Appunti ed esercizi del corso di Istituzioni di Logica Matematica

Prof. A. Berarducci

Versione del 4 Gen. 2002, Rivista 8 Marzo 2002

Le seguenti note sono provvisorie ed imperfette. Sono state scritte ad uso degli studenti che hanno seguito il corso.

Contents

1 Calcolo proposizionale

1.1 Tavole di verità

Una **proposizione** è un enunciato di cui ha senso chiedersi se sia vero o falso. Ad esempio "$3 > 2$" è una proposizione vera, mentre "$2 > 3$" è una proposizione falsa. Assumiamo la concezione classica secondo cui una proposizione è o vera o

falsa (principio del terzo escluso), ma non può essere sia vera che falsa (principio di non contraddizione).

I **connettivi booleani** sono usati per costruire proposizioni complesse a partire da proposizioni semplici. Nella formalizzazione del linguaggio matematico i connettivi di cui faremo maggiore uso sono indicati con i simboli $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$. La loro traduzione approssimativa in italiano è la seguente:

"$\neg A$" significa "non A" (negazione),
"$A \wedge B$" significa "A e B" (congiunzione),
"$A \vee B$" significa "A o B" (disgiunzione),
"$A \rightarrow B$" significa "se A, allora B" (implicazione),
"$A \leftrightarrow B$" significa "A se e solo se B" (doppia implicazione).

Le lettere A, B sopra usate indicano generiche proposizioni. La traduzione che abbiamo dato è solo approssimativa: non c'è una perfetta corrispondenza tra l'uso dei connettivi in una lingua naturale come l'italiano e il loro uso nel linguaggio matematico.

Ad una proposizione ϕ associamo il **valore di verità 1** o **0** a seconda che essa sia vera o falsa.

I connettivi booleani sono *vero-funzionali* nel senso che il valore di verità di una proposizione composta dipende solo dal valore di verità delle proposizioni semplici che la costituiscono. Questo avviene secondo le seguenti **tavole di verità** che precisano il significato dei connettivi.

A	$\neg A$
0	**1**
1	**0**

La tavola dice che la proposizione $\neg A$ è vera se A è falsa, ed è invece falsa se A è vera. La negazione inverte il valore di verità. Diamo ora le tavole degli altri connettivi.

A	B	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \leftrightarrow B$
0	**0**	**0**	**0**	**1**	**1**
0	**1**	**0**	**1**	**1**	**0**
1	**0**	**0**	**1**	**0**	**0**
1	**1**	**1**	**1**	**1**	**1**

Le prime due colonne indicano i quattro possibili valori di verità di A e B. Le altre colonne indicano i corrispondenti valori degli enunciati composti $A \wedge B$, $A \vee B$, $A \rightarrow B$, $A \leftrightarrow B$. Discutiamo ora in dettaglio le tavole del $\vee$ e $\rightarrow$.

La tavola di verità del connettivo $\vee$ dice che $A \vee B$ è vera se almeno uno di A e B è vero, senza escludere la possibilità che entrambi siano veri. Questa modalità di disgiunzione corrisponde al "vel" della lingua latina e viene chiamata *disgiunzione inclusiva*. Esiste anche una *disgiunzione escusiva*, corrispondente all' "aut" latino, che indichiamo con il simbolo $\oplus$ ed è definita dalla seguente tavola di verità:

A	B	$A \oplus B$
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**0**

Dalle tavole di verità risulta che l'implicazione $A \to B$ è falsa solo nel caso in cui la premessa A è vera e il conseguente B è falso. In particolare se la premessa A è falsa, l'enunciato $A \to B$ è sempre vero a prescindere da quale sia l'enunciato B: da una premessa falsa segue ogni proposizione. L'implicazione così definita viene detta **implicazione materiale**. Secondo le nostre definizioni un enunciato quale il seguente risulta vero per qualsiasi valore di x:

$$x \text{ è un numero primo maggiore di due } \to \ x \text{ è dispari}$$

se ad esempio $x = 3$ l'implicazione è vera in quanto sia la premessa che la conclusione sono vere, mentre se $x = 4$ l'implicazione è ugualmente vera perché la premessa è falsa.

Un enunciato composto della forma $A \to B$ equivale a $\neg A \vee B$, nel senso che ha lo stesso valore di verità comunque si scelgano le proposizioni A, B. Ciò si può verificare utilizzando le tavole di verità (si assegnino nei quattro modi possibili i valori $\mathbf{0}, \mathbf{1}$ ad A, B e si verifichi che $A \to B$ risulta avere sempre lo stesso valore di $\neg A \vee B$).

1.1.1 Associatività e parentesi.

Le parentesi hanno lo scopo di indicare l'ordine in cui si effettuano le operazioni. Non potremmo scrivere $A \wedge B \vee C$ in quanto non si capirebbe se intendiamo $(A \wedge B) \vee C$ (prendere prima la congiunzione di A e B e poi fare la disgiunzione con C) o se invece intendiamo $A \wedge (B \vee C)$. Possiamo però scrivere senza ambiguità $A \wedge B \wedge C$ in quanto il connettivo $\wedge$ è **associativo**, ovvero $(A \wedge B) \wedge C$ equivale a $A \wedge (B \wedge C)$ e l'ordine non conta. Analogamente si può verificare che $(A \vee B) \vee C$ equivale a $A \vee (B \vee C)$ (associatività di $\vee$) e quindi possiamo scrivere senza ambiguità $A \vee B \vee C$. Osserviamo che $A \vee B \vee C$ è vero se almeno uno degli enunciati A, B, C è vero mentre $A \wedge B \wedge C$ è vero se tutti e tre gli enunciati A, B, C sono veri.

Per un ulteriore risparmio di parentesi stabiliamo la convenzione che in assenza di parentesi $\wedge$ e $\vee$ legano maggiormente di $\to$ e $\neg$ lega maggiormente di $\wedge$ e $\vee$, quindi ad esempio $\neg A \wedge B \to C$ significa $((\neg A) \wedge B) \to C$.

1.2 Tautologie

Se pensiamo alle lettere A, B, C come a variabili, le espressioni $A \to B$, $\neg A \vee B$, $(A \wedge B) \vee C$ sono esempi di formule proposizionali. Da una formula proposizionale si ottiene una proposizione andando a sostituire le variabili $A, B, C, \ldots$ che che vi compaiono con delle proposizioni. Ad esempio dalla formula $A \to B$ possiamo ottenere la proposizione vera "Nevica $\to$ fa freddo" sostituendo la variabile A con la proposizione "Nevica" e la variabile B con la proposizione

"fa freddo". Dalla stessa formula possiamo anche ottenere la proposizione falsa "$3 = 3 \rightarrow 1 > 4$" sostituendo "A" con "$3 = 3$" e "B" con "$1 > 4$". In generale possiamo definire una **formula proposizionale** come una espressione ottenuta combinando tra loro alcuni simboli $A, B, C, \ldots$ detti **variabili proposizionali** tramite i connettivi e le parentesi, in modo che sostituendo delle proposizioni al posto delle variabili si ottenga una proposizione. Più precisamente:

Definizione 1.1 L'insieme delle formule proposizionali è un insieme di espressioni definito induttivamente come segue. Ogni variabile proposizionale è una formula proposizionale. Se ϕ e ψ sono formule proposizionali, lo sono anche $(\neg\phi)$, $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\phi \rightarrow \psi)$, $(\phi \leftrightarrow \psi)$. (Potremmo fare a meno di $\phi \leftrightarrow \psi$ considerandola come abbreviazione di $(\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$.) Si noti che gni formula è racchiusa da un paio di parentesi. Nello scrivere esempi di formule possiamo omettere le parentesi superflue seguendo le convenzioni date precedentemente.

Da una stessa formula proposizionale si possono ottenere infinite proposizioni diverse a seconda delle sostituzioni. Con certe sostituzioni potremmo ottenere una proposizione vera, con certe altre una proposizione falsa.

Definizione 1.2 Una formula proposizionale ϕ si dice una **tautologia** se è vera per ogni valore delle sue variabili, cioè otteniamo una proposizione vera comunque sostituiamo delle proposizioni al posto delle sue variabili.

Ad esempio $A \vee \neg A$ è una tautologia, in quanto risulta vera sia nel caso in cui A è una proposizione vera, sia nel caso in cui A è una proposizione falsa. Analogamente $(A \rightarrow B) \wedge \neg B \rightarrow \neg A$ è una tautologia, in quanto usando le tavole si vede che essa risulta vera nei quattro possibili casi per i valori di A e B (A vera e B vera, A vera e B falsa, A falsa e B vera, A falsa e B falsa). Una proposizione ottenuta per sostituzione da una tautologia sarà anch'essa detta tautologia. Ad esempio la proposizione "piove $\vee$ $\neg$piove" è una tautologia essendo ottenuta per sostituzione dalla formula tautologica $A \vee \neg A$. Come si vede da questo esempio una tautologia ha contenuto informativo nullo. Affermare "piove o non piove" non ci dà alcuna informazione sul fatto se piova o meno. In generale un enunciato che esprime una tautologia è vero a prescindere dalla verità o falsità degli enunciati elementari che lo costituiscono, e quindi non comunica nulla riguardo alla verità o falsità di questi ultimi. Possiamo dire che tautologia è vera in virtù esclusivamente della sua forma sintattica, e non del suo contenuto.

1.2.1 Complessità delle tautologie

Un metodo per riconoscere se una formula con n variabili è una tautologia è quello di considerare i 2^n possibili casi per i valori di verità delle sue variabili e verificare usando le tavole che in ognuno dei casi la proposizione composta che ne risulta è vera. Si tratta di una procedura semplice e meccanica ma che nel caso ci siano molte variabili richiede molto tempo, anche da parte di un

calcolatore. Esistono altri metodi per controllare se una formula è una tautologia, ma tutti i metodi noti richiedono una quantità di passaggi esponenziale al crescere del numero delle variabili. Il problema di stabilire se esistano metodi più efficienti (che permettano di riconoscere le tautologie in tempo polinomiale anziché esponenziale) è tuttora irrisolto.

1.3 Equivalenza logica e implicazione logica.

Due formule proposizionali ϕ e ψ si dicono **logicamente equivalenti**, e scriviamo in tal caso $\phi \equiv \psi$, se la formula $\phi \leftrightarrow \psi$ è una tautologia. Questo avviene se e solo se ϕ e ψ hanno la stessa tavola di verità, cioè se forniscono lo stesso valore di verità per qualsiasi valore $\mathbf{1}, \mathbf{0}$ che sia assegnato alle loro variabili. Ad esempio $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$, come si può verificare assegnando ad A, B, C i valori $\mathbf{1}, \mathbf{0}$ negli otto modi possibili e verificando che in ciascun caso il valore di $A \wedge (B \vee C)$ è uguale a quello di $(A \wedge B) \vee (A \wedge C)$.

Una formula proposizionale ϕ **implica logicamente** un'altra formula proposizionale ψ se la formula $\phi \rightarrow \psi$ è una tautologia. Questo equivale a dire che per tutti i valori delle variabili per cui ϕ assume il valore $\mathbf{1}$, anche ψ assume il valore $\mathbf{1}$ (ma ψ potrebbe assumere il valore $\mathbf{1}$ in un numero maggiore di casi). Ad esempio $A \wedge B$ implica logicamente $A \vee B$, in quanto se $A \wedge B$ risulta vera per certi valori di A, B, anche $A \vee B$ deve risultare vera per gli stessi valori.

Osserviamo che due formule sono equivalenti se l'una implica logicamente l'altra e viceversa.

Osservazione 1.3 Si noti la differenza tra l'implicazione materiale che abbiamo visto precedentemente e l'implicazione logica. L'implicazione materiale è una implicazione tra proposizioni, mentre l'implicazione logica è una implicazione tra formule proposizionali. Una proposizione ha un valore fisso di verità $\mathbf{1}$ od $\mathbf{0}$, mentre una formula proposizionale è una espressione contenente varibili proposizionali e di per sè non è nè vera nè falsa: solo se si fissa una specifica assegnazione di valori alle sue variabili diventa vera o falsa, e in generale potrebbe risultare vera per certi valori delle sue variabili e falsa per altri.

Esempio 1.4 (Paradossi dell'implicazione materiale) Anche se può sembrare poco intuitivo, date due proposizioni ce ne è sempre una delle due che implica materialmente l'altra: infatti se la prima delle due è una proposizione falsa, essa implica qualsiasi proposizione, e quindi in particolare la seconda, mentre se invece è una proposizione vera, essa è implicata da qualsiasi proposizione. Non è invece detto che date due formule proposizionali ce ne sia sempre una delle due che implica logicamente l'altra: basta prendere una formula che consiste solamente di una variabile proposizionale A, e un'altra formula che consiste di un'altra variabile proposizionale B, e notare che nè $A \rightarrow B$ nè $B \rightarrow A$ sono tautologie (in quanto la prima risulta falsa se diamo ad A il valore $\mathbf{1}$ e a B il valore $\mathbf{0}$, mentre la seconda risulta falsa se diamo a B il valore $\mathbf{1}$ e ad A il valore $\mathbf{0}$).

2 Sintassi del calcolo dei predicati

2.1 Segnatura

La *segnatura* di un linguaggio del primo ordine è dato da un insiemi di simboli (possibilmente anche vuoto) divisi in tre categorie, simboli di costante, simboli di funzione, e simboli di relazione, e da una funzione chiamata "arità" che associa ad ogni simbolo un numero naturale, dove l'arit di ogni simbolo di costante è zero, mentre le arità dei simboli di funzione e di relazione sono interi positivi.

Esempio 2.1 La segnatura del linguaggio degli anelli ordinati con unità è data da $L = \{0, 1, +, \cdot, \leq\}$, dove $0, 1$ sono simboli di costante, $+, \cdot$ sono simboli di funzioni binarie (cioè di arità 2), e $\leq$ è un simbolo di relazione binario.

2.2 Termini

Un linguaggio del primo ordine è costituito, oltre che dai simboli di una data segnatura L, anche da altri simboli, tra cui un insieme V di simboli chiamati *variabili*. Definiamo induttivamente l'insieme $Ter_L(V)$ degli *L-termini* (con variabili da V) come il più piccolo insieme di espressioni che soddisfa le seguenti clausole induttive:

1. Ogni variabile $x \in V$ è un L-termine;
2. ogni simbolo di costante di L è un L-termine;
3. se $t_1, \ldots, t_n$ sono L-termini, e f è un simbolo di funzione di arità n della segnatura L, allora $f(t_1, \ldots, t_n)$ è un L-termine;

Un termine in cui non occorrano variabili viene detto *termine chiuso*. Si noti che se la segnatura L non contiene simboli di costante , allora non ci sono L-termini chiusi, e se la segnatura non contiene nè simboli di costante nè simboli di funzione allora gli unici L-termini sono le variabili (questo avviene ad esempio per la segnatura $L = \{\leq\}$ della teoria degli ordini lineari, o per la segnatura $L = \{\in\}$ della teoria degli insiemi).

Esempio 2.2 Consideriamo la segnatura $L = \{0, 1, +, \cdot, \leq\}$, dove $0, 1$ sono simboli di costante, $+, \cdot$ sono simboli per funzioni binarie, $\leq$ è un simbolo di relazione binario. Esempi di L-termini sono $0, 0 + 1, z \cdot ((x + y) + 1)$, dove x, y, z sono variabili e per semplicità abbiamo usato la notazione infissa xfy anziché $f(x, y)$ quando f è un simbolo di funzione binaria (cioè per i simboli $\cdot$ e $+$). Nella segnatura di questo esempio i termini corrispondono ad espressioni algebriche polinomiali. Osserviamo che i simboli di relazione della segnatura non contribuiscono alla formazione dei termini.

2.3 Formule

Oltre ai simboli di una data segnatura L e ad un insieme infinito V di variabili, l'alfabeto di un linguaggio del primo ordine contiene anche i simboli $\neg, \wedge, \vee, \rightarrow$ per i connettivi booleani, i simboli $\forall, \exists$ per i quantificatori, il simbolo $=$ (opzionale), e le parentesi. La differenza tra due linguaggi del primo ordine è data solo dalla scelta delle segnatura, essendo tutti gli altri simboli sempre presenti (a parte il simbolo di $=$ che può esserci o no).

L'insieme delle L-formule è definito induttivamente come il più piccolo insieme di espressioni che verifica le seguenti clausole induttive:

1. Se R è un simbolo di relazione di L di arità n e $t_1, \ldots, t_n$ sono degli L-termini, allora $R(t_1, \ldots, t_n)$ è una L-formula.
2. Se α e β sono L-formule, allora $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\alpha \rightarrow \beta)$, $(\alpha \vee \beta)$ sono L-formule.
3. Se α è una L-formula e x è una variabile, allora $(\forall x\alpha)$ e $(\exists x\alpha)$ sono L-formule.

Si usa distinguere tra linguaggi con simbolo di uguaglianza e linguaggi senza simbolo di uguaglianza. Nel caso di linguaggi con simbolo di uguaglianza dobbiamo aggiungere:

4. Per ogni coppia di termini s, t, l'espressione $s = t$ è una L-formula.

Una L-formula *atomica* è una L-formula in cui non compaiono connettivi logici (ovvero i simboli $\neg, \wedge, \vee, \rightarrow, \forall, \exists$). Le formule atomiche sono dunque solo quelle della forma $R(t_1, \ldots, t_n)$ oppure della forma $t_1 = t_2$, dove i t_i sono termini, e R è un simbolo di relazione di L. Se la segnatura non contiene simboli di relazione le uniche formule atomiche sono quelle del secondo tipo.

Il simbolo di uguaglianza "=" non appartiene alla segnatura L del linguaggio, ma all'insieme dei cosiddetti *simboli logici*, al pari dei simboli dei connettivi logici $\forall, \exists, \neg$, etc. Alla segnatura appartengono solo i simboli la cui interpretazione può variare, mentre all'insieme dei simboli logici appartengono quei simboli il cui significato è fissato (si veda la sezione sulla semantica).

Negli esempi di L-formule ometteremo per comodità le parentesi ridondanti quando non sussista ambiguità di lettura, ovvero qualora esista un unico modo di aggiungere le parentesi mancanti in modo da ottenere una L-formula. Ad esempio la formula $((x = x \wedge x = y) \vee y = z)$ può essere scritta in forma abbreviata come $(x = x \wedge x = y) \vee y = z$. La stessa formula non può invece essere abbreviata come $x = x \wedge x = y \vee y = z$ in quanto aggiungendo delle parentesi potremmo ottenere, oltre a quella data prima, anche la formula $(x = x \wedge (x = y \vee y = z))$. Resta inteso che queste sono solo abbreviazioni informali, e la definizione ufficiale di L-formula rimane quella data precedentemente.

2.4 Variabili libere e legate

Una occorrenza di una variabile x in una formula α si dice *legata* se occorre in una sottoformula β di α immediatamente preceduta da un quantificatore $\forall x$ o $\exists x$. Una occorrenza non legata si dice *libera*.

Esempio 2.3 La formula $x = x \wedge \forall z(z = z)$ ha due occorrenze legate di z e due occorrenze libere di x.

È possibile che una variabile occorra sia libera che legata in una stessa formula, come ad esempio in $x = x \wedge \forall x(x = x)$, in cui le prime due occorrenze sono libere e le altre sono legate. Quando parleremo della intepretazione delle formule, sarà chiaro che la formula $x = x \wedge \forall x(x = x)$ va intepretata nello stesso modo della formula $x = x \wedge \forall z(z = z)$. Le occorrenze di variabili legate possono sempre essere "ridenominate" in modo che una stessa variabile non occorra sia libera che legata nella stessa formula.

Le *variabili libere di una una formula* sono le variabili che hanno almeno una occorrenza libera nella formula. Ad esempio le variabili libere di $x = y \wedge \forall u \exists x(x = u)$ sono la x e la y (sebbene la x abbia anche una occorrenza legata).

Indichiamo con $Fv(\alpha)$ l'insieme delle variabili libere di α. Chiaramente tutte le variabili che occorrono in una formula atomica sono libere. I quantificatori fanno calare l'insieme delle variabili libere: $Fv(\forall x\alpha) = Fv(\alpha) \setminus \{x\}$ e similmente $Fv(\exists x\alpha) = Fv(\alpha) \setminus \{x\}$. Per i connettivi booleani abbiamo $Fv(\neg\alpha) = Fv(\alpha), Fv(\alpha \to \beta) = Fv(\alpha) \cup Fv(\beta)$, e similmente per $\vee$ e $\wedge$ si prende l'unione.

Una formula senza variabili libere viene detta *formula chiusa* o *enunciato*.

2.5 Sostituzioni

Se α è un termine o una formula, e $t_1, \ldots, t_n$ sono termini, indichiamo con $\alpha(t_1/x_1, \ldots, t_n/x_n)$ il termine o formula risultante da α dalla simultanea sostituzione di ogni occorrenza libera della variabile x_i in α con t_i per $i = 1, \ldots, n$. Se le variabili $x_1, \ldots, x_n$ di cui si sta parlando sono sottointese scriviamo più semplicemente $\alpha(t_1, \ldots, t_n)$ invece di $\alpha(t_1/x_1, \ldots, t_n/x_n)$. Ad esempio $\forall x\alpha(x) \to \alpha(t)$ è la stessa cosa di $\forall x\alpha \to \alpha(t/x)$ (in quanto se sottointendiamo la x, allora $\alpha(t)$ coincide con $\alpha(t/x)$ e $\alpha(x)$ coincide con $\alpha(x/x)$, che è proprio α).

Si noti che in generale la formula $\alpha(t_1/x_1, t_2/x_2)$, ottenuta per sostituzione simultanea, non coincide con la formula $\alpha(t_1/x_1)(t_2/x_2)$, in cui la sostituzione (t_2/x_2) viene effettuata *dopo* la sostituzione (t_1/x_1), che a sua volta può non coincidere con la formula $\alpha(t_2/x_2)(t_1/x_1)$, in cui le sostituzioni vengono fatte nell'ordine inverso.

Esercizio 2.4 Se x_1 ed x_2 sono variabili distinte, $\alpha(t_1/x_1)(t_2/x_2)$ coincide con $\alpha(t_2/x_2)(t_1'/x_1)$, dove t_1' è il termine risultante dalla sostituzione di t_2 al posto

delle occorrenze di x_2 in t_1. In particolare se non vi sono occorrenze di x_2 in t_1, allora t_1' coincide con t_1 e l'ordine delle sostituzioni non conta.

