionale.

[2] [12]

3. D è numerabile.

Più avanti daremo un'idea della dimostrazione del teorema enunciato sopra. Prima però discutiamo alcune sue conseguenze.

Corollario 3.1.4. Non esiste nessuna funzione $\mu : \mathcal{P}_b(\mathcal{S}^2) \to \mathbb{R}^+$ che soddisfa (M1), (M2) e (M3') $\mu(\mathcal{S}^2) > 0$.

Dimostrazione. Supponiamo che esista una funzione μ che soddisfa (M1), (M2) e (M3'). La numerabilità di D implica che esiste un'isometria f della sfera $\mathcal{S}^2$ (precisamente, una rotazione) tale che D e $f[D]$ sono disgiunti[3]. Allora $D_1 = (D \cup f[D])$ è un sottoinsieme numerabile di $\mathcal{S}^2$ tale che $\mu(D_1) = 2\mu(D)$. Ripetendo lo stesso processo si ottiene, per ogni $n \in \mathbb{N}^+$, un sottoinsieme numerabile D_n di $\mathcal{S}^2$ tale che $\mu(D_n) = 2^n\mu(D)$. Poiché $\mu(D_n) \leq \mu(\mathcal{S}^2)$ per ogni n (la monotonia di μ è conseguenza immediata dell'additività), questo implica $\mu(D) = 0$. Quindi $\mu(\mathcal{S}^2) = \mu(A) + \mu(B) + \mu(C) = 3\mu(A)$. Ma vale anche $\mu(\mathcal{S}^2) = \mu(B \cup C) + \mu(B) + \mu(C) = 4\mu(A)$. Quindi $\mu(A) = 0$, e perciò $\mu(\mathcal{S}^2) = 0$, contraddizione. □

Corollario 3.1.5. Non esiste nessuna misura 3−dimensionale.

Dimostrazione. Se μ_3 fosse una misura 3−dimensionale, allora la funzione $\mu : \mathcal{P}_b(\mathcal{S}^2) \to \mathbb{R}^+$ definita da

$$\mu(A) = \mu_3\big(\{(\lambda x, \lambda y, \lambda z) \mid (x, y, z) \in A \text{ e } 0 < \lambda \leq 1\}\big)$$

soddisferebbe (M1), (M2) e (M3'), contraddicendo il corollario appena mostrato. □

Riguardando al Teorema di Hausdorff 3.1.3, osserviamo che la presenza dell'insieme numerabile D riduce in qualche modo la sua eleganza. Esiste un risultato più "raffinato"? Sierpiński[4] ha dimostrato che esistono partizioni

$$\mathcal{P}_1 = \{A_1, ..., A_6, B_1, ..., B_4\},$$

$$\mathcal{P}_2 = \{C_1, ..., C_6\},$$

$$\mathcal{P}_3 = \{D_1, ..., D_4\}$$

di $\mathcal{S}^2$ tali che

1. $A_i \approx C_i$ per $i = 1, ..., 6$.

[3] I punti di una sfera sono banalmente $2^{\aleph_0}$. Quindi esiste un asse di rotazione r che non interseca nessun punto di D. Sia f una rotazione di angolo θ attorno a r. Se per assurdo si avesse che per ogni $\theta \in (0; \pi)$ esistono $d_1, d_2 \in D$ tali che $r(d_1) = d_2$, allora la funzione $f : (0; \pi) \to D \times D$, $\theta \mapsto (d_1, d_2)$ sarebbe ovviamente iniettiva, contraddizione (ogni intervallo non banale di $\mathbb{R}$ è equipotente a $\mathbb{R}$). Si noti che per definire f abbiamo usato AC.

[4] [13]

2. $B_i \approx D_i$ per $i = 1, ..., 4$.

Sierpiński riuscì quindi a evitare l'uso di un insieme numerabile, ma utilizzò comunque un numero di pezzi maggiore rispetto a quelli davvero necessari, come mostrato da Robinson:

3.1.6. Teorema di Robinson sulla decomposizione della sfera[5]
Esiste una partizione $\{A_1, A_2, B_1, B_2\}$ della sfera unitaria, composta di pezzi connessi e localmente connessi, tale che

1. $A_1 \approx A_2 \approx A_1 \cup A_2$ e

2. $B_1 \approx B_2 \approx B_1 \cup B_2$.

Questo è in qualche modo il migliore (o il peggiore?) risultato possibile. Per dirlo con le parole dello stesso Robinson:

> *Thus we may cut $\mathcal{S}^2$ into four pieces, and reassemble them in pairs to form two copies of $\mathcal{S}^2$. We cannot use fewer than four pieces, since we cannot form a copy $\mathcal{S}^2$ out of a single piece which is not all of $\mathcal{S}^2$. Thus for the surface problem, the minimum number of pieces in which to cut $\mathcal{S}^2$ is four.* (Robinson, [14])

3.1.2 Gruppi indisciplinati

Dopo che Banach e Tarski[6] ebbero migliorato la costruzione di Hausdorff, ottenendo una decomposizioni di enti 3−dimensionali più semplice e impressionante, von Neumann[7] mostrò che, sotto AC, la struttura del gruppo delle isometrie di $\mathbb{R}^3$ è responsabile dell'esistenza di queste decomposizioni paradossali, e di conseguenza anche della non esistenza di misure 3−dimensionali. Tale gruppo contiene un gruppo libero con due generatori, e questo fatto è la causa di tutti i guai:

> *"Apparentemente la natura dello spazio euclideo cambia bruscamente quando raggiunge la dimensione 3: per $n < 3$, esso ammette un concetto generale di misura, per $n \geq 3$ non è più così!*
>
> *Mostrare ciò, ovvero che la spiegazione più profonda di questo strano fenomeno è una peculiarità riguardante la teoria dei gruppi e specifica del gruppo delle isometrie n−dimensionali, è il fine principale di questo articolo.*

[5] [14]
[6] [15]
[7] [16]

...
Il brusco cambiamento nella natura dello spazio euclideo quando raggiunge e sorpassa la dimensione 3 *è semplicemente causato dal fatto che il gruppo* O_n *delle isometrie — l'unico che è stato preso in considerazione finora — è "risolvibile" per* $n = 1, 2$*, ma contiene un gruppo libero con due generatori* σ, τ *per* $n = 3, 4, ...$*"* (von Neumann, [16])

Definizione 3.1.7.

