LOGICA PROPOSIZIONALE

PROPOSIZIONI: ciò che viene espresso da un enunciato del quale abbia senso chiedersi se esso sia vero o falso.

CONNETTIVI PROPOSIZIONALI: ¬, ∧ , ∨ , →, ↔ sono usati per costruire proposizioni semplici a partire dalle complesse

LINGUAGGIO PROPOSIZIONALE: un insieme L di simboli, chiamati variabili proposizionali

FORMULA PROPOSIZIONALE: stringa di simboli costruita a partire dalle variabili proposizionali e dai connettivi e dalle parentesi

INTERPRETAZIONI BOOLEANE: (o valutazione booleana) in un linguaggio proposizionale L è una funzione M che associa ad ogni
variabile proposizionale A ∈ L un valore M(A) ∈ {0, 1} (0 per falso, 1 per vero)

TAUTOLOGIA: Una formula proposizionale Φ si dice una tautologia se è vera per tutte le interpretazioni delle sue variabili

CONSEGUENZA (TAUTO) LOGICA: Una formula proposizionale β è conseguenza logica di una formula proposizionale α, se la formula α → β è un tautologia. Scriviamo α |= β. Più in generale una formula β è conseguenza logica di un insieme di altre formule α1, . . . , αn, se (α1 ∧ . . . ∧ αn) →β è una tautologia. Scriviamo α1, . . . , αn |= β.

CONSEGUENZA LOGICA: Diciamo che una formula proposizionale Φ è conseguenza logica di un insieme di formule T se i modelli di T sono contenuti in quelli di Φ, cioè se ogni modello di T rende vera Φ. Osserviamo che se T è vuoto tutte le intepretazioni sono modelli di T (in quanto, proprio perché vuoto, non può contenere una formula che viene resa falsa). In base alle definizioni |= Φ se e solo se Φ è una tautologia.

MODELLI (di un insieme di formule T): insieme delle valutazioni tali che ogni formula è sempre vera in T

FORMA NORMALE DISGIUNTIVA: Sia F un insieme di formule e sia ψ una loro combinazione booleana. Allora ψ può essere messa in forma normale disgiuntiva, ovvero equivale ad una disgiunzione di congiunzioni di formule in F o negazioni di formule in F

FORMA NORMALE CONGIUNTIVA: Sia F un insieme di formule e sia ψ una loro combinazione booleana. Allora ψ può essere messa in forma normale congiuntiva, ovvero equivale ad una congiunzione di disgiunzioni di formule in F o negazioni di formule in F

Ogni formula proposizionale può essere messa in forma normale disgiuntiva o in forma normale congiuntiva

LOGICA DEL PRIMO ORDINE

Si tratta della logica PREDICATIVA. A diffrenza di quella proposizionale, questa comprende i quantificatori.

È un linguaggio formale che serve per gestire meccanicamente enunciati e ragionamenti che coinvolgono i connettivi logici, le relazioni e i quantificatori. L' espressione "del primo ordine" indica che c'è un insieme di riferimento e i quantificatori possano riguardare solo gli elementi di tale insieme e non i sottoinsiemi; ad esempio si può dire "per tutti gli x elementi dell'insieme vale P(x)" ma non si può dire "per tutti i sottoinsiemi A vale P(A)" (le teorie in cui ci sono quantificatori che spaziano sui sottoinsiemi dell'insieme di riferimento sono dette invece del secondo ordine).

PREDICATI: Un predicato o relazione è una funzione che associa agli elementi di un dato dominio di oggetti un valore di verità, che può essere vero o falso

LINGUAGGIO: Un linguaggio è un insieme L di simboli (anche vuoto) divisi in tre categorie, simboli di costante, simboli di funzione, e simboli di relazione.

ARIETÀ: ad ogni simbolo è associato un numero naturale detto "arietà" del simbolo, che servirà ad indicare il numero degli argomenti a cui va applicato il simbolo. L'arietà di ogni simbolo di costante è zero, mentre le arietà dei simboli di funzione e di relazione sono arbitrari interi positivi (ad es. la relazione < ha arietà 2)

L-STRUTTURA: Sia L una linguaggio del primo ordine. Una L-struttura M consiste di:

Un insieme non vuoto dom(M) detto dominio della struttura

Una funzione c → c_M che associa ad ogni simbolo di costante c di L un elemento c_M ∈ dom(M), detto interpretazione del simbolo c in M

Una funzione f → f_M che associa ad ogni simbolo di funzione f di L di arietà n, una funzione f_M : dom(M)^n → dom(M), detta interpretazione del simbolo f in M

Una funzione R → R_M che associa ad ogni simbolo di relazione R di L di arietà n, una relazione R_M ⊆ dom(M)^n, detta interpretazione del simbolo R in M

Identifichiamo una relazione ad n posti con l'insieme delle n-uple che la verificano

TERMINI e FORMULE: Fissiamo un linguaggio L e un insieme infinito V di simboli chiamati variabili (ad esempio: L={0, 1,+,.,<}, V={x,y,z,...}). In generale V è numerabile.

TERMINI: Definiamo induttivamente l'insieme dei L-termini con variabili da V come il più piccolo insieme di espressioni tale che:

Ogni variabile x ∈ V è un L-termine

ogni simbolo di costante di L è un L-termine

se t1, . . . , tn sono L-termini, e f è un simbolo di funzione di arietà n della segnatura L, allora f(t1, . . . , tn) è un L-termine

Un termine in cui non occorrano variabili viene detto termine chiuso. Chiaramente i termini chiusi possono esserci solo se il linguaggio contiene almeno un simbolo di costante

FORMULE: Si distinguono in L-formule atomiche e L-formule (non atomiche)

Una L-formula atomica è una espressione della forma t1 = t2, dove t1, t2 sono L-termini, oppure della forma R(t1, . . . , tn), dove R è un simbolo di relazione n-aria di L (se ve ne sono) e t1, . . . , tn sono L-termini

L'insieme delle L-formule è definito induttivamente come il più piccolo insieme di espressioni tale che

Ogni L-formula atomica è una L-formula

Se α e β sono L-formule, allora (¬α), (α ∧ β), (α ∨ β) e (α → β) sono L-formule

Se α ` e una L-formula e x ` e una variabile, allora (∀ xα) e (∃ xα) sono L-formule

VARIABILI LIBERE DI UNA FORMULA: Un'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 ∀ x o ∃ x. Un'occorrenza non legata si dice libera. Le variabili libere di una formula sono le variabili che hanno almeno una occorrenza libera nella formula. Se le variabili libere di ϕ sono incluse in {x1, . . . , xn} scriveremo anche ϕ(x1, . . . , xn) invece di ϕ. Una formula senza variabili libere viene detta formula chiusa o enunciato.

AMBIENTE: Sia L una linguaggio del primo ordine e M una L-struttura. Un ambiente è una funzione v: Variabili → M

SEMANTICA DI TARSKI

STUDIA LA VERITÀ: Data una L-struttura M vogliamo definire cosa significhi che una L-formula ϕ è vera in M

IDEA: la formula risulta vera se si interpretano i simboli di L come prescrive la L-struttura M, e si interpretano i quantificatori ∀ x e ∃ x con ∀ x ∈ M ed ∃ x ∈ M rispettivamente, ovvero si suppone che le variabili varino su elementi di dom(M). I connettivi booleani sono intepretati come al solito tramite le tavole di verità, e il simbolo = viene interpretato come la relazione di uguaglianza.

"oggi piove" è vera se e solo se oggi piove

"ϕ è verain M"

Definizione induttiva sulla complessità di ϕ

Le formule possono contenere termini, quindi occorre prima dare la semantica dei termini

SEMANTICA DEI TERMINI

VALUTAZIONE DELLE VARIABILI: Sia { x1, . . . , xn} un insieme di variabili e sia M una L-struttura. Una valutazione in M delle variabili x1, . . . , xn è una funzione v : {x1, . . . , xn} → dom(M) che assegna a ciascuna delle variabili xi un valore ai = v(ai) nel dominio della L-struttura M. Scriveremo anche v = (a1/x1, . . . , an/xn) per indicare tale valutazione

Dato un L-termine t le cui variabili sono incluse nel dominio della valutazione v definiamo induttivamente M(t(v)) ∈ dom(M) nel modo seguente:

- Se x è una variabile e v è una valutazione che associa a x il valore a ∈ M, allora M(x(v)) = a
- Se c è un simbolo di costante di L, allora M(c(v)) = c_M
- Se t è della forma f(t1, . . . , tn), allora M(t(v)) = f_M(M(t1(v)), . . . , M(tn(v)))

Interpreto le costanti come in M, le variabili secondo la loro valutazione e le funzioni come la funzione interpretata in M dei termini interpretati

SEMANTICA DELLE FORMULE

Sia M una L-struttura, sia Φ una L-formula le cui variabili libere siano incluse in { x1, . . . , xn} e sia v = (a1/x1, . . . , an/xn) una valutazione delle variabili con v(xi) = ai ∈ M. Diciamo che Φ(v) è vera in M, e scriviamo M |= Φ(v), se ciò segue dalle seguenti clausole induttive. L'induzione viene fatta sul numero dei connettivi della formula.