Nel caso di termini chiusi tutti i modi di effettuare le sostituzioni (simultanee o in sequenza) danno lo stesso risultato.

Osservazione 2.5 L'implicazione espressa dalla formula $\forall x\alpha(x) \to \alpha(t)$ non è sempre "logicamente valida". Definiremo più tardi questo concetto, ma intanto diamo un esempio intuitivo. Sia $\phi(x)$ la formula $\exists y(x = y)$ e sia t il termine $y + 1$. Allora $\forall x\phi(x)$ è l'enunciato $\forall x\exists y(x = y)$, che è sempre vero, mentre $\phi(t)$ è l'enunciato $\exists y(y + 1 = y)$ che non è vero se interpretiamo i simboli $+, 1$ come la addizione tra numeri naturali e come il numero naturale "uno".

Affinchè l'implicazione $\forall x\alpha(x) \to \alpha(t)$ risulti logicamente valida dobbiamo porre delle restrizioni sul termine t da sostituire.

Definizione 2.6 Un termine t è *sostituibile al posto di una variabile x in una formula α* se per ogni variabile y in t, nessuna occorrenza libera di x in α appare all'interno di una sottoformula della forma $\exists y\beta$ o $\forall y\beta$. In altre parole questo significa che le variabili di t non diventano legate dopo che si è effettuata la sostituzione $\alpha(t/x)$.

Si noti che un termine chiuso è sempre sostituibile al posto di qualsiasi variabile in qualsiasi formula.

3 Semantica del calcolo dei predicati

3.1 L-strutture

Definizione 3.1 (L-struttura) Sia L una segnatura. Una *L-struttura M* consiste di:

1. Un insieme non vuoto $dom(M)$ detto *dominio* (oppure *universo*) della struttura.
2. Una corrispondenza $c \mapsto c_M$ che associa ad ogni simbolo di costante c di L un elemento $c_M \in dom(M)$, detto interpretazione del simbolo c in M.
3. Una corrispondenza $f \mapsto f_M$ che associa ad ogni simbolo di funzione f di L di arità n, una funzione $f_M : dom(M)^n \to dom(M)$, detta interpretazione del simbolo f in M.
4. Una corrispondenza $R \mapsto R_M$ che associa ad ogni simbolo di relazione R di L di arità n, una relazione $R_M \subseteq dom(M)^n$, detta interpretazione del simbolo R in M.

Notazione. È importante non confondere i simboli con le loro interpretazioni in una data struttura M. Tuttavi quando l'interpretazione dei simboli della segnatura sia chiara dal contesto, o sia suggerita dalla scelta dei simboli usati, useremo la stessa notazione per i simboli e le loro interpretazioni.

Esempio 3.2 Le strutture algebriche usuali possono essere viste come L-strutture.

Gli anelli sono esempi L-strutture dove $L = \{0, 1, +, \cdot\}$ e i simboli $0, 1, +, \cdot$ sono intepretati in modo da soddisfare gli assiomi degli anelli. Similmente i gruppi sono L-strutture con $L = \{1, \cdot\}$.

Gli spazi vettoriali sono L-strutture generalizzate in cui esistono non uno ma due tipi di oggetti nel dominio (vettori e scalari). È tuttavia anche possibile pensare agli spazi vettoriali come ad una L-struttura M dove il dominio $dom(M)$ comprende sia vettori che scalari ma ci sia un simbolo di predicato unario V nella segnatura L che serve a distinguere gli uni dagli altri (cioè V è interpretato come il sottoinsieme di $dom(M)$ consistente dei vettori).

Un ordine parziale è una L-struttura dove $L = \{\leq\}$ e $\leq$ è un simbolo di predicato binario la cui interpretazione deve soddisfare le proprietà degli ordini parziali).

Non è invece possibile pensare in modo semplice ad uno spazio topologico come ad una L-struttura.

3.1.1 Omomorfismi di L-strutture

Definizione 3.3 Un *isomorfismo* $\phi: A \to B$ tra due L-strutture A e B è dato da una mappa iniettiva e suriettiva $\phi: dom(A) \to dom(B)$ che preserva tutte le funzioni e relazioni che interpretano i simboli di L. Più precisamente:

1. se c è un simbolo di costante, allora $\phi(c_A) = c_B$;
2. se f è un simbolo di funzione di arità n e $a_1, \ldots, a_n \in dom(A)$, allora $\phi(f_A(a_1, \ldots, a_n)) = f_B(\phi(a_1), \ldots, \phi(a_n))$;
3. se R è un simbolo di relazione di arità n e $a_1, \ldots, a_n \in dom(A)$, allora $(a_1, \ldots, a_n) \in R_A$ se e solo se $(\phi(a_1), \ldots, \phi(a_n)) \in R_B$.

Esempio 3.4 Sia L una segnatura con un simbolo di relazione binario f. Sia $(\mathbf{R}; +)$ la L-struttura avente come dominio i numeri reali e in cui f è interpretato come la funzione somma, e sia $(\mathbf{R}^{>0}; \times)$ la L-struttura avente come dominio i numeri reali positivi e in cui f è interpretato come la funzione prodotto. Allora la funzione esponenziale $x \mapsto e^x$ è un isomorfismo da $(\mathbf{R}; +)$ a $(\mathbf{R}^{>0}; \times)$.

Definizione 3.5 Il concetto di *immersione* si ottiene da quello di isomorfismo rinunciando alla richiesta che ϕ sia suriettiva. Una immersione è dunque un isomorfismo verso la sua immagine.

Esempio 3.6 Sia $L = \{0, 1, +, -, \cdot, \leq\}$ e consideriamo le L-strutture $\mathbf{Z}$ e $\mathbf{R}$ (con l'ovvia interpretazione dei simboli). Allora la funzione ϕ che manda un numero intero n (inteso come elemento di $\mathbf{Z}$) nel numero n inteso come elemento di $\mathbf{R}$, è una immersione di $\mathbf{Z}$ in $\mathbf{R}$.

Definizione 3.7 Date due L-strutture A e B diciamo che A è una *sottostruttura* di B se $dom(A) \subseteq dom(B)$ e la funzione identità $i: dom(A) \to dom(B)$ è una immersione. Ciò significa che i simboli di costante sono intepretati nello stesso

modo in A e in B, e i simboli di funzione e relazione sono interpretati in A come la restrizione agli elementi di A delle funzioni e relazioni che intepretano gli stessi simboli in B. Per indicare che A è una sottostruttura di B scriviamo $A \subseteq B$. Osserviamo che un sottoinsieme del dominio di una struttura è il dominio di una sottostruttura se e solo se contiene le intepretazioni dei simboli di costante ed è chiuso rispetto alle interpretazioni dei simboli di funzione.

Esempio 3.8 Se pensiamo agli interi come inclusi nei reali, abbiamo che $\mathbf{Z}$ è una sottostruttura di $\mathbf{R}$ (notazione: $\mathbf{Z} \subseteq \mathbf{R}$).

Il concetto di omomorfismo si ottiene indebolendo il concetto di isomorfismo come segue.

Definizione 3.9 Un *omomorfismo* $\phi: A \to B$ tra due L-strutture A e B è dato da una mappa $\phi: dom(A) \to dom(B)$ tale che:

1. se c è un simbolo di costante, allora $\phi(c_A) = c_B$;
2. se f è un simbolo di funzione di arità n e $a_1, \ldots, a_n \in dom(A)$, allora $\phi(f_A(a_1, \ldots, a_n)) = f_B(\phi(a_1), \ldots, \phi(a_n))$;
3. se R è un simbolo di relazione di arità n, $a_1, \ldots, a_n \in dom(A)$, e $(a_1, \ldots, a_n) \in R_A$, allora $(\phi(a_1), \ldots, \phi(a_n)) \in R_B$.

Ad esempio sia $\mathbf{Z}/(n)$ l'anello degli interi modulo n considerato come una L-struttura con $L = \{0, 1, +, -, \cdot\}$. Allora la funzione che manda un intero x nella sua classe resto modulo n costituisce un omomorfismo da $\mathbf{Z}$ a $\mathbf{Z}/(n)$ che non è nè un isomorfismo né una immersione.

Esempio 3.10 Se consideriamo $\mathbf{Z}$ e $\mathbf{R}$ come L-strutture con $L = \{0, 1, +, -, \cdot\}$ (con la usuale interpretazione dei simboli) allora un omomorfismo $f: \mathbf{Z} \to \mathbf{R}$ è un omomorfismo di anelli (e ce ne è uno solo, che è in effetti una immersione), mentre se consideriamo $\mathbf{Z}$ e $\mathbf{R}$ come L-strutture con $L = \{\leq\}$ (e la solita intepretazione del $\leq$) allora un omomorfismo $f: \mathbf{Z} \to \mathbf{R}$ è una qualsiasi funzione $f: dom(\mathbf{Z}) \to dom(\mathbf{R})$ debolmente crescente, ovvero una funzione tale che $x \leq y$ implica $f(x) \leq f(y)$. Ad esempio la funzione $x \mapsto x^3$ è un omomorfismo d'ordine ma non di anelli.

Scegliere la segnatura in un modo anziché un altro dipende da quali funzioni vogliamo considerare come omomorfismi, ovvero da quali caratteristiche strutturali vogliamo che siano preservate.

3.2 Semantica di Tarksi

Definizione 3.11 Data una L-struttura M, una *formula con parametri da* M è una espressione che si ottiene da una L-formula φ sostituendo alcune sue variabili libere $x_1, \ldots, x_n$ con elementi $a_1, \ldots, a_n$ del dominio di M. Similmente per termini. In particolare ogni elemento $a \in dom(M)$ è un termine con parametri

da M (prendiamo come L-termine una variabile x, e sostituiamo x con a). I termini e le formule *chiusi*, con o senza parametri, sono quelli in cui non vi sono variabili libere.

Le notazioni sulle sostituzioni si estendono al caso dei parametri come segue. Se $a_1, \ldots, a_n \in dom(M)$, indichiamo con $\phi(a_1/x_1, \ldots, a_n/x_n)$ la formula con parametri da M che si ottiene sostituendo le occorrenze libere della variabile x_i con a_i $(i = 1, \ldots, n)$. Se è implicito di quali variabili $x_1, \ldots, x_n$ si sta parlando, scriviamo $\phi(a_1, \ldots, a_n)$ invece di $\phi(a_1/x_1, \ldots, a_n/x_n)$. Similmente per i termini.

Esempio 3.12 Sia $L = \{0, 1, +, \cdot\}$ e sia $\mathbf{R}$ la L-struttura dei numeri reali. Allora $(x+y)+1$ è un L-termine (senza parametri), $(\sqrt{2}+y)+1$ è un L-termine contenente il parametro $\sqrt{2}$ da $\mathbf{R}$, e $(\sqrt{2}+\sqrt{2})+1$ è un termine chiuso con parametri da $\mathbf{R}$.

In questo esempio "1" non è un parametro, ma un simbolo di costante della segnatura L. Se volessimo un L-termine che contiene come parametro il numero 1 inteso come elemento di $\mathbf{R}$, allora a rigore dovremmo usare due notazioni diverse per il simbolo $1 \in L$ e il numero $1 \in \mathbf{R}$.

Esempi di L-formule con parametri sono $(\sqrt{2}+y)+1 = y$ (aperta) e $\forall x \exists y((\sqrt{2}+y)+1 = y)$ (chiusa).

Osservazione 3.13 Volendo formalizzare in una metateoria insiemistica (ad esempio nella teoria di Zermelo-Fraenkel) la definizione appena data di formula con parametri da una struttura M possono sorgere alcune difficoltà. Essendo infatti il dominio di M un insieme del tutto arbitrario, nulla esclude che M contenga tra i suoi elementi alcuni oggetti di tipo sintattico, come i simboli, o le stringhe di simboli, che vengono usati nel costruire le L-formule. Ad esempio potrebbe capitare che il simbolo "$\forall$" appartenga al dominio di M. È ovvio che in tal caso si avrebbero dei problemi di leggibilità delle formule con parametri da M. Vi sono vari modi per ovviare a tale inconveniente. Una possibilità è quella di ridefinire una formula con parametri come una coppia costituita da una L-formula φ, e da una "sostituzione" $(a_1/x_1, \ldots, a_n/x_n)$. L'idea è che, usando le coppie, la sostituzione non viene realmente effettuata ma viene lasciata semplicemente indicata. Con questa impostazione potremmo continuare ad usare la notazione $\varphi(a_1/x_1, \ldots, a_n/x_n)$ assumendo che essa denoti la coppia, anziché il risultato della sostituzione. Nel seguito tuttavia ignoreremo queste difficoltà e continueremo a lavorare con la Definizione 3.11 precedentemente data, supponendo implicitamente di volta in volta, senza perdita di generalità, che il dominio della struttura considerata non contenga elementi che possano causare problemi di leggibilità delle formule con parametri.

Definizione 3.14 (Interpretazione dei termini chiusi) Se t è un termine chiuso con parametri dalla L-struttura M, associamo a t un elemento $M(t) \in dom(M)$ semplicemente rimpiazzando i simboli di funzione e di costante presenti in t con la loro interpretazione in M e calcolando il valore di t corrispondente. Più precisamente:

1. Se t è l'elemento $a \in dom(M)$ (abbiamo visto che gli elementi di $dom(M)$ sono casi particolari di termini con parametri), allora $M(t) = a$;

2. Se t è un simbolo di costante c di L, allora $M(t) = c_M$ (l'interpretazione del simbolo c in M).

3. Se $t = f(t_1, \ldots, t_n)$, allora induttivamente $M(t) = f_M(M(t_1), \ldots, M(t_n))$, dove $f_M: dom(M)^n \to dom(M)$ è la funzione che interpretata il simbolo f in M.

Definizione 3.15 (Interpretazione delle formule chiuse con parametri) Sia M una L-struttura, e sia ϕ è una L-formula chiusa con parametri da M. Scriviamo $M \models \phi$ per esprimere il fatto che ϕ rappresenta un enunciato vero qualora si interpretino i simboli nel modo seguente: le variabili variano su elementi del dominio di M e quindi i quantificatori "$\forall x$" ed "$existsx$" vanno quindi letti come "per ogni $x \in dom(M)$" ed "esiste $x \in dom(M)$ "; i simboli della segnatura di L hanno il significato loro attribuito dalla Definizione 3.1 e rappresentano quindi particolari elementi, funzioni e relazioni su M; il connettivo $\neg$ significa "non"; $\wedge$ significa "e"; $\vee$ significa "o"; $\to$ significa "implica"; Il simbolo $=$ significa "è uguale a".

Più formalmente, diciamo che tra M e ϕ sussiste la relazione $M \models \varphi$ se ciò segue dalle seguenti clausole induttive. L'induzione viene fatta sul numero dei connettivi di ϕ.

1. $M \models \forall x \phi(x)$ se e solo se per ogni $a \in dom(M)$, $M \models \phi(a)$;

2. $M \models \exists x \phi(x)$ se esiste $a \in dom(M)$ tale che $M \models \phi(a)$;

3. $M \models \neg\phi$ se e solo se $M \not\models \phi$ (cioè non vale $M \models \phi$);

4. $M \models \phi \wedge \psi$ se e solo se $M \models \phi$ e $M \models \psi$;

5. $M \models \phi \vee \psi$ se e solo se $M \models \phi$ o $M \models \psi$ (nel senso che almeno una delle due è vera, senza escludere il caso che lo siano entrambe);

6. $M \models \phi \to \psi$ se e solo se $M \models \psi$ o $M \not\models \phi$ (senza escludere che si presentino entrambi i casi).

Per la base dell'induzione dobbiamo considerare il caso delle formule atomiche (cioè senza connettivi). Aggiungiamo a tal fine le seguenti clausole, dove R è un simbolo di predicato di L di arità n, e L e i vari t_i sono L-termini chiusi con parametri da M.

7. $M \models R(t_1, \ldots, t_n)$ se e solo se $(M(t_1), \ldots, M(t_n)) \in R_M$;

8. $M \models t_1 = t_2$ se e solo se $M(t_1)$ e $M(t_2)$ sono lo stesso elemento.

Se vale $M \models \phi$ diciamo che ϕ è vera in M, o che M soddisfa ϕ. Anche se fossimo stati solamente interessati alla definizione di verità per formule chiuse senza parametri per poter dare una definizione induttiva della relazione di soddisfacibilità non ci saremmo potuti esimere dal definirla anche per formule chiuse con parametri, come si vede dalla clausola "$M \models \forall x \phi(x)$ se e solo se per ogni $a \in dom(M)$, $M \models \phi(a)$".

Esercizio 3.16 Sia $\alpha(x)$ è una formula la cui unica variabile libera è x. Se t e t' sono termini chiusi con $M(t) = M(t')$, allora $M \models \alpha(t)$ se e solo se $M \models \alpha(t')$.

Esercizio 3.17 Se M è isomorfa a N ed $M \models \phi$, allora $N \models \phi$.

4 Cenni sulla logica del secondo ordine

Nella logica del secondo ordine il concetto di segnatura e di L-struttura non cambia. Quello che cambia è il concetto di L-formula e di intepretazione di una L-formula in una L-struttura. In una L-formula del secondo ordine possono comparire due tipi di variabili: variabili su individui e su relazioni. Ogni variabile su relazioni ha un intero positivo ad essa associato detto la sua arità. I quantificatori $\forall$ ed $\exists$ possono essere applicati ad entrambi i tipi di variabili. Data una L-struttura M, le variabili su individui variano sugli elementi del dominio di M, mentre le variabili su relazioni di arità n variano sull'insieme di tutte le relazioni n-arie sul dominio di M.

Esempio 4.1 Sia $L = \{0, 1, +, \cdot\}$. L'assioma di induzione per i numeri naturali può essere formulato nel modo seguente usando una variabile "R" su relazioni unarie, e altre variabili x, y su individui:

$$\forall R((R(0) \wedge \forall x(R(x) \rightarrow R(x+1))) \rightarrow \forall y R(y))$$

Esempio 4.2 Sia $L = \{0, 1, +, \cdot, \leq\}$. L'assioma di completezza dei numeri reali, intesi come L-struttura, può essere formulato nel modo seguente usando una variabile "R" su relazioni unarie, e altre variabili x, y, x' su individui:

$$\forall R(\text{“}R \text{ ha un maggiorante”} \rightarrow \text{“}R \text{ ha un estremo superiore”})$$

dove "R ha un maggiorante" è la formula

$$\exists x \forall y(R(y) \rightarrow y \leq x)$$

mentre "R ha un estremo superiore" è la formula

$$\exists x[\forall y(R(y) \rightarrow y \leq x) \wedge \forall x'(\forall y(R(y) \rightarrow y \leq x') \rightarrow x \leq x')].$$

La logica del secondo ordine ha capacità espressive molto superiori a quella del primo ordine, ma ha lo svantaggio che non si è possibile definire per essa un concetto adeguato di "dimostrazione formale" per il quale valga un teorema di completezza, cosa che invece è possibile per la logica del primo ordine (si veda la sezione sul sistema dimostrativo di Hilbert-Frege).

5 Teorie assiomatiche

5.1 Teorie, modelli, e conseguenza logica

Definizione 5.1 Sia M una L-struttura e sia ϕ una L-formula(con o senza parametri da M) con variabili libere incluse in $\{x_1, \ldots, x_n\}$. La formula chiusa $\forall x_1 \ldots x_n \phi$ viene detta una *chiusura universale* di ϕ. Diciamo che ϕ è *universalmente vera* in M, oppure *valida* in M, se una sua chiusura universale è vera in M (cioè se $M \models \forall x_1 \ldots x_n \phi$). Detto in altri termini, ϕ è universalmente vera in M se è vera in M per qualsiasi valore delle sue variabili libere. Per formule chiuse la verità e la universale verità coincidono.

Notazione 5.2 La notazione $M \models \phi$ è fino ad ora stata adoperata sono nel caso in cui ϕ è una formula chiusa. Ne estendiamo ora l'uso a formule qualsiasi sottointendendo i quantificatori universali con la convenzione che $M \models \phi$ significa la stessa cosa di $M \models \forall x_1 \ldots x_n \phi$.

Ad esempio se M è un gruppo scriveremo $M \models x \cdot y = y \cdot x$ se e solo se M è commutativo.

Osservazione 5.3 Se M è una L-struttura ϕ è una L-formula, potrebbe capitare che nè ϕ nè la sua negazione $\neg\phi$ sia valida (= universalmente vera) in M. Per tali formule non vale quindi nè $M \models \phi$ nè $M \models \neg\phi$. Ad esempio la formula $x > 1$ non è universalmente vera nel campo ordinato $\mathbf{R}$ dei numeri reali, ma neppure la sua negazione $\neg(x > 1)$ è universalmente vera. Per una formula chiusa α invece si ha sempre che $M \models \alpha$ oppure $M \models \neg\alpha$ (se α non è vera, per definizione lo è la sua negazione). In generale le tavole di verità valgono solo per formule chiuse (che sono le uniche per cui ha senso chiedersi se sono vere in una data struttura). Ad esempio se $M \models \phi \vee \psi$ non è detto che $M \models \phi$ o $M \models \psi$, a meno che non assumiamo che ϕ e ψ siano formule chiuse.

Definizione 5.4 Una *teoria* T è una coppia consistente di una segnatura L e di un insieme di L-formule chiamate *assiomi di* T.

Definizione 5.5 Un *modello* di una L-teoria T è una L-struttura in cui risultano validi (universalmente veri) tutti gli assiomi di T. Se M è un modello di T scriviamo $M \models T$. Quindi $M \models T$ se per ogni assioma ϕ di T, si ha $M \models \phi$. Indichiamo con $Mod(T)$ la classe di tutti i modelli di T. Una L-teoria T si dice *semanticamente coerente*, o anche *soddisfacibile*, se ha almeno un modello.

