Lezione 1

25 Settembre

Va fatta una distinzione tra:

- Sintassi: come si scrivono le proposizioni
- Semantica: cosa significano

Spesso infatti in matematica utilizziamo dei simboli per rappresentare oggetti, ma non tutti i simboli sono uguali. Tra di questi distinguiamo i simboli logici, che sono simboli che non cambiano di significato, indipendentemente dalla branca della matematica in cui ci troviamo. Se per esempio consideriamo $+$, ci rendiamo subito conto che nel corso dei nostri studi abbiamo utilizzato questo simbolo per indicare operazioni diverse, mentre invece vi sono dei simboli il cui valore non varia. Possiamo dividere i simboli logici in:

- Connettivi booleani: $\neg$, $\wedge$, $\vee$, $\rightarrow$
- Quantificatori: $\forall$, $\exists$
- $=$, che non viene universalmente riconosciuto come tale

Diamo per scontata la conoscenza delle tavole di verità dei connettivi booleani e la loro composizione.

1.1 Logica proposizionale

Osservazione 1. Potremmo notare che, in effetti, non tutti i simboli logici ci sono necessari. Introduciamo innanzitutto un ulteriore connettivo booleano: il né ..., né ..., che indicheremo con $\wr$ (che è vero solo nel caso in cui valgono $\neg A$ e $\neg B$). Abbiamo dunque che:

- $A \rightarrow B \equiv \neg(A \wedge \neg B) \equiv B \vee \neg A$
- $A \vee B \equiv \neg(\neg A \wedge \neg B)$
- $A \wedge B = \neg(\neg A \vee \neg B)$
- $A \vee B = ((A \wr B) \wr (A \wr B))$
- $\neg A = A \wr A$

- $A \oplus B := A \vee B \wedge \neg(A \wedge B)$
- $A \leftrightarrow B := (A \wedge B) \vee (\neg A \wedge \neg B)$

Abbiamo quindi che l'unico connettivo booleano che in realtà ci serve è $\wr$, ma per praticità li usiamo tutti.

Abbiamo utilizzato quelle che vengono chiamate 'variabili proposizionali' (A, B, $\cdots$) che servono a rappresentare delle proposizioni generiche. Una proposizione è un oggetto al quale possiamo attribuire un valore: 1 (se vero), o 0 (se falso). A partire da variabili proposizionali e connettivi possiamo creare quelle che vengono chiamate 'formule proposizionali', come per esempio:

$$(A \vee B) \wedge \neg B \to A$$

Sostituendo alle variabili proposizionali proposizioni come "piove" o "fa freddo" otteniamo vere proposizioni. Le formule proposizionali dunque servono per studiare i vari tipi di ragionamento, in quanto li schematizza e aiuta a riconoscere alcune strutture che sono sempre vere o sempre false.
Si dice per esempio 'tautologia' una formula proposizionale che è vera indipendentemente dal valore che viene attribuito ad A e a B. Diciamo inoltre che due formule sono 'equivalenti' ($\equiv$) se hanno la stessa tavola di verità.

Esercizio 1. Dimostrere che, utilizzando solamente $\oplus$ e $\neg$ è possibile ottenere $\leftrightarrow$ ma non $\vee$.

Dimostrazione.
- Si verifica che $A \leftrightarrow B \equiv \neg(A \oplus B)$
- Si dimostra per induzione che una qualsiasi formula proposizionale ottenuta tramite $\oplus$ e $\neg$ ha un numero pari di casi in cui è verificata. Questo non è vero per il connettivo $\vee$.

Riflessione 1. Questi esempi ed esercizi ci fanno sorgere una domanda: date n variabili proposizionali e una qualsiasi tavola di verità su queste n variabili, è sempre possibile scrivere questa tavola di verità come composizione di connettivi booleani? La risposta a questa domanda è sì. Cioè $\vee$, $\wedge$, $\neg$ sono una base di connettivi. Vediamo come.

Esempio 1. Prendiamo subito come esempio il seguente connettivo ternario:

A	B	C	Ite(A, B, C)
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Cerchiamo una formula proposizionale equivalente. Riflettendoci attentamente potremmo trovare che $Ite(A, B, C)$ corrisponde al connettivo $if\ A\ then\ B\ else\ C$ che conosciamo dalla programmazione. Ma dando questo risultato non abbiamo dato una risoluzione generale e comunque aumentando il numero di variabili aumenterà anche la complicatezza della formula equivalente che otteniamo.

Sarebbe anche interessante saper trovare magari delle limitazioni per la profondità delle formule alle quali arriviamo tramite questo procedimento. Facciamo intanto alcune considerazioni:

- definiamo 'letterale' una scrittura del tipo A oppure $\neg A$, dove A è una variabile proposizionale

- data una formula proposizionale $\phi(A_1, \ldots, A_n)$ è sempre possibile portare ϕ in quella che viene chiamata NNF: nella quale il simbolo $\neg$ appare unicamente davanti a variabili proposizionali.

Facciamo ora un ragionamento che può essere facilmente riprodotto e generalizzato ad algoritmo:
$Ite(A, B, C)$ è verificata solamente per gli i valori di A, B, C che sono nella seconda, nella quarta, nella settima e nell'ottava colonna. Possiamo dunque certamente scrivere:

$$Ite(A, B, C) \equiv (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge B \wedge C)$$

Questa scrittura è meno sintetica di quella di prima, ma vi è un algoritmo preciso per trovarla. Inoltre con veloci osservazioni possiamo arrivare a dire che, ogni tavola di verità può essere scritta come formula proposizionale, in particolare è sempre possibile presentarla in due forme:

- DNF, e cioè disjunction normal form, la forma appena vista, nella quale si presenta
$$\phi \equiv \bigvee_i \bigwedge_j \psi_{i,j}$$

- CNF, e cioè conjunction normal form:
$$\phi \equiv \bigwedge_j \bigvee_i \psi_{i,j}$$
  Che si ottiene allo stesso modo della precedente, utilizzando de Morgan, a partire da $\phi = \neg\neg\phi$, abbiamo cioè che $CNF(\phi) = \neg DNF(\neg\phi)$ spingendo poi la negazione all'interno.

Questo ci dice anche che ogni formula proposizionale può essere trasformata in una formula proposizionale di profondità 2, se ammettiamo $\vee$, $\wedge$ (anche a tanti argomenti, non solo binarie).

Esempio 2. Vediamo per esempio che la formula $(A \to B) \wedge (\neg A \to C)$ può essere scritta come:

- CNF: $(\neg A \vee B) \wedge (A \vee C)$

- DNF: $(A \wedge B) \vee (\neg A \wedge C)$

Tutte e tre queste scritture sono equivalenti. Alternativamente per trovare la CNF considero i casi in cui la tavola dà il valore 0, $\phi \equiv$ non si verifica alcuno dei casi "0", etc.

Passiamo ora a definire alcuni sottoinsiemi interessanti delle formule proposizionali.

- Una formula $\phi(A_1, \dots, A_n)$ si dice 'soddisfacibile' se esiste un'assegnazione di valori di verità degli A_i che la rende vera. $SAT = \{\phi\ soddisfacibili\}$
- $TAU = \{Tautologie\}$
- Una formula ϕ si dice contraddittoria se $\neg\phi$ è una tautologia

Possiamo notare che $\phi \in TAU \leftrightarrow \neg\phi \notin SAT$

1.2 Metodo dei tableaux semantici

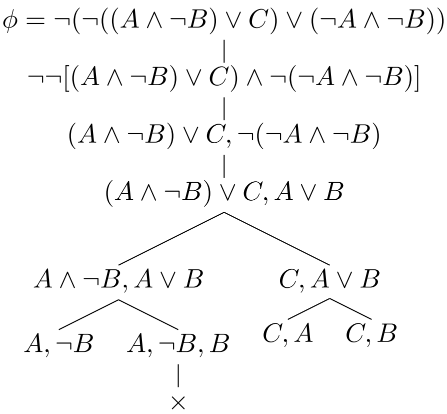
Può essere interessante studiare alberi con la seguente proprietà: ciascun nodo è un insieme di formule proposizionali (che vanno intese in congiunzione), inoltre un nodo è soddisfacibile se e solo se uno dei suoi figli è soddisfacibile. Possiamo derivarci le seguenti regole per trovare le foglie di ogni albero di questo tipo, dato il punto iniziale. Infatti sia $\psi = A \cup \{\phi\}$ (che scriveremo come A, ϕ, dove A è un insieme di formule e ϕ è una singola formula) un qualsiasi nodo, allora:

- Se siamo in NNF abbiamo:
  - se $\phi, A = \phi_1 \vee \phi_2, A$ avremo che i figli di ψ saranno ϕ_1, A e ϕ_2, A
  - se $\phi, A = \phi_1 \wedge \phi_2, A$ avremo che ψ ha un unico figlio: ϕ_1, ϕ_2, A
- Se non siamo in NNF abbiamo:
  - se $\phi, A = \neg(\neg\phi_1), A$ avremo che ψ ha un unico figlio: ϕ_1, A
  - se $\phi, A = \neg(\phi_1 \wedge \phi_2), A$ avremo che i figli di ψ saranno $\neg\phi_1, A$ e $\neg\phi_2, A$
  - se $\phi, A = \neg(\phi_1 \vee \phi_2), A$ avremo che il figlio di ψ sarà $\neg\phi_1, \neg\phi_2, A$

I tableaux ci permettono anche di scoprire se una formula proposizionale è una tautologia, infatti $\phi \in TAU$ solamente se $\neg\phi \notin SAT$, cioè se tutte le foglie del tableaux di $\neg\phi$ sono contraddittorie. Questo metodo dimostrativo è diverso da quello semantico: quello che di fatto stiamo facendo è una dimostrazione per assurdo, che lavora prettamente sulla sintassi.

Esercizio 2. Scrivere il tableaux di:

$$\phi = \neg(\neg((A \wedge \neg B) \vee C) \vee (\neg A \wedge \neg B))$$



Notiamo che i rami che contengono una formula e la sua negata sono contraddittori, per questo si chiudono.

Lezione 2

28 Settembre

Oltre ai tableaux abbiamo un altro algoritmo per la logica proposizionale: il DPLL, dai nomi di Davis–Putnam–Logemann–Loveland. Questo algoritmo consiste nel prendere una formula $\phi(A, B, \dots)$, questa risulterà vera in due soli casi:

- $A = 0$, nel qual caso equivale a $\phi(\bot, B, \dots) \wedge \neg A$
- $A = 1$, allora sarà equivalente a $\phi(\top, B, \dots) \wedge A$

Quanto detto è equivalente alla scrittura:

$$\phi(A_1, A_2, \dots, A_n) \equiv (\phi(\bot, A_2, \dots, A_n) \wedge A_1) \vee (\phi(\top, A_2, \dots, A_n) \wedge A_1)$$

Abbiamo quindi un metodo simile che ci fornisce:

$$\begin{tikzcd}[arrows=dash] & \phi(A, B, \dots) \arrow[dl] \arrow[dr] & \\ \phi(\bot, B, \dots), \neg A & & \phi(\top, B, \dots),\text{A} \end{tikzcd}$$

Il vantaggio di questa scrittura è che può essere facilmente semplificata, infatti, qualsiasi sia il valore di A, abbiamo:

- $\bot \wedge A = \bot$
- $\bot \vee A = A$
- $\top \wedge A = A$
- $\top \vee A = \top$

2.1 Quantificatori

Le cose diventano più complicate dopo l'introduzione dei quantificatori, infatti non è semplice dire quando una proposizione contenente quantificatori è vera. Vediamo intanto se è possibile esaminare casi generici, come abbiamo appena fatto per le formule proposizionali, vediamo cioè se è possibile trovare delle formule che risulatno sempre vere o sempre false, indipendentemente dal significato dei simboli di predicato.

