Disclaimer

Questi appunti sono nati ad uso e consumo di chi li ha scritti. Come conseguenza possono essere *molto* poco chiari, e difettano di alcune definizioni o risultati basilari già noti all'autore. Sentitevi liberi di insultarlo, segnalare sviste, eccetera presso `mennuni@mail.dm.unipi.it`

1 27/9

Un po' di discorsi sul fatto che mentre alcune teorie (tipicamente in algebra), come quella dei campi sono state completamente assiomatizzate, altre no (ad esempio quella delle equazioni differenziali), che "ereditano" l'assiomatizzazione da ZF(C). Nel linguaggio della logica matematica diciamo che la Teoria degli Insiemi *interpreta* altre teorie (ad esempio quella dei naturali assiomatizzati con Peano).

Robe:

- Assiomi di ZF
- Regole di inferenza (Frege): formalizzano la deduzione logica che si usa per derivare robe dagli assiomi.
- Usando le precedenti ottengo i *teoremi* di ZF.

In ZF io "dimostro" (ad esempio) che $\sqrt{2} \notin \mathbb{Q}$. In realtà non è completamente vero. Il problema è che ZF dimostra esclusivamente cose scrivibili nel suo linguaggio, formato da $\in$, dal simbolo di uguaglianza, dai connettivi e quantificatori logici e dalle variabili. Quello che dimostra ZF è una *traduzione* (o *interpretazione*).

Vediamo che requisiti deve soddisfare una traduzione.

- Cose vere devo essere tradotte in teoremi.

Verità matematica $\stackrel{?}{=}$ Dimostrabilità in ZF. NO! ZF è incompleto (teoremi di Godel). Esistono enunciati $\Theta \in L(ZF)$ tali che $ZF \nvdash \Theta \wedge ZF \nvdash \neg\Theta$. Quindi questa definizione di verità non va bene perché salta il terzo escluso. Bombieri ha fatto vedere che riusciva a dimostrare un enuciato sia aggiungendo a ZF l'ipotesi di Riemann sia aggiungendo la sua negazione, e chiaramente questo ci porta a concludere che l'enunciato è vero. Stiamo usando pesantemente il terzo escluso, quindi identificare verità e dimostrabilità non è assolutamente una buona idea.

Quindi a cosa corrisponde intuitivamente il concetto di dimostrabilità in ZF?

Una volta dati soli gli assiomi di ZF, per dimostrare le cose ho bisogno del "buon senso", cioè non posso prescindere dall'interpretazione degli assiomi. Invece, date le regole di inferenza, il procedimento di deduzione

diventa meccanico e posso pensare alle dimostrazioni come manipolazione di stringhe, dimenticandomi del significato. A questo punto posso chiedermi se ZF è consistente. L'affermazione

$$\neg\,\mathrm{Con}(ZF) = ZF \vdash \bot$$

cioè che ZF dimostra robe tipo $A \wedge \neg A$, a questo punto è di carattere combinatorio (manipolazione di stringhe). A questo punto posso tradurre questa stessa affermazione nel linguaggio di ZF, cioè $\mathrm{Con}(ZF) \in L(ZF)$, e chiedermi se

$$ZF \vdash \mathrm{Con}(ZF)$$

La risposta è NO. Si può dire che

$$\exists p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n] \text{ t.c. } \exists x \in \mathbb{Z}^n \; p(x) = 0 \Leftrightarrow ZF \vdash (0 = 1) \quad (1)$$

(tale che ZF è coerente se e solo se p non ha soluzioni intere, dove "coerenza" vuol dire che non esiste una dimostrazione di "0=1" in ZF usando le regole). Notare che la complessità delle due affermazioni è la stessa (se ho un certificato posso controllarlo, poi come trovarlo è un altro discorso, vedi NP). In sostanza

$$ZF \nvdash \forall x \, p(x) \neq 0$$

e quindi nemmeno la sua coerenza. In realtà sto polinomio è arrivato dopo, Godel l'aveva dimostrato in maniera diversa.

Ma se sto polinomio lo posso costruire, a questo punto posso effettivamente chiedermi se delle radici ce le ha o meno. Se le trovo, rimontando al contrario la dimostrazione della 1 ho dimostrato che ZFC è incoerente.

Seguono le solite menate storiche, paradosso di Russell, ecc.

Se a ZF tolgo l'assioma dell'infinito è praticamente uguale agli assiomi di Peano (e di quelli ci fidiamo molto di più). Praticamente è la stessa cosa parlare di insiemi finiti o di numeri naturali. In sostanza nella gerarchia di Von Neumann mi fermo a V_ω, gli ereditariamente finiti. V_ω è un modello di ZF meno l'assioma dell'infinito.

$$V_\omega \overset{f}{\cong} \mathbb{N}$$

$$\forall i, j \; i \neq j \Rightarrow a_i \neq a_j \qquad \{a_1, \ldots, a_n\} a \mapsto \sum_{i=0}^{n} 2^{f(a_i)}$$

$$\emptyset \overset{f}{\mapsto} 0$$

Notiamo che per dimostrare la coerenza di questa teoria degli insiemi finiti ho bisogno di un insieme infinito (V_ω) che faccia da modello. Eh eh eh...

La domanda di Hilbert era (tradotta in termini moderni)

$$ZF^{\mathrm{fin}} \overset{?}{=} \mathrm{Con}(ZF)$$

La domanda ha pienamente senso: agli insiemi finiti è molto più facile credere. Inoltre per il discorso di prima sul polinomio, ci basta fare un discorso sugli zeri interi di un polinomio, quindi è sperabile che ce la si faccia con metodi finitari. Il problema è che dato che non ce la fa nemmeno ZF (se coerente) a dimostrarlo, figuramoci ZF^{fin} che è più debole. Oggi diciamo che una teoria non dimostra la sua coerenza, ma il problema era nato per il motivo filosofico di far "ereditare" a ZF la "fiducia" che diamo a ZF^{fin}.

A quanto pare anche se venisse fuori che $ZF \vdash \neg \operatorname{Con}(ZF)$, questo non ne pregiudicherebbe la coerenza (wut?).

Esistono due tipi di coerenza: sintattica e semantica. La seconda vuol dire che ha un modello. La prima vuol dire che non esistono dimostrazioni di una contraddizione. La prima si può esprimere finitariamente, mentre per la seconda in generale il modello è infinito (vedi V_ω). Godel ha dimostrato (primo teorema di *completezza*) che le due cose sono equivalenti.

Notiamo che

$$ZF \nvdash A \Leftrightarrow ZF + \neg A \nvdash \bot$$

Quindi per i teoremi di completezza e incompletezza di Godel

$$ZF + \neg \operatorname{Con}(ZF) \nvdash \bot$$

ZF non può dimostrare la sua coerenza, quindi è consistente con la negazione della stessa. Abbiamo una teoria "inaffidabile" ma coerente. Non crolla tutto per aria perché stiamo dicendo che è ZF ad essere incoerente, non ZF più $\neg \operatorname{Con}(ZF)$. Quello che succede è che $ZF + \neg \operatorname{Con} ZF$ è coerente ma *ω-incoerente*. Questa teoria dimostra che esiste un x tale che $p(x) = 0$, ma dato un qualunque intero ti dice che x non è lui.

Ovviamente ci piace di più aggiungere $\operatorname{Con}(ZF)$ agli assiomi piuttosto che la sua negazione.

Potremmo fare qualcosa del tipo

$$T_0 = ZFT_1 \qquad = ZF + \operatorname{Con}(ZF) T_{n+1} = T_n + \operatorname{Con}(T_n)$$

e, se in una certa T_i dimostriamo ad esempio la congettura di Riemann, possiamo anche "credere" che sia vera in ZF. Verrebbe voglia di fare sta cosa per tutti gli ordinali, ma se saliamo troppo la dimostrazione non sarebbe "convincente", perché magari se lo dimostro al livello α ed α è elevato, potrei obiettare che magari per riconoscere α come ordinale potrei aver bisogno dell'ipotesi di Riemann (wut?).

Un sacco di problemi, ad esempio le congetture di Riemann, Goldbach, i teoremi dei quattro colori e di Fermat, l'affermazione "ZF è coerente" sono scrivibili con $\forall x P(x)$, con x oggetto finito e $P(x)$ "controllabile" algoritmicamente (dato un pari, posso controllare tutti i primi minori di lui e vedere se è somma di una coppia). Diciamo che sono affermazioni Π^0_1. Quasi tutti i problemi aperti rientrano qui.

Succede una cosa strana. Cose come la negazione di Goldabach iniziano con $\exists x$. Se fosse vera, sarebbe dimostrabile in ZF (basta esibire il pari che non è somma di due primi). Trovare il "testimone" di un $\exists$ ha la stessa difficoltà che dimostrare l'enunciato in ZF. La cosa strana che succede è che se dimostro (in ZF) che Goldbach è indipendente da ZF, allora ho dimostrato che in ZF è vero, perché se fosse falso per il discorso fatto prima sarebbe dimostrabile la sua negazione. Anche la Θ che ha trovato Godel era Π^0_1, e il discorso di prima dimostra che Θ è vera.

2 28/9

2.1 Regole di inferenza:Storia

Le prime regole sono dovute a Frege, ma erano piuttosto macchinose, robe tipo diagrammi bidimensionali. Ci si è messo pure Hilbert, e poi Gentzen che le ha presentate in due tipi: Calcolo dei sequenti e Calcolo della deduzione naturale. Vedremo una variante (come notazione, principalmente) della deduzione naturale.

2.2 Regole di inferenza:Ciccia

Diremo che "scarichiamo" un'ipotesi se ad asempio assumiamo A, dimostriamo B e quindi avendo dimostrato $A \to B$ possiamo cancellare A e dire che l'abbiamo "scaricata". Useremo come notazione $\Gamma, A = \Gamma \cup \{A\}$. Le lettere greche minuscole sono "formule" (poi verranno definite ammodino), le maiuscole insiemi delle stesse.
Assiomi (Ax):

$$\alpha \vdash \alpha \tag{2}$$

Indebolimento (Wk): giusto per non dover specificare in maniera troppo pignola gli insiemi di ipotesi.

$$\frac{\Gamma \vdash \varphi}{\Gamma, \alpha \vdash \varphi} \tag{3}$$

Congiunzione delle tesi: $(\vdash \wedge)$

$$\frac{\Gamma \vdash \alpha \quad \Gamma \vdash \beta}{\Gamma \vdash \alpha \wedge \beta} \tag{4}$$

Congiuzione delle ipotesi: $(\wedge \vdash)$

$$\frac{\Gamma, \alpha \vdash \gamma}{\Gamma, \alpha \wedge \beta \vdash \gamma} \tag{5}$$

$$\frac{\Gamma, \beta \vdash \gamma}{\Gamma, \alpha \wedge \beta \vdash \gamma} \tag{6}$$

Disgiunzione delle tesi: $(\vdash \vee)$

$$\frac{\Gamma \vdash \alpha}{\Gamma \vdash \alpha \vee \beta} \tag{7}$$

$$\frac{\Gamma \vdash \beta}{\Gamma \vdash \alpha \vee \beta} \tag{8}$$

Disgiunzione delle ipotesi: $(\vee \vdash)$ è praticamente la dimostrazione per casi senza ancora usare il terzo escluso

$$\frac{\Gamma, \alpha \vdash \gamma \quad \Gamma, \beta \vdash \gamma}{\Gamma, \alpha \vee \beta \vdash \gamma} \tag{9}$$

Implicazione: $(\vdash \rightarrow)$

$$\frac{\Gamma, \alpha \vdash \beta}{\Gamma \vdash \alpha \rightarrow \beta} \tag{10}$$

Modus ponens: era l'unica regola di uno dei sistemi "alla Hilbert", il prezzo da pagare era introdurre una quantità spropositata di assiomi.

$$\frac{\Gamma \vdash \alpha \quad \Gamma \vdash \alpha \rightarrow \beta}{\Gamma \vdash \beta} \tag{11}$$

Bottom 1: $(\vdash \bot)$ Connettivo 0-ario che vale sempre falso.

$$\frac{\Gamma \vdash \alpha \quad \Gamma \vdash \neg\alpha}{\Gamma \vdash \bot} \tag{12}$$

Bottom 2: $(\bot)$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \alpha} \tag{13}$$

Negazione 1: $(\neg \vdash)$

$$\frac{\Gamma \vdash \alpha}{\Gamma, \neg\alpha \vdash \bot} \tag{14}$$

Negazione 2: $(\vdash \neg)$ questa è accettata anche da quelle brutte bestie degli intuizionisti

$$\frac{\Gamma, \alpha \vdash \bot}{\Gamma \vdash \neg\alpha} \tag{15}$$

Reductio ad absurdum: l'unica differenza fra intuizionisti e persone dotate di buon senso

$$\frac{\Gamma, \neg\alpha \vdash \bot}{\Gamma \vdash \alpha} \tag{16}$$

Postponiamo le regole per i quantificatori. Per ora ci accontentiamo della logica proposizionale.

Teorema 2.1. φ formula proposizionale, $\emptyset \vdash \varphi$ se e solo se φ è una tautologia.

Teorema 2.2. Se Γ è un insieme finito di ipotesi e φ è una formula proposizionale, $\Gamma \vdash \varphi$ se e solo se $\Gamma \to \varphi$ è una tautologia.

Potrei dare il Weakening anche con $\Sigma \supset \Gamma$ invece che aggiungendo una formula alla volta (se voglio usare insiemi infiniti, ma per ora lasciamo perdere).

Teorema 2.3. φ formula proposizionale, $\Gamma \vdash \varphi$ se e solo se per ogni valutazione $v : \mathrm{Var} \to \{0, 1\}$ si ha $\Gamma^v = 1 \Rightarrow \varphi^v = 1$ (si intende che v valga 1 su ogni elemento di Γ).

$$\frac{\forall v(\Gamma^v = 1 \Rightarrow \varphi^v = 1)}{\Gamma \models \varphi}$$

(questa è una definizione del simbolo $\models$; in sostanza stiamo dicendo che ci rifacciamo alle care vecchie tavole di verità)

Tutte sti discorsi li stiamo facendo perché una volta introdotti i quantificatori non potremo più usare le tavole di verità (e per accontentare gli intuizionisti anche nel caso proposizionale).

Il $\vdash$ vuol dire che in un numero finito di passaggi passo dalla roba a sinistra a quella a destra (alberi di derivazioni, livelli di profondità...) usando le regole precedenti e gli assiomi.

Esercizio 2.4. $\neg\neg A \vdash A$ (senza tavole di verità)

Dimostrazione. Facciamola al contrario. Basta mostrare che $\neg\neg A, \neg A \vdash \bot$. Lo faccio mostrando che $\neg\neg A, \neg A \vdash \neg A$ e che $\neg\neg A, \neg A \vdash \neg\neg A$. Per fare questo uso l'indebolimento su $\neg\neg A \vdash \neg\neg A$ e su $\neg A \vdash \neg A$. □

Esercizio 2.5. $\emptyset \vdash A \vee \neg A$ (sempre senza tavole di verità)

Dimostrazione. Voglio passare da $\neg(A \vee \neg A) \vdash \bot$. Ma da $\neg(A \vee \neg A)$ ottengo sia A che $\neg A$. Per la prima uso che $\neg(A \vee \neg A), \neg A \vdash \neg(A \vee \neg A)$ (da $\neg(A \vee \neg A) \vdash \neg(A \vee \neg A)$) e che per weakening $\neg(A \vee \neg A), \neg A \vdash A \vee \neg A$ segue da $\neg A \vdash A \vee \neg A$, che segue da $\neg A \vdash \neg A$. L'altra è simile. □

Nota: per gli intuizionisti vale comunque $\neg A \equiv (A \to \bot)$. Usiamo le maiuscole latine per le variabili e le greche minuscole per formule proposizionali.

Metateorema 2.6. Da $\varphi \vdash \psi$ e $\neg\varphi \vdash \psi$ segue in un numero finito di passi $\emptyset \vdash \psi$.

Dimostrazione. L'albero non lo scriviamo per davvero. Uso che $\varphi \vee \neg\varphi \vdash \psi$ e $(\varphi \vee \neg\varphi) \to \psi$, poi il modus ponens e l'Esercizio 2.5. □

3 4/10

Se scriviamo $\models \varphi$ sottointendiamo $\emptyset \models \varphi$, cioè che φ è sempre vera (solite storie col vuoto).

Problema aperto: sostanzialmente il complementare di SAT. Una formula si dice insoddisfacibile se la sua negazione è una tautologia. Il problema è stabilire se una formula è una tautologia.

3.1 Quantificatori

3.1.1 Euristica

Il problema è che quando uso i quantificatori non posso usare le tavole di verità, perché in generale dovrei controllare un numero infinito di casi (altrimenti non ci sarebbe bisogno di usare i quantificatori, se non come abbreviazione tipografica).

Esempio 3.1. Proviamo a dimostrare che $\vdash \exists x \forall y \, \mathrm{P}(x, y) \to \forall y \exists x \, \mathrm{P}(x, y)$, oppure la stessa con la freccia girata. Chiaramente la freccia $\to$ è vera e la freccia $\leftarrow$ no. Vogliamo dimostrare la cosa vera ed estrarne le regole.

Dimostrazione. (informale)

1. Assumo $\exists x \forall y \, \mathrm{P}(x, y)$;
2. sia a tale che $\forall y \, \mathrm{P}(a, y)$;
3. qualunque sia y vale $\mathrm{P}(a, y)$;
4. in particolare $\exists x \, \mathrm{P}(x, y)$;
5. per arbitrarietà di y ho (quasi) finito: $\forall y \exists x \, \mathrm{P}(x, y)$. Posso scaricare l'ipotesi intermedia 3;
6. scarico l'ipotesi 1 e ho dimostrato che $\exists x \forall y \, \mathrm{P}(x, y) \to \forall y \exists x \, \mathrm{P}(x, y)$

□

Diamo ora una dimostrazione *sbagliata* del $\leftarrow$.

Dimostrazione SBALIATA. Voglio dimostrare che $\forall y \exists x \, \mathrm{P}(x, y) \to \exists x \forall y \, \mathrm{P}(x, y)$

1. Per ipotesi $\forall y \exists x \, \mathrm{P}(x, y)$;
2. $\exists x \, \mathrm{P}(x, b)$;
3. sia a un tale x, cioè $\mathrm{P}(a, b)$;
4. siccome b è generico $\forall y \, \mathrm{P}(a, y)$;

5. $\exists x \forall y P(x, y)$.

□

L'errore è chiaramente nel penultimo punto: a dipende da b.

3.1.2 Ciccia

Diamo le regole "stile ipotesi implicite". Le prime sono innocue:

$$\frac{\mathrm{P}(a)}{\exists x\, \mathrm{P}(x)} \tag{17}$$

$$\frac{\forall x\, \mathrm{P}(x)}{P(a)} \tag{18}$$

Ora vorrei dire che se dimostro $\mathrm{P}(a)$ con a generico ho dimostrato $\forall x\, \mathrm{P}(x)$, ma l'esempio di prima ci fa notare che la cosa è abbastanza delicata. La maniera giusta di farlo è tradurre *generico* con "non compare fra le ipotesi ancora non scaricate".

$$\frac{\mathrm{P}(a)}{\forall x\, \mathrm{P}(x)} \quad a \text{ generico} \tag{19}$$

La più complicata (sempre per evitare i problemi di prima): Se da $\mathrm{P}(a)$ ottengo φ e a non compare in φ, ho dimostrato $\exists x\, \mathrm{P}(x) \to \varphi$.

L'errore nella dimostrazione sbagliata era nella 3: b non è generico perché compare su un'ipotesi (un'ipotesi su a, ma pur sempre un'ipotesi).

Altra regola, corretta ma ridondante (poi dimostriamo correttezza e minimalità dell'insieme di regole già dato):

$$\frac{\forall y \exists x\, \mathrm{P}(x, y)}{\exists f \forall y\, \mathrm{P}(f(y), y)} \tag{20}$$

(accenni sul calcolo dei sequenti, non trascritti)

Diamo la versione delle regole con le ipotesi esplicite:

$$\frac{\Gamma \vdash \mathrm{P}(a)}{\Gamma \vdash \forall x\, \mathrm{P}(x)} \quad a \notin \Gamma, \mathrm{P}(x) \tag{21}$$

$$\frac{\Gamma \vdash \forall x\, \mathrm{P}(x)}{\Gamma \vdash \mathrm{P}(b)} \tag{22}$$

Dove b è un qualunque termine sostituibile (vedi più avanti).

$$\frac{\Gamma \vdash \mathrm{P}(a)}{\Gamma \vdash \exists x\, \mathrm{P}(x)} \tag{23}$$

$$\frac{\Gamma, \mathrm{P}(a), \vdash \varphi}{\Gamma, \exists x\, \mathrm{P}(x) \vdash \varphi} \quad a \notin \Gamma, P, \varphi \tag{24}$$

Alla faccia degli intuizionisti, ora dimostreremo

Esercizio 3.2. $\neg\forall x\,\mathrm{P}(x) \vdash \exists x\neg\,\mathrm{P}(x)$

Dimostrazione. L'idea è che con qualche passaggio arrivo a $\neg\,\mathrm{P}(a) \vdash \exists x\neg\,\mathrm{P}(x)$. Poi $\neg\exists x\neg\,\mathrm{P}(x), \neg\,\mathrm{P}(a) \vdash \neg\exists x\neg\,\mathrm{P}(x)$. Quindi dalle stesse ipotesi ottengo un assurdo, per cui $\neg\,\mathrm{P}(a) \vdash \exists x\neg\,\mathrm{P}(x)$.

$\neg\exists x\neg\,\mathrm{P}(x) \vdash \mathrm{P}(a)$ poi $\neg\exists x\neg\,\mathrm{P}(x) \vdash \forall x\,\mathrm{P}(x)$. Siccome $\neg\forall x\,\mathrm{P}(x), \neg\exists x\neg\,\mathrm{P}(x) \vdash \forall x\,\mathrm{P}(x)$ e $\neg\forall x\,\mathrm{P}(x), \neg\exists x\neg\,\mathrm{P}(x) \vdash \neg\forall x\,\mathrm{P}(x)$, da cui ho un assurdo e quindi $\neg\forall x\,\mathrm{P}(x) \vdash \exists x\neg\,\mathrm{P}(x)$. □

Esercizio 3.3. Dimostrare $\neg\forall \vdash \exists\neg$, $\neg\exists \vdash \forall\neg$ e quelle col $\dashv$.

Definizione 3.4. Se L è un linguaggio e $\{A, B, C, \ldots\}$ sono le variabili proposizionali, definiamo le L-formule proposizionali come:

- Formule atomiche: $A, B, C, \ldots$, cioè se $A \in L$ allora A è una L-formula. Sono le formule di livello 0.
- Se φ, ψ sono L-formule, allora lo sono anche $(\varphi \wedge \psi)$, $\neg\varphi$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$. Se φ, ψ sono di livello n, le altri sono di livello $n+1$.
- Consideriamo il più piccolo insieme di stringhe che verifica le precedenti, o equivalentemente quelle per cui esiste un n, livello a cui si trovano.

Definizione 3.5. Definiamo le L-formule predicative (primo ordine): nel linguaggio ci sono dei simboli di predicato $\{P, Q, R, \ldots\}$, ognuno con una certa *arietà* (numero di argomenti), vista come funzione dai simboli di predicato a $\mathbb{N}$ (se è 0 è una formula proposizionale). Inoltre c'è un insieme infinito numerabile di *variabili* $\{x, y, z, \ldots\}$ (bastano numerabili perché posso "riciclarle" in formule diverse: tanto la singola formula è una stringa *finita*). Le L-formule si definiscono come

- Atomiche: $\mathrm{P}(x_1, \ldots, x_n)$ $P \in L$ n-aria, $x_1, \ldots, x_n \in V$.
- Se φ, ψ sono L-formule, allora lo sono anche $(\varphi \wedge \psi)$, $\neg\varphi$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $\forall x\varphi$, $\exists x\varphi$, queste ultime due ovviamente con $x \in V$. Se φ, ψ sono di livello n, le altri sono di livello $n+1$.
- Al solito, minimizzo intersecando i linguaggi che verificano le precedenti o unendo le stringhe di livello n, per ogni $n \in \mathbb{N}$.

Esercizio 3.6. Se aggiungo le parentesi o metto i connettivi all'inizio invece che in mezzo, il linguaggio non è ambiguo.

4 5/10

4.1 Semantica

Vogliamo prendere una *formula* (stringa) e *interpretarla* in una *proposizione* vera o falsa (se la formula non ha variabili libere, ovviamente). Per interpretare ad esempio

$$\forall x(\mathrm{P}(x) \vee \mathrm{Q}(x)) \tag{25}$$

bisogna specificare dove spazia la variabile x (deve essere non vuoto) e chi sono P e Q.

Per la formalizzare la semantica non ci basteranno più gli insiemi finiti.