1. Il *gruppo libero* F_2 *su due generatori* a e b è l'insieme di tutte le parole $x_1x_2...x_n$ formate da lettere a, b, a^{-1}, b^{-1} tali che a e a^{-1} non sono mai adiacenti, come anche b e b^{-1}. L'operazione considerata è la seguente: se $w = x_1...x_n$ e $v = y_1...y_m$ sono elementi di F_2, allora $w \cdot v$ è ottenuto con i seguenti passaggi:
   Passo 1: Si concatenano w e v, ottenendo $x_1...x_ny_1...y_m$;
   Passo 2: Si rimuovono x_n e y_1 se e solo se $\{x_n, y_1\} = \{a, a^{-1}\}$ oppure $\{x_n, y_1\} = \{b, b^{-1}\}$;
   Passo 3: Si ripete il passo 2 finché non si ottiene un elemento di F_2.
   L'elemento neutro è la *parola vuota*, ovvero la parola che non contiene nessuna lettera, e viene indicata con Λ.

2. $x \cdot Y = \{x \cdot y \mid y \in Y\}$ per $x \in F_2$ e $Y \subseteq F_2$.

3. Due sottoinsiemi $X, Y \subseteq F_2$ si dicono *congruenti*, in simboli $X \approx Y$, se esiste qualche $z \in F_2$ tale che $Y = z \cdot X$.

Teorema 3.1.8. Esiste una partizione $\{A, B, C, D\}$ del gruppo libero F_2 tale che:

1. $A \approx (A \cup C \cup D)$.

2. $C \approx (A \cup B \cup C)$.

Dimostrazione. Per illustrare allo stesso tempo l'idea intuitiva che sta dietro alla dimostrazione e la difficoltà tecnica che è necessario superare, presentiamo prima un argomento che non funziona per un pelo.

Tentativo: Definiamo
$A = \{x_1...x_n \in F_2 \mid x_1 = a\}$,
$B = \{x_1...x_n \in F_2 \mid x_1 = a^{-1}\}$,
$C = \{x_1...x_n \in F_2 \mid x_1 = b\}$,
$D = \{x_1...x_n \in F_2 \mid x_1 = b^{-1}\}$.

Osserviamo che $\{A, B, C, D\}$ è quasi una partizione di F_2. Manca solo la parola vuota Λ. Inoltre:
$A \approx a^{-1} \cdot A = A \cup C \cup D \cup \{\Lambda\}$,

$C \approx b^{-1} \cdot C = A \cup B \cup C \cup \{\Lambda\}$.

Quindi, la parola vuota impedisce alla dimostrazione di essere del tutto corretta. Ecco allora una versione leggermente meno simmetrica, e quindi meno elegante, ma corretta:

Dimostrazione: Definiamo A e B come prima, ma ridefiniamo C e D così:
$C = \{x_1...x_n \in F_2 \mid x_1 = b\} \cup \{b^{-n} \mid n \in \mathbb{N}\}$,
$D = F_2 \setminus (A \cup B \cup C) = \{x_1...x_n \in F_2 \mid x_1 = b^{-1}\} \setminus \{b^{-n} \mid n \in \mathbb{N}\}$,
dove $b^0 = \Lambda$.
Allora $\{A, B, C, D\}$ è una partizione di F_2, e:
$A \approx a^{-1} \cdot A = A \cup C \cup D$,
$C \approx b^{-1} \cdot C = A \cup B \cup C$. □

Definizione 3.1.9. Sia X un insieme e sia G un gruppo che agisce su X. Diciamo che $x \in X$ è un *punto fisso* per $g \in G$ se $g(x) = x$. Diciamo che G agisce *senza punti fissi* se l'unico elemento di G che ha un punto fisso è l'elemento neutro.
Se $A, B \subseteq X$ ed esiste $g \in G$ tale che $g[A] = B$, allora scriviamo $A \approx B$.

I gruppi "indisciplinati" che agiscono senza punti fissi su un insieme X portano a decomposizioni paradossali di X, come mostra il seguente:

Teorema 3.1.10. Se F_2 agisce su X senza punti fissi, allora esiste una partizione $\{A^*, B^*, C^*, D^*\}$ di X tale che

1. $A^* \approx (A^* \cup C^* \cup D^*)$.
2. $C^* \approx (A^* \cup B^* \cup C^*)$.

Dimostrazione. Sia $\{A, B, C, D\}$ una partizione di F_2 tale che $A \approx (A \cup C \cup D)$ e $C \approx (A \cup B \cup C)$. Per ogni $x \in X$, sia $\text{orb}(x) = \{g(x) \mid g \in F_2\}$ l'orbita di x. Allora $\{\text{orb}(x) \mid x \in X\}$ è una partizione di X. Grazie ad AC esiste $S \subseteq X$ che contiene esattamente un elemento di ogni orbita. Definiamo

$$A^* = \{g(x) \mid g \in A \text{ e } x \in S\}$$

e analogamente B^*, C^* e D^*. Siccome F_2 agisce su X senza punti fissi, l'insieme $\{A^*, B^*, C^*, D^*\}$ è una partizione di X. Ovviamente valgono:

$$A^* \approx (A^* \cup C^* \cup D^*) \text{ e } C^* \approx (A^* \cup B^* \cup C^*).$$

□

3.1.3 Decomposizione paradossale della Palla unitaria

Il motivo per cui abbiamo parlato delle strane proprietà dei gruppi liberi che agiscono senza punti fissi è il seguente: il gruppo delle isometrie di $\mathbb{R}^3$ contiene un sottogruppo che è isomorfo a F_2 e agisce sulla palla unitaria $\mathcal{B}_3 = \{(x, y, z) \in R^3 \mid x^2 + y^2 + z^2 \leq 1\}$.

Se questa azione fosse senza punti fissi, allora il Teorema 3.1.10 ci procurerebbe immediatamente una decomposizione paradossale di $\mathcal{B}_3$ in quattro pezzi. Ma le rotazioni *hanno* punti fissi (fortunatamente, non troppi), e questo causa delle complicazioni. E infatti Robinson ha mostrato che una tale decomposizione in soli quattro pezzi non esiste. Nonostante questo però, Banach e Tarski furono in grado di dimostrare il seguente:

Teorema 3.1.11. Esistono partizioni

$$\mathcal{P}_1 = \{A_1, ..., A_n, B_1, ..., B_m\},$$

$$\mathcal{P}_2 = \{C_1, ..., C_n\},$$

$$\mathcal{P}_3 = \{D_1, ..., D_m\}$$

di $\mathcal{B}_3$ tali che

1. $A_i \approx C_i$ per $i = 1, ..., n$.
2. $B_i \approx D_i$ per $i = 1, ..., m$.