Esempio 3. - $\exists y \forall x P(x,y) \rightarrow \forall x \exists y P(x,y)$ è una verità logica, diremo quindi che è una 'formula valida'. Cioè è vera indipendentemente dal significato di $P(x,y)$.

- $\neg\exists x\ P(x) \rightarrow \forall x \neg P(x)$ è un'altra formula valida.
- $\neg\forall x\ P(x) \rightarrow \exists x \neg P(x)$ è anch'essa valida.

Vorremmo riuscire a estendere i tableaux anche ai quantificatori, vorremmo cioè trovare un modo per semplificare le formule contenenti quantificatori, magari per individuare facilmente quali formule sono soddisfacibili e quali no. Possiamo intanto fare un primo passo, in analogia con le regole di de Morgan, e renderci conto che valgono:

- $\neg\forall x\ P(x) \equiv \exists x\ \neg P(x)$
- $\neg\exists x\ P(x) \equiv \forall x\ \neg P(x)$

Ma non è facile continuare. Vediamo intanto della nomenclatura: indicheremo con $P(x,y,\dots)$ i predicati, all'interno dei predicati i termini $x,y,\dots$ sono detti variabili. Abbiamo quindi una prima idea di cosa sia un linguaggio: un insieme $\mathscr{L} = \{P, Q, \dots, a, b, \dots\}$ nel quale P, Q sono simboli di predicato con arietà assegnate, mentre invece $a, b, \dots$ sono simboli di costante. Diciamo che una struttura per il linguaggio $\mathscr{L}$ è un dominio non vuoto M in cui interpretiamo i simboli del linguaggio, a questo punto avremo che P_M verrà vista come un sottoinsieme di M mentre invece $Q_M \subseteq M^2$, diamo cioè a ogni predicato un'interpretazione come sottoinsieme.

Esercizio 3. Consideriamo ad esempio il linguaggio:

$$\mathscr{L} = \{P(x,y,z), A(x,y,z), a, b, O(x,y), U(x,y)\}$$

E la seguente struttura M:

- $dom(M) = \mathbb{N}$ che chiameremo spesso per semplicità M.
- $P_M(x,y,z) \leftrightarrow (x,y,z) \in P^M \leftrightarrow x \cdot y = z$
- $O_M(x,y) \leftrightarrow (x,y) \in O^M \leftrightarrow x \leq y$
- $U_M(x,y) \leftrightarrow (x,y) \in U^M \leftrightarrow x \leq y \wedge y \leq x$
- $a_M = 0$ e $b_M = 1$

Un utile esercizio è scrivere la congettura di Goldbach utilizzando solamente il linguaggio $\mathscr{L}$ e la struttura che abbiamo introdotto. Facciamo dei passi intermedi:

- Possiamo scrivere 'x è primo' come: $\forall u, v\ P_M(u,v,x) \rightarrow U_M(b_M, v) \vee U_M(b_M, u)$
- Possiamo scrivere 'x è pari' come: $\exists u\ A(u,u,x)$
- Componendo adeguatamente queste due scritture possiamo facilmente arrivare a scrivere la congettura di Goldbach completa.

Continuiamo ora a cercare una formula per i tableaux quando sono presenti i quantificatori. La cosa non è facile soprattutto se vogliamo mantenere tutte le caratteristiche dei tableaux proposizionali. Iniziamo quindi riflettendo sul significato che attribuiamo normalmente ai simboli $\forall$ e $\exists$ e supponiamo di avere Σ, un insieme di formule e anche la formula ϕ. Vediamo allora che:

- scrivendo $\Sigma, \forall x\ \phi(x)$ quello che vogliamo indicare è che la probrietà vale per ogni x nel dominio che stiamo considerando. Dunque se volessimo un'equivalenza nel tableaux tra padre e figli avremmo potenzialmente un nodo con un numero non finito di figli, e questo vorremmo evitarlo. Inoltre vogliamo dare regole che non dipendono dal dominio e dall'interpretazione dei simboli non logici. Possiamo però fare un primo passo e sostituire $\Sigma, \forall x\ \phi(x)$ con $\Sigma, \phi(a), \forall x\ \phi(x)$, visto che certamente se ϕ deve valere per ogni elemento deve valere anche per uno specifico a. In particolare scegliendo come a una costante che magari già appare in Σ è più facile trovare contraddizioni e quindi determinare la insoddisfacibilità del nodo iniziale.
- Se invece siamo di fronte a un nodo del tipo $\Sigma, \exists x\ \phi(x)$ quello che possiamo fare è nominare l'elemento che soddisfa ϕ, infatti $\exists x\ \phi(x)$ equivale alla possibilità di nominare un a per cui valga $\phi(a)$. In questo caso, al contrario di prima, occorre scegliere un simbolo non ancora apparso in Σ, per non rischiare di rendere falso il nodo (se abbiamo già fissato a la proposizione ϕ potrebbe essere vera per un a diversa).

Chiaramente oltre a queste trasformazioni consideriamo anche le equivalenze che ci sono date dalle 'leggi di De Morgan' modificate per quantificatori.

Esempio 4. Cerchiamo di capire se è valida:

$$\phi(x) = \neg\forall x\ P(x) \to \exists x\ \neg P(x)$$

Anzi che fare il suo tableaux direttamente, facciamo quello della sua negazione (e chiaramente poi invertiremo il risultato). Abbiamo quindi:

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

Che è una contraddizione, abbiamo quindi che ϕ è valida.

Esempio 5. Cerchiamo di fare la stessa cosa con $\phi = \exists x(P(x) \to \forall y\ P(y))$. Questa sembra non valida, e in effetti sembra quasi contraddittoria. Ma vediamo che invece è valida. Costruiamo come prima il tableaux di $\neg\phi$.

$$\begin{array}{c}
\neg(\exists x(P(x) \to \forall y\ P(y))) \\
| \\
\forall x \neg(P(x) \to \forall y\ P(y)) \\
| \\
\forall x\ (P(x) \wedge \neg(\forall y\ P(y))) \\
| \\
\forall x\ (P(x) \wedge (\exists y\ \neg P(y)))
\end{array}$$

Lezione 3

2 Ottobre

Ritorniamo con più formalità su alcuni punti visti durante la scorsa lezione.

Definizione 1. Diciamo linguaggio di primo ordine un insieme $\mathscr{L}$ costituito da simboli di tre tipologie: simboli di costante, di funzione e di predicato. Dunque

$$\mathscr{L} = \{c_i\} \cup \{f_j\} \cup \{p_k\}$$

A ciascuno di questi simboli è associata un'arietà, ovvero un numero, che indica il numero degli argomenti (nel caso delle costanti l'arietà è 0) e che fa implicitamente parte del linguaggio. Oltre al linguaggio supponiamo anche di avere un insieme di variabili $V = \{x_1, x_1, \dots\}$ e i connettivi $\{\neg, \wedge, \vee, \rightarrow, \exists, \forall\}$ e "=".
Una $\mathscr{L}$ struttura M è un'insieme formato da:

- $dom(M)$ un dominio, che spesso chiameremo M.
- interpretazione dei simboli. Interpreteremo quindi per esempio un predicato P di arietà n come un sottoinsieme P_M di M^n, oppure una funzione da M^n in $\{0, 1\}$ (la corrispondenza è data dalla funzione caratteristica).

Possiamo quindi decidere noi che significato dare ai vari simboli. Decidiamo però di interpretare sempre i connettivi booleani secondo le tavole di verità, e i quantificatori secondo le idee della logica classica. (sarebbe da aprire una parentesi sul simbolo =, ma questo non lo consideriamo come parte del linquaggio, infatti in $\mathscr{L}$ mettiamo solo cose che possiamo interpretare a nostro piacimento).

Questa definizione e l'ultima considerazione ci fa capire che vi è un problema, infatti abbiamo detto che il simbolo = non entra a tutti gli effetti a far parte del linguaggio, visto che non può essere interpretato a piacere. Ma siamo abituati a definire le funzioni tramite uguaglianza (per esempio $y = f(x, z)$), ci mettiamo dunque in un caso particolare: linguaggi senza funzioni e senza =, cioè in un linguaggio puramente predicativo. Notiamo che questo non è una restrizione, infatti ogni funzione $\phi : A \longrightarrow B$ può essere vista come sottoinsieme di $A \times B$ e quindi come predicato.

Esempio 6. Consideriamo il linguaggio $\mathscr{L} = \{0, 1, +, \cdot, <\}$, che conosciamo dalla teoria dei campi. Una sua struttura sarà ad esempio:

$$M = (\mathbb{R},\ 0^{\mathbb{R}},\ 1^{\mathbb{R}},\ +^{\mathbb{R}},\ \cdot^{\mathbb{R}},\ <^{\mathbb{R}})$$

Con i significati che conosciamo.

Definizione 2. Sia $\mathscr{L}$ un linguaggio. Definiamo $T - \mathscr{L} = V \cup \{Costanti\}$ l'insieme degli $\mathscr{L}$ termini, inoltre diciamo formula atomica una scrittura del tipo $P(t_1, \ldots, t_n)$ con $t_i \in T - \mathscr{L}$. A questo punto possiamo definire per induzione una $\mathscr{L}$ formula, ossia:

$$\phi ::= Atomica|(\phi_1 \wedge \phi_2)|(\phi_1 \vee \phi_2)|\neg\phi|\exists x\phi(x)|\forall x\phi(x)$$

Scrittura che vuole intendere che si dice $\mathscr{L}$ formula o una formula atomica, o una scrittura che è del tipo sopra indicato, con ϕ_1, ϕ_2, ϕ a loro volta formule. L'insieme delle $\mathscr{L}$ formule è il più piccolo insieme che contiene tutte le scritture di questo genere.

Possiamo notare che la logica proposizionale che abbiamo visto le scorse lezioni è contenuta in questa formulazione predicativa, infatti le proposizioni che abbiamo considerato possono essere viste come predicati di arietà 0.
Notiamo inoltre che le parentesi che sono state messe non sono facoltative, infatti garantiscono la non ambiguità della scrittura.

Esercizio 4. Provare a scrivere una grammatica non ambigua che impieghi meno parentesi di quelle usate da quella standard.
Una possibile soluzione è la cosiddetta notazione polacca, che sostituisce $\phi \wedge \psi$ con $\wedge\phi\psi$ e mette $\vee\psi\phi$ al posto di $\psi \vee \phi$.

Chiaramente questi problemi sono puramente sintattici: non riguardano il significato che noi andremo a dare al linguaggio nella struttura. Abbiamo quindi finora studiato la sintassi: abbiamo definito linguaggi e formule; ma siamo interessati anche all'aspetto semantico di quanto facciamo: al significato che viene dato alle cose. In particolare vogliamo saper dire per esempio se una $\mathscr{L}$ formula è vera o falsa in una $\mathscr{L}$ struttura. Ma fino ad ora non abbiamo nemmeno detto cosa significa che una formula è vera o falsa in una struttura.

