Scuola Estiva Aila 2015
Gargnano, 24-29/08/15

Appunti Appena Sfornati

A cura di
Rosario Mennuni

Corsi tenuti da
Antongiulio Fornasiero
Daniele Mundici
Francesco Paoli
Simona Ronchi Della Rocca
Tamara Servi

Readme

Disclaimer

Questi appunti nascono ad uso e consumo dell'autore, che li ha TEXati in diretta durante i corsi della Scuola Estiva in Logica di Gargnano del 2015. Come conseguenza possono essere inaccurati, incompleti, incomprensibili, fuorvianti, pieni di errori, offensivi, nemici dell'amore, eccetera eccetera. Eventuali omissioni volontarie sono indicate fra parentesi quadre, come ad esempio [definizione già nota all'autore o risultato che per qualche motivo non è stato trascritto].

Info

Questi appunti sono disponibili presso `http://poisson.phc.unipi.it/~mennuni/`. Per segnalazioni errori, suggerimenti, lamentele, insulti, messaggi di sdegno e quant'altro potete rivolgervi a `mennuni@mail.dm.unipi.it`. Questa versione è stata compilata il 29 agosto 2015. Il sorgente è incorporato in questo file e dovreste riuscire a recuperarlo facendo clic destro sulla graffetta o spulciando i menu[1] del vostro visualizzatore di `.pdf` preferito.

Rosario "Mufasa" Mennuni

[1] Se il vostro visualizzatore non ha i menu probabilmente sapete usare il comando `man` e non ho bisogno di spiegarvi come cavarvela da soli.

Indice

Capitolo 1

Antongiulio Fornasiero e Tamara Servi
Teoria dei Modelli

1.1 24/08

Big topics: eliminazione dei quantificatori, model-completezza e decidibilità per strutture con dominio $\mathbb{R}$ o $\mathbb{C}$. Prerequisiti assunti: come funzionano $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, livello liceo. Qualcosa richiederà un po' di algebra, topologia e analisi. Lavoreremo per tutto il corso all'intero della logica del prim'ordine (FO).

Notazione 1.1.1. Un linguaggio si chiamerà tipicamente L. Una L-struttura[1] tenderà a chiamarsi $\mathcal{A}$, e il suo dominio A. Tenderemo a usare notazioni standard e che guidino l'intuizione (in maniera da, ad esempio, poter scrivere $\mathcal{A} = \langle \mathbb{Z}, 0, 1, +, \cdot \rangle$ invece di $\mathcal{A} = \langle \mathbb{Z}, 0^{\mathcal{A}}, 1^{\mathcal{A}}, +^{\mathcal{A}}, \cdot^{\mathcal{A}} \rangle$). I linguaggi sono tutti intesi con uguaglianza.

Definizione 1.1.2. Definiamo le seguenti cose[2]:

- Espansione/restrizione di una struttura
- L-formule e loro interpretazione in una struttura
- Enunciati

Esercizio 1.1.3. Tradurre le seguenti affermazioni in un linguaggio appropriato come enunciati veri nelle relative opportune strutture:

1. $\mathbb{Z}$ è un anello

[1] Qui c'è stata la definizione di struttura, qualche esempio e altre cose di base del genere. Omesse.

[2] Definizioni non riportate, inframmezzate da esempi, anche loro lasciati a casa.

2. $\mathbb{Q}$ è un campo

3. $\mathbb{R}$ è un campo ordinato

4. $\mathbb{C}$ è un campo algebricamente chiuso

Osservazione 1.1.4. Ogni formula può essere messa in forma normale con tutti i quantificatori all'inizio, cioè nella forma

$$Q_1 x_1, \ldots, Q_n x_n \alpha(x_1, \ldots, x_n, y_1, \ldots, y_m)$$

Si può anche supporre che α sia in forma normale disgiuntiva (disgiunzione di congiunzioni di atomiche/negazione di atomiche).

Notazione 1.1.5. Quando scriviamo $\varphi(y_1, \ldots, y_m)$ intendiamo che le variabili libere di φ sono incluse in $\{y_1, \ldots, y_m\}$. Quando scriviamo $\mathcal{A} \vDash \varphi(a_1, \ldots, a_m)$ intendiamo che valutando y_i con a_i la struttura $\mathcal{A}$ (con questa valutazione) è un modello di φ.

Definizione 1.1.6 (Insieme Definibile)**.** La solita. Al solito, "definibile" vuol dire "definibile con parametri", altrimenti diciamo "$\emptyset$-definibile".

Un tema ricorrente in teoria dei modelli è lo studio degli insiemi definibili in una certa struttura; ad esempio stabilire se un insieme è definibile o meno, o descrivere gli insiemi definibili in qualche maniera "semplice".

Esempio 1.1.7. Consideriamo[3] $\overline{\mathbb{C}} = \langle \mathbb{C}, 0, 1, +, -, \cdot \rangle$.

- L'insieme delle radici di un fissato polinomio a coefficienti interi[4] è $\emptyset$-definibile.
- Consideriamo $\mathbb{C}^{\text{alg}}$, l'insieme dei complessi algebrici (cioè che sono soluzione di un qualche polinomio a coefficienti in $\mathbb{Z}$). L'insieme $\mathbb{C}^{\text{alg}}$ non è un insieme $\emptyset$-definibile (ma almeno per ora non vediamo perché)
- L'insieme $\{(a, b, c) \in \mathbb{C}^3 \mid (a \neq 0 \vee b \neq 0) \wedge \forall x(ax^2 + bx + c \neq 0)\}$ è $\emptyset$-definibile (è il vuoto!)
- (altro esempio che mi sono perso)

Definizione 1.1.8. Una funzione è definibile se il suo grafo è definibile. Un insieme è definibile con parametri se è definibile in una qualche espansione con soli nuovi simboli di costante della struttura. D'ora in poi "definibile" vuol dire "definibile con parametri"[5].

[3] Questa notazione ce la porteremo appresso. Io so già che me la dimenticherò e scriverò solo $\mathbb{C}$.

[4] Che a pensarci bene sono gli unici termini del linguaggio.

[5] In letteratura non c'è uno standard.

Esempio 1.1.9. L'insieme delle soluzioni di un sistema di equazioni polinomiali a coefficienti complessi è definibile in $\overline{C}$. $\mathbb{C}^{\text{alg}}$ non è definibile nemmeno con parametri (vedremo in seguito).

Esercizio 1.1.10. Ogni sottoinsieme finito o cofinito del dominio di una struttura è definibile.

Osservazione 1.1.11. Dato $A_0 \subseteq A$, la collezione $\text{Def}_n(\mathcal{A}, A_0)$ dei sottoinsiemi di A^n che sono A_0-definibili forma una *sottoalgebra di Boole* dell'algebra di Boole dei sottoinsiemi di A^n. Questo è ovvio appena uno si accorge di cosa fanno i connettivi logici agli insiemi definibili.

Osservazione 1.1.12. La collezione $\bigcup_{n\in\mathbb{N}} \text{Def}_n(\mathcal{A}, A_0)$ è chiusa per proiezione[6]. Questo è ovvio appena uno si accorge di cosa fa $\exists$ a un insieme definibile: se $\varphi(x_1, \ldots, x_n)$ definisce D allora $\exists x_{i+1}, \ldots, x_n \varphi(x_1, \ldots, x_n)$ definisce $\pi_i(D)$.

L'idea è che con questi strumenti magari sugli insiemi definibili ci si riesce a fare un po' di geometria.

Osservazione 1.1.13. Chiaramente esistono infinite formule che definiscono lo stesso insieme definibile (basta congiungere una tautologia...).

Uno degli scopi della Teoria dei Modelli è trovare formule "semplici" per definire gli insiemi. Per ora associamo informalmente ad ogni formula in forma normale una nozione di complessità: consideriamo le formule senza quantificatori come le più semplici; subito dopo quelle con un solo tipo di quantificatore (ripetuto quanto ci pare). In generale maggiore è l'alternanza fra quantificatore esistenziale e universale e maggiore è la complessità della formula. Questo riflette l'idea che dato un definibile D, verificare se un qualche $\bar{a}$ appartiene a D è tanto più complicato quanto più è complessa la formula che definisce D. Ci torneremo con più precisione.

Definizione 1.1.14. Consideriamo[7] $\overline{\mathbb{R}} = \langle \mathbb{R}, 0, 1, +, -, \cdot, < \rangle$. Gli insiemi definibili senza quantificatori in questa struttura si chiamano *insiemi semialgebrici*.

Basta pensarci un attimo per rendersi conto che sono combinazioni booleane di insiemi della forma $\{\bar{a} \in \mathbb{R}^n \mid p(\bar{a}) = 0\}$ e della forma $\{\bar{a} \in \ mbR^n \mid p(\bar{a}) < 0\}$, dove $n \in \mathbb{N}$ e $p(\bar{x}) \in \mathbb{R}[\bar{x}]$. Sono stati studiati abbastanza, anche indipendentemente dalla logica.

Osservazione 1.1.15. Notiamo che:

- $p(\bar{a}) \cdot q(\bar{a}) = 0 \Leftrightarrow p(\bar{a}) = 0 \vee q(\bar{a}) = 0$

[6] Si intende proiezione sulle prime i coordinate.

[7] Anche sta notazione ce la porteremo appresso e anche questa me la dimenticherò inevitabilmente e scriverò solo $\mathbb{R}$.

- $p(\bar{a})^2 + q(\bar{a})^2 = 0 \Leftrightarrow p(\bar{a}) = 0 \wedge q(\bar{a}) = 0$
- $p(\bar{a}) \neq 0 \Leftrightarrow p(\bar{a}) < 0 \vee -p(\bar{a}) < 0$

Ne segue facilmente che ogni semialgebrico si può scrivere come unione finita di insieme della forma

$$\{\bar{a} \in \mathbb{R}^n \mid p(\bar{a}) = 0, q_1(\bar{a}) < 0, \ldots, q_r(\bar{a}) < 0\}$$

Vediamo un esempio di insieme definibile in $\overline{\mathbb{R}}$ con quantificatori.

Esempio 1.1.16. Consideriamo l'insieme dei coefficienti $a, b, c \in \mathbb{R}$ tali che $ax^2 + bx + c = 0$ ha soluzione in $\mathbb{R}$, ossia

$$\{(a, b, c) \in \mathbb{R}^3 \mid \exists x\ ax^2 + bx + c = 0\}$$

Lo stesso insieme può essere definito dalla formula più semplice

$$\{(a, b, c) \in \mathbb{R}^3 \mid (a \neq 0 \wedge (4ac - b^2 \leq 0)) \vee (a = 0 \wedge (b \neq 0 \vee c = 0))\}$$

Cosa succede se consideriamo un insieme definito da una formula più complessa, con molte alternanza di quantificatori?

Spoiler 1.1.17. Un teorema di Tarski dice che tutti gli insiemi definibili in $\overline{\mathbb{R}}$ sono definibili senza quantificatori.

Osservazione 1.1.18. La relazione d'ordine $\leq$ è definibile con somma e prodotto: i positivi sono i quadrati non nulli. Quindi basta definire $a < 0 \equiv \exists x(-a \cdot x^2 = 1)$. Il problema è che questa relazione introduce un quantificatore, per cui preferiamo inserire la relazione nel linguaggio.

Esercizio 1.1.19. Descrivere i sottoinsiemi di $\mathbb{R}$ definibili in $\overline{\mathbb{R}}$ senza quantificatori.

Esercizio 1.1.20. Si consideri $\mathbb{R}$ con la topologia euclidea e siano $f\colon \mathbb{R} \to \mathbb{R}$ e $D \subseteq \mathbb{R}^n$ rispettivamente una funzione e un insieme definibili in $\overline{\mathbb{R}}$. Scrivere un enunciato che afferma che f è una funzione continua e che D è un insieme aperto.

Esempio 1.1.21. Siano $\overline{\mathbb{N}}$ e $\overline{\mathbb{Z}}$ le $\{+, \cdot\}$-strutture che ci si aspetta dalla notazione. Allora $\mathbb{Z}$ può essere definito in $\mathbb{Z}$ senza parametri (ogni intero positivo è somma di quattro quadrati). Dato che le operazioni di $\overline{\mathbb{N}}$ non sono che le restrizioni di quelle di $\overline{\mathbb{Z}}$, in un qualche senso possiamo dire che l'intera struttura $\overline{\mathbb{N}}$ è $\emptyset$-definibile in $\mathbb{Z}$. Per i teoremi di Gödel quindi anche $\mathbb{Z}$ non è decidibile (il discorso subito sopra ci permette di associare ad ogni φ una φ' tale che $\overline{\mathbb{N}} \vDash \varphi \Leftrightarrow \overline{\mathbb{Z}} \vDash \varphi'$).

1.2 25/08

Esercizio 1.2.1. Sia $\mathbb{R}^{\text{alg}}$ l'insieme dei reali algebrici (che annullano un polinomio a coefficienti interi). Allora l'insieme delle soluzioni di un sistema di equazioni polinomiali a coefficienti in $\mathbb{R}^{\text{alg}}$ è $\emptyset$-definibile in $\overline{\mathbb{R}}$.

Suggerimento. Sia $a \in \mathbb{R}^{\text{alg}}$. Trovare una $L(\overline{\mathbb{R}})$-formula $\varphi(x)$ tale che $\{a\} = \{x \in \mathbb{R} \mid \overline{\ } \vDash \varphi(x)\}$. Questo si fa partendo da un polinomio p di cui a è radice, e poi isolandola dalle altre usando la struttura d'ordine. Fatto questo è facile sbarazzarsi del parametro a: se ad esempio vogliamo mostrare la tesi per $ax^2 + 2x + 1$, definiamo l'insieme delle sue radici con

$$\{x \in \mathbb{R} \mid \exists y\big(\varphi(y) \wedge yx^2 + 2x + 1 = 0\big)\}$$

che funziona perché a è l'unica "soluzione" di φ. □

Cosa succede se proviamo a fare la stessa cosa con $\mathbb{C}^{\text{alg}}$? Ad esempio consideriamo $\{a \in \mathbb{C} \mid a^2 + 1 = 0\} = \{i, -i\}$. Succede che $\overline{\mathbb{C}}$ non "distingue" le due radici del polinomio (poi vediamo perché), dunque $\{i\}$ non è $\emptyset$-definibile.

[esempi di strutture che concordano o non concordano sul valore di verità di un enunciato e definizione di equivalenza elementare]

Domanda: come stabilire se due strutture sono elementarmente equivalenti? Come caratterizzare tutte le strutture elementarmente equivalenti a una struttura fissata?

[definizioni di teoria, modello, conseguenza logica]

Definizione 1.2.2. Data una teoria T, la sua *chiusura deduttiva* $\bar{T}$ è l'insieme degli enunciati che sono conseguenza logica di T.

Notiamo che $\text{Mod}(T) = \text{Mod}(\bar{T})$.

[definizioni di teoria completa e teoria di una struttura]

Esercizio 1.2.3. $\text{Th}(\mathcal{A})$ è una teoria completa e deduttivamente chiusa.

Notazione 1.2.4. In questo corso considereremo solo teorie coerenti, cioè dotate di almeno un modello.

Esempio 1.2.5. Un esempio di teoria non completa è la teoria dei campi.

Lemma 1.2.6. Sia T una L-teoria. TFAE:

1. $\forall \mathcal{A}, \mathcal{B} \in \text{Mod}(T)\ \mathcal{A} \equiv \mathcal{B}$
2. T è completa
3. Se $T' \supseteq T$ è una L-teoria allora $\overline{T'} = \overline{T}$
4. $\overline{T} = \text{Th}(\mathcal{A})$ per qualunque $\mathcal{A} \in \text{Mod}(T)$

Dimostrazione.

$1 \Rightarrow 2$ Sia φ un L-enunciato. Se φ non è conseguenza logica di T esiste un modello $\mathcal{A}$ di T in cui è vera $\neg\varphi$. Per ipotesi $\neg\varphi$ è vera in tutti i modelli di T, ovvero $T \vDash \neg\varphi$.

$2 \Rightarrow 3$ Sia $\varphi \in \overline{T'}$. È facile vedere che (anche senza l'ipotesi 2) $\overline{T'} \supseteq \overline{T}$. Dato che T è completa o $\varphi \in \overline{T}$ oppure $\neg\varphi \in \overline{T}$. Ma se $\neg\varphi \in \overline{T} \subseteq \overline{T'}$, avremmo che T' sarebbe incoerente, quindi necessariamente $\varphi \in \overline{T}$.

$3 \Rightarrow 4$ Sia $\mathcal{A} \in \mathrm{Mod}(T)$. Evidentemente $\overline{T} \subseteq \mathrm{Th}(\mathcal{A})$, e per massimalità queste coincidono.

$4 \Rightarrow 1$ $\forall \mathcal{A}, \mathcal{B} \in \mathrm{Mod}(T)$ abbiamo $\mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B})$, e quindi $\mathcal{A} \equiv \mathcal{B}$

□

Dunque una prima risposta alle domande che ci siamo fatti è: data una classe di L-strutture, se troviamo una teoria completa di cui sono tutte modelli, ogni coppia di strutture nella classe è elementarmente equivalente.

Definizione 1.2.7. Data una L-teoria T, un sottoinsieme $S \subseteq T$ è un insieme di *assiomi* per T se $\overline{S} = \overline{T}$.

Data una L-struttura $\mathcal{A}$, come caratterizzare tutti i modelli di $\mathrm{Th}(\mathcal{A})$? Un modo per farlo è trovare un insieme di assiomi per $\mathrm{Th}(\mathcal{A})$; dunque cerchiamo una sottoteoria $T \subseteq \mathrm{Th}(\mathcal{A})$ che sia completa e che consista in una lista esplicita di enunciati, che magari sia matematicamente "pregna di senso"[8]. Ad esempio, supponiamo di voler descrivere $\mathrm{Th}(\overline{\mathbb{C}})$. Iniziamo a elencare qualche proprietà della struttura che ci viene in mente e scriviamola come assiomi:

- $\overline{\mathbb{C}}$ è un campo. Questo non basta, perché la teoria dei campi non è completa (ad esempio $\exists x\ x^2 = 2\ldots$)
- $\overline{\mathbb{C}}$ è un campo *algebricamente chiuso*, cioè ogni polinomio non costante a coefficiente in $\mathbb{C}$ ha una radice. Questo non è fattibile con un singolo enunciato, ma con una lista infinita sì: basta scrivere, per ogni $n \in \mathbb{N}$, un enunciato che dice che tutti i polinomi monici di grado n hanno una radice, quantificando sui coefficienti:

$$\forall a_0, \ldots, a_{n-1}\ \exists x\ x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

  Questo ancora non basta: se prendiamo $\mathbb{Z}/2\mathbb{Z}$ e ne consideriamo la chiusura algebrica, questa soddisfa $1 + 1 = 0$, mentre $\overline{\mathbb{C}}$ chiaramente no

[8] Prendere $\mathrm{Th}(\mathcal{A})$ per intero siamo buoni tutti.