Definizione 5.6 (Conseguenza logica) Sia ϕ una L-formula chiusa e T una L-teoria. Diciamo che ϕ *segue logicamente* da T, e scriviamo $T \models \phi$, se non esiste nessuna L-struttura che rende validi tutti gli assiomi di T e non rende valida ϕ. In altre parole:

$$T \models \phi \text{ se e solo se } Mod(T) \subseteq Mod(\phi)$$

ovvero tutte le L-strutture in cui tutti gli assiomi di T sono universalmente veri, rendono universalmente vera ϕ. In particolare se T è *insoddisfacibile*, cioè se $Mod(T) = \emptyset$, allora vale sempre $T \models \phi$.

Notiamo che il simbolo "$\models$" viene usato in due modi diversi a seconda che a sinistra del simbolo vi sia una L-teoria (nel qual caso $\models$ rappresenta la relazione di conseguenza logica) o una L-struttura (nel qual caso $\models$ rappresenta la relazione di soddisfacibilità).

Definizione 5.7 (Teorie equivalenti) Due L-teorie T_1 e T_2 si dicono equivalenti se hanno le stesse conseguenze: $\{\phi \mid T_1 \models \phi\} = \{\phi \mid T_2 \models \phi\}$.

Esercizio 5.8 Due teorie sono equivalenti se e solo se hanno gli stessi modelli.

Ogni teoria è equivalente ad una teoria i cui assiomi sono formule chiuse: basta prendere la chiusura universale dei suoi assiomi. Senza perdita di generalità avremmo quindi potuto restringerci a teorie i cui assiomi sono formule chiuse, e usare la notazione $T \models \phi$ solo nel caso di formule chiuse. Tuttavia ammettere formule aperte risulterà conveniente quando andremo a definire il concetto di dimostrazione formale nel sistema dimostrativo di Hilbert-Frege.

Definizione 5.9 (Formule logicamente valide) Sia L una data segnatura e sia ϕ una L-formula. Diciamo che ϕ è logicamente valida, e scriviamo $\models \phi$, se ϕ è valida in ogni L-struttura.

Osserviamo che se T è la L-teoria con un insieme vuoto di assiomi, allora ogni L-struttura è modello di T, e pertanto si ha $\models \phi$ se e solo se $T \models \phi$.

Proposizione 5.10 *Sia T una L-teoria e siano α e β due L-formule chiuse. Allora $T \models \alpha \to \beta$ se e solo se $T, \alpha \models \beta$, dove con la notazione "T, α" abbiamo indicato la L-teoria che ha come assiomi la formula α e tutti gli assiomi di T. Questa equivalenza traduce il fatto intuitivo che dimostrare $\alpha \to \beta$ equivale a dimostrare β prendendo come ulteriore ipotesi α.*

Osservazione 5.11 La precedente proposizione non si estende al caso in cui α e β non siano chiuse perchè ci sono dei quantificatori universali sottointesi di cui tenere conto. Ad esempio $x = 0 \models y = 0$ significa $\forall x(x = 0) \models \forall y(y = 0)$, che esprime una affermazione vera. Invece $\models x = 0 \to y = 0$ significa $\models \forall xy(x = 0 \to y = 0)$, che è falso.

Corollario 5.12 *Se T è una teoria che ha come assiomi un numero finito di formule chiuse $\phi_1, \ldots, \phi_k$, allora $T \models \psi$ se e solo se $\models \phi_1 \wedge \ldots \wedge \phi_k \to \psi$.*

Dim. È facile dare una dimostrazione applicando direttamente le definizioni. Alternativamente possiamo applicare k volte la Proposizione 5.10 ottenendo che $T \models \psi$ se e solo se $\models \phi_1 \to (\phi_2 \to (\ldots (\to \phi_k \to \psi)))$. Per concludere basta notare che $A \to (B \to C)$ equivale a $(A \wedge B) \to C)$. QED

Il problema di stabilire se una data formula ψ segue dagli assiomi di una teoria T con un numero finito di assiomi (chiusi), si riconduce quindi al problema di stabilire se una certa altra formula a lei associata è logicamente valida. Il problema di determinare quali siano le formule logicamente valide acquista quindi una grande importanza. Purtroppo non esiste un algoritmo generale per stabilire se una formula è logicamente valida (Teorema di Church).

5.2 Teorie complete

Definizione 5.13 Una L-teoria T è *completa* (semanticamente) se innanzitutto ha un modello e inoltre per ogni L-formula chiusa ϕ, si ha $T \models \phi$ oppure $T \models \neg\phi$ (e non entrambe, altrimenti T non sarebbe semanticamente coerente).

Detto informalmente, una teoria è completa se è in grado di stabilire la verità o la falsità di qualsiasi enunciato, non lasciandone alcuno indeciso.

Osservazione 5.14 Una teoria T è completa se, preso un qualsiasi enunciato ϕ, o ϕ è vero in tutti i modelli di T, oppure $\neg\phi$ è vero in tutti i modelli di T. Non può capitare che ϕ sia vero in qualche modello e falso in un altro.

Esempio 5.15 Sia T la teoria dei gruppi, ovvero la teoria che ha come assiomi $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, $x \cdot 1 = x$, $1 \cdot x = 1$, $x \cdot x^{-1} = 1$, $x^{-1} \cdot x = 1$, formulati in un linguaggio con un simbolo di costante 1 per l'elemento neutro, un simbolo di funzione binaria $\cdot$ per l'operazione di gruppo, e un simbolo di funzione unario per l'inverso. Un gruppo è, per definizione, un modello di T. La teoria T non è completa. Sia infatti ϕ l'enunciato $\forall x, y(x \cdot y = y \cdot x)$, che esprime la legge commutativa. Poiché esistono sia gruppi commutativi che non commutativi, non si ha nè $T \models \phi$ nè $T \models \neg\phi$.

Un esempio di gruppo non commutativo è il gruppo delle matrici 2×2, dove 1 è intepretato come la funzione identità, e $\cdot$ come la moltiplicazione riga per colonne di matrici. Un esempio di gruppo commutativo è il gruppo additivo dei numeri interi, dove il simbolo $\cdot$ viene intepretato come la somma, e il simbolo 1 come lo zero (siamo liberi di farlo!).

Definizione 5.16 Un esempio di teoria completa è il seguente. Sia M una L-struttura (ad esempio un dato gruppo), e sia $Th(M)$ la teoria che ha come assiomi tutti gli L-enunciati veri in M. Allora $Th(M)$ è una L-teoria completa chiamata *teoria completa della struttura* M. L'esempio è un po' artificioso in quanto si tratta di una teoria completa di cui gli assiomi non sono dati esplicitamente.

Esercizio 5.17 Una L-teoria T è completa se e solo se per ogni coppia di L-enunciati α e β si ha: $T \models \alpha \vee \beta$ se e solo se $T \models \alpha$ o $T \models \beta$.

Esercizio 5.18 Una teoria T è completa (nel senso semantico) se è soddisfacibile e se comunque si prenda un suo modello M si ha che $Th(M)$ equivale a T.

5.3 Teorie deduttivamente chiuse

Definizione 5.19 Una L-teoria T si dice *deduttivamente chiusa* (da un punto di vista semantico) se l'insieme $\{\phi \mid T \models \phi\}$ delle sue conseguenze, coincide con l'insieme dei suoi assiomi.

Esercizio 5.20 Una teoria con un numero finito di assiomi, come ad esempio la teoria i cui assiomi sono gli assiomi dei gruppi, non è mai deduttivamente chiusa. Tuttavia ogni teoria T è equivalente ad una teoria T' deduttivamente chiusa: basta prendere come insieme di assiomi per T' l'insieme $\{\phi \mid T \models \phi\}$ (il lettore può fare per esercizio le dovute verifiche).

Abbiamo visto come da una teoria T possiamo ottenere una classe di L-strutture semplicemente prendendo la classe $Mod(T)$ dei suoi modelli. È possibile anche fare il percorso inverso, partendo da una classe di L-strutture, per ottenere una L-teoria.

Definizione 5.21 Data una classe K di L-strutture indichiamo con $Th(K)$ la L-teoria che ha come assiomi gli enunciati che sono veri in ogni struttura $\mathcal{A} \in K$.

Esercizio 5.22 La teoria $Th(K)$ sopra definita è deduttivamente chiusa. Inoltre ogni teoria deduttivamente chiusa T è della forma $Th(K)$ per una opportuna classe K di L-strutture: basta prendere $K = Mod(T)$ e osservare che $Th(Mod(T)) = \{\phi \mid T \models \phi\}$.

La seguente definizione e il conseguente esercizio mettono in luce una simmetria tra teorie e classi di strutture.

Definizione 5.23 Sia K una classe di L-strutture. Diciamo che K è una classe elementare se per qualche L-teoria T si ha $K = Mod(T)$. Ad esempio la classe dei gruppi è elementare.

Esercizio 5.24 L'operazione $T \mapsto Mod(T)$ porta da teorie a classi elementari di strutture, mentre $K \mapsto Th(K)$ porta da classi di strutture a teorie deduttivamente chiuse. Se restringiamo la prima operazione a teorie deduttivamente chiuse, e la seconda operazione a classi elementari di strutture, allora le due operazioni diventano l'una l'inversa dell'altra. In altre parole per una teoria deduttivamente chiusa T abbiamo $T = Th(Mod(T))$ (mentre per T arbitraria in generale vale solo l'inclusione "$\subseteq$") e per una classe elementare di strutture K abbiamo $K = Mod(Th(K))$ (mentre per K arbitraria in generale vale solo l'inclusione "$\subseteq$").

Dall'Esercizio 5.18 segue:

Osservazione 5.25 Sia L-teoria T semanticamente coerente e deduttivamente chiusa. Allora T è completa se e solo se preso un qualsiasi suo modello M si ha $T = Th(M)$ (ricordiamo che $Th(M)$ è la teoria che ha come assiomi tutte gli enunciati veri in M).

Esercizio 5.26 Sia T una L-teoria semanticamente coerente e deduttivamente chiusa. Allora T è completa se e solo se è massimale tra le teorie semanticamente coerenti, cioè non è possibile ampliare l'insieme dei suoi assiomi in modo da ottenere una teoria che continua ad essere semanticamente coerente.

6 Insiemi di Hintikka

Gli insiemi di Hintikka sono usati nella dimostrazione di completezza di vari sistemi dimostrativi (vedi sezione sul sistema dimostrativo di Hilbert-Frege).

Definizione 6.1 (Insiemi di Hintikka) Sia T un insieme di L-formule chiuse. Diciamo che T è un insieme di Hintikka (per L) se per ogni scelta di L-formule chiuse ϕ, ψ si ha:

1. se $\phi \in T$, allora $\neg\phi \notin T$,
2. se $\neg\neg\phi \in T$, allora $\phi \in T$,
3. se $\phi \wedge \psi \in T$, allora $\phi \in T$ e $\psi \in T$,
4. se $\neg(\phi \wedge \psi) \in T$, allora $\neg\phi \in T$ o $\neg\psi \in T$,
5. se $\phi \vee \psi \in T$, allora $\phi \in T$ o $\psi \in T$,
6. se $\neg(\phi \vee \psi) \in T$, allora $\neg\phi \in T$ e $\neg\psi \in T$,
7. se $\phi \to \psi \in T$, allora $\neg\phi \in T$ o $\psi \in T$,
8. se $\neg(\phi \to \psi) \in T$, allora $\phi \in T$ e $\neg\psi \in T$,
9. se $\forall x\phi(x) \in T$, allora per ogni L-termine chiuso t, $\phi(t) \in T$,
10. se $\neg\forall x\phi(x) \in T$, allora esiste un L-termine chiuso t tale che $\neg\phi(t) \in T$,
11. se $\exists x\phi(x) \in T$, allora esiste un L-termine chiuso t, tale che $\phi(t) \in T$,
12. se $\neg\exists x\phi(x) \in T$, allora per ogni L-termine chiuso t, $\neg\phi(t) \in T$.

Per linguaggi senza simbolo di uguaglianza $=$ possiamo fermarci qui. Altrimenti dobbiamo aggiungere le seguenti proprietà dell'uguaglianza:

1. (riflessività) per ogni L-termine chiuso t, $t = t \in T$,
2. (sostituibilità) per ogni L-formula $\phi(x)$ e termini chiusi t e t', se $t = t' \in T$, allora $\phi(t) \in T$ se e solo se $\phi(t') \in T$.

Nella ultima clausola possiamo anche limitarsi a formule atomiche $\phi(x)$.

Definizione 6.2 Un *insieme di Hintikka completo* è un insieme di Hintikka tale che per ogni L-formula chiusa ϕ, o ϕ o la sua negazione $\neg\phi$ appartengano a T (e non tutte e due, altrimenti non sarebbe di Hintikka).

Esercizio 6.3 Si consideri un linguaggio senza simbolo di uguaglianza nella segnatura $L = \{R, c\}$, dove R è un simbolo di relazione binario e c è un simbolo di costante. Si trovi un insieme di Hintikka finito contenente la formula $\forall x\exists y(R(x,y) \vee R(y,x))$. Si dimostri che se ampliamo L con l'aggiunta di un simbolo di funzione f, qualsiasi insieme di Hintikka contenente la formula sopra data è infinito.

Teorema 6.4 *Ogni insieme di Hintikka T ha un modello M. Inoltre possiamo prendere M in modo tale che ogni elemento del dominio di M è l'interpretazione di un termine chiuso della segnatura L di T.*

Dim. Per semplicità consideriamo prima il caso di linguaggi senza il simbolo di uguaglianza né simboli di funzione. In questo caso gli unici termini chiusi di L sono le costanti. Prendiamo come $dom(M)$ l'insieme delle costanti di L. Dato un simbolo di relazione R di arità n, definiamo la sua interpretazione $R^M \subseteq dom(M)^n$ come l'insieme di tutte le n-uple $(c_1, \ldots, c_k)$ tali che $R(c_1, \ldots, c_n) \in T$. In questo modo abbiamo definito una L-struttura che rende veri tutti gli enunciati atomici in T, e falsi gli enunciati atomici non in T. Sia ora ϕ un arbitrario L-enunciato. Usando le proprietà di Hintikka segue per induzione sul numero dei connettivi di ϕ che se $\phi \in T$, allora $M \models \phi$ (se T è un insieme di Hintikka completo sarà anche vero che se $\phi \notin T$, allora $M \models \neg\phi$).

Consideriamo ad esempio il caso $\neg\phi \in T$. Dalle proprietà di Hintikka segue che $\phi \notin T$. Se ϕ è atomica, concludiamo che $M \models \neg\phi$ per definizione di M. Se invece ϕ non è atomica, allora deve cominciare con un connettivo. Supponiamo ad esempio che tale connettivo sia $\vee$, cioè $\neg\phi = \neg(\alpha \vee \beta)$. Usando le proprietà di Hintikka abbiamo $\neg\alpha \in T$ e $\neg\beta \in T$. Per induzione possiamo concludere $M \models \neg\alpha$ e $M \models \neg\beta$, da cui poi segue $M \models \neg(\alpha \vee \beta)$.

Lasciamo al lettore la verifica degli altri casi. Questo conclude la dimostrazione nel caso il linguaggio non ha simboli di funzione e il simbolo di uguaglianza.

Consideriamo ora il caso in cui L può contenere il simbolo di uguaglianza e simboli di funzione. Ricordiamo che il simbolo di uguaglianza deve essere interpretato come la relazione di uguaglianza, quindi se $t = t' \in T$ dobbiamo fare in modo che t e t' siano interpretati con lo stesso elemento del modello M che vogliamo costruire.

A tal fine prendiamo come $dom(M)$ l'insieme degli L-termini chiusi quozientato rispetto alla relazione di equivalenza $\sim$ definita da $t \sim t'$ sse $t = t' \in T$. Segue dalle proprietà di Hintikka dell'uguaglianza che $\sim$ è in effetti una relazione di equivalenza. Indichiamo con $t/\sim$ la classe di equivalenza di t rispetto a $\sim$.

Dato un simbolo di funzione f di L di arità n definiamo la sua interpretazione $f^M : dom(M)^n \to dom(M)$ ponendo: $f^M(t_1/\sim, \ldots, t_n/\sim) = f(t_1, \ldots, t_n)/\sim$. Questa definizione è be posta perchè dalla proprietà di Hintikka di sostituibilità (applicata ripetute volte) segue che se $t_1 \sim t'_1, \ldots, t_n \sim t'_n$ allora $f(t_1, \ldots, t_n) \sim f(t'_1, \ldots, t'_n)$.

Resta solo da definire l'interpretazione R^M dei simboli di relazione di L (se ve ne sono). Se R ha arità n e $t_1, \ldots, t_n$ sono termini chiusi, poniamo $(t_1/\sim, \ldots, t_n/\sim) \in R^M$ sse $R(t_1, \ldots, t_n) \in T$. Questo è ben posto per la sostitutività. Abbiamo così definito una L-struttura M.

Per induzione sulla lunghezza dei termini chiusi t, segue che $t^M = t/\sim$. Quindi se $t = t' \in T$, allora $t^M = t/\sim = t'/\sim = t'^M$, e quindi $M \models t = t'$ (si noti che per abuso di linguaggio abbiamo usato "=" sia come simbolo che come la vera relazione di uguaglianza). Viceversa se $t = t' \notin T$, allora $t/\sim \neq t'/\sim$ e $M \models t \neq t'$. Quindi M rende veri per lo meno gli enunciati di T della forma $t = t'$, e falsi gli enunciati della forma $t = t'$ che non sono in T. Similmente si verifica

che $R(t_1, \ldots, t_n) \in T$ sse $M \models R(t_1, \ldots, t_n)$. Quindi tra gli enunciati atomici (senza connettivi) M rende veri tutti e soli quelli che sono in T. Ragionando per induzione sulla complessità della formula, usando le proprietà di Hintitkka per i passi induttivi, vediamo che ogni $\phi \in T$ (non necessariamente atomica) è vera M. Consideriamo nel dettaglio il caso in cui ϕ è della forma $\exists x \theta(x)$. Se $\phi \in T$, allora essendo T di Hintikka deve esistere un termine chiuso t tale che $\theta(t) \in T$. Per induzione $\theta(t)$ è vero nel modello M. Ma allora deve essere vero anche $\exists x \theta(x)$. QED

Corollario 6.5 *Se un insieme di L-enunciati T è incluso in un insieme T' di Hintikka (possibilmente in un linguaggio L' più esteso), allora T ha un modello. Se inoltre T è incluso in un insieme di Hintikka finito, allora T ha un modello finito.*

Dim. Poichè T' è di Hintikka T' ha un modello M'. Ne segue che T ha come modello la restrizione di M' al linguaggio di T. La parte sulla finitezza è lasciata al lettore. QED

Il precedente corollario è in effetti una condizione necessaria e sufficiente affinchè T abbia un modello. In effetti se T ha un modello M, il diagramma elementare di M, definito piú sotto, è un insieme di Hintikka contenente T.

Definizione 6.6 Data una L-struttura M definiamo la teoria $ED(M)$, detta *diagramma elementare* di M, come la teoria nel linguaggio $L[M]$ ottenuto da L aggiungendo un simbolo di costante c_m per ogni $m \in dom(M)$, e avente come assiomi tutti gli $L[M]$-enunciati che risultano veri in M quando si interpreta c_m con m.

7 Completezza

Data una L-teoria T e una formula ϕ, vogliamo definire il concetto di "dimostrazione formale di ϕ da T". Mostreremo che esiste una tale dimostrazione formale se e solo se $T \models \phi$ (ricordiamo che ciò significa: ogni modello di T è modello di ϕ). Quindi o esiste una dimostrazione formale di ϕ da T, oppure esiste un contromodello, ovvero una L-struttura in cui tutti gli assiomi di T sono validi, ma in cui ϕ non vale.

7.1 Il sistema dimostrativo di Hilbert-Frege

Nel sistema di Hilbert-Frege una dimostrazione formale di ϕ da T consiste di una successione finita di formule di cui l'ultima è ϕ, mentre le altre sono o assiomi di T, o "assiomi logici", oppure seguono da precedenti formula tramite una "regola di inferenza". Cominciamo con gli assiomi logici.

7.1.1 Assiomi logici

Sia L una segnatura, siano α, β, γ etc. arbitrarie L-formule (possibilmente aperte). Abbiamo i seguenti schemi di assiomi logici.

Assiomi proposizionali. Ogni tautologia è un assioma logico, dove per tautologia intendiamo una L-formula che si ottiene da una tautologia del calcolo proposizionale sostituendo le variabili proposizionali con arbitrarie L-formule (non necessariamente chiuse). Ad esempio le seguenti sono tautologie per ogni scelta di α, β, γ.

A0) $\alpha \to \alpha$

A1) $\alpha \to (\beta \to \alpha)$

A2) $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \gamma) \to (\alpha \to \gamma))$

A3) $((\neg\beta \to \neg\alpha) \to ((\neg\beta \to \alpha) \to \beta))$

Assiomi dell'uguaglianza.

Per ogni simbolo di funzione f in L (di arità n) e ogni simbolo di relazione R in L (di arità n) abbiamo i seguenti assiomi.

Riflessività) $x = x$.

Simmetria) $x = y \to y = x$.

Transitività) $x = y \to (y = z \to x = z)$.

Congruenza) $x_1 = y_1 \to (\ldots \to (x_n = y_n \to (f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n))))$.

Sostituibilità) $x_1 = y_1 \to (\ldots \to (x_n = y_n \to (R(x_1, \ldots, x_n) \to R(y_1, \ldots, y_n))))$.

Alternativamente avremmo potuto prendere come assiomi tutte le L-formule della forma $t = t$ (dove t è un L-termine), più tutte le formule della forma $t_1 = t_2 \wedge \phi(t_1) \to \phi(t_2)$ e quelle della forma $t_1 = t_2 \wedge \phi(t_2) \to \phi(t_1)$.

Assiomi sui quantificatori.

Sia α una formula e sia t un termine sostituibile al posto di una variabile x in α. Abbiamo gli assiomi.

- $\alpha(t) \to \exists x \alpha(x)$.
- $\forall x \alpha(x) \to \alpha(t)$.

7.1.2 Regole di inferenza

- (modus ponens) Dalle due premesse α e $\alpha \to \beta$ posso trarre la conclusione β.

  Notazione: $\frac{\alpha, \alpha \to \beta}{\beta}$.

- ($\forall$-introduzione) Sia x una variabile che non occorre libera nella formula α. Dalla premessa $\alpha \to \beta$ posso trarre la conclusione $\alpha \to \forall x\beta$.