Definizione 4.1 (informale)**.** Una L-formula φ è sempre vera se $\models \varphi$, cioè se è vera in ogni interpretazione.

Ci sono formule vere in ogni interpretazione finita ma non in interpretazioni infinite. Ad esempio una grossa congiunzione che definisca un ordine totale (meno l'antisimmetria per non avere noie con l'uguaglianza che è una questione delicata) $\models$ la proposizione di esistenza di un massimo per ogni ordine totale.

(seguono spoiler sul Teorema di Completezza, che dimostreremo più in là, non trascritti)

Spoiler interessante: non ci sono regole per $\underset{\text{fin}}{\models}$ per cui valga il Teorema di Completezza (Teorema di Tracktenbrot).

Come faccio a far vedere che $\Gamma \nvdash \varphi$? Se ho il Teorema di Completezza mi basta dimostrare $\Gamma \not\models \varphi$, cioè esibire un modello appropriato (tipo geometrie non euclidee per l'assioma delle parallele).

C'è un algoritmo per vedere che non ci sono dimostrazioni (stringhe) di φ? NO (Teorema di Church).

Esempio 4.2 (con uguaglianza e funzioni)**.**

$$A \overset{?}{\models} [\forall xyz\,(h(x, h(y, z)) = y \to \forall uv(u = v)] \tag{26}$$

con $A \neq \emptyset$ dominio non vuoto e $h : A \times A \to A$

Sì, c'è un trucchetto (sostituire z con $h(s, t)$, guardare la roba tipo $h(\ldots, h(\ldots))$ più esterna e quella più interna...)

4.1.1 Tableaux

Tableaux (Beth, Hintikka): ricerche sistematiche di controesempi. Cerco un'interpretazione in cui Γ è vero, φ falsa. Se riesco $\Gamma \not\models \varphi$. Se fallisco (e finisco) $\Gamma \models \varphi$, però potrei non finire. Sta cosa può servire per cercare controesempi a una cosa che so essere falsa.

In sostanza questo metodo prende in input Γ insieme di formule e cerca un suo modello (cioè un'interpretazione che rende vere le formule). Le regole sono: (conveniamo che le greche maiuscole sono insieme di formule, le minuscole sono singole formule)

1.

$$\begin{array}{ccc} & \Sigma, \alpha \vee \beta & \\ \swarrow & & \searrow \\ \Sigma, \alpha & & \Sigma, \beta \end{array}$$

2.

$$\begin{array}{c} \Sigma, \alpha \wedge \beta \\ | \\ \Sigma, \alpha, \beta \end{array}$$

3.

$$\begin{array}{ccc} & \Sigma, \alpha \to \beta & \\ \swarrow & & \searrow \\ \Sigma, \neg\alpha & & \Sigma, \beta \end{array}$$

4.

$$\begin{array}{c} \Sigma, \neg\neg\varphi \\ | \\ \Sigma, \varphi \end{array}$$

5.

$$\begin{array}{c} \Sigma, \neg(\alpha \vee \beta) \\ | \\ \Sigma, \neg\alpha, \neg\beta \end{array}$$

6.

$$\begin{array}{ccc} & \Sigma, \neg(\alpha \wedge \beta) & \\ \swarrow & & \searrow \\ \Sigma, \neg\alpha & & \Sigma, \neg\beta \end{array}$$

7.

$$\begin{array}{c} \Sigma, \neg(\alpha \to \beta) \\ | \\ \Sigma, \alpha, \neg\beta \end{array}$$

8.

$$\begin{array}{c} \Sigma, \exists x\, \mathrm{P}(x) \\ | \\ \Sigma, \mathrm{P}(a) \end{array}$$

con $a \notin \Sigma, \mathrm{P}(x)$.

9.

$$\begin{array}{c} \Sigma, \forall x\, \mathrm{P}(x) \\ | \\ \Sigma, \mathrm{P}(b), \forall x\, \mathrm{P}(x) \end{array}$$

Con b sostituibile.

Questo è il "while" che non fa terminare le cose. Mi serve perché altrimenti non avrei più il se e solo se fra esistenza di un modello per la radice ed esistenza di un modello per le foglie.

10.

$$\begin{array}{c} \Sigma, \neg(\exists x\, \mathrm{P}(x)) \\ | \\ \Sigma, \neg\, \mathrm{P}(b), \neg\exists x\, \mathrm{P}(x) \end{array}$$

Sempre con b sostituibile.

11.

$$\begin{array}{c} \Sigma, \neg\forall x\, \mathrm{P}(x) \\ | \\ \Sigma, \neg\, \mathrm{P}(a) \end{array}$$

con $a \notin \Sigma, \mathrm{P}(x)$

Notiamo che fare un tableaux vuol dire fare un albero, quindi finché non ci mettiamo in mezzo i quantificatori l'algoritmo termina sempre: arrivo a roba atomica e poi posso dare gli assegnamenti che rendono vera questa roba atomica o constatare che non ce ne sono (ci si riduce alle solite tavole di verità).

Questo metodo è comodo anche per scrivere le cose in forma normale disgiuntiva (disgiunzione di congiunzioni) partendo da una forma normale congiuntiva (congiunzione di disgiunzioni).

Inoltre se mi invento un nuovo connettivo n-ario, dalla sua tavola di verità col metodo dei tableaux arrivo alla DNF e quindi posso ricostruirlo da quelli vecchi. In realtà un solo connettivo (nè A nè B) basta per fare tutto.

Per le regole che biforcano (cioè quelle con la "o") ho che la radice ha un modello se e solo se una delle foglie ha un modello. Inoltre senza quantificatori questo modello è lo stesso; coi quantificatori può essere anche diverso (basta pensare a una proposizione della forma $\exists x$ verificata da un solo x in un modello e da diversi x_i, fra cui il vecchio x, in un altro).

Esercizio 4.3.

$$\overset{?}{\vdash} \exists x(\mathrm{P}(x) \to \forall y\, \mathrm{P}(y)) \tag{27}$$

Questa è sempre vera. Se lo approccio con i tableaux cerco di rendere vera la sua negazione e mi aspetto di vedere che venga fuori falsa (svolgimento non riportato).

5 11/10/12

Domani niente lezione.

Diamo gli assiomi per l'uguaglianza. I primi tre sono quelli di una qualunque realzione di equivalenza, inoltre ci serve la *proprietà degli indiscernibili* di Leibniz, che ci farebbe comodo enunciare come

$$\forall P(P(x) \Leftrightarrow P(y)) \Leftrightarrow x = y \tag{28}$$

Il problema è che questo è del second'ordine. Quindi invece di un assioma daremo uno schema di assiomi (uno per ogni predicato P)

$$x_1 = y_1 \wedge \ldots \wedge x_n = y_n \wedge P(x_1, \ldots, x_n) \to P(y_1, \ldots, y_n) \tag{29}$$

Oppure per fare una cosa più pulita posso definire l'uguaglianza come la relazione *diagonale* (le coppie (x, x)).

Spoiler: non è possibile dare degli assiomi che obblighino la mia teoria a interpretare l'uguaglianza come la vera uguaglianza, ma almeno di quozientare modelli posso supporre di lavorare con l'uguaglianza vera. Ne riparleremo.

5.1 Sintassi

Definizione 5.1. Un *linguaggio con* $= L$ è un insieme di simboli di

1. Predicato (relazione) $P, Q, R, \ldots$
2. Funzione $f, g, h, \ldots$
3. Costante $a, b, c, \ldots$

ognuno con una sua *arietà*: $L \to \mathbb{N}$.

In ogni linguaggio sono presenti le variabili, i connettivi logici e i quantificatori. Quello che differenzia i linguaggi è l'insieme definito sopra. Ad esempio potremmo avere i linguaggi $\{0, 1, +, \cdot\}$ dove i primi due simboli sono costanti e gli altri due funzioni binarie, $\{\in\}$, $\{\leq\}$, entrambi dove l'unico simbolo è una relazione. Tutte le definizioni a seguire si intendono dato un linguaggio L. L'idea dietro è che una *formula* è qualcosa di vero o falso, un *termine* no.

Definizione 5.2. Un L-termine è

- una variabile;
- una costante;
- $f(t_1, \ldots, t_n)$, con i t_i termini ed f simbolo di funzione n-aria
- nient'altro (l'insieme dei termini è il più piccolo che contiene quelli sopra elencati).

Notiamo che in questa maniera possiamo comporre le funzioni, ma non i predicati.

Alcuni manuali di logica fanno caso alla sottigliezza che $t_1, \ldots, t_n$ sono *variabili metalinguistiche*.

Definizione 5.3. Una L-formula è

- $P(t_1, \ldots, t_n)$, dove $t_1, \ldots t_n$ sono termini e $P \in L$ è una relazione n-aria;
- $t_1 = t_2$, con t_1, t_2 termini;
- $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $\forall x\varphi$, $\exists x\varphi$, con φ, ψ L-formule;
- nient'altro (come sopra).

5.2 Semantica

Definizione 5.4. Una L-struttura M è data da

1. un insieme non vuoto $\mathrm{dom}(M)$;
2. una funzione di interpretazione

$$\begin{aligned} c \in L &\mapsto c^M \in \mathrm{dom}(M) \\ f \in L &\mapsto f^M : (\mathrm{dom}(M))^n \to \mathrm{dom}\, M \\ P \in L &\mapsto P^M \subseteq (\mathrm{dom}(M))^n \end{aligned}$$

dove n è l'arietà di f o di P.

Ad esempio sul linguaggio $L = \{f\}$, con f simbolo di funzione binaria, possiamo dare la L-struttura $M = (\mathbb{N}, +)$, dove $\mathrm{dom}(M) = \mathbb{N}$, $f^M : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ $(x, y) \mapsto x + y$ (quest'ultimo $+$ è da intendersi come la somma vera e propria, non come simbolo).

Ora che ho dato un significato ai simboli lo posso dare anche a termini e formule.

5.2.1 Semantica di Tarski

Data φ una L-formula ed M una L-struttura, voglio definire con precisione cosa si intende dicendo "φ è *vera* in M". Notare che il fatto che stiamo definendo la verità non ci dà (in generale) un criterio per stabilire se qualcosa è vero o falso.

Esempio 5.5 (Tarski)**.** "La neve è bianca" è vera se e solo se la neve è bianca. La verità è un "invertitore di virgolette". Ad esempio $\forall x \forall y (x \cdot y \doteq y \cdot x)$ è vera in $M = (\mathbb{N}, +)$ se e solo se per ogni $a \in \mathbb{N}$ e per ogni $b \in \mathbb{N}$ $a + b = b + a$ ($\cdot$ e $\doteq$ sono simboli, $+$ e $=$ l'interpretazione). In sostanza i quantificatori li faccio spaziare nel dominio e i simboli li interpreto. Notare che stiamo usando l'italiano (e qualcos'altro) come *metalinguaggio*.

Ovviamente qui abbiamo definito la verità per una singola formula; per evitare di barare dicendo "e analogamente", diamo un po' di definizioni.

Introduciamo (tanto la useremo) la teoria dei naturali con gli assiomi di Peano. Il linguaggio è $L = \{0, s, +, \cdot\}$. Gli assiomi sono

1. $\forall x\ 0 \neq s(x)$
2. $s(x) = s(y) \to x = y$
3. $x \neq 0 \to \exists y\ s(y) = x$
4. $x + 0 = x$, $x + s(y) = s(x + y)$

5. $x \cdot 0 = 0$, $x \cdot s(y) = x \cdot y + x$

6. lo schema di assiomi (sempre per evitare di andare al second'ordine)

$$\Big(\varphi(0) \wedge \forall x\big(\varphi(x) \to \varphi(s(x))\big)\Big) \to \forall y \varphi(y)$$

al variare di φ fra le L-formule.

Indichieremo questa teoria con PA^1, che a meno di Goedelizzazione possiamo pensare come un insieme di numeri naturali, quella del second'ordine con PA^2.

Problema: vorrei dire che tutti gli assiomi di PA^1 sono veri in $(\mathbb{N}, s^{\mathbb{N}}, +^{\mathbb{N}}, \cdot^{\mathbb{N}})$, ma sono infiniti. Voglio dire che $ZF \vdash$ (gli assiomi di PA^1 sono *veri* in $(\mathbb{N}, s, +, \cdot, 0)$) ma devo definire quel *veri*.

Diamo ora la Semantica di Tarski usando come metalinguaggio l'italiano (per comodità, ma si possono usare anche i naturali, passando sempre dalla Goedelizzazione).

Definiamo ricorsivamente (usando come metalinguaggio "vero" ZF e il suo Teorema di Ricorsione; le formule sono indicizzate dai naturali, quindi *non* si passa al second'ordine) la nozione di verità

Definizione 5.6 (Variabili libere)**.** L'insieme di variabili libere di un termine è:

1. $V(c) = \emptyset$, se c è una costante

2. $V(f(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n} V(t_i)$

3. $V(x) = \{x\}$ se x è una variabile

Diciamo che un termine t è *chiuso* se $V(t) = \emptyset$.

Definizione 5.7. Se t è un termine chiuso lo interpretiamo in un modello M come

1. se il termine t è una costante c, l'interpretazione è c^M;

2. se il termine è della forma $f(t_1, \ldots, t_n)$ lo interpretiamo come $f^M(t_1^M, \ldots t_n^M)$.

Per i termini non chiusi, useremo una *funzione di valutazione* o *ambiente* $s : V \to \mathrm{dom}(M)$

$$\begin{aligned} x^{(M,s)} &= s(x) \\ c^{(M,s)} &= c^M \\ (f(t_1, \ldots, t_n))^{M,s} &= f^M(t_1^{M,s}, \ldots, t_n^{M,s}) \end{aligned}$$

Consideriamo ora la funzione

$$\text{Verità}_M : \text{Formule} \times \text{Valutazioni} \to \{0,1\} \quad (\varphi, s) \mapsto \varphi^{(M,s)}$$

$$(\varphi \wedge \psi)^{M,s} = \min(\varphi^{M,s}, \psi^{M,s})$$
$$(\neg\varphi)^{M,s} = 1 - \varphi^{M,s}$$
$$(\varphi \vee \psi)^{M,s} = \max(\varphi^{M,s}, \psi^{M,s})$$
$$(t_1 \dot{=} t_2)^{M,s} = \begin{cases} 1 & \text{se} \quad (t_1^{M,s}, t_2^{M,s}) \in \Delta^M \\ 0 & \text{se} \quad (t_1^{M,s}, t_2^{M,s}) \notin \Delta^M \end{cases}$$
$$(P(t_1,t_2))^{M,s} = \begin{cases} 1 & \text{se} \quad (t_1^{M,s}, t_2^{M,s}) \in P^M \\ 0 & \text{se} \quad (t_1^{M,s}, t_2^{M,s}) \notin P^M \end{cases}$$
$$(\forall x\varphi)^{M,s} = \min_{a \in \text{dom}(M)} \left(\varphi^{M,s_{a/x}}\right)$$

dove intendiamo

$$s_{a/x}(x) = a, \quad y \in \text{Var} \setminus \{x\} \Rightarrow s_{a/x}(y) = s(y)$$

6 18/10

Esempio 6.1. $L = \{R, c\}$, con R relazione binaria e c simbolo di costante. La L-formula $R(x,c)$ la interpretiamo nella L-struttura $\text{dom}(M) = \mathbb{N}$, $R^M \subseteq \mathbb{N}^2$ $R^M = \{(x,y) \mid x \leq y\}$, $c^M = 3 \in \mathbb{N}$ e nell'ambiente (valutazione) $S : x \mapsto 4, y \mapsto 5, z \mapsto 6 \ldots$. In questa struttura con questo ambiente la formula di prima è falsa, cioè $R(x,c)^{M,S}$ è falsa perché dice che in $\mathbb{N}$ si ha $4 \leq 3$.

Conveniamo di denotare "falso" con 0 e "vero" con 1 e a volte useremo M per denotare $\text{dom}(M)$, con abuso di notazione.

Notiamo che se scriviamo ad esempio $\forall x \exists x P(x)$ il $\forall x$ è come se non ci fosse: faccio il minimo di un massimo che una volta risolto è costante, quindi faccio il minimo di una costante.

Definizione 6.2. Definiamo (in parte già l'abbiamo fatto) chi è l'insieme delle variabili libere di una formula:

1. $V(\varphi \wedge \psi) = V(\varphi) \cup V(\psi)$
2. $V(\varphi \vee \psi) = V(\varphi) \cup V(\psi)$
3. $V(\neg\varphi) = V(\varphi)$
4. $V(\forall x\varphi) = V(\varphi) \setminus \{x\}$
5. $V(\exists x\varphi) = V(\varphi) \setminus \{x\}$

6. Se φ è atomica, $V(\varphi)$ = tutte le variabili libere di φ.

Lemma 6.3. $\varphi^{M,s}$ dipende solo da $s_{|V(\varphi)}$, cioè se $s_{1|V(\varphi)} = s_{2|V(\varphi)}$ allora $\varphi^{M,s_1} = \varphi^{M,s_2}$.

Si dimostra al solito per induzione sulla lunghezza delle formule.

Tutto quello fatto finora è stato praticamente fatto usando come metateoria l'italiano. Se uso come metateoria ZF posso definire la verità in modo induttivo senza passare al second'ordine. Questo perché ho tradotto le φ in un numero naturale e dentro ZF questo è prim'ordine (è secondo visto dal "mondo" di φ).

$$ZF \vdash \forall\varphi \text{ assioma di Peano } \varphi \text{ è vera in } \mathbb{N}$$

Se φ è una L-formula chiusa e M è una L-struttura, posso definire la semantica di Tarski in quest'altra maniera: ad esempio per la teoria dei campi posso dare

1. $L = \{0, 1, +, \cdot\}$
2. $L_M = L \cup \{c_a \mid a \in M\}$
3. $(c_a)^M = a$

In questa maniera mi libero dell'ambiente e scarico tutto sulla struttura

Definizione 6.4. Dati φ formula, t termine, $x \in V$, definiamo la *sostituzione* $\varphi(t/x)$ come l'operazione che sostituisce t a tutte le occorrenze libere di x.

1. $(\neg\varphi)(t/x) = \neg(\varphi(t/x))$
2. $(\forall x\varphi)(t/x) = \forall x\varphi$
3. $(\forall x\varphi)(t/x) = \forall y(\varphi(t/x))$

e analoghi con congiunzione, quantificatore esistenziale, eccetera.

Occhio che $\forall x\varphi \to \varphi(t/x)$ non è sempre vera. C'è il problema della *cattura delle variabili*. Ad esempio consideriamo

$$\forall x \underbrace{\exists y(x = y)}_{\varphi} \stackrel{?}{\to} \exists y(y + 1 = y)$$

Chiaramente no, quello che dà problemi è fare $\forall x\varphi \to \varphi(y + 1/x)$.

Per evitarli mi basta trasformarla in $\exists z(x = z)$ e a questo punto assegnare $y + 1$ a z non dà problemi.

Formalmente

Definizione 6.5. t è *sostituibile* al posto di x in φ se non succede che t contiene una variabile y e φ contiene una sottoformula della forma $\forall y\psi$ o $\exists y\psi$ tale che $x \in V(\psi)$. In altre parole la sostituzione non deve legare variabili libere di t.

Notiamo che la quantificazione fa perdere la dipendenza dall'ambiente: $\exists z R(x,z)$ è la stessa cosa di $\exists y R(x,y)$ ma *non* è la stessa cosa di $\exists z R(y,z)$.

Un'altra maniera di far sparire tutti i problemi di cattura è usare insiemi diversi per le variabili da quantificare e per quelle libere.

Definizione 6.6. Una *L-teoria* è una coppia (T, L), con T insieme di formule chiuse di L (assiomi).

Definizione 6.7. I *modelli* $\mathrm{Mod}_L(T)$ sono gli M L-strutture tali che $\forall \varphi \in T$ $\varphi^M = 1$, o più brevemente $T^M = 1$.

Definizione 6.8. Data T una L-teoria e φ una L-formula, diciamo che

$$T \models \varphi \Leftrightarrow \mathrm{Mod}(T) \subseteq \mathrm{Mod}(\varphi)$$

Si può definire $T \models \varphi$ anche se T, φ contengono variabili libere. Si può fare in due modi, la decisione da prendere è cosa vuol dire in tal caso $P(x) \models P(y)$. Le due scelte possibili sono

- $\models \forall xy(P(x) \to P(y))$ che non è detto che sia vera
- $\models \forall x P(x) \to \forall y P(y)$ che è sempre vera

dato che è quella che *non* si riesce a dimostrare con le regole date (non è una tautologia), ci conviene usare la prima. La convenzione che useremo per $T \models \varphi$ nel caso di variabili libere è quindi $\forall M, s \left(T^{M,s} = 1 \to \varphi^{M,s} = 1\right)$. L'altra possibile (che *non* useremo) è $\forall M \left(\forall s T^{M,s} = 1 \to \forall s \varphi^{M,s} = 1\right)$.

Anche se noi useremo formule chiuse, ci conviene considerare anche quelle non chiuse per poter enunciare il

Teorema 6.9 (di correttezza delle regole della deduzione naturale)**.** Ogni regola è corretta se interpreto $\vdash$ come $\models$.

Dimostrazione. Per esercizio. Bisogna usare le stesse regole, però nel metalinguaggio. □

Esercizio 6.10. Qualunque formula si può mettere in forma premessa (con tutti quantificatori all'inizio), ad esempio $\forall x(P(x) \wedge Q(x)) \equiv (\forall x P(x)) \wedge (\forall x Q(x))$.

Teorema 6.11 (di correttezza)**.** Se $T \vdash \varphi$, allora $T \models \varphi$.

Dimostrazione. Per induzione sul numero di regole applicate. □

7 19/10/12

Per ora abbiamo dato due sistemi di regole: la deduzione naturale e i tableaux. Per i tableaux la semantica dice che i figli hanno un modello se e solo se il padre ha un modello. Nel caso della deduzione naturale ci servono sia un modello che un ambiente, nel caso dei tableaux solo un modello. L'obiettivo della deduzione naturale è sapere se $\Gamma \vdash \varphi$, mentre tableaux ci dicono che $\Gamma, \neg\varphi$ non ha modelli se e solo se $\Gamma \models \varphi$. Infatti $\text{Mod}(\Gamma, \neg\varphi) = \text{Mod}(\Gamma) \cap \text{Mod}(\neg\varphi) = \text{Mod}(\Gamma) \setminus \text{Mod}(\varphi)$ e quest'ultimo è vuoto se e solo se $\text{Mod}(\Gamma) \subseteq \text{Mod}(\varphi)$.

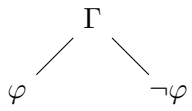
Questi due sistemi sono equivalenti, e di questo fatto ci sono due dimostrazioni. Una consiste nel mostrare la completezza della deduzione naturale, cioè che $\Gamma \underset{\text{DN}}{\vdash} \varphi \Leftrightarrow \Gamma \models \varphi$, e la completezza del sistema dei tableaux, cioè che $\Gamma \underset{\text{TAB}}{\vdash} \bot \Leftrightarrow \text{Mod}(\Gamma) = \emptyset$.

Differenza importante: quando uso i tableaux, nei rami compaiono solo sottoformule delle formule che ci sono sopra (anche eventualmente usando la sostituzione dei termini). Questo non succede nella deduzione naturale, ed è per questo che con essa è più difficile fare delle dimostrazioni, ma allo stesso tempo la rende più potente.

Definizione 7.1. $\Gamma \underset{\text{TAB}}{\vdash} \varphi$ vuol dire $\Gamma, \neg\varphi \underset{\text{TAB}}{\vdash} \bot$.

Teorema 7.2. $\Gamma \underset{\text{TAB}}{\vdash} \varphi \Leftrightarrow \Gamma \underset{\text{DN}}{\vdash} \varphi$

Come dicevamo poco sopra, possiamo dimostrare questo teorema passando per la semantica, cioè dimostando il Teorema di Completezza per entrambi i sistemi, ottenendo quindi $\Gamma \underset{\text{TAB}}{\vdash} \varphi \Leftrightarrow \Gamma \underset{\text{DN}}{\vdash} \varphi \Leftrightarrow \Gamma \models \varphi$. Un modo alternativo è per dimostrare questo teorema è usare i tableaux con la nuova regola



Questo serve per poter affrontare la questione della differenza importante fra i due sistemi.

In realtà i due sistemi sono equivalenti anche senza questa regola aggiuntiva (infatti come abbiamo detto si può dimostrare passando dalle completezze), però è difficile dimostrarlo senza passare per la semantica. Per farlo serve questo

Lemma 7.3. $(\Gamma, \varphi \underset{\text{TAB}}{\vdash} \bot) \wedge (\Gamma, \neg\varphi \underset{\text{TAB}}{\vdash} \bot) \Rightarrow \Gamma \underset{\text{TAB}}{\vdash} \bot$

Diamo ora le regole per l'=. Quelle per la deduzione naturale sono

- $\dfrac{\Gamma \vdash t_1 = t_2 \quad \Gamma \vdash (\varphi(t_1/x))}{\Gamma \vdash \varphi(t_2/x)}$ t_1, t_2 sostituibili
- $\Gamma \vdash t = t$

Per i tableaux invece

- $$\begin{array}{c} \Gamma, t_1 = t_2, \varphi(t_1/x) \\ | \\ \Gamma, t_1 = t_2, \varphi(t_1/x), \varphi(t_2/x) \end{array}$$
- $$\begin{array}{c} \Gamma \\ | \\ \Gamma, t = t \end{array}$$

Osserviamo che non abbiamo introdotto nessuna regola per la transitività di $=$, perché questa si può dimostrare dalla sostituibilità.