ATOMICHE

- M |= R(t1, . . . , tn)(v) se e solo se (M(t1(v)), . . . , M(tn(v))) ∈ RM;
- M |= t1 = t2 se e solo se M(t1(v)) e M(t2(v)) sono lo stesso elemento

CONNETTIVI BOOLEANI

- M |= ¬Φ(v) se e solo se M |≠ Φ(v) (cioè non vale M |= Φ(v));
- M |= (Φ ∧ ψ)(v) se e solo se M |= Φ(v) e M |= ψ(v);
- M |= (Φ ∨ ψ)(v) se e solo se M |= Φ(v) o M |= ψ(v);
- M |= (Φ → ψ)(v) se e solo se M |≠ Φ(v) o M |= ψ(v).

Si ottiene tramite le tavole di verità

QUANTIFICATORI

- M |= (∀ xΦ)(v) se e solo se per ogni a ∈ dom(M), M |= Φ(a/x, v);
- M |= (∃ xΦ)(v) se esiste a ∈ dom(M) tale che M |= Φ(a/x, v).

(a/x, v) = la valutazione che coincide con v sulle variabili diverse da x ed assegna ad x il valore a.

ATTENZIONE: M |= Φ(v) ≠ T|=Φ

Ogni modello (insieme di valutazioni) di T (insieme di L-formule) rende vera Φ

Φ(v) è vera in M (struttura)

ESEMPIO

Sia L = {0, 1, +, ·}. La formula ∀ x∃ y(x · y = 1) è vera nella L-struttura R (l'anello dei reali) e falsa in Z (l'anello degli interi), in quanto nei reali ogni elemento ha un inverso moltiplicativo mentre in Z ciò non è vero.

TEORIE E MODELLI

TEORIA: È il dato di

- Linguaggio L
- L-formule chiuse dette assiomi
- Esempio: La teoria dei gruppi
  - L={*,e, inv}
    - * =funzione binaria
    - e=costante (el. neutro)
    - inv= funzione inverso
  - Assiomi
    - -elemento neutro: x*e=e*x=x
    - -inverso: inv(x)*x=x*inv(x)=e
    - -associatività: x*(y*z)=(x*y)*z

MODELLO

- Un modello di una L-teoria T è una L-struttura in cui risultano veri tutti gli assiomi di T
- Se M è un modello di T scriviamo M |= T. Quindi M |= T se per ogni assioma Φ di T, si ha M |= Φ.
- Una L-teoria T si dice soddisfacibile, o semanticamente coerente, se ha almeno un modello.
- Esempio: un gruppo è, per definizione, un modello della teoria dei gruppi

CONSEGUENZA LOGICA

- Sia Φ una L-formula chiusa e T una L-teoria. Diciamo che Φ segue logicamente da T, e scriviamo T |= Φ, se Φ è vera in tutti i modelli di T, ovvero non esiste alcuna L-struttura che renda veri tutti gli assiomi di T e non renda vera Φ
- In altre parole:
  T |= Φ se e solo se ModL(T) ⊆ ModL(Φ).
- In particolare se T è insoddisfacibile, cioè se ModL(T) = ∅ , allora vale sempre T |= Φ (in quanto l'insieme vuoto è contenuto in ogni altro insieme).

ESPANSIONI

- Dati due linguaggi L ed L' ⊃ L, diciamo che la L'-struttura A è una espansione della L-struttura B (B è una restrizione di A), se A e B hanno lo stesso dominio e interpretano nello stesso modo i simboli di L
- Ad esempio il gruppo (R, +, 0) è una restrizione del campo (R, +, ·, 0, 1)
- Dato un insieme T di L-enunciati (assiomi) e L'⊇ L, possiamo pensare T come ad una L-teoria o ad una L'-teoria

ESEMPI DI TEORIE

ARITMETICA DI ROBINSON

o Q di Robinson

L={0,s,+,.}

- 0=simbolo di costante
- s=simbolo di funzione unaria
- +=simbolo di funzione binaria
- .=simbolo di funzione binaria

Assiomi: ∀ x, ∀ y

- Q1: s(x)=s(y) → x=y
- Q2: 0≠s(x)
- Q3: x≠0 → ∃ y(x=s(y))
- Q4: x+0=x
- Q5: x+s(y)=s(x+y)
- Q6: x.0=0
- Q7: x.s(y)= x.y+x

Modelli

Un modello dell'aritmetica di Robinson è per definizione un insieme non vuoto dotato di uno zero 0, un successore s, e due operazioni +, . che verificano gli assiomi Q1-Q7

Un modello ovvio è N (i numeri naturali)

L'anello dei polinomi Z[t]+ è un modello

Consideriamo Z[t] con le seguenti interpretazioni

- 0=polinomio costante 0
- s=funzione successore che manda p(t) in p(t)+polinomio costante 1
- Solite interpretazioni di + e . in Z[t]

Z[t] verifica tutti gli assiomi tranne Q2, poiché il polinomio costante -1 è il predecessore di 0

Per ottenere un modello dell'aritmetica di Robinson possiamo considerare la sottostruttura Z[t]+ ⊆ Z[t]

consiste di tutti i polinomi a0+a1.t+. . .+an.t^n con an > 0 (gli altri coefficienti ai possono anche essere negativi o zero) e dei polinomi costanti a0 con a0 ≥ 0.

∀ x∃ y(y + y = x) ∨ ∃ y(y + y + S(0) = x)
(ogni numero è pari o dispari)

- vera in N
- falsa in Z[t]+ (non c'è il polinomio t/2)

La formula non è conseguenza logica degli assiomi Q1-Q7

La formula è "indipendente" dagli assiomi di Robinson, i quali pertanto sono "incompleti"

La sua negazione neanche lo è (vale in Z[t]+ ma non in N)

ARITMETICA DI PEANO

PA=Peano Arithmetic

L'aritmetica di Peano del primo ordine si ottiene aggiungendo a Q infiniti assiomi chiamati assiomi di induzione

Consideriamo una coppia (Φ, x) dove Φ è una formula del primo ordine di L, e x è una variabile libera di Φ (la variabile su cui facciamo l'induzione)

Alla coppia (Φ, x) associamo l'assioma Ind(Φ, x) definito come [Φ(0) ∧ ∀ x(Φ(x) → Φ(Sx)) → ∀ yΦ(y)]

La notazione Φ(t), indica la formula ottenuta sostituendo t al posto delle occorrenze libere di x in Φ

La formula Φ potrebbe contenere altre variabili libere oltre alla x

Se Φ = Φ(x, z) ha come variabili libere x e z, l'assioma Ind(Φ,x) è: ∀ z[Φ(0, z)∧ ∀ x(Φ(x, z) → Φ(Sx, z)) → ∀ yΦ(y, z)], dove l'induzione si fa su x e l'altra variabile libera z si comporta come un parametro

DEDUZIONE NATURALE

T |- Φ

- È una relazione di dimostrabilità formale
- A posteriori risulterà equivalente alla relazione di conseguenza logica
- A sinistra del segno metteremo un insieme di formule, a destra una singola formula
- Se vale la relazione diremo che Φ è dimostrabile a partire da T

REGOLE DI INFERENZA

- Caso Proposizionale — Riguarda i connettivi booleani e la RAA (reductio ad absurdum)
- Caso Predicativo — Si parte dal caso proposizionale e si aggiungono le regole per i quantificatori e l' uguaglianza

TEOREMA DI CORRETTEZZA

Una regola di inferenza è corretta se, rimpiazzando nella regola |= al posto di |-, il giudizio al di sotto della barra verticale è valido ogniqualvolta lo sono quelli al di sopra della barra

- Tutte le regole della deduzione naturale sono corrette — Si dimostra verificando la correttezza di tutte le regole
- Teorema di correttezza: Se T|- θ, allora T |= θ — Si dimostra per induzione sulla definizione di T |- ϕ

TEOREMA DI COMPATTEZZA SINTATTICA

- Se T |- θ allora esiste un sottoinsieme finito T ' $\subseteq$ T tale che T' |- θ. — Si dimostra per induzione sulla definizione di T |- θ
- In particolare, prendendo come θ la formula sempre falsa $\perp$, si ottiene che una teoria T è sintatticamente coerente se e solo se ogni sua sottoteoria finita è sintatticamente coerente