- $\overline{\mathbb{C}}$ è un campo algebricamente chiuso *di caratteristica* 0, cosa esprimibile usando, per ogni $n \in \mathbb{N}$, un assioma che dice che la somma di n volte 1 è diversa da 0

Spoiler 1.2.8 (Tarski)**.** Questo basta: la teoria ACF_0 dei campi algebricamente chiusi di caratteristica 0 è completa.

Mostrarlo (o in generale mostrare che una data teoria è completa) non è banalissimo. Comunque questo ci dice che $\overline{\mathbb{C}}$ è caratterizzato, a meno di elementare equivalenza, dagli assiomi di campo algebricamente chiuso di caratteristica 0.

Esercizio 1.2.9 (Cattivello)**.** Abbiamo già incontrato (di sfuggita) un altro modello di questa teoria (o meglio il suo dominio); quale?

La descrizione di $\mathrm{Th}(\overline{\mathbb{C}})$ come ACF_0 ha il vantaggio di identificare delle proprietà algebrica note come "tutto quello che c'è da dire al prim'ordine" su $\overline{\mathbb{C}}$. C'è anche un altro vantaggio: la lista è "esplicita", nel senso che esiste un algoritmo che decide in tempo finito se un enunciato è un assioma oppure no.

Spoiler 1.2.10. Come conseguenza di questo fatto otteniamo un algoritmo che, dato un qualunque enunciato, decide in tempo finito se questo è una conseguenza logica degli assiomi.

[giustificazione informale di questa cosa passando dal teorema di completezza: provo tutte le dimostrazioni, dato che gli assiomi sono decidibili e la teoria è completa basta provare tutte le dimostrazione per φ e in parallelo per $\neg\varphi \ldots$]

Definizione 1.2.11. Una L-teoria T è *ricorsivamente assiomatizzabile* se esiste un insieme di assiomi S per T e un algoritmo che, dato un L-enunciato φ, stabilisce in tempo finito se $\varphi \in S$ oppure no. È *decidibile* se esiste un algoritmo che in tempo finito decide se φ è conseguenza logica di T oppure no.

Dunque ieri abbiamo detto che $\mathrm{Th}(\overline{\mathbb{N}})$ e $\mathrm{Th}(\overline{\mathbb{Z}})$ non sono decidibili, e la giustificazione informale di sopra dice che

Teorema 1.2.12. Una teoria ricorsivamente assiomatizzabile e completa e decidibile.

Osservazione 1.2.13. Le ipotesi possono essere indebolite, richiedendo che l'assiomatizzazione sia solamente *ricorsivamente enumerabile*.

Corollario 1.2.14. ACF_0 è decidibile.

Definizione 1.2.15. Data una L teoria T e due formule $\varphi(\bar{x})$ e $\psi(\bar{x})$, diciamo che φ e ψ sono T*-equivalenti* se $T \vDash \forall \bar{x}\ (\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$.

In altre parole, in tutti i modelli di T l'insieme definito da ψ e da φ è lo stesso. L'idea ora è, data una formula φ, cercare una L-formula ψ più semplice che sia T-equivalente a φ.

Definizione 1.2.16. Una L-teoria T *ammette eliminazione dei quantificatori* se ogni L-formula è T-equivalente a una formula senza quantificatori.

In altre parole, se tutti gli insiemi definibili sono definibili senza quantificatori. L'idea è che gli insiemi definiti senza quantificatori hanno una descrizione geometrica semplice. Prendiamo ad esempio $\overline{\mathbb{R}}$ e consideriamo l'insieme dei coefficienti di un polinomio monico di grado 3 che abbia tre soluzioni reali distinte:

$$A = \left\{ (a,b) \in \mathbb{R}^2 \;\middle|\; \exists x_1, x_2, x_3 \left(\bigwedge_{i \neq j} x_i \neq x_j \wedge \bigwedge_{i=1,2,3} x_i^3 + a x_i + b = 0 \right) \right\}$$

A può essere definito, grazie alla formula di Cardano, come $A = \{(a,b) \in \mathbb{R}^2 \mid 4a^3 + 27b^2 < 0\}$. Geometricamente, usare la prima definizione ci costringe a partire da un sottoinsieme di $\mathbb{R}^5$, capire com'è fatto, proiettarlo, eccetera, e questo non dà tantissima informazione sulla forma di A. La seconda intanto non costringe ad andare in uno spazio più grande, inoltre la descrizione è molto semplice: sono i punti dove una funzione polinomiale è negativa, in questo caso una regione delimitata da una cuspide.

Osservazione 1.2.17. Supponiamo di avere un algoritmo che dato un L-enunciato φ restituisca ψ a lui T-equivalente e senza quantificatori. Supponiamo inoltre di avere un algoritmo di decisione per gli enunciati senza quantificatori di T. Allora T è chiaramente decidibile.

Consideriamo di nuovo $\overline{\mathbb{R}}$. Come già detto (in altri termini), per un risultato di Tarski $\mathrm{Th}(\mathbb{R})$ ha eliminazione dei quantificatori. Il Teorema è in realtà più forte: l'eliminazione dei quantificatori è algoritmica. Ma cosa sono gli enunciati senza quantificatori di $\mathrm{Th}(\overline{\mathbb{R}})$? Non sono altro che combinazioni booleane di enunciati della forma $m = n$ e $m < n$, con $m, n \in \mathbb{Z}$, e decidere se questi sono veri o falsi è fattibile algoritmicamente. Dunque $\mathrm{Th}(\overline{\mathbb{R}})$ è completa.

Osservazione 1.2.18. Sia T una L-teoria *incompleta*. Un modo per estenderla a una teoria completa e prendere $\mathcal{A} \in \mathrm{Mod}(T)$ e considerare $\mathrm{Th}(\mathcal{A})$. Supponimao di voler classificare tutti i completamenti di T. Se $\mathcal{A}, \mathcal{B}$ sono due modelli di T non elementarmente equivalenti, esiste φ tale che $\mathcal{A} \vDash \varphi$ e $\mathcal{B} \vDash \neg\varphi$. Se T ammette eliminazione dei quantificatori possiamo supporre che φ sia senza quantificatori.

Consideriamo ACF, la teoria dei campi algebricamente chiusi (di caratteristica arbitraria). Per un altro Teorema di Tarski questa ha eliminazione dei

quantificatori; ma chi sono gli enunciati senza quantificatori di ACF? Sono esattamente le combinazioni booleane de enunciati della forma $m = 0$, con $m \in \mathbb{Z}$. Dunque, i completamenti di ACF sono interamente determinati dalla *caratteristica* dei loro modelli. In altre parole tutti e soli i completamenti di ACF sono della forma ACF_p, dove p è 0 oppure un primo.

Proposizione 1.2.19. Sia $\mathcal{K} = \langle K, 0, 1, +, -, \cdot \rangle$ un campo tale che $\mathrm{Th}(\mathcal{K})$ ammetta eliminazione dei quantificatori. Allora ogni sottoinsieme definibile di K (dunque quelli di dimensione 1) è finito o cofinito.

Dimostrazione. Sia $A \subseteq K$ definibile. Prendiamo una formula senza quantificatori che lo definisce. Questa è combinazione booleana di formule del tipo $p(x) = 0$, con $p(x)$ a coefficienti in K, e la tesi segue immediatamente (esercizio) dal fatto che un polinomio non nullo ha un numero finito di radici. □

Corollario 1.2.20. I sottoinsiemi di $\mathbb{C}$ definibili in $\overline{\mathbb{C}}$ sono finiti o cofiniti. In particolare $\mathbb{C}^{\mathrm{alg}}$ non è definibile in $\overline{\mathbb{C}}$ (è infinito e coinfinito).

Definizione 1.2.21. Una struttura infinita tale che tutti i sottoinsiemi definibili del dominio sono finiti o cofiniti è detta *minimale*. Una teoria completa i cui modelli siano tutti minimali è detta *fortemente minimale*.

Esempio 1.2.22. Segue da quanto visto che $\overline{\mathsf{ACF}_0} = \mathrm{Th}(\overline{\mathbb{C}})$ è fortemente minimale.

Perché "minimale"? L'idea è che i sottoinsiemi del dominio sono i più semplici che ci si possa aspettare, ovvero definibili da formule senza quantificatori che coinvolgono solo il simbolo $=$. Perché "fortemente"? La finitezza/cofinitezza non è esprimibile con un insieme di enunciati (poi vedremo) e non si preserva per elementare equivalenza. Ci sono esempi di teoria complete che hanno alcuni modelli minimali e altri no.

Esercizio 1.2.23. $\mathbb{C}^{\mathrm{alg}}$ è un campo algebricamente chiuso di caratteristica 0.

Sia $\overline{\mathbb{C}^{\mathrm{alg}}} = \langle \mathbb{C}^{\mathrm{alg}}, 0, 1, +, -, \cdot \rangle \vDash \mathsf{ACF}_0$. Per completezza della teoria $\overline{\mathbb{C}} \equiv \mathbb{C}^{\mathrm{alg}}$. Dunque il fatto che $\mathbb{C}$ contenga trascendenti (elementi non algebrici) non può essere espresso con un enunciato del linguaggio dei campi.

Vediamo ora perché $\{i\}$ non è $\emptyset$-definibile in $\overline{\mathbb{C}}$ (anche se $\{i, -i\}$ lo è). Supponiamo di avere $\varphi(x)$ tale che $\{i\} = \{x \mid \overline{\mathbb{C}} \vDash \varphi(x)\}$, che per Tarski possiamo supporre essere priva di quantificatori. Mettiamola in forma normale disgiuntiva, cioè scriviamola come disgiunzione finita di formule della forma

$$p_1(x) = 0 \wedge \ldots \wedge p_k(x) = 0 \wedge q_1(x) \neq 0 \wedge \ldots \wedge q_\ell(x) \neq 0$$

con i $p_i, q_j \in \mathbb{Z}[x]$.

Claim 1.2.24. i e $-i$ soddisfano esattamente le stesse relazioni polinomiali.

Per quanto detto finora, mostrare il Claim conclude.

Dimostrazione del Claim, prima maniera. Il coniugio lascia invariati i polinomi a coefficienti in $\mathbb{Z}$:

$$p(i) = 0 \Leftrightarrow \overline{p(i)} = 0 \Leftrightarrow p(-i) = 0$$

□

Dimostrazione del Claim, seconda maniera. Mostriamo via divisione euclidea che se $p(i) = 0$ allora $p(x)$ è divisibile per $x^2 + 1$: scriviamo $p(x) = (x^2 + 1)q(x) + r(x)$, con $r(x) = ax + b$. Sostituendo i a x otteniamo che $a = b = 0$, cioè $r(x)$ è nullo e p è divisibile per $x^2 + 1$. □

Osservazione 1.2.25. Questo può essere generalizzato facilmente per mostrare la stessa cosa per qualunque algebrico di grado > 1, rimpiazzando $x^2 + 1$ con il polinomio minimo dell'elemento algebrico in questione. Anche il primo metodo può essere generalizzato, modulo sapere un po' di Teoria di Galois.

Il teorema di Tarski richiamato più volte dice che $\mathrm{Th}(\overline{\mathbb{R}})$ ha eliminazione dei quantificatori ed è decidibile. Enunceremo un teorema più generale che fornirà anche un'assiomatizzazione ricorsiva di $\mathrm{Th}(\overline{\mathbb{R}})$.

Definizione 1.2.26. Un campo ordinato K è *reale chiuso* se vale il teorema del valor medio, ossia se ogni polinomio a coefficienti in K che cambia segno ha uno zero (fra i due punti in cui cambia segno): se $p(x) \in K[x]$ ed esistono $a, b \in K$ tali che $a < b$ e $p(a) \cdot p(b) = 0$ allora esiste $c \in (a, b)$ tale che $p(c) = 0$. Chiamiamo la teoria dei campi ordinati reali chiusi RCF.

Esercizio 1.2.27. Scriverlo nel linguaggio dei campi ordinati (anche usando infiniti enunciati).

Notiamo che RCF è ricorsivamente assiomatizzata.

Teorema 1.2.28. RCF ammette eliminazione *effettiva* dei quantificatori.

Dato che $\mathsf{RCF} \subseteq \mathrm{Th}(\overline{\mathbb{R}})$, anche questa teoria ha eliminazione dei quantificatori effettiva, perché

Corollario 1.2.29. RCF è una teoria completa.

Idea della Dimostrazione. Sia φ un enunciato del linguaggio dei campi ordinati, che per il Teorema è WLOG combinazione booleana di enunciati della forma $m = n$ e $m < n$, con $m, n \in \mathbb{Z}$. Il valore di verità di questi enunciati è indipendente dalla scelta del modello di RCF (domani vediamo perché). □

Esistono esempi di grande interesse matematico di campi reali chiusi diversi da $\overline{\mathbb{R}}$ (ad esempio alcuni campi di serie formali). Grazie al Corollario precedente tutte le proprietà di $\overline{\mathbb{R}}$ esprimibili nel linguaggio dei campi ordinati sono vere in tutti i campi reali chiusi. Questo principio di *transfer* della verità degli enunciati da $\overline{\mathbb{R}}$ ad altri modelli di RCF permette di ottenere automaticamente dei risultati in tali modelli che sarebbero altrimenti complicati da dimostrare direttamente. In altre parole dato un enunciato φ vero in $\overline{\mathbb{R}}$, anche se sappiamo che è vero perché l'abbiamo dimostrato usando strumenti non a disposizione in altri campi reali chiusi[9] sappiamo che esiste una dimostrazione in RCF e quindi possiamo "fare finta" di lavorare con $\overline{\mathbb{R}}$.

1.3 26/08

Una definizione alternativa di campo reale chiuso è

Definizione 1.3.1. Un campo ordinato K è *reale chiuso* se ogni polinomio di grado dispari ha almeno una radice in K.

Il Teorema 1.2.28 ha il seguente

Corollario 1.3.2. RCF è un'assiomatizzazione ricorsiva di $\mathrm{Th}(\overline{\mathbb{R}})$, che è dunque una teoria decidibile: esiste una procedura algoritmica per decidere la verità e la falsità degli $L(\overline{\mathbb{R}})$-enunciati nella struttura $\overline{\mathbb{R}}$

L'algoritmo della dimostrazione del Teorema ha un difetto: ha una complessità troppo alta per renderlo utile a fini pratici. Ci sono stati studi per migliorarlo, ma comunque Fischer e Rabin (1974) e Davenport e Heinz (1997) hanno mostrato che qualunque algoritmo è almeno doppiamente esponenziale; dato che un algoritmo del genere è stato dato da Collins (1975, Cylindrical Algebraic Decompositions), la ricerca si è poi mossa su metodi di decisione per alcune sottoclassi della classe di tutte le formule. In altre parole la teoria dei modelli non ci fornisce algoritmi efficienti (ma comunque sapere che qualcosa è decidibile è un bel plus).

Altro corollario immediato:

Corollario 1.3.3. I definibili di $\overline{\mathbb{R}}$ sono tutti e soli i semialgebrici.

In particolare, dato che i definibili sono stabili per complemento (basta prendere la negazione), anche i semialgebrici lo sono (e mostrare questo direttamente con mezzi geometrici non è facilissimo). Dato che i semialgebrici sono "semplici" per il risultato di eliminazione dei quantificatori, salta fuori che hanno un sacco di proprietà geometriche interessanti; d'altra parte le famiglie di definibili sono sufficientemente "ricche" da avere una struttura interessante.

[9] Per esempi: ce n'è un libro: Michel Coste, Roy, [terzo autore] - real closed fields qualcosa

Riprendiamo l'esempio dell'equazione di secondo grado

$$A = \{(a,b,c) \in \mathbb{R}^3 \mid \overline{\mathbb{R}} \vDash a \neq 0 \wedge \exists x(ax^2 + bx + c = 0)\}$$

abbiamo già visto che questo è definibile anche dalla formula $b^2 - 4ac \geq 0$. D'altra parte abbiamo anche una formula risolutiva (la solita).

Osservazione 1.3.4. Le funzioni (viste come funzioni delle variabili a, b, c sono definibili).

Esercizio 1.3.5. Scrivere la definizione.

È anche vero che non sono esprimibili come termini del linguaggio dei campi ordinati, dato che non abbiamo né un simbolo di divisione né un simbolo di radice quadrata. In altre parole avere l'eliminazione dei quantificatori non implica saper risolvere le equazioni come termini del linguaggio. Dunque l'idea è espandere il linguaggio aggiungendo un simbolo di divisione (convenendo che la divisione per 0 fa 0) e per ogni $n \in \mathbb{N}$ un simbolo per $\sqrt[n]{}$. Questo è sufficiente? No: per un noto teorema di Galois esistono equazioni polinomiali senza formule risolutive per radicali (cioè che coinvolgano solo somma, prodotto, quozienti e radici). Chiaramente se espandiamo il linguaggio con un simbolo di funzione per ogni soluzione di ogni equazione polinomiale andiamo in porto; il problema è che questo linguaggio è troppo ricco (e "implicito") e non ci fornisce nessuna nuova informazione sull(a natura dell)e soluzioni, (mentre sapere che una è $(-b + \sqrt{b^2 - 4ac})/2a \ldots$. Dunque la domanda diventa: esiste un'espansione "ragionevole" del linguaggio in cui esprimere le soluzioni (o, più in generale, le funzioni definibili) come termini?