Esercizio 7.4. $\Gamma, x = y, y = z \vdash x = z$

Dimostrazione.

$$\frac{\Gamma, x = y, y = z \vdash x = y \quad \Gamma, x = y, y = z \vdash \overbrace{y = z}^{\varphi(y)}}{\Gamma, x = y, y = z \vdash \underbrace{\varphi(x)}_{x=z}}$$

□

7.1 Teoria Q di Robinson

Il linguaggio di questa teoria è $L = \{0, s, +, \cdot\}$, gli assiomi sono

1. $\forall x \, \neg(0 = s(x))$
2. $\forall x \forall y \, (s(x) = s(y) \to x = y)$
3. $\forall y \, \big(\neg(y = 0) \to \exists x(s(x) = y)\big)$
4. $\forall x \, (x + 0 = x)$
5. $\forall x \forall y \, (x + s(y) = s(x + y))$
6. $\forall x \, (x \cdot 0 = 0)$
7. $\forall x \forall y \, (x \cdot s(y) = x \cdot y + x)$

Consideriamo in questa teoria le L-formule

- $P(x) = \exists y(y + y = x)$
- $D(x) = \exists y(y + y + 1 = x)$

Voglio far vedere che $Q \nvdash \forall x\ (P(x) \vee D(x))$, cioè questa teoria non dimostra che ogni numero è pari o dispari.

Dimostrazione. Costruisco un modello di Q che non è un modello di φ. Consideriamo dunque l'insieme $\mathbb{Z}[t]^{\geq 0} = \left\{\sum_{i=0}^{n} a_i t^i \mid a_n > 0\right\} \cup \{0\}$. Questo soddisfa gli assiomi di Q e quindi è un suo modello. Tuttavia t non è pari nè dispari. □

Diciamo che Q non è *categorica*.

Definizione 7.5. Una teoria Q si dice *categorica* se ha un unico modello a meno di isomorfismi,

dove un isomorfismo di modelli è una bigezione fra i due domini e le due interpretazioni dei simboli che funziona come ci si aspetta.

Oltre a non essere categorica, Q non è neanche completa.

Definizione 7.6. Una teoria T è *completa* quando data una qualsiasi L-formula chiusa φ, si ha $T \vdash \varphi$ oppure $T \vdash \neg\varphi$, e inoltre T è coerente, cioè $T \nvdash \bot$.

Osserviamo che una teoria incoerente dimostra tutto. Questo si vede sia sintatticamente

$$\dfrac{\dfrac{\Gamma \vdash \bot}{\Gamma, \neg\varphi \vdash \bot}}{\Gamma \vdash \varphi}$$

che semanticamente

$$\Gamma \models \bot \Leftrightarrow \mathrm{Mod}(\Gamma) = \emptyset$$

e il vuoto è contenuto ovunque.

Dunque Q non è completa, perché nel modello $\mathbb{N}$ la formula $\forall x(P(x) \vee D(x))$ è valida.

7.2 Sottostrutture e morfismi

Alternativamente, possiamo dire che una teoria T è completa se e solo se $\forall M, N \models T$ si ha $M \equiv N$, cioè per ogni formula chiusa φ vale $\varphi^M = \varphi^N$.

Esercizio 7.7. Dimostrare l'equivalenza con l'altra definizione.

Esercizio 8. Se due modelli sono isomorfi, allora sono equivalenti, ma non è vero il viceversa.

$$M \cong N \underset{\not\Leftarrow}{\Rightarrow} M \equiv N$$

dunque T categorica $\Rightarrow T$ completa.

Definizione 7.9. $f : M \to N$ biunivoca si dice un *isomorfismo di L-strutture* se per ogni formula atomica $\varphi = \varphi(x_1, \ldots, x_n)$ si ha

$$M \models \varphi(a_1, \ldots, a_n) \Leftrightarrow N \models \varphi(f(a_1), \ldots, f(a_n))$$

questo modo di definire l'isomorfismo è equivalente a quello fatto simbolo per simbolo.

Definizione 7.10. $f : M \to N$ è un *morfismo* se per ogni φ atomica $M \models \varphi(a_1, \ldots, a_n) \Rightarrow N \models \varphi(f(a_1), \ldots, f(a_n))$ (o alternativamente se conserva funzioni, relazioni e costanti).

Definizione 7.11. M è una *sottostruttura* di N se $\mathrm{dom}(M) \subseteq \mathrm{dom}(N)$ e la funzione inclusione è un isomorfismo sull'immagine.

Esempio 7.12. $(\mathbb{Z}, +, \cdot) \hookrightarrow (\mathbb{R}, +, \cdot)$ è un morfismo (infatti non è biunivoca), però è vero che per la storia delle formule atomiche vale il se e solo se. Per quelle non atomiche non è detto, ad esempio $\exists x(x + x = 1)$ è vera in $\mathbb{R}$ e falsa in $\mathbb{Z}$.

Teorema 7.13. Se $f : M \to N$ è un isomorfismo, allora per ogni formula $\varphi = \varphi(x_1, \ldots, x_n)$ e per ogni $a_1, \ldots, a_n \in M$ si ha

$$M \models \varphi(a_1, \ldots, a_n) \Leftrightarrow N \models \varphi(f(a_1), \ldots, f(a_n))$$

Dimostrazione. Per induzione sulla struttura di φ. Il fatto che sia bigettiva serve a dimostrare questo teorema per i quantificatori. □

Corollario 7.14. Se φ è chiusa ed f è un isomorfismo $M \models \varphi \Leftrightarrow N \models \varphi$.

(per dimostrarlo era necessario prima dimostrarlo coi parametri)

Esempio 7.15. $(\mathbb{R}, <) \overset{?}{\equiv} (\mathbb{Z}, <)$ No, una formula che distingue questi due modelli è

$$\forall x \forall y(x < y \to \exists z(x < z < y))$$

che è vera in $\mathbb{R}$ ma non in $\mathbb{Z}$. Però, al prim'ordine, vale $(\mathbb{R}, <) \equiv (\mathbb{Q}, <)$, ma non al second'ordine (la proprietà del sup è del second'ordine). Tuttavia, pur essendo equivalenti, questi non sono isomorfi.

Diamo una definizione alternativa di sottostruttura:

Definizione 7.16. $M \subseteq N$ è una sottostruttura se $\mathrm{dom}\, M \subseteq \mathrm{dom}\, N$ e

- $\forall c$ costante $c^M = c^N \in M$
- $\forall f$ funzione, $\forall a_1, \ldots, a_n \in M$ $f^N(a_1, \ldots, a_n) = f^M(a_1, \ldots, a_n) \in M$

Data una struttura N e un sottinsieme $A \subseteq \mathrm{dom}\, N$, se A contiene le interpretazioni (in N) delle costanti ed è chiuso rispetto alle funzioni di N, allora esiste un'unica L-struttura $M \subseteq N$ tale che M è una sottostruttura di N e $\mathrm{dom}(M) = A$.

7.3 Assiomi di Peano

Al primo ordine ($PA^{(1)}$), ci sono gli assiomi di Q e per ogni formula $\varphi = \varphi(x, \vec{y})$ c'è l'assioma

$$\forall \vec{y}\Big[\varphi(0,\vec{y}) \wedge \forall n\big(\varphi(n,\vec{y}) \to \varphi(s(n),\vec{y})\big) \to \forall n \varphi(n,\vec{y})\Big] \tag{30}$$

Esercizio 7.17. $(PA)^{(1)} \vdash \forall x(P(x) \vee Q(x))$

Vedremo che $PA^{(1)}$ non è categorica, e anzi non è nemmeno completa. Curiosità: $PA^{(2)}$ è categorica, però in $PA^{(2)}$ non esistono le dimostrazioni.

8 25/10/12

Supponendo di avere a disposizione il Teorema di Completezza (delle regole), un suo corollario è il

Teorema 8.1 (di Compattezza)**.** $T \models \varphi \Rightarrow \exists T' \subset T$, T' finito, tale che $T' \models \varphi$

Dimostrazione. Ovvio per $\vdash$. □

Consideriamo la teoria T dei campi coi soliti assiomi. T non è completa (parliamo in questo caso di completezza come teoria, non come regole), ad esempio non dimostra $1 + 1 = 0$ nè $1 + 1 \neq 0$. Potrei volerla completare, ad esempio aggiungendo l'assioma che ogni polinomio di grado positivo ha uno zero (non posso quantificare sui polinomi quindi metto un assioma per ogni n, con n grado del polinomio). (Teoria ACF, Algebraic Closed Fields).

Non è ancora completa, chiaramente. Se aggiungo anche l'assioma che la caratteristica sia 0 ottengo ACF_0, che questa volta è completa.

Se una formula φ è chiusa, ho $ACF_0 \vdash \varphi \Rightarrow \mathbb{C} \models \varphi$ oppure $ACF_0 \vdash \neg\varphi \Rightarrow \mathbb{C} \models \neg\varphi$, inoltre per completezza $ACF_0 \nvdash \varphi \Rightarrow ACF_0 \vdash \neg\varphi$. Quindi $ACF_0 \vdash \varphi \Leftrightarrow \mathbb{C} \models \varphi$.

Osserviamo che $ACF_0 \vdash \varphi \Rightarrow \exists n$ tale che φ è vera in tutti i campi algebricamente chiusi di caratteristica 0 oppure $p \geq n$. Questo è vero per compattezza, perché ho usato solo un numero finito di assiomi, e gli assiomi di caratteristica ($\sum_{i=1}^{p} 1 \neq 0$) sono infiniti.

Teorema 8.2 (Forma equivalente della compattezza)**.** Se T è una L-teoria e $\forall T' \subset T$ finito T' ha un modello $M_{T'}$, allora $\exists M$ $M \models T$.

Dimostrazione. Se T non ha modelli, $T \models \perp$, cioè $\mathrm{Mod}(T) \subseteq \mathrm{Mod}(\perp) = \emptyset$, per completezza $T \vdash \perp$ e per compatteza $\exists T' \subseteq T$ tale che $T' \vdash \perp$, quindi sempre per completezza $T' \models \perp$ e quindi $\mathrm{Mod}\, T' = \emptyset$. □

Definizione 8.3. Se $L \subseteq L'$, ed M è una L'-struttura, la *restrizione* $M_{|L}$ è una L-struttura con $\mathrm{dom}(M) = \mathrm{dom}(M_{|L})$ e $\forall R \in L \quad R^{M_{|L}} = R^M$.

Se φ è una L-formula, allora $M \models \varphi \Leftrightarrow M_{|L} \models \varphi$.

Corollario 8.4. PA^1 ha modelli non isomorfi a $\mathbb{N}$.

Dimostrazione. Prendiamo $PA^{(1)}$ estesa con una costante c e con gli assiomi (infiniti) $c \neq 0, c \neq s(0), c \neq s(s(0)) \ldots$. Chiamiamo questa teoria T e chiediamoci se ha un modello. Sì per compattezza basta verificare sui sottoinsiemi finiti degli assiomi, e i naturali standard fanno da modello per ognuno di questi (interpretando c a dovere). Sia M un modello di T. M ristretta al linguaggio di $PA^{(1)}$ (cioè "tolgo il nome" alla costante c) *non* è isomorfo ai numeri naturali, perché un eventuale isomorfismo non può mandare c da nessuna parte (deve commutare, fra le altre cose, col successore). □

Un modello non standard (cioè non isomorfo a $\mathbb{N}$) di $PA^{(1)}$ non può essere ad esempio $\mathbb{N} \cup \{c\}$, perché c deve avere successore e predecessore, e in genere vengono fuori anche cose piuttosto brutte. Un modello può essere $\mathbb{N} \cup (\mathbb{Z} \times \mathbb{Q})$, con le interpretazioni adeguate. Si riesce a dimostrare che il $+$ e il $\cdot$ devono per forza essere abbastsanza complicate da non essere calcolabili.

Dato un modello $M \models Q$ esiste sempre un morfismo $f : \mathbb{N} \to M$ iniettivo, quello definito mandando lo 0 nello 0 e chiedendo la stabilità per successore. L'unico punto delicato è quando devo verificare che $+$ e $\cdot$ si comportano bene. Quello che so su $\mathbb{N}$ è che è un modello di $PA^{(2)}$, quindi uso l'induzione del secondo ordine (cioè che ogni sottoinsieme che contiene le 0 ed è chiuso per successore è tutto $\mathbb{N}$). L'iniettività è una verifica.

Teorema 8.5. Esiste un unico modello di $PA^{(2)}$ a meno di isomorfismi.

Dimostrazione. $\mathbb{N}$ è un modello. Se M è un altro modello, dato che so già che la $f : \mathbb{N} \to M$ definita sopra è iniettiva, mi basta dimostrarne la surgettività. Sia P l'immagine di f. Questo contiene lo 0 ed è chiuso per successore ed è quindi tutto, e questo conclude. □

Per fare le cose ammodino usando ZFC come metateoria devo ovviamente usare il Teorema di Ricorsione per definire f.

Teorema 8.6. Non esistono regole di deduzione $\mathcal{R}^2$ tali che $T \underset{\mathcal{R}^2}{\vdash} \varphi \Leftrightarrow T \models \varphi$, con T teoria del second'ordine.

Dimostrazione. Segue dal fatto che non vale il teorema di compattezza. Facciamo vedere che il teorema fallisce sulla L-teoria

$$T = PA^{(2)} + \{c \neq 0, c \neq s(0), \ldots\}$$

dove $L = \{0, s, +, \cdot, c\}$. Ogni sottoinsieme finito degli assiomi ha $\mathbb{N}$ come modello, ma tutta la teoria non ne ha perché dovrebbe essere isomorfo a $\mathbb{N}$ e in $\mathbb{N}$ non so dove mettere c (si scrive bene supponendo che esista f isomorfismo, ...). □

Il problema sotto è che se quantifico sulle formule non è detto che la complessità cali quando istanzio le cose (vedremo meglio quando vedremo la dimostrazione del Teorema di Completezza).

9 26/10

Definizione 9.1. Se T è una L-teoria, diciamo che T è *finitamente soddisfacibile* se ogni sottoinsieme finito $T' \subseteq T$ ha un modello.

Il Teorema di Compattezza in una delle sue forme (Teorema 8.2) afferma che se una teoria è finitamente soddisfacibile, allora è soddisfacibile (e il viceversa è ovvio).

Consideriamo un grafo, ossia considero il linguaggio $L = \{E\}$, dove E è un simbolo di relazione binaria, e un grafo G è una L-struttura $G = (V, E^G)$, dove $V = \operatorname{dom} G$ è l'insieme dei *vertici* e E^G è un sottoinsieme $E^G \subseteq V \times V$, i cui elementi sono detti *spigoli*. Concentriamoci sui grafi *non orientati* e *senza loop*, aggiungendo gli assiomi

1. $\forall xy(\mathrm{E}(x, y) \leftrightarrow \mathrm{E}(y, x))$
2. $\forall x \neg \mathrm{E}(x, x)$

(tutto ciò si può anche fare usando due domini, vertici e spigoli, e le funzioni source e target che ad uno spigolo associano rispettivamente il primo e il secondo vertice)

Ora ci chiediamo se un grafo non orientato senza loop $G = (V, E^G)$ è 4-colorabile, ossia se esiste $C : V \to \{1, 2, 3, 4\}$ tale che $\forall x, y \in V(\mathrm{E}(x, y) \leftrightarrow C(x) \neq C(y))$.

Teorema 9.2. Se ogni sottografo finito di G è 4-colorabile, anche G lo è.

Dimostrazione. L'idea è trovare una teoria i cui modelli siano le colorazioni e usare il Teorema di Compattezza. Mettiamoci nel linguaggio

$$L = \{E, P_1, P_2, P_3, P_4\}$$

con P_i predicato 1-ario che significa $P_i(x) \Leftrightarrow C(x) = i$, e usiamo la teoria T_C i cui assiomi sono

1. $\forall x \left(\bigvee_{i=1}^{4} P_i(x) \right)$ (ogni vertice ha almeno un colore)
2. $\forall x \left(P_i(x) \to \bigwedge_{j \neq i} \neg P_j(x) \right)$ (ogni vertice ha al più un colore)
3. $\forall x, y \, (\mathrm{E}(x, y) \to (P_i(x) \to \neg P_i(y)))$ (vertici adiacenti non hanno lo stesso colore)

dove gli ultimi due sono intesi da replicarsi per ogni i (uno per colore).

Un modello di questa teoria è un grafo colorato, infatti se $M \models T_C$ $M = (V, E^M, P_1^M, \ldots, P_4^M)$ posso ricavare la colorazione

$$C : V \to \{1, 2, 3, 4\} \quad C(x) = i \Leftrightarrow x \in P_i^M$$

e viceversa.

Fissiamo ora un particolare grafo $G = (\mathbb{N}, E^G)$ e supponiamo che sia finitamente 4-colorabile. Consideriamo poi il linguaggio $L = \{E, P_1, \ldots, P_n, \underline{0}, \underline{1}, \underline{2}, \ldots\}$ e la L-teoria T_G i cui assiomi sono quelli di T_C più

1. $\{\mathrm{E}(\underline{i}, \underline{j}) \mid (i, j) \in E^G\}$
2. $\{\neg\, \mathrm{E}(\underline{i}, \underline{j}) \mid (i, j) \notin E^G\}$
3. $\{\underline{i} \neq \underline{j} \mid i \neq j\}$

Chi sono i modelli di questa teoria T_G? Sicuramente, se G è 4-colorabile, $G \models T_G$ e se $M \models T_G$, allora $G \subseteq M$ come sottografo (ossia come sottostruttura) con l'inclusione $G \hookrightarrow M \;\; i \mapsto (\underline{i})^M$. Se T_G ha un modello M, G è una sottostruttura di M.

Ma ora noi mostriamo che T_G è soddisfacibile! Infatti, se consideriamo un sottoinsieme finito di assiomi, questo menzionerà solo finiti $\underline{0}, \ldots \underline{n}$. Quindi come modello di $T \subseteq T_G$ (T finito) fisso una colorazione C per il sottografo limitato ai vertici $0, \ldots, n$. Dunque ho

$$(G_{|\{1,\ldots,n\}}, C) \models T$$

Abbiamo mostrato che T_G è finitamente soddisfacibile, e quindi soddisfacibile per compattezza, quindi ha un modello, e per quanto detto prima questo conclude. □

Esercizio 9.3. Provare a dimostrarlo a mano (la cosa si basa sul Lemma di König e sul Teorema di Completezza).

9.1 Hao Wang

Sono delle tessere quadrate colorate divise in quattro settori (un colore per lato). Abbiamo un numero *finito* di tipi di piastrelle, ma un numero infinito di piastrelle di ciascun tipo. Vogliamo pavimentare tutto il piano, e posso affiancare due piastrelle solo se i lati su cui si toccano hanno lo stesso colore (non posso ruotarle).

Teorema 9.4. Se posso ricoprire tutto un quadrante, posso ricoprire tutto il piano.

Nel caso con un numero infinito di tipi esiste un controesempio.

Esercizio 9.5. Dimostrare il Teorema precedente usando la compattezza.

Hint: Bisogna dimostrare che il piano è finitamente ricopribile, ma questo si deduce dal fatto che posso ricoprire i quadranti.

Diamone comunque un'altra

Dimostrazione. Supponiamo di poter ricoprire il quadrante, e costruiamo un albero che ha in cima il piano vuoto e il padre è la parte centrale dei figli. In questo albero può capitare che a un certo punto qualcuno non abbia figli.

La prima cosa che notiamo è che questo albero ha infiniti nodi (perché possiamo ricoprire un quadrante per ipotesi). Inoltre ogni nodo ha un numero finito di figli (perché c'è un numero finito di tipi). Per il Lemma di König esiste un ramo infinito. L'unione di questo ramo infinito ricopre tutto il piano. □

Bisogna ora dimostrare il

Lemma 9.6 (di König)**.** Se in un albero infinito ogni nodo ha un numero finito di figli, allora esiste un ramo infinito.

Dimostrazione. Definiamo induttivamente il ramo. $x_0 = *$ (radice). x_0 ha infiniti discendenti ma finiti figli, quindi uno dei figli ha infiniti discendenti. Sia x_1 uno di tali figli (eccetera). □

Spoiler: per dimostrare il Teorema di Completezza applicheremo il Lemma di Konig ad un albero di Tableaux.

9.2 Classi di strutture

Definizione 9.7. Se K è una classe di L-strutture, diciamo che K è *elementare* se esiste una L-teoria T tale che $K = \{\text{Modelli di } T\}$.

Una classe chiusa per isomorfismo non necessariamente è elementare, un controesempio è $K = \{\text{grafi connessi}\}$, che non è elementare perché al prim'ordine non è possibile assiomatizzare la connessione di un grafo.

Definizione 9.8. $G = (V, E^G)$ è *sconnesso* se verifica il seguente assioma del second'ordine.

$$\exists A, B \subseteq V \; A \cap B = \emptyset, \; A \cup B = V \; \forall x \in A, \; \forall y \in B \neg \, \mathrm{E}(x, y)$$

Equivalentemente G è connesso se $\forall a, b \in V \exists n \in \mathbb{N} \; \exists (x_0, \ldots, x_n), x_0 = a, a_n = b$ tali che $\forall 0 \leq i \leq n \, \mathrm{E}(x_i, x_{i+1})$. Anche questo è un enunciato del second'ordine perché sto quantificando su successioni finite di elementi del dominio.

Dimostriamo che K non è elementare.

Dimostrazione. Supponiamo per assurdo che esista una L-teoria T tale che $\{\text{Grafi connessi}\} = \{\text{Modelli di } T\}$. Sia $L^* = \{E, a, b\}$ e applichiamo il Teorema di Compattezza alla L^*-teoria

$$T^* = T \cup \{a \neq b, \neg \,\mathrm{E}(a,b), \neg\exists x(\mathrm{E}(a,x) \wedge \mathrm{E}(x,b)), \ldots\}$$

Per scriverlo meglio definiamo $\varphi_n(a,b)$ nel modo ovvio e scriviamo

$$T^* = T \cup \{\neg\varphi_n(a,b) \mid n \in \mathbb{N}\}$$

Ora T^* è finitamente soddisfacibile, infatti basta un grafo lineare sufficientemente lungo. Il problema è che se $M \models T^*$, M ristretto al linguaggio dei grafi risulta sconnesso. Infatti a^M e b^M non sono collegabili da un cammino finito. Però dovrebbe allo stesso tempo soddisfare T, ma non può proprio perché è sconnesso. Abbiamo ottenuto un assurdo. □

Definizione 9.9. Data una classe di strutture K, definiamo la *teoria di* K

$$\mathrm{Th}(K) = \{\varphi \mid \forall M \in K \quad M \models \varphi\}$$

Ad esempio $\mathrm{Th}(\{\text{Grafi connessi}\}) = \{\varphi \mid \varphi \text{ è vera in ogni grafo connesso}\}$.
Per quanto abbiamo dimostrato poco fa, possiamo dire che

$$\{\text{Grafi connessi}\} \subsetneq \mathrm{Mod}(\mathrm{Th}(\{\text{Grafi connessi}\}))$$

dunque esistono modelli che non sono grafi connessi che però verificano tutto ciò che è verificato dai grafi connessi. Un esempio di formula che sta in $\mathrm{Th}(\{\text{Grafi connessi}\})$ è (FORSE È SBAGLIATA, DA RIVEDERE)

$$\varphi = \neg\exists x, y\,(\forall z(z \neq x \wedge z \neq y) \to \neg\,\mathrm{E}(z,y))$$

Un grafo unione disgiunta di due grafi lineari infiniti è un modello di $\mathrm{Th}(\{\text{Grafi connessi}\})$ pur non essendo connesso. Un'altra cosa spiacevole che accade è che

$$\{\text{Gruppi finiti}\} \subsetneq \mathrm{Mod}(\mathrm{Th}(\{\text{Gruppi finiti}\}))$$

questo ci dà un altro esempio di classe non elementare e succede perché

Dimostrazione. Se T è la teoria dei gruppi finiti e $K = \mathrm{Mod}(T)$, basta considerare

$$T^* = T \cup \{\exists xy(x \neq y), \exists x, y, z(x \neq y \wedge y \neq z \wedge x \neq z), \ldots\}$$

ottenendo come prima un assurdo dal fatto che se suppongo K elementare T^* è finitamente soddisfacibile, ma non ha un modello. □

10 8/11

Nei tableaux il padre ha un modello se e solo se almeno uno dei figli ha un modello. Nel caso proposizionale l'albero è sempre finito e quindi è facile (segue esempio con $A \oplus B \leftrightarrow A$, dove $\oplus$ è lo XOR).