TEOREMA DI COMPLETEZZA

TIPI DI TEORIE

- TEORIE COERENTI E INCOERENTI
  - Una teoria T si dice incoerente (o contraddittoria) se T |- ⊥ (formula sempre falsa)
  - Diciamo che T è coerente se non è incoerente
- TEORIE COMPLETE
  - Una L-teoria coerente T si dice completa se data una Lformula Φ vale T |- Φ oppure T |- ¬Φ
  - Esempi
    - La teoria dei gruppi non è completa: tramite gli assiomi non riesco a dimostrare se un gruppo è abeliano o no
    - ZFC (teoria degli insiemi di Zermelo-Frenkel con l'assioma della scelta) non è completa: non riesco a dimostrare l'ipotesi del continuo (ogni sottoinsieme infinito di R è in bigezione con R o con N)
    - La teoria degli anelli commutativi con soli due elementi è completa perché ha un unico modello a meno di isomorfismo: Z/(2)
    - ACF0 (teoria dei campi algebricamente chiusi di caratteristica 0) è completa
- TEORIE COERENTI MASSIMALI
  - Fissato un linguaggio (proposizionale o predicativo) L, una L-teoria T si dice coerente massimale se è coerente e non è propriamente inclusa in alcun'altra L-teoria coerente
  - T coerente massimale equivale a T completa

TEOREMA DI COMPLETEZZA NEL CASO PROPOSIZIONALE

- RISULTATI PRELIMINARI
  - (*) L'unione di una catena di teorie coerenti è coerente
  - LEMMA DI LINDEMBAUM: Ogni L-teoria coerente T è contenuta in una L-teoria coerente massimale
    - Se L è numerabile: fissiamo un'enumerazione delle L-formule e costruiamo n teorie coerenti. L'unione è coerente massimale
    - Se L è più che numerabile: applichiamo il lemma di Zorn all'insieme di tutte le L-teorie coerenti contenenti T ordinate per inclusione (posso applicare Zorn per (*))
  - **LEMMA DI ZORN: Se X è un insieme non vuoto su cui è definita una relazione d' ordine parziale tale che ogni sua catena possiede un maggiorante in X, allora X contiene almeno un elemento massimale**
  - PROPRIETÀ DELLE TEORIE COERENTI
    - se ¬¬Φ ∈ T, allora T, Φ è coerente
    - se Φ ∧ ψ ∈ T, allora T, Φ, ψ è coerente
    - se ¬(Φ ∧ ψ) ∈ T, allora T, ¬Φ è coerente, o T, ¬ψ è coerente
    - se Φ ∨ ψ ∈ T, allora T, Φ è coerente, o T, ψ è coerente
    - se ¬(Φ ∨ ψ) ∈ T, allora T, ¬Φ, ¬ψ è coerente
    - se Φ → ψ ∈ T, allora T, ¬Φ è coerente, o T, ψ è coerente
    - se ¬(Φ → ψ) ∈ T, allora T, Φ, ¬ψ è coerente
    - Si dimostrano tutte per assurdo
- COMPLETEZZA PROPOSIZIONALE
  - Sia L un linguaggio proposizionale e sia T una teoria proposizionale coerente nel linguaggio L. Allora T ha un modello proposizionale
    - Dimostro che ogni teoria coerente massimale ha un modello tramite l'induzione sulla complessità delle formule e le proprietà delle teorie coerenti.
    - Posso estendere una teoria coerente T a una coerente massimale T': il modello di T' va bene anche per T
  - Corollario: Sia T una teoria proposizionale, e sia Φ una formula proposizionale. Se T |= Φ allora T |- Φ
    - Si dimostra per assurdo, è ovvio se T è finito

TEOREMA DI COMPLETEZZA NEL CASO PREDICATIVO

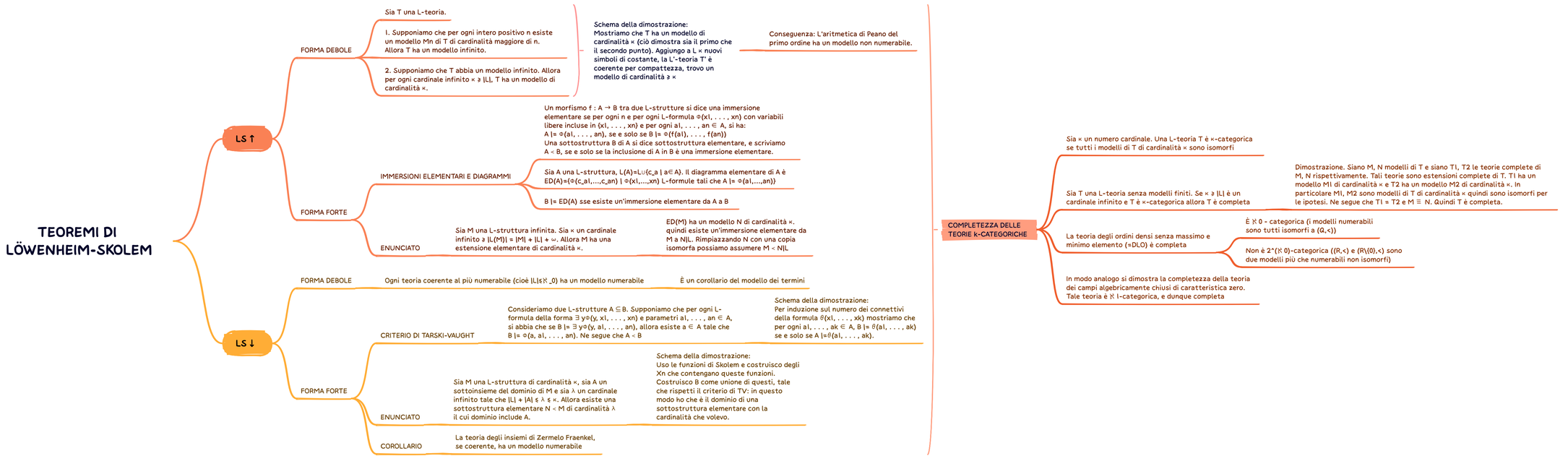
- RISULTATI PRELIMINARI
  - HENKIN
    - LEMMA DELLE COSTANTI: Sia T un insieme di L-formule e sia ϕ una L-formula. Sia c un simbolo di costante non in L. Se T |- ϕ(c/x) nel linguaggio L∪{c}, allora esiste una variabile y tale che T |- ϕ(y/x) nel linguaggio L. Inoltre T |- ∀xϕ nel linguaggio L.
      - Lo dimostro per compattezza e per la regola di generalizzazione
    - LEMMA DI HENKIN: Sia T una L-teoria, c nuova costante che non sta in L e sia ϕ una L-formula, VL(ϕ) contenute in {x}. Se T è coerente allora T∪{∃xΦ→Φ[c/x]} è coerente
      - A livello semantico semantico è banale
      - A livello sintattico si dimostra tramite il lemma delle costanti
    - Sia T una L-teoria. Diciamo che T è una teoria di Henkin se per ogni L-formula chiusa della forma ∃xΦ(x) esiste almeno un simbolo di costante c in L tale che la formula T |- ∃xΦ(x) → Φ(c) e T è coerente
      - Esempio:
        - Sia T la teoria nel linguaggio L = {0, 1, +, ·} che ha come assiomi tutti gli L-enunciati veri nel campo dei numeri reali R. Allora T non è una teoria di Henkin
        - Infatti T dimostra ∃x(x·x=1 + 1) ma non esiste alcuna costante c del linguaggio tale che T |- c·c= 2
        - La radice quadrata di due esiste nel dominio della struttura R, ma non corrisponde ad alcun simbolo del linguaggio L
    - Sia T una L-teoria coerente. Allora esiste un linguaggio L' ⊇ L e una L'-teoria T' ⊇ T tale che T' è coerente e di Henkin.
      - Per ogni L-formula ∃xΦ(x) ci inventiamo una nuova costante. T*=T∪{∃xΦ→Φ[c/x] | Φ L-formula} è coerente per compattezza + lemma di Henkin. Siano T0= T, T1=T*,...,Tn+1=Tn*: l'unione di queste teorie è coerente di Henkin.
      - Posso estendere T' a una teoria coerente massimale T'' nel linguaggio L' e questa rimarrà di Henkin
    - Una L-teoria è di Hintikka se contiene solo termini chiusi e
      1. se Φ ∈ T, allora ¬Φ∉T
      2. se ¬¬Φ ∈ T, allora Φ ∈ T
      3. se Φ ∧ ψ ∈ T, allora Φ ∈ T e ψ ∈ T
      4. se ¬(Φ ∧ ψ) ∈ T, allora ¬Φ ∈ T o ¬ψ ∈ T
      5. se Φ ∨ ψ ∈ T, allora Φ ∈ T o ψ ∈ T
      6. se ¬(Φ ∨ ψ) ∈ T, allora ¬Φ ∈ T e ¬ψ ∈ T
      7. se Φ → ψ ∈ T, allora ¬Φ ∈ T o ψ ∈ T
      8. se ¬(Φ → ψ) ∈ T, allora Φ ∈ T e ¬ψ ∈ T
      9. se ∀xΦ(x) ∈ T, allora per ogni L-termine chiuso t, Φ(t) ∈ T
      10. se ¬∀xΦ(x) ∈ T, allora esiste un L-termine chiuso t tale che ¬Φ(t) ∈ T
      11. se ∃xΦ(x) ∈ T, allora esiste un L-termine chiuso t, tale che Φ(t) ∈ T
      12. se ¬∃xΦ(x) ∈ T, allora per ogni L-termine chiuso t, ¬Φ(t) ∈ T
      13. (riflessività) per ogni L-termine chiuso t, t = t ∈ T
      14. (sostituibilità) per ogni L-formula Φ(x) e termini chiusi t e t', se t=t'∈ T, allora Φ(t) ∈ T se e solo se Φ(t')∈ T
    - Ogni teoria 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 del linguaggio L di T, ovvero M è una struttura ricca
      - Costruiamo il modello dei termini
        - dom(M)=l'insieme degli L-termini chiusi quozientato rispetto alla relazione di equivalenza ~ definita da t~t' sse t=t'∈ T
        - Interpreto i simboli di costante, funzione e relazione nel modo ovvio
        - Per induzione M è una L-struttura ricca
      - Cardinalità del modello dei termini
        - L'insieme delle L-formule ha cardinalità |L| + ω. L'insieme degli L-termini ha cardinalità ≤ |L| + ℵ 0.
        - La cardinalità del modello dei termini è ≤ max(|L|, ℵ 0)
    - T coerente allora T ha un modello
      - Se T ` e coerente esiste una teoria di Hintikka T' ⊇ T in un linguaggio L' ⊇ L. Allora T' ha un modello M. Quindi anche T ha un modello (la restrizione di M al linguaggio L).
  - Sia T una L-teoria coerente massimale di Henkin. Allora T è di Hintikka.
    - Si dimostra clausola per clausola
- COMPLETEZZA PREDICATIVA
  - Sia T una L-teoria. Se T |= Φ, allora T |- Φ.
    - Se T non dimostra Φ allora T, ¬Φ è coerente, e quindi ha un modello. Tale modello testimonia che T |≠ Φ.