Quanti pezzi $n + m$ sono necessari per "duplicare" una palla?

- Stromberg mostrò che $40 = 24 + 16$ sono sufficienti,
- Bruckner e Ceder ne usarono $30 = 18 + 12$,
- von Neumann ne usò $9 = 5 + 4$,
- Sierpiński ne usò $8 = 5 + 3 = 6 + 2$,
- Robinson[8] diede la risposta definitiva, ovvero $5 = 3 + 2$:

3.1.12. Teorema di Robinson sulla decomposizione della palla unitaria Esistono partizioni

$$\mathcal{P}_1 = \{A_1, A_2, A_3, B_1, B_2\},$$

$$\mathcal{P}_2 = \{C_1, C_2, C_3\},$$

[8] [14]

$$\mathcal{P}_3 = \{D_1, D_2\}$$

di $\mathcal{B}_3$ tali che

1. $A_i \approx C_i$ per $i = 1, 2, 3$.
2. $B_i \approx D_i$ per $i = 1, 2$.

Inoltre, ogni pezzo è connesso e localmente connesso.

Come già accennato, Robinson mostrò anche che quattro pezzi non sono sufficienti.

Terminiamo con una descrizione molto riassuntiva della dimostrazione sulla decomposizione della sfera.

3.1.13. Sketch di dimostrazione del Teorema di Hausdorff
Hausdorff, nella sua dimostrazione del Teorema 3.1.3, non fece uso di un sottogruppo libero del gruppo delle isometrie di $\mathcal{S}^2$. Ne usò invece uno "quasi" libero, mostrando che esistono rotazioni α e β di $\mathcal{S}^2$ tali che $\alpha^2 = \mathrm{id} = \beta^3$ sono le uniche relazioni del gruppo G generato da $\{\alpha, \beta\}$. Ogni elemento $g \in G$ ha esattamente due punti fissi. L'unione di questi insiemi di punti fissi è proprio l'insieme numerabile D dell'enunciato. Hausdorff prosegue poi costruendo accuratamente una partizione $\{A, B, C\}$ di G tale che $\beta A = B$, $\beta^2 A = C$ e $\alpha A = B \cup C$. Se X è un insieme ottenuto selezionando esattamente un elemento dall'orbita di ogni punto $x \in \mathcal{S}^2 \setminus D$, allora la partizione $\{A \cdot X, B \cdot X, C \cdot X\}$ di $\mathcal{S}^2 \setminus D$ ha le proprietà richieste.

3.1.4 Il paradosso di Banach-Tarski

Grazie ai risultati della sezione precedente, qualsiasi palla $3-$dimensionale può essere "duplicata". Segue facilmente che per ogni sottoinsieme limitato A di $\mathbb{R}^3$ e per ogni palla $\mathcal{B}$ di $\mathbb{R}^3$ esiste una partizione $\{A_1, ..., A_n\}$ di A e una partizione $\{B_1, ..., B_n\}$ di un qualche sottoinsieme di $\mathcal{B}$ tali che $A_i \approx B_i$ per ogni $i = 1, ..., n$ [9]. Quindi per ogni $A, B \subseteq \mathbb{R}^3$ che sono limitati e che contengono a loro volta una palla ciascuno, è possibile decomporre ognuno in un numero finito di pezzi e "riassemblare" questi pezzi per formare un sottoinsieme dell'altro.

Il paradosso di Banach-Tarski afferma ancora di più. Diamo prima una definizione:

[9] Suggerimento: si inizi osservando che possiamo "moltiplicare" ogni palla in un numero finito arbitrario di palle uguali. In particolare, poiché A è limitato, esiste una quantità finita di palle che lo ricoprono.

Definizione 3.1.14. Due sottoinsiemi A e B di $\mathbb{R}^3$ si dicono *equidecomponibili*, in simboli $A \sim_e B$, se esistono partizioni $\{A_1, ..., A_n\}$ di A e $\{B_1, ..., B_n\}$ di B tali che $A_i \approx B_i$ per $i = 1, ..., n$.

3.1.15. Paradosso di Banach-Tarski[10] Ogni due sottoinsiemi limitati A e B di $\mathbb{R}^3$ che contengono ognuno una palla, sono equidecomponibili.

> *It certainly does seem to be folly to claim that a billiard ball can be chopped into pieces which can be put back together to form a life-size statue of Banach.* (K. Stromberg, [22])

Dimostrazione. Per le osservazioni appena fatte, A e B sono equidecomponibili ognuno con un qualche sottoinsieme dell'altro. Perciò il risultato segue immediatamente dal prossimo teorema.

Teorema 3.1.16. [11] Se due sottoinsiemi A e B di $\mathbb{R}^3$ sono ognuno equidecomponibile in qualche sottoinsieme dell'altro, allora A e B sono equidecomponibili.

Dimostrazione. Sia $\{A_1, ..., A_n\}$ una partizione di A e sia $\{B_1, ..., B_n\}$ una partizione di un sottoinsieme B' di B tale che $A_i \approx B_i$ per ogni i. Allora per ogni $i = 1, ..., n$ esiste un'isometria $f_i : A \to B_i$. Quindi la mappa $f : A \to B'$ definita da $f(a) = f_i(a)$ per $a \in A_i$ è una biezione che soddisfa:

(A) $C \sim_e f[C]$ per ogni $C \subseteq A$.

Analogamente, esiste una biezione $g : B \to A'$ con $A' \subseteq A$ che soddisfa la condizione

(B) $D \sim_e g[D]$ per ogni $D \subseteq B$.

Definiamo per ricorsione una sequenza $(C_n)_{n\in\mathbb{N}}$ di sottoinsiemi C_n di A così:

$$\begin{cases} C_0 & = A \setminus A' \\ C_{n+1} & = g[f[C_n]]. \end{cases}$$

Consideriamo $C = \bigcup_{n\in\mathbb{N}} C_n$. Si verifica facilmente che $A\setminus C = g[B\setminus f[C]]$. Allora la condizione (B) implica $A\setminus C \sim_e B\setminus f[C]$. Poiché (A) implica $C \sim_e f[C]$, segue che $A = (A \setminus C) \cup C \sim_e (B \setminus f[C]) \cup f[C] = B$. □

[10] [15]

[11] [17]. Si osservi che la dimostrazione di questo teorema non fa uso di AC.