  Notazione: $\frac{\alpha \to \beta}{\alpha \to \forall x \beta}$.

- ($\exists$-introduzione) Sia x una variabile che non occorre libera nella formula α. Dalla premessa $\alpha \to \beta$ posso trarre la conclusione $\exists x\alpha \to \beta$.

  Notazione: $\frac{\alpha \to \beta}{\exists x \alpha \to \beta}$.

Alcuni degli assiomi e regole sono ridondanti. Ad esempio si sarebbe potuto definire $\exists x\alpha$ come $\neg\forall x\neg\alpha$ ed eliminare tutti gli assiomi e regole che riguardano $\exists$. Viceversa si sarebbe potuto definire $\forall x\alpha$ come $\neg\exists x\neg\alpha$ ed eliminare gli assiomi e regole del $\forall$. Cosí facendo non si perde nulla nel senso che gli assiomi e regole che sono stati omessi diventano derivabili dagli altri.

7.1.3 Teoremi

Sia T una L-teoria. I teoremi di T si definiscono induttivamente nel modo seguente (nel sistema di Hilbert-Frege): tutti gli assiomi di T e tutti gli assiomi logici (nella segnatura L) sono teoremi di T. Se le premesse di una regola di inferenza sono teoremi di T, anche la sua conclusione è un teorema di T. Niente altro è un teorema di T.

Se ϕ è un teorema di T, scriviamo $T \vdash \phi$. Se T è la L-teoria con un insieme vuoto di assiomi scriviamo $\vdash \phi$ per $T \vdash \phi$. Ciò significa che ϕ è deducibile usando solamente gli assiomi logici.

7.1.4 Dimostrazioni formali

Una *dimostrazione formale* di ϕ da una L-teoria T (nel sistema Hilbert-Frege) è una sequenza finita di L-formule $(\alpha_0, \alpha_1, \ldots, \alpha_n)$ tale che $\alpha_n = \phi$ e ogni formula o è un assioma di T, o è un assioma logico, o segue da formule precedenti nella sequenza tramite una regola di inferenza. È facile verificare che ϕ è un teorema di T se e solo se esiste una dimostrazione di ϕ da T.

7.1.5 Alcuni utili metateoremi

Lemma 7.1 *(compattezza, versione sintattica) Se $T \vdash \phi$, esiste una sottoteoria finita (cioè con un numero finito di assiomi) T' di T tale che $T' \vdash \phi$. In particolare , prendendo $\phi = \bot$, se T non è HF-coerente anche una sua sottoteoria finita non lo è.*

Dim. Basta osservare che una dimostrazione formale può usare solo un insieme finito di assiomi. QED

Esercizio 7.2

$T \vdash \alpha(x)$ se e solo se $T \vdash \forall x\alpha(x)$.

Dim. Una delle implicazioni segue dall'assioma $\forall x \alpha(x) \to \alpha(t)$ prendendo $t = x$. L'altra direzione segue dalla regola di inferenza $\frac{\phi \to \alpha}{\phi \to \forall x \alpha}$ prendendo come ϕ una formula dimostrabile in T e che non contiene la x libera e poi applicando il modus ponens e opportune tautologie (completare per esercizio). QED

Più difficile è il seguente:

Esercizio 7.3 Ogni tautologia si può dedurre dai quattro schemi di tautologia A0 - A3 sopra elencati, usando solamente la regola di Modus Ponens.

Definizione 7.4 Diciamo che una L-formula α è una conseguenza tautologica di L-formule $\beta_1, \ldots, \beta_n$ se $(\beta_1 \wedge \ldots \beta_n) \to \alpha$ è una tautologia, o equivalentemente $\beta_1 \to (\beta_2 \to \ldots \to (\beta_n \to \alpha))$ è una tautologia.

Usando ripetute volte il modus ponens si dimostra:

Esercizio 7.5 Se $T \vdash \beta_1, \ldots, T \vdash \beta_n$ e α è conseguenza tautologica di $\beta_1, \ldots, \beta_n$, allora $T \vdash \alpha$.

7.2 Teorema di correttezza per il calcolo dei predicati

Mostreremo che gli assiomi e le regole di inferenza che abbiamo dato corrispondono a metodi di ragionamento corretti.

Teorema 7.6 *(Correttezza degli assiomi logici) Gli assiomi logici (su una segnatura L) sono logicamente validi (cioè universalmente veri in ogni L-struttura).*

Dim. La dimostrazione userà a livello di "metateoria" gli stessi principi logici (se non ancora più complicati) di quelli di cui si vuole giustificare la correttezza a livello di "teoria oggetto" (la teoria oggetto è il sistema di Hilbert-Frege, la metateoria sono i ragionamenti che facciamo, al di fuori di tale sistema, per dimostrare proprietà del sistema). Se non altro per illustrare la differenza tra i vari livelli linguistici diamo comunque una dimostrazione.

Tralasciamo la verifica per gli assiomi proposizionali.

Il fatto che gli assiomi della uguaglianza siano logicamente validi segue semplicemente dal fatto che nella semantica di Tarski abbiamo imposto che il simbolo $=$ venga interpretato come la relazione di uguaglianza, la quale gode ovviamente di tutte le proprietà espresse dagli assiomi della uguaglianza.

Restano da verificare gli assiomi che riguardano i quantificatori. Verifichiamo solamente la validità dell'assioma $\forall x \alpha(x) \to \alpha(t)$ dove t è un termine sostituibile per x in α. È qui che interviene in modo cruciale la definizione di "sostituibile". Osserviamo che la formula $\forall x \alpha(x) \to \alpha(t)$ non è necessariamente un enunciato in quanto in primo luogo il termine t potrebbe contenere delle variabili, e in secondo luogo la formula $\alpha(x)$ stessa può contenere delle variabili libere diverse da x. Supponiamo che le variabili libere di $\forall x \alpha(x) \to \alpha(t)$ siano incluse in $\{y_1, \ldots, y_n\}$ (non escludiamo il caso in cui qualche y_i coincida con x che può

verificarsi se t contiene la x). Dobbiamo mostrare che per ogni L-struttura M, abbiamo

$$M \models \forall y_1, \ldots, y_n(\forall x \alpha(x) \to \alpha(t)) \tag{1}$$

Poichè t è sostituibile per x in α, le variabili di t sono incluse in $\{y_1, \ldots, y_n\}$. Infatti se t contenesse qualche altra variabile z, allora z non non potendo essere libera in $\forall x \alpha(x) \to \alpha(t)$ (se no sarebbe una delle y_i), non può essere libera nemmeno in $\alpha(t)$ e pertanto deve essere stata legata dopo la sostituzione di t in $\alpha(x)$, contraddicendo il fatto che t era sostituibile.

Per la semantica di Tarski (1) equivale a:

Per ogni $a_1, \ldots, a_n \in dom(M)$,

$$M \models (\forall x \alpha(x) \to \alpha(t))^s \tag{2}$$

dove s è la sostituzione $(a_1/y_1, \ldots, a_n/y_n)$.

La (2) equivale a

$$M \models ((\forall x \alpha(x))^s \to \alpha^s(t^s)) \tag{3}.$$

Ora poichè le variabili di t sono incluse in $\{y_1, \ldots, y_n\}$, t^s è un termine senza variabili, e quindi esiste $b \in dom(M)$ con $b = M(t^s)$. Ne segue che $M \models \alpha^s(t^s) \leftrightarrow \alpha^s(b)$, e quindi (3) equivale a:

$$M \models (\forall x \alpha^s(x) \to \alpha^s(b)) \tag{4}$$

La verità di questa ultima asserzione segue dalla semantica di Tarski del $\forall$ applicata alla formula con parametri α^s. QED

Cosa vuol dire che una regola di inferenza corrisponde a un metodo di ragionamento corretto? La seguente definizione fornisce una possibile risposta.

Definizione 7.7 Diciamo che una regola di inferenza è *corretta*, se ogniqualvolta le premesse della regola sono universalmente vere in una L-struttura M, allora la conclusione è universalmente vera in M.

Osservazione 7.8 La correttezza di una regola equivale alla validità logica di un enunciato corrispondente, cioè l'enunciato che esprime che la congiunzione delle quantificazioni universali delle premesse della regola implica la quantificazione universale della conclusione della regola.

Teorema 7.9 *(Correttezza delle regole) Le regole di inferenza del sistema di Hilbert-Frege sono corrette.*

Dim. Consideriamo solo la regola $\frac{\alpha \to \beta}{\alpha \to \forall x \beta}$ dove x non appare libera in α. Supponiamo che le variabili libere di α e β siano incluse in $\{y_1, \ldots, y_n\}$. Supponiamo che

$$M \models \forall y_1, \ldots, y_n(\alpha \to \beta) \tag{1}.$$

Dobbiamo verificare che $M \models \forall y_1, \ldots, y_n(\alpha \to \forall x\beta)$. Ciò significa che per ogni valutazione delle variabili $s\colon \{y_1, \ldots, y_n\} \to dom(M)$

$$M \models \alpha^s \to (\forall x\beta)^s \tag{2}$$

Poichè x non occorre libera nè in α (per ipotesi) nè in $\forall x\beta$ (perchè è quantificata da $\forall x$), la (2) equivale a

$$M \models \alpha^{s'} \to (\forall x\beta)^{s'}$$

dove $dom(s') = dom(s) \setminus \{x\}$ e s' coincide con s nel dominio comune. Notiamo che $(\forall x\beta)^{s'}$ coincide con $(\forall x\beta^{s'})$ (usando $x \notin dom(s')$). Supponiamo per assurdo che $M \models \alpha^{s'}$ e che $M \not\models \forall x\beta^{s'}$. Allora esiste $a \in dom(M)$ tale che $M \not\models \beta^{s'}(a/x)$. Sia f l'unione delle sostituzioni s' e (a/x). Allora $M \not\models \beta^f$. D'altra parte $M \models \alpha^f$ (perché $M \models \alpha^{s'}$ e le due formule con parametri α^f e $\alpha^{s'}$ coincidono in quanto x non è libera in α). Ora $M \models \alpha^f$ e $M \not\models \beta^f$ contraddicono la (1). QED

Teorema 7.10 *(Teorema di correttezza) Se $T \vdash \phi$, allora $T \models \phi$.*

Dim. Supponiamo $T \vdash \phi$ e sia M un modello di T. Ne segue che tutti gli assiomi di T sono universalmente veri in M. D'altra parte anche gli assiomi logici sono universalmente veri in M (in quanto sono universalmente veri in ogni L-struttura) e le regole di inferenza preservano la universale verità in M. Quindi tutti i teoremi di T sono universalmente veri in M e in particolare $M \models \phi$. QED

In particolare prendento come T la L-struttura senza assiomi non-logici, abbiamo che se $\vdash \phi$ allora $\models \phi$, cioè ϕ è logicamente valida.

Definizione 7.11 Sia $\perp$ una formula chiusa tale che $\vdash \neg \perp$, ad esempio una formula chiusa della forma $\perp = A \wedge \neg A$.

Definizione 7.12 1. T è HF-coerente se e solo se $T \nvdash \perp$.

2. T è HF-completa se è HF-coerente e per ogni L-formula chiusa ϕ si ha $T \vdash \phi$ oppure $T \vdash \neg\phi$.

Dal teorema di correttezza segue:

Corollario 7.13 *Se T ha un modello, allora T è HF-coerente.*

7.3 Teorema di deduzione

Teorema 7.14 *Sia L una segnatura, β una L-formula, e α una L-formula chiusa. Se $T \cup \{\alpha\} \vdash \beta$, allora $T \vdash \alpha \to \beta$ (il viceversa è semplice).*

Dim. Sia $(\beta_1, \ldots, \beta_n)$ una dimostrazione formale di β da $T \cup \{\alpha\}$. Mostreremo per induzione su $i \leq n$ che $T \vdash \alpha \to \beta_i$. Assumiamo per ipotesi induttiva che per ogni $j < i$, $T \vdash \alpha \to \beta_j$. Per mostrare che $T \vdash \alpha \to \beta_i$ distinguiamo vari casi.

Caso 1. β_i è un assioma logico oppure un assioma di T. Ne segue che $T \vdash \beta_i$ e quindi per conseguenza tautologica $T \vdash \alpha \to \beta_i$.

Caso 2. β_i è α. Poichè $\alpha \to \alpha$ è uno degli assiomi logici del sistema HF, $T \vdash \alpha \to \beta_i$.

Caso 3. β_i segue da due formule precedenti per modus ponens, diciamo da β_j e β_k (con $j, k < i$) dove $\beta_k = \beta_j \to \beta_i$. Per ipotesi induttiva abbiamo $T \vdash \alpha \to \beta_j$ e $T \vdash \alpha \to (\beta_j \to \beta_i)$. Per conseguenza tautologica $T \vdash \alpha \to \beta_i$.

Caso 4. β_i segue da β_j per $\exists$-introduzione ($j < i$). Allora β_j è della forma $\gamma \to \delta$ e β_i è $\exists x\gamma \to \delta$, dove $x \notin Fv(\delta)$. Per ipotesi induttiva $T \vdash \alpha \to (\gamma \to \delta)$. Per conseguenza tautologica $T \vdash \gamma \to (\alpha \to \delta)$. Poichè α è un enunciato, α non contiene la x libera, e quindi $x \notin Fv(\alpha \to \delta)$. Possiamo quindi applicare la regola di $\exists$-introduzione per concludere $T \vdash \exists x\gamma \to (\alpha \to \delta)$ e quindi per conseguenza tautologica $T \vdash \alpha \to (\exists x\gamma \to \delta)$, ovvero $T \vdash \alpha \to \beta_i$.

Caso 5. β_i segue da β_j per $\forall$-introduzione. Simile al caso 3. QED

Osservazione 7.15 Il teorema di deduzione non vale se α non è un enunciato. Ad esempio $\{x = 0\} \vdash \{y = 0\}$, ma $\not\vdash \{x = 0\} \to \{y = 0\}$.

7.4 Completezza del sistema di Hilbert-Frege

Per HF-dimostrazione intendiamo una dimostrazione nel sistema di Hilbert-Frege.

Definizione 7.16 T è una *teoria di Henkin* se e solo se per ogni $L(T)$-enunciato della forma $\exists x\beta(x)$, esiste una costante $c \in L(T)$, tale che $T \vdash \exists x\beta(x) \to \beta(c)$.

Esercizio 7.17 Gli assiomi logici e le regole di inferenza del sistema Hilbert-Frege sono tali che rimpiazzando un simbolo di costante c con una veriabile y in un assioma o una regola di inferenza in cui non occorre la y, si ottiene di nuovo un assioma o una regola del sistema. L'ipotesi che y non occorra nell'assioma o regola è essenziale: $\forall z\phi(z) \to \phi(c)$ è un assioma logico del sistema di Hilbert-Frege, mentre $\forall z\phi(z) \to \phi(y)$ non lo è a meno che y non sia sostituibile per z in ϕ.

Lemma 7.18 *(Lemma sulle costanti) Se c è un simbolo di costante di $L(T)$ che non viene menzionato in alcun assioma di T, e se $T \vdash \alpha(c/x)$, allora $T \vdash \forall x\alpha(x)$. Inoltre è possibile dare una HF-dimostrazione di $\forall x\alpha(x)$ da T che non menziona in alcuna sua formula la costante c.*

Dim. Sia p una dimostrazione di $\alpha(c)$ da T. Rimpiazzando ovunque nella dimostrazione c con una nuova variabile y che non appare nè libera nè legata nelle formule di p, otteniamo una dimostrazione di $\alpha(y)$ da T. Per verificare ciò usiamo, oltre al fatto che c non è menzionata negli assiomi logici di T, anche l'esercizio precedente. Per concludere notiamo che da una dimostrazione di $\alpha(y)$ se ne ottiene una di $\forall y\alpha(y)$ per un risultato precedente, e da qui una di $\alpha(x)$ per particolarizzazione, e infine una di $\forall x\alpha(x)$. QED

Definizione 7.19 Un *un enunciato di Henkin* è un enunciato del tipo $\exists x\alpha(x) \to \alpha(c)$ dove c è un simbolo di costante.

Lemma 7.20 *Se T è una teoria HF-coerente e T' è ottenuta da T aggiungendo ai suoi assiomi un enunciato di Henkin $\exists x\alpha(x) \to \alpha(c)$, dove c è un nuovo simbolo di costante che non appartenere alla segnatura L di T, allora T' è HF-coerente. (La segnatura di T' è data da $L' = L \cup \{c\}$).*

Dim. Se T' è incoerente, allora $T \cup \{\exists x\alpha \to \alpha(c)\} \vdash_{L'} \bot$ dove $\vdash_{L'}$ indica che la dimostrazione consiste di formule nella segnatura L'. Per il teorema di deduzione $T \vdash_{L'} (\exists x\alpha(x) \to \alpha(c)) \to \bot$. Per conseguenza tautologica $T \vdash_{L'} \exists x\alpha(x)$ e $T \vdash_{L'} \neg\alpha(c)$. Poichè c non compare nè in α nè tra gli assiomi di T, da $T \vdash_{L'} \exists x\alpha(x)$ possiamo dedurre $T \vdash_L \exists x\alpha(x)$ (rimpiazzando nella dimostrazione ogni occorrenza della variabile c con una variabile y che non compare nella dimostrazione), e da $T \vdash_{L'} \neg\alpha(c)$ otteniamo per il lemma sulle costanti $T \vdash_L \forall x\neg\alpha(x)$. D'altra parte $T \vdash_L \exists x\alpha$ e ne segue facilmente che T è incoerente (basta mostrare nel sistema HF che $\vdash \exists x\alpha \to \neg\forall x\neg\alpha$ e poi ragionare per conseguenza tautologica). QED

Lemma 7.21 *L'unione di una catena $\{T_i \mid i \in I\}$ di L-teorie HF-coerenti è HF-coerente.*

Dim. Sia $T = \bigcup_{i\in\omega} T_i$ e supponiamo che $T \vdash \bot$. Poichè una dimostrazione formale nel sistema HF può coinvolgere solo un numero finito di assiomi deve esistere un T_i che contiene tutti gli assiomi usati nella dimostrazione di $\bot$ da T, e quindi $T_i \vdash \bot$. QED

Lemma 7.22 *Se T è HF-coerente, esiste una teoria HF-coerente e di Henkin T_H, ottenuta aggiungendo a T un insieme di enunciati di Henkin, tale che $L(T) \subseteq L(T_H)$ e $Ax(T) \subseteq Ax(T_H)$.*

Dim. Definiamo una operazione tra teorie $T \mapsto T^*$ nel modo seguente. Sia L^* il linguaggio che si ottiene da $L = L(T)$ con l'aggiunta, per ogni enunciato di L della forma $\exists x\alpha$, di una corrispondente nuova costante che indicheremo $c(\exists x\alpha)$ (distinti enunciati corrispondendo a distinte costanti). Sia T^* la teoria formulata nel linguaggio L^* e i cui assiomi comprendono quelli di T e tutti

gli enunciati di Henkin della forma $\exists x\alpha(x) \to \alpha(c(\exists x\alpha)/x)$ dove $\exists x\alpha(x)$ è un enunciato di L.

Usando ripetutamente il Lemma precedente si dimostra che qualsiasi sotto-teoria finita di T^* è HF-coerente, quindi anche T^* è HF-coerente (in quanto una eventuale HF-dimostrazione di $\perp$ può usare solo un numero finito di assiomi).

Si noti che T^* non è necessariamente una teoria di Henkin perchè, pur essendo vero che tutti gli $\exists$-enunciati di $L(T)$ hanno una corrispondente costante di Henkin, cio' non è necessariamente vero per tutti gli $\exists$-enunciati di $L(T^*)$. Per porre rimedio a ciò dobbiamo iterare il procedimento $T \mapsto T^*$ infinite volte come segue.

Sia $T_0 = T, T_{n+1} = T_n^*$. Sia T_ω l'unione delle teorie T_n per $n \in \omega$. Poichè tutte le T_n sono coerenti lo è anche T_ω per il lemma precedente.

Per finire verifichiamo che T_ω è una teoria di Henkin. Sia infatti $\exists x\alpha$ un $\exists$-enunciato di $L(T_\omega)$. Poichè $\exists x\alpha$ puo' contenere solo un numero finito delle nuove costanti, esiste $n \in \omega$ tale che $\exists x\alpha$ è un enunciato di $L(T_n)$. Ma allora $\exists x\alpha(x) \to \alpha(c(\exists x\alpha)/x)$ è un assioma di T_{n+1} e quindi di T_ω. QED

Lemma 7.23 *Sia T una teoria HF-coerente e sia ϕ un L-enunciato. Allora almeno una delle due teorie $T \cup \{\phi\}$ e $T \cup \{\neg\phi\}$ (possibilmente anche tutte e due) è HF-coerente.*

Dim. Supponiamo per assurdo che $T, \phi \vdash \perp$ e $T, \neg\phi \vdash \perp$. Allora per il teorema di deduzione $T \vdash \phi \to \perp$ e $T \vdash \neg\phi \to \perp$, e quindi per conseguenza tautologica $T \vdash \perp$. QED

Lemma 7.24 *(Lemma di Lindembaum) Sia T una L-teoria HF-coerente. Allora esiste una teoria HF-coerente T' nello stesso linguaggio L, tale che per ogni L-enunciato ϕ abbiamo $\phi \in T'$ oppure $\neg\phi \in T'$. In particolare T' è HF-completa.*

Dim. Nel caso che L sia numerabile anche l'insieme degli L-enunciati lo sarà e possiamo procedere nel modo seguente. Sia $\{\phi_n \mid n \in \omega\}$ una enumerazione di tutti gli L-enunciati. Definiamo $T_0 = T$. Supponiamo induttivamente di aver già definito una teoria HF-coerente T_n. Per il lemma precedente sappiamo che almeno una delle due teorie $T_n \cup \{\phi_n\}$ e $T_n \cup \{\neg\phi_n\}$ è HF-coerente. Scegliamone una delle due che lo sia e chiamiamola T_{n+1}. Ora consideriamo la teoria $T_\omega = \bigcup_{n\in\omega} T_n$. Poiché l'unione di una catena di teorie HF-coerenti è HF-coerente T_ω è HF-coerente, e possiamo porre $T' = T_\omega$.