Definizione 10.1. Diciamo che φ *giustifica* ψ se in un tableau φ è figlio di ψ (in particolare le formule atomiche si giustificano da sole).

Definizione 10.2. Σ insieme di formule è un *insieme di Hintikka* se è chiuso per giustificazione (nel senso che se contiene una formula contiene *una* sua giustificazione) e non contiene sia φ che $\neg\varphi$.

Teorema 10.3. Nel caso proposizionale, ogni insieme di Hintikka ha un modello $v : \{\text{variabili proposizionali}\} \to \{0, 1\}$.

Dimostrazione. Si esplicita il modello.

$$v(A) = \begin{cases} 1 & \text{se} \quad A \in T \\ 0 & \text{se} \quad \neg A \in T \\ 1 & \quad \text{altrimenti} \end{cases}$$

e si fanno le verifiche (ovvie) per induzione. □

Teorema 10.4. Se Σ è finito e *tableaux-coerente*, cioè non esiste tableaux chiuso (che porta a tutte contraddizioni) con radice Σ, allora Σ è incluso in un insieme di Hintikka (e quindi ha un modello).

Dimostrazione. Faccio un tableaux con radice Σ finché non termina (nel caso proposizionale questo succede sempre). Per l'ipotesi di coerenza ho una foglia aperta. Se T è un ramo che la contiene, $T \supset \Sigma$ ed è di Hintikka. □

Abbiamo quindi dimostrato il Teorema di Completezza nel caso proposizionale.

Corollario 10.5. $\Sigma \underset{\text{Tab}}{\vdash} \varphi \Leftrightarrow \Sigma \models \varphi$, (cioè $\Sigma, \neg\varphi$ ha un Tableaux chiuso, se e solo se $\forall v(\Sigma^v = 1 \Rightarrow \varphi^v = 1)$).

Dimostrazione. Completezza: se $\Sigma \models \varphi$ e per assurdo $\Sigma \nvdash \varphi$, allora $\Sigma, \neg\varphi$ è un tableaux coerente, quindi per il teorema precedente esiste un modello che rende vere le ipotesi di Σ e falsa φ.

Correttezza: se $\Sigma \vdash \varphi$ si ha che (per induzione sulla profondità del Tableaux) $\Sigma, \neg\varphi$ non ha modelli, e quindi $\Sigma \models \varphi$. □

Nel caso predicativo il problema è che i tableaux non è detto che terminino.

Definizione 10.6. Una L-teoria T è *di Hintikka* in L se per ogni $\varphi \in T$ esiste $\Lambda \subseteq T$ tale che Λ giustifica φ. Se c'è il simbolo di uguaglianza bisogna aggiungere le clausole che contiene tutti i $t = t$ al variare di t fra i termini e che se contiene $a = b$ e $\varphi(a)$ contiene anche $\varphi(b)$ (e simmetricamente).

Ovviamente cambia il concetto di giustificazione. Per giustificare $\exists x\varphi(x)$ mi basta $\varphi(t/x)$, con t termine chiuso di L. Per giustificare $\forall x\varphi(x)$ servono tutti i $\varphi(t/x)$ al variare di t fra gli L-termini chiusi (quindi T per essere di Hintikka, se contiene un $\forall$ deve contenerne *tutte* le istanze).

Attenzione: è importante che il linguaggio sia fissato. Ad esempio se $L = \{P, a\}$ ed $L' = \{P, a, b,\}$, si ha che $\Sigma = \{\forall x P(x), P(a)\}$ è di Hintikka per L ma non per L'.

Segue esempio di tableaux con la formula $\forall x \exists y[R(x, y) \vee R(y, x)]$ sul linguaggio $L = \{R, a\} \subset L'$ (in L' aggiungo le costanti datemi ogni tot rami dal $\exists$). Se prendo un ramo infinito ottengo un insieme di Hintikka.

11 9/11

Diamo, questa volta ammodino, la

Definizione 11.1. Un insieme T di L-formule è *di Hintikka* se

1. $\varphi \in T \Rightarrow \neg\varphi \notin T$
2. $\neg\neg\varphi \in T \Rightarrow \varphi \in T$
3. $\varphi \wedge \psi \in T \Rightarrow \varphi \in T, \psi \in T$
4. $\neg(\varphi \wedge \psi) \in T \Rightarrow \neg\varphi \in T$ oppure $\neg\psi \in T$
5. $\varphi \vee \psi \in T \Rightarrow \varphi \in T$ oppure $\psi \in T$
6. $\neg(\varphi \vee \psi) \in T \Rightarrow \neg\varphi \in T, \neg\psi \in T$
7. $\varphi \to \psi \in T \Rightarrow \neg\varphi \in T$ oppure $\psi \in T$
8. $\neg(\varphi \to \psi) \in T \Rightarrow \varphi \in T, \neg\psi \in T$
9. $\exists x\varphi \in T \Rightarrow$ esiste un termine chiuso t tale che $\varphi(t) \in T$
10. $\forall x\varphi \in T \Rightarrow$ per tutti gli L-termini chiusi t $\varphi(t) \in T$
11. $\neg\exists x\varphi \in T \Rightarrow$ per tutti gli L-termini chiusi t $\neg\varphi(t) \in T$
12. $\neg\forall x\varphi \in T \Rightarrow$ esiste un L-termine chiuso t tale che $\neg\varphi(t) \in T$

Se c'è anche l'uguaglianza, bisogna aggiungere anche

13. $(t = t) \in T$ per ogni L-termine chiuso t

14. $(t = t'), \varphi(t) \in T \Leftrightarrow \varphi(t') \in T$

Esercizio 11.2. Da 13 e 14 segue la transitività.

Definizione 11.3. Una L-struttura M è *ricca* se $\forall a \in M\ \exists t \in L_0\ a = t^M$, dove L_0 è l'insieme degli L-termini chiusi.

Esempio 11.4.

- $(\mathbb{R}, +, \cdot, 0, 1)$ non è ricca per il linguaggio $L = \{0, 1, +, \cdot\}$
- $(\mathbb{N}, +, \cdot, 0, 1)$ è ricca (per ogni naturale c'è un termine)
- $(\mathbb{N}, <)$ non è ricca

Il vantaggio delle strutture ricche è in tal caso vale

$$M \models \forall x \varphi(x) \Leftrightarrow \forall t \in L_0\ M \models \varphi(t) \tag{31}$$

mentre per strutture in generale vale solo il $\Rightarrow$.

Teorema 11.5. Se T è un insieme di Hintikka, T ha un modello ricco.

Dimostrazione. Se la teoria è senza $=$, sceglo $\mathrm{dom}(M) = L_0$. Se c'è prendo $\mathrm{dom}(M) = {}^{L_0}\!/\!_{\sim}$, dove $t \sim t' \overset{\text{def}}{\Leftrightarrow} t = t' \in T$. Il modello ${}^{L_0}\!/\!_{\sim}$ è detto *modello dei termini*. Un tipico elemento di questo dominio si scrive $[t] \in \mathrm{dom}(M)$ (notiamo che i termini 1 e $0 + 1$ sono nella stessa classe di equivalenza per $\mathrm{Th}(\mathbb{N})$). Ora vediamo come interpretare i simboli (a patto di verificare la buona definizione di quanto segue):

- Se $c \in L$ è una costante, $c^M = [c] \in \mathrm{dom}(M)$
- Se $f \in L$ è una funzione, $f^M([t_1], \ldots, [t_n]) = [f(t_1, \ldots, t_n)] \in \mathrm{dom}(M)$
- Se $P \in L$ è un predicato, $P^M = \{([t_1], \ldots, [t_n]) \in \mathrm{dom}(M)^n \mid P(t_1, \ldots, t_n) \in T\}$

Quest'ultima cosa fa sì che $P(t_1, \ldots, t_n) \in T \Leftrightarrow P^M([t_1], \ldots, [t_n])$. Chiamiamo M_T questo modello dei termini. Verifico che se T è di Hintikka, allora $M_T \models T$, cioè $\varphi \in T \Rightarrow M_T \models \varphi$. È abbastanza chiaro (induzione sulla lunghezza del termine) che se t è un termine chiuso, $t^M = [t]$.

- Se φ è una formula atomica

$$M \models (t_1 = t_2) \overset{\text{Tarski}}{\Longleftrightarrow} t_1^M = t_2^M \Leftrightarrow [t_1] = [t_2] \Leftrightarrow (t_1 = t_2) \in T$$

-

$$M \models P(t_1, \ldots, t_n) \Leftrightarrow P^M(t_1^M, \ldots, t_n^M) \Leftrightarrow P^M([t_1], \ldots, [t_n]) \Leftrightarrow P(t_1, \ldots, t_n) \in T$$

Dunque abbiamo mostrato che se $\varphi \in T$ è atomica, allora $M_T \models \varphi$. Se $\varphi = \neg\psi \in T$, con ψ atomica, allora $\psi \notin T$, quindi per quanto appena mostrato $M_T \not\models \psi$ e allora $M_T \models \neg\psi$. Vediamo altre formule:

$$\forall x\varphi(x) \in T \Rightarrow \forall t \in L_0\ \varphi(t) \in T \xRightarrow{\text{induzione}} M_T \models \varphi(t) \xRightarrow{M_T \text{ ricca}} M_T \models \forall x\varphi(x)$$

Questo era il punto delicato, dove si usa la ricchezza, gli altri sono facili. □

Da questo Teorema segue in particolare che ZF ha un modello numerabile.

Esempio 11.6. Sia M una L-struttura ricca. Prendo come insieme di Hintikka la teoria di quella struttura

$$T = \mathrm{Th}(M) = \{\varphi \mid M \models \varphi\}$$

Questo è un insieme di Hintikka. L'ipotesi che M sia ricca è necessaria, infatti se $M \models \exists x\varphi(x)$ allora esiste $a \in M$ tale che $M \models \varphi(a)$, e solo se M è ricca esiste un L-termine chiuso t tale che $t^M = a$, e quindi $M \models \varphi(t)$.

Esempio 11.7. $PA \subseteq T = \mathrm{Th}(\mathbb{N}, +, \cdot, 0, 1)$. Anche questa T è di Hintikka, poiché questa struttura è ricca (occhio che $T \neq PA^2$).

Teorema 11.8. Se una teoria finita T è tableaux-coerente, allora T è un sottoinsieme di un insieme di Hintikka.

Dimostrazione. Una maniera per provare a dimostrarlo potrebbe essere fare un tableau con radice T, poi prendere un ramo massimale (non chiuso), dopo aver portato a termine il tableau finché possibile. L'unione delle formule del ramo è di Hintikka. In realtà non funziona perché potrei avere situazioni del tipo: c'è un $\forall$ e una cosa come $\varphi \wedge \psi$. Se mi incaponisco col $\forall$, potrei finire per non spezzare mai $\varphi \wedge \psi$, e quindi fare casino. Quindi, nella dimostrazione, devo iniziare con "Faccio un tableau *giudiziosamente* con radice T".

Assumiamo L numerabile. In tal caso l'insieme delle L-formule è numerabile, quindi enumero le formule con un ordine $\{\varphi_n \mid n \in \mathbb{N}\}$ di tipo ω. Fare un tableaux *giudiziosamente* significa dare la priorità alle formule con numeri più bassi, quindi spezzando prima quelle con numeri più piccoli. Quindi, se non spezzo φ_n è perché sto spezzando φ_k con $k < n$. Però questo lo posso fare solo un numero finito di volte. Inoltre, se è il turno di $\forall x\varphi(x)$, produco la formula $\varphi(t)$ con indice più basso. A questo punto il ramo è di Hintikka per davvero. **Nota bene:** questo *giudiziosamente* non funziona molto bene, ha dei bug. Il concetto però è lo stesso, basta trovare un modo buono di fare il tableau per far sì che il ramo sia di Hintikka. Dovrebbe funzionare spezzare per prima la formula che, una volta spezzata, produce la formula di numero minimo.

Alla fine dovrò restringere il linguaggio (si è allargato con le costanti generate dall'$\exists$). □

Dato che i rami sono numerabili, L' sarà numerabile. Quindi il modello di T' è numerabile. Essendo questo anche un modello di T, T ha un modello numerabile.

Ora, se una teoria T ha un modello, allora è coerente. Se è coerente è contenuta in un insieme di Hintikka, e quindi T ha un modello numerabile (se il linguaggio non è più che numerabile).

Corollario 11.9. La $\mathrm{Th}(\mathbb{R}, +, \cdot, 0, 1) = \{\varphi \mid \mathbb{R} \models \varphi\}$ ha un modello numerabile.

(abbiamo un po' barato perché avevamo supposto la finitezza e qui invece è numerabile, ma torna)

Teorema 11.10. Se T è una teoria e se ogni sottoinsieme finito di T è tableaux-coerente, allora T ha un modello.

Forse questo teorema non ci aiuta. Però il corollario è vero: il modello è quello dei *numeri reali algebrici* (dovrebbe essere proprio il modello dei termini). Dunque non posso distinguere i numeri algebrici dai trascendenti usando solo formule del prim'ordine.

12 15/11

Teorema 12.1 (Paradosso di Skolem)**.** Se ZF è coerente, ha un modello numerabile.

Notiamo che stiamo usando ZF sia come teoria che come metateoria. Quando la usiamo come metateoria forse ci fa comodo togliere l'assioma dell'infinito, ma per ora sorvoliamo.

Un modello M di ZF è un dominio (non diciamo "insieme" per evitare di fare casino) con una relazione binaria $\underset{M}{\in}$ che verifica gli assiomi.

Esempio 12.2 (Modello di ZF senza l'assioma dell' infinito)**.** Prendiamo $M = \mathbb{N}$, $n \underset{M}{\in} k$ se e solo se $\exists a_1 < a_2 < \ldots < a_\ell$ con $K = 2^{a_1} \cdot \ldots \cdot 2^{a_\ell}$ ed n è uno degli a_i. L'unico k che non si esprime in questo modo è 0, quindi $\emptyset^M = 0$. Questo modello è isomorfo ad un modello con la "vera" appartenenza, cioè ad un modello M' in cui $\underset{M'}{\in}$ è la restrizione a $\mathrm{dom}(M')$ della $\in$ della metateoria. L'isomorfismo è

$$(\mathbb{N}, \underset{M}{\in}) = M \xrightarrow{f} V_\omega \qquad n \mapsto f(n) = \left\{ f(i) \mid i \underset{M}{\in} n \right\}$$

In questo modo $n \underset{M}{\in} k \Leftrightarrow f(n) \in f(k)$

Esempio 12.3. $(\mathbb{N}, <)$ *non* è un modello di ZF. Infatti salta l'assioma della coppia.

Definizione 12.4. Sia $L = \{\in\}$ con $\in$ simbolo di relazione binaria e $(M, \underset{M}{\in})$ una L-struttura. Diciamo che M è *ben fondato* se non esistono successioni infinite $\{a_n \mid n \in \mathbb{N}\}$ tali che $\forall n\ a_{n+1} \in a_n$ oppure equivalentemente (usando la scelta) se a è $\underset{M}{\in}$-minimale, cioè

$$\forall \emptyset \neq X \subseteq M\ \exists a \underbrace{\underset{M}{\in}}_{\text{vera}} X \quad \forall \mu \in X\ \mu \underset{M}{\notin} a$$

Chiediamoci ora se ogni modello è isomorfo ad un modello con la "vera" (nel senso prima specificato) appartenenza. Una parziale risposta è data dal

Teorema 12.5 (collasso di Mostowski)**.** Se $(M, \underset{M}{\in}) \models$ Estensionalità ed è ben fondato, allora esiste $f : (M, \underset{M}{\in}) \xrightarrow{\cong} (M', \in)$.

Dimostrazione. $f(a) = \left\{ f(b) \mid b \underset{M}{\in} a \right\}$, poi basta fare le verifiche; la buona fondazione serve per la buona definizione (che è ricorsiva, e quindi se ci sono catene infinite...). Poi prendo $M' = \mathrm{Im}(f)$. □

Chiediamoci: è vero che ogni modello $(M, \underset{M}{\in})$ di ZF è ben fondato? La risposta è *no*. In quanto modello di ZF, $(M, \underset{M}{\in}) \models$ Fondazione, cioè

$$\forall x \neq \emptyset\ \exists y \left((y \in x) \wedge (\forall z \in y \quad z \notin x) \right)$$

ma la buona fondazione "vera" significa

$$\forall X \subseteq M \quad X \neq \emptyset \Rightarrow \exists y \in X \big(\forall z \in X\ z \underset{M}{\notin} y \big)$$

Definizione 12.6. Un ordine lineare è un *buon ordine* se è ben fondato.

Proposizione 12.7. La classe K dei buoni ordini non è elementare: non esiste T tale che $K = \mathrm{Mod}(T)$ $(L(T) = \{<\})$.

Dimostrazione. Se per assurdo esistesse una tale T, prendiamo

$$L' = \{<, c_0, c_1, \ldots\} \qquad T^* = T \cup \{c_1 < c_0, c_1 < c_2, \ldots\}$$

T^* è finitamente soddisfacibile, e per compattezza ha quindi un modello $(M, \underset{M}{<}, c_0^M, c_1^M, \ldots) \models T$ e questo è assurdo perché in M c'è una successione infinita decrescente. □

Ricordiamo la

Definizione 12.8. α è un *ordinale* se

1. $\forall a, b \big(a \in b \in \alpha \to a \in \alpha \big)$

2. $(\alpha, \in)$ è ben ordinato

"α è un ordinale" si può scrivere come $\varphi(\alpha)$ formula del linguaggio $L = \{\in\}$ di ZF, e si può anche scrivere ω in una formula dello stesso linguaggio (minimo ordinale infinito (o diverso da $\emptyset$) senza predecessore). In generale, $\emptyset, \omega, \mathscr{P}(\omega), A \times B, \bigcup A$, sono *nozioni definite*, cioè ad esempio

$$ZF \vdash \varphi(\emptyset) \underset{\text{def}}{\Leftrightarrow} ZF \vdash \exists x\big(x = \emptyset \wedge \varphi(x)\big)$$

dove $x = \emptyset \Leftrightarrow \forall u(u \notin x)$.

A questo punto, dato $M \models \text{ZF}$, possiamo parlare di $\omega^M \in M$, cioè l'unico $b \in M$ tale che $M \models$"b è il minimo ordinale senza predecessore". Se $(M, \underset{M}{\in}) = (M, \in)$ ed M è transitivo, allora si riesce a vedere che $\omega^M = \omega$.

Definizione 12.9. M è un *ω-modello* di ZF se $(\omega^M, \underset{M}{\in}) \cong (\omega, \in)$.

Dato $M \models ZF$, consideriamo $f : \mathbb{N} \to M$ tale che $f(0) = \emptyset^M$, $f(n+1) = s^M(f(n))$. Esiste un modello M tale che $M \models (b \in \omega)$, e tuttavia $b \notin \text{Im}(f)$, cioè può esistere una successione vista da fuori $(a_n \mid n \in \mathbb{N})$, con $a_n \in M$, $a_n \underset{M}{\in} \omega^M$ e $\ldots, \underset{M}{\in} a_2 \underset{M}{\in} a_1 \underset{M}{\in} a_0, \ldots$, ma questa successione è diversa dall'estensione di b, per ogni $b \in M$.

È plausibile che esista un modello $(M, \in)$ transitivo ben fondato di ZF. Vedremo che dalla sua esistenza segue l'esistenza di un modello numerabile transitivo ben fondato. Questa cosa della numerabilità lascia un po' perplessi, perché $ZF \vdash \mathscr{P}(\omega)$ non sono numerabili, cioè $\neg\exists f : \omega \to \mathscr{P}(\omega)$ surgettiva. Quindi $(M, \in) \models \neg\exists f : \omega \to \mathscr{P}(\omega)$, ma non esiste *dentro* il modello. Da fuori magari posso benissimo numerare tutto (seguono le storie sul fatto che formule con quantificazione ristretta sono assolute). Il punto è che $\omega^M = \omega$, ma $\mathscr{P}(\omega)^M$ chi è?

$$M \models b = \mathscr{P}(\omega) \Leftrightarrow M \models \forall x\big(x \in b \leftrightarrow x \subseteq \omega\big) \Leftrightarrow \forall x \in M\ M \models \big(x \in b \leftrightarrow x \subseteq \omega\big)$$

L'oggetto che ci interessa è $b = \mathscr{P}(\omega) \cap M \subset M$, che è numerabile, ma da fuori. Esiste $g : \mathbb{N} \to b$, ma $g \notin M$.

13 16/11

Teorema 13.1 (Löweneheim-Skolem verso il basso)**.**

1. Se M è una L-struttura, ed $M \models T$, allora esiste una sottostruttura $N \subseteq M$ tale che $N \models T$ e $|N| \leq \max\{|L|, \aleph_0\}$.

2. Se $A \subseteq \text{dom}(M)$, esiste una L-struttura N tale che $A \subseteq N \subseteq M$, $N \models T$ e $|N| \leq |A| + \max\{|L|, \aleph_0\}$ (cioè possiamo richiedere che N contenga un certo sottoinsieme A).

Per enunciare meglio il punto 2 dobbiamo dare la seguente

Definizione 13.2. Diciamo che N è una *sottostruttura elementare* di M, e scriviamo $N \prec M$, se

1. N è una sottostruttura di M
2. Per ogni L formula $\varphi(x_1, \ldots, x_n)$ e per ogni $a_1, \ldots, a_n \in N$ si ha che $N \models \varphi(a_1, \ldots, a_n) \Leftrightarrow M \models \varphi(a_1, \ldots, a_n)$.

Esempio 13.3. Nel linguaggio degli ordini $(2\mathbb{Z}, <) \subseteq (\mathbb{Z}, <)$, ma *non* è una sottostruttura elementare. Infatti

$$\exists x(2 < x \wedge x < 4)$$

è vera in $\mathbb{Z}$ e falsa in $2\mathbb{Z}$, questo nonostante le due strutture siano isomorfe (ma questo non ci sorprende).

Esempio 13.4. $(\mathbb{Q}, <) \prec (\mathbb{R}, <)$, ma $(\mathbb{Q}, +, \cdot) \not\prec (\mathbb{R}, +, \cdot)$.

Possiamo così riformulare la 2 come

2. Se $A \subseteq \mathrm{dom}(M)$, $|L|, |A| \leq \lambda \leq |M|$, allora esiste $N \prec M$ tale che $A \subseteq \mathrm{dom}(N)$ e $|N| = \lambda$.

Esempio 13.5. $(V_\omega, \in) \models \mathrm{ZF} \setminus \mathrm{Infinito}$. $(V_{\omega+\omega}, \in) \models \mathrm{ZF} \setminus \mathrm{Rimpiazzamento}$. Dunque, per Löweneheim-Skolem verso il basso (d'ora in poi abbreviato in LS$\downarrow$) esiste $N \prec V_{\omega+\omega}$ *numerabile* ed $N \models \mathrm{ZF} + \mathrm{Rimpiazzamento}$ (WUT?). In N c'è il "vero" ω, e c sarà $\mathscr{P}(\omega) \cap N = (\mathscr{P}(\omega))^N$.

Osserviamo inoltre che affinché $V_\alpha \models$ Coppia è necessario che α sia limite.

Dimostreremo ora questa cosa, che è più forte di LS$\downarrow$ come enunciato prima.

Dimostrazione. Assumiamo WLOG $|A| = \lambda$, a meno di ingrandirlo. Le L_A-formule saranno le L-formule con parametri di A. Abbiamo $|L_A\text{-formule}| = \lambda$. Per ogni L_A-formula $\varphi(x, \vec{a})$ tale che $M \models \exists x \varphi(x, \vec{a})$, scelgo un $b_{\varphi,\vec{a}}$ tale che $M \models \varphi(b, \vec{a})$. Sia ora $A_1 = A \cup \{b_{\varphi,\vec{a}}\}$, al variare di φ nelle L-formule e di $\vec{a}$ nelle successioni finite di parametri in A (insieme dei *testimoni delle formule esistenziali*). Proseguiamo in questo modo costruendo per ricorrenza una successione $A \subset A_1 \subset A_2 \subset \ldots \subset M$ dove ad ogni passo aggiungiamo l'insieme dei testimoni delle formule esistenziali. $N = \bigcup_{n\in\omega} A_n$ verifica la tesi. Infatti $|A_n| = \lambda$ per induzione su n, dato che i parametri sono λ e le formule ancora meno. Quindi $|N| = \lambda \cdot \aleph_0 = \lambda$. Resta da dimostrare che N è una sottostruttura e che è elementare.