3.1 Semantica di Tarski

Ci chiediamo dunque se, dato il linguaggio dei campi già introdotto (con il suo modello) vale ad esempio $<(0, 1)$. Secondo Tarski abbiamo che $M \vDash \phi \leftrightarrow (0^{\mathbb{R}}, 1^{\mathbb{R}}) \in <^{\mathbb{R}}$. Abbiamo quindi un'interpretazione che sembra banale, ma che era necessario dare. In particolare useremo le scritture $M \vDash \phi, M \nvDash \phi$ per dire che ϕ è vera o falsa in M.
Quello che stiamo facendo è trasformare una formula, cioè una stringa di simboli sintatticamente senza significato, in un'affermazione che può essere vera o falsa. Quello che vogliamo fare dunque è estendere quanto abbiamo visto a un caso più generale e riuscire a dare significato semantico a tutte le formule.
Proviamo a esemplificare quanto detto: se noi scriviamo 'la neve è bianca', quello che intendiamo è una variabile, un nome senza significato, privato del suo senso semantico, stiamo semplicemente considerando una stringa. Al contrario scrivendo: "la neve è bianca", quello che intendiamo dire è una proposizione, che è solo incidentalmente indicata da quelle parole. Abbiamo dunque:

'La neve è bianca' è vero $\leftrightarrow$ La neve è bianca

Quindi da una parte abbiamo una stringa, a cui attribuiamo il valore vero solo nel caso in cui la proposizione che indica è vera. Possiamo quindi dire che la verità è l'inversione delle virgolette.
Abbiamo anche un'altra possibile interpretazione della veridicità dei predicati, infatti avevamo già detto che questi possono essere interpretati come applicazioni da M^n in $\{0,1\}$. In questo caso è ovvia la semantica, inoltre questo ci permette di dare altre definizioni.

Osservazione 2. Possiamo definire quanto fatto fino ad ora in modo diverso, infatti possiamo introdurre una funzione $v_M : Formule \longrightarrow \{0,1\}$, in particolare allora potremmo dire che $M \vDash \phi \leftrightarrow v_M(\phi) = 1$, e $M \nvDash \phi$ nell'altro caso. Questa scrittura ci permette di dare significati di verità a tutte le formule, sapendo i valori delle sottoformule che le compongono. Ci sarebbe quindi sufficiente saper il valore di verità delle formule atomiche (che però ci è dato dall'interpretazione dei predicati nella struttura) e dei modi per calcolare facilmente il valore di verità di sovraformule, e ci è sufficiente fare questo per le strutture che abbiamo usato per definire induttivamente le $\mathscr{L}$ formule. Abbiamo quindi:

- $v_M(\phi_1 \wedge \phi_2) = min(v_M(\phi_1), v_M(\phi_2))$
- $v_M(\phi_1 \vee \phi_2) = max(v_M(\phi_1), v_M(\phi_2))$
- $v_M(\neg\phi) = 1 - v_M(\phi)$

Più delicati sono i quantificatori. Abbiamo comunque delle regole generali (anche se per ora solo parziali) di derivazione della verità delle $\mathscr{L}$ formule dalla conoscenza della verità delle formule atomiche, ma questa informazione ci è data dalla struttura, che rappresenta quindi la situazione particolare in cui ci troviamo. Vediamo il problema dei quantificatori con un esempio.

Esempio 7. Sia $\mathscr{L} = \{<\}$ e $M = \left\{\mathbb{R}, <^{\mathbb{R}}\right\}$. Sia inoltre $\phi = \forall x \exists y (x < y)$. Possiamo dire che $M \vDash \phi$? E in generale come facciamo a dire se è vero?
Potremmo provare un approccio induttivo, si potrebbe infatti vedere $\forall x\ P(x)$ come un minimo su infiniti termini (e questo corrisponderebbe alla visione del $\forall$ come un $\wedge$ con infiniti termini). Ma il problema che abbiamo è che in generale abbiamo delle variabili libere che non sappiamo come gestire, se cioè definiamo

$$v_{\mathbb{R}}(\forall x\ \psi) = \min_a v_{\mathbb{R}}(\psi[a/x])$$

abbiamo che $\psi[a/x]$ non è una formula, proprio perché abbiamo variabili libere.

In realtà c'è una soluzione piuttosto semplice, infatti la funzione v_M prende due input: la formula ϕ e un'assegnazione, cioè una scrittura del tipo $[a_1/x_1, \dots, a_n/x_n]$, dove $a_i \in M$. Abbiamo quindi a questo punto delle formule con variabili liber e un'assegnazione e, e di queste possiamo facilmente calcolare la verità.
Diciamo quindi assegnazione una funzione $s : Variabili \longrightarrow M$ e possiamo a questo punto creare un'altra funzione:

$$v_M : Formule \times Assegnazioni \longrightarrow \{0,1\}$$

Introduciamo un'altra scrittura: se s è un'assegnazione, scriviamo $s[a/x]$ per indicare un'assegnazione ottenuta da s modificando solamente il valore di x dal suo valore precedente ad a. Possiamo a questo punto definire:

- $v_M(\exists x\ \phi(x), s) = max_{a\in M} v_M(\phi, s[a/x])$
- $v_M(\forall x\ \phi(x), s) = min_{a\in M} v_M(\phi, s[a/x])$

Esempio 8. Secondo quanto appena detto:

$$v_{\mathbb{R}}(\exists x\ (y = x\cdot x), [2/y, 3/x, 0/z, \dots]) = max_{a\in\mathbb{R}} v_{\mathbb{R}}(y = x\cdot x, [2/y, a/x, 0/z, \dots])$$

Che sappiamo essere 1 per $a = \sqrt{2}$.

Come versione alternativa potremmo dire che $M \vDash \phi_1 \wedge \phi_2\ s$ solo nel caso in cui $M \vDash \phi_1(s) \wedge M \vDash \phi_2(s)$, oppure potremmo sostituire il minimo e il massimo appena visti con 'per ogni' e 'esiste'. Anche se in realtà questo ci sembra fittizio è interessante notare che le definizioni appena date, per quanto apparentemente fondate logicamente, presentano un problema: abbiamo definito i $\forall$ e $\exists$ a partire dal concetto di *min* e *max*, ma questi concetti a loro volta non esistono senza la definizione di $\forall$ ed $\exists$, abbiamo quindi solamente spostato il problema, visto che abbiamo usato strumenti che comunque non abbiamo definito a partire dal nulla.

Ci resta da fare un'interpretazione esplicita delle formule atomiche. Diremo che $M \vDash P(x_1, \dots, x_n)(s)$ nel caso ovvio in cui i valori dell'assegnazione appartengono all'insieme che è definito nella struttura come interpretazione di P.

Definizione 3. Ci sarà anche utile definire gli $\mathscr{L}$ termini (che potrebbero essere contenuti in formule atomiche). Anche questa definizione la faremo induttivamente:

$$\mathscr{L}\ termine ::= Variabile|costante|f(t_1, \dots, t_n)$$

dove f è una funzione e i t_i sono sottotermini. Inoltre definiamo induttivamente $t^M(s)$, se s è un'assegnazione, come:

- $cost^M(s) = cost^M$
- $var^M(s) = s(var)$
- $f(t_1, \dots, t_n)^M(s) = f^M(t_1^M(s), \dots, t_n^M(s))$

Per quanto riguarda le formule atomiche, semplicemente diciamo che $M \vDash P(t_1, \dots, t_n)(s)$ se e solo se $(t_1^M(s), \dots, t_n^M(s)) \in P^M$.

Lezione 4

5 Ottobre

Abbiamo visto la semantica di Tarski e i tableaux. Adesso vorremmo metterle in rapporto, ma i tableaux sono puramente sintattici, mentre la semantica cerca di mettere in relazione formule e strutture. Compito della semantica è dirci quando una formula vale in un modello: quando un modello M rende vera una formula, e da questo si può generare valori di verità per ogni formula.

Definizione 4. Introduciamo ora un altro concetto per induzione, quello di variabile libera. Data una formula ϕ, si indicano con $VL(\phi)$ le sue variabili libere. In particolare abbiamo:

- $VL(\phi) = \{\textit{tutte le variabili che compaiono}\}$ se ϕ è atomica.
- $VL(\forall x \phi) = VL(\phi) - \{x\}$
- $VL(\exists x p) = VL(\phi) - \{x\}$
- $VL(\phi \land \psi) = VL(\phi) \cup VL(\psi)$
- $VL(\phi \lor \psi) = VL(\phi) \cup VL(\psi)$

Esempio 9. Una variabile può apparire in una formula sia libera che legata. Se per esempio abbiamo:

$$VL[(\forall x(x > y) \land (x > 0)) = \{y, x\}]$$

In questa formula, che notiamo essere ammessa nell'insieme delle formule secondo le nostre definizioni, abbiamo che la x appare sia come variabile libera che come variabile legata allora quello che possiamo fare è distinguere più occorrenze. Possiamo dire quindi che la prima volta la x occorre come variabile legata, la seconda è un'occorrenza libera.

Esercizio 5. Il valore di una formula nella struttura M e nella assegnazione s dipende solo da s ristretto alle variabili libere. Ossia $v_M(\phi)(s)$ dipende unicamente da $s \restriction_{VL(\phi)}$. Ossia se s coincide con s' sulle variabili libere abbiamo $v_M(\phi)(s) = v_M(\phi)(s')$.
Si dimostra per induzione sulla complessità di ϕ.

Se ϕ è chiusa, ossia senza variabili libere, allora il valore di ϕ non dipende da s, quindi possiamo semplicemente scrivere $M \vDash \phi$, in realtà è comunque necessario utilizzare formalmente un'assegnazione, ma il risultato non è dipendente dalla scelta dell'assegnazione. Ricordiamo una cosa detta la scorsa lezione:

- $v_M(x)(s) = s(x) \in M$, se x è una variabile.
- $v_M(c)(s) = c^M \in M$ se c è una costante.
- $v_M(f(t_1, \ldots, t_n))(s) = f^M(v_M(t_1)(s), \ldots, v_M(t_n)(s)) \in M$

Prima di passare al prossimo esercizio precisiamo quanto detto le scorse lezioni circa l'uguaglianza. Sia $\mathscr{L}$ un linguaggio fissato; abbiamo detto che, oltre ai simboli definiti esplicitamente in $\mathscr{L}$ noi consideriamo definito anche il simbolo $=$, che sta ad indicare un predicato di arietà 2. Abbiamo in particolare che $M \vDash t_1 = t_2(s)$ se e solo se $v_M(t_1)(s) = v_M(t_2)(s)$, dove il secondo uguale è un uguale semantico, mentre il primo è puramente sintattico. Formalmente potremmo introdurre l'uguale come la relazione determinata dalla diagonale del prodotto $M \times M$, cioè diciamo che $a_1 = a_2$ (elementi del dominio M) se $(a_1, a_2) \in \Delta_M$, la diagonale appena citata.
Inoltre ricordiamo che, in generale, diciamo che $M \vDash P_1(t_1, \ldots, t_n)(s)$ se e solo se $< t_1^M(s), \ldots, t_n^M(s) > \in P^M$.

Esercizio 6. $\mathscr{L} = \{0, 1, +, \cdot\}$ e $M = \mathbb{Z}/1000\mathbb{Z}$, con $0^M = [0]_{1000}$, $1^M = [1]_{1000}$, e le operazioni del gruppo.
Ci chiediamo se esiste un algoritmo che, data una formula ϕ chiusa, determina se $\mathbb{Z}/1000\mathbb{Z} \vDash \phi$.
La risposta è che sì, esiste, visto che il dominio è finito. Posso trasformare la formula in una formula proposizionale. Infatti sappiamo che è possibile convertire i $\forall$ e gli $\exists$ con $\wedge$ e $\vee$, se il numero di casi è finito. L'algoritmo a partire dall'interno e andando verso l'esterno, consiste nel trasformare i $\exists x \psi x$ in $\bigvee_a \psi(a)$ e i $\forall a \psi(a)$ vengono trasformati in $\bigwedge_a \psi(a)$.