3.1.5 Di chi è la colpa

Come abbiamo visto in tutta questa sezione, in ZFC si può dimostrare l'esistenza già in $\mathbb{R}^3$ di decomposizioni geometriche che sono controintuitive e obiettivamente piuttosto fastidiose.

È lecito chiedersi allora chi sia il reale colpevole di tutto questo. È davvero AC? La risposta è: sì.

Infatti, la misura di Lebesgue in $\mathbb{R}^3$ è additiva, invariante e tale che il cubo unitario ha misura 1. Quindi i paradossi presentati implicano che esistono sottoinsiemi limitati di $\mathbb{R}^3$ che non sono misurabili. Si dimostra però che esistono modelli[12] di ZF in cui tutti i sottoinsiemi limitati di $\mathbb{R}^3$ sono misurabili secondo Lebesgue. Perciò il responsabile è davvero AC.

[12] Ad esempio M38 in [9].

Capitolo 4

Assioma delle Scelte Dipendenti

Nel capitolo precedente abbiamo visto diversi problemi che si incontrano assumendo AC. Per questi ed altri motivi, alcuni matematici non accettano l'Assioma di Scelta. Non necessariamente però rifiutano anche forme più deboli di "scelta".

Uno dei modi naturali per indebolire AC è ridurre la taglia massima dell'insieme di indici per il quale è valido. Un esempio degno di nota[1] è CC.

Definizione 4.0.17. CC (Countable Choice), l'Assioma delle Scelte Numerabili, afferma che per ogni successione $(X_n)_{n\in N}$ di insiemi non vuoti, il prodotto cartesiano generalizzato $\times_{n\in\mathbb{N}} X_n$ è non vuoto.

Osservazione 4.0.18. Si osservi che nella nostra dimostrazione della Proposizione 1.2.1 è sufficiente disporre di CC. Ovvero, ZF +CC dimostra che unione numerabile di insiemi numerabili è numerabile.

Strettamente correlato a CC è DC:

Definizione 4.0.19. DC, l'Assioma delle Scelte Dipendenti, afferma che per ogni coppia (X, ϱ) dove X è un insieme non vuoto e ϱ è una relazione su X tale che

$$\text{per ogni } x \in X \text{ esiste } y \in X \text{ tale che } x \varrho y$$

esiste una successione $(x_n)_{n\in\mathbb{N}}$ in X tale che $x_n \varrho x_{n+1}$ per ogni $n \in \mathbb{N}$.

Proposizione 4.0.20.

1. AC $\Rightarrow$ DC.
2. DC $\Rightarrow$ CC.

Dimostrazione. 1. Sia (X, ϱ) come in DC. Allora, per ogni $x \in X$ l'insieme $S_x = \{y \in X \mid x \varrho y\}$ è non vuoto. Quindi, per AC, esiste un elemento $(s_x)_{x\in X} \in \times_{x\in X} S_x$. Scegliamo arbitrariamente $x_0 \in X$ e definiamo per ricorsione la sequenza $(x_n)_{n\in\mathbb{N}}$ data da $x_{n+1} := s_{x_n}$. Allora $(x_n)_{n\in\mathbb{N}}$ ha la proprietà richiesta.

[1] Si confronti la prossima definizione con la citazione di E. Borel a pagina 15.

2. Sia $(A_n)_{n\in\mathbb{N}}$ una successione di insiemi non vuoti. Definiamo

$$A = \biguplus_{n\in\mathbb{N}} A_n$$

dove $\uplus$ indica l'unione disgiunta. Sia ϱ la relazione su A definita da

$$(x,m)\ \varrho\ (y,n) \iff n = m+1$$

Osserviamo che

$$\text{per ogni } a \in A \text{ esiste } b \in A \text{ tale che } a\varrho b$$

Per DC esiste una successione $(x_n)_{n\in\mathbb{N}}$ in A tale che $x_n \varrho x_{n+1}$ per ogni $n \in \mathbb{N}$. Se scriviamo $x_n = (a_n, N_n)$ per ogni $n \in \mathbb{N}$, dalla definizione di ϱ segue che $N_{n+1} = N_n + 1$. Una semplice induzione mostra che $N_n = N + n$ per qualche $N \in \mathbb{N}$. Perciò $x_n \in A_{n+N}$ per ogni $n \in \mathbb{N}$. Se fosse vero che $N = 0$ avremmo finito, ma questo non è necessariamente vero. Il resto della dimostrazione risolve questo problema.

Il prodotto cartesiano $A_0 \times ... \times A_{N-1}$ è non vuoto. Quindi esiste una sequenza finita $y_0, ..., y_{N-1}$ con $y_i \in A_i$ per ogni $i < N$. Definiamo allora $y_n := x_{n-N}$ per ogni $n \geq N$. Allora $y_n \in A_n$ per ogni $n \in \mathbb{N}$, ovvero $(y_n)_{n\in\mathbb{N}} \in \times_{n\in\mathbb{N}} A_n$. □

Nessuna delle implicazioni dell'ultima proposizione è invertibile. Infatti esistono modelli che soddisfano DC ma non AC (ad esempio M38 in [9]) e modelli che soddisfano CC ma non DC (ad esempio N38 in [9]).

DC e Löwenheim-Skolem

Lo scopo di questa sezione è dimostrare un risultato poco conosciuto: DC è equivalente al Teorema di Löwenheim-Skolem all'ingiù. Riteniamo questa equivalenza davvero interessante, in quanto mette in (forte) relazione due principi molto importanti per la Logica Matematica.

La dimostrazione che seguiremo quasi fedelmente si può trovare nell'articolo di marzo 2014 di Asaf Karagila[2]. Nello stesso articolo, Karagila afferma che Christian Espíndola aveva già provato questo risultato, estendendolo. Inoltre, nelle sue note (non ancora pubblicate), dichiara che l'equivalenza era già nota, seppur non largamente, e appare in un libro di G. Boolos.

[2] [18]

Notazione e nozioni di base In questa sezione daremo per scontata una minima famigliarità con i concetti della logica del prim'ordine. Procediamo tuttavia con una rapida rassegna dei simboli usati.

Se $\mathcal{L}$ è un linguaggio, denotiamo le $\mathcal{L}$-strutture con lettere gotiche $\mathfrak{M}, \mathfrak{N}, \mathfrak{U}, ...$ e i loro universi con le rispettive lettere $M, N, U, ...$

Per facilitare la lettura, scriviamo $\vec{a} \subseteq A$ per indicare che $\vec{a}$ è una tupla finita in A di lunghezza arbitraria.

