Formulario di logica

MC

Nothing is more fecund than a mistake, provided one gets out of it.

1 Vuoto, universo, singoletto

Universo

$$\mathbb{U} \triangleq \{x \,|\, x = x\}$$

Vuoto

$$\varnothing \triangleq \{x \,|\, x \neq x\}$$

Singoletto

$$\{a\} \triangleq \{x \,|\, x = a\}$$

Definizione degli ordinali

$$\begin{cases} 0 & = & \varnothing \\ n+1 & = & n \cup \{n\} \end{cases}$$

2 Coppie ordinate

Una definizione adeguata di coppia ordinata deve permettere di dimostrare il seguente principio:

$$(x, y) = (z, u) \text{ sse } x = z \wedge y = u$$

Una definizione adeguata nel caso degli insiemi è dovuta a Kuratowsky:

$$(x, y) \triangleq \{\{x\}, \{x, y\}\}$$

che permette di definire le proiezioni.
Nota: è incluso il caso particolare della coppia $(x, x) = \{x, \{x, x\}\} = \{\{x\}\}$.

3 Relazioni

Se A e B sono insiemi, una relazione $R \subseteq A \times B$ è un insieme di coppie, le cui prime componenti formano il *dominio* della relazione, e le seconde componenti il *rango*.
Usiamo la notazione $R : A \nrightarrow B$.

Relazione (funzione) identica

Sia S un insieme. Allora
$Id_S \triangleq \{(x, x') \mid x \in S \wedge x = x'\}$

Relazione inversa

$R^\circ \triangleq \{(y, x) \mid (x, y) \in R\}$

Composizione

Date R e S relazioni tali che $ran(R) \cap dom(S) \neq \varnothing$:

$$R\,;S \triangleq \{(x, y) \mid \exists z.R(x, z) \wedge S(z, y)\}$$

A volte si trova $R \circ S$, RS o $S \circ R$.

Residui

$$S/R = \{(x, y) \mid \forall z.(y, z) \in R \to (x, z) \in S\}$$
$$S\backslash R = \{(x, y) \mid \forall z.(z, x) \in R \to (z, y) \in S\}$$

Spazio

Una relazione $R : A \nrightarrow B$ è un elemento di $2^{A \times B}$ (o se vogliamo, un sottoinsieme di $A \times B$, o una funzione da A in 2^B).

Chiusure

Data una relazione R su un insieme A, definiamo:

- l'n-esima *potenza* (l'n-esima composizione di R con se stessa):

$$R^n \triangleq \begin{cases} Id_A & \text{se} \quad n = 0 \\ R^{n-1} \circ R & \text{se} \quad n > 0 \end{cases}$$

- la chiusura transitiva di R:

$$R^+ \triangleq \bigcup_{n \geq 1} R^n$$

  (la più piccola relazione transitiva su A contenente R)

- la chiusura riflessiva-transitiva di R:

$$R^* \triangleq \bigcup_{n \geq 0} R^n$$

Nota:

- $R^+ = R \circ R^*$
- $R^* = Id_A \cup R^+$
- $(R \cup R^{-1})^*$ è la più piccola relazione di equivalenza su A contenente R.

Proprietà relazioni

Sia R relazione di tipo $R : A \nrightarrow B$ su un universo U. Allora:

- R è riflessiva sse $Id_U \subseteq R$
- R è transitiva sse $R; R \subseteq R$
- R è simmetrica sse $R^\circ \subseteq R$
- R è interpolativa (densa) sse $R \subseteq R; R$
- R è antisimmetrica sse $R \cap R^\circ \subseteq Id_U$
- R è funzionale sse $R^\circ ; R \subseteq Id_B$
- R è totale sse $Id_A \subseteq R ; R^\circ$
- R è iniettiva sse R° è funzionale sse $R; R^\circ \subseteq Id_A$
- R è suriettiva sse R° è totale sse $id_B \subseteq R^\circ; R$
- R è biettiva sse $R ; R^\circ = Id_A$ e $R^\circ = Id_B$

4 Logica modale

Per ogni proprietà, R soddisfa la proprietà in un frame $F = (W, R)$ sse l'assioma corrispondente è valido per F.
Inseriamo anche la proprietà di connessione debole: $\forall x, y, z(Rxy \wedge Rxz \rightarrow Ryz \vee y = z \vee Rzy)$, di cui l'assioma modale è L: $\Box(A \wedge \Box A \rightarrow B) \vee \Box(B \wedge \Box B \rightarrow A)$.
La logica modale proposizionale non è equivalente a FOL:

- ci sono classi di frames non definibili al primo ordine: e.g. quelli che rendono valido l'assioma M (di McKinsey) $\Box\Diamond A \rightarrow \Diamond\Box A$
- ci sono proprietà elementari di R non catturabili da alcun assioma modale (e.g. la proprietà irriflessiva)

Una logica modale Δ è detta *normale* se:

- contiene lo schema:
$$K : \Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$$
- ed è chiusa sotto necessitazione:
$$\frac{A}{\Box A}\ (Nec)$$

Teorema: se in una logica normale vale $\Diamond A \rightarrow \Box A$, allora $\Box$ commuta con $\vee$ e con $\rightarrow$.
Teorema (Scott-Lemmon): sia ϕ una formula positiva[1]. Allora lo schema di assiomi:
$$\Diamond^h \Box^i \phi \rightarrow \Box^j \Diamond^k \phi$$
è valido in tutti e soli i frames con R:
$$R^h wv \wedge R^j vu \rightarrow \exists x. R^i vx \wedge R^k ux$$
dove $\Box^n$ denota n boxes, mentre R^n denota la composizione n-esima di R.

[1] Una formula ϕ è *positiva* se è atomica o se è costruita con i soli connettivi $\wedge$, $\vee$, $\Box$, $\Diamond$.