TEOREMA DI COMPATTEZZA

- Se T |= Φ, esiste un sottoinsieme finito T' ⊆ T tale che T' |= Φ. In particolare, prendendo come Φ la formula sempre falsa ⊥ una teoria ha un modello se e solo se tutti i suoi sottoinsiemi finiti hanno un modello
  - Immediato dalla compattezza sintattica e dalla completezza

APPLICAZIONI DEL TEOREMA DI COMPATTEZZA E COMPLETEZZA

- Sia ϕ una formula vera in tutti i campi di caratteristica zero. Allora esiste un primo p tale che ϕ è vera in tutti i campi di caratteristica ≥p
- Esiste un modello di Peano non isomorfo ad N (non standard)
- Sia G un grafo infinito tale che ogni sottografo finito è k-colorabile. Allora G è k-colorabile
- Tessere di Hao Wang (basta il caso proposizionale)
- Sia ZF la teoria degli insiemi di Zermelo-Fraenkel nel linguaggio L = {∈}. Se ZF è coerente, esiste un modello (M, ∈) di ZF in cui vi è una catena discendente infinita an+1 ∈ an di elementi ai ∈ M tali che M |= ai ∈ ω



MACCHINE A REGISTRI

è un modello idealizzato di calcolatore proposto da Shepherdson e Sturgis nel 1963

COM'È FATTA

- REGISTRI E CONFIGURAZIONE DI MEMORIA
  - Ha infiniti registri di memoria R0,R1,R2,...
  - Ri contiene un numero naturale ai
  - Solo un numero finito di ai sono diversi da 0
  - (a0,a1,a2,...) viene detta configurazione di memoria
- CONTATORE DI PROGRAMMA
  - Contiene un numero che indica la prossima istruzione da seguire
  - All'inizio è 1
- STATO
  - È dato dal contenuto dei registri di memoria e dal contenuto del contatore di programma

ISTRUZIONI E PROGRAMMI

- PROGRAMMA
  - Un programma P è una lista finita (I1,...,In) di istruzioni
- ISTRUZIONI
  - ASSEGNAZIONE
    - Rn:=0 — memorizza il numero 0 nel registro di Rn
    - Rn:=(Rn)+1 — incrementa di 1 il registro di Rn
    - Rn:=Rm — memorizza nel registro Rn il contenuto di Rm
    - non modifica la configurazione di memoria
      - il contatore viene incrementato di 1 a ogni istruzione
  - SALTO CONDIZIONATO — if Rn=Rm go to q
    - se i contenuti dei registri Rn e Rm sono uguali il contatore di programma viene posto uguale a q
    - altrimenti viene incrementato di 1

SEMANTICA DEI PROGRAMMI

- FUNZIONI PARZIALI E TOTALI: Data una relazione f ⊆ AxB definiamo:
  - dom(f) = {a ∈ A | ∃ b ∈ B (a, b) ∈ f}
  - Im(f) = {b ∈ B | ∃ a ∈ A (a, b) ∈ f}
  - Se per ogni a ∈ dom(f) esiste un unico b ∈ B tale che (a, b) ∈ f, allora diciamo che f è una funzione PARZIALE da A a B, e scriviamo f : A → B
  - Se dom(f) = A diciamo che f è una funzione TOTALE da A a B.
  - a ∈ A
    - f(a) ↓ se a ∈ dom(f)
    - f(a) ↑ altrimenti
- COMPOSIZIONE — f : A → B e g : B → C, g ∘ f =h: A → C funzione parziale : h(x) ↓ se e solo se x ∈ dom(f) e f(x) ∈ dom(g)
- CALCOLO DI UN PROGRAMMA
  - È una successione finita o infinita di stati
  - Il calcolo ha termine quando si raggiunge uno stato di arresto: il contatore del programma contiene un numero che n corrisponde ad alcuna istruzione del programma

FUNZIONI CALCOLABILI

- Voglio costruire un programma che calcoli una funzione definita sui naturali. Definisco tre registri:
  - Registri di input: contengono, all'inizio del calcolo, i dati di ingresso (a1, . . . , am) ∈ N^m
  - Registri di output: conterranno alla fine del calcolo, se questo ha termine, il risultato finale b∈ N
  - Registri di lavoro: consistono di tutti gli altri registri che vengono usati dal programma e contengono informazioni utili al suo funzionamento
- Una funzione parziale è calcolabile se e solo se coincide con la funzione calcolata da un programma P — es: la somma e il prodotto sono calcolabili

FUNZIONI RICORSIVE PARZIALI

ASSOCIATA AD UN ROGRAMMA

La funzione parziale ϕ associata al programma P usando come registri di input R1,...,Rn e registro di output R0

- ϕ(a1, . . . , an) = b se eseguendo il programma P si determina un calcolo che si arresta dopo un numero finito di passi con b nel registro R0
- ϕ(a1, . . . , an) ↑ (indefinita) se partendo dallo stato iniziale si determina un calcolo che non si arresta mai

f: N^n → N è ricorsiva parziale (o calcolabile parziale) se e solo se esiste un programma P tale che f = ϕ associata a P

- Se inoltre dom(f) = N^n diciamo che f è ricorsiva totale (o calcolabile totale)
- Funzioni ricorsive totali = Funzioni ricorsive parziali ∩ Funzioni totali

La composizione di funzioni ricorsive parziali è ricorsiva parziale

PRIMITIVE RICORSIVE

Date due funzioni parziali h:N^(n+2)→ N, g:N^n→ N, definiamo una funzione parziale f:N^(n+1)→ N tale che

- f(x1,...,xn,0)=g(x1,...,xn) (x1,...,xn,0)∈ dom(f) sse (x1,...,xn)∈ dom(g)
- f(x1,...,xn,y+1)=h(x1,...,xn,y,f(x1,...,xn,y)) (x1,...,xn,y+1)∈ dom(f) sse (x1,...,xn,y)∈ dom(f) e (x1,...,xn,y, f(x1,...,xn,y))∈ dom(h)
- Diciamo che f è primitiva ricorsiva (ottenuta per ricorsione primitiva da g e h). Se h e g sono totali anche f lo è. Se h e g sono calcolabili anche f lo è.