Diciamo che $\mathfrak{U}$ è una *sottostruttura elementare* di $\mathfrak{M}$ se è una sottostruttura e per ogni $\vec{a} \subseteq A$ e $\varphi(\vec{x})$ vale $\mathfrak{M} \models \varphi(\vec{a}) \iff \mathfrak{U} \models \varphi(\vec{a})$[3]. Se $\mathfrak{M}$ è una $\mathcal{L}$-struttura, A è un sottoinsieme di M, e φ è una $\mathcal{L}$-formula della forma $\exists y \psi(\vec{x}, y)$, diciamo che f è una *A-funzione di Skolem* per φ se $\operatorname{dom} f = \{\vec{a} \subseteq A \mid \mathfrak{M} \models \exists y \psi(\vec{a}, y)\}$, $\operatorname{ran} f \subseteq M$ e per ogni $\vec{a} \in \operatorname{dom} f$ vale $\mathfrak{M} \models \psi(\vec{a}, f(\vec{a}))$.

Lemma 4.0.21. Sia X un insieme numerabile e sia ϱ una relazione su X tale che

$$\text{per ogni } x \in X \text{ esiste } y \in X \text{ tale che } x \varrho y.$$

Allora esiste una successione $(x_n)_{n \in \mathbb{N}}$ in X tale che $x_n \varrho x_{n+1}$ per ogni $n \in \mathbb{N}$.

Dimostrazione. Sia $\{y_n \mid n \in \mathbb{N}\}$ una enumerazione di X. Definiamo la successione $(x_n)_{n \in \mathbb{N}}$ per ricorsione: sia $x_0 = y_0$ e supponiamo di aver definito x_i per ogni $i < n+1$. Per ipotesi l'insieme $\{x \in X \mid x_n \varrho x\}$ è non vuoto. Allora definiamo x_{n+1} come l'y_j di quell'insieme che ha indice minimo rispetto alla nostra enumerazione. Ovviamente la successione $(x_n)_{n \in \mathbb{N}}$ ha la proprietà richiesta. □

Definizione 4.0.22. LS, il Principio di Löwenheim-Skolem all'ingiù, afferma che se $\mathcal{L}$ è un linguaggio numerabile e T è una $\mathcal{L}$-teoria, allora per ogni modello infinito $\mathfrak{M}$ di T esiste una sottostruttura elementare di $\mathfrak{M}$ che è numerabile (e che quindi è a sua volta modello di T).

Teorema 4.0.23. Sono equivalenti:

(1) LS.

(2) DC.

Dimostrazione.
(1) $\implies$ (2) Sia X un insieme infinito e sia ϱ una relazione su X tale che

$$\text{per ogni } x \in X \text{ esiste } y \in X \text{ tale che } x \varrho y.$$

[3]Si osservi che $\vec{a}$ può essere anche la tupla vuota. Quindi la definizione di sottostruttura elementare coinvolge anche le formule chiuse, ovvero gli enunciati. Perciò se $\mathfrak{U}$ è sottostruttura elementare di $\mathfrak{M}$ abbiamo immediatamente che soddisfano gli stessi enunciati, ovvero sono *elementarmente equivalenti*, in simboli $\mathfrak{U} \equiv \mathfrak{M}$. Segue che se una delle due strutture è modello per una teoria, anche l'altra lo è.

L'esistenza di un tale insieme è evidente. Possiamo vedere (X, ϱ) come un modello di della $\mathcal{L}$-teoria, con $\mathcal{L} = \{\varrho\}$, il cui unico enunciato è

$$\forall x \exists y (x \varrho y).$$

Per ipotesi esiste (X', ϱ') sottostruttura elementare numerabile di (X, ϱ). Per elementarità anche X' soddisfa $\forall x \exists y (x \varrho' y)$. Quindi per il Lemma 4.0.21 esiste una successione $(x_n)_{n\in\mathbb{N}}$ in X' tale che $x_n \varrho' x_{n+1}$ per ogni $n \in \mathbb{N}$. Poiché $X' \subseteq X$, $(x_n)_{n\in\mathbb{N}}$ è una successione anche in X. Inoltre, per definizione di sottostruttura, ϱ' e ϱ coincidono sugli elementi di X', e quindi su tutti gli elementi di $(x_n)_{n\in\mathbb{N}}$. Perciò $x_n \varrho x_{n+1}$ per ogni $n \in \mathbb{N}$.
(2) $\implies$ (1) Sia $\mathcal{L}$ un linguaggio numerabile e sia T una $\mathcal{L}$-teoria. Sia $\mathfrak{M}$ un modello infinito per T. Vogliamo trovare una sottostruttura elementare $\mathfrak{U}$ di $\mathfrak{M}$. Possiamo assumere senza perdità di generalità che $\mathcal{L}$ contenga solo simboli relazionali. Infatti, possiamo vedere i simboli di costante semplicemente come relazioni 0-arie. Inoltre, possiamo vedere le funzioni come relazioni (ricordiamo che le funzioni *sono* relazioni, per le quali si aggiunge la richiesta di esistenza e unicità dell'immagine). Se $\mathcal{R}$ è una relazione, affermare che "$\mathcal{R}$ è una funzione" è esprimibile al prim'ordine mediante la formula $\forall \vec{x}\, \exists! y R(\vec{x}, y)$. Allora, se $\mathcal{R}$ è una funzione in $\mathfrak{M}$, tale formula è vera in $\mathfrak{M}$, e quindi per ipotesi vale anche in $\mathfrak{U}$, e perciò $\mathcal{R}$ sarà una funzione anche in $\mathfrak{U}$.

Definiremo simultaneamente per induzione una successione crescente di sottostrutture di $\mathfrak{M}$ e una successione di famiglie di funzioni di Skolem. Il modo in cui definiremo questi oggetti ci permetterà di dimostrare che l'unione di tutte le sottostrutture è una sottostruttura elementare di $\mathfrak{M}$. Tale sottostruttura sarà banalmente numerabile per costruzione.

Sia $A_0 = \emptyset$. Per ogni φ scegliamo una A_0-funzione di Skolem e chiamiamo F_0 la famiglia di tutte queste funzioni. Si osservi che possiamo effettuare questa scelta grazie a CC, dato che le formule in un linguaggio numerabile sono in quantità numerabile[4].

Supponiamo ora che A_k e F_k siano stati definiti e siano tali che

(a) A_k è numerabile.

(b) F_k contiene una ed una sola A_k-funzione di Skolem per ogni formula in $\mathcal{L}$.