Ma quanto tutto questo può essere generalizzato? Vediamo che:

Teorema 1. *Sia $\mathscr{L} = \{0, 1, +, \cdot\}$, con le interpretazioni naturali su $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}/1000\mathbb{Z}$. Al contrario di quanto si potrebbe immaginare abbiamo che, tranne per $\mathbb{Z}$ e per $\mathbb{Q}$ è possibile trovare un algoritmo che ci dica se le formule sono valide o no. Cioè paradossalmente i reali e complessi sono più facili dei razionali e di $\mathbb{Z}$.*

Che non è possibile trovare un algoritmo risolutivo per le formule in $\mathbb{Z}$ lo dimostrò Godel nel 1931; che si potesse in $\mathbb{R}$ e $\mathbb{C}$ lo dimostrò Tarski. In $\mathbb{Q}$ lo dimostrò Julia Robinson. L'idea che sta dietro a questo risultato apparentemente strano è che $R \vDash \phi$ se e solo se $Assiomi \vDash \phi$, dove chiaramente sarebbe da definire cosa intendiamo per assiomi. Il problema di rendere esplicite queste cose ora è che per dare per esempio l'assioma di completezza, dovremmo utilizzare della sintassi di secondo ordine, che però non conosciamo. Per ora abbiamo introdotto la semantica di Tarski, che ci dice che ci sono alcuni simboli, i cui significati sono dati dalle tavole, e ci dice come interpretarli; ma se noi vogliamo estendere queste cose in modo che contengano l'assioma di completezza, dobbiamo lavorare su sottoinsiemi, e quindi dovremmo introdurre dei quantificatori di second'ordine (che non trattano direttamente la struttura su cui stiamo lavorando) e il problema sorge dal fatto che non abbiamo dei tableaux che funzionano per il secondo ordine.
Il fatto che la teoria dei sottoinsiemi di $\mathbb{R}$ sia di secondo ordine in questo caso può confondere perché la teoria degli insiemi è una teoria di primo ordine, ma nella teoria degli insiemi possiamo parlare di sottoinsiemi di reali. Il fatto che

sia del primo o del secondo ordine dipende dalla struttura che prendiamo: se la struttura sono i reali quello che facciamo è quantificare sui reali, e non possiamo farlo sui loro sottoinsiemi. Se prendessimo come struttura tutti gli insiemi non sarebbe un problema.

Nei tableaux che abbiamo visto tutte le formule sono chiuse, infatti sostituiamo i $\forall$ con delle formule e dei $\forall$ e diamo nomi di costanti agli $\exists$, quindi tendiamo a rendere i quantificatori delle formule chiuse, anche se chiaramente facendo questo il linguaggio si espande. Completiamo ora i nostri tableaux con i tableaux dell'uguaglianza:

$$\begin{array}{c} \Gamma, t_1 = t_2, \phi[t_1/x] \\ | \\ \Gamma, t_1 = t_2, \phi[t_2/x], \phi[t_1/x] \end{array}$$

Vale anche

$$\begin{array}{c} \Gamma \\ | \\ \Gamma, t = t \end{array}$$

Definizione 5. Introduciamo ora l'Aritmetica di Robinson, questa è una struttura del linguaggio $\mathscr{L} = \{0, s, +, \cdot\}$ nella quale valgono gli assiomi:

Q_1 $\forall x \forall y,\ [s(x) = s(y) \implies x = y]$

Q_2 $\forall x,\ 0 \neq s(x)$

Q_3 $\forall x,\ x \neq 0 \implies \exists y\ t.c.\ x = s(y)$

Q_4 $\forall x,\ x + 0 = x$

Q_5 $\forall x \forall y,\ x + s(y) = s(x + y)$

Q_6 $\forall x,\ x \cdot 0 = 0$

Q_7 $\forall x \forall y,\ x \cdot s(y) = x \cdot y + x$

Esempio 10. Proviamo a dimostrare che $2 \cdot 2 \neq 3$ nell'Aritmetica di Robinson. Per praticità (sarà già abbastanza complicato così) scriveremo $2 = s(s(0))$ e $3 = s(2)$. Procediamo per assurdo come al solito:

$$
\begin{array}{c}
Q, \neg(2 \cdot 2 \neq 3) \\
| \\
Q, 2 \cdot 2 = 3 \\
| \\
Q, Q_7, \forall y 2 \cdot s(y) = 2 \cdot y + 2, \quad 2 \cdot 2 = 3 \\
| \\
Q, Q_7, 2 \cdot s(1) = 2 \cdot 1 + 2, \quad 2 \cdot 2 = 3 \\
| \\
Q, Q_7, 2 \cdot s(1) = (2 \cdot 0 + 2) + 2, \quad 2 \cdot 2 = 3 \\
| \\
Q, Q_7, 2 \cdot s(1) = (0 + s(s(0))) + 2, \quad 2 \cdot 2 = 3 \\
| \\
Q, Q_7, 2 \cdot s(1) = (s(0) + s(0)) + 2, \quad 2 \cdot 2 = 3 \\
| \\
Q, Q_7, 2 \cdot s(1) = s(s(0)) + s(s(0)), \quad 2 \cdot 2 = 3 \\
| \\
Q, Q_1, Q_7, 2 \cdot 2 = s(s(s(s(0)))), \quad 2 \cdot 2 = 3 \\
| \\
\text{Assurdo}
\end{array}
$$

Lezione 5

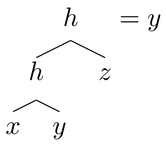
9 Ottobre

Esercizio 7. Sia h una funzione. Si dimostri che vale:

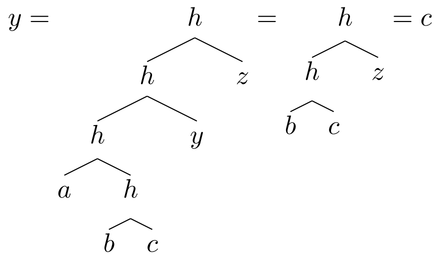
$$(\forall x, y, z \; h(h(x, y), z) = y) \longrightarrow \forall x, y \; x = y$$

Dimostrazione. Vediamo due diverse dimostrazioni:

- Dimostrazione semantica; per semplicità di notazione rappresentiamo la funzione come alberi in maniera piuttosto intuitiva. Riscriviamo le ipotesi come:



  E prendiamo un caso particolare, visto che il tutto vale $\forall x, y, z$:



  Visto che tutte le variabili sono generiche possiamo dire che $\forall c, y \; y = c$.

- Dimostrazione sintattica, tramite i tableaux.

$$\begin{array}{c} \neg\phi \\ | \\ \forall x, y, z \; h(h(x, y), z) = y, \;\; \neg\forall x, y \; x = y \\ | \\ \forall x, y, z \; a = h(h(h(x, h(y, b)), a), z) = h(h(y, b), z) = b, \;\; a \neq b \end{array}$$

Definizione 6. Sia $\mathscr{L} = \{c_i, f_j, p_k\}$ un linguaggio, una $\mathscr{L}$-teoria è un insieme Γ, anche vuoto, di $\mathscr{L}$ enunciati; le formule appartenenti a Γ sono dette assiomi. Un modello di una $\mathscr{L}$-teoria Γ è un'interpretazione di $\mathscr{L}$ che rende vere tutte le formule di Γ.

Riflessione 2. Sorge a questo punto un problema: supponiamo di avere $\mathscr{L}$ un linguaggio e Γ una $\mathscr{L}$-teoria. Vorremmo poter dire se una data formula ϕ segue dalla teoria che abbiamo costruito, ma con gli strumenti che abbiamo costruito potremmo dare due differenti definizioni, scriveremo infatti:

- $\Gamma \vDash \phi$ se ogni modello che soddisfa Γ soddisfa anche ϕ.
- $\Gamma \vdash \phi$ se il tableaux di $\neg\phi$ è chiuso, cioè se ϕ segue sintatticamente da Γ.

Teorema 2. *Sia $\mathscr{L}$ un linguaggio e T una $\mathscr{L}$-teoria. Abbiamo:*

$$T \vdash \phi \longleftrightarrow T \vDash \phi$$

Questo teorema è in realtà l'unione di due teoremi:

$\rightarrow$ *è detto teorema di correttezza. Dice che ogni formula che è dimostrabile tramite tableaux è soddisfatta da ogni modello della teoria.*

$\leftarrow$ *è detto teorema di completezza. Ci dice che ogni formula che è soddisfatta da ogni modello della teoria segue anche dai tableaux.*

Il termine completezza è usato anche per indicare un concetto totalmente diverso:

Definizione 7. Un insieme T di assiomi si dice completo se $\forall\phi$ enunciato si ha $T \vDash \phi \vee T \vDash \neg\phi$.
T si dice semanticamente coerente se ha almeno un modello; si dice sintatticamente coerente se $T \nvdash \perp$.

Osservazione 3. Se T è coerente non può dimostrare A e $\neg A$.
Dire $T \vDash (A \vee \neg A)$ è completamente diverso da dire $T \vDash A \vee T \vDash \neg A$ (il primo dei due è sempre vero, mentre è possibile che esista una formula verificata in alcuni modelli della teoria e non in altri).

Osservazione 4. Abbiamo che valgono le seguenti equivalenze:
Non esiste una dimostrazione sintattica per $\phi \longleftrightarrow T \nvdash \phi \longleftrightarrow T \nvDash \phi \longleftrightarrow Mod_{\mathscr{L}}(T) \supsetneq Mod_{\mathscr{L}}(T, \phi) \longleftrightarrow \exists M(M \vDash T \text{ e } M \nvDash \phi)$. Infatti $T \vDash \phi \longleftrightarrow Mod_{\mathscr{L}}(T) \supseteq Mod_{\mathscr{L}}(\phi, T)$

Esempio 11. Abbiamo visto la scorsa lezione Q: l'insieme degli assiomi dell'aritmetica. Mostriamo che Q non è un insieme completo di assiomi; consideriamo infatti $\phi(x) = x$ *è pari* $\vee\, x$ *è dispari*. Dobbiamo ben definire parità, infatti se definissimo i numeri dispari come 'i numeri non pari' avremmo chiaramente che ogni modello di Q soddisfa ϕ, infatti abbiamo sempre che $\vDash A \vee \neg A$. Diciamo quindi:

- x si dice pari se $\exists y$ tale che $x = y + y$.
- x si dice dispari se $\exists y$ tale che $x = y + y + 1$.

Possiamo certamente dire che $Q \nvDash \neg\phi$, infatti conosciamo un modello in cui ϕ é vera. Vogliamo però dimostrare che $Q \nvDash \phi$, quindi esiste un modello in cui vi sono elementi non pari nè dispari. Prendiamo come controesempio l'insieme K dei polinomi con il coefficiente di termine massimo positivo, unito lo 0, cioè:

$$K = \{0\} \cup \left\{ \sum_{i=0}^{n} a_i t^i \ t.c. \ a_n > 0 \right\}$$

Vediamo che ϕ non è verificata in questo modello, e che K è in effetti un modello di Q. La verifica che Q sia un modello di Q è piuttosto immediata, infatti 0 è l'unico elemento a non avere un predecessore, e la somma rispetta gli assiomi. Possiamo però notare che t non è né pari né dispari.