Viceversa, supponiamo di avere una struttura $\mathcal{A}$ in un linguaggio L abbastanza ricco da esprimere ogni funzione definibile come termine. Allora $\mathrm{Th}(\mathcal{A})$ ammette l'eliminazione dei quantificatori[10]: infatti se $B \subseteq A^n$ è definibile consideriamo

$$\chi_B(\bar{x}) = \begin{cases} 1 & \text{se } \bar{x} \in B \\ 0 & \text{se } \bar{x} \notin B \end{cases}$$

Dato che B è definibile in $\mathcal{A}$, allora $\chi : B$ è definbile in $\mathcal{A}$ (esercizio), e per ipotesi si esprime come un termine. Ma allora $\chi_B(\bar{x}) = 1$ è una L-formula senza quantificatori che definisce B.

Qui abbiamo leggermente "barato", nel senso che questa situazione è troppo bella per capitare; in genere si riescono a definire le cose a "pezzi", nel senso che non ci basta un termine e dobbiamo definire le cose lungo una partizione.

Domanda: dato che $<$ è definibile, se togliamo il simbolo dal linguaggio dei campi ordinati, abbiamo ancora eliminazione dei quantificatori? La risposta è no:

[10] Anzi, questo è uno dei metodi per mostrare l'eliminazione dei quantificatori.

Dimostrazione. L'insieme definibile $\{a \in \mathbb{R} \mid \exists x \ -a \cdot x^2 = 1\}$ è la semiretta dei negativi, che è infinito e coinfinito, il che cozza con la Proposizione 1.2.19. □

Chiaramente lo stesso argomento vale in qualunque $\mathcal{R} \vDash \mathsf{RCF}$, il che mostra che

Corollario 1.3.6. I campi reali chiusi non sono minimali.

Quindi la domanda diventa: dato un RCF, c'è una maniera "semplice" per descrivere i suoi sottoinsiemi definibili? Per Tarski sappiamo che sono insiemi definibili senza quantificatori, ossia combinazioni booleane di luoghi di zeri di polinomi e luoghi di negatività di polinomi (a coefficienti nel campo in questione). Gli insiemi di zeri sono chiaramente finiti; d'altra parte quelli del secondo tipo, per la proprietà del valore intermedio, sono unioni di intervalli aperti come $(-\infty, a_1), (a_1, a_2), \ldots, (a_r, +\infty)$. Infatti fra—ad esempio—a_1 e a_2 il polinomio non può cambiare segno perché altrimenti avrebbe uno zero per ipotesi. Ne segue che

Proposizione 1.3.7. I sottoinsiemi di R definibili in $\mathcal{R} \vDash \mathsf{RCF}$ sono unioni finite di intervalli aperti (illimitati o illimitati) e punti.

Questa cosa è sufficientemente interessante da meritarsi un nome:

Definizione 1.3.8. Una struttura infinita totalmente ordinata[11] tale che tutti i sottoinsiemi definibili del dominio sono unioni finite di intervalli e punti è detta *o-minimale*.

In analogia al caso minimale, i sottoinsiemi definibili del dominio sono definibili con formule senza quantificatori che coinvolgono solo $=$ e $<$ (a prescindere da cosa altro ci sia nel linguaggio). In un certo senso sono quindi le strutture totalmente ordinate più "semplici".

Come nel caso minimale non è possibile esprimere la proprietà di o-minimalità con un insieme di enunciati (vedremo) Tuttavia (Knight, Pillay, Steinhorn), data T teoria completa di strutture totalmente ordinate, se T ha un modello o-minimale *tutti i suoi modelli lo sono*. Dunque si parla di *strutture o-minimali* senza bisogno di aggiungere *fortemente*.

Un sacco di funzioni reali interessanti non sono semialgebriche: ad esempio

Esercizio 1.3.9. $\exp(x) = e^x$ non è semialgebrica

Soluzione. Se lo fosse esisterebbero polinomi $p(x, y), q_1(x, y), \ldots, q_r(x, y)$ tali che

$$\{(x, y) \in \mathbb{R}^2 \mid y = e^x\} = \left\{ (x, y) \in \mathbb{R}^2 \;\middle|\; p(x, y) = 0 \wedge \bigwedge q_i(x, y) < 0 \right\}$$

[11] Chiaramente nel linguaggio ci deve essere un simbolo interpretato come ordine. La *o* di "o-minimale" sta proprio per "ordine".

in altre parole per ogni $x \in \mathbb{R}$ avremmo $p(x, e^x) = 0$ e $q_i(x, e^x) < 0$, e questo è impossibile: infatti intanto notiamo che $p(x, e^x) = 0$ deve comparire "per davvero" (con solo disuguaglianze avremmo aperti, e il grafico dell'esponenziale non lo è). Scriviamo

$$p(x, y) = \sum_{i=0}^{n} a_i(x) y^i$$

con gli a_i polinomi. Sostituendo $y = e^x$ otteniamo

$$a_n(x)e^{nx}\left(1 + \frac{a_{n-1}}{a_n}(x)e^{-x} + \ldots + \frac{a_0}{a_n}(x)e^{-nx}\right) = 0$$

passando al limite per $x \to +\infty$ otteniamo $1 = 0$. □

Quindi se vogliamo l'esponenziale bisogna aggiungercelo a calci:

Definizione 1.3.10. Consideriamo $L_{\exp}$, espansione del linguaggio dei campi ordinati con un simbolo di funzione unario exp da interpretare come la funzione esponenziale e definiamo $\mathbb{R}_{\exp}$ espandendo $\overline{\mathbb{R}}$ come ci si aspetta.

È possibile ottenere risultati come quelli precedenti per questa struttura?

Spoiler 1.3.11. È o-minimale.

Questo non è facilissimo da mostrare; intanto vediamo cosa sappiamo sui definibili senza quantificatori. I termini in una variabile qui possono essere bestie del tipo

$$x^2 e^{3x^5+e^5} - 1 \qquad e^{e^{e^{e^x}}} - x^5 \qquad e^{3x^2+4x^5-e^{x^2}}$$

i termini più semplici sono i *polinomi esponenziali* $f(x) = p(x, e^x)$, dove $p \in \mathbb{Z}[x, y]$. Persino per questi oggetti non sappiamo nemmeno se un'equazione della forma $f(x) = 0$ ha o meno un numero finito di soluzioni. (È vero ma non facile, è un risultato di Khovanskii). Anche sapendo questa cosa non sappiamo se $\operatorname{Th}\mathbb{R}_{\exp}$ ha eliminazione dei quantificatori; quindi a priori gli insiemi definibili sono parecchio complicati, e non è chiaro come stabilire se $\mathbb{R}_{\exp}$ sia o-minimale o meno. Questo per dire che la questione è tutt'altro che ovvia.

I definibili in strutture o-minimali (di tutte le arietà) hanno delle proprietà geometriche interessanti, molte delle quali "ereditate" dai semialgebrici. Ad esempio sapere che $\mathbb{R}_{\exp}$ è o-minimale ha le seguenti conseguenze:

- I sottoinsiemi di $\mathbb{R}^n$ definibili in $\mathbb{R}_{\exp}$ hanno un numero finito di componenti connesse
- Le funzione $f\colon \mathbb{R} \to \mathbb{R}$ deifnibili sono continue (derivabili) a tratti e con un numero finito di zeri (in particolare dimentichiamoci di definire cose come il seno)

- Uniforme finitezza: sia $\varphi(x, y_1, \ldots, y_n)$ una $L_{\exp}$-formula tale che $\forall \bar{a} \in mbR^n$ l'insieme $A_{\bar{a}} = \{x \in \mathbb{R} \mid \mathbb{R}_{\exp} \vDash \varphi(x, \bar{a})\}$ è finito. Allora esiste $N \in \mathbb{N}$ tale che $\forall \bar{a} \in \mathbb{R}^n$ si ha che $A_{\bar{a}}$ ha al più N punti.

Definizione 1.3.12. Sia L un linguaggio e siano $\mathcal{A}$, $\mathcal{B}$ due strutture tali che $A \subseteq B$. Diciamo che $\mathcal{A}$ è una *sottostruttura* di $\mathcal{B}$ (e scriviamo $\mathcal{A} \subseteq \mathcal{B}$) se

- Per ogni simbolo di costante c si ha $c^{\mathcal{A}} = c^{\mathcal{B}}$
- Per ogni $\bar{a} \in A^n$ e ogni simbolo f di funzione n-ario di L, si ha $f^{\mathcal{A}}(\bar{a}) = f^{\mathcal{B}}(\bar{a})$
- Per ogni $\bar{a} \in A^n$ e R simbolo di relazione n-ario in L, si ha $\bar{a} \in R^{\mathcal{A}} \Leftrightarrow \bar{a} \in R^{\mathcal{B}}$

Diciamo anche che $\mathcal{B}$ è un *estensione*[12] di $\mathcal{A}$.

Proposizione 1.3.13. $\mathcal{A} \subseteq \mathcal{B}$ sse per ogni L-formula senza quantificatori $\varphi(\bar{x})$ e ogni $\bar{a} \in A^n$ si ha $\mathcal{A} \vDash \varphi(\bar{a}) \Leftrightarrow \mathcal{B} \vDash \varphi(\bar{a})$.

Esercizio 1.3.14. Dimostrarlo (si fa per induzione sulla complessità della formula).

Cosa succede se testiamo la verità di *tutte* le formule?

Definizione 1.3.15. Diciamo che $\mathcal{A}$ è una *sottostruttura elementare* di $\mathcal{B}$ (e scriviamo $\mathcal{A} \preceq \mathcal{B}$) se per ogni L-formula $\varphi(\bar{x})$ e $\bar{a} \in A^n$ si ha $\mathcal{A} \vDash \varphi(\bar{a}) \Leftrightarrow \mathcal{B} \vDash \varphi(\bar{a})$.

Osservazione 1.3.16. Se $\mathcal{A} \preceq \mathcal{B}$ allora $\mathcal{A} \equiv \mathcal{B}$: basta guardare solo gli enunciati (cioè ignorare $\bar{a}$). Per le normali sottostrutture questo non è vero.

Esempio 1.3.17. Nelle notazioni usate finora $\overline{\mathbb{N}} \subseteq \overline{\mathbb{Z}}$, ma (esercizio) $\overline{\mathbb{N}} \not\equiv \overline{\mathbb{Z}}$ (in particolare $\overline{\mathbb{N}} \not\preceq \overline{\mathbb{Z}}$).

Esempio 1.3.18. $\langle \mathbb{Z}/2\mathbb{Z}, 0, 1, +, \cdot \rangle$ non è nemmeno una sottostruttura di $\overline{\mathbb{Z}}$: non sono d'accordo un particolare enunciato senza quantificatori $(1+1=0)$

Esempio 1.3.19. $\overline{\mathbb{C}}^{\text{alg}} \preceq \mathbb{C}$: infatti sono entrambi modelli di ACF_0, che ha eliminazione dei quantificatori. Dunque verificare che una è una sottostruttura elementare si riduce a verificare che è una sottostruttura, e questo è immediato.

Anche questo è sufficientemente importante da meritarsi un nome

Definizione 1.3.20. Una L-teoria è detta *model-completa* se per ogni $\mathcal{A}, \mathcal{B} \vDash T$ con $\mathcal{A} \subseteq \mathcal{B}$ si ha $\mathcal{A} \preceq \mathcal{B}$.

[12] Occhio a non confondersi con *espansione*.

Osservazione 1.3.21. Una teoria che ammette eliminazione dei quantificatori è model-completa.

Teorema 1.3.22 (Test di Robinson)**.** Una L-teoria T è model-completa se e solo se ogni L-formula è T-equivalente a una formula esistenziale.

Vedremo la dimostrazione in seguito, ma intanto

Corollario 1.3.23. Nei modelli di una teoria model-completa tutti gli insiemi definibili sono esistenzialmente definibili, ossia sono proiezioni di insiemi definibili senza quantificatori.

Esempio 1.3.24. Consideriamo $\mathbb{R}_f$, ossia $\mathbb{R}$ col solo linguaggio di campo, senza la relazione d'ordine. Abbiamo visto che la relazione d'ordine è esistenzialmente definibile in $\mathbb{R}_f$. Abbiamo anche visto che $\mathrm{Th}(\mathbb{R}_f)$ non ha eliminazione dei quantificatori; tuttavia questa teoria è model-completa.

Dimostrazione. Infatti se L' è il linguaggio dei campi e L è il linguaggio dei campi ordinati, ogni L'-formula è una L-formula e viceversa ad ogni L-formula φ corrisponde una L'-formula φ' dove abbiamo sostituito la relazione d'ordine con la sua definizione esistenziale. Notiamo che se ϑ è un L-enunciato, allora $\mathrm{Th}(\mathbb{R}) \vDash \vartheta \Leftrightarrow \mathrm{Th}(\mathbb{R}_f) \vDash \vartheta'$. Ne se segue che se ψ è una L'-formula, allora ψ è $\mathrm{Th}(\mathbb{R})$-equivalente a una L-formula φ senza quantificatori. Ne segue che ψ è $\mathrm{Th}(\mathbb{R}_f)$-equivalente a φ', che è esistenziale. □

Che legame c'è fra completezza e model-completezza?

Definizione 1.3.25. Se T è una L-teoria, un suo modello che sia sottostruttura di tutti i modelli di T si chiama *modello primo*.

Esempio 1.3.26. $\overline{\mathbb{C}^{\mathrm{alg}}}$ è un modello primo di ACF_0-

Esercizio 1.3.27. L'insieme $\mathbb{C}^{\mathrm{alg}} \cap \mathbb{R}$ è il dominio di una struttura $\overline{\mathbb{R}^{\mathrm{alg}}}$ che è modello primo di RCF.

Proposizione 1.3.28. Sia T model-completa. Se T ammette un modello primo allora T è completa.

Dimostrazione. Sia $\mathcal{P}$ primo e siano $\mathcal{A}, \mathcal{B} \vDash T$. Per ipotesi $\mathcal{P} \subseteq \mathcal{A}, \mathcal{B}$, e per model completezza $\mathcal{P} \preceq \mathcal{A}, \mathcal{B}$. Ma allora $\mathcal{A} \equiv \mathcal{P} \equiv \mathcal{B}$. □

Come conseguenza,

Corollario 1.3.29. RCF è completa, e quindi coincide con $\mathrm{Th}(\overline{\mathbb{R}})$ (a meno di chiusura deduttiva).

Teorema 1.3.30. La teoria $T_{\exp} = \mathrm{Th}(\mathbb{R}_{\exp})$ non ammette eliminazione dei quantificatori.

Tuttavia

Teorema 1.3.31 (Wilkie)**.** La teoria $T_{\exp}$ è model-completa.

Teorema 1.3.32 (Macintyre, Wilkie)**.** Esiste una procedura effettiva per trasformare una $L_{\exp}$-formula φ in un'altra esistenziale e a lei T-equivalente. [Più o meno; prendiamo questo enunciato come morale]

Domanda: possiamo concludere che $T_{\exp}$ è decidibile? Il problema è che non sappiamo se esiste un algoritmo per decidere la verità o falsità degli enunciati esistenziali. Addirittura non sappiamo se esiste un algoritmo per decidere la verità o falsità degli enunciati senza quantificatori. Tuttavia...

Teorema 1.3.33 (Macintyre, Wilkie)**.** Se assumiamo la congettura di Schanuel[13] allora $T_{\exp}$ è decidibile. Sempre assumendo la congettura, c'è un'assiomatizzazione esplicita per $T_{\exp}$.

Bonus: sia $\mathbb{R}_{\text{an}}$ l'espansione di $\overline{\mathbb{R}}$ con un simbolo per ogni funzione analitica reale ristretta[14] al cubo n-dimensionale (al variare di $n \in \mathbb{R}$).

(Osgood, 1916): Sia $y = \varphi(x)$ analitica trascendente[15]. Facciamo il cono su $y = \varphi(x)$ (uniamo tutte i segmenti fra i punti di questa cura e l'origine); questo è definibile:

$$E = \{(x, y, z) \mid \exists u\ 0 \leq x, z, u \leq 1, x = uz, y = z\varphi(u)\}$$

Claim 1.3.34. Questo insieme non è definibile senza quantificatori.

Dimostrazione. Supponiamo che E sia descritto da un'equazione analitica $F = 0$ in un intorno di 0. Allora $F(x, y, z) = \sum p_n(x, y, z)$, con p_n omogeneo di grado n. Dunque scriviamo

$$0 = F(uz, z\varphi(z), z) = \sum z^n p_n(u, \varphi(u), 1)$$

(per omogeneità) e quindi $\forall n\ p_n(u, \varphi(u), 1) = 0$. Dato che F è una serie non nulla almeno uno dei p_n non è il polinomio nullo; però questo si annulla sui punti del grafico di φ, contro l'assunzione di non semialgebricità. □

Già che ci siamo

Teorema 1.3.35 (Gabrielov, 1968)**.** $\mathbb{R}_{\text{an}}$ è model-completa e o-minimale.

Teorema 1.3.36 (Hironaka 1973; Denef-van den Dries 1988)**.** $\mathbb{R}_{\text{an}}$ ha eliminazione dei quantificatori se si espande il linguaggio con $x \mapsto 1/x$.

Esempio 1.3.37. Il cono: $E = \{(x, y, z) \mid 0 \leq x, z \leq 1, y = z\varphi(x/z)\}$.

Per $\mathbb{R}_{\exp}$ non è questo il caso, bisogna aggiungere molto di più per avere eliminazione dei quantificatori; in genere espansioni non banali di $\overline{\mathbb{R}}$ con eliminazione dei quantificatori tendono ad avere un linguaggio molto ricco.

[13] Una congettura in teoria dei numeri trascendenti.

[14] Nel senso che fuori è 0.

[15] Non semialgebrica; ad esempio exp.

1.4 27/08

Definizione 1.4.1. Una teoria T è *soddisfacibile* se ha un modello. È *fintamente soddisfacibile* se ogni sua sottoteoria finita S ha un modello.

Teorema 1.4.2 (di Compattezza)**.** Una teoria T è soddisfacibile se e solo se è finitamente soddisfacibile.

Conseguenze immediate: un grafo è n-colorabile se e solo se ogni suo sottografo finito è n-colorabile, analogo per SAT, eccetera.

Dimostrazione.