Sia $A_{k+1} := A_k \cup \bigcup\{\operatorname{ran} f \mid f \in F_k\}$. Ovviamente A_{k+1} è numerabile in quanto le A_k-funzioni di Skolem in F_k sono in quantità numerabile e hanno immagine numerabile (cfr. Osservazione 4.0.18). Grazie a CC, per ognuna di queste formule scegliamo allora delle A_{k+1}-funzioni di Skolem e definiamo F_{k+1} come la famiglia di tali funzioni, assicurandoci che estendano quelle in F_k, ovvero: se $f \in F_k$ è una A_k-funzione

[4]Se il lettore ritiene poco chiara questa affermazione, osservi che le formule si possono interpretare come stringhe finite su un alfabeto finito.

di Skolem per φ e $f' \in F_{k+1}$ è una A_{k+1}-funzione di Skolem per φ, allora imponiamo che per ogni $\vec{a} \subseteq A_k$ le funzioni f e f' siano compatibili, i.e. $f(\vec{a}) = f'(\vec{a})$.

Sia ora $A = \bigcup_{k\in\mathbb{N}} A_k$. Allora A è numerabile in quanto unione numerabile di insiemi numerabili. Sia $\mathfrak{U}$ la sottostruttura di $\mathfrak{M}$ il cui universo è A. Per definizione di sottostruttura, l'interpretazione delle relazioni è semplicemente la restrizione ad A delle relazioni di $\mathfrak{M}$. Resta da mostrare che $\mathfrak{U}$ è sottostruttura elementare di $\mathfrak{M}$. Procediamo per induzione sulla complessità di ψ, dove ψ è una formula arbitraria in $\mathcal{L}$:

- Se ψ è atomica, allora è del tipo $R(\vec{x})$ per qualche simbolo di relazione R. Per quanto appena detto, vale $\mathfrak{M} \models \psi(\vec{a}) \iff \mathfrak{U} \models \psi(\vec{a})$ per ogni $\vec{a} \subseteq A$.

- Se ψ è negazione o congiunzione di altre formule, l'affermazione segue banalmente per la tavola di verità della negazione e della congiunzione, insieme all'ipotesi induttiva.

- Se $\psi(\vec{x})$ è $\exists y \theta(\vec{x}, y)$ e $\vec{a} \subseteq A$, allora esiste un k tale che $\vec{a} \subseteq A_k$ ed esiste $f \in F_k$ che è una A_k-funzione di Skolem per φ. Se $\mathfrak{M} \models \varphi(\vec{a})$, allora $b = f(\vec{a})$ è tale che $\mathfrak{M} \models \theta(\vec{a}, b)$ e $b \in A_{k+1} \subseteq A$. Per ipotesi induttiva $\mathfrak{U} \models \theta(\vec{a}, b)$ e perciò $\mathfrak{U} \models \psi(\vec{a})$. Viceversa, se $\mathfrak{U} \models \psi(\vec{a})$ allora esiste qualche $b \in A$ tale che $\mathfrak{U} \models \theta(\vec{a}, b)$, quindi per ipotesi induttiva $\mathfrak{M} \models \theta(\vec{a}, b)$ e perciò $\mathfrak{M} \models \psi(\vec{a})$, come richiesto.

□

4.0.6 Il paradosso di Skolem

Abbiamo dimostrato che DC (e quindi AC) implica il Teorema di Löwenheim-Skolem all'ingiù. Da questo teorema segue un famoso risultato apparentemente contraddittorio, detto *Paradosso di Skolem* e messo in luce da T. Skolem stesso nel 1922[5].

Se ZFC fosse incoerente, allora sarebbe davvero un grosso problema![6] Supponiamo allora che ZFC abbia un modello (ovviamente infinito). Per LS[7], esiste una sua sottostruttura elementare numerabile. Ovvero esiste un modello $\mathfrak{M}$ numerabile per ZFC. Ma Cantor ha dimostrato che esistono insiemi non numerabili (e la dimostrazione è fatta in ZFC)! Quindi $\mathfrak{M}$ deve soddisfare l'enunciato "esiste un insieme più che numerabile", perciò $\mathfrak{M}$ è numerabile ma contiene un insieme più che numerabile!

[5] [19]

[6] Non possiamo essere certi che ZFC sia coerente, dato che per il secondo teorema di incompletezza di Gödel è impossibile provare la consistenza di ZFC lavorando in ZFC stesso, a meno che ZFC non sia incoerente: in quel caso, siccome una teoria incoerente dimostra qualsiasi cosa, ZFC dimostrerebbe anche la propria coerenza.

[7] Il linguaggio della teoria ZFC è semplicemente $\mathcal{L} = \{\in\}$, quindi è numerabile.

Sembra proprio che qualcosa non vada. Ma in realtà la contraddizione è solo apparente. Cerchiamo di capire perché, descrivendo la situazione in modo più preciso. Dire che "Cantor ha dimostrato che esistono insiemi più che numerabili" significa in realtà dire che Cantor ha dimostrato

$$\mathsf{ZFC} \vdash \exists X[\neg\exists f\varphi(X, f)]$$

dove φ è la formula nel linguaggio $\mathcal{L} = \{\in\}$ che dice "f è un insieme $\wedge$ f è una funzione $X \to \mathbb{N} \wedge f$ è iniettiva". È facile controllare che questa affermazione è effettivamente esprimibile con una $\mathcal{L}$-formula $\varphi(x, y)$ del prim'ordine. Grazie al Teorema di Correttezza (Gödel[8]), ogni modello di ZFC deve soddisfare la formula $\exists X[\neg\exists f\varphi(X, f)]$, e perciò, in effetti, anche $\mathfrak{M}$. Sia allora $\overline{X}$ un tale insieme di $\mathfrak{M}$. Vorremmo dire che anche nel nostro "modello esterno" in cui lavoriamo quell'insieme è più che numerabile, ma questo non è necessariamente vero (e anzi, in questo caso *sicuramente* non è vero, altrimenti avremmo davvero una contraddizione)! Infatti è possibile (ed è proprio così) che il nostro modello esterno, che è molto più grande, contenga un insieme che è proprio un'iniezione $\overline{X} \to \mathbb{N}$. Essenzialmente, dall'esterno "vediamo" che $\overline{X}$ è numerabile, ma $\mathfrak{M}$, dal suo interno, non se ne accorge. Un po' più precisamente, possiamo dire che il modello esterno ha molte funzioni iniettive $\overline{X} \to \mathbb{N}$, ma $\mathfrak{M}$ è talmente piccolo che non ne contiene nessuna.