Teoria della corrispondenza

Se R è una relazione binaria, le proprietà più importanti di cui può godere sono:

R	FOL	Assioma	
riflessiva	$\forall x(Rxx)$	$\Box A \to A$	(T)
irriflessiva	$\forall x(\neg Rxx)$	non rappr.	
simmetrica	$\forall xy(Rxy \to Ryx)$	$A \to \Box\Diamond A$	(B)
asimmetrica	$\forall xy(Rxy \to \neg Ryx)$	non rappr.	
antisimmetrica	$\forall xy(Rxy \wedge Ryx \to x = y)$	non rappr.	
transitiva	$\forall xyz(Rxy \wedge Ryz \to Rxz)$	$\Box A \to \Box\Box A$	(4)
intransitiva	$\forall xyz(Rxy \wedge Ryz \to \neg Rxz)$		
lineare	$\forall xy(Rxy \vee Ryx \vee x = y)$		
seriale	$\forall x\exists y(Rxy)$	$\Box A \to \Diamond A$	(D)
funzionale	$\forall x\exists!y(Rxy)$	$\Diamond A \to \Box A$	
funz. parziale	$\forall x\exists!!y.(Rxy)$	$\Diamond A \to \Box A$	
euclidea	$\forall xyz(Rxy \wedge Rxz \to Ryz)$	$\Diamond A \to \Box\Diamond A$	(5)
debolmente densa	$\forall x\forall y(Rxy \to \exists z(Rxz \wedge Rzy))$	$\Box\Box A \to \Box A$	
debolmente diretta	$\forall xyz(Rxy \wedge Rxz \to \exists w(Ryw \wedge Rzw))$	$\Diamond\Box A \to \Box\Diamond A$	

4.1 Barcan-formula

La formula di Barcan:

$$\forall x(\Box Fx) \to \Box\forall x(Fx)$$

è valida in strutture di Kripke con dominio anti-monotòno.

La conversa:

$$\Box\forall x(Fx) \to \forall x(\Box Fx)$$

è valida in strutture con dominio monotòno.

In strutture di dominio costante le due formule sono entrambe valide.
In strutture con dominio relativo nessuna delle due è valida in generale.

Il dominio costante tra mondi corrisponde alla prospettiva *possibilista*, secondo la quale i quantificatori variano su tutti gli individui, compresi i possibili. Questo è adeguato quando si vuole quantificare su concetti individuali.

Una controindicazione è che se si vuole distinguere tra oggetti attuali e non attuali si è costretti a usare un qualche predicato di esistenza o le logiche libere.

Il dominio relativo cattura (forse) meglio le nostre intuizioni modali. Nei sistemi a dominio relativo spesso si definisce un predicato di esistenza:

$$E!x \triangleq \exists y.(y = x)$$

In tali sistemi, vale:

$$\Box\forall x.E!x$$

(necessariamente ogni cosa esiste), ma non:

$$\forall x.\Box E!x$$

(la Necessary Existence: ogni cosa esiste necessariamente).
Un problema del dominio relativo (che corrisponde alla prospettiva *attualista*) è però di dover assumere limitazioni, come la chiusura universale di tutte le formule e il non uso delle costanti.

Proprietà valide con dominio costante

- $\forall x.\Box\exists y(y = x)$ (Necessary Existence)
- Barcan Formula
- Converse Barcan Formula

L'attualista non può accettare questi principi, perché vorrebbe oggetti contingenti, ossia x tali che: $\Diamond E!x \wedge \Diamond\neg E!x$. Ma necessitando NE si ha $\Box\forall x.\Box E!x$, che implica che non ci sono oggetti contingenti.
Ora, CBF implica il Serious Actualism:

$$\Box(P(x) \rightarrow \exists y.x = y)$$

che è accettato dall'attualista. Ma da CBF e SA si deriva NE.

Nel sistema di Kripke 1963 i domini sono relativi ai mondi, BF, CBF e NE non sono valide (i domini possono essere vuoti). Per bloccare la derivazione di BF, CBF e NE Kripke assume l'interpretazione di generalità delle variabili libere, ed è costretto a non usare costanti. Nec è derivabile, mentre Gen è inutile. Nel sistema non si possono provare modalità *de re*, come $\forall x.\Box(P(x) \rightarrow P(x))$, che però grazie Nec e all'interpretazione di generalità sono assunte come assiomi.

5 Funzioni

Dati due insiemi A e B, $f : A \rightarrow B$ sse

(i) $f \subseteq A \times B$

(ii) $\forall a \in A.\exists! b \in B.(a, b) \in f$

Nota: A e B sono detti *dominio* e *codominio* della funzione. Qui trattiamo le funzioni come particolari relazioni, ma in questo modo trattiamo solo la parte estensionale della nozione di funzione. La nozione di codominio ad esempio non può essere caratterizzata dal grafo della funzione.

Funzioni parziali

Dati due insiemi A e B, $f : A \rightharpoonup B$ sse

(i) $f \subseteq A \times B$

(ii) $\forall a \in A.\exists!! b \in B.(a, b) \in f$

Nota: sotto l'ipotesi che $f : A \rightarrow B$, $a \in A$ e $P(x)$ sia una proprietà, le due affermazioni

- $\exists b \in B((a, b) \in f \wedge P(b))$
- $\forall b \in B((a, b) \in f \Rightarrow P(b))$

sono equivalenti, ed esprimono $P(f(a))$.

Grafo di una funzione

Data $f : A \to B$, il grafo di f (la sua applicazione) è l'insieme
$\hat{f} = \{(x, y) \,|\, (x, y) \in f\}$

Per le funzioni, come per gli insiemi, vale un *principio di estensionalità*: date $f, g : A \to B$, se per ogni $a \in A$ si ha $f(a) = g(a)$, allora $f = g$.