"$\Rightarrow$" Sia T soddisfacibile e sia quindi $\mathcal{M} \vDash T$. Allora $\mathcal{M} \vDash S$ per ogni $S \subseteq T$, e in particolare per ogni $S \subseteq_{\text{fin}} T$.

"$\Leftarrow$" Lo vediamo dopo.[16]

□

Definizione 1.4.3. Sia I un insieme e $\mathcal{F}$ una famiglia di sottoinsiemi di I. La famiglia $\mathcal{F}$ è un *filtro* se

- $I \in \mathcal{F}$
- se $A, B \in \mathcal{F}$ allora $A \cap B \in \mathcal{F}$
- se $A \in \mathcal{F}$ e $B \supseteq A$ allora $\mathcal{B} \in \mathcal{F}$

Esempio 1.4.4.

- Su $I = \mathbb{N}$ il filtro dei cofiniti $\mathcal{F}$, ossia la famiglia degli $X \subseteq \mathbb{N}$ tale che $\mathbb{N} \setminus X$ è finito. È immediato verificare le proprietà di filtro.
- Su $I = [0, 1]$, se μ è una misura su I, il filtro $\mathcal{F}$ dei sottoinsiemi X di $[0, 1]$ tali che $\mu([0, 1] \setminus X) = 0$.
- $\mathcal{F} = \mathscr{P}(I)$, il *filtro banale*.

Definizione 1.4.5. Un filtro $\mathcal{F}$ è un *ultrafiltro* se è massimale fra i non banali, ossia se $\mathcal{F} \subseteq \mathcal{F}'$ allora $\mathcal{F}' = \mathcal{F}$ oppure $\mathcal{F} = \mathscr{P}(I)$.

Esercizio 1.4.6. Sia $\mathcal{F}$ un filtro su I non banale. Allora $\mathcal{F}$ è un ultrafiltro se e solo se per ogni $A \subseteq I$ si ha che $A \in \mathcal{F}$ oppure[17] $A^c \in \mathcal{F}$.

Inoltre, solo uno dei due casi si può presentare: altrimenti per stabilità per intersezione avremmo $\emptyset = A \cap A^c \in \mathcal{F}$, e per stabilità per sovrainsieme $\mathcal{F} = \mathscr{P}(I)$, contro le ipotesi, perché $\emptyset$ è contenuto in ogni insieme.

Come si fa a produrre un filtro? Si parte da qualcosa di più semplice

[16] Usando la scelta, ma se T è numerabile si può fare senza.

[17] $A^c = I \setminus A$ è il complementare di A in I.

Definizione 1.4.7. Una famiglia $\mathcal{C} \subseteq \mathscr{P}(I)$ ha la *finite intersection property (*FIP*)* se per ogni $C_1, \dots, C_n \in \mathcal{C}$ si ha $C_1 \cap \dots \cap C_n \neq \emptyset$.

Ad esempio un filtro è non banale se e solo se ha la FIP.

Proposizione 1.4.8. Data $\mathcal{C}$ con la FIP l'insieme

$$\mathcal{F} = \{X \subseteq I \mid \exists C_1, \dots, C_n \in \mathcal{C}\ C_1 \cap \dots \cap C_n \subseteq X\}$$

è un filtro non banale (e si dice *filtro generato* da $\mathcal{C}$).

E per costruire gli ultrafiltri? Alcuni sono molto facili da costruire: se $a \in I$ l'*ultrafiltro principale su* a è $\mathcal{F}_a = \{X \subseteq I \mid a \in X\}$. La proprietà di ultrafiltro segue facilmente dal fatto che se $X \subseteq I$ allora $a \in X$ oppure $a \in X^c$.

Esistono ultrafiltri non principali? Se I è finito la risposta è *no*. Se I è infinito dipende da[18] AC: è consistente con ZF che tutti gli ultrafiltri su un insieme infinito siano principali.

Sia I un insieme, L un linguaggio, $\langle \mathcal{M}_i \mid i \in I\rangle$ una famiglia di L-strutture, e $\mathcal{U}$ un ultrafiltro su I. Consideriamo su $\prod_{i\in I} M_i$ la relazione di equivalenza definita da[19] $a \sim_{\mathcal{U}} b$ se $\{i \in I \mid a_i = b_i\} \in \mathcal{U}$. Consideriamo il quoziente $\prod M_i/\sim_{\mathcal{U}}$, dove denotiamo con $[a]$ la classe di equivalenza di a. Questo ci fornisce il dominio di una L-struttura $\mathcal{M}$. Come interpretiamo i simboli di L? Se R è un simbolo di relazione n-aria, diciamo che $R^{\mathcal{M}}([a_1], \dots, [a_n])$ sse $\{i \in R^{\mathcal{M}_i}(a_{1,i}, \dots, a_{n,i})\} \in \mathcal{U}$. Analogamente interpretiamo i simboli di funzione come $f([a_1], \dots, [a_n]) = [f(a_1, \dots, a_n)]$.

Ovviamente bisogna verificare che sono buone definizioni, cioè che non dipendono dai rappresentanti scelti per gli $[a_k]$. Ma se $a_{1,i} = b_{1,i}, \dots, a_{n,i} = b_{n,i}$ quasi ovunque allora $R^{\mathcal{M}_i}(a_{1,i}, \dots, a_{n,i})$ vale quasi ovunque se e solo se $R^{\mathcal{M}_i}(b_{1,i}, \dots, b_{n,1})$ vale quasi ovunque. Discorso analogo per le funzioni. Questa costruzione si chiama *ultraprodotto*.

Teorema 1.4.9 (Łoś)**.** Siano L un linguaggio, $\langle \mathcal{M}_i \mid i \in I\rangle$ una famiglia di L-strutture, $\mathcal{U}$ un ultrafiltro su I, e $\mathcal{M}$ il relativo ultraprodotto. Sia $p(x_1, \dots, x_n)$ una L-formula e siano $a_1, \dots, a_n \in \prod_{i\in I} M_i$. Allora

$$\mathcal{M} \vDash \varphi([a_1], \dots, [a_n]) \iff \mathcal{M}_i \vDash \varphi(a_{1,i}, \dots, a_{n,i})\ \mathcal{U}\text{-quasi ovunque}$$

Dimostrazione. Definiamo $\varphi(a_1, \dots, a_n)^I = \{i \in I \mid \mathcal{M}_i \vDash \varphi(a_{1,i}, \dots, a_{n,i})\}$. Vogliamo mostrare che $\mathcal{M} \vDash \varphi([a_1], \dots, [a_n])$ se e solo se $\varphi(a_1, \dots, a_n)^I \in \mathcal{U}$.

[18] Info bonus (non detta a lezione): che ogni filtro non banale si estenda a ultrafiltro è strettamente più debole di AC.

[19] L'idea è che un ultrafiltro dà una nozione di "quasi ovunque": se A succede quasi ovunque e $B \supseteq A$ anche B ci aspettiamo che accada quasi ovunque, se due cose succedono quasi ovunque succedono insieme quasi ovunque, e (proprietà di ultrafiltro) una cosa succede quasi ovunque o quasi ovunque non succede. Quindi qui stiamo incollando le funzioni che coincidono quasi ovunque o, se ci piace di più, $\mathcal{U}$-quasi ovunque.

Lavoriamo per induzione sulla complessità[20] di φ. Supponiamo $n = 1$ per non impantanarci nella notazione (in generale non cambia niente, a parte che compaiono più indici).

Vediamo che se $t(x)$ è un termine $t([a]) = [t(a)]$ per induzione sulla complessità dei termini. Se $t = f(x)$, con f simbolo di funzione, questa è la definizione. Induttivamente componendo funzioni.

Ora passiamo alle formule atomiche; abbiamo due casi:

$t_1(x) = t_2(x)$ Vogliamo vedere che $t_1^{\mathcal{M}}([a]) = t_2^{\mathcal{M}}([a])$ se e solo se $\{i \in I \mid t_1^{\mathcal{M}_i}(a) = t_2^{\mathcal{M}_i}(a)\} \in I$. Questa è semplicemente l'osservazione precedente sui termini, perché $t_j^{\mathcal{M}}([a]) = [t_j(a)]$, e $[t_1(a)] = [t_2(a)]$ se e solo se coincidono quasi ovunque.

$R(t_1(x), \ldots, t_n(x))$

Caso induttivo: abbiamo φ di una delle seguenti forme:

1. $\varphi = \alpha \wedge \beta$
2. $\varphi = \alpha \vee \beta$
3. $\varphi = \neg\alpha$
4. $\varphi = \exists y\ \alpha(x, y)$
5. $\varphi = \forall y\ \alpha(x, y)$

dove per α e β vale l'ipotesi induttiva. Facciamo il caso della congiunzione:

$$\mathcal{M} \vDash \varphi([a]) \Leftrightarrow \mathcal{M} \vDash (\alpha \wedge \beta)([a]) \Leftrightarrow \mathcal{M} \vDash \alpha([a]) \text{ e } \mathcal{M} \vDash \beta([a])$$
$$\Leftrightarrow \alpha(a)^I \in \mathcal{U} \text{ e } \beta(a)^I \in \mathcal{U} \Leftrightarrow \alpha(a)^I \cap \beta(a)^I \in \mathcal{U} \Leftrightarrow (\alpha \wedge \beta)(a)^I \in \mathcal{U} \Leftrightarrow \varphi(a)^I \in \mathcal{U}$$

Analogamente[21] per la negazione *usando la proprietà di ultrafiltro.* Vediamo l'esistenziale: se $\varphi = \exists y\ \alpha(x, y)$ abbiamo

$$\mathcal{M} \vDash \varphi(a) \Leftrightarrow \text{ esiste } b \in M\ \mathcal{M} \vDash \alpha(a, b) \Leftrightarrow \alpha(a, b)^I \in \mathcal{U}$$

Se $\alpha(a, b)^I \in \mathcal{B}$ allora anche $(\exists y\ \alpha(a, b))^I \in mcU$, e questo è $(\varphi[a])^I$. Viceversa supponiamo $D = (\varphi([a]))^I \in \mathcal{U}$, cioè per ogni $i \in D$ esiste $b_i \in M_i$ tale che $\mathcal{M}_i \vDash \alpha(a_i, b_i)$. Definiamo allora

$$b_i = \begin{cases} b_i & \text{se } i \in D \\ \text{elemento qualsiasi} & \text{se } i \notin D \end{cases}$$

Allora $\alpha(a, b)^{\mathcal{M}} \supseteq D \in \mathcal{U}$, per cui $\mathcal{M} \vDash \alpha(a, b)$ e quindi $\mathcal{M} \vDash \varphi(a)$. Per disgiunzione e quantificatore universale si può fare in maniera analoga oppure si riscrivono in termini di $\wedge, \exists, \neg$. □

[20] Per noi è la lunghezza.

[21] A lezione è stato fatto nel dettaglio, ma non l'ho trascritto.

Cosa succede se $\mathcal{U} = \mathcal{F}_a$ è principale? Che non creiamo nulla di nuovo: $\mathcal{M} \cong \mathcal{M}_a$. Infatti in questo caso due elementi del prodotto sono equivalenti se coincidono nel punto a, per cui non ci interessa niente del resto delle strutture coinvolte (da qui a scrivere una dimostrazione vera è un attimo).

Definizione 1.4.10. Il *filtro di Frèchet* è il filtro dei cofiniti.

Osservazione 1.4.11. Un ultrafiltro $\mathcal{U}$ è non principale se e solo se estende il filtro di Frèchet.

Lemma 1.4.12. Ogni filtro non banale $\mathcal{F}$ è contenuto in un ultrafiltro.

Dimostrazione. Zorn. □

Corollario 1.4.13. Se I è infinito esiste $\mathcal{U}$ ultrafiltro non principale su I.

Esempio 1.4.14. Prendiamo $\mathcal{I} = \mathbb{N}$, $\mathcal{U}$ un ultrafiltro su $\mathbb{N}$ e come $\mathcal{M}_i$ prendiamo sempre (la copia di) una stessa, fissata, struttura $\mathcal{A}$ (in questo caso parliamo di *ultrapotenza*). Se $\mathcal{U}$ è principale, l'ultrapotenza ci viene isomorfa a $\mathcal{A}$. Se $\mathcal{U}$ non è principale abbiamo una struttura nuova: ad esempio se $\mathcal{A} = (\mathbb{R}, +, \cdot, <)$, nell'ultraprodotto $\mathcal{M} = \prod_{i\in I} \mathcal{A}_i/\mathcal{U}$ esiste un elemento c tale che $c > 1$, $c > 2$, $c > 3$, eccetera: basta prendere $[(1, 2, 3, 4, \ldots)]$.

Tuttavia

Proposizione 1.4.15. $\mathcal{A} \preceq \prod_{i\in I} \mathcal{A}_i/\mathcal{U}$

Dimostrazione. Segue immediatamente dal Teorema di Łoś. □

Torniamo al Teorema di Compattezza: abbiamo T finitamente soddisfacibile e vogliamo mostrare T soddisfacibile. In altre parole abbiamo un modello per ogni sottoinsieme finito di T e vogliamo montare un modello per T. Prendiamo dunque $I = \mathscr{P}_{\text{fin}}(T)$, e per ogni $S \subseteq_{\text{fin}} T$ fissiamo $\mathcal{M}_S \vDash S$. Fissiamo $\mathcal{U}$ ultrafiltro non principale[22] su I. Un ultrafiltro non principale qualunque, per i nostri scopi, potrebbe non andare bene; ci serve anche che $\mathcal{U}$ verifichi quando segue.

Sia $S \in I$ e sia $X_S = \{A \subseteq T \mid S \subseteq A\}$. Chiamiamo poi $\mathcal{X} = \{X_S \mid S \in I\}$. Questo insieme ha la FIP, perché $X_{S_1} \cap \ldots \cap X_{S_n} = X_{S_1 \cup \ldots \cup S_n} \neq \emptyset$. Dunque $\mathcal{X}$ si può estendere ad un ultrafiltro $\mathcal{U}$ non principale. Prendiamo quindi un $\mathcal{U} \supseteq \mathcal{X}$ non principale.

Claim 1.4.16. $\mathcal{M} = \prod_{i\in I} \mathcal{M}_i/\mathcal{U}$ è un modello di T.

Dimostrazione. Data $\varphi \in T$ vogliamo mostrare che $\mathcal{M} \vDash \varphi$, cioè che $\varphi^I \in \mathcal{U}$ per Łoś. A noi basta mostrare $\varphi^I \in \mathcal{X}$. Se $S \in X_{\{\varphi\}}$ allora $\mathcal{M}_S \vDash \varphi$. Dunque $\varphi^I \supseteq X_{\{\varphi\}} \in \mathcal{X}$. Dato che $X_{\{\varphi\}} \in \mathcal{U}$ anche $\varphi^I \in \mathcal{U}$, e quindi $\mathcal{M} \vDash \varphi$. □

[22] Se T è finita non c'è niente da fare...

Definizione 1.4.17. Sia L un linguaggio e $\mathcal{C}$ una classe di L-strutture. Diciamo che $\mathcal{C}$ è *elementare* (o *assiomatizzabile*) se $\mathcal{C} = \mathrm{Mod}(T)$, per una qualche L-teoria T.

Osservazione 1.4.18. Le classi elementari sono chiuse per ultraprodotti, sempre per il Teorema di Łoś.

Questo ci permette di mostrare facilmente che certe classi *non* sono elementari.

Esempio 1.4.19. Sia L un linguaggio, T una L-teoria e chiamiamo $\mathcal{C}_\infty$ la classe dei modelli infiniti di T. Questa è una classe elementare. Per mostrarlo dobbiamo produrre una $T' = T \cup \Delta$ tale che $\mathcal{C}_\infty = \mathrm{Mod}(T')$. A tale scopo basta prendere $\Delta = \bigcup_{n\in\mathbb{N}}\{\alpha_n\}$, dove

$$\alpha_n \equiv \exists x_1, \dots, x_n \bigwedge_{\substack{i,j=1 \\ i\neq j}}^{n} x_i \neq x_j$$

La cosa divertente è che il viceversa non vale, nel senso che

Proposizione 1.4.20. $\mathcal{C}_{\text{fin}}$, la classe delle L-strutture finite, non è una classe elementare.

Dimostrazione. Per quanto detto basta mostrare che non è chiusa per ultraprodotto. Prendiamo per ogni $n \in \mathbb{N}$ una struttura $\mathcal{M}_n$ con almeno n-elementi: questo si fa semplicemente prendendo un insieme sufficientemente grande e interpretando i simboli di L a piacimento. Prendiamo poi $\mathcal{U}$ ultrafiltro non principale su $\mathbb{N}$ e consideriamo l'ultraprodotto $\mathcal{M} \models= \prod_{i\in\mathbb{N}} \mathcal{M}_i/\mathcal{U}$. Per Łoś, dato che $\mathcal{U}$ è non principale e quindi estende il filtro dei cofiniti, per ogni n abbiamo $\mathcal{M} \vDash \alpha_n$, dove le α_n sono quelle dell'Esempio precedente, per cui $\mathcal{M}$ è infinita. □

Chiaramente potevamo usare anche direttamente il Teorema di Compattezza: $T' = T \cup \Delta$ è finitamente soddisfacibile, quindi soddisfacibile e ha un modello $\mathcal{M}$, che però dev'essere infinito...

Proposizione 1.4.21. Sia $L = \langle 0, 1, +, \cdot, R\rangle$, con R simbolo di relazione 1-aria. Sia $\mathcal{C}_{\min}$ la classe delle L-strutture minimali che sono campi quando ristrette a $\langle 0, 1, +, \cdot\rangle$. Allora $\mathcal{C}_{\min}$ non è elementare.