Riflessione 3. Abbiamo dimostrato quindi che non si può dimostrare semanticamente ϕ, visto che esistono sia modelli che la verificano sia modelli che verificano $\neg\phi$, da questo segue che ϕ non si dimostra con i tableaux (per il teorema di correttezza, infatti se si dimostrasse con i tableaux non avremmo un contromodello).
Possiamo quindi dire che Q è incompleta, potremmo allora voler aggiungere alcuni assiomi per completarla: vorremmo poter arrivare a una teoria completa, contenente Q, della quale $\mathbb{N}$ sia ancora un modello. Eiste un modo molto veloce per completarla, infatti potremmo definire $Th(N) = \{\phi \ t.c. \ \mathbb{N} \vDash \phi\}$, cioè l'insieme degli enunciati veri in $\mathbb{N}$, questa teoria ha il vantaggio di essere completa, ma ha l'enorme svantaggio che non conosciamo esplicitamente i suoi elementi, viene chiamata teoria completa di $\mathbb{N}$.
Lasciamo quindi questa strada e proviamo a introdurre altri assiomi. Ci piacerebbe aggiungere l'induzione:

$$\forall P(P(0) \wedge \forall x(P(x) \longrightarrow P(s(x)))) \longrightarrow \forall y P(y)$$

Se infatti aggiungessimo questo asisoma la teoria sarebbe completa, in quanto, a meno di isomorfismi, ha un unico modello (i numeri naturali, in questo caso si dice che la teoria è categorica: ammette un solo modello); ma questo assioma ha un problema a livello sintattico, infatti non abbiamo tableaux per quantificatori su predicati, che fanno parte della logica del secondo ordine. Abbiamo quindi che per rendere completo Q dovremmo aggiungere un assioma del secondo ordine, ma così facendo non saremmo più in grado di lavorare tramite tableaux, o comunque non con i tableaux che conosciamo. Dunque per avere un Q completo dovremmo introdurre una semantica di Tarski per il secondo ordine e delle regole di tableaux. Per quanto riguarda la semantica possiamo immaginarla senza troppa difficoltà, avremo infatti, per esempio, che:

$$M \vDash (\forall^{(2)} P^{(1)} \phi)(s) \longleftrightarrow \forall A \subseteq M, \ M \vDash \phi(s[A/P])$$

Dove con $^{(p)}$ intendiamo che l'espressione in questione é del p-esimo ordine, il problema dunque non è nella semantica, è nei tableaux: non conosciamo regole per questo tipo di $\forall$.

Esercizio 8. Trovare tableaux per i $\forall$ del secondo ordine. Ci può aiutare il ricordarci come funzionavano i tableaux per i quantificatori per il primo ordine: si sotituiva $\forall x \phi$ con $\forall x \phi, \phi(t/x)$. Possiamo fare qualcosa di simile in questo caso e sostituire a $\forall^{(2)} P \phi$ con $\forall^{(2)} P \phi, \phi[P := \psi]$ dove ψ è una qualsiasi proposizione, come potrebbe esserlo x è pari.

Abbiamo già detto che se ammettiamo di avere l'induzione e quindi i quantificatori del seonco ordine, quello che possiamo fare è ottenere una teoria completa (in particolare una teoria con un solo moodello, a meno di isomorfismi), allora in particolare possiamo dimostrare sintatticamente che $\phi(x) \equiv \exists y, \ x = y + y \vee x = y + y + 1$ segue da Q + *Induzione* (tramite una banale dimostrazione per induzione).

Abbiamo quindi che introdurre i quantificatori di secondo ordine apparentemente risolve tutti i nostri problemi, ma così non è, infatti non è possibile avere una teoria completa per il secondo ordine; il problema è dato dal fatto che nei tableaux del primo ordine i nodi figli non erano mai più complicati dei padri, infatti nel caso degli esiste quello che si faceva era assegnare dei nomi di costante alle variabili legate dagli esiste, e i $\forall$ si istanziavano, mentre per i quantificatori del secondo ordine questo non avviene, infatti istanziando un $\forall^{(2)}P$ possiamo ottenere formule complicate a piacere, quindi i tableaux tendono a non chiudersi, infatti mentre i termini al posto delle variabili fanno diminuire il numero di quantificatori, nel secondo ordine non diminuisce nulla. Questa situazione si dice impredicativa, ed è quella che crea problemi al teorema di completezza.

Quello che possiamo fare è arrivare arrivare a un compromesso per espandere Q: non lo allarghiamo con l'induzione del secondo ordine, ma creiamo una specie di induzione parziale, introduciamo cioè uno schema infinito di assiomi: per ogni formula ϕ introduciamo l'assioma $Ax_{\phi(x)}$ che ci dice che vale l'induzione per ϕ, cioè

$$Ax_{\phi(x)} \equiv \phi(0) \wedge \forall x(\phi(x) \longrightarrow \phi(s(x))) \longrightarrow \forall y\ \phi(y)$$

Assiomi che possiamo definire unicamente tramite il linguaggio del primo ordine. Chiamiamo questa teoria $PA^{(1)}$. Vediamo che anche con questa forma modificata possiamo dire che vale $\phi(x) \equiv \exists y,\ x = y + y \vee x = y + y + 1$. Sorge a questo punto la domanda: $PA^{(1)}$ è completa? No.

Lezione 6

12 Ottobre

Abbiamo visto che l'aritmetica di Robinson Q senza l'induzione è molto debole, facciamo quindi riferimento per i naturali agli assiomi di Peano, che abbiamo visto esistere in due forme; la prima, quella pensata da Peano, è quella contenente l'induzione (che però è un enunciato del secondo ordine, con tutti i problemi che abbiamo visto conseguire), la seconda è formata da un insieme infinito di assiomi e quindi non è possibile scriverla esplicitamente. Questa seconda è una sorta di compromesso: infatti mettiamo un insieme infinito di assiomi del primo ordine anzi che un unico assioma del secondo ordine, che semplificherebbe infinitamente la notazione però renderebbe impossibile lavorare con i tableaux. Abbiamo quindi che $PA = Q \cup \{Ax_\phi\}$ dove ϕ varia all'interno di tutte le formule possibili e Ax_ϕ è l'assioma del primo ordine che abbiamo visto la scorsa lezione (l'induzione ristretta alla fomula ϕ). Questo ci consente di assiomatizzare $\mathbb{N}$ senza usare la teoria completa, che ha il vantaggio di essere semplice e completa, ma di contro non conosciamo quali siano i suoi assiomi.

Esercizio 9. L'aritmetica di peano del primo ordine dimostra che tutti i numeri naturali sono pari o dispari.

Riflessione 4. Torniamo al problema di completezza e correttezza; abbiamo visto che nel caso proposizionale abbiamo che i tableaux terminano sempre e quindi possiamo sempre dire se una formula è soddisfacibile o no, seguendo questa idea potremmo pensare ai tableaux non come metodi dimostrativi ma come metodo per trovare modelli; infatti quello che facciamo (sviluppando i tableaux) è vedere che il padre è soddisfacibile se e solo se un figlio è soddisfacibile e questo semplifica la ricerca di modelli. Quindi se quello che vogliamo fare è creare modelli i tableaux potrebbero essere uno strumento, almeno nel caso proposizionale; nel caso predicativo invece la cosa si complica, possono infatti capitare tre situazioni:

- Esiste un tableaux chiuso con radice Γ, ϕ. Abbiamo quindi che la radice non ha modelli. Possiamo quindi dire che per definizione che $\Gamma \models \neg\phi$ (equivalentemente $\Gamma \vdash \neg\phi$). Quindi possiamo dimostrare con i tableaux che $\neg\phi$ è valida, e che per tutti i modelli di Γ vale $\neg\phi$.

- Il tableaux che ha come radice Γ, ϕ finisce, arriviamo a formule atomiche, ma non si chiude (pensare al tableaux che ha $\phi = \forall x \forall y \; sx = sy \to x = y$)

Se fosse solo per questi due casi la matematica del primo ordine sarebbe tutta risolta. Infatti o troviamo un modello oppure dimostriamo che non possiamo trovarne. Ma c'è un terzo caso:

- Il tableaux non termina mai. Potremmo dire che questo è possibile, visto che i $\forall$ rimangono sempre attivi: vengono copiate nei nodi figli ma non è questo il problema, infatti potremmo mettere limitazioni aggiuntive al quantificatore $\forall$ per fare in modo che produca solo un numero finito di elementi, quindi non è questo in effetti il problema, anche se questa cosa dovrebbe essere formalizzata. I problemi nascono da formule del tipo:

  $$\Gamma = \{\neg P(a,a),\ \forall x \exists y P(x,y)\}$$

  Facendo i tableaux di questa formula l'esiste istanza nuove variabili, che vengono utilizzate per mandare avanti, non a vuoto, il $\forall$, quindi questo permette al tableaux di non fermarsi mai. Anche se esiste un modello di soli due elementi che soddisfa Γ, se noi seguissimo le regole dei tableaux senza fermarci non riusciremmo ad arrivare a nessuna conclusione.

La domanda sorge dunque nel terzo caso: se ci troviamo di fronte a una situazione simile è possibile trovare un modello? E come è possibile vedere se è possibile trovarlo? Potrebbe sia esistere un modello finito, come nel caso visto, sia esistere un modello infinito ma nessun modello finito (e non esistere modello?). Non possiamo dunque dire nulla. Per esempio se consideriamo

$$\Gamma' = \Gamma \cup \{\forall x,\ \neg P(x,x),\ \forall x,y,x\ [P(x,y) \wedge P(y,z) \to P(x,z)]\}$$

Γ' ha come modello $\mathbb{N}$ con $P^{\mathbb{N}} = (<)$ e $q^M = \{0\}$, ma non esistono modelli finiti. Ci rimane solo da chiedere: se il tableaux non finisce, c'è sempre un modello? Si, se facciamo con cura il tableaux. Consideriamo il caso:

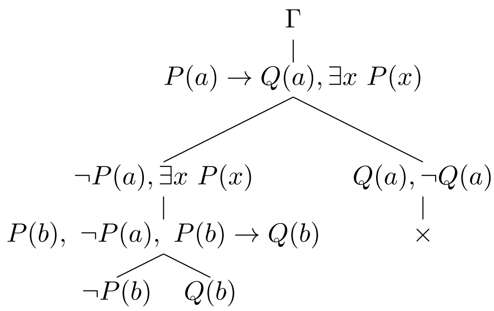
$$\Gamma = \{P(a,a) \wedge \neg P(a,a),\ \forall x \exists y P(x,y)\}$$

Se noi sviluppassimo prima tutti i $\forall\exists$ chiaramente non ci accorgeremmo del fatto che questa cosa non può avere modelli e quindi ci troveremmo in una situazione particolare: il tableaux non finisce mai ma non può sperare di avere modelli. Ma si può evitare?

Esempio 12. Si pensi al tableaux che ha come radice Γ, ϕ con $\Gamma = \forall x(P(x) \to Q(x)), \neg Q(a), \exists x\ P(x)$, formule nel linguaggio $\mathscr{L} = \{P, Q, a, \dots\}$. Abbiamo che esiste un modello di Γ, consideriamo infatti M modello in cui:

- $dom(M) = \{a^M, b^M\}$
- $Q^M = \{b^M\}$
- $P^M = \{b^M\}$

Vediamo se saremmo riusciti ad ottenere lo stesso modello tramite soli tableaux, che abbiamo detto essere metodi per trovare modelli.



Da cui il ramo $Q(b)$ fornisce il modello che abbiamo visto.