Una funzione è primitiva ricorsiva se si ottiene, a partire dalle funzioni iniziali, per composizione e ricorsione primitiva applicate a funzioni

FUNZIONI INIZIALI

- La funzione costante zero c0 : N → N
- La funzione successore s: N → N
- La funzione proiezione P_i:N^n→N che manda (x1,...,xn) in xi

Le funzioni primitive ricorsive sono un sottoinsieme proprio dell'insieme delle funzioni ricorsive totali

MINIMALIZZAZIONE

Sia h: N^(n+1) → N una funzione totale e sia f(x1,...,xn) = μz(h(x1,...,xn, z) = 0) :

DEF. 1

- f(x1,...,xn)=min{z | h(x1,...,xn,z) = 0} se ∃ z(h(x,z) = 0)
- f(x1,...,xn) = ↑ altrimenti

DEF. 2 (più forte)

- min{z|h(x1,...,xn,z)=0∧ ∀ u<zh(x1,...,xn,u)↓ } se tale z esiste
- ↑ altrimenti

Se h è calcolabile (totale) allora f è calcolabile parziale

FUNZIONI μ-RICORSIVE DI KLEENE

Una funzione parziale f : N^n → N è μ-ricorsiva se si ottiene, a partire dalle funzioni iniziali, per composizione, ricursione primitiva e minimalizzazione, applicate a funzioni precedentemente ottenute

La classe delle funzioni μ-ricorsive è inclusa nella classe delle funzioni calcolabili da un programma per macchine a registri

Oltre alla composizione, alla ricursione primitiva, e alla minimalizzazione, ci sono molti altri operatori che applicati a funzioni ricorsive parziali generano funzioni ricorsive parziali

- Sommatorie e produttorie limitate
- Minimalizzazione limitata
- Ricorsione sul decorso dei valori

TESI DI CHURCH

DUE NOZIONI DI FUNZIONE CALCOLABILE

- INFORMALE: una funzione è calcolabile se esiste un'algoritmo per calcolarla (lasciando indefinito il concetto intuitivo di algoritmo)
- FORMALE: una funzione è calcolabile se esiste un programma per macchine a registri per calcolarla

→ Church dice che coincidono

TUTTE LE FUNZIONI INTUITIVAMENTE CALCOLABILI SONO CALCOLABILI CON MACCHINA A REGISTRI

- Church faceva riferimento alle macchine di Turing, ma si può dimostrare la loro equivalenza con le macchine a registri
- La tesi di Church non è dimostrabile formalmente in quanto collega una nozione formale con una nozione informale
- La fiducia nella verità della tesi si basa sull'esperienza e sul fatto che diverse formalizzazioni della nozione di funzione calcolabile si sono dimostrate equivalenti

APPLICAZIONE

- Sia f(n) l'n-sima cifra dello sviluppo decimale di π. La funzione f è calcolabile con una macchina a registri
- Lo so fare con le serie, quindi per la tesi di Church lo saprò fare anche con una macchina a registri

PREDICATI DECIDIBILI

PREDICATI VISTI COME INSIEMI

- $M \subseteq N^m$: $M(x1,...,xm)$ se e solo se $(x1,...,xm) \in M$
- Se vale $M(x1,...,xm)$ diciamo che $(x1,...,xm)$ verifica il predicato (o relazione) M.

DEFINIZIONE

- Un insieme $A \subseteq N^k$ è decidibile se la sua funzione caratteristica è calcolabile
- Funzione caratteristica: $\chi A: N^k \rightarrow \{0,1\}$
  - vale 1 su A
  - 0 altrimenti

ESEMPI

- Se f è una funzione ricorsiva totale, allora il suo grafico è decidibile
- Sia g una funzione definita per casi: g=f1 se vale M, g=f2 altrimenti. Se M è un predicato primitivo ricorsivo e f1, f2 sono funzioni calcolabili totali allora g è calcolabile totale

ALGEBRA DI BOOLE

- INSIEMI
  - L'unione o l'intersezione di due insiemi decidibili è decidibile
  - Il complemento di un insieme decidibile è decidibile
- PREDICATI
  - La congiunzione o disgiunzione di predicati decidibili è decidibile
  - La negazione di un predicato decidibile è decidibile

QUANTIFICATORI LIMITATI

- $M1(x1,...,xn,y) \equiv \forall z<y R(x1,...,xn,z)$
- $M2(x1,...,xn,y) \equiv \exists z<y R(x1,...,xn,z)$
- Se R è un predicato decidibile, anche M1 ed M2 sono predicati decidibili
  - $\chi M1$ equivale alla produttoria limitata di χR
  - $\chi M2$ equivale a not produttoria di not χR

PREDICATI SEMIDECIDIBILI

DEFINIZIONE E PROPRIETÀ

- $M \subseteq N^m$ è semidecidibile se e solo se esiste un predicato decidibile $R \subseteq N^{(m+1)}$ tale che $M(x1,\dots,xm) \equiv \exists y R(x1,\dots,xm, y)$.
- Se R è decidibile allora è anche semidecidibile: $R(x1,\dots,xm) \equiv \exists y R(y=y \wedge R(x1,\dots,xm))$
- Se $M \subseteq N^m$ è un insieme semidecidibile, allora M è il dominio di una funzione ricorsiva parziale $f : N^m \to N$. Sia $M(X) \equiv \exists y R(X,y)$, definiamo $f(X) = \mu y R(X, y)$.
- I predicati semidecidibili sono chiusi per $\wedge, \vee, \exists x, \forall x<y$

$X=(x1,\dots,xm)$

TEOREMA DI POST

- Sia $A \subseteq N^m$. Se A e $\sim A = N^m \setminus A$ sono semidecidibili allora A è decidibile
- Si dimostra costruendo una funzione totale ricorsiva $f(X) = \mu y(R(X,y) \vee S(X,y))$ dove R e S sono predicati decidibili che definiscono A e $\sim A$. Ottengo $A(X) \equiv R(X,f(X))$
- Vale anche il viceversa

RICORSIVAMENTE ENUMERABILE

- $A \subseteq N$ è r.e. se e solo se è vuoto oppure è della forma $A = \{f(n) \mid n \in N\}$ con f calcolabile totale
- S semidecidibile $\iff$ S r.e.
  - $\implies S=\{x \mid \exists x R(x,y)\}$:
    1. $S=\emptyset$ allora S è r.e. per definizione
    2. prendo un elemento di S e costruisco una funzione f opportuna tale che $S=Im(f)$
  - $\impliedby S=Im(f)$ allora $S=\{y \mid \exists x f(x)\}$ che è semidecidibile
- Sia $A \subseteq N$ un insieme infinito. A è semidecidibile se e solo se esiste una funzione calcolabile totale crescente $f : N \to N$ tale che $A = Im(f)$
- Ogni insieme ricorsivamente enumerabile infinito $A \subseteq N$ ha un sottoinsieme infinito ricorsivo

CODIFICHE

DEFINIZIONE

- Una codifica di un insieme numerabile D è una funzione biunivoca da D a N
- Più in generale una codifica è una funzione iniettiva da D a N la cui immagine sia un sottoinsieme ricorsivo di N
- Sia f : D → D una funzione parziale. f è calcolabile rispetto alla codifica biunivoca α: D → N se α ∘ f ∘ α^(−1) : N → N è una funzione ricorsiva parziale.
- ESEMPIO: Posso codificare gli interi in questo mondo:
  - se n≥0 lo mando in 2n
  - se n<0 lo mando in -2n-1

CODIFICA DELLE STRINGHE

Sia Σ = {a1,...,ak} un alfabeto finito. Sia Σ* l'insieme delle stringhe (successioni finite) su Σ. Indichiamo con λ ∈ Σ* la stringa vuota. Diamo una codifica α: Σ* → N come segue

- α(λ) = 0
- α(a_r0 ...a_rm)=r0 +r1.k+...+rm.k^m

Possiamo parlare di funzioni calcolabili su stringhe riferendoci a questa codifica

CODIFICA DELLE COPPIE

DEF.1

Coppia: N^2 → N
Coppia(x,y) = 2x(1 + 2y) − 1

- è una corrispondenza biunivoca tra N^2 ed N
- Coppia e le due funzioni inverse sono primitive ricorsive

Tripla : N^3 → N
Tripla(x, y, z) = Coppia(x, Coppia(y, z))

- è una corrispondenza biunivoca tra N^3 ed N
- Tripla e le due funzioni inverse sono primitive ricorsive

DEF.2

<>:N^2→ N
<x,y>=[(x+y)(x+y+1)]/2 +x — è una corrispondenza biunivoca tra N^2 ed N

<>:N^3→ N
<x,y,z>=<x,<y,z>> — è una corrispondenza biunivoca tra N^3 ed N

CODIFICA DELLE SUCCESSIONI A SUPPORTO FINITO

NUMERI PRIMI

Sia p(x) = lo x + 1-esimo numero primo

- p(0)=2
- p(1)=3
- p(2)=5
- ...