Immagine, controimmagine, immagine diretta

Siano $f : A \to B$, $C \subseteq A$, $D \subseteq B$. Definiamo tre operatori[2]:

- **immagine** (di C lungo f)

$$f_!(C) \triangleq \{y \in B \,|\, \exists x \in C.f(x) = y\}$$

- **controimmagine**

$$f^*(D) \triangleq \{x \in A \,|\, f(x) \in D\}$$

- **immagine diretta**

$$f_*(C) \triangleq \{y \in B \,|\, \forall x \in A.f(x) = y \Rightarrow x \in C\}$$

Aggiunzioni

Sotto le ipotesi precedenti,

$$f_!(C) \subseteq D \text{ sse } C \subseteq f^*(D)$$

e

$$f^*(C) \subseteq D \text{ sse } C \subseteq f_*(D)$$

Per cui vale

$$f_! \dashv f^* \dashv f_*$$

Spazio

Lo spazio delle funzioni da A in B è notato con B^A, e la sua cardinalità è $|B|^{|A|}$.

Matrici

Una matrice $A \times B$ a valori in C è una funzione di tipo $A \times B \to C$, cioè un elemento di $C^{A \times B}$.
Nel caso particolare che $C = Bool$ si avrà una matrice elemento di $2^{A \times B}$, cioè una relazione da A a B.

[2] Gli operatori *immagine* e *immagine diretta* hanno tipo $\mathbb{P}(A) \to \mathbb{P}(B)$, l'operatore di *controimmagine* ha tipo $\mathbb{P}(B) \to \mathbb{P}(A)$.

Kernel e proiezione

Data $f : X \to S$ si definisce il *kernel* (o *nucleo di equivalenza*) di f:

$$E_f \triangleq \{(x, y) \in X \times X \mid f(x) = f(y)\}$$

Inoltre, data una relazione di equivalenza E su un insieme X si definisce una funzione di proiezione $p : X \to X/_E$, che assegna a ogni $x \in X$ la sua classe di equivalenza.

Ogni funzione $f : X \to S$ può essere scritta come composizione $g \circ p$:

$$X \overset{p}{\to} X/_{E_f} \overset{g}{\rightarrowtail} S$$

dove p è la proiezione di ogni elemento di X verso il quoziente $X/_{E_f}$, e g è iniettiva.

6 Proprietà dell'esponenziazione

Questi isomorfismi sono in effetti trasformazioni naturali. Il prodotto e l'oggetto terminale danno:

$$(C^B)^A \simeq C^{(A \times B)}$$

$$A^{\mathbf{1}} \simeq A$$

$$(A \times B)^C \simeq A^C \times B^C$$

La somma e l'oggetto iniziale danno:

$$C^{A+B} \simeq C^A \times C^B$$

$$C^{\mathbf{0}} \simeq \mathbf{1}$$

$$A \times (B + C) \simeq A \times B + A \times C$$

$$A \times \mathbf{0} \simeq \mathbf{0}$$

$$\mathbb{P}(X) \simeq Bool^X$$

$$X^{\mathbf{1}} \simeq X$$

$$\mathbf{1}^X \simeq \mathbf{1}$$

$$X^{\mathbf{0}} \simeq \mathbf{1}$$

$$\mathbf{0}^X \simeq \mathbf{0}$$

7 Aggiunzioni

Logica	**Insiemi**	**Funzioni**
$\dfrac{C \models A \quad C \models B}{C \models A \wedge B}$	$\dfrac{C \subseteq A \quad C \subseteq B}{C \subseteq A \cap B}$	$\dfrac{C \to A \quad C \to B}{C \to A \times B}$
$\dfrac{A \models C \quad B \models C}{A \vee B \models C}$	$\dfrac{A \subseteq C \quad B \subseteq C}{A \cup B \subseteq C}$	$\dfrac{A \to C \quad B \to C}{A \uplus B \to C}$
$\dfrac{A \wedge C \models B}{C \models A \Rightarrow B}$	$\dfrac{A \cap C \subseteq B \quad C \subseteq S}{C \subseteq (S \backslash A) \cup B}$	$\dfrac{A \times C \to B}{C \to B^A}$
$\dfrac{\bot \models C}{\text{sempre}}$	$\dfrac{\varnothing \subseteq C}{\text{sempre}}$	$\dfrac{\varnothing \to C}{\text{sempre}}$
$\dfrac{C \models \top}{\text{sempre}}$	$\dfrac{C \subseteq S}{\text{sempre}}$	$\dfrac{C \to \{0\}}{\text{sempre}}$

Con $A \uplus B$, o anche $A + B$, intendiamo l'unione disgiunta:

$$A \uplus B \triangleq A \times \{0\} \cup B \times \{1\}$$

8 Interazione quantificatori-connettivi

Movimento

$$\begin{aligned}
\forall x(Ax \to B) &\equiv \exists x Ax \to B \\
\exists x(Ax \to B) &\equiv \forall x Ax \to B \\
\forall x(A \to Bx) &\equiv A \to \forall x Bx \\
\exists x(A \to Bx) &\equiv A \to \exists x Bx \\
\forall x(Ax \to Bx) &\models \forall x.Ax \to \forall x.Bx \\
A \wedge \forall x Bx &\equiv \forall x(A \wedge Bx) \\
A \wedge \exists x Bx &\equiv \exists x(A \wedge Bx) \\
A \vee \forall x Bx &\equiv \forall x(A \vee Bx) \\
A \vee \exists x Bx &\equiv \exists x(A \vee Bx)
\end{aligned}$$

Distribuzione

È semplice: $\forall$ commuta con $\wedge$, $\exists$ con $\vee$.
$\forall$ raccoglie su $\vee$ (e non distribuisce).
$\exists$ distribuisce su $\wedge$ (e non raccoglie).

Dipendenza quantificatori

$\exists x \forall y (Axy) \models \forall y \exists x (Axy)$
ma non viceversa.