Sia f un simbolo di funzione n-aria, $f^M : M^n \to M$. Dobbiamo verificare che $f^M : N^n \to N$. Dati $a_1, \ldots, a_n \in N = \bigcup A_k$, siccome sono finiti esiste k tale che $a_1, \ldots, a_n \in A_k$. Ora $M \models \exists x(x = f(a_1, \ldots, a_n))$ e

quindi esiste un testimone $b \in A_{k+1}$. Dunque $f^M(a_1, \ldots, a_n) \in A_{k+1} \subseteq N$ (osserviamo inoltre che in questo caso il testimone b è unico). Dato che le costanti si possono restringere banalmente, abbiamo mostrato che N è una sottostruttura di M.

Il fatto che sia una sottostruttura elementare è un corollario del Teorema seguente. □

Teorema 13.6 (Criterio di Tarski-Vaught)**.** Se N è una sottostruttura di M e vale

$$M \models \exists x \varphi(x, \vec{a}), \vec{a} \in N \Rightarrow \exists b \in N \; M \models \varphi(b, \vec{a})$$

allora è una sottostruttura elementare.

Dimostrazione. Per induzione su $\Theta(\vec{x})$ mostro che per ogni $\vec{a} \in N$ si ha $N \models \Theta(\vec{a})$ se e solo se $M \models \Theta(\vec{a})$ (cioè $N \prec M$). Se Θ è atomica, questo segue semplicemente dal fatto che N è una sottostruttura di M. Se $\Theta = \neg\psi$, allora $N \models \psi(\vec{a}) \Leftrightarrow M \models \psi(\vec{a})$, quindi $N \models \neg\psi(\vec{a}) \Leftrightarrow M \models \neg\psi(\vec{a})$. Con i connettivi booleani è la stessa cosa, perché essi hanno lo stesso significato in N ed in M. Vediamo cosa succede per $\Theta(\vec{x}) = \exists y \psi(y, \vec{a})$, con $\vec{a} \in N$.

$$\begin{aligned} N \models \exists y \in \psi(y, \vec{a}) &\overset{Tarski}{\Longleftrightarrow} \exists b \in N \; N \models \psi(b, \vec{a}) \\ &\Leftrightarrow M \models \psi(b, \vec{a}) \Leftrightarrow M \models \exists y \psi(y, \vec{a}) \end{aligned}$$

□

Esempio 13.7 (in cui queste cose non funzionano)**.** $L = \{<\}$, $\varphi = \forall x \exists y (y > x)$ (il problema è nei quantificatori misti). $(]0,1[, \in) \subset ([0,1], <) \subset (\mathbb{R}, <)$, e mentre il primo e l'ultimo oggetto verificano φ, l'altro verifica $\neg\varphi$.

La dimostrazione di questo teorema, così come la dimostrazione dell'esistenza di un modello numerabile di una L-teoria con $|L| = \aleph_0$, è non costruttiva. Infatti ci si pone davanti a delle scelte (in questa bisognava scegliere i testimoni b, nell'altra bisognava segliere un ramo del tableaux come insieme di Hintikka).

Teorema 13.8 (Löweneheim-Skolem verso l'alto in forma debole)**.** Se M è una L-struttura infinita e $\lambda \geq |L(T)|$, allora $\exists N \models T, |N| = \lambda$ (potrei anche richiedere $N \succ M$, prendendo $T = \mathrm{ED}(M)$, dove ED è il diagramma elementare, guardare gli appunti di Berarducci).

Dimostrazione. Prendo $C = \{c_i \mid i \in I\}$ insieme di simboli di costante, con $|C| = \lambda$. Considero $L_C = L \cup C$. Ora creo la teoria $T_C = T \cup \{c_i \neq c_j \mid i \neq j \in I\}$. T_C è finitamente soddisfacibile, perché M è infinito. Dunque, per compattezza, T_C è soddisfacibile, ossia ha un modello $N_C = (N, \underbrace{c_i \mapsto a_i}_{\text{interpretazione delle nuove costanti}})$, dove $N \models T$. Naturalmente $|N| \geq \lambda$ perché gli $a_i \in N$ sono tutti distinti (altrimenti T_C non sarebbe soddisfacibile). Se $|N| > \lambda$ lo posso rendere di cardinalità λ usando LS↓. □

Definizione 13.9. Se k è un cardinale infinito, diciamo che una teoria T è k-categorica se ha un unico modello di cardinalità k (a meno di isomorfismi).

Esempio 13.10. $L = \{<\}$, T =ordini totali densi senza estremi. Questa è $\aleph_0$-categorica (l'unico modello è $(\mathbb{Q}, <)$). Non è $2^{\aleph_0}$-categorica, perché oltre a $(\mathbb{R}, <)$ c'è $(\mathbb{R} \setminus \{0\})$, e questi non sono isomorfi. Più in là forse vedremo degli esempi con gli spazi vettoriali.

Teorema 13.11. Se T è una L-teoria senza modelli finiti, k-categorica per un cardinale $k \geq |L| + \omega$, allora T è *completa*, cioè $T \vdash \varphi$ oppure $T \vdash \neg\varphi$ per ogni formula chiusa φ.

Dimostrazione. Siano A, B modelli di T. Basta dimostrare che $A \equiv B$. Fisso $\lambda > k, |A|, |B|, |L|$. Siano, per LS, $A' \succ A$, $B' \succ B$, rispettivamente modelli di $\mathrm{Th}(A)$ e $\mathrm{Th}(B)$ e tali che $|A'| = |B'| = k$. Ora A' e B' sono in particolare modelli di T di cardinalità k, quindi sono per ipotesi isomorfi e $A \equiv B$.

□

14 22/11

Vediamo un'applicazione del Teorema 13.11:

Esempio 14.1. Consideriamo la teoria DLO degli ordini lineari densi senza estremi, con $L = \{<\}$. Abbiamo che $(\mathbb{Q}, <) \models \mathrm{DLO}$, $(\mathbb{R}, <) \models \mathrm{DLO}$. DLO è $\aleph_0$-categorica, quindi è completa, per cui data $\varphi \in L$ si ha

$$(\mathbb{Q}, <) \models \varphi \Leftrightarrow \mathrm{DLO} \vdash \varphi \Leftrightarrow (\mathbb{R}, <) \models \varphi$$

Poniamoci il problema di stabilire quando una teoria è k-categorica.

Definizione 14.2. Date due L-strutture M, N, $f : M \underset{\cong}{\rightsquigarrow} N$ è un *isomorfismo parziale* se $\mathrm{dom}(f) \subseteq M$ e data $\varphi(x_1, \ldots, x_n)$ atomica e $a_1, \ldots, a_n \in \mathrm{dom}(f)$ si ha

$$M \models \varphi(a_1, \ldots, a_n) \Leftrightarrow N \models \varphi(f(a_1), \ldots, f(a_n))$$

Usiamo questa nozione per dimostrare che $(\mathbb{Q} \cup \{\pi\}, <) \cong (\mathbb{Q}, <)$. Definiamo l'isomorfismo parziale $\pi \mapsto 4, 5 \mapsto 5$. Sia $I(M, N) = \{f \mid f : M \rightsquigarrow N\}$ l'insieme degli isomorfismi parziali fra M ed N.

Definizione 14.3. Sia $\emptyset \neq \mathcal{C} = I(M, N)$. $\mathcal{C}$ gode della proprietà *va e vieni* se dato $f \in \mathcal{C}$ si ha $\forall a \in M \exists b \in N$ tale che $f \cup \{(a, b)\} \in \mathcal{C}$ e similmente $\forall b \in N \exists a \in M$ tale che $f \cup \{(a, b)\} \in \mathcal{C}$.

Esempio 14.4. $(\mathbb{Z}, <) \to (\mathbb{R}, <)$ $0 \mapsto 0$, $1 \mapsto 1$ non è estendibile perché non so dove mandare $1/2$. Il problema è che $\mathbb{Z}$ non è denso.

Esempio 14.5. Un isomorfismo parziale $\mathbb{R} \to \mathbb{R}$ che manda tutti i reali nell'intervallo $(0, 1)$ non è estendibile.

Proposizione 14.6. Siano $M, N \models \text{DLO}$ e $\mathcal{C} \subseteq I(M, N)$ la classe degli isomorfismi parziali con dominio finito. Ogni elemento di $\mathcal{C}$ è estendibile.

Dimostrazione. $\mathcal{C} \neq \emptyset$ e $\mathcal{C}$ ha il va e vieni, perché se $f \in C$, $f = \{(a_1, b_1), \dots (a_n, b_n)\}$, dato $a \in M$ è facile scegliere dove mandarlo. □

Teorema 14.7. Se $\exists \emptyset \neq \mathcal{C} \subseteq I(M, N)$ con il va e vieni, e se inoltre $|M| = |N| = \aleph_0$, allora $M \cong N$.

Dimostrazione. $M = \{a_n \mid n \in \omega\}$, $N = \{b_n \mid n \in \omega\}$. Costruisco induttivamente $f_0 \subseteq f_1 \subseteq \dots$, con $f_n \in \mathcal{C}$. Al solito, l'isomorfismo totale sarà $f = \bigcup_n f_n$. f_0 la prendo in modo arbitrario. Data f_n, se n è pari prendo $a \in M \setminus \text{dom}(f_n)$ con indice minimo e un b tale che $f_{n+1} = f_n \cup \{(a, b)\} \in \mathcal{C}$ (posso farlo perché $\mathcal{C}$ ha il va e vieni). Se n è dispari prendo $b \in N$ con indice minimale, $a \in M$ corrispondente, ecc.

Ora f è totale (cioè $(\text{dom}(f) = M)$) perché ogni a_k viene pescato da f_{2k} (magari c'è un off-by-one o qualcosa di simile ma il concetto è chiaro). Discorso analogo per l'immagine. È un isomorfismo perché mi basta controllare che preservi le formule atomiche e queste hanno un numero finito di variabili, quindi basta verificarlo per le singole f_n. □

Corollario 14.8. DLO è $\aleph_0$-categorica.

Definizione 14.9. Un *grafo random* è un grafo con $\aleph_0$ vertici, dove ogni coppia di nodi è collegata con probabilità $1/2$.

Consideriamo la la L-teoria T, con $L = \{E\}$ i cui assiomi sono

1. $E(x, y) \leftrightarrow E(y, x)$
2. $\neg E(x, x)$
3. La famiglia di assiomi

$$\varphi_{k,n} = \forall x_1, \dots x_k \forall y_1, \dots y_n \exists z \bigwedge_{i=1}^{k} E(x_i, z) \wedge \bigwedge_{j=1}^{n} \neg E(y_i, z)$$

Teorema 14.10. Dati due grafi random, questi sono isomorfi con probabilità 1, e sempre con probabilità 1 sono l'unico modello (a meno di isomorfismi) numerabile di T (in particolare T è $\aleph_0$-categorica).

Dimostrazione. La prima parte sono conti, per il resto basta dimostrare che ha una classe di isomorfismi parziali col va e vieni. Dati G_1 e G_2 modelli numerabili di T, consideriamo la classe $\mathcal{C} \neq \emptyset$ degli isomorfismi parziali finiti fra G_1 e G_2. Che si possono estendere si fa vedere nella maniera ovvia per induzione (usando la famiglia di assiomi 3). □

Definizione 14.11. Un'*algebra di Boole* è una L-struttura, dove $L = \{0, 1, \cap, \cup, \sim\}$, i cui assiomi sono

1. $\cap, \cup$ sono commutative, associative, e distribuiscono una rispetto all'altra;

Il fatto di scegliere la "o" inclusiva è proprio per far distribuire tutte e due le operazioni rispetto all'altra.

2. $x \cup \sim x = 1$
3. $x \cap \sim x = 0$
4. $x \cap 0 = 0$
5. $x \cup 0 = x$
6. le idempotenze;
7. le leggi di De Morgan;
8. $\sim\sim x = x$

(molto probabilmente sono sovrabbondanti o ne mancano)

Definizione 14.12. Data un'algebra di boole possiamo definire $x \subseteq y \Leftrightarrow x \cap y = x$.

Viene fuori che questo è un ordine parziale.

Esempio 14.13. $\langle \mathscr{P}(X), \emptyset, X, \cap, \cup, ^c \rangle$

Si dimostra che ogni algebra di Boole è isomorfa a una sottoalgebra delle parti di qualcosa. Inoltre un'algebra di Boole finita è isomorfa alle parti di un insieme finito (in particolare ha cardinalità 2^n). Che non tutte le algebre di Boole sono isomorfe ad un'algebra di parti si vede ad esempio considerando l'algebra sulla parti di $\mathbb{N}$ fatta dagli insiemi finiti o cofiniti.

Definizione 14.14. B algebra di Boole è *atomica* se

$$\forall x \exists y \subseteq x \big(0 \neq y \wedge \forall z z \subseteq y \to z = y \vee z = \emptyset\big)$$

e senza atomi (*atomless*) se

$$\forall y \big(\exists z \subseteq y (z \neq y \wedge z \neq \emptyset)\big)$$

Un esempio di algebra di Boole senza atomi è quella delle L-formule proposizionali, con $L = \{A_n \mid n \in \omega\}$ variabili proposizionali, con $B = \Big(\text{formule}/\!\sim, 0, 1, \cap, \cup, \sim\Big)$, dove $\varphi \sim \psi \Leftrightarrow \models \varphi \leftrightarrow \psi$, $\cap = \wedge$, $\sim = \neg$, $\cup = \vee$, $0 = [A \wedge \neg A]$, $1 = [A \vee \neg A]$. Notiamo che il $\subseteq$ è il $\to$. Quindi ad esempio per trovare una formula che implica una formula φ basta prendere $\varphi \wedge C$, con C variabile non presente in φ.

Esercizio 14.15. L'algebra di sopra è unica a meno di isomorfismi.

Data una L-teoria T posso anche fare l'algebra di Boole della teoria (*algebra di Lindenbaum*) prendendo

$$B(T) = \{[\varphi] \mid \varphi \in L\text{formule}\} \quad [\varphi] = [\psi] \Leftrightarrow T \vdash \varphi \leftrightarrow \psi$$

Notiamo che T è completa se e solo se $B(T) = \{0, 1\}$ (ogni formula equivale a una contraddizione o a una tautologia).

Lemma 14.16 (di Lindenbaum)**.** T tableaux-coerente $\rightarrow \exists T' \supseteq T$ $L(T') = L(T)$ completa.

Questo è ovvio avendo il Teorema di Completezza (prendo un modello e le formule vere in quel modello), oppure è uno strumento per dimostrarlo (in questo caso lo si dimostra come caso particolare di un teorema sulle algebre di Boole; ogni filtro sulle algebre di Boole di formule corrisponde ad una teoria coerente ed ogni ultrafiltro ad una completa, quindi per il Teorema di completamento ad ultrafiltro...).

15 23/11

Teorema 15.1. Se esiste $\emptyset \neq \mathcal{C} \subseteq L(M, N)$ classe non vuota di isomorfismi parziali finiti con va e vieni, allora

1. M, N numerabili $\Rightarrow M \cong N$ (visto nella scorsa lezione)
2. In ogni caso $M \equiv N$ (sono elementarmente equivalenti)

Il secondo punto non lo dimostriamo. Possiamo quindi passare per $\mathcal{C}$ se vogliamo dimostrare che una data teoria è completa.

Corollario 15.2. Se T è una L-teoria e $\forall M, N \in \text{Mod}(T) \exists \mathcal{C} \subseteq L(M, N)$ come sopra, allora T è completa.

Sappiamo che per dimostrare che una teoria è completa basta mostrare che una qualsiasi coppia di suoi modelli è elementarmente equivalente.

15.1 Ordini discreti

Un esempio di ordine discreto è $(\mathbb{Z}, <)$. Gli assiomi sono

1. $\forall x \exists y \big(y > x \wedge \neg \exists z (x < z < y)\big)$ (successore)
2. $\forall x \exists y \big(y < x \wedge \neg \exists z (y < z < x)\big)$ (predecessore)
3. Assiomi degli ordini totali.

Questa teoria è completa. Come faccio a mostrare che $\mathbb{Z} \equiv \mathbb{Z} \times \{0, 1\}$?

Definizione 15.3. Date M, N L-strutture, $a_1, \ldots, a_k \in M, b_1, \ldots, b_k \in N$ dico che

$$M, a_1, \ldots, a_k \underset{n}{\sim} N, b_1, \ldots, b_k$$

cioè, che sono *n-equivalenti* se e solo se $(n = 0)$ $\forall \varphi(x_1, \ldots, x_k)$ atomica $M \models \varphi(\vec{a}) \Leftrightarrow N \models \varphi(\vec{b})$, mentre nel caso $n > 0$ se e solo se

$$\forall a \in M \exists b \in N \quad M, a_1, \ldots, a_k, a \underset{n-1}{\sim} N, b_1, \ldots, b_k, b$$
$$\forall b \in N \exists a \in M \quad M, a_1, \ldots, a_k, a \underset{n-1}{\sim} N, b_1, \ldots, b_k, b$$

Teorema 15.4. $M \equiv N \Leftrightarrow \forall n M \underset{n}{\sim} N$

Dimostrazione. Omessa. □

Esempio 15.5. $(\mathbb{R}, <) \not\equiv (\mathbb{Z}, <)$, infatti uno è discreto e l'altro è denso, e una formula che li distingue è $\forall xy \left(x < y \to \exists z\, x < z < y\right)$.

Esempio 15.6. $\mathbb{Z} \times \{0, 1\} \equiv \mathbb{Z}$. Col va e vieni tradizionale questo non riesco a dimostrarlo.

Ora considero la teoria di Presburger, in sostanza l'artimetica di Peano senza il $\cdot$ (lo tolgo anche dal linguaggio), con l'induzione.

Teorema 15.7. Presburger è completa.

Dimostrazione. Si fa con le tecniche appena viste. □

Dunque $(\mathbb{N}, s, +, 0) \models \varphi$ se e solo se Presburger $\vdash \varphi$, e questo fornisce un algoritmo per verificare la verità o falsità delle formule nel linguaggio di Peano in cui compaiono solo $+, 0, s$. Alcune teorie complete sono

- Presburger
- Campi algebricamente chiusi con caratteristica 0
- Ordini densi
- Ordini discreti

mentre alcune incomplete sono

- ZF
- Peano al prim'ordine
- Campi
- Gruppi

Osserviamo che tuttavia $\mathrm{Th}(\mathbb{N}, +, \cdot)$ è banalmente completa in quanto teoria di un modello, però è *indecidibile*, ossia non esiste un algoritmo per stabilire se una formula è vera o meno. È chiaro che Teoria completa + assiomi decidibili $\Rightarrow$ teoria decidibile.

Scriveremo $T \underset{d}{\vdash} \varphi$ per indicare che d è una dimostrazione di φ in T.

Se l'insieme degli assiomi di T è decidibile, allora $\left\{(d, T) \mid T \underset{d}{\vdash} \varphi\right\}$ è decidibile, ma questo non è l'insieme dei teoremi, ma delle dimostrazioni. L'insieme dei teoremi è $\left\{\varphi \mid \exists d T \underset{d}{\vdash} \varphi\right\}$, e questo è semi-decidibile. Tuttavia, se T è completa, diventa decidibile. Dunque la decidibilità e la completezza sono collegate, anche se una teoria può essere decidibile e incompleta o indecidibile e completa.

In Q (aritmetica di Robinson) abbiamo che

$$\forall x < y \; \varphi \equiv \forall x (x < y \to \varphi)$$

dove $x < y \equiv \exists z (z + x = y)$.

Definizione 15.8. Una formula si dice *limitata* se tutti i quantificatori che vi compaiono sono limitati.

Chiamiamo Δ_0 la classe delle formule limitate. Esiste un algoritmo per decidere se una formula chiusa $\varphi \in \Delta_0$ è vera o falsa in $\mathbb{N}$ (i quantificatori limitati possono essere trasformati in una serie finita di congiunzioni o disgiunzioni). Precisamente, se $\varphi \in \Delta_0$, allora $\exists \psi$ senza quantificatori tale che $\mathbb{N} \models \psi \leftrightarrow \varphi$. Quindi $\mathbb{N} \models \varphi \Leftrightarrow \mathbb{N} \models \psi$, e una formula senza quantificatori è una combinazione booleana di formule atomiche, quindi è facile stabilire se è vera o falsa. Tutto questo discorso vale anche in Q, e quindi non solo nel modello standard $\mathbb{N}$.

In Q, dato $n \in \mathbb{N}$ (nella metateoria), $\overline{n} = s^n(0)$

Lemma 15.9.

$$Q \vdash \forall x \big(x \leq \overline{n} \leftrightarrow x = \overline{0} \vee \ldots \vee x = \overline{n}\big)$$

cioè possono anche esserci numeri non stardard, ma non sono minori dei numeri stardard (nel senso della somma).

Dimostrazione. Per induzione su n. Per $n = 0$ si ha $Q \vdash x \leq 0 \leftrightarrow x = 0$. Se $x < 0$ vuol dire che $\exists z \; z + x = 0$. Se per assurdo $x \neq 0$, allora per un assioma di Q $\exists y (x = s(y))$. Allora $z + s(y) = 0$. Ma un altro assioma dice $z + s(y) = s(z + y)$ e ciò contraddice l'assioma $\forall x s(x) \neq 0$. Per $n > 0$, se $x \leq n$, sia z tale che $z + x = \overline{n}$. Se $x = \overline{0}$ ho fatto, altrimenti sia u tale che $x = s(u)$. Allora, sostituendo, ho $s(z + u) = z + s(u) = \overline{n}$. Dato che $n > 0$, $\overline{n} = \overline{k + 1} = s(\overline{k})$, e per un altro assioma il successore è inettivo, quindi $z + u = \overline{k}$, e allora $u \leq \overline{k}$, e quindi $u = \overline{0} \vee \ldots \vee u = \overline{k}$. Dato che $x = s(n)$, possiamo concludere $x = \overline{1} \vee \ldots x = \overline{k + 1} = \overline{n}$. □

Corollario 15.10. $Q \vdash \forall x\big(x \leq \overline{n+1} \leftrightarrow x \leq \overline{n} \vee x = \overline{n+1}\big)$

Corollario 15.11. Sia $n \in \mathbb{N}$. Sono equivalenti:

1. $\forall a \leq n\ Q \vdash \varphi(\overline{a})$
2. $Q \vdash \forall x \leq \overline{n}\varphi(x)$

cioè i quantificatori limitati hanno lo stesso significato nella teoria e nella metateoria.

Dimostrazione. Entrambe le cose sono equivalenti a

$$Q \vdash \varphi(\overline{0}) \wedge \varphi(\overline{1}) \wedge \ldots \wedge \varphi(\overline{n})$$

Inoltre vale la stessa cosa sostituendo $\forall$ con $\exists$ e $\wedge$ con $\vee$. □

Nella prossima lezione dimostreremo che Q è completa rispetto alle formule Δ_0. Da questa cosa segue che

Corollario 15.12. Se $\varphi \in \Delta_0$, allora $Q \vdash \varphi \Leftrightarrow \mathbb{N} \models \varphi$.

16 29/11

Lemma 16.1.
1. $\forall k \leq n\ Q \vdash \varphi(\overline{k}) \Leftrightarrow Q \vdash \forall x \leq \overline{n}\varphi(x)$
2. $\exists k \leq n\ Q \vdash \varphi(\overline{k}) \Leftrightarrow Q \vdash \exists x \leq \overline{k}\varphi(x)$

Ora c'è una serie di lemmetti noiosi. Ne dimostriamo uno, gli altri sono lasciati per esercizio.

Lemma 16.2. $\forall a, b \in \mathbb{N}\ a + b = c \Rightarrow Q \vdash \overline{a} + \overline{b} = \overline{c}$

Dimostrazione. Per induzione su b (nella metateoria). Se $b = 0$ siamo apposto perché $Q \vdash \forall x(x + 0 = x)$. Se $b > 0$ e $a + b = c$, allora $a + (b - 1) = c - 1$. Per ipotesi induttiva quindi $Q \vdash \overline{a} + \overline{b-1} = \overline{c-1}$. Inoltre $Q \vdash x + s(y) = s(x + y)$ e questo conclude. □

In modo analogo, usando il Lemma, si mostra che

Lemma 16.3. $a, b, c \in \mathbb{N}, a \cdot b = c \Rightarrow Q \vdash \overline{a} \cdot \overline{b} = \overline{c}$

Corollario 16.4. Se T è un termine chiuso e $n = t^{\mathbb{N}}$, $Q \vdash t = \overline{n}$.

Dimostrazione. Per induzione sulla complessità di t (come stringa). □

Lemma 16.5. $a = b \Rightarrow Q \vdash \overline{a} = \overline{b}$

Dimostrazione. Ovvio perché $Q \vdash x = x$. □

Lemma 16.6. $a \neq b \Rightarrow Q \vdash \overline{a} \neq \overline{b}$.