Nel caso in cui L non sia numerabile dobbiamo iterare la costruzione precedente nel transfinito, oppure fare appello al lemma di Zorn (se un insieme parzialmente ordinato gode della proprietà che ogni catena ha un maggiorante, allora esiste un elemento massimale). Applichiamo il lemma di Zorn alla classe di tutte le L-teorie HF-coerenti e contenenti T, ordinate per inclusione. Sappiamo che in questo ordine ogni catena ha un maggiorante (l'unione), e quindi esiste una teoria HF-coerente massimale T' contenente T. Tale T' ha le proprietà

richieste perché se no esisterebbe un L-enunciato ϕ tale che T' non contiene né ϕ né la sua negazione. Ma una delle teorie $T' \cup \{\phi\}$ e $T' \cup \{\neg\phi\}$ è HF-coerente, e questo contraddice la massimalità di T'. QED

Teorema 7.25 *(Teorema di completezza del sistema di Hilbert - Frege) Se una L-teoria T è HF-coerente, allora T è soddisfacibile.*

Dim. Applicando prima il Lemma 7.22 e poi il Lemma di Lindembaum 7.24 abbiamo che T è inclusa in una teoria T' di Henkin e HF-completa, in un linguaggio ampliato L'. In effetti i Lemmi ci forniscono una teoria T' con l'ulteriore proprietà che per ogni L-formula chiusa ϕ, o ϕ o la sua negazione appartengono agli assiomi di T'. Ne segue che T' è deduttivamente chiusa (in senso sintattico), cioè per ogni enunciato ϕ tale che $T' \vdash \phi$, si ha che ϕ appartiene agli assiomi di T' (altrimenti la sua negazione ci apparterrebbe e T' non sarebbe HF-coerente).

Per il teorema 6.4 basta mostrare che T' è un insieme di Hintikka (identifichiamo la teoria T' con l'insieme dei suoi assiomi). Per verificare la clausola relativa al quantificatore esistenziale supponiamo che $\exists x\phi(x) \in T'$. Essendo di Henkin, T' contiene l'assioma $\exists x\phi(x) \rightarrow \phi(c)$ per un certo simbolo di costante c. Dobbiamo mostrare che T' contiene $\phi(c)$. In caso contrario T' conterrebbe $\neg\phi(c)$, e questo è assurdo perchè allora per conseguenza tautologica T' conterrebbe $\neg\exists x\phi(x)$, contraddicendo il fatto che una teoria HF-coerente non può contenere al tempo stesso una formula e la sua negazione. Le verifica delle altre clausole nella definizione di insieme di Hintikka sono lasciate al lettore. QED

Corollario 7.26 *$T \vdash \phi$ se e solo se $T \models \phi$.*

Dim. Possiamo assumere che $T \cup \{\phi\}$ consista unicamente di formule chiuse (se no mettiamo dei quantificatori universali, e nulla cambia). La direzione $\rightarrow$ segue dal teorema di correttezza. Per l'altra direzione osserviamo che se $T \nvdash \phi$, allora $T, \neg\phi \nvdash \perp$ (se no per il teorema di deduzione $T \vdash \neg\phi \rightarrow \perp$ e per conseguenza tautologica $T \vdash \phi$). Dal teorema precedente segue ora che esiste un modello di $T, \neg\phi$, e quindi $T \not\models \phi$. QED

8 Compattezza

8.1 Teorema di compattezza

Teorema 8.1 *(Teorema di compattezza) Sia T una L-teoria e ϕ una L-formula.*

1. *Se $T \models \phi$, allora esiste una sottoteoria finita T' di T tale che $T' \models \phi$.*
2. *Se ogni sottoteoria finita di T ha un modello anche T ha un modello.*

Dim. 1. Per il teorema di completezza $T \models \phi$ equivale a $T \vdash \phi$, ovvero all'esistenza di una dimostrazione formale di ϕ da T. Poichè dimostrazione formale è una successione finita di formule, basta prendere come sottoteoria finita T' quella formata dagli assiomi che occorrono in una fissata dimostrazione formale di ϕ.

2. Il fatto che T non abbia modello equivale all'affermazione che $T \models \perp$ (si ricordi che $\perp$ denota una formula che equivale alla negazione di una tautologia). Ora basta applicare il punto 1. prendendo $\phi = \perp$. QED

8.2 Teorema di Löweinheim - Skolem verso l'alto

Teorema 8.2 *(Löweinheim - Skolem verso l'alto)*

1. *Sia T una L-teoria. Se per ogni intero positivo n esiste un modello M_n di T di cardinalità maggiore di n, allora T ha un modello infinito.*

2. *Se T ha un modello infinito, allora T ha modelli di cardinalità arbitrariamente grande.*

Dim. Supponiamo che per ogni n T abbia un modello di cardinalità maggiore di n. Sia κ un numero cardinale infinito e sia L' il linguaggio ottenuto da L con l'aggiunta di un insieme C di cardinalità κ di nuovi simboli di costante. Sia T' la L'-teoria i cui assiomi sono quelli di T più tutti gli assiomi della forma $c \neq c'$, dove c, c' sono costanti distinte di C. Dimostriamo innanzitutto che ogni sottoteoria finita S di T' ha un modello. A tal fine osserviamo che S può contenere solo un numero finito dei nuovi assiomi, ed esiste dunque un numero naturale n tale che i nuovi assiomi sono della forma $c_i \neq c_j$, per $1 \leq i < j \leq n$. Scegliamo un modello $\mathcal{A}$ di T di cardinalità $\geq n$, e consideriamo n elementi distinti $a_1, \ldots, a_n$ di $\mathcal{A}$. Sia $\mathcal{A}'$ la L'-struttura che espande $\mathcal{A}$ interpretando c_i con a_i. Tale $\mathcal{A}'$ è un modello di S. Per il teorema di compattezza possiamo concludere che T' ha un modello $\mathcal{B}$, che deve essere di cardinalità $\geq \kappa$ in quanto deve verificare tutti i nuovi assiomi $c \neq c'$. La restrizione di $\mathcal{B}$ al linguaggio originale L è una L-struttura di cardinalità $\geq \kappa$ modello di T. QED

9 Elementare equivalenza e sottostrutture elementari

9.1 Elementare equivalenza

Definizione 9.1 Due L-strutture $\mathcal{A}$ e $\mathcal{B}$ si dicono *elementarmente equivalenti*, $\mathcal{A} \equiv \mathcal{B}$ se e solo se hanno la stessa teoria completa: $Th(\mathcal{A}) = Th(\mathcal{B})$.

In altre parole due strutture $\mathcal{A}$ e $\mathcal{B}$ sono elementarmente equivalenti se e solo se non cè nessuna proprietà del primo ordine che le distingue, cioè per ogni L-enunciato ϕ, $\mathcal{A} \models \phi$ se e solo se $\mathcal{B} \models \phi$.

Un caso particolare di due strutture elementarmente equivalenti è dato da due strutture isomorfe, le quali non sono distinguibili da nessuna proprietà strutturale (che non faccia riferimento cioè alla natura degli elementi del dominio), e quindi a maggior ragione da nessuna proprietà del primo ordine.

9.2 Sottostrutture elementari

Definizione 9.2 (Immersione elementare) Un morfismo $f: \mathcal{A} \to \mathcal{B}$ tra due L-strutture si dice una *immersione elementare* se per ogni n e per ogni L-formula $\phi(x_1, \ldots, x_n)$ con variabili libere incluse in $\{x_1, \ldots, x_n\}$ e per ogni $a_1, \ldots, a_n \in A$, si ha:

$$\text{se } \mathcal{A} \models \phi(a_1, \ldots, a_n), \text{ allora } \mathcal{B} \models \phi(f(a_1), \ldots, f(a_n))$$

Siccome questa implicazione deve valere per tutte le ϕ, allora rimpiazzando ϕ con la sua negazione vediamo che deve in effetti valere un doppia implicazione: $\mathcal{A} \models \phi(a_1, \ldots, a_n)$, se e solo se $\mathcal{B} \models \phi(f(a_1), \ldots, f(a_n))$.

In generale la maggior parte dei morfismi che un algebrista considera non sono elementari. Essere elementare è una condizione molto forte che non si verifica molto spesso.

Poichè tra le formule ϕ c'è anche il predicato di non-uguaglianza $\neg(x = y)$, una immersione elementare è necessariamente iniettiva (ed è quindi un isomorfismo sulla sua immagine).

Un esempio di immersione elementare è l'inclusione del campo dei numeri reali algebrici nel campo dei numeri reali. Un esempio più semplice è l'immersione dei numeri razionali nei numeri reali se consideriamo solo la struttura di ordine. Invece l'immersione dei razionali nei reali come anelli non è elementare: basta considerare la formula (senza variabili libere) $\neg\exists x(x^2 = 2)$. Essa è vera in $\mathbf{Q}$ e non in $\mathbf{R}$.

Una ovvia condizione necessaria, ma non sufficiente, affinché esista una immersione elementare di $\mathcal{A}$ in $\mathcal{B}$ è che $\mathcal{A} \equiv \mathcal{B}$, cioè che $\mathcal{A}$ sia elementarmente equivalente a $\mathcal{B}$: (basta considerare nella definizione di immersione elementare formule senza variabili libere).

Definizione 9.3 (Sottostruttura elementare) Una sottostruttura $\mathcal{B}$ di $\mathcal{A}$ si dice *sottostruttura elementare*, e scriviamo $\mathcal{A} \prec \mathcal{B}$, se e solo se la inclusione di $\mathcal{A}$ in $\mathcal{B}$ è una immersione elementare.

Il seguente esempio illustra la differenza tra elementare equivalenza e sottostruttura elementare. Il punto cruciale da osservare è che il concetto di elementare equivalenza fa riferimento a formule senza parametri, mentre quello di sottostruttura elementare fa riferimento a formule con parametri.

Esempio 9.4 Sia $L = (<)$ e consideriamo la L-struttura costituita dall'insieme ordinato dei numeri interi $\mathbf{Z}$, e la sua sottostruttura $2\mathbf{Z}$ costituita dai numeri pari. Allora $2\mathbf{Z}$ è elementarmente equivalente a $\mathbf{Z}$ (in quanto è addirittura isomorfo), ma non è una sua sottostruttura elementare perchè la formula $\exists x(2 < x < 4)$, con parametri da $2\mathbf{Z}$, è vera in $\mathbf{Z}$ ma non in $2\mathbf{Z}$.

La seguente proposizione mostra come rimpiazzare un'immersione con una sottostruttura (che sarà elementare se l'immersione era elementare).

Proposizione 9.5 *Se $f: \mathcal{A} \to \mathcal{B}$ è una immersione (elementare), allora esiste una L-struttura $\mathcal{B}'$ isomorfa a $\mathcal{B}$ tale che $\mathcal{A}$ è una sottostruttura (elementare) di $\mathcal{B}'$.*

Dim. Sia $f(A) \subseteq B$ l'immagine di f, e sia X un insieme della stessa cardinalità di $B \setminus f(A)$ e disgiunto da A. Definiamo $B' = A \cup X$. Ne segue che c'è una corrispondenza biunivoca $h: B' \to B$ che coincide con f su A. Definiamo le funzioni e le relazioni su B' in modo da ottenere una struttura $\mathcal{B}'$ con dominio B' tale che h sia non solo una corrispondenza biunivoca, ma un isomorfismo da $\mathcal{B}'$ a $\mathcal{B}$. QED

Definizione 9.6 Data una sottostruttura (non necessariamente elementare) $\mathcal{A}$ di $\mathcal{B}$, diciamo che una formula $\phi(x_1, \ldots, x_n)$ è *preservata verso l'alto* se per ogni $a_1, \ldots, a_n \in A$, si ha:

$$\text{se } \mathcal{A} \models \phi(a_1, \ldots, a_n), \text{ allora } \mathcal{B} \models \phi(a_1, \ldots, a_n)$$

Se invece vale l'implicazione da $\mathcal{B}$ ad $\mathcal{A}$ diciamo che ϕ è *preservata verso il basso.*

Usando questa terminologia vediamo che $\mathcal{A}$ è una sottostruttura elementare di $\mathcal{B}$ se e solo se tutte le formule sono preservate sia verso l'alto che verso il basso (prendendo le negazioni si vede che se tutte sono preservate verso l'alto lo sono anche verso il basso).

Esempio 9.7 Consideriamo due anelli $\mathcal{A} \subseteq \mathcal{B}$, intesi come L-strutture con $L = \{0, 1, -1, +, \cdot\}$, e un polinomio f a coefficienti in $\mathcal{A}$. Il fatto che f abbia uno zero in $\mathcal{A}$ può essere espresso con la formula $\exists \vec{x} f(\vec{x}) = 0$. Questa formula contiene i coefficienti $a_1, \ldots, a_n$ del polinomio come parametri, e per esplicitare la loro presenza possiamo riscrivere la formula come $\exists \vec{x} g(\vec{x}, a_1, \ldots, a_n) = 0$ dove $g(\vec{x}, y_1, \ldots, y_n)$ è un polinomio a coefficienti in $\mathbf{Z}$ (rappresentabile con una L-formula senza parametri). La L-formula $\exists \vec{x} g(\vec{x}, x_1, \ldots, x_n) = 0$ è ovviamente preservata verso l'alto, perchè se un polinomio a coefficienti in $\mathcal{A}$ ha una soluzione in $\mathcal{A}$, ha anche una soluzione in $\mathcal{B}$.

In generale tutte le formule *esistenziali*, cioè del tipo $\exists \vec{x} \phi(\vec{x}, \vec{y})$, dove ϕ non ha quantificatori, sono preservate verso l'alto. Vicerversa tutte le formule *universali*, cioè del tipo $\forall \vec{x} \phi(\vec{x}, \vec{y})$, dove ϕ non ha quantificatori, sono preservate verso il basso. Ad esempio una sottostruttura di un gruppo è sempre un gruppo, perché gli assiomi dei gruppi sono di tipo universale.

Per gli altri tipi di formule può non esserci nè la preservabilità verso l'alto nè verso il basso. Ad esempio la formula $\exists x \forall y (x \leq y)$ che esprime l'esistenza di un minimo in un ordine lineare non è preservata nè verso l'alto nè verso il basso ($\mathbf{Z}$ non ha un minimo, $\mathbf{N} \subseteq \mathbf{Z}$ lo ha).

Tutte le formule atomiche sono preservate sia verso l'alto che verso il basso come segue facilmente dalla definizione di sottostruttura. Sono solo i quantificatori che distruggono la preservabilitá. Se una classe di formule è preservata sia verso l'alto che verso il basso, lo è anche la classe di tutte le formule che si ottengono da queste con i connettivi booleani $\neg, \wedge, \vee$. I due connettivi $\wedge$ e $\vee$, mantengono la preservabilità verso l'alto, il connettivo $\neg$ inverte la preservabilitá verso l'alto con quella verso il basso.

Osservazione 9.8 Si può dimostrare che una L-formula è preservate verso l'alto per tutte le possibili scelte di L-strutture $\mathcal{A} \subseteq \mathcal{B}$ se e solo se è logicamente equivalenti a una formula esistenziale.

9.3 Teorema di Lowenheim - Skolem verso il basso

Lemma 9.9 *(Criterio di Tarski - Vaught) Consideriamo due L-strutture $\mathcal{A} \subseteq \mathcal{B}$. Supponiamo che per ogni L-formula della forma $\exists y \phi(y, x_1, \ldots, x_n)$ e parametri $a_1, \ldots, a_n \in A$, si abbia che se $\mathcal{B} \models \exists y \phi(y, a_1, \ldots, a_n)$, allora esiste $a \in A$ tale che $\mathcal{B} \models \phi(a, a_1, \ldots, a_n)$. Ne segue che $\mathcal{A} \prec \mathcal{B}$. ($\exists y \phi(y, x_1, \ldots, x_n)$ non è necessariamente una formula esistenziale perchè potrebbe contenere altri quantificatori all'interno.)*

Dim. Per induzione sul numero dei connettivi della formula $\theta(x_1, \ldots, x_k)$ mostriamo che per ogni $a_1, \ldots, a_k \in A$, $\mathcal{B} \models \theta(a_1, \ldots, a_k)$ se e solo se $\mathcal{A} \models \theta(a_1, \ldots, a_k)$, cioè θ è preservata in entrambe le direzioni.

Se θ è atomica, allora l'equivalenza da dimostrare segue dal fatto che $\mathcal{A}$ è una sottostruttura di $\mathcal{B}$.

Se una classe di formule è preservata in entrambe le direzioni, anche tutte le formule che si ottengono da esse usando i connettivi booleani lo è.

L'unico caso interessante è quello di formule della forma $\exists y \phi(y, x_1, \ldots, x_n)$ per le quali possiamo usare le nostre ipotesi:

$\mathcal{A} \models \exists y \phi(y, \vec{a})$

se e solo se esiste $c \in A$ tale che $\mathcal{A} \models \phi(c, \vec{a})$

se e solo se, per ipotesi induttiva (poiché ϕ ha meno connettivi di $\exists y \phi$), esiste $c \in A$ tale che $\mathcal{B} \models \phi(c, \vec{a})$

se e solo se, per le ipotesi, $\mathcal{B} \models \exists y \phi(y, \vec{a})$. QED

In modo simile si dimostra:

Esercizio 9.10 Una condizione necessaria e sufficiente affinché $\mathcal{A}$ sia una sottostruttura elementare di $\mathcal{B}$ è che le formule esistenziali siano preservate verso il basso (cioè in direzione opposta rispetto a quella in cui sono naturalmente preservate).

Definizione 9.11 (Chiusura di un insieme rispetto ad una famiglia di funzioni). Sia A un insieme, e sia $\mathcal{F}$ una collezione di funzioni tali che ogni $f \in \mathcal{F}$ è una funzione da A^n ad A per qualche $n \in \mathbf{N}$ (se $n = 0$, f è un elemento di A). Sia B un sottoinsieme di A. Diciamo che B è **chiuso** rispetto alle funzioni

di $\mathcal{F}$ se per ogni funzione $f \in \mathcal{F}$ e per ogni $b_1, \ldots, b_n \in B$ (dove n è il numero degli argomenti di f), si ha $f(b_1, \ldots, b_n) \in B$. Sia X un sottoinsieme di A. La **chiusura** di X rispetto a $\mathcal{F}$, denotata $\langle X \rangle^{\mathcal{F}}$, è l'intersezione della famiglia di tutti i sottoinsiemi di A che contengono X e sono chiusi rispetto alle funzioni di F (tale famiglia non è vuota in quanto A stesso vi appartiene). L'insieme $\langle X \rangle^{\mathcal{F}}$ è il più piccolo (nel senso che è incluso in tutti gli altri) sottoinsieme B di A che contiene X ed è chiuso rispetto alle funzioni di $\mathcal{F}$.

Lemma 9.12 *$\langle X \rangle^{\mathcal{F}}$ coincide con l'unione $\bigcup_{k \in \omega} X_k$ dove $X_0 = X$ e X_{k+1} è l'insieme di tutti gli elementi $a \in A$ che si ottengono applicando ad elementi di $\bigcup_{i=0}^{k} X_i$ una delle funzioni di $\mathcal{F}$.*

Dim. L'inclusione $X_k \subseteq \langle X \rangle^{\mathcal{F}}$ si mostra facilmente per induzione su k usando, per il passo induttivo, il fatto che $\langle X \rangle^{\mathcal{F}}$ è chiuso rispetto alle funzioni di $\mathcal{F}$. Ne consegue che $\bigcup_{k \in \mathbf{N}} X_k \subseteq \langle X \rangle^{\mathcal{F}}$. Per l'inclusione inversa $\langle X \rangle^{\mathcal{F}} \subseteq \bigcup_{k \in \mathbf{N}} X_k$ è sufficiente dimostrare che $\bigcup_{k \in \mathbf{N}} X_k$ è chiuso rispetto alle funzioni di $\mathcal{F}$ (essendo $\langle X \rangle^{\mathcal{F}}$ contenuto in tutti gli insiemi chiusi per $\mathcal{F}$ e contenenti X). Se $f \in F$ ha arità n e $a_1, \ldots, a_n \in \bigcup_{n \in \mathbf{N}} X_k$, per vedere che $f(a_1, \ldots, a_n)$ appartiene a $\bigcup_{n \in \mathbf{N}} X_k$ usiamo il fatto che, essendo in numero finito, gli elementi $a_1, \ldots, a_n$ apparterranno tutti ad una certa unione finita $Y_k = \bigcup_{i=0}^{k} X_i$, e pertanto $f(a_1, \ldots, a_n)$ apperterrà a $Y_{k+1} = \bigcup_{i=0}^{k+1} X_i$, che è incluso in $\bigcup_{n \in \mathbf{N}} X_k$. QED

Lemma 9.13 *La cardinalità di $\langle X \rangle^{\mathcal{F}}$ è minore o uguale al massimo tra la cardinalità di X, la cardinalità di $\mathcal{F}$, ed $\aleph_0$.*

Dim. Scriviamo $\langle X \rangle^{\mathcal{F}} = \bigcup_{k \in \mathbf{N}} X_k$ come sopra e sia α il massimo tra la cardinalità di X, la cardinalità di $\mathcal{F}$, ed $\aleph_0$. Mostriamo per induzione su k che $Card(X_k) \subseteq \alpha$. Il caso $k = 0$ è ovvio. Per il passo induttivo useremo il fatto che il prodotto e la somma di due numeri cardinali infinity β, γ coincide con il massimo dei due. In particolare che se X_k ha cardinalità $\leq \alpha$, anche qualsiasi prodotto cartesiano finito $(X_k)^n$ ha cardinalità $\leq \alpha$ (qui usiamo il fatto che α è almeno $\aleph_0$). Ne segue che se f è una funzione di $\mathcal{F}$ di arità n, l'insieme $Im(f_{|X_k})$ dei valori che f può assumere quando viene applicata ad n argomenti in X_k ha cardinalità $\leq \alpha$ (in quanto l'immagine di una funzione ha cardinalità minore o uguale alla cardinalità del suo dominio). Ora per definizione X_{k+1} è l'unione $\bigcup_{f \in \mathcal{F}} Im(f_{|X_k}$ delle immagini delle varie f ristrette ad X_k, e possiamo limitare la cardinalità di tale unione con il prodotto $|\mathcal{F}| \times \alpha$, che è uguale a α. QED