9 Logica intuizionista

Consideriamo il calcolo proposizionale intuizionista (IPC). Essendo sottoposto all'interpretazione BHK, esso è restrittivo su disgiunzione, negazione ed esistenziale. Ne segue che nessun connettivo è definibile in termini di altri. In IPC falliscono ad esempio i seguenti teoremi classici:

- $A \vee \neg A$
- $(A \to B) \to (\neg A \vee B)$
- $(A \to B \vee C) \to (A \to B) \vee (A \to C)$
- $((A \to B) \to B) \to (A \vee B)$

E ancora *non* sono valide:

- DeMorgan: $\neg(A \wedge B) \to (\neg A \vee \neg B)$
- contrapposizione: $(\neg A \to \neg B) \to (B \to A)$
- la legge di Peirce: $((A \to B) \to A) \to A$
- interdefinibilità: $\neg \forall x.\phi \to \exists x.\neg\phi$
- doppia negazione: $\forall x.\neg\neg\phi(x) \to \neg\neg\forall x.\phi(x)$[3]

Il calcolo intuizionista gode della proprietà della disgiunzione:

$$\text{se } \vdash_{IPC} (A \vee B) \text{ allora } \vdash_{IPC} A \text{ oppure } \vdash_{IPC} B$$

La logica classica non ne gode: un esempio è $A \vee \neg A$.
Nota: consideriamo la CWA. Essa in generale non preserva la consistenza, infatti assumiamo di avere un database $\Delta = \{\alpha \vee \beta\}$. Allora $\Delta \vdash \alpha \vee \beta$. Siccome né α né β sono conseguenze di Δ, applicando CWA avremo $\Delta \models \neg\alpha \wedge \neg\beta \wedge (\alpha \vee \beta)$. Questa è una contraddizione.
E infatti CWA(Δ) preserva la consistenza di Δ sse Δ ha modello minimo.
È come dire che la logica intuizionista opera su "modelli minimi"?

Teorema di Glivenko

$$\vdash_{CPC} \phi \text{ sse } \vdash_{IPC} \neg\neg\phi$$

Nota: il risultato non si estende al caso predicativo.

[3] Mentre non ci sono problemi con $\wedge$ e $\to$: la doppia negazione commuta con essi.

La traduzione di Gödel
Analogo risultato è la traduzione di Gödel (1932), che mappa la logica classica nella logica intuizionista negando doppiamente atomi, disgiunzioni ed esistenziali[4]. Gödel ha anche fornito un mapping con S4.

$$\vdash_{CPC} \phi \text{ sse } \vdash_{IPC} \phi^{\neg\neg}$$

e

$$\vdash_{IPC} \phi \text{ sse } \vdash_{S4} \phi^{\Box}$$

Col senno di poi, il mapping con S4 non è una sorpresa: data una struttura di Kripke riflessiva e transitiva, si possono interdefinire un'algebra di Heyting e uno spazio topologico.

Logiche intermedie
Il calcolo intuizionista più il terzo escluso dà il calcolo classico. Ma ci sono logiche intermedie:

- LC (Dummett): IPC+$(A \to B) \vee (B \to A)$. Caratterizza frames lineari, ed è completa per quelli finiti.
- KC (logica del terzo escluso debole): IPC+$\neg A \vee \neg\neg A$, completa rispetto a frames finiti con elemento massimo
- (3-Peirce): IPC+$((C \to (((A \to B) \to A) \to A)) \to C) \to C$. Caratterizza i frames di profondità 2 ed è completa rispetto a quelli finiti
- IPC+$\forall x(A \vee Bx) \to A \vee \forall x.Bx$. Completa per i frames con dominio costante

10 Proprietà proof-teoretiche

Cut-elimination theorem
La regola del taglio è eliminabile.
Da esso:

- *quasi sempre* segue la subformula property

Subformula property
Ogni prova di un sequente non contiene formule che non siano già nel sequente.
Da essa seguono:

- consistenza del sistema (l'assurdo non è derivabile)
- decidibilità
- teorema dell'interpolante di Craig

Per **S5** vale, anche se non si ha l'eliminazione del taglio.

[4] Anche per questo motivo è fuorviante dire che la logica intuizionista è un indebolimento della logica classica. Lo è per un aspetto, ma ne è arricchimento sotto altri aspetti.

Disjunction property
La logica intuizionista gode della *disjunction property*: per ogni α e β, se $\vdash \alpha \vee \beta$, allora $\vdash \alpha$ o $\vdash \beta$.
Nella logica intuizionista, segue dall'eliminazione del taglio.

Prova: si assuma dimostrato il sequente $\Rightarrow \alpha \vee \beta$. L'ultima regola applicata, escludendo il taglio, sarà un'introduzione di $\vee$. Quindi il sequente precedente deve essere α o β.
L'argomento non vale se si ha contrazione a destra (ad es. il caso classico).

11 Semantica per la logica intuizionista

Ci sono due modi per dare una semantica al calcolo intuizionista: le algebre di Heyting e le strutture di Kripke. Vediamo le prime.

11.1 Algebre di Heyting

11.1.1 Reticoli

In teoria degli ordini, un *reticolo* $L = (S, \leq)$ è un ordine parziale in cui:

- per ogni $\{a, b\}$ con $a, b \in S$ sono definiti *il* massimo $a \vee b$ (il *join, o least upper bound*) e *il* minimo $a \wedge b$ (il *meet*, o *greatest lower bound*)[5]
- assumiamo che un reticolo sia *limitato*[6], ossia abbia due elementi $\top$ e $\bot$ tali che:
$$a \vee \bot = a$$
e
$$a \wedge \top = a$$

Avremmo potuto definire un reticolo per via algebrica, infatti $a \leq b$ sse $a \wedge b = a$, o (equivalentemente) $a \leq b$ sse $a \vee b = b$. Da questo punto di vista un reticolo è una struttura $L = (S, \wedge, \vee)$ in cui $\wedge$ e $\vee$ sono commutative, associative e idempotenti, e tra loro vale l'assorbimento. Un reticolo limitato è un reticolo in cui si hanno le identità per entrambe le operazioni. **Nota**: in un reticolo limitato, sono definiti il join vuoto (che è $\bot$) e il meet vuoto (che è $\top$).