Una trattazione del tutto rigorosa richiederebbe concetti di Teoria degli Insiemi piuttosto tecnici, quindi ci limitiamo a questa spiegazione abbastanza informale, sperando che risulti sufficientemente chiara.

Terminiamo indicando che, al giorno d'oggi, la comunità matematica non ritiene il paradosso di Skolem un risultato problematico, ma quando Skolem pubblicò il suo lavoro nel 1922, nonostante avesse già compreso la causa del problema così come spiegata da noi, vide in questo risultato una debolezza della teoria degli insiemi (del prim'ordine), e infatti utilizzò il paradosso per criticarne il ruolo di sistema fondazionale.

[8]Si veda eventualmente `http://web.mat.bham.ac.uk/R.W.Kaye/logic/soundness`.

Capitolo 5

Cappelli e prigionieri

Vogliamo concludere questo lavoro trattando un divertente puzzle riguardante AC e la Teoria della Probabilità. Il puzzle è stato preso da `cornellmath.wordpress.com`[1]. Iniziamo descrivendo un problema più semplice:

100 prigionieri vengono messi in fila. Ad ogni prigioniero viene permesso di guardare solo in avanti, in modo che egli possa vedere tutti i prigionieri che lo seguono, ma nessuno di quelli che lo precedono. Una guardia appoggia un cappello sulla testa di ogni prigioniero, stando attento a non mostrare il colore del cappello al prigioniero che lo indossa. Il cappello può essere di colore nero o bianco, e la scelta del colore da parte della guardia avviene in modo casuale. Poi, partendo dal primo prigioniero (ovvero quello che può vedere tutti gli altri), chiede ad ogni prigioniero qual è il colore del proprio cappello. Ogni prigioniero diventa libero se indovina il proprio colore, altrimenti viene ucciso. Inoltre, ogni prigioniero può ascoltare la risposta di quelli che lo precedono e se il guardiano li ha liberati oppure no (quindi, una volta che il guardiano arriva da lui, egli conosce il colore di tutti i cappelli che lo precedevano, oltre ovviamente al colore di tutti quelli che lo seguono). Supponendo che a tutti i prigionieri sia permesso di decidere una comune strategia prima dell'assegnazione dei cappelli, qual è la strategia che salva più prigionieri possibile?

Soluzione. La soluzione più ingenua è quella in cui ogni prigioniero tenta a caso. In questo modo, il valore atteso di prigionieri che si salvano è $100/2 = 50$. Si può fare molto meglio: il primo prigioniero conta il numero totale di cappelli bianchi. Se è dispari, allora dice bianco, altrimenti dice nero. Il prigioniero successivo conta anch'egli il numero di cappelli bianchi che vede davanti a lui, e se la parità differisce da quella che ha urlato il primo prigioniero, allora sa che il suo cappello è bianco. Quindi il secondo prigioniero si salva. Il terzo può fare lo stesso ragionamento, in

[1] L'indirizzo esatto della pagina è `http://cornellmath.wordpress.com/2007/09/13/the-axiom-of-choice-is-wrong/`.

quanto ha sentito ciò che ha urlato il primo e conosce anche il colore del secondo. Proseguendo in questo modo risulta che tutti i prigionieri si salvano, eccetto il primo (la cui sorte dipende dalla fortuna).

Passiamo ora alla variante che interessa a noi:

Stavolta, anziché 100, i prigionieri sono in quantità infinita numerabile. Il guardiano si comporta allo stesso modo, ma stavolta i prigionieri non possono ascoltare ciò che dicono quelli che li precedono, e nemmeno sapere se hanno indovinato oppure no. In questa nuova situazione, qual è la strategia migliore?

Intuitivamente, non è possibile elaborare nessuna strategia sensata, dato che nessun prigioniero può ricevere alcun tipo di informazione da chiunque sappia di che colore è il suo cappello. Sembra quindi che tutti i prigionieri debbano tentare alla cieca. Ma in realtà, esiste una strategia per la quale tutti tranne un numero finito di prigionieri sopravvive!

Soluzione. Innanzitutto, anziché pensare in termini di cappelli colorati, convertiamo bianco in 1 e nero in 0. Quindi ogni possibile assegnazione di cappelli diventa in realtà una sequenza infinita di 1 e 0, ovvero un elemento di 2^ω. Definiamo una relazione di equivalenza su 2^ω in questo modo: due sequenze sono equivalenti se e solo se differiscono al più per una quantità finita di entrate, ovvero se sono uguali da un certo punto in poi. Grazie all'Assioma di Scelta, scegliamo un rappresentante per ogni classe di equivalenza, e lo memorizziamo (o meglio, tutti i prigionieri scelgono gli stessi rappresentanti e li memorizzano). Ora, quando un prigioniero verrà messo in fila e osserverà i cappelli degli altri, sarà in grado di vedere tutta la sequenza tranne un numero finito di entrate (ovvero i cappelli di quelli che lo precedono), quindi potrà capire in quale classe di equivalenza sta la sequenza in questione. La strategia allora è quella di tentare il colore relativo alla propria posizione nella sequenza che era stata scelta a priori come rappresentante di quella classe. In questo modo, poiché il rappresentante scelto e la sequenza in cui si trovano realmente coincidono a meno di un insieme finito, tutti i prigionieri tranne una quantità finita sopravvivono![2]

A primo impatto, la situazione è chiaramente controintuitiva: ci sembra che ogni prigioniero abbia *probabilità* di salvarsi pari a $1/2$, ma alla fine si salvano tutti i prigionieri tranne un numero finito, il che sicuramente non è "la metà di $\mathbb{N}$", qualunque sia il modo (sensato) in cui vogliamo interpretare questa espressione.

[2]Un ulteriore particolare curioso è che la guardia non può impedire ciò, nemmeno conoscendo la strategia dei prigionieri e nemmeno conoscendo tutti i rappresentanti scelti dai prigionieri.