Teorema 3. *Data una $\mathscr{L}$ teoria Γ ci troviamo in uno di questi casi:*

- *c'è un tableaux chiuso, dunque Γ non ha modelli*
- *se c'è un tableaux finito ma non chiuso allora esiste un modello finito*
- *se facciamo il tableaux in modo sistematico e il tableaux non si chiude, allora c'è un modello (possibilmente non finito)*

Definizione 8. Diciamo che una teoria Γ (insieme finito di formule) è tableaux-coerente se non esiste un tableaux chiuso con radice Γ: se non riusciamo a trovare una contraddizione con il metodo dei tableaux.

Osservazione 5. Notare che non possiamo applicare la definizione per esempio agli assiomi di Peano, che abbiamo visto essere uno schema infinito di assiomi.

Corollario. *Se Γ è tableaux-coerente se e solo se ha modello.*

Dimostrazione. Vediamo entrambe le frecce velocemente (rifarsi alle dispense):

$\rightarrow$ Facciamo un tableaux sistematico e uso il teorema precedente.

$\leftarrow$ I tableaux sono stati costruiti di modo tale che la radice ha modello se e solo se esiste un figlio che ha modello. Se per assurdo Γ fosse tableaux-incoerente esisterebbe un tableaux chiuso, quindi tutte le foglie sarebbero senza modello, quindi non è possibile che la radice avesse modello.

Corollario. *Vediamo che il teorema di correttezza e completezza è un corollario. Abbiamo infatti che $\Gamma \vdash_{Tab} \phi \iff \Gamma \vDash \phi$, ma $\Gamma \vdash_{Tab} \phi$ se e solo se, per definizione, $\Gamma, \neg\phi$ è tableaux incoerente, questo solo se $\Gamma, \neg\phi$ non ha modelli, e quindi in ogni modello di Γ vale ϕ, cioè $\Gamma \vDash \phi$.*

Definizione 9. Sia $\mathscr{L} = \{a, b, P, \dots\}$ un linguaggio finito di partenza e $C = \{c_i\}_{i\in\mathbb{N}}$ un insieme di costanti di riserva prodotte per esempio dagli esiste, quando li sviluppiamo. Le $\mathscr{L} \cup C$-formule chiuse sono in quantità numerabile, quindi possiamo numerarle (diciamo mettendole in ordine alfabetico), quindi $\mathscr{L} \cup C - formule = \{\phi_n\}_{n\in\mathbb{N}}$. Quando sviluppiamo un nodo Γ del tableaux, analizziamo la $\phi \in \Gamma$ con indice minimo tra quelle non ancora considerate. Avremo anche un insieme di $\mathscr{L} \cup C$-termini chiusi$= \{t_i\}_{n\in\mathbb{N}}$, anche questi in quantità numerabile. Allora quando analizziamo un $\forall x\phi(x)$ sostituiamo in x

il termine t con indice minimo non ancora sostituito. Se sviluppiamo un $\exists$, utilizziamo una costante c_i nuova non ancora adoperata in quel ramo, dunque $\exists x\phi(x)$ diventa $\phi(c_i)$.
Questo è l'algoritmo per sviluppare i tableaux.

Esempio 13. Vediamo il caso di prima: $P(a,a) \wedge \neg P(a,a), \forall x \exists y\ P(x,y)$visto che $P(a,a) \wedge \neg P(a,a)$ è una formula, allora è numerata, allora in al massimo un numero finito di passi, dovremo trattarla, e quindi non possiamo continuare a ignorarla. Cioè all'interno di ogni nodo, per decidere quale formula spezzare, prendiamo sempre quelle di priorità più alta. Dunque certamente tutte le formule saranno sviluppate in un numero finito di passaggi e quindi se c'è una contraddizione verrà trovata in un numero finito di passi.

Riflessione 5. Ma questo non è esattamente un algoritmo: infatti l'algoritmo potrebbe fermarsi e dire che il tableaux è chiuso, oppure esiste modello. Ma potrebbe anche non fermarsi, ma in quel caso non sappiamo se non si sta fermando perché non è ancora arrivato a una risposta: potremmo dover attendere all'infinito.

Definizione 10 (Insieme di Hintikka)**.** Le formule che si trovano in un ramo non chiuso finito o infinito, è un insieme di Hintikka. Possiamo dire che un insieme di Hinticca è un insieme H di $\mathscr{L}' = \mathscr{L} \cup C$-formule (supponendo di avere almeno una costante) tale che:

- $\phi \in \implies \neg\phi \notin H.$
- $\phi \vee \psi \in H \implies \phi \in H \vee \psi \in H.$
- $\phi \wedge \psi \in H \implies \psi, \phi \in H.$
- $\neg\neg\phi \in H \implies \phi \in H.$
- $\neg(\phi \vee \psi) \in H \implies \neg\phi, \neg\psi \in H.$
- $\neg(\phi \wedge \psi) \in H \implies \neg\phi \in H \vee \neg\psi \in H.$
- $\forall x\phi(x) \in H,\ t \in \mathscr{L}' - termini \implies \phi(t) \in H.$
- $\exists x\phi(x) \in H \implies \exists t \in \mathscr{L}' - termini\ t.c.\ \phi(t) \in H.$
- $t_1 = t_2 \in H \wedge \phi(t_1) \in H \implies \phi(t_2) \in H.$
- $t = t \in H.$

Osservazione 6. Dovrebbe essere ovvio che un ramo di un tableaux sia un insieme di Hintikka.

Arriveremo a dimostrare che ogni insieme di Hintikka ha un modello, e dunque sarà dimostrato il teorema di completezza e correttezza.

Lezione 7

16 Ottobre

Abbiamo visto come funzionano gli insiemi di Hintikka.

Esempio 14. Vediamo per ora senza funzioni e uguaglianze. Sono insiemi di Hintikka:

- $\{A \wedge B \to A,\ A\}$
- $\{(A \wedge B) \to A,\ \neg(A \wedge B),\ \neg A\}$
- Cerchiamo un insieme di Hintikka che contenga $H = \{\forall x \exists y P(x,y)\}$, concentriamoci su linguaggi con almeno una costante, quindi $\mathscr{L} = \{c, a, P\}$ almeno. L'insieme H non è ancora di Hintikka, dobbiamo aggiungere almeno $\{\exists y P(a,y),\ \exists y P(c,y)\}$ ma non è ancora di Hintikka: mancano i testimoni degli $\exists$. Abbiamo dunque che è di Hintikka l'insieme:

  $$H' = \{\forall x \exists y P(x,y), \exists y P(a,y),\ \exists y P(c,y)\}$$

  Sappiamo che un ramo massimale non chiuso di un tableaux sistematico è di Hintikka. Questo è vero perché prima o poi tutte le formule saranno considerate, se il tableaux è sistematico: ogni formula, prima o poi questa avrà la priorità, e quindi verrà spezzata. Quindi un ramo non chiuso e non ulteriormente prolungabile di un tableaux è un insieme di Hintikka (esercizio).

Possiamo vedere un insieme di Hintikka come un insieme in cui ogni formula deve essere giustificata: se vi è un $\exists x \phi(x)$ allora ci dovrà anche essere $\phi(a)$ per un qualche costante a che giustifica l'$\exists$. La giustificazione di una formula quasi sempre la implica: $A \to A \vee B$, oppure $\phi(a) \to \exists x \phi(x)$; il problema sorge nei $\forall$, infatti un certo numero di $\phi(a)$ non implica di per se che si abbia $\forall x \phi(x)$.

Esercizio 10. Mettiamoci nel linguaggio $\mathscr{L} = \{0, 1, +, \cdot\}$ degli anelli; prendiamo come insieme $T = \{\phi \ t.c.\ \mathbb{R} \vDash \phi\}$, questo è di Hintikka? No. Infatti possiamo vedere che $\mathbb{R} \vDash \exists x(x \cdot x = 1 \cdot 1)$. Questa cosa non ha testimone tra i termini del linguaggio (un testimone sarebbe la radice di 2, ma con i simboli del nostro linguaggio $\mathscr{L}$ possiamo solo creare termini che denotano numeri naturali). Se invece consideriamo $T' = \{\phi \ t.c.\ \mathbb{N} \vDash \phi\}$, allora abbiamo che T' è in effetti di Hintikka.

Definizione 11. Sia $\mathscr{L}$ un linguaggio, una struttura M si dice ricca se ogni $m \in dom(M)$, esiste t un $\mathscr{L}$ termine chiuso tale che $a = t^M$.

Esercizio 11. Se M è ricca, allora $Th(M)$ (la teoria completa di M) è un insieme di Hintikka.

Ci possiamo chiedere il contrario: se partiamo da un insieme di Hintikka, possiamo costruirne un modello?

Osservazione 7. Notiamo che se abbiamo un modello M ricco, e $\forall t$ termine chiuso abbiamo $M \vDash \phi(t)$, allora $M \vDash \forall x \phi(x)$.

Teorema 4. *Dato un linguaggio $\mathscr{L}$, ogni insieme di Hintikka T ha modello M. Inoltre possiamo prendere M ricco.*

Osservazione 8. Supponiamo di avere già la dimostrazione del teorema, è necessario che $Th(M) = T$? No, anche se sicuramente abbiamo $Th(M) \supseteq T$, per definizione di modello. Ma solitamente l'inclusione è stretta, infatti $Th(M)$ è completo, T non necessariamente, inoltre di sicuro $Th(M)$ è infinito, infatti per ogni formula ϕ abbiamo che $\phi \in Th(M)$ o $\neg\phi \in Th(M)$.
Dato un insieme di Hintikka, esiste un unico modello ricco? No, prendiamo come esempio $\mathscr{L} = \{P, a, c, Q\}$ e prendiamo come insieme di Hintikka $T = \{\exists x P(x), P(a), Q(c)\}$. Questo è un insieme di Hintikka, ma non ha un unico modello, infatti esistono almeno due modelli diversi: uno in cui vale $Q(a)$ e uno in cui vale $\neg Q(a)$.

Esercizio 12. Un insieme di Hintikka massimale è completo. Per massimale si intende che non può essere ulteriormente esteso ad un insieme di Hintikka più grande nello stesso linguaggio.

Dimostrazione. Dimostriamo dunque che se T è di Hintikka, allora ha un modello ricco. Prendiamo il caso di $\mathscr{L}$ senza simbolo di $=$ o simboli di funzioni.

- $dom(M)$, scegliamo come dominio un insieme in bigezione con i simboli di costante, abbiamo quindi un'associazione biunivoca tra l'insieme delle costanti C e $dom(M)$. L'associazione manda c in un elemento del dominio che chiamiamo c^M. Tale elemento c^M sarà proprio l'interpretazione di c nella struttura che andiamo a costruire.

- Un predicato $P \in \mathscr{L}$ di arietà n verrà interpretato come un sottoinsieme di M^n, in particolare diciamo che $(a_1, \dots, a_n) \in P^M \iff P(c_1, \dots, c_n) \in T$ dove $a_i = c_i^M$.

  Abbiamo che vale (sempre supponendo che T sia di Hintikka):

  - ϕ atomica $\in T \iff M \vDash \phi$
  - $\neg\theta \in T \implies M \vDash \neg\theta$, se θ è atomica.

  Mostreremo che M è un modello di T, ovvero che per ogni $\varphi \in T$ abbiamo $M \vDash \varphi$. Per ora lo abbiamo dimostrato per le formule atomiche.

- Osserviamo che per costruzione la struttura M è ricca.