Teorema 9.14 *(Teorema di Lowenheim-Skolem verso il basso) Se $\mathcal{A}$ è una L-struttura e $X \subseteq A$ è un sottoinsieme del suo dominio, allora esiste una sottostruttura elementare $\mathcal{B} \prec \mathcal{A}$ con dominio $B \supseteq X$ e tale che B ha cardinalità minore o uguale al massimo tra $|X|$, $|L|$, ed $\aleph_0$.*

Dim. Possiamo associare ad ogni formula della forma $\exists y \phi(y, x_1, \ldots, x_n)$ una funzione $f_{\exists y \phi}: A^n \to A$, detta funzione di Skolem della formula, nel modo seguente (l'esistenza di f sarà garantita dall'"assioma della scelta"). Dati $a_1, \ldots, a_n \in A$, se esiste un $a \in A$ tale che $\mathcal{A} \models \phi(a, a_1, \ldots, a_n)$, allora scegliamo un tale a (se ne esiste più di uno facendo una scelta arbitraria) e poniamo $f(a_1, \ldots, a_n) = a$. Se invece un tale a non esiste, definiamo $f(a_1, \ldots, a_n)$ come un arbitrario elemento di A. In entrambi i casi, se $f(a_1, \ldots, a_n) = a$, si avrà $\mathcal{A} \models \exists y \phi(y, a_1, \ldots, a_n) \to \phi(a, a_1, \ldots, a_n)$. Sia $\mathcal{F}$ l'insieme di tutte le funzioni di Skolem, una per ogni formula. La cardinalità di $\mathcal{F}$ è minore o uguale alla cardinalità delle L-formule, che è il massimo tra $|L|$ ed $\aleph_0$. Sia $\mathcal{B} = \langle X \rangle^{\mathcal{F}}$ la chiusura di X rispetto alle funzioni di Skolem (per assicurarci che $\mathcal{B}$ non sia vuota, possiamo prendere, senza perdita di generalità, X non vuoto). Ne segue che $\mathcal{B}$ è chiusa in particolare rispetto alle funzioni $h^{\mathcal{A}}$ che interpretano i simboli di funzione h della segnatura L. Infatti se $h \in L$ è un simbolo di funzione di arità n, la funzione di Skolem associata alla formula $\exists y(y = h(x_1, \ldots, x_n))$ coincide con $h^{\mathcal{A}}$. Similmente, ponendo $n = 0$, si mostra che $\mathcal{B}$ contiene le interpretazioni dei simboli di costante di L. Pertanto $\mathcal{B}$ è il dominio di una sottostruttura di $\mathcal{A}$. Per vedere che $\mathcal{B}$ è una sottostruttura elementare si applica il criterio di Tarski - Vaught osservando che le funzioni di Skolem $f_{\exists y \phi}$ forniscono quei testimoni $a = f_{\exists y \phi}(a_1, \ldots, a_n) \in \langle X \rangle^{\mathcal{F}}$ dei quantificatori esistenziali che sono richiesti nel criterio. QED

Corollario 9.15 *Se la teoria degli insiemi di Zermelo-Fraenkel ha un modello, ne ha anche uno numerabile.*

Esempio 9.16 Per il teorema di Lowenheim - Skolem il campo ordinato dei numeri reali $\mathbf{R} = (\mathbf{R}; +, \cdot, 0, 1, <)$ ha una sottostruttura elementare numerabile. Una tale sottostruttura è il campo F dei numeri reali algebrici.

10 Cenni di teoria della calcolabilità

10.1 Algoritmi e funzioni calcolabili

Una funzione f si dice *calcolabile* se esiste un *algoritmo* che dato in ingresso $x \in dom(f)$ fornisce in uscita il valore $y = f(x)$.

Questa definizione ha bisogno di varie precisazioni. La nozione di algoritmo è data per intuitivamente nota. L'idea è che un algoritmo è un insieme finito di istruzioni che possono essere eseguite in modo del tutto meccanico senza che sia richiesta alcuna "creatività" da parte di chi esegue le istruzioni (che quindi può essere una macchina).

Poichè un algoritmo deve necessariamente operare su *rappresentazioni finite*, affinchè la definizione abbia senso assumiamo che gli elementi del dominio e codominio di f siano rappresentati da stringhe finite di simboli presi da un alfabeto finito Σ. Questo implica in particolare che il dominio e il codominio di una funzione calcolabile è necessariamente un insieme finito o numerabile. Esempi di domini e codomini ammissibili, oltre all'insieme Σ^* di tutte le stringhe

finite di simboli dall'alfabeto Σ, sono i numeri naturali $\mathbf{N}$ con la usuale rappresentazione in notazione decimale, oppure i numeri razionali, dove un razionale $q \in \mathbf{Q}$ è rappresentato dando il numeratore e denominatore della frazione ridotta ai minimi termini che corrisponde a q. Non considereremo invece funzioni su numeri reali in quanto non è possibile fissare una rappresentazione finita per i numeri reali: l'usuale rappresentazione decimale richiede in genere infinite cifre dopo la virgola.

A priori potrebbe capitare che una funzione sia calcolabile rispetto ad una data rappresentazione degli elementi del dominio e codominio e non calcolabile rispetto ad un'altra rappresentazione. Se però consideriamo due rappresentazioni tali che esiste un algoritmo per passare dall'una all'altra, ad esempio la rappresentazione in base decimale e quella in base due per i numeri naturali, allora è chiaro che una qualsiasi funzione è calcolabile rispetto alla prima rappresentazione se e solo se lo è rispetto alla seconda[1].

In genere tutte le rappresentazioni comunemente considerate hanno la proprietà che si può passare in modo algoritmico dall'una all'altra rappresentazione. Possiamo quindi parlare di funzioni calcolabili lasciando implicita la scelta della particolare rappresentazione usata.

Un esempio classico di funzione calcolabile è dato dalla funzione da $\mathbf{N}^2$ a $\mathbf{N}$ che dati due numeri x e y fornisce il massimo comun divisore di x ed y (usiamo l'algoritmo di Euclide delle divisioni successive). Probabilmente tutte le funzioni da $\mathbf{N}$ ad $\mathbf{N}$ conosciute da uno studente che non abbia seguito un corso di logica sono calcolabili. Chiaramente può esistere più di un algoritmo per calcolare la stessa funzione, alcuni più efficienti altri meno.

10.2 Funzioni calcolabili parziali

L'esecuzione di un algoritmo procede per passi discreti. Certi algoritmi, come l'algoritmo di Euclide per trovare il massimo comun divisore, terminano dopo un numero finito di passi per qualsiasi dato di ingresso. Altri algoritmi terminano dopo un numero finito di passi solamente per certi valori dei dati di ingresso, mentre per altri valori vanno avanti all'infinito senza fermarsi mai.

Esempio 10.1 Consideriamo il problema di stabilire, dato un polinomio $p(x_1, \ldots, x_n)$ a coefficienti interi, se l'equazione $p(x_1, \ldots, x_n) = 0$ ha soluzioni intere (non ci interessa trovare la soluzione, solo stabilire se esista o no). È certamente possibile progettare un algoritmo che, preso in ingresso un polinomio $p(\vec{x})$, prova a sostituire alle variabili del polinomio tutti i possibili valori interi l'uno dopo l'altro in qualche ordine, fermandosi se e quando si trova una soluzione intera di $p(\vec{x}) = 0$. Chiaramente tale algoritmo si ferma in un numero finito di passi se la soluzione c'è, ma va avanti all'infinito senza fornire alcuna risposta, nè positiva

[1] Ad esempio se ho un algoritmo per scomporre in fattori primi in numero naturale scritto in base due, posso facilmente ottenere un secondo algoritmo per scomporre in fattori primi un numero scritto in base dieci. Il secondo algoritmo prende in ingresso un numero in base 10, ne trova la rappresentazione binaria, applica il primo algoritmo per scomporlo, e infine riscrive il risultato in base 10.

nè negativa, se la soluzione non c'è. Abbiamo qui un esempio di algoritmo che non si ferma per certi dati di ingresso (in questo caso il dato di ingresso è il polinomio).

Ci si può ovviamente chiedere se si può far di meglio, ovvero se sia possibile progettare un algoritmo che fornisca sempre dopo un numero finito di passi una risposta positiva o negativa alla domanda se $p(\vec{x}) = 0$. Se ci limitiamo a polinomi in una variabile, o ad altri casi particolari, ciò è possibile, ma per polinomi arbitrari si può dimostrare che un algoritmo che termini sempre non c'è. L'analogo problema in cui si chiede la soluzione di soluzioni reali anzichè intere, può invece sempre essere risolto in un numero finito di passi grazie al cosiddetto "algoritmo di Sturm".

Il concetto di algoritmo che può non fermarsi su alcuni dati di ingresso, conduce in modo naturale alla considerazione di "funzioni parziali". L'idea è di introdurre una distinzione tra il dominio dei possibili valori di ingresso, e il sottodominio di quei valori per i quali l'algoritmo termina.

Definizione 10.2 Una *funzione parziale* da A a B può essere definita come una funzione da A a $B \cup \{\uparrow\}$ (unione disgiunta). Possiamo associare ad ogni algoritmo M una funzione parziale f_M nel modo seguente. Supponiamo che l'algoritmo M prenda in ingresso elementi dall'insieme A (in una fissata rappresentazione) e fornisca in uscita, nei casi in cui la computazione termina dopo un numero finito di passi, elementi di un insieme B (in una fissata rappresentazione). La funzione parziale $f_M : A \to B \cup \{\uparrow\}$ è così definita:

$f_M(a) = b$ se M con input a fornisce in uscita b,

$f_M(a) = \uparrow$ se M con input a non si ferma mai.

Una funzione parziale $f : A \to B \cup \{\uparrow\}$ si dice *calcolabile parziale* se esiste un algoritmo M tale che $f = f_M$. Useremo anche la notazione $f : A \rightharpoonup B$ per indicare il fatto che f è una funzione parziale da A a B. Una funzione parziale che non assume mai il valore $\uparrow$ si dice totale.

10.3 Macchine di Turing

Un tentativo di formalizzare il concetto di funzione calcolabile senza far riferimento al concetto intuitivo di algoritmo è stato compiuto da Alan Turing nel 1936. Una macchina di Turing è un calcolatore ideale fornito di due tipi di memoria: interna ed esterna. Ad ogni dato momento entrambi i tipi di memoria possono contenere una quantità finita di informazione, ma mentre la memoria esterna è potenzialmente illimitata, la memoria interna ha una fissata capacità massima che non può essere superata nell'intero processo di elaborazione. La macchina è inoltre fornita di un puntatore che scandisce l'area della memoria esterna sotto esame in un dato momento e di un "programma" che determina come deve essere alterata la memoria e la posizione del puntatore durante un passo di esecuzione. Più precisamente, in funzione del contenuto della memoria interna e della parte della memoria esterna scandita dal puntatore, il programma specifica: 1) come deve essere modificato il contenuto della memoria esterna

scandito in quel momento; 2) dove si deve spostare il puntatore (deve essere una zona contigua); 3) come deve essere alterata la memoria interna. A partire dalla configurazione iniziale della memoria la macchina esegue ripetutamente le operazioni specificate dal programma arrestandosi se, e quando, viene raggiunto un determinato stato della memoria interna, detto stato di arresto.

Questa è l'idea e diamo ora la definizione formale. Nelle clausole che seguono la memoria esterna è rappresentata dal contenuto delle celle di un nastro, mentre l'insieme finito Q rappresenta i possibili stati della memoria interna. Una macchina di Turing è costituita da:

0. Un *alfabeto* finito Σ contenente almeno i simboli $0, 1, \#$ (dove $\#$ è un simbolo speciale per lo spazio bianco).

1. Un *nastro* diviso in celle che formano una successione infinita nei due versi. Ogni cella contiene uno dei simboli di Σ. In ogni dato momento il nastro conterrà solamente un numero finito di simboli diversi da $\#$.

2. Un insieme finito Q di *stati*. Assumiamo che tra gli stati $q \in Q$ vi siano due stati speciali di INIZIO $\in Q$ e di ARRESTO $\in Q$

3. Un *puntatore* del nastro che ad ogni dato momento si trova in uno degli stati di Q e scandisce una cella del nastro. Esso può spostarsi lungo le celle del nastro, cambiare il contenuto delle celle stesse, e cambiare stato secondo delle regole che vedremo. Ad ogni movimento il puntatore scrive un simbolo di Σ nella cella che viene scandita, sostituendo ciò che vi era scritto, e poi si sposta di una cella a sinistra o a destra.

4. Le regole che governano il comportamento del puntatore sono date da un *programma*. Esso consiste di una *funzione di transizione* $\delta: Q \times \Sigma \to Q \times \Sigma \times \{S, D\}$ (dove S, D stanno per sinistra e destra)[2]. Supponiamo che in un certo momento della computazione il puntatore si trovi nello stato $q \in Q$ e stia scandendo una cella contenente il simbolo $\alpha \in \Sigma$. Sia $(q', \alpha', i) = \delta(q, \alpha)$ (dove $i \in \{S, D\}$). In questa situazione il puntatore compie le seguenti azioni: scrive il simbolo α' sulla cella che in quel momento sta scandendo (cancellando il simbolo α che vi si trovava), si porta nello stato q', e se $q' \neq ARRESTO$ si sposta di una cella a sinistra o a destra a seconda che $i = S, D$. Nel caso $q' = ARRESTO$ la macchina di Turing si arresta.

10.3.1 Funzione parziale calcolata da una macchina di Turing.

Fissiamo $k \in \mathbf{N}$. Una macchina di Turing M con un alfabeto Σ di input-output contenente i simboli $0, 1$ calcola una funzione parziale $f_M^k: \mathbf{N}^k \rightharpoonup \mathbf{N}$ nel modo seguente.

Rappresentiamo $x \in \mathbf{N}$ con la parola $11\ldots1$ (x volte 1).

Se $k > 1$ rappresentiamo $(x_1, x_2, \ldots, x_k) \in \mathbf{N}^k$ con la parola che contiene x_1 volte il simbolo 1, seguita da uno 0, seguita dalla rappresentazione di $(x_2, \ldots, x_k)$.

Esempio: $(4, 3, 5)$ è rappresentata dalla parola 11110111011111.

[2] Poichè $Q \times \Sigma$ è un insieme finito, la funzione di transizione può essere data sotto forma di una tabella finita

Diciamo che $f_M^k(x_1, \ldots, x_k) = y$ se e solo se, facendo partire la macchina M nello stato INIZIO con la parola che rappresenta $(x_1, \ldots, x_n)$ scritta inizialmente sul nastro (con tutte le altre caselle del nastro contenenti il simbolo bianco) e con il puntatore all'inizio della parola, abbiamo che dopo un certo numero finito di passi la macchina M si arresta con la parola rappresentante y scritta sul nastro e il puntatore all'inizio della parola.

Negli altri casi definiamo $f_M^k(x_1, \ldots, x_k) = \uparrow$[3].

Chiaramente possiamo usare una macchina di Turing anche per calcolare funzioni parziali non numeriche $f: A \rightharpoonup B$. Basta fissare una rappresentazione degli elementi di A e B come parole sull'alfabeto Σ.

10.4 Tesi di Church

Nella seconda metà degli anni trenta vari autori, tra cui Turing, Post, Church e Kleene, hanno indipendentemente cercato di rendere rigoroso il concetto di funzione calcolabile in senso intuitivo (si tenga presente che non esistevano ancora i calcolatori). A tal fine Turing ha introdotto il concetto di "macchina di Turing", Kleene ha definito le funzioni "μ-ricorsive", e Church le funzioni "λ-calcolabili". È stato successivamente dimostrato che le funzioni Turing calcolabili, μ-ricorsive, e λ-calcolabili coincidono. Questi tre concetti individuano dunque una unica classe di funzioni, dette *funzioni parziali ricorsive*. La coincidenza di questi diversi tentativi di rendere rigoroso il concetto di funzione calcolabile ha portato all'accettazione della:

Tesi di Church Le funzioni calcolabili parziali coincidono con le funzioni parziali Turing calcolabili.

Questa è una tesi che può essere giustificata e motivata in vari modi ma che ovviamente non può essere "dimostrata" in quanto il concetto di algoritmo è intuitivo e informale.

L'accettazione della Tesi di Church rende possibile dimostrare la non-esistenza di algoritmi per calcolare determinate funzioni o risolvere determinati problemi.

10.5 Insiemi decidibili e semidecidibili

Consideriamo per semplicità sottoinsiemi di $\mathbf{N}$ sebbene le seguenti definizioni si applichino a sottoinsiemi di $\mathbf{N}^k$ ed anche ad insiemi non numerici, ad esempio sottoinsiemi di Σ^*, ovvero insiemi i cui elementi siano rappresentati da stringhe finite di simboli da un certo alfabeto finito Σ.

Un insieme $A \subseteq \mathbf{N}$ si dice *decidibile* (come sottoinsieme di $\mathbf{N}$) se esiste un algoritmo che, dato in ingresso $x \in \mathbf{N}$ (in una certa notazione fissata) stabilisce se x appartiene o non appartiene ad A (ad esempio fornendo in uscita 1 o 0 a seconda che x appartenga o non appartenga ad A).

[3] È facile vedere che possiamo sempre modificare una macchina di Turing in modo da ottenerne un'altra che ha esattamente lo stesso comportamento della prima eccetto che, nel caso la prima si ferma senza fornire in uscita la rappresentazione di un intero, la seconda non si ferma mai.

In altre parole A è decidibile se la sua funzione caratteristica $\chi_A: U \to \{0,1\}$ (definita da $\chi_A(x) = 1$ se $x \in A$, $\chi_A(x) = 0$ se $x \notin A$) è calcolabile.

Esempio: l'insieme dei numeri primi (come sottoinsieme dei numeri naturali) è decidibile. Dato $x \in \mathbf{N}$ possiamo stabilire se x è primo o no esaminando tutti i possibili divisori di x minori di x.

Un insieme $A \subseteq \mathbf{N}$ si dice *semidecidibile* se esiste un algoritmo tale che, se viene dato in ingresso un elemento $x \in A$, l'esecuzione dell'algoritmo termina dopo un numero finito di passi, mentre se in ingresso viene dato un elemento $x \in \mathbf{N} - A$, l'esecuzione dell'algoritmo non termina mai.

Chiaramente $\mathbf{N}$ e l'insieme vuoto e l'insieme sono sia decidibili che semidecidibili (come sottoinsiemi di $\mathbf{N}$). Basta considerare un algoritmo che non si ferma per alcun input ed uno che si ferma per ogni input. Abbiamo:

Proposizione 10.3 *Ogni insieme decidibile è anche semidecidibile.*

Dim. Sia $A \subseteq \mathbf{N}$ decidibile. Ne segue, per definizione, che esiste un algoritmo M_1 che dato $x \in \mathbf{N}$ stabilisce se x appartiene o no ad A (dando come uscita 1 o 0 rispettivamente). Consideriamo ora un algoritmo ausiliario M_2 che avendo in ingresso 1 si ferma subito, ed avendo in ingresso 0 comincia un calcolo senza fine. Sia M_3 l'algoritmo che si ottiene componendo M_1 ed M_2 in modo tale che l'uscita di M_1 viene fornita in entrata ad M_2. Ne segue che se $x \in A$, l'algoritmo M_3 si ferma dopo un numero finito di passi, e se $x \in \mathbf{N} - A$, l'algoritmo M_3 non si ferma mai. Quindi A è semidecidibile. QED

Teorema 10.4 *(Teorema di Post) Supponiamo che sia A che il suo complemento $\mathbf{N} - A$ siano semidecidibili. Allora A è decidibile.*

Dim. Dato $x \in \mathbf{N}$ possiamo dare x come ingresso ai due semi-algoritmi per A e $\mathbf{N} - A$ e eseguirli simultaneamente in modo alternato (eseguendo cioè un passo dell'uno ed uno dell'altro). Poichè x appartiene ad A oppure ad $\mathbf{N} - A$, uno dei due semi-algoritmi si ferma dopo un numero finito di passi. Se è il primo a fermarsi, abbiamo stabilito che $x \in A$, se invece si ferma il secondo, $x \notin A$. In questo modo abbiamo definito un algoritmo per stabilire se x appartiene o no ad A e quindi A è decidibile. QED

Ricordiamo che un insieme A è *numerabile* se è vuoto oppure esiste una lista $a_0, a_1, a_2, \ldots$ indiciata dai numeri naturali che esaurisce tutti e soli gli elementi di A (non è detto che nella lista non ci siano ripetizioni, e non escludiamo il caso in cui A sia finito).

Definizione 10.5 Un insieme $A \subseteq \mathbf{N}$ si dice *ricorsivamente enumerabile* se A è vuoto oppure esiste una enumerazione $a_0, a_1, a_2, \ldots$ degli elementi di A che è effettiva, nel senso che la funzione $n \mapsto a_n$ (da $\mathbf{N}$ ad $\mathbf{N}$) è calcolabile.

Quindi un insieme non-vuoto A è ricorsivamente enumerabile se e solo se è l'immagine di una funzione calcolabile con dominio $\mathbf{N}$.

Esiste una importante differenza tra gli insiemi numerabili e quelli ricorsivamente numerabili: mentre ogni sottoinsieme di un insieme numerabilie è numerabile, un sottoinsieme di un insieme ricorsivamente enumerabile non è necessariamente ricorsivamente enumerabile. Ad esempio $\mathbf{N}$ è ricorsivamente enumerabile, ma vedremo che $\mathbf{N}$ possiede sottoinsiemi non ricorsivamente enumerabili.

Teorema 10.6 *Un insieme $A \subseteq \mathbf{N}$ è semidecidibile se e solo se è ricorsivamente enumerabile.*

Dim. Se A è vuoto è sia semidecidibile che ricorsivamente enumerabile. Assumiamo che A non sia vuoto.

Supponiamo che A sia ricorsivamente enumerabile e fissiamo una funzione calcolabile $f: \mathbf{N} \to A$ suriettiva. Definiamo ora un algoritmo H nel modo seguente. Avendo $x \in \mathbf{N}$ in ingresso H comincia a enumerare uno dopo l'altro $f(0), f(1), f(2), \ldots$ (usando un algoritmo per calcolare f) e si ferma solamente se nel corso di questa enumerazione trova un elemento $f(n)$ uguale ad x. È chiaro che l'algoritmo H così definito si ferma su input $x \in \mathbf{N}$ se e solo se $x \in A$. Quindi A è semidecidibile.