Dimostrazione. Per iniettività del successore. □

Notiamo che se $M \models Q$, possiamo considerare la mappa $\mathbb{N} \to M$ $n \mapsto (s^n(0))^M$ e immergerci una copia isomorfa di $\mathbb{N}$. Inoltre gli elementi "standard" sono un segmento iniziale. Più precisamente

$$\forall b \in \mathbb{N}\ Q \vdash \forall x(x \leq \overline{b} \leftrightarrow x = \overline{0} \vee \ldots \vee x = \overline{b})$$

Notiamo che questo ci fa "comportare bene" i quantificatori limitati. Se dico $\forall x \leq t$, x è forzato ad essere standard per quanto detto sopra.

Lemma 16.7.

$$\forall a, b \in \mathbb{N}\ \big(Q \vdash \overline{a} \leq \overline{b}\big) \vee \big(Q \vdash \neg(\overline{a} \leq \overline{b})\big)$$

Dimostrazione. Se $a \leq b$, $Q \vdash \overline{a} = \overline{0} \vee \ldots \vee \overline{a} = \overline{b}$ (perché là in mezzo c'è anche $\overline{a} = \overline{a}$). Ma per un Lemma di quelli precedenti questo implica $\overline{a} \leq \overline{b}$. Se $a > b$, $Q \vdash \forall x(x = \overline{0} \vee \ldots \vee x = \overline{b} \to x \neq \overline{a})$. Ma $Q \vdash \forall x(x \leq \overline{b} \to x \neq \overline{a})$. Quindi $Q \vdash \overline{a} \leq \overline{b} \to \overline{a} \neq \overline{a}$, e allora per assurdo $Q \models \neg(\overline{a} \leq \overline{b})$. □

Lemma 16.8. $\forall b \in \mathbb{N}\ Q \vdash \forall x(x \leq \overline{b} \vee \overline{b} \leq x)$.

Definizione 16.9. Una formula θ è *decibidile* in Q se $Q \vdash \theta$ oppure $Q \vdash \neg\theta$.

Teorema 16.10. Se $\varphi \in \Delta_0$ è chiusa, $Q \vdash \varphi$ oppure $Q \vdash \neg\varphi$.

Dimostrazione. Per induzione sulla complessità della formula. Se φ è atomica, è della forma $t_1 = t_2$. Prendiamo $a = t_1^{\mathbb{N}}, b = t_2^{\mathbb{N}}$. Allora $Q \vdash t_1 = s^a(0)$, e $Q \vdash t_2 = s^b(0)$. Allora se $a = b$ $Q \vdash t_1 = t_2$, altrimenti $Q \vdash t_1 \neq t_2$.

Osserviamo ora che se φ, ψ sono decise in Q, allora lo sono anche $\varphi \vee \psi$, $\varphi \wedge \psi$, $\neg\varphi$ (ovvio, per casi). Resta da capire cosa succede coi quantificatori limitati.

Sia $\varphi = \forall x \leq t\ \psi(x)$, con $\psi(x) \in \Delta_0$. Prendiamo $a = t^{\mathbb{N}}$, osserviamo che $Q \vdash t = \overline{a}$, e quindi $Q \vdash \forall x \leq t\ \psi(x) \leftrightarrow \forall x \leq \overline{a}\ \psi(x)$. Inoltre $Q \vdash \forall x \leq \overline{a}\ \psi(x) \Leftrightarrow \forall b \leq a\ Q \vdash \psi(b)$, perché se la seconda è vera la prima è decisa, altrimenti vuol dire che $\exists b \leq a$ tale che $Q \nvdash \psi(\overline{b})$, ma per ipotesi induttiva allora $Q \vdash \neg\psi(\overline{b})$ e a maggior ragione $Q \vdash \neg\forall x \leq \overline{a}\ \psi(x)$. Col quantificatore esistenziale limitato è analogo, o si passa da $\neg\forall\neg$. □

Notiamo che abbiamo incidentalmente dimostrato una cosa più forte: non solo le Δ_0 sono decidibili, ma la classe delle formule decidibili è chiusa per connettivi e quantificazione limitata.

Consideriamo ora la classe Σ_1^0, definita come

$$\frac{\varphi \in \Delta_0}{\varphi \in \Sigma_1^0} \qquad \frac{\varphi, \psi \in \Sigma_1^0}{\varphi \wedge \psi, \varphi \vee \psi, \forall x \leq t\varphi, \exists x \leq t\varphi \in \Sigma_1^0}$$

e sopratutto

$$\frac{\varphi \in \Delta_0}{\exists x \varphi(x) \in \Sigma_1^0}$$

notare che Σ_1^0 non è chiusa per negazione e che posso riportare un sacco di formule nella forma con l'$\exists$ all'inizio (se lavoro nel modello standard), ad esempio

$$\mathbb{N} \models \forall x \leq 5 \; \exists y \; \Delta_0(x, y)$$

se e solo se

$$\mathbb{N} \models \exists z \; \forall x \leq 5 \; \exists y \leq z \; \Delta_0(x, y)$$

Data φ, posso considerare

$$\varphi(x_1, \ldots, x_n)^{\mathbb{N}} = \{(a_1, \ldots, a_n) \in \mathbb{N}^n \mid \mathbb{N} \models \varphi(a_1, \ldots, a_n)\}$$

(i cosiddetti *insiemi definibili*, che chiaramente non sono tutti per questioni di cardinalità).

Definizione 16.11. $A \subseteq \mathbb{N}$ è *decidibile* (o *ricorsivo*) se esiste un algoritmo P che $\forall a \in \mathbb{N}$ termina e mi dice se $a \in A$ o meno.

Definizione 16.12. $A \subseteq \mathbb{N}$ è *semi-decidibile* (o *ricorsivamente enumerabile*) se esiste un algoritmo P tale che $\forall a \in \mathbb{N}$ se $a \in A$ l'algoritmo termina e dice che $a \in A$, altrimenti non termina (diverge).

Proposizione 16.13. Decidibile implica semi-decidibile.

Dimostrazione. Basta far andare in loop l'algoritmo quando mi direbbe "no". □

Teorema 16.14 (Post)**.** Se A e $\mathbb{N} \setminus A$ sono semi-decidibili, A è decidibile.

Dimostrazione. Ovvia facendo un passo di uno, un passo dell'altro, eccetera. □

Teorema 16.15. A è semi-decidibile se e solo se è Σ_1^0-definibile in $\mathbb{N}$, cioè se esiste una formula $\varphi(x) \in \Sigma_1^0$ tale che $A = \{n \in \mathbb{N} \mid \mathbb{N} \models \varphi(n)\}$.

Dimostrazione. Se A è Σ_1^0-definibile da φ, per induzione su φ costruisco l'algoritmo. Se è atomica è ovvio. Per congiunzioni eccetera idem (inclusa quantificazione ristretta). Per la quantificazione esistenziale non ristretta faccio provare tutti gli interi un passo alla volta all'algortimo, (un passo per il primo, uno per il secondo, il secondo del primo, il secondo del secondo, il primo del terzo, eccetera) se non termina va comunque bene.

Per l'altra freccia serve una definizione precisa di algoritmo (probabilmente si passa dalla forma normale di Kleene) □

Corollario 16.16. A è decidibile se è Δ_0-definibile in $\mathbb{N}$.

Dimostrazione. Si vede direttamente oppure notando che se Δ_0 è chiuso per negazione e passando dal Teorema di Post. □

Ovviamente non vale il viceversa. La caratterizzazione dei decidibili è data da

$$\left(\Sigma_1^0\right)^{\mathbb{N}} \cap \left(\neg\Sigma_1^0\right)^{\mathbb{N}}$$

cioè dagli insiemi di naturali definibili sia da una formula Σ_1^0 che da una formula $\neg\Sigma_1^0$.

Teorema 16.17. Se $\varphi \in \Sigma_1^0$ è chiusa, $\mathbb{N} \models \varphi \Rightarrow Q \vdash \varphi$.

Notiamo che se $\mathbb{N} \not\models \varphi$ (e quindi per Tarski $\mathbb{N} \models \neg\varphi$), allora $Q \nvdash \varphi$, altrimenti sarebbe vera in tutti i modelli ma *non* è vero che $Q \vdash \neg\varphi$.

17 30/11

Teorema 17.1. $\varphi \in \Sigma_1^0$ chiusa, $\mathbb{N} \models \varphi \Rightarrow Q \vdash \varphi$.

Dimostrazione. Se $\varphi \in \Delta_0$ lo sappiamo già. Al solito per casi sulla forma (o induzione sulla complessità, o quello che ci pare). Se $\varphi = \psi \vee \theta$ ed $\mathbb{N} \models \psi \vee \theta$, allora WLOG $\mathbb{N} \models \psi$ e quindi $Q \vdash \psi$, e a maggior ragione $Q \vdash \psi \vee \theta$. Per il $\wedge$ è analogo. Se $\varphi = \forall x \leq t\ \psi$ (con t termine chiuso, altrimenti φ non sarebbe chiusa) e $\mathbb{N} \models \varphi$, se $b = t^{\mathbb{N}}$ si ha che $\forall a \leq b\ \mathbb{N} \models \psi(a)$, quindi $\forall a \leq b\ Q \vdash \psi(\overline{a})$, e allora $Q \vdash \forall x \leq \overline{b}\ \psi(x)$ e $Q \vdash \forall x \leq t\ \psi(x)$. Se invece $\varphi = \exists x\ \psi(x)$ ed $\mathbb{N} \models \varphi$ vuol dire che $\exists a \in \mathbb{N}$ tale che $\mathbb{N} \models \psi(a)$, dunque $Q \vdash \psi(\overline{a})$ e a maggior ragione $Q \vdash \exists x \psi(x)$. □

Il viceversa è ovvio dato che $\mathbb{N} \models Q$. Dunque le Σ_1^0 chiuse sono vere in $\mathbb{N}$ se e solo se sono dimostrabili in Q.

Segue euristica per giustificare la freccia del Teorema 16.15 che si fa con la forma normale di Kleene (non riportata).

Ora, per ragioni che saranno chiare in seguito, vogliamo codificare le successioni finite di naturali coi naturali. Un modo è mappare iniettivamente

$$\mathbb{N}^{<\omega} \to \mathbb{N} \qquad \langle a_1, \ldots, a_n \rangle \mapsto \prod_{i=1}^{n} p_i^{a_i+1}$$

Questa cosa è utile per quantificare *al prim'ordine* su successioni finite, dato che vengono codificate in un singolo naturale. Purtroppo non funziona, perché richiede l'uso della produttoria, della successione dei primi, eccetera. Per ovviare a questo inconveniente usiamo la

Definizione 17.2. *Funzione β di Gödel.*

$$\beta : \mathbb{N}^3 \to \mathbb{N} \quad \beta(c,d,i) = r \Leftrightarrow \exists q \leq c\ \big(c = q[d(i+1)+1]+r \wedge 0 \leq r \leq (i+1)d+1\big)$$

In parole povere $\beta(c,d,i)$ è il resto della divisione euclidea di c per $d(i+1)+1$.

Questa, al contrario di quella sopra, rientra a pieno titolo nelle formule Δ_0.

Proposizione 17.3 (Proprietà fondamentale della β)**.** $\forall\langle a_0,\dots,a_n\rangle\exists c,d\ \forall i \le n\ \beta(c,d,i)=a_i$, cioè conoscendo c,d,n conosco tutta la successione.

La dimostrazione userà il Teorema Cinese del Resto e il seguente

Lemma 17.4. $\forall n,x\ \exists d>x$ tale che $d+1, 2d+1,\dots,nd+1$ sono coprimi. In altre parole esistono progressioni aritmetiche arbitrariamente lunghe e arbitrariamente grandi di numeri coprimi.

Dimostrazione. È un esercizio di aritmetica. Basta prendere $d=y!$, dove $y=\max(n,x)$. □

Torniamo alla Proprietà fondamentale della β e diamone quindi la

Dimostrazione. Voglio codificare con c,d la successione $\langle b_0,\dots,b_n\rangle$. Sia d tale che $d+1, 2d+1,\dots(n+1)d+1$ siano coprimi e tali che $d>\max(b_i)$ (posso farlo per il Lemma precedente). Siano ora $a_i=d(i+1)+1$ e c tale che $\forall i\le n\ c\equiv b_0 \pmod{a_0}$ (posso farlo per il Teorema Cinese del Resto). Dato che $b_i<a_i$, b_i è semplicemente il resto della divisione euclidea di c per a_i, e questa è la tesi. □

Notiamo che aver usato il fattoriale nella dimostrazione non è un problema, perché non compare nella formula per la β, e comunque lo sto facendo nella metateoria.

Osserviamo che stiamo codificando le successioni finite con successioni lunghe 2, che però sono facili da codificare in un solo naturale. Le teorie "potenti" sono quelle sequenziali, cioè quelle che codificano le successioni.

Adesso abbiamo modo di Σ_1^0-definire la formula $x^y=z$, assumendo x,y numeri standard.

$$x^y=z \Leftrightarrow \exists <b_0,\dots,b_y> \big((b_0=1)\wedge(\forall i<y\ b_{i+1}=b_i\cdot x)\wedge(b_y=z)\big)$$
$$\Leftrightarrow \underbrace{\exists c,d\big((\beta(c,d,0)=1)\wedge(\forall i<y\ \beta(c,d,i+1)=\beta(c,d,i)\cdot x)\wedge(\beta(c,d,y)=z)\big)}_{\stackrel{\text{def}}{=}\varphi_{\exp}(x,y,z)\in\Sigma_1^0}$$

Ora dobbiamo mostrare che

Proposizione 17.5. $a^b=e \Leftrightarrow \mathbb{N}\models\varphi_{\exp}(a,b,e)$.

Dimostrazione. Se $a^b=e$, siano, per $1\le i\le n$, $b_i=a^i$ (siamo nella metateoria quindi questo discorso è perfettamente lecito) e c,d tali che $\beta(c,d,i)=a^i$. Con questa scelta di c,d si ha $\beta(c,d,0)=1$ e $\beta(c,d,i+1)=\beta(c,d,i)\cdot a$, per cui $\mathbb{N}\models\varphi_{\exp}(a,b,e)$ e quindi per quanto visto sopra $Q\vdash\varphi_{\exp}(\overline{a},\overline{b},\overline{e})$.

Viceversa, supponiamo che $\mathbb{N}\models\varphi_{\exp}(a,b,e)$. Allora $\exists c,d$ tali che $\mathbb{N}\models\gamma(c,d,a,b)$, dove γ è $\varphi_{\exp}$ senza il quantificatore esistenziale che c'è all'inizio.

Allora fisso c, d, e mostro per induzione su $i \leq b$ che $\beta(c, d, i) = a^i$. Così $\beta(c, d, b) = e$ per la formula, e per induzione $\beta(c, d, b) = a^b$, quindi $a^b = e$. □

Abbiamo dunque dimostrato che

$$a^b = e \Leftrightarrow \mathbb{N} \models \varphi_{\exp}(a, b, e) \Leftrightarrow Q \vdash \varphi_{\exp}(\overline{a}, \overline{b}, \overline{e})$$

Teorema 17.6. Se $a, b \in \mathbb{N}$ (quindi sono standard), allora $Q \vdash \exists! x \varphi_{\exp}(\overline{a}, \overline{b}, x)$

Nota bene: $Q \nvdash \forall u, v \exists! x \varphi_{\exp}(u, v, x)$.

Dimostrazione. Prendiamo un qualsiasi modello $M \models Q$ e facciamo vedere che

$$M \models \forall x \left[\varphi_{\exp}(\overline{a}, \overline{b}, x) \leftrightarrow x = a^b\right]$$

Sia $e \in M$ tale che $M \models \varphi_{\exp}(\overline{a}, \overline{b}, e)$. Il problema sta nel fatto che c, d potrebbero essere non-standard. Ma in realtà non è un problema perché tanto l'induzione si fa su $i \leq b$, quindi basta ripercorrere la dimostrazione precedente. Osserviamo che non serve che a sia standard, basta che lo sia b. □

Definizione 17.7. $f : \mathbb{N}^n \to \mathbb{N}$ è *binumerata* in Q se esiste una formula φ_f tale che

1. $f(a) = b \Rightarrow Q \vdash \varphi_f(\overline{a}, \overline{b})$
2. $f(a) \neq b \Rightarrow Q \vdash \neg\varphi_f(\overline{a}, \overline{b})$

Se inoltre vale

3. $Q \vdash \forall y(\varphi_f(\overline{a}, y) \leftrightarrow y = \overline{b})$

allora si dice che f è *binumerata funzionalmente*. In questo caso la 2 è ridondante perché si dimostra dalle altre due.

18 6/12

Il prodotto diretto di strutture in generale non preserva le cose. Ad esempio il prodotto di campi non è in generale un campo. Bisogna introdurre la nozione di *ultraprodotto*. Segue definizione di filtro, ultrafiltro e altra roba. Sia ora $\widetilde{\mathcal{A}} = \prod_{i \in I} A_i /_{\approx}$, dove $\approx$ la definiremo in maniera furba fra poco.

Definizione 18.1. $\widetilde{\mathcal{A}} \models R([\sigma], [\tau]) \overset{\text{def}}{\Leftrightarrow} \mathcal{A}_i \models R(\sigma(i), \tau(i))$ quasi ovunque (nel senso dell'ultrafiltro).

Seguono verifiche sulla buona definizione delle cose.

Notazione 18.2. $\mathcal{I}_i(\cdot)$ indica l'interpretazione nel modello i-esimo.

Definizione 18.3. $\{\mathcal{A}_i \mid i \in I\}$ famiglia di L-strutture, $\mathcal{F}$ filtro su I. Il *prodotto ridotto* $\prod_{i\in I} A_i/\mathcal{F}$ è la L-struttura tale che

1. Il suo dominio è il quoziente $\prod_{i\in I} A_i/\mathcal{F}$
2. I simboli di costante $\underline{c}$ sono interpretati come $[\langle \mathcal{I}_i(\underline{c}) \mid i \in I\rangle]$.
3. R simbolo di relazione k-aria viene interpretato come
$$\widetilde{\mathcal{A}} \models R([\sigma_1], \dots, [\sigma_k]) \Leftrightarrow \{i \in I \mid \mathcal{A}_i \models R(\sigma_1(i), \dots, \sigma_k(i))\} \in \mathcal{F}$$
4. I simboli F di funzione k-aria vengono interpretati come
$$F([\sigma_1], \dots, [\sigma_k]) = [\langle \mathcal{I}_i(F)(\sigma_1(i), \dots, \sigma_k(i)) \mid i \in I\rangle]$$

Seguono definizioni di filtro principale e filtro di Frechet. La definizione è buona per le proprietà di filtro.

Esempio 18.4. $\prod_{n\in\mathbb{N}} \mathbb{Z}_n/\mathcal{F}$, dove $\mathcal{F}$ è il filtro di Frechet su $\mathbb{N}$, è un anello commutativo infinito. Se mi limito ai primi, cioè prendo $\prod_{n\in\mathbb{N}} \mathbb{Z}_{p_n}/\mathcal{F}$ dove p_n è l'n-esimo primo, c'è un problema: ho fatto un prodotto di campi, ma quello che ottengo non è un campo (il prodotto dell'indicatrice dei pari e dell'indicatrice dei dispari fa 0).

Si riesce a caratterizzare quali sono le formule che si preservano passando al quoziente (bisogna ragionare sulla parità delle negazioni).

Definizione 18.5. Un *ultraprodotto* è un prodotto ridotto su un ultrafiltro.

(ci sono state un sacco di cose basilari sugli ultrafiltri, non riportate; ci sono pari pari negli appunti del corso di Ultrafiltri e Metodi non-standard) Notare che l'ultrapotenza è un caso particolare di ultraprodotto fatto sempre con lo stesso oggetto.

Teorema 18.6. Non esiste nessuna formula $\varphi(x, y, z)$ del linguaggio $L = \{0, s\}$ (dove s è al solito il successore) tale che $\mathbb{N} \models \varphi(a, b, c) \Leftrightarrow a + b = c$.

Dimostriamo una proprietà più forte:

Teorema 18.7. I pari non sono definibili, cioè non esistono formule $\theta(x)$ tali che $(\mathbb{N}, s) \models (\theta(a))$ se e solo se a è pari.

Chiaramente se so definire la somma so definire anche i pari, quindi...

Dimostrazione. Prendiamo ${}^*\mathbb{N}$ modello non standard e definiamo

$$\psi(\xi) = \begin{cases} \xi & \text{se} \quad \xi \in \mathbb{N} \\ s(\xi) & \text{se} \quad \xi \in {}^*\mathbb{N} \setminus \mathbb{N} \end{cases}$$

Ora si ha $\mathbb{N} \models \forall x P(x) \leftrightarrow \neg P(s(x))$, dove P è la proprietà di essere pari. $\psi(x)$ è un automorfismo (facile verifica; è un morfismo perché nel linguaggio non ho somma e prodotto). Si ha quindi $\mathbb{N} \prec {}^*\mathbb{N} \Rightarrow \mathbb{N} \equiv {}^*\mathbb{N}$, quindi ${}^*\mathbb{N} \models \forall x P(x) \leftrightarrow \neg P(s(x))$. Se ξ è infinito (cioè $\xi \notin \mathbb{N}$), abbiamo

$$\begin{aligned} {}^*\mathbb{N} &\models P(\xi) \leftrightarrow \neg P(s(\xi)) \\ {}^*\mathbb{N} \models \neg P(s(\xi)) &\Leftrightarrow {}^*\mathbb{N} \models \neg P(\psi(\xi)) \end{aligned}$$

ma ψ è un automorfismo, e allora ${}^*\mathbb{N} \models P(\xi) \Leftrightarrow {}^*\mathbb{N} \models P(\psi(\xi))$, assurdo. □

19 07/12

Teorema 19.1 (Łoś)**.** Se $\{\mathcal{A}_i \mid i \in I\}$ è una famiglia di α-strutture, e $\mathcal{U}$ è un ultrafiltro su I, per ogni α-formula $\varphi(x_1, \dots, x_n)$ e per ogni $[\sigma_1], \dots, [\sigma_n] \in \prod \mathcal{A}_i /_{\approx_\mathcal{U}}$ vale

$$\prod \mathcal{A}_i /_\mathcal{U} \models \varphi\left(x_1 /_{[\sigma_1]}, \dots, x_n /_{[\sigma_n]}\right) \Leftrightarrow \{i \in I \mid \mathcal{A}_i \models \varphi(\sigma_1(i), \dots, \sigma_n(i))\} \in \mathcal{U}$$

In particolare se θ è un enunciato (formula chiusa)

$$\prod \mathcal{A}_i /_\mathcal{U} \models \theta \Leftrightarrow \{i \in I \mid A_i \models \theta\} \in \mathcal{U}$$

Dimostrazione. Al solito per induzione sulla complessità della formula (l'utilizzo dell'ipotesi induttiva è spesso non riportato).

In base alla definizione si può verificare (esercizio) che per ogni termine $t(x_1, \dots, x_n)$ e per ogni $[\sigma_1], \dots, [\sigma_n] \in \prod A_i /_\mathcal{U} = \widetilde{A}$ vale

$$t\left(x_1 /_{[\sigma_1]}, \dots, x_n /_{[\sigma_n]}\right) = \left[\left\langle t\left(x_1 /_{\sigma_1(i)}, \dots, x_n /_{\sigma_n(i)}\right) \mid i \in I \right\rangle\right]_\mathcal{U}$$

Per le formule atomiche si fa la verifica noiosa ma diretta che (dove $t_i = t_i(x_1, \dots, x_n)$)

$$\begin{aligned} \widetilde{A} &\models \underline{R}(t_1, \dots, t_k)\left[x_1 /_{[\sigma_1]}, \dots, x_n /_{[\sigma_n]}\right] \\ &\overset{\text{def}}{\Leftrightarrow} \left\{i \in I \mid \underline{R}(t_1, \dots, t_k)\left[x_1 /_{\sigma_1(i)}, \dots, x_n /_{\sigma_n(i)}\right]\right\} \in \mathcal{U} \end{aligned}$$

Per il $\wedge$

$$\widetilde{\mathcal{A}} \models (\varphi \wedge \psi)([\sigma_1], \dots, [\sigma_n]) \overset{\text{def}}{\Leftrightarrow} \left(\widetilde{\mathcal{A}} \models \varphi([\sigma_1], \dots, [\sigma_n])\right) \wedge \left(\widetilde{\mathcal{A}} \models \psi([\sigma_1], \dots, [\sigma_n])\right.$$

se e solo se

$$\Gamma = \{i \in I \mid \mathcal{A}_i \models \varphi(\sigma_1(i), \dots, \sigma_n(i))\} \in \mathcal{U}$$
$$\wedge\Lambda = \{i \in I \mid \mathcal{A}_i \models \psi(\sigma_1(i), \dots, \sigma_n(i))\} \in \mathcal{U}$$

ma $\Gamma \cap \Lambda \in \mathcal{U}$

Per il $\vee$ è analogo, e per $\neg$ si usa la proprietà di ultrafiltro.