- Vogliamo dimostrare che $\theta \in T \implies \vDash \theta$. E lo dimostriamo per induzione sulla complessità di θ. Ragioniamo per casi:

- $\theta = \alpha \vee \beta$, allora per definizione di insieme di Hintikka $\alpha \in T$ o $\beta \in T$, dunque $M \vDash \alpha$ oppure $M \vDash \beta$ per induzione, quindi $M \vDash \alpha \vee \beta$.
- $\theta = \neg\alpha \in T$. Qui dobbiamo distinguere due casi: se α è atomica abbiamo visto prima la situazione. Se invece ci troviamo in una situazione tipo $\alpha = \gamma \wedge \delta$, allora, visto che è un insieme di Hintikka, la negazione entra, e otteniamo $\neg\gamma \in T$ o $\neg\delta \in T$. Quindi $M \vDash \neg\gamma$ o $M \vDash \neg\delta \implies M \vDash \neg\alpha$. L'induzione torna, visto che γ e δ devono essere più semplici di α.
- $\exists x\phi(x) \in T \implies M \vDash \exists x\phi(x)$. Infatti se $\exists x\phi(x) \in T$, visto che T è di Hintikka ci deve essere un termine c tale che $\phi(c) \in T$. Per induzione $M \vDash \phi(c)$, e a maggior ragione $M \vDash \exists x\phi(x)$.
- $\forall x\phi(x) \in T$, per definizione di insieme di Hintikka, $\forall c$ termine chiuso di $\mathscr{L}$,$\phi(c) \in T$, quindi per induzione $\forall c$ termine chiuso di $\mathscr{L}$, $M \vDash \phi(c)$, ma M è ricco, dunque, $\forall m \in M$, $M \vDash \phi(m/x)$, ovvero $M \vDash \forall x\phi(x)$.

Dovremmo estendere la dimostrazione al caso in cui vi sono i simboli = o simboli di funzione. Intanto, come prendiamo il dominio? Il problema è che alcuni termini potrebbero essere identificati. Prenderemo quindi $dom(M) = \{\text{termini chiusis}/E\}$, dove E è una relazione di equivalenza, dove

$$E(t_1, t_2) \iff (t_1 = t_2) \in T$$

Il dominio dunque è fatto di classi di equivalenza di termini. Interpretiamo dunque una costante a come $a^M = [a]$.

Definizione 12. Per vedere come interpretare i simboli di funzioni, prendiamo per semplicità un simbolo f di arietà 2, e definiamo $f^M([t_1], [t_2]) = [f(t_1, t_2)]$.

Dobbiamo dimostrare che la definizione è ben posta, ovvero che non dipende dai rappresentanti particolari che abbiamo scelto. Supponiamo dunque che $E(t_1, t_1')$ e $E(t_2, t_2')$. Occorre dimostrare $E(f(t_1, t_2), f(t_1', t_2'))$. Consideriamo la formula $\phi(x)$ data da $f(x, t_2) = f(t_1, t_2)$. Per le regole dei tableaux, $\phi(t_1) \in T$ (detagli: quanto ogni T di Hintikka contiene le formule $t = t$ per ogni termine chiuso t, e prendendo come t il termine $f(t_1, t_2)$ otteniamo che $f(t_1, t_2) = f(t_1, t_2) \in T$, ovvero $\phi(t_1) \in T$). Inoltre per ipotesi $t_1 = t_1' \in T$ (in quanto stiamo supponendo $E(t_1, t_1')$). Per una delle regole dell'uguaglianza, $\phi(t_1') \in T$, ovvero $E(f(t_1, t_2), f(t_1', t_2))$. Con un altro passaggio simile si ottiene $E(f(t_1, t_2), f(t_1', t_2'))$, che è quello che volevamo.

Esercizio 13. Se t è un termine, l'interpretazione t^M di t è proprio la classe di equivalenza $[t]$.

Definizione 13. Interpretiamo i simboli di predicato P nel modo seguente. Per semplicità prendiamo P binario. Vale $P^M([t_1], [t_2])$ se e solo se $P(t_1, t_2) \in T$.

Per costruzione M è ricca. Infatti un suo generico elemento è della forma $[t]$ per qualche termine chiuso t, e sappiamo che tale elemento è l'interpretazione di qualche termine, ovvero di t stesso (in quanto abbiamo visto che $t^M = [t]$). Abbiamo ora definito una struttura M, detta modello dei termini.

Teorema 5. *Possiamo ora dimostrare $\phi \in T \implies M \vDash \phi$ in modo analogo a quanto fatto nel caso senza simboli di funzione e di uguaglianza.*

Dimostrazione. Vediamo per esempio il caso in cui ϕ sia una formula atomica, il resto è analogo a prima. Se ϕ è atomica, può essere della forma $t_1 = t_2$ oppure $P(t_1, \ldots, t_n)$.

- $t_1 = t_2 \in T \implies E(t_1, t_2) \implies [t_1] = [t_2] \implies t_1^M = t_2^M \implies M \vDash t_1 = t_2$.
- $P(t_1, \ldots, t_n) \in T \implies P^M([t_1], \ldots, [t_n]) \implies P^M(t_1^M, \ldots, t_n^M) \implies M \vDash P(t_1, \ldots, t_n)$.

Corollario. *Sia* Γ *un insieme finito di formule. Allora* Γ *è un tableaux coerente* $\iff \Gamma$ *ha modello.*

Dimostrazione. Facciamo solo una freccia per ora:

$\implies$ Il tableaux sistematico non si chiude, ogni suo ramo massimale non chiuso è di Hintikka, quindi ha modello, quindi in particolare anche la radice ha modello.

Lezione 8

19 Ottobre

Esercizio 14. Consideriamo il linguaggio $\mathscr{L} = \{\cap, \cup, \sim, 0, 1\}$ e come $\mathscr{L}$ teoria T gli assiomi (validi $\forall x, y$):

- $x \cup 0 = x$
- $x \cap 0 = 0$
- $x \cup 1 = 1$
- $x \cap 1 = x$
- $x \cup y = y \cup x$
- $x \cap y = y \cap x$
- $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$
- $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$
- $x \cup \sim x = 1$
- $x \cap \sim 1 = 0$
- $\sim 1 = 0$
- $\sim 0 = 1$
- $(x \cup y) \cup z = x \cup (y \cup z)$
- $(x \cap y) \cap z = z \cap (y \cap z)$

Il modello dei termini M, cioè i termini chiusi quozientati per equivalenza (due termini t_1, t_2 si dicono equivalenti $E(t_1, t_2)$ se e solo se $T \vdash t_1 = t_2$). L'insieme dei termini è infinito, ci chiediamo però in questo caso la cardinalità del modello dei termini; in questo caso la cardinalità del modello dei termini è 2, infatti $M = \{[0], [1]\}$, dato un generico termine, come ad esempio $\phi \equiv (o \cap 1) \cup 1$ abbiamo che $T \vdash \phi = 1$, e dunque la classe che abbiamo è comunque 1. Se ad $\mathscr{L}$ aggiungiamo una costante a otteniamo che il nuovo modello dei termini avrà cardinalità 4: $M = \{0, 1, a, \sim a\}$. Quanto viene la cardinalità se mettiamo anche un ulteriore elemento?

Dimostrare che $x \cup y = y \iff x \cap y = x$, e in questo caso diciamo che $x \subseteq y$
Notiamo che anche se avessimo che $a \subseteq b$ e quindi anche se avessimo $a \cup b = b$, avremmo che b e $a \cup b$ sono in classi diverse nei modelli dei termini, infatti sono equivalenti solo i termini che tramite gli assiomi si possono dimostrare uguali; nel caso di $a \subseteq b$, invece, non potremmo dedurre dalla teoria che $b = a \cup b$, è un'ipotesi aggiuntiva; avremo quindi che M ha 16 elementi e così via.

Esempi come quello sopra vengono detti algebra di Boole.

Esempio 15. Siano A, B variabili proposizionali, $\mathscr{L} = \{\vee, \wedge, \forall, A, B\}$. Diciamo che $\phi \equiv \psi$ se e solo se $\vDash \phi \leftrightarrow \psi$, questo linguaggio coincide con quello appena visto, è anch'esso un'algebra di Boole. In particolare possiamo vedere $[\phi] \cap [\theta] = [\phi \wedge \theta]$. Possiamo quindi tramutare quanto detto prima, diremo quindi che $[\phi] \subseteq [\psi]$ se $[\phi] \cap [\psi] = [\phi] \iff [\phi \wedge \psi] = [\phi]$, dunque solo se $\phi \wedge \psi = \phi \iff \vDash \phi \to \psi$. Questa viene detta algebra di Lindembaum; possiamo riportare in questa algebra tutti i gli oggetti di prima, dunque avremo per esempio che 0 diventa $\perp$, 1 diventa $\top$ e così via.
Forse in questo modo è più facile vedere che il modello dei termini ha 16 elementi, infatti abbiamo A, B e possiamo avere 16 funzioni che vanno da $\{0,1\} \times \{0,1\} \to \{0,1\}$; che quindi rappresentano tutti i termini possibili.

Esercizio 15. Cercare un'algebra di Boole senza elementi atomici (che non stiamo alla base, come le intersezioni, i singoletti (se si considerano i sottoinsiemi di $\mathbb{N}$)).
L'algebra di Lindembaum di infinite variabili proposizionali $A_1, A_2, \ldots$ è di questo tipo, infatti le formule proposizionali modulo equivalenza di queste sono comunque un'algebra di Boole, ma non è atomica, infatti A_1 non è atomica, sotto di lei c'è $A_1 \cap A_2$ e così via, infatti $A_1 \wedge A_2 \implies A_1$, e questo non arriva a una fine.

Esercizio 16. Se prendiamo l'aritmetica Q di Robinson e definiamo il modello dei termini M come i termini chiusi modulo equivalenza (l'equivalenza t.c. $t_1 = t_2 \iff Q \vdash t_1 = t_2$). Ricordiamoci che il linguaggio era dato solo da $\mathscr{L} = \{0, 1, +, \cdot\}$. Possiamo dire che M è isomorfo a $\mathbb{N}$, infatti, modulo gli assiomi, ogni termine, per quanto complicato, corrisponde a un numero naturale.

Esempio 16. Sia $M_1 = (\mathbb{R}^{>0}, \cdot, 1) \cong (\mathbb{R}, +, 0) = M_2$, infatti sono entrambi modelli dello stesso linguaggio $\mathscr{L} = \{f, c\}$, l'isomorfismo h è semplicemente l'esponenziale: $h(x) = e^x$.

Esercizio 17. Dimostrare che due strutture isomorfe verificano le stesse formule.

Esempio 17. Se prendiamo il linguaggio dei gruppi $\mathscr{L} = \left\{1, \cdot, ()^{-1}\right\}$ con la teoria dei gruppi, abbiamo che il modello dei termini è solo $\{1\}$, se invece aggiungiamo un altri due termini termini a, b quello che otteniamo è il gruppo libero generato da due generatori, infatti otteniamo il gruppo con meno relazioni possibili tra i gruppi che soddisfano la teoria dei gruppi.

Abbiamo visto che se T è di Hintikka allora ha un modello (il modello dei termini, eventualmente quozientato, se abbiamo l'uguaglianza), e quindi è coerente. Inoltre abbiamo anche fatto che, dato un tableaux sistematico con radice

Γ, questo o si chiude dopo un numero finito di passi, oppure produce un modello (eventualmente infinito); infatti se non si chiude c'è almeno un ramo massimale non chiuso, che sappiamo essere di Hinitkka, e che quindi sappiamo avere modello.