[5] Il *least upper bound* di un insieme $A \subseteq S$ è:
- un *upper bound*, ovvero un elemento $c \in S$ tale che $x \leq c$ per ogni $x \in A$
- non esistono upper-bounds y tali che $y \leq x$

[6] Possiamo assumerlo nella definizione perché ogni reticolo non vuoto e finito può essere esteso a un reticolo limitato, prendendo:
$$\top = \bigvee S = s_1 \vee \dots s_n$$
e
$$\bot = \bigwedge S = s_1, \cdots, s_n$$

11.1.2 Residui

In generale, siano P e Q ordini parziali. Una mappa $f : P \to Q$ è *residuata* se esiste una mappa $g : Q \to P$ (il residuo di f) tale che per ogni $p \in P$, $q \in Q$:

$$f(p) \leq q \text{ iff } p \leq g(q)$$

Dato che, se esiste, g è unica, la possiamo chiamare f^*. Si noti che:

- $f^*(q) = max\{p \in P \mid f(p) \leq q\}$
- $f(p) = min\{q \in Q \mid p \leq f^*(q)\}$

f commuta con i *joins*, f^* con i *meets*. f e g costituiscono una connessione di Galois.

Se $P = Q$ possiamo considerare il caso specifico dei reticoli residuati, prendendo per ogni fissato $u \in P$ mappe da P in P: $g_u(x) = u \cdot x$ e $h_u(x) = x \cdot u$. I residui saranno $g_u^*(y) = u\backslash y$ e $h_u^*(y) = y/u$.

Quindi, un semigruppo parzialmente ordinato $(P, \cdot, \leq)$ è *residuato* sse si hanno due operazioni $\backslash$ e $/$ (il residuo destro e sinistro di $\cdot$) tali che, per ogni $x, y, z \in P$:

$$x \cdot y \leq z \text{ iff } y \leq x\backslash z \text{ iff } x \leq z/y$$

Se P è un reticolo e $(P, \cdot)$ ha unità si ha un *reticolo residuato*[7]. In ogni reticolo residuato valgono:

- $(x \vee y)\backslash z = (x\backslash z) \wedge (y\backslash z)$
- $z/(x \vee y)(z/x) \wedge (z/y)$
- $z\backslash(x \wedge y) = (z\backslash x) \wedge (z\backslash y)$
- $(x \wedge y)/z = (x/z) \wedge (y/z)$
- $x\backslash z = max\{y \mid x \cdot y \leq z\}$
- $z/y = min\{x \mid x \cdot y \leq z\}$

Se $\cdot$ è commutativa, allora $a\backslash b = b/a$. In questi casi si usa un solo simbolo, $a \to b$.

11.1.3 Algebre di Heyting

In ogni reticolo vale una distributività debole, ossia:

$$x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$$

$$x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$$

Se valgono le uguaglianze (che peraltro si implicano a vicenda), il reticolo è *distributivo*.

Un'*algebra di Heyting* è un reticolo distributivo $L = (S, \leq)$ con minimo $\bot$, in cui per ogni $a, b \in S$ esiste un elemento $a \to b$ tale che $\to$ è residuo di $\wedge$, ossia:

$$a \wedge c \leq b \text{ sse } c \leq a \to b$$

[7] In generale si distinguono $\cdot$, l'operazione del monoide, e $\wedge$, la congiunzione reticolare, così come 1, l'unità monoidale, e $\top$, l'elemento top del reticolo.

per ogni $c \in S$.
In un'algebra di Heyting si definiscono $\neg a \triangleq a \to \bot$ (lo pseudo-complemento di a relativo a $\bot$) e $\top \triangleq \bot \to \bot$.

Si dimostra che:

$$a \to b = \bigvee \{c \in S \mid a \wedge c \leq b\}$$

Un'*algebra di Boole* è un'algebra di Heyting in cui per ogni $a, b \in S$:

$$a \to b = \neg a \vee b$$

o (equivalentemente) in cui:

$$a \vee \neg a = \top$$

oppure in cui:

$$\neg\neg a = a$$

Nota: nelle algebre di Boole ogni elemento a ha il suo *complemento* (unico, in strutture distributive), ovvero un b tale che:

$$a \vee b = \top$$

e

$$a \wedge b = \bot$$

Come già visto, le algebre di Heyting hanno una nozione più debole, lo *pseudo-complemento*, ossia il più grande y tale che $x \wedge y = \bot$.

11.1.4 Filtri e ideali

Dato un poset L, un sottoinsieme non vuoto $D \subseteq L$ è *diretto* se, per ogni $x, y \in D$, esiste $z \in D$ t.c. $x \leq z$ e $y \leq z$.

Una funzione tra posets $f : P \to Q$ preserva joins diretti se esiste:

$$\bigvee f(S) = \bigvee \{f(s) \mid s \in S\} \text{ e } f(\bigvee(S) = \bigvee f(S))$$

per ogni poset diretto $S \subseteq P$ tale che abbia $\bigvee(S)$.
Analogo per la preservazione dei meets diretti.
La preservazione di joins (o meets) diretti implica la monotonìa per f.

f è detta *Scott-continua* se preserva joins diretti.

Dato un insieme X, definiamo:

$$\downarrow X \triangleq \{y \mid \exists x \in X.(y \leq x)\}$$

e chiamiamo *lower sets* quegli insiemi X t.c. $X = \downarrow X$. La nozione di *upper set* è definita dualmente.
Di particolare interesse sono i casi in cui l'insieme interessato è un singoletto $\{x\}$, denotati $\downarrow x$.

Dato un poset P, un **ideale** $I \subseteq P$ è un lower set diretto.
Nota:

- i lower sets $x \downarrow$ sono sempre ideali, e sono detti gli *ideali principali* generati dall'elemento x
- il vuoto non è mai un ideale (perché non è diretto per definizione di "diretto")

La nozione di *filtro* è duale a quella di *ideale*.

La *ideal completion* di un poset P è il poset di tutti gli ideali di P ordinati per inclusione. Grazie a questa costruzione, dato un semireticolo superiore si può costruire un reticolo completo.