Dimostrazione. Mostriamo la non chiusura per ultraprodotti: fissiamo $n \in \mathbb{N}$ e prendiamo $\mathbb{C}$. Chiamiamo $\mathcal{M}_n$ l'espansione di $\overline{\mathbb{C}}$ a L-struttura che interpreta R con $\{0, 1, \dots, n\}$. Ora $\mathcal{M}_n$ è minimale: ogni insieme definibile in $\mathcal{M}_n$ è già definibile in $\mathbb{C}$. Prendiamo un ultraprodotto non principale $\mathcal{M} = (\mathbb{C}^*, R^{\mathcal{M}})$ degli $\mathcal{M}_n$. Ora $R^{\mathcal{M}}$ è chiaramente definibile, ma è infinito (contiene ogni n) e coinfinito (non contiene nessun $1/n$), per cui $\mathcal{M}$ non è minimale. □

Proposizione 1.4.22 (Principio di Lefschetz)**.** Siano $L = (0, 1, +, \cdot)$ e α un L-enunciato. Allora sono equivalenti:

1. $\mathsf{ACF}_0 \vDash \alpha$
2. $\mathsf{ACF}_p \vDash \alpha$ per cofiniti p
3. $\mathsf{ACF}_p \vDash \alpha$ per infiniti p

(in realtà per alcune dipendenze ci si può anche dimenticare della chiusura algebrica)

Dimostrazione.

"$2 \Rightarrow 3$" è ovvio.

"$3 \Rightarrow 1$" Sia $\mathcal{P}$ l'insieme dei primi. Prendiamo $\mathcal{U}$ ultrafiltro non principale su $\mathcal{P}$ e per ogni $p \in \mathcal{P}$ scegliamo $\mathcal{M}_p \vDash \mathsf{ACF}_p$. Consideriamo $\mathcal{M} = \prod_{p\in\mathcal{P}} \mathcal{M}_p/\mathcal{U}$. Dato che che tutte le strutture coinvolte sono campi, $\mathcal{M}$ è ancora un campo e ci basta vedere che ha caratteristica 0. Questo si mostra con gli stessi giochetti di prima considerando gli enunciati, al variare di $p \in \mathcal{P}$,

$$\underbrace{1 + 1 + 1 \ldots + 1}_{p \text{ volte}} = 0$$

Se ora abbiamo cura di scegliere $\mathcal{U}$ in maniera che contenga $D = \{p \in \mathcal{P} \mid \mathsf{ACF}_p \vDash \alpha\}$, che è infinito e quindi si può aggiungere al filtro di Frèchet preservando la FIP ed estendere tutto a ultrafiltro, otteniamo che $\mathcal{M} \vDash \alpha$ per il Teorema di Łoś. Ma dato che ACF_0 è completa questo basta per avere la tesi.

"$1 \Rightarrow 2$" Se la tesi fosse falsa avremmo $\mathsf{ACF}_p \vDash \neg\alpha$ per infiniti p. Basta allora usare il punto precedente.

□

1.5 28/08

Corollario 1.5.1. Sia α un enunciato del linguaggio dei campi; allora $\mathbb{C} \vDash \alpha$ se e solo se per quasi ogni[23] primo p si ha $\mathsf{ACF}_p \vdash \alpha$.

Esercizio 1.5.2 (Ax-Groethendieck)**.** Sia $p\colon \mathbb{C}^n \to \mathbb{C}^n n$ una funzione polinomiale, ossia $p(\bar{x}) = (p_1(\bar{x}), \ldots, p_n(\bar{x}))$, con i $p_i \in \mathbb{C}[x_1, \ldots, x_n]$. Allora se p è iniettiva è surgettiva[24].

Soluzione. Sia F la chiusura algebrica di un campo finito e sia $p\colon F^n \to F^n$ polinomiale. Fatto: se p è iniettiva allora è surgettiva (segue dal principio dei cassetti), e per Lefschetz abbiamo finito[25]. □

[23] Che può essere inteso sia come "cofiniti" sia come "infiniti".

[24] Il viceversa è chiaramente falso; basta prendere il quadrato.

[25] Per scriverlo al prim'ordine si fissa il grado del polinomio e poi diventa prim'ordine.

Definizione 1.5.3. Una *catena* di enunciati è una successione $\alpha_0, \alpha_1, \ldots, \alpha_i, \ldots$ (per $i \in \mathbb{N}$) tale che $\vdash \alpha_{n+1} \to \alpha_n$ ma $\alpha_n \not\vdash_{n+1}$.

Esempio 1.5.4. Quella di ieri:

$$\alpha_n \equiv \exists x_1, \ldots, x_n \bigwedge_{\substack{i,j=1 \\ i \neq j}}^{n} x_i \neq x_j$$

Lemma 1.5.5. Sia $T = \{\alpha_i \mid i \in \mathbb{N}\}$. Allora $\mathrm{Mod}(T)$ è una classe elementare, ma il suo complemento nella classe delle L-strutture non lo è.

Dimostrazione. Esercizio. □

Ora puntiamo verso la dimostrazione del Teorema 1.3.22, il test di Robinson.

Sia L un linguaggio, $\mathcal{M}$ una L struttura e $A \subseteq M$. Chiamiamo L_A il linguaggio $L \cup \{c_a \mid a \in A\}$, con i c_a simboli di costante. L'idea è usare L_A per scrivere le formule con parametri da A. Ad esempio se $\mathcal{M} = \overline{\mathbb{R}}$ e $A = \{\pi\}$, una $L(A)$-formula è $\pi + x = 1$.

Definizione 1.5.6. Il *diagramma elementare* di $\mathcal{M}$ è l'insieme delle L_M-formule vere[26] in $\mathcal{M}$.

Ad esempio $\exists x_1, x_2, x_3, x_4 \ \sum x_i^2 = 1203$ è una formula in $\mathrm{El\,diag}(\mathbb{N})$. Analogamente si definisce

Definizione 1.5.7. Il *diagramma* di $\mathcal{M}$ $\mathrm{Diag}(\mathcal{M})$ è l'insieme degli $L(M)$-enunciati *senza quantificatori* veri in $\mathcal{M}$.

Se $\mathcal{A} \subseteq \mathcal{B}$ sono L strutture allora B è una $L(A)$-struttura interpretando ogni c_a con a. Inoltre $\mathcal{B} \vDash \mathrm{Diag}(\mathcal{A})$, perché per guardare se le formule senza quantificatori sono vere basta vedere l'interpretazione dei simboli del linguaggio, che coincide per definizione di sottostruttura. Analogamente, riguardando la definizione di sottostruttura elementare, $\mathcal{A} \preceq \mathcal{B}$ se e solo se $\mathcal{B} \vDash \mathrm{El\,diag}(\mathcal{A})$.

Supponiamo ora di avere $L' \supseteq L$, e T' una L'-teoria. Sia $\mathcal{A}$ una L-struttura. Allora una L'-struttura $\mathcal{B}$ è contemporaneamente modello di T' e sovrastruttura di $\mathcal{A}$ se e solo se $\mathcal{B} \vDash \mathrm{Diag}(\mathcal{A}) \cup T'$. Un tale $\mathcal{B}$ esiste se e solo se $T \cup \mathrm{Diag}(\mathcal{A})$ è (finitamente) soddisfacibile.

Siamo pronti per affrontare la dimostrazione del Teorema 1.3.22, che rienunciamo in maniera più precisa

Teorema 1.5.8. Sia T una L teoria. TFAE:

1. T è model-completa

[26] Ovviamente si intende che interpretiamo ogni c_a col rispettivo a.

2. Ogni formula è T-equivalente ad un'esistenziale
3. Ogni formula è T-equivalente ad un'universale

Dimostrazione.

"$2 \Leftrightarrow 3$" Basta negare: se $\neg\varphi$ è equivalente ad un esistenziale (cosa vera per ipotesi) allora φ è equivalente ad un'universale, e viceversa.

"$2 \Rightarrow 1$" Sia $\varphi(\bar{x})$ una L-formula, e siano $\mathcal{A} \subseteq \mathcal{B}$ modelli di T. Sia $\bar{a} \in A^n$. Per avere la tesi dobbiamo mostrare che $\mathcal{A} \vDash \varphi(\bar{a}) \Rightarrow \mathcal{B} \vDash \varphi(\bar{a})$ (dato che φ è arbitraria...). Dato che φ è equivalente a $\exists\bar{y}\ \beta(\bar{a}, \bar{y})$ basta scegliere un testimone $\bar{b}$ e abbiamo $\mathcal{A} \vDash \beta(\bar{a}, \bar{b})$, per cui $\mathcal{B} \vDash \beta(\bar{a}, \bar{b})$ perché β non ha quantificatori, da cui $\mathcal{B} \vDash \exists\bar{y}; \beta(\bar{a}, \bar{y})$.

"$1 \Rightarrow 3$" Sia $\varphi(\bar{x})$ una L-fomula. Definiamo $\Gamma(\bar{x})$ come l'insieme di tutte le formule universali che sono conseguenza di φ modulo T. Lo scopo è trovare $\gamma \in \Gamma$ equivalente[27] a φ. Chiaramente, visto che le formule universali sono stabili per congiunzione, basta trovare $\gamma_1, \dots, \gamma_n \in \Gamma$ tali che $T \vdash \forall\bar{x}(\gamma_1 \wedge \dots \wedge \gamma_n \to \varphi)$. Sia a una nuova costante[28]. Cerchiamo $S \subseteq_{\text{fin}} \Gamma$ tale che $T \cup S(a) \vdash \varphi(a)$. Per il Teorema di Compattezza questo succese se e solo se $T \cup \Gamma(a) \vdash \varphi(a)$. Supponiamo per assurdo che questo non sia vero e sia $\mathcal{A}$ una $L(\{a\})$-struttura modello di $T \cup \Gamma(a) \cup \neg\varphi(a)$.

Claim 1.5.9. Esiste $\mathcal{B} \supseteq \mathcal{A}$ tale che $\mathcal{B} \vDash T \cup \{\varphi(a)\}$.

Se il Claim è vero allora abbiamo un assurdo: infatti in tal caso $\mathcal{A} \preceq \mathcal{B}$, ma $\mathcal{A} \vDash \neg\varphi(a)$ e $\mathcal{B} \vDash \varphi(a)$. Curiamoci quindi di dimostrare il Claim. Per i discorsi precedenti ci basta mostrare che

$$\text{Diag}(\mathcal{A}) \cup T \cup \{\varphi(a)\}$$

è (finitamente) soddisfacibile. Supponiamo per assurdo che esistano $\beta_1, \dots, \beta_n \in \text{Diag}(\mathcal{A})$ tali che se chiamiamo $\beta(a, \bar{c}) = \bigwedge \beta_i(a, \bar{c})$ abbiamo $T \vdash \beta(a, \bar{c}) \to \neg\varphi(a)$. Dunque $T \vdash \varphi(a) \to \neg\beta(a, \bar{c})$; dato che a non compare un L, e idem per $\bar{c}$, abbiamo $T \vdash \forall x \forall\bar{y}(\varphi(x) \to \neg\beta(x, \bar{y}))$, riscrivibile come $\forall x(\varphi(x) \to \forall\bar{y}\neg\beta(x, \bar{y}))$. Ma questo vuol dire che $\forall\bar{y}\neg\beta(x, \bar{y})$ è una conseguenza universale di φ, cioè sta in Γ, e allora $\mathcal{A} \vDash \forall\bar{y}(\neg\beta(a, \bar{y}))$. Questo è assurdo perché $\beta \in \text{Diag}(\mathcal{A})$ (il diagramma è da intendersi come $L_A \cup \{a\}$-struttura).

[27] D'ora in poi "equivalente" vuol dire "equivalente modulo T".

[28] Dato che a è una nuova costante, se funziona per a funziona per qualunque x che mettiamo nel modello (semplicemente, T non dice niente su a, per cui possiamo interpretarla come vogliamo; se $\forall\bar{x}[\dots]$ fosse falsa in un modello basterebbe espanderlo interpretando a nella maniera opportuna...

□

Ovviamente l'interpretazione geometrica di una formula esistenziale è più "bella" di quella universale: è una proiezione, mentre nell'altro caso c'è da complementare, proiettare e poi ricomplementare.

Teorema 1.5.10 (Löwenheim-Skolem)**.** Sia L un linguaggio numerabile[29] e T una L-teoria munita di un modello infinito. Allora per ogni cardinali κ infinito esiste un modello di $\mathcal{M}$ di cardinalità κ.

In particolare un teoria del genere non può essere categorica, cioè avere un solo modello a meno di isomorfismo. Vediamo la dimostrazione di una parte del teorema:

Lemma 1.5.11 (Löwenhem-Skolem verso l'alto)**.** Sia $\mathcal{A}$ una struttura infinita e sia κ un cardinale qualsiasi. Allora esiste $\mathcal{B}$ sovrastruttura elementare di $\mathcal{A}$ tale che $|B| \geq \kappa$.

Dimostrazione. Sia C un insieme di costanti di cardinalità κ e consideriamo il linguaggio[30] $L(C) = L \sqcup C$. Definiamo poi

$$T' = \mathrm{El}\,\mathrm{diag}_L(\mathcal{A}) \cup \{c_i \neq c_j \text{ se } c_i \text{ e } c_j \text{ sono costanti diverse}\}$$

Se $\mathcal{B} \vDash T'$ allora $\mathcal{B} \preceq \mathcal{A}$ e $|B| \geq |C| = \kappa$, da cui la tesi. Ci basta dunque mostrare che T' è soddisfacibile. Per compattezza basta mostrare che T' è finitamente soddisfacibile; sia $S \subseteq_{\text{fin}} T'$. Allora $S \subseteq \mathrm{Diag}\,\mathrm{el}(\mathcal{A}) \cup \{c_1 \neq \ldots \neq c_n\}$ per un qualche insieme finito di costanti $c_1, \ldots, c_n \in C$. Un modello di S è $\mathcal{A}$ espanso interpretando le costanti a caso, purché siano distinte, cosa possibile perché A è infinito. □

Per l'altro verso serve più lavoro e non c'è tempo di farlo qui.
[paradosso di Skolem e breve discussione, non riportati]

Definizione 1.5.12. Sia $\mathcal{M}$ una L-struttura, $\bar{c} \in M^n$ e $A \subseteq \mathcal{M}$. Il *tipo di* $\bar{c}$ *a parametri da* A, denotato $\mathrm{tp}(\bar{c}/A)$, è l'insieme delle L-formule a parametri da A soddisfatte da $\bar{c}$.

Esempio 1.5.13. Se $\mathcal{M} = \overline{\mathbb{C}}$ e $c = i$ allora $(x^2+1 = 0) \in \mathrm{tp}(i/A) \cap \mathrm{tp}(-i/A)$.

Osservazione 1.5.14. $\mathrm{tp}(i/\mathbb{Z}) = \mathrm{tp}(-i/\mathbb{Z})$

Dimostrazione. Il coniugio fissa gli interi pointwise. Quindi se $\varphi(x)$ è una formula a parametri da $\mathbb{Z}$ si ha $\mathbb{C} \vDash \varphi(c) \leftrightarrow \varphi(\bar{c})$. □

Definizione 1.5.15. Un n-tipo *parziale* su A è un insieme $\Gamma(\bar{x})$ di formule con parametri da $\mathcal{A}$ finitamente soddisfacibile in $\mathcal{M}$, cioè tale che per ogni $\gamma_1, \ldots, \gamma_k \in \Gamma$ si ha $\mathcal{M} \vDash \exists \bar{x}(\gamma_1 \wedge \ldots \wedge \gamma_n)$.

[29] C'è una versione per linguaggi arbitrari, ma enunciamo questa per semplicità.
[30] Si intende che l'unione è disgiunta.

Esempio 1.5.16. Su $(\mathbb{N}, <)$, con $A = \mathbb{N}$, il tipo parziale $\{x > 0, x > 1, x > 2, \ldots\}$ non è realizzato.

Lemma 1.5.17. Sia $\Lambda(\bar{x})$ un tipo su $\mathcal{M}$. Allora esistono $\mathcal{N}$ estensione elementare di $\mathcal{M}$ e $\bar{c} \in N^n$ tale che c realizza Λ (cioè soddisfa tutte le formule di Λ).

Dimostrazione. Sia $T' = \operatorname{El}\operatorname{diag}_L(\mathcal{M}) \cup \Lambda(\bar{d})$. Per ipotesi T' è finitamente soddisfacibile, dunque ha un modello $\mathcal{N}$, che soddisfa la tesi per le ipotesi su T'. □

Un'altra maniera di pensare un tipo è quindi "un insieme di formule che può essere realizzato in un'estensione elementare".

Definizione 1.5.18. Un *tipo totale* (più spesso *tipo* e basta) $p(\bar{x})$ è un insieme di formule con parametri da A e variabili libere $x_1, \ldots, x_n$ della forma $p = \operatorname{tp}(\bar{c}/A)$ per un qualche $\bar{c} \in N^n$, dove $\mathcal{N}$ è un'estensione elementare di $\mathcal{M}$. L'insieme degli n-tipi a parametri da A si indica con $S_n(A)$.

Osservazione 1.5.19. Sia $\Lambda(\bar{x})$ un tipo parziale a parametri da A. Allora Λ è totale se e solo se per ogni $L(A)$-formula $\varphi(\bar{x})$ allora $\varphi \in \Lambda$ oppure $\neg\varphi \in \Lambda$.

Esercizio 1.5.20. Dimostrarlo.

Osservazione 1.5.21. Fissato $\mathcal{M}$ esiste una sua estensione elementare $\mathcal{N}$ che realizza ogni tipo su M.

Prima di dimostrarlo notiamo che deve necessariamente essere $\mathcal{N} \neq \mathcal{M}$: c'è sempre il tipo

$$\{x \neq c_i \mid c_i \in M\}$$

che dice "x è un elemento nuovo".

Dimostrazione. Facciamolo per gli 1-tipi, ma si può fare anche per gli n-tipi tutto in una volta. Basta aggiungere per ogni 1-tipo p una costante nuova c_p. Ora prendiamo $T' = \operatorname{El}\operatorname{diag}(\mathcal{M}) \cup \{p(c_p) \mid p \in S_n(M)\}$. Questa teoria è finitamente soddisfacibile e un qualunque suo modello soddisfa la tesi. □

Ora: abbiamo detto che in $\mathcal{M}$ c'è sempre un tipo che non si può mai soddisfare. Il problema è che ci sono troppi parametri. Per parlare di strutture "con tanti tipi realizzati" quindi diamo bound sul numero di parametri:

Definizione 1.5.22. $\mathcal{M}$ è ω-satura se soddisfa ogni n-tipo con un numero finito di parametri.

Teorema 1.5.23. Ogni $\mathcal{M}$ ha un'estensione elementare ω-satura.