Il predicato "x è primo" è primitivo ricorsivo. La funzione x → p(x) è ricorsiva primitiva. — può essere espresso a partire da predicati primitivi ricorsivi usando i connettivi booleani e i quantificatori limitati

BIGEZIONE

Sia (ai | i ∈ N) una successione di numeri naturali. Diciamo che la successione ha supporto finito l'insieme degli i tali che ai ≠ 0 è un insieme finito

Mettiamo in bigezione le successioni a supporto finito con N in questo modo:

- alla successione (ai | i ∈ N) corrisponde il prodotto p(i)^ai tale che i ∈ N
- la produttoria è ben definita perché tutti i fattori eccetto un numero finito sono =1
- è chiaro sia una bigezione: riesco a trovare l'inversa fattorizzando

CALCOLABILITÀ

Questa bigezione è calcolabile?
Non ha senso chiederselo: va da N^∞ in N

La funzione che estrae l'i-esimo elemento da una successione è μ-ricorsiva?
Sì, è primitiva ricorsiva: riesco a definirla con la minimalizzazione limitata

CODIFICA DEGLI INSIEMI FINITI

Creiamo la bigezione:

- All'insieme vuoto associo lo 0
- All'insieme {a1,...,an} associo 2^(a1)+...+2^{an}

CODIFICA DELLE SUCCESSIONI FINITE

BIGEZIONE

Ad una successione finita (a1, . . . , an) di numeri naturali, associamo un numero naturale <a1,...,an> ∈ N

- <>=0 (successione vuota)
- <a1>=2^a1
- <a1,...,an>=2^a1(1+2<a2,...,an>) cioè =2^(a1) + 2^(a1+a2+1) + 2^(a1+a2+a3+2)+...+2^(a1+...+an+n-1)

Perché è biunivoca: <a1,a2,a3,...,an> è il numero espresso in binario che inizia con a0 cifre uguali a zero, seguite dalla cifra 1, seguite da a1 cifre uguali a zero, seguita da 1, e così via — es: (1,2,3) è codificata da 2+2^4+2^8 che in binario corrisponde a 100010010

FUNZIONI ASSOCIATE

Esistono funzioni ricorsive primitive che prendono in input le codifiche delle successioni finite

- LUNGHEZZA: lh(<a1,...,an>)=n
- CONCATENAZIONE: Cat(<a1,...,an>,<b1,...,bm>)=<a1,...,an,b1,...,bm>
- PROIEZIONE: π(i,<a1,...,an>) = ai se 1 ⩽ i ⩽ n

CODIFICA DEI PROGRAMMI E PROGRAMMI UNIVERSALI

CODIFICA DELLE ISTRUZIONI

- Rn:=0 4n
- Rn:=R(n+1) 4n+1
- Rm:=Rn 4Coppia(m,n)+2
- if Rm =Rn go to q 4Tripla(m,n,q)+3

CODIFICA DEI PROGRAMMI

- Un programma P è una successione finita di istruzioni P=(I1,...,In)
- Sia ai la codifica di ogni istruzione Ii, allora il programma P è codificato da <a1,...,an>=2^(a1)+...+2^(a1+...+an+n-1)
- La codifica dei programmi è una corrispondenza biunivoca tra programmi e numeri naturali

Chiamo (Φ_e)^n : N^n → N la funzione parziale calcolata dal programma P codificato da e∈ N

LA MIA PRIMA FUNZIONE NON CALCOLABILE

- f(n)=
  - Φ_n(n) + 1 se Φn(n) ↓
  - 0 altrimenti

Se fosse calcolabile esiste e ∈ N tale che f=Φ_e
f è totale per definizione, quindi Φ_e(e) è definita
f(e)=Φ_e(e)+1, ma questo contraddice f=Φ_e, assurdo

- la funzione n → Φ_n(n) è una funzione calcolabile parziale
- la funzione f(n) non è calcolabile perché il predicato Φn(n) ↓ che discrimina i due casi non è decidibile

FORMA NORMALE DI KLEENE

- Sia n ∈ N. Esiste una funzione primitiva ricorsiva U e un predicato primitivo ricorsivo T^n tale che
  - (Φ_e)^n (x1,...,xn) ↓ sse ∃ zT^n(e,x1,...,xn,z)
  - (Φ_e)^n (x1,...,xn) = U(μzT^n(e,x1,...,xn,z))
- Il predicato T^n(e,x1,...,xn,z) è detto predicato di Turing, ed esprime il fatto che z codifica l'output e il tempo di calcolo del programma P_e su input x1, . . . , xn (quindi z esiste se la macchina si arresta)
- La funzione U estrae l'output da tale codifica

CONSEGUENZE

- A è semidecidibile se e solo se è il dominio di una funzione ricorsiva parziale
- Sia Wx = dom(Φ_x). Allora la successione W0, W1, W2, . . . enumera tutti e soli i sottoinsiemi semidecidibili di N
- Una funzione parziale è calcolabile con una macchina a registri se e solo se è μ-ricorsiva
  - ogni funzione μ- ricorsiva può essere definita usando una sola volta l'operatore di minimalizzazione

FUNZIONE UNIVERSALE

- Esiste una funzione U: N^2 → N calcolabile parziale tale che ∀ e,n U(e,n)=Φ_e(n)

INSIEMI INDECIDIBILI

PROBLEMA DELLA FERMATA

- Definiamo K0 e K
  - K0={x | Φ_x(x) ↓ }
  - K={(x,y)|Φ_x(y) ↓ }
- Prima via
  - K0 non è decidibile
    - Se lo fosse, lo sarebbe f con
      f(n)=Φ_n(n) + 1 se n∈K0
      0 altrimenti
      e abbiamo visto che f non è calcolabile
  - K non è decidibile
    - Sia f:N→NxN che manda n in (n,n): n∈K0 sse f(n)∈K, cioè se K è decidibile anche K0 lo è
- Seconda via
  - K0 e K sono semidecidibili
    - (x,y)∈ K sse ∃ t(Φx(y) ↓ ≤t): il predicato tra parantesi è decidibile, quindi K è semidecibibile
    - x ∈ K0 se e solo se (x, x) ∈ K , quindi anche K0 è semidecidibile
  - K0 e K non sono decidibili
    - K e K0 sono domini di una funzione calcolabile poiché sono semidecidibili
    - x ∈ K0 ⇐⇒ x ∈ Wx=dom(Φ_x)
    - Se K0 fosse decidibile, anche il suo complemento lo sarebbe, quindi x ∉ Wx sarebbe decidibile
    - x ∉ Wx ⇐⇒ x ∈ Wx, assurdo
    - K non è decidibile, altrimenti anche K0 lo sarebbe

PROBLEMA DELLA TOTALITÀ

- TOT = {x | Φ_x è totale }
- TOT non è decidibile
  - Sia f(n)=
    - Φ_n(n) + 1 se Φ_n è totale
    - 0 altrimenti
  - f è totale ma non è calcolabile quindi TOT non è decidibile
- TOT non è semidecidibile
  - Se lo fosse avrei TOT={h(n) | n∈N}.
    Sia f(x) = Φ_h(x)(x) + 1, è totale perché ∈ TOT e calcolabile per la funzione universale.
    Quindi f = Φ_e con e ∈ TOT = Im(h), e = h(n).
    Dunque abbiamo f(n)=f(n)+1, assurdo.
- x ∈ TOT se e solo se ∀ υ∃ t(Φx(υ) ↓ ≤t), con il predicato in parentesi decidibile

RIDUZIONI

RIDUZIONE MANY-ONE

A≤mB con A,B ⊆ N (anche N^k) se esiste una funzione f calcolabile totale tale che per ogni n, n∈A sse f(n)∈B

"B è più complicato di A"

Se B è decidibile allora A è decidibile

χA(x) = χB(f(x))

RIDUZIONE DI TURING

A≤tB con A,B ⊆ N se χA è calcolabile con oracolo B, una macchina a registri con un' operazione in più: x:=χB

A≤mB implica A≤tB

TEOREMA S.M.N.