12 Valori di verità

Chiamiamo Ω l'insieme dei valori di verità. Le costanti $\top$ e $\bot$ sono valori di verità (rappresentati eventualmente da enunciati). Ω ha due elementi *nel senso debole*: ha due elementi distinti $\top$ e $\bot$ e, dato un $x \in \Omega$, x non è distinto da essi (ma non è detto che si abbia un algoritmo per decidere se $x = \top$ o $x = \bot$).
Consideriamo poi un insieme $\mathbf{2}$ di due elementi, *nel senso forte*: $\mathbf{2}$ ha due elementi distinti $\top$ e $\bot$ e si ha un algoritmo che decide, dato un elemento $x \in \mathbf{2}$, se $x = \top$ o $x = \bot$. È l'insieme dei valori di verità *decidibili*:

$$\mathbf{2} = \{p \in \Omega \mid p \text{ oppure } \neg p\}$$

Da un punto di vista costruttivista possiamo considerare l'insieme Ω_C dei valori di verità *classici*:

$$\Omega_C = \{p \in \Omega \mid p \leftrightarrow \neg\neg p\}$$

Quindi abbiamo gli insiemi Ω, Ω_C, $\mathbf{2}$, che hanno tutti e tre "due elementi", ma in sensi diversi. Vale:

$$\mathbf{2} \subseteq \Omega_C \subseteq \Omega$$

Nel caso classico si ha: $\mathbf{2} = \Omega_C = \Omega$.
$\mathbf{2} = \Omega$ significa "possiamo calcolare valori di verità". Questo è vero ad esempio nel caso proposizionale.

13 Gerarchie

Teorema: un insieme S è R.E. sse esiste un predicato decidibile P t.c.

$$x \in S \text{ sse } \exists y.P(x, y)$$

Teorema: un insieme S è il complemento di un insieme RE sse esiste un predicato decidibile P t.c.

$$x \in S \text{ sse } \forall y.P(x, y)$$

Estendendo, si ha la gerarchia aritmetica.

13.1 Gerarchia aritmetica

È la gerarchia dei "gradi di indecidibilità". Parallelamente, classifica le formule della logica del primo ordine.
Definiamo la classe Σ_n degli insiemi S tali che esiste un predicato ricorsivo P e una sequenza di n quantificatori alternati iniziante per $\exists$ tale che:

$$x \in S \text{ sse } \exists y_1, \ldots, y_n.P(x, y_1, \ldots, y_n)$$

Π_n si definisce in modo duale[8].

Avremo che:

- $\Sigma_0 = \Pi_0 = R$ (proprietà decidibili)
- $\Sigma_1 = RE$ (Girard chiama le proprietà definite da queste formule *espansive*, ad esempio la derivabilità nell'aritmetica o al primo ordine)
- $\Pi_1 = \overline{RE}$ (Girard chiama le proprietà definite da queste formule *recessive*, ad esempio la consistenza dell'aritmetica, che equivale alla non derivabilità dell'assurdo)

In generale un insieme Σ_n è il complemento di un insieme Π_n e viceversa. Ad es:

- $K \in \Sigma_1$ e $K \in RE$
- $\overline{K} \in \Pi_1$ e $\overline{K} \notin RE$
- $T \in \Pi_2$
- $\overline{T} \in \Sigma_2$

Nota:

- in alcune trattazioni si indica anche un apice su Σ_n e Π_n. L'apice indica l'ordine di quantificazione. Nel caso della gerarchia aritmetica si quantifica su numeri, quindi l'ordine è 0, e scriveremmo Σ_n^0 e Π_n^0. Nel caso di quantificazione su funzioni di tipo $\mathbb{N} \to \mathbb{N}$ l'ordine è 1, e quindi avremmo Σ_n^1 e Π_n^1 come nella gerarchia proiettiva (quantificazione su numeri e insiemi, corrisponde al caso della logica del secondo ordine: quantificazione su individui e proprietà)
- 1. $\forall i(\Sigma_i \subset \Sigma_{i+1})$ e $\forall i(\Pi_i \subset \Pi_{i+1})$
  2. $\forall i(\Sigma_i \cup \Pi_i \subset \Sigma_{i+1} \cap \Sigma_{i+1})$
- una formula ϕ con solo quantificatori vincolati (del tipo $\exists x < t$ o $\forall x < t$) è considerata in $\Sigma_0 = \Pi_0$.

13.2 Algoritmo Tarski-Kuratowski

L'algoritmo di Tarski-Kuratowski per la gerarchia aritmetica: data una formula ϕ

1. converti la formula in forma normale prenessa
2. se la formula è senza quantificatori, allora è in $\Sigma_0^0 = \Pi_0^0$
3. altrimenti, conta il numero k di alternanze di quantificatori
4. se il primo quantificatore è $\exists$, la formula è in Σ_{k+1}^0
5. se il primo quantificatore è $\forall$, la formula è in Π_{k+1}^0

[8] Con "quantificatori" intendiamo anche gruppi di quantificatori. Ad esempio, $\forall\forall\exists\exists$ ha alternanza 2.

13.3 Gerarchia analitica

Estensione higher-type della gerarchia aritmetica.
$\Sigma^1_0 = \Pi^1_0 = \Delta^1_0$ è la classe delle formule del linguaggio dell'aritmetica del II ordine senza quantificatori per insiemi. In questo linguaggio non ci sono parametri per insiemi, e il fatto che usiamo questo linguaggio è mostrato dal font lightface dei simboli.

Ogni simbolo **boldface** corrispondente indica invece la classe corrispondente del linguaggio esteso con parametri per i reali (la *gerarchia proiettiva*). Una formula dell'aritmetica del II ordine è definita Σ^1_{n+1} se è (logicamente equivalente a) una formula della forma:

$$\exists X_1, \ldots, \exists X_k \psi$$

dove ψ è Π^1_n. Definizione analoga per Π^1_{n+1}.
Un insieme di numeri naturali è al livello Σ^1_1 della gerarchia se è definibile con una formula del II ordine con soli quantificatori esistenziali per insiemi. Analogo per Π^1_1. n conta l'alternanza di quantificatori del II ordine.
Gli insiemi *iperaritmetici* sono esattamente gli insiemi $\Delta^1_1 = \Sigma^1_1 \cap \Pi^1_1$[9]. Un insieme iperaritmetico è l'insieme dei gödeliani delle formule vere dell'aritmetica.