Il viceversa è più complicato e richiede di fissare una funzione calcolabile suriettiva $f: \mathbf{N} \to \mathbf{N} \times \mathbf{N}$ (si usi una codifica delle coppie di numeri). Supponiamo che A sia semidecidibile. Esiste quindi un algoritmo H_1 che si ferma su input $x \in \mathbf{N}$ se e solo se $x \in A$. Fissiamo un elemento $a \in A$ e definiamo una funzione calcolabile $g: \mathbf{N} \to \mathbf{N}$ nel modo seguente: per calcolare $g(n)$ calcoliamo dapprima $f(n) = (a_n, b_n) \in \mathbf{N} \times \mathbf{N}$. Ora poniamo $g(n) = a_n$ se l'algoritmo H_1 su input a_n si ferma in al più b_n passi (questo può essere controllato algoritmicamente semplicemente eseguendo H_1 per al più b_n passi), e $g(n) = a$ nel caso contrario. È chiaro che i valori di g appartengono tutti ad A. Resta da vedere che ogni elemento $u \in A$ è nell'insieme dei valori di g. Fissiamo dunque $u \in A$. Ne segue che H_1 applicato ad u si ferma dopo un certo numero di passi, diciamo m passi. Poichè $f: \mathbf{N} \to \mathbf{N} \times \mathbf{N}$ è suriettiva, esiste $n \in \mathbf{N}$ tale che $f(n) = (u, m)$. Per definizione di g, $g(n) = u$. Quindi $g: \mathbf{N} \to A$ è suriettiva (e calcolabile) e A è ricorsivamente enumerabile. QED

Esercizio 10.7 l'unione, l'intersezione, e il prodotto cartesiano di insiemi ricorsivamente enumerabili è ricorsivamente enumerabile. Tutto ciò è vero a fortiori per gli insiemi decidibili che però hanno una proprietà in più: il complemento di un insieme decidibile è decidibile. Quindi i sottoinsiemi decidibili di $\mathbf{N}$ formano un algebra di Boole (rispetto a unioni, intersezioni e complementi).

Esercizio 10.8 Dimostrare il teorema precedente per insiemi non numerici $A \subseteq \Sigma^*$. Cosa prende il posto della funzione calcolabile suriettiva $f: \mathbf{N} \to \mathbf{N} \times \mathbf{N}$?

Esercizio 10.9 Siano A, B, C tre insiemi ricorsivamente enumerabili disgiunti la cui unione sia $\mathbf{N}$. Dimostrare che A, B, C sono decidibili.

10.6 Ricorsiva enumerabilità dei teoremi

Il teorema che segue fornisce l'esempio più importante di un insieme semidecidibile che non è in generale decidibile.

Teorema 10.10 *L'insieme dei teoremi di una teoria del primo ordine con un numero finito di assiomi, o più in generale con un insieme decidibile di assiomi, è semidecidibile.*

Dim. Una formula ϕ appartiene all'insieme $Th(T)$ dei teoremi di T se e solo se esiste una dimostrazione formale d di ϕ da T. Data una stringa di simboli d possiamo controllare se essa è una dimostrazione formale verificando che essa è costituita da una successione di formule ben formate ognuna delle quali è un assioma di T, o un assioma logico, o segue da formule precedenti tramite una regola di inferenza. Il controllo se una data formula sia una assioma logico o segua da altre formule tramite una singola applicazione di una regola di inferenza è decidibile. Il controllo che una data formula sia un assioma di T è decidibile per ipotesi. Ne segue che possiamo decidere in un numero finito di passi se una data stringa d è una dimostrazione. Per mostrare che $Th(T)$ è semidecidibile consideriamo la seguente procedura: data una formula ϕ, enumeriamo tutte le possibili stringhe di simboli d, controllando di volta in volta se siano dimostrazioni di ϕ, e fermandoci con risposta positiva appena ne si trovi una che sia effettivamente una dimostrazione di ϕ. Questa procedura termina se e solo se ϕ è un teorema di T, mostrando dunque che l'insieme dei teoremi di T è semidecidibile. QED

Teorema 10.11 *Sia T una teoria del primo ordine coerente e completa con un insieme decidibile di assiomi. Allora i teoremi di T sono un insieme decidibile.*

Dim. Per teorie T coerenti e complete per ogni enunciato ϕ nel linguaggio della teoria, o ϕ o la sua negazione è dimostrabile in T ma non entrambi. Ne segue che se enumeriamo tutte le dimostrazioni, prima o poi ne troveremo una di ϕ o della sua negazione, e a quel punto avremo stabilito se ϕ è un teorema. QED

Osservazione 10.12 Una dimosrazione alternativa si basa sul teorema di Post: l'insieme dei teoremi è semidecidibile, l'insieme degli enunciati refutabili (ciò gli enunciati la cui negazione è un teorema) è per lo stesso motivo semidecidibile. Per teorie coerenti e complete questi due insiemi sono l'uno il complemento dell'altro all'interno dell'insieme di tutti gli enunciati ben formati. Poichè gli enunciati ben formati sono un sottoinsieme decidibile di Σ^*, una semplica applicazione del teorema di Post garantisce che entrambi questi insiemi sono decidibili.

Esercizio 10.13 Nei due teoremi precedenti si possono indebolire le ipotesi: basta che l'insieme di assiomi di T sia semidecidibile.

Resta da vedere se esistono interessanti teorie coerenti e complete. Gödel ha dimostrato che non è possibile avere una teoria coerente e completa nemmeno per quella parte della matematica che si occupa delle proprietà "elementari" (cioè esprimibili al primo ordine) dei numeri naturali. Tuttavia Tarski ha mostrato che esiste una teoria completa per le proprietà elementari dei numeri reali.

11 Eliminazione dei quantificatori

Definizione 11.1 Sia T una L-teoria. Due formule θ, ϕ sono equivalenti in T, o T-equivalenti, se $T \vdash \theta \leftrightarrow \phi$. Osserviamo che ciò equivale a dire $T \vdash \forall \vec{y}(\theta \leftrightarrow \phi)$, dove $\vec{y}$ è la lista delle variabili libere in θ o ϕ.

Esercizio 11.2 Rimpiazzando, in una formula ϕ, una sottoformula α con un'altra formula T-equivalente ad α, si ottiene una formula ϕ' T-equivalente a ϕ.

Definizione 11.3 Sia T una L-teoria. T ammette eliminazione dei quantificatori se per ogni formula θ esiste una formula ϕ senza quantificatori T-equivalente a θ.

Esempio 11.4 La formula $\exists x(x^2 = y)$ equivale, nella teoria dei numeri reali (come campo ordinato), alla formula senza quantificatori $y \geq 0$.

Il seguente semplice risultato mostra sostanzialmente che per eliminare i quantificatori basta eliminarne "uno alla volta".

Lemma 11.5 *Sia T è una L-teoria. Supponiamo che ogni formula esistenziale della forma $\exists x\theta$, con θ senza quantificatori, equivalga in T ad una formula ϕ senza quantificatori. Allora T ammette eliminazione dei quantificatori.*

Dim. Mostriamo per induzione sul numero dei connettivi e quantificatori che ogni formula γ in cui non occorra il quantificatore $\forall$ equivale in T ad una formula senza quantificatori. Ciò basta ai nostri fini in quanto il quantificatore $\forall$ è eliminabile usando le equivalenze logiche $\forall xA \leftrightarrow \neg\exists x\neg A$. Sia dunque γ una formula in cui non occorre il $\forall$ e distinguiamo i seguenti tre casi. Se γ è già senza quantificatori non c'è nulla da dimostrare. Se γ è una combinazione booleana di altre formule, per ipotesi induttiva possiamo rimpiazzare queste ultime con formule T-equivalenti senza quantificatori, e usando l'Esercizio 11.2 otteniamo una formula senza quantificatori T-equivalente a γ. L'unico caso rimasto è allora quando γ ha la forma $\exists x\theta$ (essendoci premurati di escludere il caso $\forall x\theta$). In questo caso le nostre ipotesi ci dicono che γ equivale in T ad una formula senza quantificatori, completando il passo induttivo. QED

Definizione 11.6 Sia D un insieme di L-enunciati. Date due L-strutture $\mathcal{A}$ e $\mathcal{B}$ scriviamo $\mathcal{A} \equiv_D \mathcal{B}$ per indicare il fatto che $\mathcal{A}$ e $\mathcal{B}$ verificano gli stessi enunciati di D. Se $D = \{\theta\}$ consiste di un singolo enunciato scriviamo anche $\mathcal{A} \equiv_\theta \mathcal{B}$. Ciò significa che θ è vero in entrambe le strutture, o falso in entrambe.

Diamo ora un criterio, non costruttivo in quanto basato sul teorema di compattezza, affinché un dato enunciato θ sia T-equivalente ad uno senza quantificatori.

Lemma 11.7 *Sia T una L-teoria, sia D un insieme di L-enunciati chiuso per connettivi booleani (ad esempio l'insieme di tutti gli enunciati senza quantificatori), e sia θ un L-enunciato. Supponiamo che per ogni coppia $\mathcal{A}, \mathcal{B}$ di modelli di T tali che $\mathcal{A} \equiv_D \mathcal{B}$ si abbia $\mathcal{A} \equiv_\theta \mathcal{B}$. Allora $T \vdash \theta \leftrightarrow \delta$ per qualche $\delta \in D$.*

Dim. Sia $H = \{\varphi \in D \mid T \vdash \theta \to \varphi\}$ l'insieme di tutti gli enunciati di D implicati da θ nella teoria T. È sufficiente motrare che esiste un enunciato di H che implica θ (sempre in T). Per il teorema di compattezza e il fatto che T è chiuso per congiunzioni, ciò equivale a dire che θ è deducibile da $T \cup H$. Se ciò non fosse, esisterebbe un modello $\mathcal{A}$ di $T \cup H$ che non verifica θ. Per le nostre ipotesi, ogni modello $\mathcal{B} \equiv_D \mathcal{A}$ coincide con $\mathcal{A}$ sul valore di verità di θ, e quindi non verifica θ. Indicando con $D_A \supseteq H$ l'insieme degli enunciati di D veri in $\mathcal{A}$, ciò significa che $\neg\theta$ è deducibile $T \cup D_A$. Per compattezza ed il fatto che D_A è chiuso per congiunzioni, esiste una singola formula $\delta \in D_A$ che implica $\neg\theta$ (in T). Ciò equivale a dire che $T \vdash \theta \to \neg\delta$, cioè $\neg\delta \in H$ (osservando che D, essendo chiuso per negazione, contiene $\neg\delta$). Ciò è assurdo in quanto $\mathcal{A}$ verifica sia δ che tutte le formule di H. QED

Definizione 11.8 Una teoria T ha la proprietà dell'isomorfismo se ogni isomorfismo $f: \mathcal{B} \to \mathcal{B}'$ tra sottostrutture $\mathcal{B} \subset \mathcal{A}$ e $\mathcal{B}' \subset \mathcal{A}'$ di due modelli $\mathcal{A}$ ed $\mathcal{A}'$ di T, si estende ad un isomorfismo $\tilde{f}: \mathcal{C} \to \mathcal{C}'$ di modelli di T con $\mathcal{B} \subseteq \mathcal{C} \subseteq \mathcal{A}$ e $\mathcal{B}' \subseteq \mathcal{C}' \subseteq \mathcal{A}'$. In breve: ogni isomorfismo tra sottostrutture si estende ad un isomorfismo tra sottomodelli.

Esempio 11.9 Vedremo che la teoria dei campi algebricamente chiusi ha la proprietà dell'isomorfismo: se due campi algebricamente chiusi hanno sottostrutture isomorfe, i più piccoli sottocampi algebricamente chiusi che contengono tali sottostrutture sono isomorfi, con un isomorfismo che estende quello dato. Simile discorso vale per i campi reali chiusi.

Esercizio 11.10 La teoria degli ordini lineari densi senza massimo e minimo ha la proprietà dell'isomorfismo.

Definizione 11.11 Una teoria T ha la proprietà del sottomodello se per ogni $\mathcal{A} \subset \mathcal{B}$ modelli di T, e per ogni enunciato esistenziale della forma $\exists x \theta(x, \vec{a})$, dove $\theta(x, \vec{a})$ è una formula senza quantificatori con parametri $\vec{a}$ da $\mathcal{A}$, se $\mathcal{B}$ verifica l'enunciato anche $\mathcal{A}$ lo verifica.

Esempio 11.12 Vedremo che la teoria dei campi algebricamente chiusi ha la proprietà del sottomodello: ciò dipende dal fatto che se un sistema di equazioni e disequazioni polinomiali in una variabile, a coefficienti in un campo algebricamente chiuso, ha soluzione in una estensione del campo, esso ha soluzioni anche nel campo stesso. Stesso discorso vale per i campi reali chiusi.

Esercizio 11.13 La teoria degli ordini lineari densi senza massimo e minimo ha la proprietà del sottomodello.

Ci sarà utile il seguente lemma tecnico la cui dimostrazione dettagliata è lasciata come esercizio.

Lemma 11.14 *Sia T una L-teoria con la proprietà dell'isomorfismo (o del sottomodello), sia $\vec{c}$ una n-upla di nuovi simboli di costanti non in L, e sia $T[\vec{c}]$ è la teoria con gli stessi assiomi di T ma formulata nel linguaggio ampliato $L \cup \{\vec{c}\}$. Allora $T[\vec{c}]$ ha anch'essa la proprietà dell'isomorfismo (o rispettivamente del sottomodello).*

Dim.(Cenno) La dimostrazione si basa sul fatto che un modello di $T[\vec{c}]$ può essere visto semplicemente come una coppia $(\mathcal{A}, \vec{a})$ costituita da un modello $\mathcal{A}$ di T e una n-pla $\vec{a}$ di elementi di $\mathcal{A}$ arbitrariamente fissata che serve a interpretare le $\vec{c}$ (n è la lunghezza di $\vec{c}$). Il concetto di sottostruttura e di isomorfismo nel linguaggio ampliato si caratterizzano nel modo seguente. Dati due modelli $(\mathcal{A}, \vec{a})$ e $(\mathcal{B}, \vec{b})$ di $T[\vec{c}]$, si ha che il primo è una sottostruttura del secondo se e solo se $\mathcal{A}$ è una sottostruttura di $\mathcal{B}$ nel liguaggio L, e $\vec{b} = \vec{a}$. Notiamo anche che f è un isomorfismo tra le $L \cup \{\vec{c}\}$-strutture $(\mathcal{A}, \vec{a})$ a $(\mathcal{B}, \vec{b})$, se f manda $\mathcal{A}$ isomorficamente in $\mathcal{B}$ come L-strutture, e inoltre $f(a_i) = b_i$ (dove a_i è l'i-esimo elemento di $\vec{a}$ e b_i l'i-esimo elemento di $\vec{b}$). Con queste osservazioni la fine della dimostrazione si ottiene in modo del tutto automatico applicando le definizioni. QED

Teorema 11.15 *Se T è una L-teoria con la proprietà del sottomodello e la proprietà dell'isomorfismo, e il linguaggio L ha almeno un simbolo di costante, allora T ammette eliminazione dei quantificatori.*

Dim. Per il Lemma 11.5 basta dimostrare che ogni L-formula esistenziale della forma $\exists x\theta$, con θ senza quantificatori, equivale in T ad una formula senza quantificatori.

Consideriamo d'apprima il caso speciale in cui $\exists x\theta$ è chiusa, ovvero θ non contiene altre variabili libere oltre la x.

Per trovare una enunciato equivalente a $\exists x\theta$ senza quantificatori useremo il Lemma 11.7. Sia D l'insieme degli L-enunciati senza quantificatori (D è non vuoto in quanto L ha almeno un simbolo di costante) e siano $\mathcal{A}, \mathcal{A}'$ modelli di T con $\mathcal{A} \equiv_D \mathcal{A}'$. Dobbiamo mostrare che $\mathcal{A} \equiv_{\exists x\theta} \mathcal{A}'$. L'ipotesi $\mathcal{A} \equiv_D \mathcal{A}'$ (cioè $\mathcal{A}$ ed $\mathcal{A}'$ rendono veri gli stessi enunciati senza quantificatori) implica (e in effetti equivale) al fatto che le sottostrutture $\mathcal{B} \subseteq \mathcal{A}$ e $\mathcal{B}' \subseteq \mathcal{A}'$ costituite dalle interpretazioni dei termini chiusi, sono isomorfe tramite l'isomorfismo $f{:}\mathcal{B} \to \mathcal{B}'$ che manda $t^{\mathcal{A}}$ in $t^{\mathcal{A}'}$, dove t è un L-termine chiuso e $t^{\mathcal{A}}$ e $t^{\mathcal{A}'}$ sono le sue interpretazioni rispettivamente in $\mathcal{A}$ e in $\mathcal{A}'$. Questa mappa è ben definita in quanto se $t_1^{\mathcal{A}} = t_2^{\mathcal{A}}$, l'enunciato senza quantificatori $t_1 = t_2$ è vero in $\mathcal{A}$ e dunque in $\mathcal{A}'$, da cui $t_1^{\mathcal{A}} = t_2^{\mathcal{A}'}$. Lo stesso ragionamento con i ruoli di

$\mathcal{A}$ e $\mathcal{A}'$ scambiati mostra che la funzione è iniettiva. Il fatto che sia surgettiva dipende dal fatto che il dominio di $\mathcal{B}'$ è costituito dalle intepretazioni dei termini chiusi. Il fatto che preserva ogni funzione h del linguaggio è ovvio: $h^{\mathcal{A}}(t_1^{\mathcal{A}}, \ldots, t_n^{\mathcal{A}}) = h(t_1, \ldots, t_n)^{\mathcal{A}} \mapsto h(t_1, \ldots, t_n)^{\mathcal{A}'} = h^{\mathcal{A}'}(t_1^{\mathcal{A}'}, \ldots, t_n^{\mathcal{A}'})$. La proprietà dell'isomorfimo ci permette di estendere l'isomorfismo di L-strutture $f{:}\mathcal{B} \to \mathcal{B}'$ così stabilito ad un isomorfismo $\tilde{f}{:}\mathcal{C} \to \mathcal{C}'$ di modelli di T, con $\mathcal{B} \subseteq \mathcal{C} \subseteq \mathcal{A}$ e $\mathcal{B}' \subseteq \mathcal{C}' \subseteq \mathcal{A}'$. Per mostrare che $\mathcal{A} \equiv_{\exists x\theta} \mathcal{A}'$ supponiamo che $\mathcal{A}$ soddisfi $\exists x\theta$ e mostriamo che anche $\mathcal{A}'$ la soddisfa (il viceversa segue simmetricamente). La proprietà del sottomodello ci garantisce innanzitutto che l'enunciato $\exists x\theta$ è vero nel sottomodello $\mathcal{C} \subseteq \mathcal{A}$. Essendo $\mathcal{C}'$ isomorfo a $\mathcal{C}$ esso sarà vero anche in $\mathcal{C}'$ e poiché gli enunciati esistenziali veri in una struttura sono veri in qualsiasi sua estensione, esso sarà vero in $\mathcal{A}'$.

Abbiamo così concluso il caso in cui $\exists x\theta$ è una formula chiusa. Se invece θ contiene delle variabili libere $\vec{y}$ oltre la x, cioè $\theta = \theta(x, \vec{y})$, ci ricondurremo al caso precedente ampliando il linguaggio L con nuove costanti $\vec{c}$ che andremo a sostituire al posto delle $\vec{y}$. A tal fine osserviamo che dalla proprietà dell'isomorfismo e del sottomodello per la teoria T, segue che anche la teoria $T[\vec{c}]$ ha queste proprietà, dove $T[\vec{c}]$ è la teoria con gli stessi assiomi di T ma formulata nel linguaggio ampliato $L \cup \{\vec{c}\}$. Possiamo ora concludere la dimostrazione considerando la formula chiusa $\exists x\theta(x, \vec{c})$ del linguaggio ampliato ottenuta sostituendo le $\vec{y}$ con le $\vec{c}$. Per il caso speciale precedentemente dimostrato, applicato però alla teoria $T[\vec{c}]$, esiste un enunciato senza quantificatori $\phi(\vec{c})$ del liguaggio ampliato tale che $T[\vec{c}] \vdash \phi(\vec{c}) \leftrightarrow \exists x\theta(x, \vec{c})$. Visto che $T[\vec{c}]$ non contiene assiomi sulle constanti $\vec{c}$, possiamo dedurne che $T \vdash \forall\vec{y}(\phi(\vec{y}) \leftrightarrow \exists x\theta(x, \vec{y}))$ (a condizione che $\phi(\vec{c})$ non contenga quantificazioni sulle $\vec{y}$, cosa che possiamo assumere con un cambio di variabili vincolate). QED

12 Decidibilità della teoria dei campi algebricamente chiusi e della teoria dei numeri complessi

Si veda [van der Waerden, Algebra]. Un campo è algebricamente chiuso se ogni polinomio non nullo in una variabile, a coefficienti nel campo, ha uno zero nel campo. L'esempio più importante di campo algebricamente chiuso è dato dai numeri complessi. Non è difficile scrivere degli assiomi del primo ordine, in un linguaggio con $0, 1, +, \cdot$, i cui modelli siano tutti e soli i campi algebricamente chiusi. La condizione di esistenza di zeri per i polinomi non nulli richiede infiniti assiomi, uno per ogni grado. La teoria dei campi estesa con questi assiomi si chiama teoria dei campi algebricamente chiusi.