Corollario. *Se Γ è tableaux-coerente se e solo se ha modello (finito o numerabile, abbiamo infatti usato la numerabilità per numerare le formule).*

Corollario. $\Gamma \vdash \phi \iff \Gamma \vDash \phi$. *Lo abbiamo già visto, infatti $\Gamma \vdash \phi$ se e solo se $\Gamma, \neg\phi$ tab. incoerente, se e solo se $\Gamma, \neg\phi$ non ha modello, se e solo se $\Gamma \vDash \phi$.*

In particolare se abbiamo M una $\mathscr{L}$ struttura e M' una $\mathscr{L}'$ struttura, diciamo che M' è una espansione di M se, interpretando per M solamente i simboli di $\mathscr{L}$ abbiamo che sono il modello M. Un esempio potrebbe essere considerare il campo $\mathbb{R}$ come espansione del gruppo additivo $\mathbb{R}$.

Esercizio 18. Se $M \mid_{\mathscr{L}} = M$ allora se ϕ è una $\mathscr{L}$ formula, allora si ha che $M' \vDash \phi \iff M \vDash \phi$.

Corollario (Compattezza)**.** *Sia T una $\mathscr{L}$ teoria numerabile; se T non ha modelli allora esiste $T' \subseteq T$ finita tale che T' non ha modelli.*

Dimostrazione. T non ha modelli, quindi T è tableaux incoerente, ma i tableaux se si chiudono si chiudono dopo un numero finito di passi; quindi la stessa dimostrazione della contraddittorietà può essere fatta partendo solo da un numero finito di assiomi: infatti abbiamo fatto solo un numero finito di passaggi, e alla fine abbiamo per ogni ramo una contraddizione, quindi possiamo risalire le formule contraddittorie fino ad arrivare a un T', che anch'esso non avrà modelli.

Una teoria si dice finitamente soddisfacibile se tutte le sottoteorie finite sono soddisfacibili; abbiamo dimostrato che una teoria finitamente soddisfacibile è anche soddisfacibile.

Esempio 18. Consideriamo la teoria $T = PA^{(1)}$ la teoria di Peano del primo ordine, sul linguaggio $\mathscr{L} = \{0, s, +, \cdot\}$. Aggiungiamo al linguaggio la costante c e alla teoria T il gli assiomi $\{c \neq 0, c \neq s(0), c \neq s(s(0)), \dots\}$.
Sappiamo che questa teoria ha modello, infatti una qualunque sottoteoria finita T' ha chiaramente modello, infatti se prendiamo solo un numero finito di assiomi, abbiamo che possiamo interpretare come c un numero naturale qualsiasi k tale che $c \neq k$ non stia in T'. Quindi abbiamo che per ogni sottoteoria finita $\mathbb{N}$ è un modello; per il teorema di compattezza allora avremo un modello di tutta la teoria.
Ma non si riesce a costruire esplicitamente un modello, sappiamo solo che esiste; il problema sorge dal fatto che abbiamo più rami non chiusi e non abbiamo metodi costruttivi per scegliere da quale ramo 'tirare fuori' il modello.

Sia M un modello della teoria T appena vista; se restringiamo questo modello a $\mathscr{L}$ il linguaggio $\{0, s, +, \cdot\}$ otteniamo $\mathbb{N}$? No, infatti anche se abbiamo tolto il nome, rimane comunque l'elemento c, che anche se non è valutato comunque esiste con tutta la sua struttura; quello che vogliamo dire è che se esistesse un isomorfismo dovremmo avere che $a = c^M$ viene mandato in un elemento a' che non può essere uguale a nessun numero naturale, per gli assiomi imposti.
Dunque gli assiomi di Peano del primo ordine non sono sufficienti a caratterizzare i naturali: Peano non è categorica.

Lezione 9

23 Ottobre

Ricapitoliamo quanto abbiamo visto sugli assiomi di Peano e l'aritmetica di Robinson:

- Inizialmente avevamo Q: gli assiomi dell'aritmetica di Robinson, di cui abbiamo trovato due modelli, infatti $\mathbb{N} \models Q$ e anche i polinomi in $\mathbb{Z}$ con primo termine positivo rispettavano Robinson.
- Abbiamo poi considerato $PA^{(1)}$, cioè gli assiomi dell'aritmetica di Robinson, più lo schema generale dell'induzione: infiniti assiomi aggiuntivi che estendono a tutte le formule l'induzione. Abbiamo visto che esiste un modello di questa teoria diverso da $\mathbb{N}$, anche se in effetti non lo abbiamo trovato esplicitamente.
- $PA^{(2)}$ individua unicamente $\mathbb{N}$ a meno di isomorfismo

Definizione 14 (Albero)**.** Un albero è un insieme V di nodi, unito una relazione binaria E tra di essi (diciamo che x è antenato di y se vale $E(x, y)$); E deve essere tale che:

- $\exists x,\ \forall y,\ [E(x, y) \vee y = x]$
- $E(x, y) \wedge E(y, z) \implies E(x, z)$
- $\forall x\ \neg E(x, x)$
- Diremo che $P(x, y) \iff E(x, y) \wedge \neg\exists z[E(x, z) \wedge E(z, y)]$
- Diciamo che $R(x) \iff \neg\exists y E(y, x)$
- $P(x, z) \wedge P(y, z) \implies x = y$
- $\exists x, y\ E(x, y) \implies \exists z P(x, z)$

Questa è una buona definizione per modelli finiti, ma non per alberi infiniti (non esistono assiomatizzazioni del primo ordine degli alberi).

Esempio 19. Vediamo come fallisce la nostra definizione. Consideriamo $V = \mathbb{N} \times \{0\} \cup \mathbb{Z} \times \{1\}$ con le relazioni:

- $\forall n, m\ E(< n, 0 >, < m, 1 >)$

- $E(< n, 0 >, < k, 0 >) \iff n < k$

Questo non vorremmo definirlo come albero, ma rispetta gli assiomi visti.

Definizione 15 (Albero (secondo ordine))**.** Proviamo a definire albero utilizzando anche il secondo ordine; prendiamo dunque come assiomi:

- Gli assiomi di prima
- $\forall^{(2)} Q \ \{\forall x, y \ [P(x,y) \wedge Qx \implies Qy] \wedge \exists x[R(x) \wedge Qx] \implies \forall y \ Qy\}$

Quindi abbiamo introdotto una forma di induzione sugli alberi.

Osservazione 9. $PA^{(2)}$ ha un unico modello; vediamo una spiegazione provvisoria. Abbiamo infatti che $0^M \in M$, se $a \in M$ allora $s^M(a) \in M$. Prendiamo allora come Q il più piccolo sottoinsieme di M che contiene 0^M e tale che $a \in Q \implies s^M(a) \in Q$ (sappiamo che esiste il minimo: è l'intersezione). Q contiene solamente gli elementi della forma $(s^M)^n(0^M)$, cioè solo successori finiti di 0^M (potremmo dire altrimenti che $Q = \{t^M : t \text{ termine chiuso}\}$). Se vale l'induzione del secondo ordine, allora $Q = M$. Quindi per l'induzione abbiamo che in M vi sono solo i numeri denotati da termini, che sono in effetti isomorfi ai numeri naturali.

Esercizio 19. Verificare che i numeri denotati da termini sono isomorfi ai naturali.

Definizione 16. Un albero etichettato è un albero e una funzione, che va da ogni nodo a un insieme di formule (un'etichetta).

Esempio 20. Un tableaux è un albero etichettato.

Lemma 1 (di König)**.** *Se abbiamo un albero infinito a ramificazione finita (ogni nodo ha un numero finito di figli), allora esiste un ramo infinito (una successione di nodi* $\{a_n\}$ *e* $P(a_n, a_{n+1})$*).*

Dimostrazione. Prendiamo a_0 la radice, almeno uno dei figli di a_0 ha infiniti discendenti (se ogni figlio avesse un numero finito di discendenti avremmo un numero finito di elementi, usiamo il fatto che unione finita di insiemi finiti è finita) prendiamo questo come a_1. Si itera il ragionamento.

Definizione 17. Si dice piastrella di Hao wang un quadrato con orientazione, tale che ad ogni suo lato sia associato un numero (o un colore).

Osservazione 10 (Piastrelle di Hao Wang). Consideriamo di avere un numero finito di tipi di piastrelle diverse e supponiamo di poter affiancare due piastrelle solamente se i loro lati hanno colori che combaciano, senza ruotarle o ribaltarle. La domanda è: sapendo che tipi di piastrelle abbiamo, possiamo tassellare il piano? La domanda è molto più difficile di quanto possa sembrare.

Esercizio 20. Supponiamo che si riesca a tassellare un quadrante con un numero finito di tipi di piastrelle diverse. Si riesce a tassellare il piano?

Dimostrazione. Costruiamo un albero, nella radice inseriamo una piastrella; i figli di un nodo contenente una tabella $n \times n$ di piastrelle contengono una tabella $n + 2 \times n + 2$ che estende esternamente il padre (aggiungiamo un contorno).

Sappiamo che questo albero è infinito (infatti abbiamo che un intero quadrante è stato tassellato), ogni ramificazione è finita (infatti abbiamo un numero finito di tassellature e ciascuna tabella ha un numero finito di piastrelle). Per König abbiamo un ramo infinito, e dunque possiamo fare una tassellazione completa del piano.

Osservazione 11. Dimostrando il teorema di completezza abbiamo implicitamente utilizzato il lemma di König, e in effetti, a una seconda analisi, si può vedere che le due cose si equivalgono: si dimostra König a partire dal teorema di completezza e si dimostra il teorema di completezza a partire dal lemma di König.

Esempio 21. Prendiamo la teoria vista la scorsa lezione: $PA \cup \{c \neq 0, c \neq s(0), \dots\}$. Abbiamo detto che questa teoria è coerente, visto che tutte le sottoteorie finite erano coerenti. Ma come tutti i tentativi di estrarre un modello generico dai modelli delle sottoteorie finite erano senza risultati, nello stesso modo se cerchiamo di estrarre una tassellatura generale dalla tassellatura di un quadrante non riusciamo di fatto ad arrivare da nessuna parte.

Definizione 18. Si dice grado una coppia (V, E) in cui V è l'insieme dei nodi, ed $E \subseteq V^2$, con gli assiomi:

- $\neg E(x, x)$
- $E(x, y) \iff E(y, x)$

Diciamo che un grafo è planare se possiamo disegnare i lati senza che questi si intersechino.

Teorema 6. *Ogni grafo planare può essere colorato con* 4 *colori in modo tale che ogni nodo abbia colore diverso dai suoi adiacenti.*

Esercizio 21. Sia (V, E) un grafo infinito (vertici numerabili, supponiamo $V = \mathbb{N}$), se tutti i sottografi finiti sono colorabili con 3 colori, anche l'intero grafo lo è (fare la dimostrazione utilizzando il teorema di König, ora lo faremo con il teorema della compattezza).

Dimostrazione. Sia $G = (V, E)$ il nostro grafo, una colorazione è una funzione $f : V \to \{0, 1, 2\}$. Vogliamo che $E(x, y) \implies f(x) \neq f(y)$; e cerchiamo di costruire una teoria tale che i modelli di T siano isomorfi alle $3-$ colorazioni di G.
Il linguaggio della teoria sarà $\mathscr{L} = \{E, Blu, Giallo, Rosso, c_0, c_1, \dots\}$ dove $Blu, Giallo, Rosso$ sono predicati unari; introduciamo come assiomi:

- $\forall x,\ B(x) \vee R(x) \vee G(x)$
- ogni x ha un unico colore
- $E(x, y) \wedge B(x) \implies \neg B(y)$ (e uguale con gli altri colori)
- $\{E(c_i, c_j)\}$ se $< i, j > \in E^G$; cioè inseriamo nel modello la relazione di adiacenza