Il $\forall$ segue dal fatto che vale per $\neg$ e per $\exists$, e per quest'ultimo supponiamo che

$$\widetilde{\mathcal{A}} \models \exists x \varphi(x, [\sigma_1], \dots, [\sigma_n])$$
$$\overset{Tarski}{\Longleftrightarrow} \exists[\tau] \quad \widetilde{\mathcal{A}} \models \underbrace{\varphi([\tau], [\sigma_1], \dots, [\sigma_n])}_{\text{ha complessità minore}} \Leftrightarrow \Lambda = \{i \in I \mid \mathcal{A}_i \models \varphi(\tau(i), \sigma_1(i), \dots, \sigma_n(i))\} \in \mathcal{U}$$

Ma ora $\{i \in I \mid \mathcal{A}_i \models \exists x \varphi(x, \sigma_1(i), \dots, \sigma_n(i))\} \supseteq \Lambda \in \mathcal{U}$.

Viceversa supponiamo $\Gamma = \{i \in I \mid \mathcal{A}_i \models \exists x \varphi(x, \sigma_1(i), \dots, \sigma_n(i))\} \in \mathcal{U}$. Con l'assioma di scelta scegliamo $\tau \mid \forall i \in \Gamma$ sia un *testimone*, cioè $\mathcal{A}_i \models \varphi(\tau(i), \sigma_1(i), \dots, \sigma_n(i))$. Allora

$$\{i \in I \mid \mathcal{A}_i \models \varphi(\tau(i), \sigma_1(i), \dots, \sigma_n(i))\} \supseteq \{i \in I \mid \mathcal{A}_i \models \exists x \varphi(x, \sigma_1(i), \dots, \sigma_n(i))\} \in \mathcal{U}$$
$$\widetilde{\mathcal{A}} \models \varphi([\tau], [\sigma_1], \dots, [\sigma_n])$$
$$\Rightarrow \widetilde{A} \models \exists x \varphi(x, [\sigma_1], \dots, [\sigma_n])$$

□

Se immergiamo nella maniera canonica $\mathcal{A}$ in ${}^{\mathcal{A}^I}\!/_{\mathcal{U}}$, il Teorema di Łoś ci dice che $\mathcal{A} \prec {}^{\mathcal{A}^I}\!/_{\mathcal{U}}$.

Richiamiamo la seguente

Definizione 19.2. Date $\mathcal{A}, \mathcal{B}$ α-strutture, $f : \mathcal{A} \prec \mathcal{B}$ è una *immersione elementare* se per ogni α-formula $\varphi(x_1, \dots, x_n)$ e per ogni $a_1, \dots, a_n \in \mathcal{A}$ si ha

$$\mathcal{A} \models \varphi(a_1, \dots, a_n) \Leftrightarrow \mathcal{B} \models \varphi(f(a_1), \dots, f(a_n))$$

Osserviamo che $\mathcal{A} \prec \mathcal{B} \underset{\not\equiv}{\Rightarrow} \mathcal{A} \equiv \mathcal{B}$. Infatti

$${}^{\mathcal{A}^I}\!/_{\mathcal{U}} \models \varphi(d(a_1), \dots, d(a_n)) \underset{\text{Łoś}}{\Leftrightarrow} \{i \in I \mid \mathcal{A} \models \varphi(a_1, \dots, a_n)\} \in \mathcal{U} \Leftrightarrow \varphi(a_1, \dots, a_n)$$

se è vera allora è tutto $I \in \mathcal{U}$, altrimenti è $\emptyset \notin \mathcal{U}$.

Esempio 19.3. Sia ${}^*\mathbb{N} = {}^{\mathbb{N}^{\mathbb{N}}}\!/_{\mathcal{U}}$ con $\mathcal{U}$ ultrafiltro non principale. Allora $d : \mathbb{N} \prec_d {}^*\mathbb{N}$. Si identifica $d(n)$ con n in maniera da avere $\mathbb{N} \subset {}^*\mathbb{N}$

Osserviamo che questo tipo di struttura se ne frega del linguaggio: $\mathbb{R} \prec {}^*\mathbb{R}$ è un'*immersione elementare completa*, nel senso che prendiamo su $\mathbb{R}$ il linguaggio più ricco possibile, cioè posso mettere simboli per l'intervallo $[0,1]$, per il sin, eccetera e in ${}^*\mathbb{R}$ ho ${}^*\sin, {}^*\cos, {}^*\exp$, eccetera, che hanno le stesse proprietà.

Esercizio 19.4. Se $\mathcal{U}$ è un ultrafiltro su $\mathbb{N}$, considero $\mathcal{M}_\mu = \{\sigma : \mathbb{N} \to \mathbb{R}\}, E(\sigma) \in \mathcal{U}$ è un ideale massimale di $\mathbb{R}^\mathbb{N}$, e se $\mathcal{M}$ è un ideale massimale su $\mathbb{R}^\mathbb{N}$, allora $\mu_\mathcal{M} = \{A \subseteq \mathbb{N} \mid \exists \sigma \in \mathcal{M}\ E(\sigma) = A\}$ è un ultrafiltro.

Esempio 19.5 (Campi di caratteristica 0)**.** $\forall x \neq 0\ x \cdot n \neq 0 \forall n \in \mathbb{N}$ è del second'ordine! Per enunciarla al prim'ordine si usa una quantità infinita di formule. Si può dimostrare che *non* esiste un enunciato σ nel linguaggio dei campi ordinati che definisce la proprietà di caratteristica 0, cioè tale che $\mathbb{F} \models \sigma \Leftrightarrow \mathbb{F}$ ha caratteristica 0. Infatti se per assurdo esistesse tale σ, prendo $\mathcal{U}$ ultrafiltro non principale su $\mathbb{N}$ e considero $\mathbb{F} = \prod_{n\in\mathbb{N}} \mathbb{Z}_{p_n}/\mathcal{U}$ dove p_n è l'n-esimo primo. Per Łoś $\mathbb{F}$ è un campo. Se esistesse tale σ allora $\forall n \in \mathbb{N}\ \mathbb{Z}_{p_n} \models \neg\sigma \underset{\text{Łoś}}{\Rightarrow} \mathbb{F} \models \neg\sigma$, cioè $\mathbb{F}$ non ha caratteristica 0. Questo è assurdo perché $\forall p_n$ primo $\mathbb{Z}_{p_k} \models \forall x \neq 0\ x \cdot p_n \neq 0$ per ogni $n \neq k$ e $\{k \mid n \neq k\} \in \mathcal{U}$, quindi per Łoś $\mathbb{F} \models \forall x \neq 0\ x \cdot p_n \neq 0$ vale per ogni n, e quindi $\mathbb{F}$ ha caratteristica 0.

Le proprietà che si mantengono sono quelle definibili al prim'ordine, per quelle che non possiamo definire si possono esibire automorfismi che sballano tutto.

Con questi strumenti possiamo dare una dimostrazione alternativa del Teorema 8.2, cioè della forma del Teorema di Compattezza che ci dice che una teoria è soddisfacibile se e solo se è finitamente soddisfacibile.

Dimostrazione. Per ogni $T_0 \subset T$ finito, prendo $\mathcal{M}_{T_0} \models T_0$. L'idea è fare un ultraprodotto degli M_{T_0}, e prendere come insieme di indici $I = \mathscr{P}_{\text{fin}}(T)$. Bisogna scegliere un ultrafiltro $\mathcal{U}$. Vorrei che preso $\sigma \in T$ enunciato, si abbia, dove $\widetilde{\mathcal{M}} = \prod_{T_0 \in I} \mathcal{M}_{T_0}/\mathcal{U}$,

$$\widetilde{\mathcal{M}} \models \sigma \underset{\text{Łoś}}{\Leftrightarrow} \underbrace{\{T_0 \in I \mid \mathcal{M}_{T_0} \models \sigma\}}_{\supseteq \{T_0 \in I \mid \sigma \in T_0\}} \in \mathcal{U}$$

Quindi basta trovare $\mathcal{U}$ tale che $\forall \sigma$ si abbia $\hat{\sigma} = \{T_0 \in I \mid \sigma \in T_0\} \in \mathcal{U}$. Notiamo che la famiglia $\{\hat{\sigma} \mid \sigma \in I\}$ ha la FIP: infatti $\hat{\sigma_1} \cap, \ldots, \cap \hat{\sigma_{100}} \supseteq \{\sigma_1, \ldots, \sigma_{100}\} = T_0$, e quindi esiste un ultrafiltro che la estende. □

Da qui possiamo dimostrare il Teorema di Completezza nella seguente maniera

Dimostrazione. Che se T ha un modello è coerente segue dalla correttezza dei tableaux. Per l'altra freccia sappiamo che T è coerente (per definizione)

se e solo se $T \nvdash \bot$, se e solo se (per compattezza sintattica, cioè per il fatto che ogni dimostrazione usa solo un numero finito di assiomi) $\forall T_0 \subset T$ finito $T_0 \nvdash \bot$, e questo se e solo se $\forall T_0 \subset T$ finito $\exists \mathcal{M}_{T_0} \models T_0$, se e solo se (per compattezza) $\exists \mathcal{M} \models T$. □

Corollario 19.6. $T \vdash \sigma \Leftrightarrow T \models \sigma$

Dimostrazione. $T \vdash \sigma \Leftrightarrow T \cup \neg\sigma \vdash \bot$, se e solo se, per completezza, non esistono $\mathcal{M} \models T \cup \{\neg\sigma\}$, se e solo se $\forall \mathcal{M}\ \mathcal{M} \models T \Rightarrow \mathcal{M} \not\models \neg\sigma$, cioè $\forall \mathcal{M}\ \mathcal{M} \models T \Rightarrow \mathcal{M} \models \sigma$. □

Esercizio 19.7. Ogni ordine parziale si estende ad un ordine totale (per compattezza).

Esercizio 19.8. Non esiste un enunciato σ nel linguaggio dell'ordine totale tale che

$$x \models \sigma \Leftrightarrow X \text{ è ben ordinato}$$

Esercizio 19.9 (difficile)**.** Esistono $2^{\aleph_0}$ modelli numerabili non isomorfi della teoria $T = \mathrm{Th}(\mathbb{N}, \cdot, s, 0)$.

Hint: $\forall S \subseteq P$ con P insieme dei primi considero l'insieme di formule

$$\Gamma_s(x) = \left\{ \text{“}p \mid x'' \mid p \in S \right\} \cup \left\{ \text{“}p \nmid x'' \mid p \notin S \right\}$$

$\Gamma_s(\underline{c})$ è finitamente soddisfacibile e quindi ha un modello $\mathcal{M}_s$ numerabile (compattezza + LS). $\{\mathcal{M}_S \mid S \subset P\} \supseteq 2^{\aleph_0}$ classi di isomorfismo.

20 13/12

Robe su funzioni primitive ricorsive, Tesi di Church, forma normale di Kleene (non dimostrata), problema della fermata, eccetera (vedi appunti Linguaggi di Programmazione). Cose in più: il grafico $G(f)$ di una funzione calcolabile f è Σ_1^0: per le primitive ricorsive si fa e se $f = \mu g$ con g primitiva ricorsiva continua a funzionare. Se invece del μ prendo il min esco da Σ_1^0 (è la negazione di una Σ_1^0). In sostanza

Teorema 20.1. f funzione parziale $\mathbb{N}^n \to \mathbb{N}$ è calcolabile se e solo se $G(f) \in \left(\Sigma_1^0\right)^{\mathbb{N}}$.

Teorema 20.2. Le μ-calcolabili totali sono binumerabili funzionalmente in Q.

Dimostrazione. Vediamo solo la verifica della chiusura per minimalizzazione. Bisognerebbe anche verificare la chiusura per ricorsione primitiva e il fatto che sono binumerabili la costante 0, il successore e le proiezioni (ma ci crediamo). Sia $f(x) = \mu y[g(x, y) = 0]$.

$$f(x) = z \Leftrightarrow g(x, z) = 0 \wedge \forall i < z\ \exists v \neq 0\ g(x, i) = v$$

Quindi una formula che binumera funzionalmente f è

$$\varphi_f(x,z) = \varphi_g(x,z,0) \wedge \forall i < z \; \exists v \neq 0 \; \varphi_g(x,i,v)$$

□

Ora vorremo estendere il concetto di funzione calcolabile alle funzioni da formule a formule. Ovviamente la maniera per farlo è codificare le formule con i naturali. Non serve che la codifica sia bigettiva (si può fare ma è noioso), basta che $\widetilde{f}$ sia iniettiva e definita 0 sugli n che non codificano nessuna formula.

$$\begin{array}{ccc} \text{Formule} & \xrightarrow{f} & \text{Formule} \\ \lceil\ \rceil \downarrow & & \lceil\ \rceil \downarrow \\ \mathbb{N} & \xrightarrow[\widetilde{f}]{} & \mathbb{N} \end{array}$$

Una maniera per fare la codifica è la seguente: prendiamo una funzione $\# : L \to \mathbb{N}$ iniettiva che mandi ad esempio le n-uple ordinate in nel prodotto dei primi n primi con la k-esima componente all'esponente

$$\begin{aligned} \lceil v_i \rceil &= \langle \#(v), i \rangle \\ \lceil 0 \rceil &= \langle \#0 \rangle \\ \lceil s(t) \rceil &= \langle \#(s), \lceil t \rceil \rangle \\ \lceil t_1 + t_2 \rceil &= \langle \#(+), \lceil t_1 \rceil \, \lceil t_2 \rceil \rangle \\ \lceil t_1 \cdot t_2 \rceil &= \langle \#(\cdot), \lceil t_1 \rceil \, \lceil t_2 \rceil \rangle \end{aligned}$$

(manca il resto, vedere appunti Berarducci)

21 14/12

Esempio esplicito di codifica, non riportato.

Lemma 21.1 (di diagonalizzazione, o primo Teorema di punto fisso)**.** Sia $\varphi(x)$ nel linguaggio $L = \{0, s, +, \cdot\}$. Allora $\exists \beta$ tale che $Q \vdash \beta \leftrightarrow \varphi(\overline{\lceil \beta \rceil})$.

Questo in particolare implica che $\mathbb{N} \models \beta \leftrightarrow \varphi(\overline{\lceil \beta \rceil})$.

Esempio 21.2. Sia $\varphi(x) = \exists y(y + y = x)$. Allora per il Lemma precedente esiste β tale che $\mathbb{N} \models \beta \Leftrightarrow \lceil \beta \rceil$ è pari.

In sostanza β dice "io godo della proprietà φ". Dimostriamo il Lemma.

Dimostrazione. Abbiamo visto che se $f : \mathbb{N} \to \mathbb{N}$ è μ-ricorsiva totale, allora esiste $\varphi_f(x, y)$ tale che se $f(a) = b$, allora $Q \vdash \varphi_f(\underline{a}, \underline{b}) \wedge Q \vdash \exists! y \varphi_f(\underline{a}, y)$. Consideriamo la funzione sub : $\mathbb{N}^2 \to \mathbb{N}$ tale che

$$\begin{cases} \text{sub}(\ulcorner\varphi\urcorner, n) = \ulcorner\varphi(s^n 0/x)\urcorner \\ \text{sub}(m, n) = 0 \qquad\qquad\qquad \text{se } m \text{ non è della forma } \ulcorner\varphi\urcorner \end{cases}$$

Ad esempio $\text{sub}(\ulcorner x_0 = x_0\urcorner, 3) = \ulcorner sss0 = sss0\urcorner$. È intuitivo che sub sia calcolabile, inoltre è primitiva ricorsiva.

Useremo la seguente notazione: date $\alpha(x)$, $f : \mathbb{N} \to \mathbb{N}$ calcolabile binumerata con $\varphi_f(x, y)$, indichiamo con $\alpha(\bar{f}(x))$ la formula $\exists y(\varphi_f(x, y) \wedge \alpha(y))$. In Q funziona bene solo quando x è standard in modo da avere un unico output $\alpha(\bar{f}(\bar{n})) = \exists y(\varphi_f(\bar{n}, y) \wedge \alpha(y))$ (serve che f sia binumerata funzionalmente). Ma $Q \vdash \varphi_f(\bar{n}, y) \leftrightarrow y = \overline{f(n)}$, allora in Q si ha $\alpha(\bar{f}(\bar{n})) = \exists y(\ldots) \leftrightarrow \alpha(\overline{f(n)})$. Dato che sub è binumerata funzionalmente in quanto ricorsiva, $\exists \varphi_{\text{sub}}(x, y, z)$. Definisco ora $\gamma(x) = \varphi(\overline{\text{sub}}(x, x)) = \exists y\big(\varphi(y) \wedge \varphi_{\text{sub}}(x, x, y)\big)$. Basta prendere $\beta = \gamma(\overline{\ulcorner\gamma\urcorner})$ e convincersi che funziona. Infatti si ha

$$\beta = \gamma(\overline{\ulcorner\gamma\urcorner}) = \varphi(\overline{\text{sub}}(\overline{\ulcorner\gamma\urcorner}, \overline{\ulcorner\gamma\urcorner})) \leftrightarrow_Q \varphi(\overline{\text{sub}(\ulcorner\gamma\urcorner, \ulcorner\gamma\urcorner)}) = \varphi(\ulcorner\gamma(\overline{\ulcorner\gamma\urcorner})\urcorner) = \varphi(\ulcorner\beta\urcorner)$$

Lo schema è il seguente: voglio β tale che $\beta \leftrightarrow \varphi(\beta)$, provo che $\beta = \gamma\gamma$, allora trovo $\gamma\gamma \leftrightarrow \varphi(\gamma\gamma) \Rightarrow \gamma x = \varphi(xx)$. Questa cosa si chiama "principio del DNA": per riprodursi c'è bisogno di una coppia. □

Diamo ora qualche cenno sul secondo Teorema di punto fisso. Definiamo $a \sim b \Leftrightarrow \varphi_a = \varphi_b$. Data h calcolabile totale, $\exists a\ a \sim h(a)$ (visto a Linguaggi di Programmazione). Vogliamo che $\varphi_b(b) \sim h(\varphi_b(b))$, allora definiamo $\varphi_b(x) = h(\varphi_x(x))$.

Qua c'è stato un po' di casino.

Dobbiamo introdurre la funzione s. Sia $\varphi_e^n : \mathbb{N}^n \to \mathbb{N}$ $\qquad \varphi^1_{s(e,a)}(x) = \varphi^2_e(a, x)$. Ad esempio sia $e : x + y$, $s(e, 3) = 3 + y$ (sempre roba vista a Linguaggi di Programmazione). Arrivati a $\exists a\ a \sim h(a)$, scegliamo $a = s(b, b)$ e poi devo scegliere b.

$$a \sim h(a) \Leftrightarrow \varphi_a(x) = \varphi_{h(a)}(x)$$

$$\varphi_a(x) = \varphi^1_{s(b,b)}(x) = \varphi^2_b(b, x) \stackrel{?}{=} \varphi_{h(s(b,b))}(x)$$

basta scegliere b tale che $\varphi_b(y, x) = \varphi_{h(s(y,y))}(x)$.

Tornando a Gödel, diamo la seguente

Definizione 21.3. $A \subseteq \mathbb{N}$ è *aritmetico* se $\exists \varphi(x)$ nel linguaggio $L = \{0, s, +, \cdot\}$ tale che $A = \{n \mid \mathbb{N} \models \varphi(n)\}$.

Proposizione 21.4. Decidibili $\subset$ Semidecidibili $\subset$ Aritmetici

Dimostrazione. I semidecidibili sono chiusi per $\wedge, \vee, \forall x \leq t, \exists x$, gli aritmetici anche per $\forall x, \neg$. L'inclusione è stretta perché ad esempio $\{a \mid \varphi_a \text{ è totale}\}$ è aritmetico. Scritto bene sarebbe $\{a \mid \forall x \exists t \varphi_a(x) \downarrow t\}$, e la formula di cui è estensione è Π^0_2. Un insieme non aritmetico esiste sicuramente per questioni di cardinalità. □

Teorema 21.5 (di Tarski)**.** $A = \{\ulcorner\varphi\urcorner \mid \mathbb{N} \models \varphi\}$ non è aritmetico.

"La definizione di verità non è aritmetica".

Dimostrazione. Supponiamo per assurdo che esista una formula aritmetica $\mathrm{True}(x)$ che lo definisce, cioè tale che $n \in A \Leftrightarrow \mathbb{N} \models \mathrm{True}(n)$. Si ha $\mathbb{N} \models \varphi \Leftrightarrow \mathbb{N} \models \mathrm{True}(\ulcorner\varphi\urcorner)$, cioè $\forall\varphi\ \mathbb{N} \models \varphi \leftrightarrow \mathrm{True}(\ulcorner\varphi\urcorner)$. Ma se applico il Lemma di diagonalizzazione a $\neg\,\mathrm{True}(x)$ trovo β tale che $\mathbb{N} \models \beta \leftrightarrow \neg\,\mathrm{True}(\ulcorner\beta\urcorner)$ (paradosso del mentitore). Questo è assurdo perché allora $\mathbb{N} \models \beta \leftrightarrow \neg\,\mathrm{True}(\ulcorner\beta\urcorner) \leftrightarrow \neg\beta$. □

Proposizione 21.6. $\beta = \left\{\ulcorner\varphi\urcorner \mid PA^1 \vdash \varphi\right\}$ è aritmetico

Dimostrazione. È semidecidibile. Basta provare a dimostrare φ provando tutte le dimostrazioni (o i tableaux) un passo alla volta nella solita maniera diagonale. □

Corollario 21.7. $\left\{\ulcorner\varphi\urcorner \mid PA^1 \vdash \varphi\right\} \subsetneq \{\ulcorner\varphi\urcorner \mid \mathbb{N} \models \varphi\}$, cioè esiste una formula φ vera in $\mathbb{N}$ ma non dimostrabile.

Notiamo che aggiungere una tale φ a calci non migliorerebbe la situazione. L'ipotesi usata è che l'insieme di assiomi è decidibile (in realtà basta semidecidibile), e aggiungendo φ agli assiomi rimarrebbe tale, quindi ne spunterebbe fuori un'altra.

Vogliamo esibire una tale φ. (segue dimostrazione che usa la Tesi di Church, non riportata; nella prossima lezione esibiamo una tale φ in un'altra maniera)

22 20/12

$\{x \in \mathbb{N} \mid \varphi_x(x) \downarrow\}$ ($\downarrow$ vuol dire "termina", cioè $\exists t\ \varphi_x(x) \downarrow_t$) è semidecidibile ed aritmetico .

Abbiamo dimostrato che PA non è completo per assurdo, ma non abbiamo esibito una φ tale che $\mathbb{N} \models \varphi$ ma $PA \nvdash \varphi$. Ora vogliamo esibirne una.

Consideriamo la bigezione

$$\mathbb{N} \to V_\omega \qquad a = 2^{a_1} + \ldots + 2^{a_n} \mapsto f(a) = \{f(a_1), \ldots, f(a_n)\}$$

e notiamo che $a \overset{*}{\in} b \Leftrightarrow b = 2^{a_1} + \ldots + 2^{a_n}$ con $a \in \{a_i \mid 1 \leq i \leq n\}$. Questo posso scriverlo come

$$a \overset{*}{\in} b \leftrightarrow \exists u, v \leq b\big(u < 2^a \wedge b = u + 2^a v\big)$$

l'esponenziale si fa con la β di Gödel, quindi questa è una formula Δ_0. In quanto Δ_0 definibile, questa cosa è vera in $\mathbb{N}$ se e solo se è dimostrabile in Q. Quindi ad esempio $\emptyset \in \{\emptyset\}$ diventa $0 \overset{*}{\in} 1$ che è vera se e solo se $Q \vdash 0 \overset{*}{\in} 1$ perché Δ_0.

Si può addirittura dimostrare che $PA \vdash \big(ZF \setminus \text{Infinito}\big)^t$, dove $(x \in y)^t = (x \overset{*}{\in} y)$.

Sappiamo che se f è ricorsiva totale, allora è binumerata funzionalmente in Q. $\exists \varphi_f(x, u)$ tale che $Q \vdash \varphi_f(\overline{a}, \overline{b})$ e $Q \vdash \forall y(\varphi_f(\overline{a}), y \leftrightarrow y = \overline{b})$.

$A \subseteq \mathbb{N}$ è decidibile se e solo se la sua funzione caratteristica χ_A è ricorsiva totale. Ora ho una formula per φ_{χ_a}, quindi

$$a \in A \Leftrightarrow \chi_A(a) = 1 \Leftrightarrow Q \vdash \varphi_{\chi_A}(\overline{a}, 1)$$

Chiamiamo $\varphi_{\chi_A}(x, \overline{1}) = \varphi_A(x)$, e quindi

$$a \in A \Leftrightarrow Q \vdash \varphi_A(\overline{a})$$
$$a \notin A \Leftrightarrow Q \vdash \neg\varphi_A(\overline{a})$$

Consideriamo ora Γ insieme finito di formule, φ formula e d tableau tali che $\Gamma \vdash_d \varphi$. Avevo una codifica $\ulcorner \cdot \urcorner$ per le formule. Posso codificare analogamente anche gli insiemi finiti di formule (componendo con la bigezione di $\mathbb{N}$ con V_ω) e i tableaux. Ora considero le terne

$$\big\{(\ulcorner\Gamma\urcorner, \ulcorner d\urcorner, \ulcorner\varphi\urcorner) \in \mathbb{N}^3 \mid \Gamma \vdash_d \varphi\big\} = \text{Tab}$$

Si vede facilmente che questo insieme è decidibile.