Dimostrazione. Partiamo da $\mathcal{M} = \mathcal{M}_0$ e costruiamo $\mathcal{M}_1$ sua estensione elementare che realizza tutti i tipi con parametri da M_0 (basterebbe con parametri finiti). Dato che saranno spuntati nuovi elementi, saranno spuntati anche nuovi tipi, per cui iteriamo, costruendo

$$\mathcal{M}_0 \preceq \mathcal{M}_1 \preceq \mathcal{M}_2 \preceq \dots$$

A questo punto costruiamo una struttura $\mathcal{N}$ unendo tutte le $\mathcal{M}_i$ ($\mathcal{N}$ è ben definita proprio perché non stiamo unendo modelli a caso ma una catena elementare).

Lemma 1.5.24. $\mathcal{N}$ è una sovrastruttura elementare di ogni $\mathcal{M}_i$.

Il Lemma si dimostra per induzione sulla complessità delle formule e non lo faremo qui (è facile). Mostriamo che $\mathcal{N}$ è ω-satura. Se $p(\bar{x})$ è un tipo con un numero finito di parametri $\{a_i\}$, esisterà M_i che contiene tutti gli a_i. Ma allora $p(\bar{x})$ è realizzato in $\mathcal{M}_{i+1}$, e la stessa realizzazione va bene pure per $\mathcal{N}$. □

Esempio 1.5.25. Un esempio di tipo con finiti parametri non soddisfatto è, in $\overline{\mathbb{R}}$, il tipo parziale $\{x > 1, x > 1 + 1, x > 1 + 1 + 1, \dots\}$.

Questo è "moralmente" lo stesso tipo di prima ma non usa nessun parametro. Il teorema ci dice che i reali sono inclusi in una struttura elementare ω-satura, dove quindi ci sarà questo "reale infinito". Ma se c è un tale "reale infinito" allora per ω-saturazione ce ne sarà anche uno "più infinito di lui": una realizzazione di

$$\{x > c, x > c + c, x > c + c + c, \dots\}$$

e il discorso può essere reiterato.

Definizione 1.5.26. Una tipo $p(\bar{x})$ è *isolato* se esiste una formula $\alpha(\bar{x}) \in p(\bar{x})$ tale che $\forall \varphi \in p \ \alpha \to \varphi$. In altre parole p è implicato da una singola formula, α.

Dato che i tipi sono finitamente soddisfacibili *ogni tipo isolato è sempre realizzato.*

Esempio 1.5.27. $p = \mathrm{tp}_{\overline{\mathbb{C}}}(i/\mathbb{Z})$ è isolato da $x^2 + 1 = 0$. In generale un qualunque polinomio irriducibile isola il tipo delle sue radici.

Esempio 1.5.28. $p = \mathrm{tp}_{\overline{\mathbb{C}}}(\pi/\mathbb{Z})$ non è isolato, perché c'è un modello che non lo realizza: la chiusura algebrica di $\mathbb{Q}$. Questa è una sottostruttura elementare di $\mathbb{C}$ e contiene $\mathbb{Z}$, ma non realizza il tipo di π. Lo stesso discorso funziona con tutti i trascendenti.

Di fatto, i trascendenti hanno tutti lo stesso tipo: se a,b sono trascendenti $\mathrm{tp}(a/\mathbb{Z}) = \mathrm{tp}(b/\mathbb{Z})$ è determinato da $\{q(x) \neq 0 \mid q \in \mathbb{Z}[x] \setminus \{0\}\}$. Per chi ha visto un po' di geometria algebrica questo corrisponde allo spettro di un anello, e questa è la versione model-teoretica.

Enunciamo (ma non avremo il tempo di dimostrarlo), il *Teorema di Omissione*[31] *di Tipi*. Prima una

Definizione 1.5.29. Un n-tipo su una *teoria* T è un insieme $p(\bar{x})$ di formule con variabili $x_1, \dots, x_n$ compatibile con T, ossia per ogni $\varphi_1, \dots, \varphi_k \in p$ si ha $T \vdash \exists \bar{x}(\bigwedge \varphi(\bar{x}))$. Diciamo che p è *isolato* se c'è una formula $\alpha(\bar{x})$ tale che per ogni $\varphi \in p$ si ha $T \vdash \forall \bar{x}(\alpha \to \varphi)$ e[32] $T \vdash \exists \bar{x} \alpha(\bar{x})$.

Teorema 1.5.30. Sia L numerabile e T una L-teoria soddisfacibile. Siano $p_1, p_2, \dots$ (numerabili) tipi in T *non isolati*. Allora esiste $\mathcal{M} \vDash T$ che omette tutti i p_i e $\mathcal{M}$ è numerabile.

In generale non si riesce a omettere quantità arbitrarie di tipi non isolati (come già visto per quelli isolati non c'è speranza): ad esempio prendiamo $L = \{<, a_q \mid q \in \mathbb{Q}, P_{\mathbb{Q}}(x)\}$ e come modello $\mathcal{M} = (\mathbb{R}, <, q \mid q \in \mathbb{Q}, \mathbb{Q})$. Sia $T = \mathrm{Th}(\mathcal{M})$.

1.6 29/08

Libri di riferimento Shorter Model Theory di Hodges, Saturated Model Theory di Sacks, Tame Topology and O-minimal Structures di Van Den Dries, e A Course in Model Theory di Tent-Ziegler.

Parliamo di o-minimalità; per semplicità ci limitiamo a strutture reali, cioè espansioni S di $\overline{\mathbb{R}}$. Ricordiamo che S è o-minimale se ogni sottoinsieme definibile (con parametri) di $\mathbb{R}$ è unione finita di punti e intervalli (in particolare è già definibile in $(\mathbb{R}, <)$ per sottoinsiemi di, ad esempio $\mathbb{R}^2$, questo non è più detto (altrimenti avremmo eliminazione dei quantificatori!); si pensi a una faccina sorridente come sottoinsieme di $\mathbb{R}^2$. Un esempio non banale di struttura o-minimale è, come già detto, $\mathbb{R}_{\mathrm{an}}$; questa è importante perché a pensarci un attimo vuol dire studiare le varietà analitiche compatte.

Definizione 1.6.1. Una funzione $f\colon \mathbb{R}^n \to \mathbb{R}$ è definibile (in S) se il suo graf(ic)o è un sottoinsieme definibile.

Teorema 1.6.2. Se $f\colon \mathbb{R} \to \mathbb{R}$ è definibile allora è dominata da un polinomio: esiste $p(x)$ tale che $|f(x)| \leq p(x)$ per ogni $x \gg 0$.

Un altro risultato è che le funzioni definibili sono analitiche a tratti.

[31] Ovviamente omettere un tipo vuol dire non realizzarlo.
[32] Altrimenti...

Esempio 1.6.3. $(\overline{\mathbb{R}}, \mathbb{Z})$ *non* è o-minimale: ci si può definire ogni chiuso (con tutta la struttura selvaggia che ne consegue, topologia/teoria descrittiva degli insiemi), anche frattali o cose del genere.

Ci sono casi intermedi:

Esempio 1.6.4. $(\overline{\mathbb{R}}, 2^{\mathbb{Z}})$ è *bi-minimale*: ogni definibile è unione di un aperto e di un insieme discreto. Non è o-minimale ma non ci si può definire $\mathbb{Z}$. I frattali ad esempio non ce li si definisce.

Esempio 1.6.5. $(\overline{\mathbb{R}}, \mathbb{R}^{\text{alg}})$ non è o-minimale, ma i chiusi definibili qui dentro sono semialgebrici, e quindi già definibili in $\overline{\mathbb{R}}$.

Notazione 1.6.6. D'ora in poi S è una struttura o-minimale.

Sia $f\colon \mathbb{R} \to \mathbb{R}$ definibile in S. Sappiamo che f è continua e costante o strettamente monotona a tratti, cioè ci sono un numero finito di punti $a_1, \ldots, a_n$ tali che in ogni (a_i, a_{i+1}) la funzione è costante, oppure è monotona, e la stessa cosa succede su $(-\infty, a_1)$ e $(a_n, +\infty)$. Si può dire di meglio: per ogni r si può dire che f è C^r su ogni intervallo. Non si può dire C^∞ perché magari al crescere di r bisogna raffinare la partizione[33].

Ogni insieme definibile può essere partizionato come unione finita di *celle*. Cos'è una cella? Lo definiamo tra poco, ma iniziamo a dire che una proprietà delle celle di dimensione n è essere omeomorfe al disco n-dimensionare D^n.

Una cella 0-dimensionale è un punto. Una cella 1-dimensionale è un segmento[34] verticale o il grafico di una funzione definibile. Una cella 2-dimensionale è qualcosa della forma

$$\{(x, y) \in \mathbb{R}^2 \mid x \in T, \alpha(x) < y < \beta(x)\}$$

con T cella. In generale in dimensione più alta, senza scrivere la dimensione precisa, si prendono celle di dimensione più bassa, si prendono funzioni definibili su queste celle[35] e si prende tutto quello che sta "in mezzo" ai grafici. Poi ci si mette anche grafici di funzioni definibili e cose del genere.

[esempio di decomposizione di una faccina sorridente come unione finita di celle]

Se X è unione di celle C_i, si definisce la sua dimensione come massimo della dimensione delle sue celle, che è ben definita! Le celle sono in particolare varietà topologiche. Comunque basta dire che una cella ha dimensione n se contiene un aperto n-dimensionale (a meno di proiezioni opportune, ad

[33] Ed esiste veramente una bestia del genere, ma è sufficientemente complicata da evocare da aver reso questa cosa un problema aperto per un po' di tempo.

[34] Possibilmente illimitato, come gli intervalli nella definizione di o-minimalità. Non lo diremo più.

[35] Possibilmente costantemente infinite: si può prendere tutto quello che sta al di sopra del grafico di α prendendo β costantemente infinita, e simmetricamente.

esempio nel caso di grafici di funzioni). In altre parole X (che non è necessariamente una cella) ha dimensione $\geq d$ se e solo se esiste una proiezione su uno degli spazi coordinati di dimensione d tale che $\pi(X)$ ha interno non vuoto. Un risultato importante è che questo *non dipende dalla particolare decomposizione in celle scelta.*

Insomma, l'idea è di buttare a mare la curva di Peano[36] e altri oggetti patologici simili, ed è da qui che viene il nome "Tame Topology". Questa cosa in contesto o-minimale non può succedere: se $f\colon X \to \mathbb{R}^n$ è definibile $\dim(f(x)) \leq \dim(X)$ (non serve manco richiedere che sia continua), e vale l'uguaglianza se f è iniettiva.

Sia $f\colon \mathbb{R}^n \to \mathbb{R}$ definibile (e fissiamo $r \in \mathbb{N}$). Allora fuori[37] da un insieme definibile di dimensione $< n$ si ha che f è continua (C^r).

Definizione 1.6.7. Una *famiglia definibile di insiemi* è una famiglia di insiemi definibili uniformemente con la stessa formula cambiando parametri: l'idea è che la formula che definisce questi insiemi è "sempre la stessa". La si può vedere in questa maniera: prendiamo $X \subseteq \mathbb{R}^{n+m}$ definibile e prendiamo le sue fibre $\{X_a \mid a \in \mathbb{R}^n\}$, dove $X_a = \{y \mid (a,y) \in X\}$. Se $X = \{(x,y) \mid \varphi(x,y)\}$ allora $X_a = \{y \mid \varphi(a,y)\}$.

In teoria potrebbe succedere che ogni definibile è semplice ma che la famiglia è molto complicata, ad esempio un albero di insiemi finiti. In una struttura o-minimale nemmeno questo può succedere: se $\{X_a \mid\in A\}$ è una famiglia definibile allora esiste $d \in \mathbb{N}$ tale che per ogni a si ha che o X_a è infinito (e quindi ha dimensione almeno 1) oppure $|X_a| < d$. In realtà questa è la versione 0-dimensionale, ma c'è un risultato più forte:

Teorema 1.6.8. Sia $\{X_a \mid a \in A\}$ una famiglia definibile. Allora si può decomporre A in un numero finito di celle $C_1, \ldots, C_k$ tali che se a, a' sono nella stessa cella allora $X_a \cong X_{a'}$.

Cos'è quel $\cong$? Se ad esempio siamo interessati solo alla struttura topologica vuol dire omeomorfi (in particolare sono in bigezione) in maniera definibile. Si può anche avere C^r-diffeomorfi con diffeomorfismo definibile.

[esempio con un toro (per i non matematici: una ciambella), dove le sezioni/fibre sono vuote, punti o circonferenze]

Questi risultati valgono in generale per strutture o-minimali, anche se non espandono il campo reale, almeno finché si parla solo di continuità (ad esempio senza una moltiplicazione non ha senso parlare di differenziabilità). Quello che vediamo ora invece funziona solo in espansioni del campo reale.

Proposizione 1.6.9. Ogni insieme definibile è triangolabile, cioè definibilmente omeomorfo ad un complesso simpliciale[38].

[36] Una funzione $[0,1] \to [0,1]^2$ continua e surgettiva.

[37] Notare che è più forte di "quasi ovunque".

[38] Quasi, magari mancano dei bordi.

[esempio]

Come sono fatti gli 1-tipi? I prototipi di tipi sono il tipo di $a \in \mathbb{R}$, o il tipo di a^+, cioè $\{x > a, x < a + \epsilon, \epsilon > 0\}$ (lui non è totale ma ha un'unica estensione a tipo totale). Similmente a^+ con $\{x < a, x > a - \epsilon, \epsilon > 0\}$. Poi ci sono i tipi $+\infty = \{x > b \mid b \in \mathbb{R}\}$ e $-\infty = \{x = b \mid b \in \mathbb{R}\}$. (anche qui non è che siano totali, ma si estendono in maniera unica). Nel caso, ad esempio di $(\overline{\mathbb{R}}, 2^{\mathbb{Z}})$, l'estensione in maniera unica non c'è più: c'è da chiedersi se il predicato è vero o meno, e questo produce di tipi in più. Comunque

Esercizio 1.6.10. Nel caso o-minimale non ci sono altri tipi di tipi[39].

Chiudiamo parlando di caratteristica di Eulero. Per un poliedro è numero di vertici meno numero di spigoli meno numero di facce. In generale, per X definibile, lo si decompone in celle e poi, chiamando e_i il numero di celle di dimensione i, si pone $E(X) = e_0 - e_1 + e_2 - e_3 + \ldots \pm e_d$. Se $f\colon X \to Y$ è una bigezione definibile allora $E(X) = E(Y)$, e non dipende dalla decomposizione in celle scelta. Se X è una varietà compatta comunque E coincide con la caratteristica di Eulero-Poincaré. Occhio che non è la solita caratteristica di Eulero-Poincaré in generale: non è invariante per omotopia. Ad esempio se $X = [0, 1)$ allora $E(X) = 0$.

Abbiamo visto due invarianti: se $f\colon X \to Y$ è una bigezione definibile allora $\dim(X) = \dim(Y)$ e $E(X) = E(Y)$. La cosa bella è che presi insieme fanno un invariante completo!

Proposizione 1.6.11. Se X e Y sono definibili, $d(X) = d(Y)$ e $E(X) = E(Y)$, allora esiste $f\colon X \to Y$ bigezione definibile.

Ultima cosa: le celle sono connesse per archi. Ne segue che ogni definibile ha un numero finito di componenti connesse per archi.

[39] Nel senso che $+\infty$, $-\infty$ e a, a^+, a^- al variare di a li esauriscono.

Capitolo 2

Daniele Mundici
Teoria della Calcolabilità e Teoria della Complessità

In questo corso ci sono stati *tanti* discorsi motivazionali/storici/eccetera, ma non sono stati riportati. Stesso discorso per vagonate di dettagli. Per questo motivo gli appunti sono più corti di quanto uno si aspetterebbe (qualche lezione è omessa quasi per intero per scarsa voglia mia di prendere appunti).

2.1 24/08

Definizione 2.1.1 (Macchina di Turing)**.** In questo corso una *macchina di Turing* (o *macchina* e basta) è una tripla $M = (A, S, I)$, con $A = \{s_1, \dots, s_n\}$ un *alfabeto* finito, S un insieme finito di naturali chiamati *stati*, e I un insieme finito di *istruzioni*, ossia quintuple della forma $(s, a, b, +1, t)$, o $(s, a, b, -1, t)$ dove $s, t \in S$ e $a, b \in A$ tali che nessuna coppia di quintuple comincia con la stessa coppia (s, a).

La quintupla $(s, a, b, \pm 1, t)$ la leggiamo come "se nello stato s leggi il simbolo a, allora[1] lì stampa b, vai a destra/sinistra e vai in stato in t".

Definizione 2.1.2. Una *configurazione* di una macchina M è una tripla $c = (s, x, f)$, con $s \in S$, $x \in \mathbb{Z}$ (che pensiamo come "casella" di memoria, abbiamo un nastro in mente) e f una "fotografia di nastro", cioè una funzione $\mathbb{Z} \to A$ a supporto finito, nel senso che tranne un numero finito di eccezioni f assume valore $\square \in A$ che chiamiamo "casella vuota" o "blank".

C attiva al più una ben precisa istruzione di M: quella che comincia con $(s, f(x))$; se non ce n'è una la macchina "si ferma" su c, altrimenti "va" in

[1] Notiamo che abbiamo assunto che ce ne sia solo una; questa è l'assunzione di *determinismo*.

una nuova configurazione $c' = (s', x', f')$: se l'istruzione è $(s, f(x), b, \pm 1, t)$ sarà $c' = (t, \pm 1, f')$, dove f' coincide con f tranne che per $f'(x) = b$.

Un *passo di calcolo* è una coppia (c, c'), dove c' è la configurazione successiva a c secondo quanto detto sopra.

Esempio 2.1.3. $M = (A, S, I)$, dove $A = \{\square, |\}$, come stati useremo dei naturali, e I ha questi due elementi (e basta):

- $(0, |, |, +1, 0)$
- $(0, \square, |, +1, 1)$

È facile convincersi che su ogni configurazione che parte in stato 0 la macchina va avanti fino al primo $\square$ a destra, lo cambia in un $|$, va a destra e si ferma. In altre parole su input fatto da n asticelle calcola $n + 1$, o se ci piace di più calcola la funzione successore nella notazione del carcerato che conta i giorni di prigione.