Dati m,n∈ N, esiste una funzione calcolabile totale s:N^(m+1)→N tale che per ogni X=(x1,...,xn),Y=(y1,...,ym),e (Φ_e)^(m+n)(X,Y)=(Φ_s(e,X))^(m)(Y)

Parte dell'input lo incorporo nel programma

Ad esempio: Se ho un programma P_e con codice e per calcolare + allora posso ottenere un programma P_c con codice c per calcolare y→3+y

SECONDO TEOREMA DEL PUNTO FISSO

Data h: N → N ricorsiva totale esiste e ∈ N tale che Φ_e = Φ_(h(e)) (Similmente con Φ^n al posto di Φ)

Si dimostra tramite il teorema s.m.n.

Pongo e=s(a,a), Φ_e(x) = Φ_s(a,a)(x) = ((Φ_a)^2)(a,x)=*
Scelgo a in modo che * sia uguale a Φ_j(x) con j=h(s(y,y))
e lo posso fare perché (y,x) → Φ_j(x) è calcolabile parziale

FUNZIONE DI ACKERMANN

A=Ack(m,n)=

- n + 1 se m = 0
- A(m−1,1) se m>0 e n=0
- A(m−1,A(m,n−1)) se m>0 e n>0

A è calcolabile

Modifichiamo la definizione in questo modo:

A(m,n)=

- n + 1 se m = 0
- B(m−1,1) se m>0 e n=0
- B(m−1,B(m,n−1)) se m>0 e n>0

B è una qualsiasi funzione calcolabile.
Conoscendo il codice b di B si può facilmente calcolare il codice h(b) di A tramite una funzione calcolabile totale h.
Per il teorema del punto fisso esiste b tale che (Φ_b)^2 = (Φ_h(b))^2

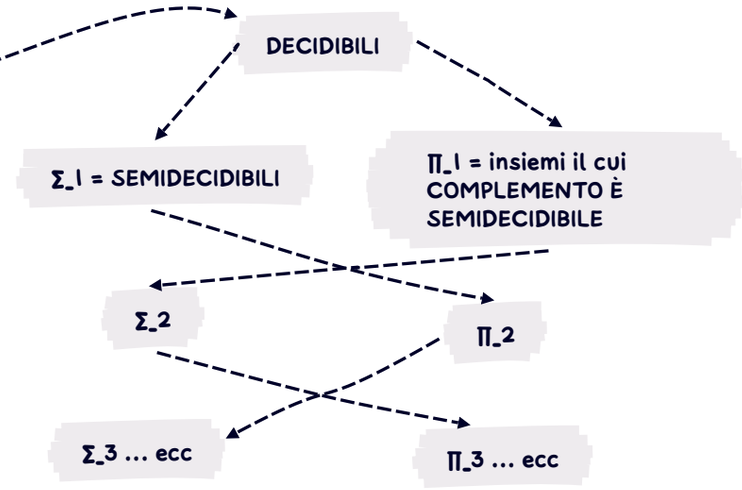
Per tale b si ha A = B = la funzione di Ackermann

GERARCHIA ARITMETICA

DEFINIZIONE

È una gerarchia di insiemi fatta così:

- Σ_{n+1} si ottiene applicando $\exists$ davanti a Π_n
- Π_{n+1} si ottiene applicando $\forall$ davanti a Σ_n



PROPRIETÀ

Tutti i Σ_n, Π_n sono stabili per $\wedge, \vee, \forall x<y, \exists x<y$

- Σ_n è chiuso per $\exists$
- Π_n è chiuso per $\forall$

INSIEMI DEFINIBILI IN (N,+,.)

I predicati definibili in (N, +, ·) coincidono con quelli definibili in (N, +, ·, ≤)

La relazione ≤: infatti x≤y sse $\exists$ z(x + z = y)

Il predicato "x è primo": "$\forall$ u, v(x = u · v → u = 1 $\vee$ v = 1)"

Un insieme è definibile se è della forma {(a1, . . . , an) | P (a1 , . . . , an)}, dove P è un predicato definibile

Una funzione è definibile se il suo grafico è definibile

x^y=z è definibile in (N,+,.) si dimostra definendo una relazione $\in^*$

INSIEMI R.E:

Ogni funzione ricorsiva parziale è definibile in (N, +, ·)

Definiamo le formule Δ0 come formule aritmetiche in cui tutti i quantificatori appaiono limitati

Nel modello standard N dell'aritmetica, ogni formula Σ_1 equivale ad una formula della forma Δ0 preceduta da un quantificatore esistenziale

Gli insiemi aritmetici sono esattamente quelli definibili nel modello standard dell'aritmetica

ALCUNE FORMULE DIMOSTRABILI IN Q

NUMERALE

Dato $n \in N$, il termine s(s(...s(0))) n volte s, viene detto il numerale di n e lo indichiamo con 'n' o s^n(0)

SOMMA

$\forall a,b,c \in N$, se a+b = c, allora $Q \vdash$ 'a'+'b'='c'

Cioè l'enunciato 'a'+'b'='c' è vero in tutti i modelli di Q

Si dimostra per induzione nella metateoria

Non riesco a dimostrare però che il + è commutativo

PRODOTTO

$\forall a,b,c \in N$, se a·b=c, allora $Q \vdash$ 'a'·'b'='c'

Si dimostra per induzione nella metateoria usando il lemma sulla somma

TERMINI

Per ogni termine chiuso t di L esiste $n \in N$ tale che $Q \vdash t = 'n'$

Per induzione sulla lunghezza di t usando il lemma della somma e del prodotto

Se t1 e t2 sono termini chiusi di L(Q) allora $Q \vdash t1 = t2$ oppure $Q \vdash t1 \neq t2$

Per il lemma precedente e i seguenti lemmi su uguaglianza e disuguaglianza

UGUAGLIANZA E DISUGUAGLIANZA

$\forall a,b \in N$, se a=b, allora $Q \vdash$ 'a'='b'

Segue dal fatto che Q, così come ogni altra teoria, dimostra $\forall x(x = x)$

$\forall a,b \in N$, se a=b, allora $Q \vdash$ 'a'≠'b'

Assumo a<b e procedo per induzione su a

NUMERI NON STANDARD

PRENDIAMO UN MODELLO M DI Q

- Consideriamo M′ ⊆ M di quegli elementi di M che sono l'interpretazione di qualche numerale n, ovvero M′ = {x ∈ M | ∃ n ∈ N x = 'n'M}, dove 'n'M = sM(sM(...sM(0M))) (con n occorrenze di sM)
- Gli elementi di M′ sono chiamati numeri standard di M, mentre gli elementi di M − M ′ sono chiamati numeri non-standard di M
- I numeri standard costituiscono il più piccolo sottoinsieme di M contenente lo 0 di M e chiuso per la funzione successore s di M
  - Se M è un modello di PA2 tutti i numeri sono standard grazie all'induzione
  - Lo stesso ragionamento non vale in PA1
- Il sottoinsieme M′ ⊆ M dei numeri standard costituisce una sottostruttura di M isomorfa ad N con le usuali operazioni di addizione e moltiplicazione
  - L'isomorfismo è unico in quanto la mappa manda 0→0M e preserva la funzione successore
- N è immergibile in ogni modello M di Q, e che M è isomorfo ad N se e solo se M non ha numeri non-standard
- Nel modello Z[x]+ di Q i numeri non-standard sono esattamente i polinomi non-costanti

LA RELAZIONE ⩽

- ∀ n∈ N, Q⊢∀ x(x⩽'n'↔x='0'∨ x='1'∨ ...∨ x='n') — Si mostra per induzione su n
- Un numero ⩽ di un numero standard è standard
- Sia n ∈ N. Sono equivalenti:
  1. ∀ a⩽nQ⊢Φ('a')
  2. Q⊢∀ x⩽'n'Φ(x)
- ∀ a,b∈ N,Q⊢'a'⩽'b' se a⩽b oppure Q⊢¬('a'⩽'b') se a>b
- ∀ b∈ N, Q⊢∀ x(x⩽'b'∨ 'b'<x)
  - c'è una relazione di ordine totale sui numeri standard
  - In un modello non-standard M di Q la relazione ⩽ non è un buon ordine, nel senso che contiene delle successioni discendenti infinite
  - In alcuni modelli di Q la relazione ⩽ non è neppure un ordine totale MA
- Sia M |= Q e sia A ⊆ M un sottoinsieme di M contenente un numero standard n. Allora A ha un minimo elemento m, ovvero esiste m ∈ A tale che ∀ a∈A, M |=m⩽a