Cerchiamo ora di capire cosa sta avvenendo da un punto di vista formale[3]. Possiamo vedere la situazione come il prodotto diretto numerabile di spazi di Bernoulli, ovvero 2^ω, dove assumiamo che ogni singola prova di Bernoulli ha parametro $\frac{1}{2}$ (in realtà la struttura della dimostrazione che segue resta valida per qualsiasi parametro positivo). Chiamiamo ora $c : 2^\omega \to 2^\omega$ la funzione decisa a priori dai prigionieri che associa ad ogni sequenza un rappresentante della classe di equivalenza, come spiegato sopra. Allora, l'evento "il j-esimo prigioniero sbaglia colore" è definito formalmente come

$$E_j = \{x \in 2^\omega : x(j) \neq c(x)(j)\}$$

Intuitivamente vorremmo dire che $\mathbb{P}(E_j) = 1/2$ per ogni $j \in \omega$, dove $\mathbb{P}$ è la misura di probabilità di Bernoulli su 2^ω. Il problema è che non tutti gli E_j sono misurabili. Mostriamolo: supponiamo per assurdo che gli insiemi E_j siano tutti misurabili. Allora osserviamo innanzitutto che $\mathbb{P}(E_j) > 0$ per ogni $j \in \omega$. Infatti, sia $\overline{x} \in 2^\omega$. Consideriamo

$$A_{\overline{x}} = \{x \in 2^\omega : x(i) = \overline{x}(i) \text{ per ogni } i < j \text{ e } x(j) = 1 - c(\overline{x})(j)\}$$

È chiaro che $A_{\overline{x}} \subseteq E_j$. Ma, per come è definita la misura di Bernoulli, otteniamo $\mathbb{P}(A_{\overline{x}}) = (\frac{1}{2})^{j+1}$. Quindi $\mathbb{P}(E_j) \geq \mathbb{P}(A_{\overline{x}}) \geq (\frac{1}{2})^{j+1}$.
Sia ora $D_n = \bigcup_{k \geq n} E_k$. Vogliamo trovare degli A_{s_k} tali che per ogni $k, w \in \omega$ distinti si abbia $A_{s_k} \subseteq E_k$ e $A_{s_k} \cap A_{s_w} = \emptyset$. Per fare questo definiamo $(s_k)_{k \in \omega}$ ad hoc, nel seguente modo:

$$s_k(j) = \begin{cases} c(0^\omega)(j) & \text{se } j \leq k \\ 0 & \text{se } j > k+1. \end{cases}$$

Perciò, definendo per ogni $k \in \omega$ in modo simile a prima

$$A_{s_k} = \{x \in 2^\omega : x(i) = s_k(i) \text{ per ogni } i < k \text{ e } x(j) = 1 - s_k(k)\}$$

otteniamo banalmente $A_{s_k} \subseteq E_k$ e $A_{s_k} \cap A_{s_w} = \emptyset$, come richiesto. Inoltre, $\mathbb{P}(A_{s_k}) = (\frac{1}{2})^{k+1}$. Allora

$$\mathbb{P}(D_n) = \mathbb{P}\left(\bigcup_{k \geq n} E_k\right) \geq \mathbb{P}\left(\bigcup_{k \geq n} A_{s_k}\right) = \sum_{k=n}^{\infty} \left(\frac{1}{2}\right)^{k+1} = \left(\frac{1}{2}\right)^n$$

Osserviamo poi che $(D_n)_{n \in \omega}$ è una successione decrescente di insiemi. Inoltre ogni $x \in 2^\omega$ appartiene solo ad un numero finito di E_j. Quindi $\bigcap_{n \in \omega} D_n = \emptyset$. Poiché per

[3]La seguente spiegazione formale prende spunto dal commento di Terence Tao alla pagina citata sopra. Link diretto al commento: `http://cornellmath.wordpress.com/2007/09/13/the-axiom-of-choice-is-wrong/#comment-606`.

ipotesi gli insiemi E_j sono tutti misurabili, allora lo sono anche i D_n, e quindi per continuità delle misure di probabilità sugli insiemi misurabili abbiamo:

$$\lim_{n\to\infty} \mathbb{P}(D_n) = \mathbb{P}(\emptyset) = 0,$$

contraddizione.

Bibliografia

[1] H. Herrlich. *Axiom of Choice.* Springer Berlin Heidelberg, 2006.

[2] G. Peano. *Démonstration de l'intégrabilité des équations différentielles ordinaires.* Math. Annalen 37 (1890) 182-229.

[3] E. Zermelo, *Beweis, das jede Menge wohlgeordnet werden kann.* Math. Annalen 59 (1904) 514-516.

[4] E. Schechter. *Handbook of Analysis and its Foundation.* Acad. Press, 1997.

[5] K. Kunen. *Set theory.* College Publications, 2011.

[6] E. Borel. *Lecons sur la théorie des fonctions* Paris, 1914.

[7] A. Tarski. *Sur les ensembles finis.* Fund. Math., 6:45–95, 1924.

[8] G.P. Monro. *Independence results concerning Dedekind–finite sets.* J. Austral. Math. Soc. (Series A), 19:35–46, 1975.

[9] P. Howard and J.E. Rubin. *Consequences of the Axiom of Choice.* Amer. Math. Soc. 1998.

[10] B. Russell. *On some difficulties in the theory of transfinite numbers and order types.* Proc. London Math. Soc., 49–53, 1907.

[11] S. Wagon. *The Banach–Tarski Paradox.* Cambr. Univ. Press. Encyl. Mathem. and its Appl. 24, 1986.

[12] F. Hausdorff. *Grundzüge der Mengenlehre.* Berlin 1914.

[13] W. Sierpiński. *Sur l'équivalence des ensembles par d écomposition en deux parties.* Fund. Math., 35:151–158, 1948.

[14] R.M. Robinson. *On the decomposition of spheres.* Fund. Math., 34:246-260, 1947.

[15] S. Banach and A. Tarski. *Sur la d écomposition des ensembles de points in parties respectivement congruents.* Fund. Math., 6:244–277, 1924.

[16] J. von Neumann. *Zur allgemeinen Theorie des Maßes.* Fund. Math., 30:73-116, 1929.

[17] S. Banach. *Sur le probléme de la mesure.* Fund. Math., 4:7–33, 1923.

[18] A. Karagila. *Downward Löwenheim-Skolem Theorems and Choice Principles.*, 2014. `http://boolesrings.org/asafk/2014/lowenheim-skolem-choice/`.

[19] T. Skolem. *Axiomatized set theory.* 1922. Reprinted in *From Frege to Gödel*, van Heijenoort, 1967, in English translation by Stefan Bauer-Mengelberg, pp. 291–301.

[20] S. Willard. *General Topology.* Addison–Wesley Publ. Co., 1970.

[21] R. Dedekind. *Was sind und was sollen die Zahlen?* Vieweg Verlag, 1888.

[22] K. Stromberg. *The Banach–Tarski Paradox.* Amer. Math. Monthly, 86:151-161, 1979.