Lemma 12.1 *La teoria ACF dei campi algebricamente chiusi ha la proprietà del sottomodello.*

Dim. Siano $\mathcal{A} \subseteq \mathcal{B}$ campi algebricamente chiusi. Sia $\theta(x, \vec{a})$ una formula senza quantificatori con parametri $\vec{a}$ in $\mathcal{A}$, e sia $b \in \mathcal{B}$ tale che $\theta(b, \vec{a})$. Dobbiamo mostrare che esiste $a^* \in \mathcal{A}$ tale che $\theta(a^*, \vec{a})$. Possiamo assumere che $b \notin \mathcal{A}$ altrimenti non c'è nulla da dimostrare. Usando gli assiomi dei campi possiamo dimostrare che $\theta(x, \vec{a})$ equivale, in $\mathcal{A}$, ad una combinazione booleana di formule $f_1(x) = 0, \ldots, f_k(x) = 0$, dove gli f_i sono polinomi non nulli a coefficienti nel sottoanello generato dai parametri $\vec{a}$. Gli assiomi dei campi garantiscono che ogni f_i ha un numero finito di radici. Sia $S \subset \mathcal{A}$ un insieme finito che contiene le radici di ogni f_i. Poichè $\mathcal{A}$ è algebricamente chiuso, $\mathcal{A}$ è infinito. Ciò è ovvio se $\mathcal{A}$ ha caratteristica zero, poiché in quel caso $\mathcal{A}$ contiene una copia isomorfa dei razionali. Nel caso generale basta osservare che dato un sottoinsinsieme finito $\{a_1, \ldots, a_k\}$ di $\mathcal{A}$ possiamo sempre trovare un elemento di $\mathcal{A}$ che non vi appartiene considerando uno zero del polinomio $(x-a_1)(x-a_2)\cdot\ldots\cdot(x-a_k)+1$. Tale zero esiste in quanto $\mathcal{A}$ è algebricamente chiuso. Essendo dunque $\mathcal{A}$ infinito, possiamo fissare un elemento $a^* \in \mathcal{A}$, $a^* \notin S$. Dobbiamo avere $f_i(a^*) \neq 0$ e $f_i(b) \neq 0$ per ogni i. Abbiamo quindi $f_i(b) = 0 \leftrightarrow f_i(a^*) = 0$, e pertanto $\theta(b, \vec{a}) \leftrightarrow \theta(a^*, \vec{a})$, essendo $\theta(x, \vec{a})$ una combinazione booleana delle formule $f_i(x) = 0$. Ciò conclude la dimostrazione. QED

Data una estensione $\mathcal{B} \subseteq \mathcal{C}$ di campi, diciamo che $c \in \mathcal{C}$ è algebrico su $\mathcal{B}$, se c è uno zero di un polinomio a coefficienti in $\mathcal{B}$. L'insieme degli elementi si $\mathcal{C}$ algebrici su $\mathcal{B}$ è un sottocampo $\mathcal{F}$ di $\mathcal{C}$. Ogni elemento di $\mathcal{C}$ algebrico su $\mathcal{F}$ appartiene a $\mathcal{F}$. Ne segue che se $\mathcal{C}$ è algebricamente chiuso anche $\mathcal{F}$ lo è: infatti dato un polinomio a coefficienti in $\mathcal{F}$, questo ha uno zero in $\mathcal{C}$, ed essendo tale zero algebrico su $\mathcal{F}$ deve appartenervi.

Definizione 12.2 Una chiusura algebrica di un campo $\mathcal{B}$ è un campo algebricamente chiuso $\mathcal{C} \supseteq \mathcal{B}$ tale che ogni elemento di $\mathcal{C}$ è algebrico su $\mathcal{B}$.

Teorema 12.3 *(Esistenza e unicità della chiusura algebrica) Ogni campo ha una chiusura algebrica. Dato un isomorfismo f tra due campi, e considerate due chiusure algebriche dei campi dati, l'isomorfismo f si estende ad un isomorfismo delle due chiusure. In particolare due chiusure algebriche di uno stesso campo sono isomorfe, tramite un isomorfismo che fissa ogni elemento del campo base.*

Corollario 12.4 *La teoria ACF dei campi algebricamente chiusi ha la proprietà dell'isomorfismo.*

Dim. Useremo il teorema di unicità della chiusura algebrica. Sia $f: \mathcal{D} \to \mathcal{D}'$ un isomorfismo tra sottostrutture di campi algebricamente chiusi $\mathcal{A}$ ed $\mathcal{A}'$. Poiché il linguaggio della teoria contiene $0, 1, -1, +, \cdot$, $\mathcal{D}$ e $\mathcal{D}'$ sono anelli, ed essendo sottoanelli di un campo sono domini di integrità (cioè verificano $xy = 0 \to x = 0 \vee y = 0$). Possiamo estendere f ad un isomorfismo $f_1: \mathcal{B} \to \mathcal{B}'$ tra i campi dei quozienti $\mathcal{B} \subseteq \mathcal{A}$ e $\mathcal{B}' \subseteq \mathcal{A}'$ di $\mathcal{D}$ e $\mathcal{D}'$ rispettivamente, ponendo $f_1(x/y) = f_1(x)/f_1(y)$ $(x, y \in \mathcal{B})$. Sia ora $\mathcal{C}$ l'insieme dei punti di $\mathcal{A}$ algebrici su $\mathcal{B}$ e sia $\mathcal{C}'$ l'insieme dei punti di $\mathcal{A}'$ algebrici su $\mathcal{B}'$. Segue dalle proprietà generali dei campi che $\mathcal{C}$ e $\mathcal{C}'$ sono campi. Inoltre, poiché $\mathcal{A}$ ed $\mathcal{A}'$ sono algebricamente

chiusi, anche $\mathcal{C}$ e $\mathcal{C}'$ lo sono. Possiamo concluderne che $\mathcal{C}$ e $\mathcal{C}'$ sono chiusure algebriche di $\mathcal{B}$ e $\mathcal{B}'$, e per l'unicità della chiusura algebrica l'isomorfismo f_1, e quindi anche f, si estende ad un isomorfismo tra $\mathcal{C}$ e $\mathcal{C}'$. QED

Corollario 12.5 *La teoria dei campi algebricamente chiusi ammette eliminazione dei quantificatori.*

Corollario 12.6 *La teoria ACF_0 dei campi algebricamente chiusi di caratteristica zero fornisce una assiomatizzazione ricorsiva e completa della teoria dei numeri complessi. La teoria dei numeri complessi è quindi decidibile.*

Dim. Basta dimostrare che una formula chiusa ϕ è vera in un modello di ACF_0 se e solo se è vera in tutti i modelli. Osserviamo che ogni modello di ACF_0 contiene una sottostruttura isomorfa ai numeri razionali. Poiché ACF_0 contiene ACF, ϕ equivale, in ACF_0, ad una formula chiusa θ priva di quantificatori. Essendo priva di quantificatori θ vale in una struttura se e solo se vale in una sottostruttura. Possiamo concludere che ϕ vale in un modello di ACF_0 se e solo se θ vale nei razionali. QED

13 Decidibilità della teoria dei campi reali chiusi e della teoria dei numeri reali

Si veda [van der Waerden, Algebra]. Un campo ordinato è reale chiuso se ogni polinomio in una variabile che cambia segno, a coefficienti nel campo, ha uno zero nel campo. L'esempio più importante di campo reale chiuso è dato dai numeri reali (dove ogni funzione continua che cambia segno, non necessariamente polinomiale, ha uno zero). Non è difficile scrivere degli assiomi del primo ordine, in un linguaggio con $0, 1, +, \cdot, \geq$, i cui modelli siano tutti e soli i campi reali chiusi. La condizione di esistenza di zeri richiede infiniti assiomi, uno per ogni grado. La teoria dei campi ordinati estesa con questi assiomi si chiama teoria dei campi reali chiusi.

Proposizione 13.1 *Se $\mathcal{F}$ è un campo reale chiuso, l'estensione algebrica $\mathcal{F}(\sqrt{-1})$ è un campo algebricamente chiuso. Ne segue che in un campo reale chiuso $\mathcal{F}$, ogni polinomio monico $f(x)$ si fattorizza in fattori lineari o quadratici della forma $(x-\alpha)$, $(x-\beta)^2+c$, con $\alpha, \beta, c \in \mathcal{F}$, $c > 0$.*

Corollario 13.2 *Data un'estensione di campi ordinati reali chiusi $\mathcal{A} \subseteq \mathcal{B}$, e un polinomio $f(x) \in \mathcal{A}[x]$, $f(x)$ ha gli stessi zeri in $\mathcal{A}$ e in $\mathcal{B}$. Inoltre dati due elementi $b, b' \in \mathcal{B}$ situati nello stesso intervallo determinato dagli zeri di $f(x)$, i segni di $f(b)$ e di $f(b')$ devono coincidere.*

Dim. I fattori quadratici $(x-\beta)^2 + c$, $c > 0$, della scomposizione di $f(x)$ in $\mathcal{A}$ non possono avere degli zeri in $\mathcal{B}$ in quanto in ogni campo ordinato i quadrati

sono non negativi. Questo dimostra la prima affermazione. Per la seconda basta osservare che tra due punti che determinano un cambiamento di segno di $f(x)$ ci deve essere uno zero di $f(x)$. QED

Lemma 13.3 *La teoria dei campi ordinati reali chiusi ha la proprietà del sottomodello.*

Dim. Siano $\mathcal{A} \subseteq \mathcal{B}$ campi ordinati reali chiusi. Sia $\theta(x, \vec{a})$ una formula senza quantificatori con parametri $\vec{a}$ in $\mathcal{A}$, e sia $b \in \mathcal{B}$ tale che $\theta(b, \vec{a})$. Dobbiamo mostrare che esiste $a^* \in \mathcal{A}$ tale che $\theta(a^*, \vec{a})$. Poiché $\theta(x, \vec{a})$ è senza quantificatori, essa equivale ad una combinazione booleana di formule atomiche, ovvero uguaglianze e disuguaglianze tra termini. Usando gli assiomi dei campi ordinati possiamo dimostrare che ogni termine definisce una funzione polinomiale, e pertanto $\theta(x, \vec{a})$ equivale, in $\mathcal{A}$, ad una combinazione booleana di espressioni della forma "$f(x) = 0$" con $f(x) \in \mathcal{A}[x]$, oppure "$g(x) \leq 0$" con $g(x) \in \mathcal{A}[x]$. Esiste un insieme finito $S \subseteq \mathcal{A}$ che contiene le radici di tutti questi polinomi. Poiché in ogni campo ordinato l'ordine è denso e senza massimo e minimo, possimo certamente trovare un punto a^* di $\mathcal{A}$ tale che a^* e b sono situati nello stesso intervallo determinato dai punti di S (se $b \in S$ prendiamo $a^* = b$). Per il corollario 13.2 a^* e b verificheranno le stesse uguaglianze e disuguaglianze polinomiali, rispetto all'insieme finito di polinomi considerato, ed essendo $\theta(x, \vec{a})$ una combinazione booleana di tali uguaglianze e disuguaglianze, si avrà $\theta(a^*, \vec{a}) \leftrightarrow \theta(b, \vec{a})$. Ne segue $\theta(a^*, \vec{a})$, come desiderato. QED

Definizione 13.4 Una chiusura reale di un campo ordinato $\mathcal{B}$ è un campo ordinato reale chiuso $\mathcal{C} \supseteq \mathcal{B}$ (estensione di campi ordinati) tale che ogni elemento di $\mathcal{C}$ è algebrico su $\mathcal{B}$.

Teorema 13.5 *(Esistenza e unicità della chiusura reale di un campo ordinato) Ogni campo ordinato $\mathcal{A}$ ha una chiusura reale. Dato un isomorfismo $f: \mathcal{A} \to \mathcal{A}'$ tra due campi ordinati, e considerate due loro rispettive chiusure reali $\mathcal{B}$ e $\mathcal{B}'$, l'isomorfismo f si estende ad un isomorfismo $\tilde{f}: \mathcal{B} \to \mathcal{B}'$ delle chiusure. In particolare, prendendo come f l'identità, due chiusure reali di un campo ordinato sono isomorfe.*

Dim. (Cenno) Dato un campo ordinato $\mathcal{A}$, consideriamo un sottocampo $\mathcal{B}$ della chiusura algebrica $\overline{\mathcal{A}}$ di $\mathcal{A}$ che contiene tutte le radici quadrate degli elementi positivi di $\mathcal{A}$ (ciò garantisce che ogni ordine di campo su $\mathcal{B}$ deve estendere quello di $\mathcal{A}$) ed è massimale rispetto alla proprietà che -1 non è somma di quadrati (un campo è ordinabile se e solo se ha questa proprietà). Tale $\mathcal{B}$ ammette un unico ordine, e con tale ordine è una chiusura reale di $\mathcal{A}$.

Dato ora un isomorfimo $f: \mathcal{A} \to \mathcal{A}'$ tra due campi ordinati, e considerate due loro rispettive chiusure reali $\mathcal{B}$ e $\mathcal{B}'$, l'isomorfismo f si estende ad un isomorfismo $\tilde{f}: \mathcal{B} \to \mathcal{B}'$ che manda l'n-sima radice (nell'ordine di $\mathcal{B}$) di un polinomio $p(x) = \Sigma_i a_i x^i$ a coefficienti in $\mathcal{A}$, nell'n-esima radice (nell'ordine di $\mathcal{B}'$) del polinomio

$p^f(x) = \Sigma_i f(a_i)x^i$ (un teorema di Sturm ci garantisce che il numero delle radici di $p(x)$ e $p^f(x)$ è lo stesso). QED

Teorema 13.6 *La teoria dei campi reali chiusi ha la proprietà dell'isomorfismo.*

Dim. Useremo il teorema di unicità della chiusura reale. Sia $f: \mathcal{D} \to \mathcal{D}'$ un isomorfismo tra sottostrutture di campi algebricamente chiusi $\mathcal{A}$ ed $\mathcal{A}'$. Poiché il linguaggio della teoria contiene $0, 1, -1, +, \cdot, \geq$, $\mathcal{D}$ e $\mathcal{D}'$ sono anelli ordinati ed f è un isomorfismo di anelli ordinati. Essendo sottoanelli di un campo $\mathcal{D}$ e $\mathcal{D}'$ sono domini di integrità (cioè verificano $xy = 0 \to x = 0 \vee y = 0$). Possiamo estendere f ad un isomorfismo $f_1: \mathcal{B} \to \mathcal{B}'$ tra i campi dei quozienti $\mathcal{B} \subseteq \mathcal{A}$ e $\mathcal{B}' \subseteq \mathcal{A}'$ di $\mathcal{D}$ e $\mathcal{D}'$ rispettivamente, ponendo $f_1(x/y) = f_1(x)/f_1(y)$ $(x, y \in \mathcal{B})$. Osserviamo che f_1 deve rispettare l'ordine in quanto il segno di un quoziente è univocamente determinato dal segno del numeratore e denominatore. Sia ora $\mathcal{C}$ l'insieme dei punti di $\mathcal{A}$ algebrici su $\mathcal{B}$ e sia $\mathcal{C}'$ l'insieme dei punti di $\mathcal{A}'$ algebrici su $\mathcal{B}'$. Segue dalle proprietà generali dei campi che $\mathcal{C}$ e $\mathcal{C}'$ sono campi. Inoltre, poiché $\mathcal{A}$ ed $\mathcal{A}'$ sono reali chiusi, anche $\mathcal{C}$ e $\mathcal{C}'$ lo sono. Possiamo concluderne che $\mathcal{C}$ e $\mathcal{C}'$ sono chiusure reali di $\mathcal{B}$ e $\mathcal{B}'$, e per l'unicità della chiusura reale l'isomorfismo f_1, e quindi anche f, si estende ad un isomorfismo tra $\mathcal{C}$ e $\mathcal{C}'$. QED

Corollario 13.7 *La teoria dei campi ordinati reali chiusi ammette eliminazione dei quantificatori.*

Corollario 13.8 *La teoria RCF dei campi ordinati reali chiusi fornisce una assiomatizzazione completa della teoria dei numeri reali. La teoria dei numeri reali è quindi decidibile.*

Dim. Basta dimostrare che una formula chiusa ϕ è vera in un modello di RCF se e solo se è vera in tutti i modelli. Osservarviamo ora che ogni modello di RCF contiene una sottostruttura isomorfa ai numeri razionali come campo ordinato. Poiché RCF elimina i quantificatori, ϕ equivale, in RCF, ad una formula θ priva di quantificatori. Essendo priva di quantificatori θ vale in una struttura se e solo se vale in una sottostruttura. Possiamo concludere che ϕ vale in un modello di RCF se e solo se θ vale nei razionali. QED

14 Esercizi

Alcuni esercizi possono essere eccessivamente difficili. Non ci si scoraggi e si provi comunque a pensarci.

Esercizio 14.1 Fare tutti gli esercizi menzionati in classe o scritti nelle note.

Esercizio 14.2 Si mostri nel sistema di Hilbert Frege che $\vdash \exists x\alpha \to \neg\forall x\neg\alpha$.

Esercizio 14.3 Sia Γ il seguente insieme di assiomi:
1) $\forall x(x + 0 = x)$,
2) $\forall xy(x + s(y) = s(x + y))$,
3) $\forall xy(s(x) = s(y) \to x = y)$,
4) $\forall x\neg(s(x) = 0)$,
5) $\forall x(x \neq 0 \to \exists y(x = s(y))$.
Stabilire se:
a) $\Gamma \models \forall x(x + x = s(0) \to x \neq 0)$.
b) $\Gamma \models \neg\exists y[y + y = s(0)]$.
c) $\Gamma \models \forall xy(x + y = y + x)$.

Esercizio 14.4 Sia $L = (0, s, R, \min)$ dove 0 è un simbolo di costante, s è un simbolo di funzione unaria, R è un simbolo di predicato binario, min è un simbolo di predicato ternario.

Sia Γ il seguente insieme di L-formule:
$\forall xy(R(x, y) \to \min(x, y, x)$
$\forall xyz(R(x, y) \wedge R(y, z) \to R(x, z))$
$\forall xR(x, x)$
$\forall xR(x, s(x))$

Nella interpretazione che abbiamo in mente R è la relazione di minore o uguale, ma ci potrebbero essere altre interpretazioni. Trovate l'insieme di tutti i termini chiusi t tali che:
a) $\Gamma \models \min(s0, sss0, t)$.
Trovate l'insieme di tutti i termini chiusi t tali che:
b) $\Gamma \models \min(s0, t, s0)$.
Giustificate la risposta.

Esercizio 14.5 Si dimostri in modo dettagliato che ogni formula ϕ in un linguaggio del primo ordine è logicamente equivalente ad una formula ψ in forma normale prenessa (ovvero con tutti i quantificatori all'inizio).

Esercizio 14.6 Si dimostri che la teoria degli ordini lineari densi senza nè massimo nè minimo elemento è completa, e pertanto equivale alla teoria completa dei numeri razionali come insieme ordinato. Se ne deduca che la teoria degli ordini lineari densi ha esattamente quattro estensioni complete non equivalenti. Suggerimento: per dimostrare la completezza si usi la proprietà dell'isomorfismo e del sottomodello.

Esercizio 14.7 Usare il teorema di compattezza per dimostrare che se un grafo infinito non può essere colorata con 3 colori in modo da avere nodi adiacenti di colore diverso, allora anche un suo sottografo finito non può essere colorato con 3 colori.

Suggerimento: si trovi una teoria i cui modelli corrispondono alle colorazioni del grafo.

Esercizio 14.8 Usare il teorema di compattezza per mostrare che non esiste alcuna formula del primo ordine ϕ nella segnatura $\{\leq\}$ tale che $M \models \phi$ se e

solo se M è un buon ordine, dove un buon ordine è un ordine lineare senza successioni decrescenti infinite. In altre parole la classe dei buoni ordini non è una classe elementare.

Esercizio 14.9 Mostrare che se A è una L-struttura finita e B è una L-struttura che soddisfa gli stessi L-enunciati di A, allora A è isomorfa a B. Mostrare che ciò non è vero se non si assume la finitezza.

Esercizio 14.10 Sia $T = ED(\mathbf{R})$ il diagramma elementare di $(\mathbf{R}; \leq)$ (nella segnatura $L = \{\leq\} \cup \{c_a \mid a \in \mathbf{R}\}$). Sia c un nuovo simbolo di costante. Si determini quante sono le teorie complete nella segnatura $L \cup \{c\}$ i cui assiomi includono quelli di T .

Esercizio 14.11 Una teoria si dice decidibile se l'insieme dei suoi teoremi è un insieme ricorsivo. Si dimostri che ogni teoria coerente decidibile ha una estensione completa decidibile.

Esercizio 14.12 Si dimostri che esiste un campo ordinato M elementarmente equivalente al campo ordinato dei numeri reali ma contenente degli elementi non nulli minori in modulo di ogni razionale (possiamo supporre che M contenga i razionali, essendo i razionali isomorficamente immergibili in ogni campo ordinato).

Esercizio 14.13 Si dimostri per induzione sul numero degli elementi che su ogni insieme finito è possibile dare un ordine totale. Si usi poi il teorema di compattezza per il calcolo dei predicati per estendere il risultato ad insiemi infiniti.

Esercizio 14.14 Si assuma il seguente fatto: $Th(\mathbf{N}, 0, s, +)$ è una teoria decidibile mentre $Th(\mathbf{N}, 0, s, +, \cdot)$ non lo è.

1) Dedurre che non esiste nessuna L-formula $\phi(x, y, z)$, con $L = \{0, s, +\}$, tale che $\mathbf{N} \models \phi(a, b, c)$ se e solo se $a \cdot b = c$.

Quindi la moltiplicazione non è definibile al primo ordine a partire da zero successore e addizione.

2) Mostrare che la moltiplicazione è definibile al secondo ordine a partire da zero successore e addizione. (In effetti è definibile a partire dal nulla!).

Esercizio 14.15 Dimostrare che esistono $2^{\aleph_0}$ modelli numerabili, a due a due non isomorfi, e ciascuno elementarmente equivalenti alla struttura dei numeri naturali (con $+, \cdot$).

Suggerimento: si consideri un sottoinsieme S dei numeri primi, si ampli il linguaggio con un simbolo di costante c, e si consideri una teoria che estende la teoria completa dei numeri naturali con degli assiomi che dicono che c è divisibile per tutti i primi di S e non è divisibile per i primi non in S. Si usi il teorema di compattezza per mostrare la coerenza della teoria.

Esercizio 14.16 (Difficile) Ogni tautologia si può dedurre dai quattro schemi di tautologia A0 - A4 (definiti in queste note nella sezione sugli assiomi logici proposizionali), usando solamente la regola di Modus Ponens.