ENUNCIATI DECIDIBILI IN Q

- Un enunciato si dice indipendente da Q se Q ⊬Φ e Q ⊬¬Φ — es: ∀ x∃ y(2y = x ∨ 2y = x + 1)
- Un enunciato si dice decidibile in Q se Q ⊢ Φ oppure Q ⊢ ¬Φ
- Dire che Φ è indipendente da Q significa che Φ è vero in certi modelli di Q e falso in altri
- Dire che Φ è decidibile in Q significa che Φ ha lo stesso valore di verità in tutti i modelli di Q
- Una combinazione booleana di enunciati decidibili in Q è decidibile in Q.
- Le formule Δ0 chiuse sono decidibili in Q
- Se Φ è un enunciato Σ_1 e N |= Φ, allora Q ⊢ Φ

Riassumendo

- Gli enunciati Δ0 veri in N sono dimostrabili in Q
- Gli enunciati Δ0 falsi in N sono refutabili in Q
- Gli enunciati Σ_1 veri in N sono dimostrabili in Q
- Gli enunciati Σ_1 falsi in N non sono dimostrabili in Q

RAPPRESENTABILITÀ IN Q DELLE FUNZIONI RICORSIVE

- Un insieme A è binumerabile in Q se esiste una formula Φ(x1,...,xk) tale che ∀ a1,...,ak ∈ N
  - se (a1,...,ak) ∈ A, allora Q ⊢ Φ('a1',...,'ak')
  - se (a1,...,ak) ∉ A, allora Q ⊢ ¬Φ('a1',...,'ak')
- Ogni insieme Δ0-definibile è binumerabile in Q
- Una funzione totale f è binumerabile in Q, se il suo grafo è binumerabile in Q, cioè esiste una formula Φ (x1, . . . , xk, y) tale che ∀ a1,...,ak ∈ N:
  - 1) Se f(a1,...,ak)=b allora Q⊢Φf('a1',...,'ak','b')
  - 2) Se f(a1,...,ak)≠b allora Q⊢¬Φf('a1',...,'ak','b')

  Se valgono queste due condizioni diciamo che Φ binumera f
- Diciamo che f è binumerata funzionalmente da Φ se oltre a 1) e 2) vale: — 3) Q ⊢ ∃ !yΦ('a1',...,'ak',y)
- Ogni funzione ricorsiva totale f è binumerata funzionalmente in Q e la formula binumerante può essere scelta di complessità Σ_1
  - Possiamo definire x^y=z e x!=y in PA

TEOREMA DI INCOMPLETEZZA

ARITMETIZZAZIONE DELLA SINTASSI

Sia L un linguaggio del primo ordine con un numero finito di simboli di funzione, relazione e costante.
Sia #:L∪{ ¬, ∨ , ∧ , → , ∀ , ∃ , =, v } → N la funzione che associa ad ogni simbolo s il numero naturale #(s)

Fissiamo <a1,...,an> la codifica delle successioni di numeri naturali al fine di codificare la sintassi

L-TERMINI

Associamo alla variabile vi il numero ⌜vi⌝ = <#(v), i>

Se c è un simbolo di costante di L, ⌜c⌝ = <#(c)>

Se f è un simbolo di funzione n-aria di L, e t è un L-termine della forma f(t1,...,tn), ⌜t⌝ = <#f,⌜t1⌝,...,⌜tn⌝>

L-FORMULE

Se t1, t2 sono L-termini, ⌜t1 = t2⌝ = <#(=), ⌜t1⌝, ⌜t2⌝>

Se R è un simbolo di relazione n-aria di L, e t1,...,tn sono L-termini, allora ⌜R(t1,...,tn)⌝ = <#R,⌜t1⌝,...,⌜tn⌝>

Se α, β sono L-formule, allora ⌜¬α⌝ = <⌜¬⌝, ⌜α⌝>, ⌜(α∨β)⌝ = <⌜∨⌝, ⌜α⌝, ⌜β⌝>, ecc... per tutti i connettivi e quantificatori

INSIEMI PRIMITIVI RICORSIVI

{⌜t⌝ | t è un L-termine } è P.R.

{⌜Φ⌝ | Φ è una L-formula } è P.R.

Esiste una funzione primitiva ricorsiva sub: N^3 → N tale che sub(⌜Φ⌝, i, ⌜t⌝) = ⌜Φ[t/vi]⌝ per ogni L-formula Φ e ogni L-termine t

Sia T una L-teoria tale che l'insieme AxT={⌜Φ⌝ | Φ è un assioma di T} è ricorsivo. Allora l'insieme delle conseguenze logiche (codificate) di T è ricorsivamente enumerabile

Basta mostrare che esiste un insieme ricorsivo ProvT tale che Φ è un teorema di T sse ∃ n∈ N:(n,⌜Φ⌝)∈ ProvT

È possibile codificare con dei numeri le dimostrazioni formali:
ProvT={(n, ⌜Φ⌝) | n codifica T⊢Φ} è ricorsivo a condizione che gli assiomi di T costituiscano un insieme ricorsivo (basta r.e.)

Una teoria T (in un linguaggio finito) è decidibile se TeoT={⌜Φ⌝ | T ⊢ Φ} (le codifiche dei suoi teoremi) è ricorsivo, ed è indecidibile nel caso contrario

T è decidibile se esiste un algoritmo per stabilire, data un enunciato nel linguaggio di T , se esso è un teorema

Sia T una teoria completa con un insieme ricorsivo di assiomi (ovvero l'insieme delle codifiche degli assiomi è ricorsivo, ma basta anche r.e.)
Allora T è decidibile

PRIMO TEOREMA DI INCOMPLETEZZA DI GÖDEL

Sia L={+,.,s,0}. Esiste una funzione primitiva ricorsiva num: N → N tale che per ogni n ∈ N, num(n) = ⌜s^n(0)⌝, dove il termine s^n(0) è definito da s^0(0) = 0 e s^(n+1)(0) = s(s^n(0))

Se ⌜α⌝ = n ∈ N, indichiamo con '⌜α⌝' il termine s^n(0)

Esiste una funzione primitiva ricorsiva D : N → N tale che per ogni formula α, D(⌜α⌝) = ⌜α('⌜α⌝')⌝

LEMMA DI DIAGONALIZZAZIONE

Sia α(x) una formula nella variabile libera x. Allora esiste una formula β tale che Q dimostra l'equivalenza β ↔ α('⌜β⌝')

Dim: considero una formula δ(x,y) che binumera funzionalmente D in Q. Poniamo β = γ('⌜γ⌝') con γ =∀ y(δ(v0,y) → α(y)). In Q si ha: γ('⌜γ⌝') sse ∀ y(δ('⌜γ⌝',y) → α(y)), e visto che l'unico y che verifica δ(⌜γ⌝, y) è ⌜γ('⌜γ⌝')⌝, questo vale sse α('⌜γ('⌜γ⌝')⌝')

PRIMO TEOREMA

Esiste una formula G tale che PA⊬G e PA⊬¬G

G non è dimostrabile in PA ⟹ ¬Teo('⌜G⌝') è vero (in N) ⟹ G è vero in N ⟹ PA⊬¬G in quanto PA dimostra solo cose vere in N (essendo N un suo modello)

G dice "io non sono dimostrabile": per il lemma di diagonalizzazione ho G ↔ ¬Teo('⌜G⌝')

PA ⊢ G: ∃ n: (n, ⌜G⌝) ∈ Prov ⟹ Q ⊢ Prov (n, ⌜G⌝). Quindi Q ⊢ ∃ dProv (d, ⌜G⌝), ovvero Q ⊢ Teo(⌜G⌝). Ma allora per la scelta di G, Q ⊢ ¬G, e poiché PA contiene Q, PA ⊢ ¬G. Questo è impossibile, in quanto PA è coerente.

INDECIDIBILITÀ ESSENZIALE DI Q

Se una estensione finita di una teoria T è indecidibile, allora T è indecidibile

Una teoria T è essenzialmente indecidibile se ogni estensione coerente di T nello stesso linguaggio è indecidibile

La teoria Q di Robinson è essenzialmente indecidibile

Si dimostra per assurdo

TEOREMA DI TARSKI SULLA INDEFINIBILITÀ DELLA VERITÀ

Sia V = {⌜θ⌝ | N |= θ} l'insieme dei codici delle formule aritmetiche vere in N (nel linguaggio 0, S, +, ·). Allora V non è definibile in N, ovvero non esiste nessuna formula Φ(x) tale che, per ogni enunciato θ, si abbia θ ∈ V se e solo se N |= Φ(⌜θ⌝)

Supponiamo per assurdo che V sia definibile da Φ(x). Per il lemma di diagonalizzazione esiste un L-enunciato θ tale che N |= θ ↔ ¬Φ('⌜θ⌝'). Ne concludiamo che N |= θ se e solo se N |= ¬θ, assurdo.