Esercizio 2.1.4. "Upgradare" M ad una macchina M' che calcola il successore in "notazione carceraria" (aggiunge un'asticella in fondo all'input), dopodiché torni indietro alla prima casella dell'input e si fermi lì.[2]

Soluzione. Basta aggiungere[3] 2 agli stati e alle istruzioni

- $(1, \square, \square, -1, 2)$
- $(2, |, |, -1, 2)$
- $(2, \square, \square, +1, 3)$

□

Da ora la notazione "del carcerato" la chiameremo "asticolare" e ci sarà un off-by-one, nel senso che in questa notazione 0 è $|$, 1 è $||$, n è $n+1$ asticelle.

Esempio 2.1.5. Una macchina che calcola la funzione $z(x) = 0$ per ogni x asticolare (sempre tornando indietro). $S = \{0, 1, 2, 3\}$, le istruzioni di I sono

- $(0, |, |, +1, 1)$
- $(1, |, \square, +1, 1)$
- $(1, \square, \square, +1, 2)$
- $(2, \square, \square, -1, 2)$

[2] Si richiede il comportamento corretto solo su input corretto: la politica è garbage in-garbage out.

[3] Si può fare anche senza aumentare stati ma cambiando uno dei "vecchi" stati di M, ma per qualche motivo in questo momento a me piace di più aggiungere roba senza toglierla.

- $(2, |, |, -1, 3)$
- $(3, \square, \square, +1, 4)$

Osservazione 2.1.6. Le ultime due istruzioni non servono (a patto di togliere 3 dagli stati).

Esercizio 2.1.7. Scrivere

- una macchina che calcola il successore del successore, sempre in notazione asticolare, e sempre tornando indietro;
- una macchina che calcola la costante 1.

Abbiamo scritto delle macchine per il successore e lo 0. "Ci mancano" ancora un po' di funzioni: l'identità (calcolata dalla macchina senza istruzioni), le proiezioni $p_1^2(x, y) = x$ e $p_2^2(x, y) = y$.

Esercizio 2.1.8. Scrivere una macchina che calcola p_1^2. Come notazione, i due elementi della coppia vanno separati da $*$.

La p_2^2 va calcolata copiando l'input (vogliamo l'output che inizia in casella 1).

Esercizio 2.1.9. Farlo. Con 15 quintuple ce la si dovrebbe fare.

Fatto questo, moralmente abbiamo anche i p_k^n, e na volta che c'abbiamo 0, identità, successore e proiettori, componendole e usando la ricorsione ci si calcola un sacco di roba (*quasi* tutto quello che un computer sa calcolare).

2.2 25/08

Notazione 2.2.1. Da oggi invece di $+1$ e -1 useremo anche $\rightarrow$ e $\leftarrow$.

[soluzione per la macchina che calcola p_2^2 dando per buono di avere quella che sposta una stringa a sinistra fino ad un marcatore] Per "passare il controllo" a un'altra macchina bisogna rinominarne gli stati aggiungendo un opportuno naturale (tipo, massimo stati prima macchina più uno) avendo cura che il primo stato della macchina cui va il controllo sia l'ultimo della macchina che cede il controllo.

Esercizio 2.2.2 (Gradus ad Parnassum)**.** Si riescono a scrivere le seguenti macchine:

- Duplicatrice, o fotocopiatrice: duplica una stringa di asticelle inserendo una virgola fra originale e copia
- Matching: su input due stringhe separate da virgola decide se sono uguali, nel senso che restituisce un $=$ se sono uguali, un $\neq$ altrimenti.

- Evidenziatore: sostituisce le asticelle con "asticelle ingrassate" (un altro simbolo)
- Evidenziatore binario: grassetto come prima su alfabeto binario
- Zero binaria: restituisce 0 in binario
- Proiettori p_k^n binari (che useranno uno "sposta a sinistra binario")
- Successore binario (questo è un po' meno banale)

La definizione precisa di ricorsione è sulle dispense. Ora due Teoremi, senza dimostrazione anche sulle dispense (ma facile da reperire in letteratura):

Teorema 2.2.3 (La Turing-calcolabilità si conserva per composizione)**.** Siano $f_1, \ldots, f_k \colon \mathbb{N}^t \to \mathbb{N}$ e $g \colon \mathbb{N}^k \to \mathbb{N}$ calcolate rispettivamente da macchine $\mathcal{F}_1, \ldots, \mathcal{F}_k$ e $\mathcal{G}$, allora la composizione $g(f_1, \ldots, f_k)$ è calcolata da una macchina di Turing.

["proof by handwaving" non riportata]

Teorema 2.2.4 (La Turing-calcolabilità si conserva per ricorsione)**.** Anche questo come da nome.

Ma magari a sto punto la definizione vera di ricorsione diamola:

Definizione 2.2.5. Siano $b \colon \mathbb{N}^k \to \mathbb{N}$ e $p \colon \mathbb{N}^{k+2} \to \mathbb{N}$. Allora $f \colon \mathbb{N}^{k+1} \to \mathbb{N}$ ottenuta *per ricorsione dalla base b e dal passo p* è definita come segue[4]

$$\begin{cases} f(x, 0) = b(x) \\ f(x, y+1) = p(x, y, f(x, y)) \end{cases}$$

["proof by handwaving" dell'altro teorema, non riportata]

Nota: per dieci anni hanno pensato che questo esaurisse le calcolabili. E invece...

Definizione 2.2.6. Una funzione è *primitiva ricorsiva* se è ottenibile da[5] successore, zero e proiettori tramite composizioni e ricorsione.

Esempio 2.2.7. Esempi di primitive ricorsive (e quindi Turing-calcolabili):

- Somma
- Prodotto
- Esponenziale

[4] Qui $x = (x_1, \ldots, x_k)$.

[5] Se sta nella chiusura di... per...

- Fattoriale
- Massimo comun divisore
- Quoziente
- Resto
- $\dot{-}$, cioè $\max(x - y, 0)$
- Distanza fra due interi
- n-esima cifra di π
- φ di Eulero
- Un macello di altra roba

Comunque, come detto prima, ci sono funzioni calcolabili che non sono primitive ricorsive, nonché funzioni non calcolabili. Cosa manca ancora per avere tutte le Turing-calcolabili?

Definizione 2.2.8. Una funzione $f\colon \mathbb{N}^{k+1} \to \mathbb{N}$ (con $k \geq 1$) è detta *regolare* se per ogni $x_1, \ldots, x_k$ esiste y tale che $f(x_1, \ldots, x_k, y) = 0$

Esempio 2.2.9. $\mathrm{add}(x, y)$ non è regolare; $\mathrm{prod}(x, y)$ è regolare.

Quell'"esiste" nella definizione è problematico (o, vista in un altra maniera, è il responsabile dell'aumento della potenza di calcolo): come si fa a calcolarlo?

Definizione 2.2.10. La funzione $g\colon \mathbb{N}^k \to \mathbb{N}$ ottenuta per *minimizzazione* di f (regolare) è definita come segue: $g(x_1, \ldots, x_k)$ è il minimo y tale che $f(x_1, \ldots, x_k, y) = 0$.

Teorema 2.2.11. La Turing-calcolabilità si conserva per minimizzazione di funzioni regolari.

2.3 26/08

Vogliamo costruire una *macchina universale*; in breve, una macchina in grado di simulare tutte le altre macchine. Questa sarà una tripla $U = (A_U, S_U, I_U)$, dove tutto è finito come in tutte le macchine. L'idea di fondo è che le macchine si possono codificare, scrivere su un nastro e dare in pasto a questa macchina. L'alfabeto sarà

$$A_U = \{\square, a, |, s, \rightarrow, \leftarrow, A, I, S, \Rightarrow, \Leftarrow, M, N, P, Q\}$$

l'idea è simulare i simboli della macchina da simulare in questa maniera: il primo sarà a, il secondo $a|$, e in generale l'n-esimo sarà a seguito da $n - 1$

asticelle; stessa cosa per gli stati con s. Gli altri servono per "evidenziare" (quelli in grassetto) e gli ultimi come marcatori. Usando questo non è difficile[6] codificare una macchina, nonché le sui configurazioni. Chiamiamo queste codifiche "verbalizzazioni".

Teorema 2.3.1 (Turing, 1936)**.** Esiste[7] una macchina $U = (A_U, S_U, I_U)$ che per ogni macchina[8] $M = (A_M, S_M, I_M)$ fa quanto segue: se sul suo nastro troviamo scritta la verbalizzazione $\bar{M}$ seguita da * seguita da una configurazione verbalizzata $\bar{c}$ allora

Caso 1 Se c'è c' (cioè se M fa il passo (c, c')) allora dopo un numero finito di passi U produce $\bar{M}$ seguita da * seguita da $\overline{c'}$ e va in stato ω

Caso 2 Se M su c si arresta, ossia c' non c'è, allora dopo un numero finito di passi U produce la configurazione $\bar{M}$ seguito da * seguito da $\bar{c}$ e va in stato Ω.

Corollario 2.3.2. Nel caso 1, anziché far terminare U su ω, se la facciamo terminare in stato 0 succede che via via la nuova macchina U^* produrrà una configurazione dietro l'altra.

Dimostrazione del Teorema. La macchina si va a pescare l'istruzione rilevante nella codifica e modifica quello che deve modificare di conseguenza. Visto che non ho scritto la codifica eccetera non scrivo nemmeno i dettagli di questo (si vedano dispense/libro di Mundici). □

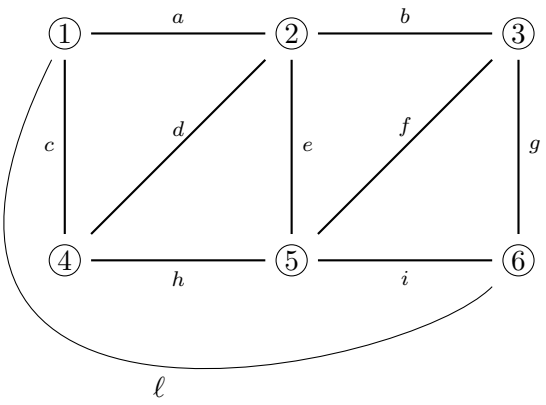
2.4 27/08

Problema: colorare i nodi del seguente grafo con tre colori in maniera che nessuna coppia di vertici adiacenti (collegati da un arco) abbia lo stesso colore:

[6] Ma furbo/macchinoso; tipo, per indicare la posizione della testina basta scrivere lo stato nel punto di nastro in cui si trova, e cose del genere.

[7] Ed è un esiste onesto, nel senso che volendo le quintuple si scrivono per davvero (l'ha dato come tesi a una studentessa).

[8] Tra l'altro c'è un minimo di ambiguità fra M dell'alfabeto A_U e M la macchina, ma ci siamo capiti.



[riduzione polinomiale di COLORABILITY a SAT from scratch] Riduzioni come morfismi fra problemi.

2.5 28/08

[ancora sulle riduzioni]

KNAPSACK: un'istanza è data da numeri $a_1, \ldots, a_n, a \in \mathbb{N}$. Domanda: esiste un sottoinsieme di $a_1, \ldots, a_n$ la cui somma è a?

[definizione di NP con i primi di Fermat come esempio per il certificato] Descrizione suggestive di NP: "Quei problemi dove se riesci ad assumere un genio gli puoi dare da lavorare e il cui lavoro puoi controllare"

Nota: anche se $\mathsf{P} = \mathsf{NP}$ i certificati potrebbero non essere l'informazione che cerchiamo (ad esempio AKS non fornisce una fattorizzazione). [suggestione sul fatto che analogamente le "dimostrazioni" date da certificati potrebbero sfidare la nozione occidentale di dimostrazione, che in fondo a scavare fino ai greci "viene dagli avvocati"]

2.6 29/08

`mundici@math.unifi.it`

[ciclo hamiltoniano/tsp]

[teorema di Cook-Levin]

Nota: senza perdita di generalità il nondeterminismo si può avere solo sugli stati (e non sui simboli) (non è difficile da mostrare, basta aggiungere stati appositi e transizioni deterministiche per stampare...). Si usa nella dimostrazione[9].

[9] IMHO a puro titolo di comodità, nel senso che probabilmente si fa anche senza.

Altra nota: cambiando modello di calcolo cambiano solo le classi di problemi lineari e sublineari: i vari sistemi tendono a simularsi a vicenda in tempo quadratico o qualcosa del genere ("invarianza delle definizioni per professore e libro di testo")

Levin: il calcolo booleano è universale per il *perebor* (3 anni dopo Cook). Il paper di Cook stava per essere rigettato "perché banale" (nota da Wikipedia: nell'approccio di Levin ci sono degli algoritmi che terminano in tempo polinomiale se e solo se $\mathsf{P} = \mathsf{NP}$).

Capitolo 3

Lezioni Magistrali

3.1 Francesco Paoli—Relazioni di Conseguenza su Multinsiemi

3.1.1 Logica Algebrica

- Boole era un "algebrista della logica"
- Continua sto filone con Pierce e altri, ma diventa un "dialetto minoritario" rispoetto a Frege, Russell, Hilbert e compagnia cantante.
- Finché Lindenbaum e Tarski non fondono i due approcci.
- Facciamo un minicorso di introduzione alla logica seguendo l'approccio "logica algebrica"
- Connettivo e simbolo sono sinonimi, idem termini e formula, variabile individuale e variabile proposizionale
- Linguaggio proposizionale su un insieme numerabile di variabili X: è un insieme nonvuoto $\mathcal{L}$, i cui membri sono chiamati connettivi, ognuno munito di arietà. Le $\mathcal{L}$-formule sono definite induttivamente dichiarando che ogni $p \in X$ è una formula e che se c è un connettivo n-ario anche $c(\alpha_1, \ldots, \alpha_n)$ è una formula.
- Assumeremo $\mathcal{L}$ finito e useremo la notazione infissa per i connettivi binari.
- Per come abbiamo dato le definizioni possiamo definire l'*algebra delle formule*, dove le operazioni sono i connettivi. Chiaramente ora ha senso parlare di omomorfismi, che chiamiamo *valutazioni*. Data un'algebra $\mathbf{A}$ di un linguaggio $\mathcal{L}$ e $a_1, \ldots, a_n \in \mathbf{A}$ definiamo $\alpha^{\mathbf{A}}(a_1, \ldots, a_n)$ come l'applicazione dell'unico omomorfismo h dalle formule ad $\mathbf{A}$ che manda $h(p_i) = a$. [manca roba]

- A questo punto si definisce *relazione di conseguenza* su $\mathscr{P}(Fm_{\mathcal{L}}) \times Fm_{\mathcal{L}}$ come una relazione riflessiva, monotona, e con la cesura, cioè tale che se $\Gamma \vdash \alpha$ e $\Delta \vdash \gamma$ per ogni $\gamma \in \Gamma$ allora $\Delta \vdash \alpha$.

- Un modo per caratterizzare la "formalità" e definire l'invarianza per sostituzione: se $\Gamma \vdash \alpha$ e σ è un endomorfismo di $FM_{\mathcal{L}}$ allora $\sigma(\Gamma) \vdash \Sigma(\alpha)$.

- Un'altra nozione è quella di essere una relazione finitaria: se $\Gamma \vdash \alpha$ allora esiste $\Delta \subseteq_{\text{fin}} \Gamma$ tale che $\Delta \vdash \alpha$.

- (le due proprietà sopra sono opzionali, per un relazione di conseguenza)

- Tarski definisce anche un *operatore di conseguenza* come un operatore di chiusura sul poset $(\mathscr{P}(Fm_{\mathcal{L}}), \subseteq)$.

- Lemma: c'è una bigezione fra gli operatori di conseguenza e le relazioni di conseguenza (algebra delle formule fissata). Più nello specifico se $\vdash$ è una relazione di conseguenza su $Fm_{\mathcal{L}}$ allora $\xi_{\vdash} \colon \mathscr{P}(Fm_{\mathcal{L}}) \to \mathscr{P}(Fm_{\mathcal{L}})$ definita da $\xi_{\vdash}(\Gamma) = \{\alpha \mid \Gamma \vdash \alpha\}$ è un operatore di conseguenza [mi sono perso l'altro verso]

- Chiamiamo logica proposizionale una coppia $(Fm_{\mathcal{L}}, \vdash)$, con $\vdash$ invariante per sostituzione. Una formula α è un teorema della logica se $\emptyset \vdash \alpha$.

- Regola di inferenza: una coppia (Γ, α), con $\Gamma \in \mathscr{P}_{\text{fin}}(Fm_{\mathcal{L}})$ e $\alpha \in Fm_{\mathcal{L}}$. Se Γ è vuoto la chiamiamo assioma. Un calcolo alla Hilbert è un insieme di regole di inferenza con almeno una regola propria (cioè che non sia un assioma) [esempio]

- Costante proposizionale: connettivo di arietà 0

- Per tirare fuori una relazione di conseguenza da un calcolo alla Hilbert si introduce la nozione di derivazione, cioè una successione finita di formule che finisce con β (se parliamo di una derivazione di β), dove ogni β_i si ottiene da Δ o tramite regole di deduzione eccetera [manca la definizione precisa]

- Da qui si tira fuori una nozione di conseguenza invariante per sostituzione dicendo che $\Gamma \vdash_{HL} \alpha$ se nel sistema HL c'è una derivazione di α da Γ.

- Lindenbaum e Tarski: in un certo senso preciso le algebre di Boole sono la controparte algebrica della logica classica formalizzata nel sistema finora presentato

- Logiche 1-asserzionali: Sia $\mathcal{K}$ una classe di algebre sullo stesso linguaggio $\mathcal{L}$ che includa una costante (connettivo 0-ario) 1, che pensiamo come "vero". Diciamo che $\Gamma \models_{\mathcal{K},1} \alpha$ sse per ogni $\mathbf{A} \in \mathcal{K}$ e $\vec{a} \in A^n$, se $\gamma^{\mathbf{A}}(\vec{a}) = 1^{\mathbf{A}}$ per ogni $\gamma \in \Gamma$ allora $\alpha^{\mathbf{A}}(\vec{a}) = 1^{\mathbf{A}}$.