Supponiamo ora di avere una teoria T ricorsivamente assiomatizzata, ad esempio $T = PA$. L'insieme degli assiomi è ricorsivo e quindi lo posso binumerare con una formula $\text{Ax}_T(x) \in L(+, \cdot, 0, s)$, cioè φ è un assioma di T se e solo se $Q \vdash \text{Ax}_T(\overline{\ulcorner\varphi\urcorner})$. Questo è un piccolo abuso di notazione perché Ax_T non dipende solo da T ma anche da come ho scritto Ax_T. Esiste inoltre $\text{Dim}(x, y, z) \in L(+, \cdot, s, 0)$ che binumera Tab in Q, quindi

$$(a, b, c) \in \text{Tab} \Leftrightarrow Q \vdash \text{Dim}(\overline{a}, \overline{b}, \overline{c})$$

Ora voglio rappresentare i teoremi. $\{\ulcorner\varphi\urcorner \mid PA \vdash \varphi\}$ è semidecidibile. Però $T \vdash \varphi \Leftrightarrow \exists T' \subseteq_{\text{fin}} T\ \exists d\ T' \vdash_d T$ (uso solo finiti assiomi per dimostrare le cose). "$\subseteq_{\text{fin}}$" si scrive con l'appartenenza che abbiamo visto poter essere usata, quindi non stiamo barando. Scriviamo (intendendo φ, d come variabili libere)

$$\text{Prov}_T(d, \varphi) = \exists T' \leq d\big((\forall u \leq d\ u \overset{*}{\in} T' \to \text{Ax}_T(u)) \wedge \text{Dim}(T', d, \varphi)\big)$$

i quantificatori sono limitati da d perché d è l'intero tableau e contiene tutto, quindi questa è Δ_0. Notiamo inoltre che Prov dipende solo da Ax, cioè è l'unica cosa che devo cambiare se cambio teoria.

Ora d, φ cessano di essere variabili e diventano un vero tableau e una vera formula. Si ha

$$T \vdash_d \varphi \Leftrightarrow \mathbb{N} \models \mathrm{Prov}_T(\ulcorner d \urcorner, \ulcorner \varphi \urcorner) \Leftrightarrow Q \vdash \mathrm{Prov}_T(\ulcorner d \urcorner, \ulcorner \varphi \urcorner)$$

sempre perché Prov $\in \Delta_0$ relativamente ad Ax.

Ora introduciamo

$$\mathrm{Teo}_T(y) = \exists x \, \mathrm{Prov}_T(x, y) \in \Sigma_1^0$$

(se $\mathrm{Ax}_T \in \Sigma_1^0$). Sappiamo che se φ è Σ_0^1 ed è vera nei naturali, è dimostrabile in Q. Quindi

$$T \vdash \varphi \Leftrightarrow \exists d \; T \vdash_d \varphi \Leftrightarrow \exists d Q \vdash \mathrm{Prov}_T(\ulcorner d \urcorner, \ulcorner \varphi \urcorner)$$
$$\Rightarrow Q \vdash \exists x \, \mathrm{Prov}_T(x, \ulcorner \varphi \urcorner) \Rightarrow \mathbb{N} \models \exists x \, \mathrm{Prov}_T(x, \overline{\ulcorner \varphi \urcorner}) \Rightarrow T \vdash \varphi$$

Quindi sono tutti se e solo se. In particolare

$$T \vdash \varphi \Leftrightarrow Q \vdash \mathrm{Teo}_T(\overline{\ulcorner \varphi \urcorner})$$

ma questo non mi autorizza a dire che $T \nvdash \varphi \Rightarrow Q \vdash \neg \, \mathrm{Teo}_T(\overline{\ulcorner \varphi \urcorner})$. Questo è in generale falso.

Introduciamo la notazione $\Box\varphi = \mathrm{Teo}_T(\overline{\ulcorner \varphi \urcorner}) \in \Sigma_1^0$ e $\Box_x \varphi = \mathrm{Prov}_T(x, \overline{\ulcorner \varphi \urcorner}) \in \Delta_0$. Inoltre $\Box_{<x}\varphi = \exists x' \leq x \;\; \mathrm{Prov}_T(x', \overline{\ulcorner \varphi \urcorner})$.

Per ora ci conviene pensare $T = PA$, poi vedremo di capire cosa ci serve di T.

Per diagonalizzazione esiste G tale che

$$Q \vdash G \leftrightarrow \neg \Box G$$

(notiamo che G non compare nel membro di destra, compare il suo numero di Gödel nascosto nel $\Box$).

T non può essere ad esempio $\mathrm{Th}(\mathbb{N})$, sennò non potrei scrivere Ax_T, quindi supponiamo che T sia ricorsivamente assiomatizzabile. La seconda ipotesi che faccio su T quindi è che $T \supseteq Q$, (e che il linguaggio sia lo stesso di Q) così per quanto appena visto ho che

$$T \vdash G \leftrightarrow \neg \Box G$$

cioè G dice di non essere dimostrabile.

Proposizione 22.1. 1. $T \nvdash G$

2. $T \nvdash \neg G$

Dimostrazione. 1. Se $T \vdash G$ vuol dire che $\exists n T \vdash_n G$ quindi $\exists n Q \vdash \Box_n G$ da cui $Q \vdash \Box G$ e quindi $T \vdash \Box G$. In sostanza, se T dimostra qualcosa, T "sa" di dimostrarlo. Per definizione di G però avrei dimostrato che $T \vdash \neg G$, quindi $T \vdash G \wedge \neg G$, e perciò $T \vdash \bot$ che non è assurdo di per sè, ma lo è se assumo che T è coerente. Questa è la terza ipotesi che assumiamo su T.

2. Per $T = PA$ si fa al volo. Visto che $T \nvdash G$ ho che $\mathbb{N} \models \neg\Box G$ ma questa equivale per definizione a G, quindi $\mathbb{N} \models G$, per cui $PA \nvdash \neg G$. Qui stiamo assumendo in maniera cruciale che $\mathbb{N} \models T$. Indeboliamo l'ipotesi.

   Per assurdo, se $T \vdash \neg G$, per definizione di G si ha $T \vdash \Box G$, quindi

   $$T \vdash \exists x \Box_x G \tag{32}$$

   Siccome $T \nvdash G$ per la 32 $\forall n\ T \nvdash_n G$, quindi $\forall n\ Q \vdash \neg\Box_n G$, per cui

   $$\forall n\ T \vdash \neg\Box_n G \tag{33}$$

   C'è qualcosa di strano: T dimostra che esiste un certo naturale, ma dimostra che non è 0, non è 1, non è 2, eccetera

   Definizione 22.2. T teoria del linguaggio dell'aritmetica è ω-coerente se non esiste θ tale che $T \vdash \exists x \theta(x)$ e $\forall n T \vdash \neg\theta(\overline{n})$.

   Notiamo che questa non è una contraddizione, quindi può benissimo capitare che una teoria sia coerente ma ω-incoerente. Inoltre se una teoria è ω-coerente è anche coerente (ovvio).

   Ora se $\mathbb{N} \models T$, sicuramente T è ω-coerente. La proprietà che ci serve è questa, quindi assumeremo per T l'ω-coerenza, che è una proprietà intermedia fra la coerenza e l'avere $\mathbb{N}$ come modello.

□

Occhio che il fatto che $T \nvdash G$ non ci autorizza a dire che G è vera (nel senso che è vera in tutti i modelli di T). Questo non succede perché altrimenti per il Teorema di Completezza avrei $T \models G \Rightarrow T \vdash G$.

In sostanza abbiamo dimostrato il cosiddetto *Primo Teorema di Gödel* sotto l'ipotesi di ω-coerenza. Ricapitolando

Teorema 22.3 (Primo Teorema di Gödel)**.** Se $T \supseteq Q$ è ω-coerente e ricorsivamente assiomatizzata, allora $T \nvdash G$, $T \nvdash \neg G$, e quindi T è incompleta.

Ad esempio vale per $T = PA$. Un esempio di teoria ω-incoerente ma coerente è $PA + \neg G$. Le ipotesi possono essere indebolite: si può richiedere la semplice coerenza (vedi più avanti) e basta che l'insieme delle codifiche

degli assiomi sia solo ricorsivamente enumerabile (e non per forza ricorsivo), visto che comunque Ax_T continua ad essere in Σ_1^0.

Nell'ipotesi $T = PA$ (giusto per non vedere esattamente quali ipotesi servono su T, ma si generalizza) vedremo ora il

Teorema 22.4 (Secondo Teorema di Gödel)**.** $PA \vdash G \leftrightarrow \mathrm{Coer}(PA)$, e in particolare $PA \nvdash \mathrm{Coer}(PA)$, dove $\mathrm{Coer}(PA) = \neg\Box \bot$.

Dimostrazione. Vediamo che $PA \vdash G \to \neg\Box \bot$. Dentro PA ho $G \to \neg\Box G$ per definizione di G. Voglio dimostrare che $\neg\Box G \to \neg\Box \bot$, ma questa è equivalente a $\Box \bot \to \Box G$, e questo nella metateoria so che è vero, perché dall'assurdo dimostro qualsiasi cosa. Voglio vedere se PA "lo sa".

Torniamo nella metateoria. $PA \vdash \bot \to G$. Quindi $PA \vdash \Box(\bot \to G)$. Mi serve la distributività di $\Box$ su $\to$, che per ora diamo per scontato. È vero di più, cioè che PA dimostra che i teoremi sono chiusi per modus ponens, cioè

Lemma 22.5. $PA \vdash \big(\Box(A \to B)\big) \to \big(\Box A \to \Box B\big)$

Quindi $PA \vdash \Box \bot \to \Box G$.

Vediamo il viceversa. Ragionando sempre in PA. L'idea è formalizzare la 32 in PA. Nella 32 ho dimostrato nella metateoria che T coerente $\to T \nvdash G$. Tutti i passaggi fatti si possono trasportare dalla metateoria dentro PA, cioè $PA \vdash \neg\Box \bot \to \neg\Box G$ che è equivalente a G. Vediamo questa cosa passo per passo.

In PA, assumo $\neg\Box \bot$ e voglio dimostrare G, cioè $\neg\Box G$. Ricalcando la dimostrazione della 32, supponiamo per assurdo $\Box G$. Segue $\Box\Box G$, perché

Lemma 22.6. $PA \vdash \Box\theta \to \Box\Box\theta$

anzi, più in generale ($\Box\theta$ è sempre Σ_1^0)

Lemma 22.7. Se $\sigma \in \Sigma_1^0$, $PA \vdash \sigma \to \Box\sigma$.

Dimostrazione. Questo (e analogamente per altre cose) si vede ripercorrendo in PA (usando l'induzione) la dimostrazione del Teorema 17.1. □

Ora torniamo fuori da PA nella metateoria. So che $PA \vdash \Box G \leftrightarrow \neg G$, quindi in particolare per quanto detto $PA \vdash \Box\Box G \leftrightarrow \Box\neg G$. Rientrando in PA ho che $\Box\Box G \to \Box\neg G$, per cui ho $\Box\neg G$, dunque ho $\Box G \wedge \Box\neg G$, e quindi $\Box(G \wedge \neg G)$, cioè $\Box \bot$, che è assurdo perché avevamo assunto $\neg\Box \bot$.

Abbiamo usato anche che

Lemma 22.8. $PA \vdash (\Box\alpha \wedge \Box\beta) \to \Box(\alpha \wedge \beta)$

Dimostrazione. Si parte dalla tautologia $\alpha \to (\beta \to (\alpha \wedge \beta))$, ci si mette il quadratino davanti, si distribuisce rispetto alle implicazioni e si smanetta un po'. □

Riscritto in maniera più pulita e stringata:

$$\begin{aligned} & PA \vdash \neg G \to \Box G \wedge PA \vdash \Box G \to \Box\Box G \\ \Rightarrow & PA \vdash \neg G \to \Box\Box G \\ \Rightarrow & PA \vdash \neg G \to \Box\neg G \\ \Rightarrow & PA \vdash \neg G \to \Box G \wedge \Box\neg G \\ \Rightarrow & PA \vdash \neg G \to \Box(G \wedge \neg G) \end{aligned}$$

□

23 21/12

PA è incompleta. $PA \nvdash \mathrm{Con}(PA)$. Anche $ZF \nvdash \mathrm{Con}(ZF)$. Data una teoria T ricorsivamente assiomatizzabile (in realtà l'ipotesi si può indebolire), $ZF \vdash \mathrm{Con}(T) \leftrightarrow$ "T ha un modello". Per dire che T ha un modello, si riesce a definire un predicato $\mathrm{Sat}(x, y, z)$, dove al posto di x metto una L-struttura (per un certo L fissato), al posto di y una formula, e al posto di z un assegnamento alle varibili libere di φ (il tutto a meno di codifiche). Sostanzialmente Sat dice $M \models \varphi(z)$. Comunque $ZF \nvdash$ "ZF ha un modello".

$V_\omega \models ZF \setminus$ Infinito e $V_{\omega+\omega} \models ZF \setminus$ Rimpiazzamento. Ma per parlare di V_ω serve l'assioma dell'Infinito e per parlare di $V_{\omega+\omega}$ serve il Rimpiazzamento, perché devo fare il sup degli $\omega + n$, cioè dell'immagine di ω secondo la funzione-classe $n \mapsto \omega + n$. Ovviamente di $\mathbb{N} \times \mathbb{N}$ posso parlare, serve il rimpiazzamento per dire che è isomorfo ad un ordinale.

Formalmente $ZF \setminus$ Rimpiazzamento $\vdash \mathrm{Con}(ZF \setminus$ Infinito), e $ZF \vdash \mathrm{Con}(ZF \setminus$ Rimpiazzamento). (forse serve la scelta)

Definizione 23.1. Una teoria T è *indecidibile* se $\{\ulcorner\varphi\urcorner \mid T \vdash \varphi\}$ non è ricorsivo.

	Completa	Incompleta
Decidibile	$ACF_0 \equiv \mathrm{Th}(\mathbb{C}), DLO$	ACF
Indecidibile	$\mathrm{Th}(\mathbb{N}, +, \cdot), \mathrm{Th}(\mathbb{Z}, +, \cdot), \mathrm{Th}(\mathbb{Q}, +, \cdot)$	PA, ZF, anelli, campi

Dove ACF indica la teoria dei campi algebricamente chiusi, e ACF_0 la stessa però con caratteristica zero.

T ricorsivamente assiomatizzabile completa $\Rightarrow T$ decidibile. Infatti se gli assiomi di T sono ricorsivi, $\{\ulcorner\varphi\urcorner \mid T \vdash \varphi\}$ è semidecidibile, $\{\ulcorner\varphi\urcorner \mid T \vdash \neg\varphi\}$ è anche semidecidibile, se è compelta sono complementari, quindi per il Teorema di Post... In realtà non è così liscia perché la codifica non è surgettiva, ma posso spezzare l'insieme in tre classi tutte semidecidibili (la terza è quella fuori dall'immagine) e funziona uguale. Anche qui vale lo stesso risultato anche sotto l'ipotesi (più debole) che l'insieme delle codifiche degli assiomi sia ricorsivamente enumerabile (l'insieme delle codifiche dei teoremi rimane semidecidibile).

Definizione 23.2. T è *essenzialmente indecidibile* se $\forall T' \supset T$ coerente e tale che $L(T') = L(T)$, T' è indecidibile.

Ad esempio la teoria dei campi è indecidibile ma si può estendere a una decidibile, quindi non è essenzialmente indecidibile.

Teorema 23.3. Q è essenzialmente indecidibile.

Dimostrazione. Prendiamo per assurdo $T \supset Q$ coerente e decidibile. Quindi $\{\ulcorner\varphi\urcorner \mid T \vdash \varphi\}$ è ricorsivo e perciò binumerabile in Q. Quindi esiste $\mathrm{Teo}(x)$ tale che

$$T \vdash \varphi \Rightarrow Q \vdash \mathrm{Teo}(\overline{\ulcorner\varphi\urcorner}) \qquad T \nvdash \varphi \Rightarrow Q \vdash \neg\,\mathrm{Teo}(\overline{\ulcorner\varphi\urcorner})$$

Per diagonalizzazione esiste β tale che $Q \vdash \beta \leftrightarrow \neg\,\mathrm{Teo}_T(\overline{\ulcorner\beta\urcorner})$ e quindi anche $T \vdash \beta \leftrightarrow \neg\,\mathrm{Teo}_T(\overline{\ulcorner\beta\urcorner})$. Ora se $T \vdash \beta$ si ha $Q \vdash \mathrm{Teo}(\overline{\ulcorner\beta\urcorner})$ quindi a maggior ragione $T \vdash \mathrm{Teo}(\overline{\ulcorner\beta\urcorner})$, ma allora $T \vdash \neg\beta$, per cui $T \vdash \bot$, assurdo. Quindi deve essere $T \nvdash \beta$, allora $\ulcorner\beta\urcorner \notin \{\ulcorner\varphi\urcorner \mid T \vdash \varphi\}$, $Q \vdash \neg\,\mathrm{Teo}(\overline{\ulcorner\beta\urcorner})$, allora anche $T \vdash \neg\,\mathrm{Teo}(\overline{\ulcorner\beta\urcorner})$, ma quindi $T \vdash \beta$ assurdo. □

Corollario 23.4. Se $T \supset Q$, e T è ricorsivamente assiomatizzata, allora T è incompleta.

Questo rafforza il Teorema di Gödel perché non stiamo usando l'ipotesi di ω-coerenza.

C'è una seconda dimostrazione di questo stesso fatto di Rosser, si trova sugli appunti di Berarducci. L'idea è costruire una formula che dice "io non sono dimostrabile prima della mia negazione".

Teorema 23.5. Se $L(S) = L(Q)$ e $Q \cup S$ è coerente, allora S è indecidibile.

Dimostrazione. $Q \cup S \vdash \varphi$ se e solo se $S \vdash \bigwedge Q \to \varphi$. Quindi se S fosse decidibile potremmo decidere se la seconda affermazione è vera o falsa, quindi anche la prima, e perciò $Q \cup S$ è decidibile, assurdo perché Q è essenzialmente indecidibile. □

Corollario 23.6. $L = \left\{c, f^2, g^2, h^1\right\}$ (l'apice è l'arietà). L'insieme delle L-formule che sono verità logiche, cioè $\{\varphi \mid\vdash \varphi\}$ è indecidibile.

Dimostrazione. È coerente con Q. Basta chiamare $c = 0, f = +, g = \cdot, h = s$. □

Questo è il Teorema di Church e in sostanza dice che il calcolo dei predicati è indecidibile a patto che il linguaggio sia abbastanza ricco. Notiamo che basta anche che nella segnatura ci sia un simbolo di relazione binaria, in questo caso si usa il Lemma 23.11 prendendo ZF come T e l'insieme degli enunciati logicamente validi come S (Church l'aveva dimostrato col λ-calcolo).

Esempio 23.7. $\mathrm{Th}((\mathbb{Z}, +, \cdot, 0, 1))$ è indecidibile. Questa non estende Q (ad esempio qui c'è il predecessore di 0). Il trucco è osservare che $x \in \mathbb{Z}$ è non negativo se e solo se è somma di quattro quadrati. Quindi posso parlare di naturali dentro $\mathbb{Z}$. Più precisamente posso dire che $\mathbb{N} \models \varphi(\vec{a}) \Leftrightarrow \mathbb{Z} \models \varphi^t(\vec{a})$, dove la traduzione (o interpretazione) t consiste semplicemente nel restringersi ai naturali col trucco sopra menzionato.

In particolare, per le φ chiuse vale $\mathbb{N} \models \varphi \Leftrightarrow \mathbb{Z} \models \varphi^t$. Osserviamo che $\varphi \mapsto \varphi^t$ è calcolabile.

Come corollario so che se $\mathrm{Th}(\mathbb{Z})$ fosse decidibile, lo sarebbe anche $\mathrm{Th}(\mathbb{N})$, e questo è assurdo perché estende Q.

In generale per dare una traduzione (interpretazione) $t : L_A \to L_B$ bisogna dire come si traducono le formule atomiche e il dominio.

Definizione 23.8. T è *interpretabile* in S se esiste una traduzione da $L(T)$ a $L(S)$ che verifica le proprietà che ci si aspetta, che sia calcolabile e tale che $S \vdash T^t$ (per i dettagli vedere gli appunti di Berarducci).

Questo è un caso molto particolare, in generale posso mappare una singola variabile da una parte in tante nell'altra, ad esempio se mappo $\mathbb{P}(\mathbb{R})$ in $\mathbb{R}^2 \setminus \{0\}_{/\sim}$... Posso anche parlare di interpretazione tra modelli, oltre che tra teorie, e chiaramente una tra teorie ne induce una fra ogni coppia di modelli delle teorie. Ad esempio $\mathrm{Th}(\mathbb{N}, +, \cdot, 0, s)$ interpreta $\mathrm{Th}(V_\omega, \in)$ e viceversa, come già visto (a un certo punto ci sarebbe bisogno di scrivere, in V_ω, una cosa del tipo $\forall x \in \omega$; chiaramente così non si può scrivere, ma si riesce a scrivere un predicato che esprime l'essere un numero naturale, tipo $N(x) \leftrightarrow \forall u((x \in u \wedge s(a) \in u \to a \in u) \to \emptyset \in u)$, dove $s(x) = x \cup \{x\}$. Con qualche sforzo in più dimostro che PA interpreta ZF senza l'infinito e viceversa (nella maniera che ci si aspetta si arriva a dire che ZF è indecidibile).

Anche la teoria dei grafi (sul linguaggio $L = \{E\}$ dove E è una relazione binaria) è indecidibile. Cioè:

Teorema 23.9. $\mathrm{Th}(\text{Grafi}) = \{\varphi \mid \varphi \ L\text{-formula} \ , \models \varphi\}$ è indecidibile.

Dimostrazione. Indicando con $\overset{t}{\subseteq}$ l'essere contenuto a meno di traduzioni, si ha

$$Q \subseteq \mathrm{Th}(\mathbb{N}, +, \cdot, 0, s) \overset{t}{\subseteq} \mathrm{Th}(V_\omega, \in) \supseteq \mathrm{Th}(\text{Grafi})$$

Lemma 23.10. $Q \overset{t}{\subset} T \Rightarrow T$ (se coerente) è essenzialmente indecidibile.

Dimostrazione. Ovviamente basta mostrare che è indecidibile. Sia $S = \{\varphi \in L(Q)\text{-formule} \mid T \vdash \varphi^t\} \supset Q$. Quindi S è indecidibile. Ora basta osservare che $S \vdash \varphi \Leftrightarrow \varphi \in S \Leftrightarrow T \vdash \varphi^t$, dove il primo $\Leftrightarrow$ è perché S è deduttivamente chiusa, in sostanza serve che se $\vdash \varphi \to \psi$ allora $T \vdash \varphi^t \Rightarrow T \vdash \psi^t$.

Quindi in sostanza "allargo" Q ad S che è equivalente a T a meno di traduzioni e quindi ho finito. □

Ora mi serve il fatto che Q ha un numero finito di assiomi.

Lemma 23.11. Se $Q \overset{t}{\subset} T \supset S$, e $L(T) = L(S)$, allora S è indecidibile.

Dimostrazione. Siccome Q è finitamente assiomatizzata e $T \vdash Q^t$, per compattezza $\exists T' \subset_{\text{fin}} T$ tale che $T' \vdash Q^t$. Quindi esiste un numero finito di formule $\varphi_1, \dots, \varphi_k$ tale che $Q \overset{t}{\subset} S + \varphi_1, \dots, \varphi_k \supset S$. Ora $S + \varphi_1, \dots, \varphi_k$ è indecidibile perché interpreta Q, ed è un'estensione *finita* di S, e per le estensioni finite le cose funzionano bene, cioè

$$S + \varphi_1, \dots, \varphi_k \vdash \varphi \Leftrightarrow S \vdash \bigwedge \varphi_i \to \psi$$

e quindi se S fosse decidibile lo sarebbe anche $S + \varphi_1, \dots, \varphi_k$, assurdo. □

Questi trucchetti col fatto che gli assiomi sono finiti sono il motivo per cui si lavora con Q invece che con PA. □

Per la teoria degli anelli basta fare

$$Q \subset \text{Th}(\mathbb{N}, +, \cdot) \overset{t}{\subset} \text{Th}(\mathbb{Z}, +, \cdot) \supset \text{Teoria degli anelli}$$

Per i campi è analogo ma serve

Teorema 23.12 (Julia Robinson)**.** In $(\mathbb{Q}, +, \cdot)$ riesco a definire $\mathbb{N}$.