13.4 Gerarchia logica

Conta solo l'alternanza di quantificatori del II ordine. La notazione è Σ^n, Π^n.
Una formula $\exists^0_1$, ad es. $\exists n.A(n)$, è traducibile nella formula $\exists x(x \in \mathbb{N} \wedge A(x))$, che è Π^1, perché:

$$x \in \mathbb{N} \iff \forall X.(X(0) \wedge \forall y.(X(y) \to X(Sy)) \to X(x))$$

In generale, una formula Π^1_n è riscrivibile in una formula Π^{n+1}.

13.5 Gerarchia polinomiale

Intuitivamente caratterizza quanto una funzione decidibile sia polinomialmente non computabile.

La gerarchia si basa sulla nozione di Turing machine con *oracolo*: un oracolo per la classe C è una sotto-procedura per i problemi in C che richiede tempo unitario.
Data una classe di problemi di decisione C, la classe P^C è la classe dei problemi di decisione risolubili in tempo polinomiale da una DTM che usa un oracolo per i problemi in C. Definiamo la gerarchia per induzione[10].

Base:	Δ^P_0	$=$	$\Sigma^P_0 = \Pi^P_0 = P$
Passo:	Δ^P_{k+1}	$=$	$P^{\Sigma^P_k}$
	Σ^P_{k+1}	$=$	$NP^{\Sigma^P_k}$
	Π^P_{k+1}	$=$	$coNP^{\Sigma^P_k}$

Nota:

- il primo livello è $\Delta^P_1 = P$, $\Sigma^P_1 = NP$, $\Pi^P_1 = coNP$
- il secondo livello è $\Delta^P_2 = P^{NP}$, $\Sigma^P_2 = NP^{NP}$, $\Pi^P_2 = \overline{NP^{NP}}$

[9] Δ^1_1 è più grande di tutti i Σ^0_n e Π^0_n.
[10] Ricordiamo che coNP=$\{\pi$ problema di decisione$|\overline{\pi} \in NP\}$.

- tutta la gerarchia polinomiale è contenuta nella Δ_1 della gerarchia aritmetica, e quindi è contenuta in R
- si definisce la classe PRIMES=$\Sigma_1^P \cap \Pi_1^P - \Delta_1^P$

14 Categorie

Categorie concrete: categoria dei grafi, categoria dei monoidi, etc.

Categorie piccole: (oggetti e frecce sono insiemi): grafi, monoidi, etc.

Categorie localmente piccole: quelle categorie in cui per ogni coppia di oggetti A e B, Hom(A,B) è un insieme.

Ogni insieme può essere visto come una categoria piccola *discreta*: oggetti i suoi elementi e uniche frecce le identità; oppure come un funtore da $\mathbb{1}$ in Set.

Una sottocategoria $\mathbf{D}\subset\mathbf{C}$ è *full* se per ogni coppia di oggetti X e Y in $\mathbf{D}$, ogni morfismo da X a Y in $\mathbf{C}$ è anche in D.

Isomorfismi: una freccia $f : A \to B$ in una categoria è un *isomorfismo* se c'è una freccia $g : B \to A$ tale che $gf = 1_A$ e $fg = 1_B$, e si scrive $A \cong B$. Stessa cosa si definisce a livello dei funtori.
Si definisce il prodotto tra categorie, che ha $\mathbb{1}$ come unità ed è associativo e commutativo a meno di isomorfismi.

Per ogni categoria A esiste un funtore $U : A \to Set$ che è *dimenticante*, ossia tale che dimentica la struttura. U è anche *fedele*, nel senso che per ogni $f, g : A \to B$, se $U(f) = U(g)$ allora $f = g$.
Per ogni categoria A ci sono funtori $\Delta : A \to A \times A$ che dato un oggetto a di A produce la coppia (a, a) e $\bigcirc : A \to \mathbb{1}$ che dato un oggetto a di A ritorna l'oggetto di $\mathbb{1}$.

Considerando le categorie di funtori, vale per ogni categoria A, B, C che:

$$A^{\mathbb{1}} \cong A$$

$$C^{A\times B} \cong (C^B)^A)$$

$$(A \times B)^C \cong A^C \times B^C$$

Se A è una categoria localmente piccola, c'è un funtore $Hom(A^{op}\times A \to Set)$, che manda ogni oggetto (A, B) di $A^{op} \times A$ in $Hom(A, B)$, e per ogni coppia di frecce (che agiscono per componenti) $(g, h) : (A, B) \to (A', B')$ il funtore manda ogni f in $Hom(A, B)$ in hfg in $Hom(A', B')$.
Sappiamo che da $Set^{A^{op}\times A} \to (Set^A)^{A^{op}}$ possiamo ottenere ora un funtore $Hom* : A^{op} \to Set^A$ e dualmente un funtore $Hom*_{A^{op}} : A \to Set^{A^{op}}$.

Yoneda Lemma: se A è localmente piccola e $F : A^{op} \to Set$ allora $Nat(h_A, F)$ è in corrispondenza biunivoca con $F(A)$.
Idea: per ogni $a \in F(A)$ otteniamo una trasformazione naturale $\breve{a} : h_A \to F$ stipulando che $\breve{a}(B) : Hom(B, A) \to F(B)$ manda $g : B \to A$ in $F(g(a))$. (ricorda che F è controvariante). Viceversa, ad ogni trasformazione naturale $t : h_A \to F$ associamo un elemento $t(A)(1_A) \in F(A)$.

Funtori full e faithful Un funtore $H_a \to B$ è *fedele* se mappa le frecce di A in modo iniettivo in B, e *full* se lo fa in modo suriettivo. Un *full embedding* è un funtore full e faithful che è anche iniettivo sugli oggetti.
Se A è localmente piccola, il funtore di Yoneda $Hom*_{A^{op}} : A \to Set^{A^{op}}$ è un full embedding.