- Questo si può riscrivere come $\Gamma \models_{\mathcal{K},1} \alpha$ sse $\{\gamma \approx 1 \mid \gamma \in \Gamma\} \vdash_{Eq(\mathcal{K})} \alpha \approx 1$

- Questa $\models_{\mathcal{K},1}$ è una relazione di conseguenza tarskiana, dunque genera una logica $S(\mathcal{K}, 1)$.

- Algebra di Boole: reticolo distributivo limitato (cioè 1 è un massimo e 0 è un minimo) con $a \wedge \neg a = 0$ e $a \vee \neg a = 1$. Per averci lo stesso linguaggio delle algebre della logica classica aggiungiamo anche $\rightarrow$ definito nel modo classico

- Teorema di Lindenbaum-Tarski: la logica classica è $S(\mathcal{BA}, 1)$ (dove $\mathcal{BA}$ sono le algebre di Boole)

- La parte difficile è mostrare $\supseteq$ (l'altra si fa per induzione sulla lunghezza della derivazione): si fa montando un'algebra di boole dove Γ funge e α no ogni volta che $\Gamma \nvdash_{HCL} \alpha$.

- Questa si costruisce come quoziente dell'algebra di Boole delle formule per la dimostrabile equivalenza in ogni teoria che include Γ.

- Problema: questo Teorema è bello, una pietra miliare, e tande care couse, ma è difficile da estendere ad altre logiche.

- Si rimedia parlando di *traduzioni* τ: insiemi di equazioni in una sola variabile di $\mathcal{L}$. La possiamo pensare come una funzione che mappa formule in insiemi di equazioni dello stesso linguaggio. Poi si definisce $\tau(a)$ come l'insieme dove si sostituisce l'unica variabile delle equazioni con a

- Con questo si può definire una *logica τ-asserzionale* sbarazzandoci della necessità dell'1: $\Gamma \models_{\mathcal{K},\tau} \alpha$ sse $\{\tau(\gamma) \mid \gamma \in \Gamma\} \vdash_{Eq(\mathcal{K})} \tau(\alpha)$

- In pratica invece di dire "se sta roba è vera allora" diciamo "se ste robe hanno lo stesso valore di verità", e così non c'è bisogno di un 1 che stia per "vero"

- Con $\tau = \{p \approx 1\}$ ritroviamo la vecchia nozione

- Da qui ci sono un po' di problemi e tecnicaglie che omettiamo per questioni di tempo. Ci sono un po' di punti deboli in questo approccio. Negli anni '80 Blok e Pigozzi hanno introdotto la nozione di *algebrizzabilità* per rimediare.

3.1.2 Logiche Sottostrutturali

- Prima un paio di prerequisiti
- Un multinsieme è una funzione da un insieme ai naturali
- Lo pensiamo come insieme dove gli elementi possono apparire più volte
- La radice di $\mathfrak{X}$ è $|\mathfrak{X}| = \{a \in A \mid \mathfrak{X}(a) > 0\}$
- Indichiamo i multiinsiemi con le quadre, tipo $[a, a, b, c]$
- Un multinsieme è finito se ha radice finito.
- Sottomultiinsiemi: $\mathfrak{Y} \leq \mathfrak{X}$ sse $\forall a \in A\ \mathfrak{Y}(a) \leq \mathfrak{X}(a)$. Il multi powerset è definito come ci si aspetta. Si può definire anche per insiemi [mi sono perso la definizione]
- Join meet differenza e somma $(\mathfrak{X}, \mathfrak{Y})$ si definiscono come sup, inf, differenza $\mathfrak{X}(a) - (\mathfrak{X} \wedge \mathfrak{Y})(a)$ e somma (notare l'unione che si è "sdoppiata")
- Gentzen e sequenti: un sequente è una coppia ordinalta di multinsiemi di formule $\alpha_1, \ldots, \alpha_n \Rightarrow \beta_1, \ldots, \beta_m$, da leggersi "la disgiunzione delle β è segue dalla congiunzione delle α"
- Anche qui si può definire un calcolo dei sequenti [esempio per la logica classica]: qui weakening e cancellazione dicono praticamente che "in realtà" stiamo lavorando con insiemi (per le sottostrutturali non sarà così)
- Il calcolo dei sequenti classico GCL si fa diventare un calcolo GIL per la logica intuizionista semplicemente richiedendo di usare solo sequenti che hanno al più una formula nel conseguente, senza parlare di terzi esclusi o cose del genere. Questo dice ad esempio che non c'è una regola di contrazione a destra, che il weakening a destra è confinita a roba con conseguente vuoto...
- Si può andare oltre?
- Prima idea: logiche resource-conscious, dove gli enunciati sono token di informazioni di un qualche tipo: qui la contrazione è sospetta: se una cosa segue da due occorrenze di α magari una sola non basta
- Seconda: logiche rilevanti: le premesse dovrebbero essere veramente usate per arrivare alle conclusioni. Ma allora il weakening non va bene: da $\Gamma \vdash \gamma$ non vogliamo $\Gamma, \alpha \vdash \gamma$.
- Effetto collaterale: la logica si arricchisce, nel senso che senza certe regole strutturali definizioni equivalenti di—metti—la congiunzione si trasformano in concetti effettivamente diversi di congiunzione

- FL_e-algebra: un'algebra $\mathbf{L} = (L, \wedge, \vee, \cdot, \to, 1, 0)$ tali che $(L, \wedge, \vee)$ è un reticolo, $(L, \cdot, 1)$ è un monoide commutativo, $\cdot$ è residuato con residuo $\to$ (nell'ordine indotto dalle operazioni reticolari) e 0 è un elemento su cui non si fanno ipotesi (una puntatura) (serve per definire la negazione come $a \to 0$

- Le algebre di Boole e Heyting sono equivalenti per temrini a certe particolari FL_e-algebre. Ad esempio per $\mathcal{B}A$ si aggiungono le equazioni $0 \to x \approx 1$, $xy \approx x \wedge y$ e $(y \to x) \to x \approx x \vee y$; togliere l'ultima dà quelle di Heyting

- Come si definisce una nozione di conseguenza? $\Gamma \vdash_{FL_e} \alpha$ sse il sequente $\Rightarrow \alpha$ è dimostrabile aggiungendo a FL_e come essiomi i sequenti in $\{\Rightarrow \gamma \mid \gamma \in \Gamma\}$. Sia inoltre $\tau = \{p \wedge 1 \approx 1\}$

- Teorema: $\Gamma \vdash_{FL_e} \alpha$ sse $\Gamma \vdash_{HFL_e} \alpha$ sse $\Gamma \vdash_{\mathcal{FL}_e,\tau} \alpha$, e queste sono nozioni di conseguenza Tarskiane

3.1.3 Conseguenza su Multinsiemi

- Claim: questo approccio e poco soddisfacente o perlomeno poco interessante: l'idea è che finiamo per lavorare con relazioni su insiemi, quindi monotone, e quindi con weakening/contrazione impliciti. Per essere fedeli allo spirito delle logiche sottostrutturali vorremmo formalizzare una nozione di conseguenza interna $\Gamma \vdash^*_{FL_e} \alpha$ sse $\Gamma \Rightarrow \alpha$ è un sequente di FL_e dimostrabile.

- A sto punto bisognerebbe abbandonare la monotonia, a una relazione di conseguenza dovrebbe essere penato come una relazione fra un multinsieme finito di formule e una formula. Questo approccio è stato seguito da Avron, Meye.McRobbie, Troelstra e qualche altro

- Ma forse è troppo estremista; proviamo a mischiare le cose

- Chiamiamo una relazione di conseguenza per multinsiemi naïve (nmcr) come una relazione $\subseteq \mathscr{P}^M(FM_{\mathcal{L}}) \times Fm_{\mathcal{L}}$ riflessiva, monotona e col taglio/cesura

- (mancano un paio di nozioni opzionali extra)

- nmco (operatore di conseguenza): [definizione]

- Ripley's bombshell: se definiamo $\Gamma \vdash_\xi \alpha$ sse $\alpha \in |\xi(\Gamma)|$ ci viene fuori sempre una cosa contrattiva [mi sono perso la definizione]

- Approccio a conclusione multipla: l'idea è che $\Gamma \vdash \Delta$ vuol dire che usando al massimo una volta tutte le assunzioni di Γ si possono derivare simultaneamente tutte le conclusioni in Δ

- Multiset consequence relation mcr: riflessiva, taglio, monotonia
- Qui il tecnicismo si impenna, comunque si parla di mcr a conseguenza singola
- Se uno prova a usare la logica di Łukasiewicz a infiniti valori come logica delle risorse incontra qualche problema; $\nvdash_{\text{Luk}} a \to a \otimes a$ va bene (se un caffè costa un euro non è che con un euro mi compro due caffè), però $a \vdash_{\text{Luk}} a \otimes a$.
- Quindi vogliamo un cugino di questa logica in cui queste "brutture" non accadono
- Diciamo che $a_1, \ldots, a_n \vdash \beta$ sse $\vdash_{\text{Luk}} a_1 \otimes \ldots \otimes a_n \to \beta$, e questo è il cugino che cercavamo
- Qui definire una teoria è delicato perché parlare di "chiusura deduttiva" è problematico: visto che dimostrare richiede risorse...
- Definiamo quindi una teoria di una mcr come un insieme di multinsiemi di formule tali che se $T \vdash \Delta$ allora $\Delta \in T$. Con $\text{Th}(\vdash)$ indichiamo l'insieme di tutte le teorie di $\vdash$. Questo salta fuori essere un sistema di chiusura...
- Salta fuori che la generalizzazione di operatore di conseguenza conveine darla come operatore $\mathscr{P}^{\mathbf{M}}(Fm_{\mathcal{L}}) \to \mathscr{P}(\mathscr{P}^{\mathbf{M}}(Fm_{\mathcal{L}}))$ con enlargement, preservazione dell'ordine e idempotenza
- Da qui si mette in piedi tutta una teoria che non abbiamo il tempo di vedere qui.
- Ci si dà pure un teorema di completezza con semantica matriciale, dove una matrice è un'algebra con un sottoinsieme dell'universo di quest'algebra che pensiamo come valori designati, ossia possibili valori di formule vere.
- Un'idea sarebbe rimpiazzare tutte le nozioni set-teoretiche con roba multiset-teoretica, ma vorrebbe dire rifare tutta l'algebra universale dall'inizio
- Invece si definiscono i monoid matrix: per un linguaggio $\mathcal{L}$ una quadrupla $M = (A, D, G, f)$ tale ceh A è un'algebra di tipo $\updownarrow$, $D = (D, \cdot, 1, \sqsubseteq)$ è un po-monoide commutativo integro, G un filtro d'ordine su D e f un omomorfismo di po-monoidi $(\mathscr{P}^M(A), \uplus, \emptyset, \geq) \to (D, \cdot, 1, \sqsubseteq)$
- Matrici fuzzy; monoid matrix più una T-norma

- (finale troppo veloce da trascrivere, ma si finisce a parlare di funzioni reali per motivi che mi sono perso; questo produce un teorema di completezza per il "cugino di Łukasiewicz")
- L'idea è che la logica di Łukasiewicz si comporta in maniera più booleana: niente è designato "finché l'1 lo diventa", nel cugino c'è una separazione netta fra designati e no (il disegnino è un quadrato contro un quadrato con la diagonale)

3.2 Simona Ronchi Della Rocca Logica Lineare, Tipi e Complessità

- In genere per studiare la complessità si fissa un modello computazionale; di solito le macchine di Turing (per la loro semplicità). Qui il tempo è il numero di passi e lo spazio la dimensione del nastro utilizzato.
- Primo problema di questo approccio: la progettazione di un programma e il calcolo della sua complessità sono effettuati in due momenti separati, in qualche maniera duplicando il lavoro
- Secondo problema: è difficile dare dimostrazioni formali di complessità (formalizzare in dettaglio una dimostrazione su una macchina di Turing è macchinoso)
- ICC: Implicit Computational Complexity: l'idea è non usare *nessun* modello di calcolo, sostituendoli con teoria della dimostrazione, ella ricorsione, dei modelli. Gli scopi sono due: caratterizzare "implicitamente" le classi di complessità e fornire prove certificate di complessità dei programmi
- Ci concentreremo sulla prima parte, ma le due sono collegate.
- Idea: partire da un linguaggio di programmazione L e fornire una "disciplina di tipi" ("tipo" nel senso informatico del termine) in maniera che se un programma è ben tipato la sua complessità sta in una certa classe; inoltre vogliamo che tutte le funzioni in quella classe di complessità siano calcolabili da un programma ben tipato.
- Realizzazione: λ-calcolo (esteso in qualche maniera) come linguaggio e tipi ispirati dalla Soft Linear Logic (una versione "light" della logica lineare)
- Questo approccio caratterizza PTIME, FPTIME, NP, PSPACE
- λ-calcolo: (solita sintassi); la β-riduzione è $(\lambda x.M)N \underset{\beta}{\rightarrow} M[N/x]$, con qualche cautela sulla cattura delle variabili.

- Nota: questo non ci dice niente sulla complessità, in altre parole non è ancora un modello di costo; a seconda di quanto è grande ad esempio $x\ldots$
- Nel λ-calcolo ci si codificano i naturali, le parole binarie, e tutte le funzioni calcolabili.
- Logica lineare: due tipi di formule, A (risorsa lineare, può essere usata solo una volta), $!A$, può essere usata quante volte si vuole, anche 0
- ! è idempotente
- L'implicazione intuizionista $A \to B$ è decomposta in $!A \multimap B$ (la logica lineare e intuizionista hanno la stessa potenza espressiva). Questa "implicazione lineare" è una "freccia di uso": uso *una sola volta* A per produrre B. Usare ! permette di "duplicare" A
- Non entriamo nei dettagli della logica lineare (non trascrivo i sequenti) intuizionista (ILL)
- Si usano i sequenti perché le logiche modali hanno problemi a essere trattate in deduzione naturale
- Però noi non vogliamo solo contare se una cosa è usata una o più volte; vogliamo proprio contarle. La soluzione è buttare a mare l'idempotenza di !. Questa si chiama SLL (soft linear logic)
- In realtà non lavoreremo con la SLL, ma l'idea viene da qui
- Praticamente l'idea sarebbe contare i ! usati e pensarli come risorse.
- STA: stile deduzione naturale ispirato alla SLL
- I tipi sono un sottoinsieme proprio delle formule ("proprio" per ragioni tecniche di trattabilità, ma non si perde potenza estensiva)
- Nel λ-calcolo il tempo di calcolo dipende da quante sostituzioni si fanno, quindi c'è da contare le sostituzioni
- L'operatore modale ! diventa la certificazione che la formula è stata duplicata
- (regole di STA)
- (il λ-calcolo era stato inventato per trattare la logica intuizionista in deduzione naturale)
- Differenza dalla deduzione naturale: c'è una regola che nella parte in basso aggiunge assiomi a sinistra (il multiplex, che tratta il !; pensarci un attimo...)

- Ci sono dei teoremi di normalizzazione(che in sostanza garantiscono che le computazioni terminano) e "subject reduction" (che in sostanza garantisce che il sistema funziona bene e nelle manipolazioni di termini non si cambia tipo)
- La storia di contare i ! formalmente diventa il *rango* di un'applicazione del mpx.
- (esempio)
- Tutto il macchinario poi può essere implementato in una macchina di Turing e un teorema fornisce upper bound su quanto tempo ci mette a fare le deduzioni.
- Ogni derivazione di tipo (deduzione che alla fine dice: "sto termine c'ha sto tipo") fornisce un bound (ma chiaramente si va a vedere il più basso)
- (esempio di codifica di tipi di dati(valori di verità, naturali,...) nel λ-calcolo; esempio di codifica di funzioni)
- Teorema: i termini che codificano funzioni riducono a forma normale in tempo polinomiale
- Caratterizzazione di PTIME: tutti i problemi in P possono essere codificati in STA; la dimostrazione è pesantissima (il viceversa mi sembra di aver capito che sarebbe la "correttezza polinomiale"; questa la completezza)
- Problemi: programmare in questo λ-calcolo ben tipato è un casino; è un problema più profondo di quello che sembra: già il fatto che i programmi devono sempre terminare mi impedisce di usare la ricorsione, quindi non è un problema di questo specifico sistema. Non c'è nemmeno l'iterazione, se non in forme ristrette
- In breve: programmare qui richiede una disciplina programmativa diversa da quella cui siamo abituati
- E se vogliamo parlare di spazio e nondeterminismo?
- Per lo spazio si usa l'equivalenza PSPACE = APTIME (macchine di Turing alternanti)
- Il fatto è che finora nessuno ha usato questo ordine di idee per codificare direttamente lo spazio, per quello si passa dal tempo alternante
- Uno dei motivi è che nella programmazione reale non si sostituisce mai per davvero un termine con un altro, si usano link o cose del genere;

quindi usare la lunghezza dei termini come spazio non è una buona idea

- Quindi si definisce una macchina astratta di riduzione per il λ-calcolo che evita quando possibile le sostituzioni
- L'equivalenza PSPACE = APTIME permette di riciclare i risultati noti per il tempo
- (non riporto la definizione di macchina alternante di Turing)
- Ai termini si aggiunge l'"if" (e alle regole e i tipi di conseguenza)
- Il type system si chiama STAB
- Ci sono anche qui subject reduction e normalizzazione forte (che è più facile da dimostrare di quanto si pensi)
- (esempi e tecnicismi)
- Anche qui soundess e completeness e quindi STAB cattura PSPACE
- Per il nondeterminismo non c'è più l'if, ma ci sono tipi $M+M$; qui non ci sono più forme normali (il sistema di calcolo non è più confluente)
- La subject reduction c'è
- Serve della cautela tecnica perché permettere la scelta nondeterministica in ogni punto può produrre anche cose esponenziali, che non vogliamo codificare
- Il sistema corretto e completo si chiama STA+
- Problemi pure qui: queste caratterizzazioni sono implicite fino a un certo punto, nel senso che una certa macchina astratta comunque c'è bisogno di usarla per misurare lo spazio
- Nomi di riferimento: Girard, Lafont, Gaboardi, Ronchi Della Rocca, Gaboardi, Marion.
- Leggere per la prima volta la logica lineare è un'esperienza mistica.
- Nota: questo sistema è indecidibile (non si può tipare automaticamente) per colpa di $\forall$, quindi avere certificati di polinomialità è un problema. Togliere $\forall$ sistema le cose.