14.1 Funtori aggiunti

Dato un funtore F tra preordini A e F visti come categorie, un funtore $G : B \to A$ è *aggiunto destro* di F se per ogni $a \in A$, $b \in B$:

$$F(a) \leq b \text{ iff } a \leq G(b)$$

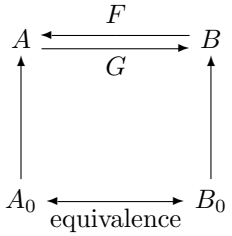
e la coppia (F, G) è detta una *connessione di Galois* covariante.
Si nota che $GF : A \to A$ è un *operatore di chiusura* su A, infatti:

inflazionario: $a \leq GF(a)$

idempotente: $GFGF(a) \leq GF(a)$

monotòno: se $a \leq a'$ allora $GF(a) \leq GF(a')$

mentre $FG : B \to B$ è un'operazione *di interno*, o di *co-chiusura*, o di *kernel*, ossia tale che $FG(x) \leq x$ per ogni x.
In un preordine $a \cong a'$ significa $a \leq a'$ e $a' \leq a$. Ne segue che $GFGF(a) \cong GF(a)$ e dualmente $FGFG(b) \cong FG(b)$ (idempotenza a meno di isomorfismi).
F e G instaurano una corrispondenza uno-a-uno tra classi di equivalenza di elementi a di A "chiusi", ossia tali che $GF(a) \cong a$ e classi di equivalenza di elementi b di B "aperti", ossia tali che $FG(b) \cong b$. Ossia F e G stabiliscono un'equivalenza tra il preordine A_0 di elementi chiusi di A e il preordine B_0 di elementi aperti di B. Questa situazione può essere descritta come un' "unità degli opposti".



Un caso particolare si ha considerando relazioni binarie $R \subseteq X \times Y$. Consideriamo $A = (\mathbb{P}(X), \subseteq)$ e $B = (\mathbb{P}(Y), \supseteq)$. Siano:

- $F(A) = \{y \in Y \mid \forall x \in A.(x, y) \in R\}$
- $G(B) = \{x \in X \mid \forall y \in B.(x, y) \in R\}$

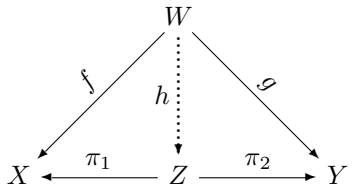
per ogni $A \subseteq X$ e $B \subseteq Y$. Questa situazione è detta una *polarità*, un isomorfismo tra il reticolo A_0 dei sottoinsiemi chiusi di X e il reticolo dei sottoinsiemi chiusi di Y.

L'usuale definizione di aggiunzione si ha generalizzando il discorso da preordini a categorie. La notazione per gli aggiunti è di solito non F e G ma F (per "free") e U (per "underlying").
Un'aggiunzione (F, G, ν, ϵ) tra categorie A e B localmente piccole è data da un isomorfismo naturale $Hom_B(F(-), -) \cong Hom_A(-, U(-))$ tra funtori $A^{op} \times B \to Set$. Un'aggiunzione tra categorie è inoltre una *equivalenza* se ν e ϵ sono isomorfismi naturali (ossia $UF \cong 1_A$ e $FU \cong 1_B$).

Una dualità tra categorie A e B è quindi una equivalenza tra A e B^{op}.

14.2 Il prodotto

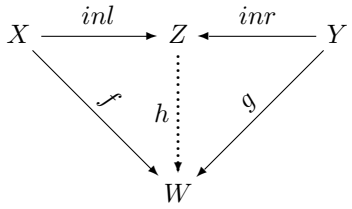
Il prodotto categoriale è costituito da un oggetto Z e da due frecce π_1 e π_2 in oggetti X e Y tali che se c'è un altro oggetto W con frecce in X e Y, c'è un'unica freccia h tale che il diagramma commuta:



La proprietà definitoria stabilisce una biezione tra coppie di frecce $(C \to A, C \to B)$ e frecce $C \to A \times B$.
Nota: il prodotto vuoto coincide con l'oggetto terminale.

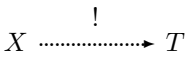
14.3 Il coprodotto

Il coprodotto è il duale del prodotto.



14.4 Oggetto terminale

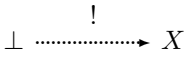
Un oggetto T in una categoria $\mathbf{C}$ è *terminale* se per ogni oggetto $X \in C_0$ c'è un'unica freccia (denotata $\bigcirc_X : X \to T$) verso T:



Nota: dire che una categoria A ha oggetto terminale $\mathtt{1}$ (risp. iniziale) equivale a dire che il funtore $\bigcirc_A : A \to \mathtt{1}$ ha aggiunto destro (risp. sinistro).

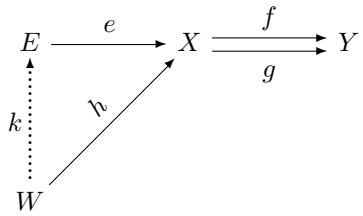
14.5 Oggetto iniziale

È il duale del terminale.



14.6 Equalizer

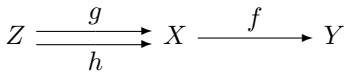
Data una coppia di frecce parallele f e g da X in Y un loro *equalizer* è una freccia e tale che $f \circ e = g \circ e$ e universale rispetto a questa proprietà.



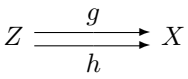
In $\mathbb{S}et$, $E = \{a \in A \mid f(a) = g(a)\}$, e $e = \subseteq$.

14.7 Monics e epics

Una mappa $f : X \to Y$ è un *monomorfismo* (o *monic*) se, quando:



commuta, allora



commuta. In altre parole, la condizione è:

$$\text{se } fg = fh \text{ allora } g = h$$

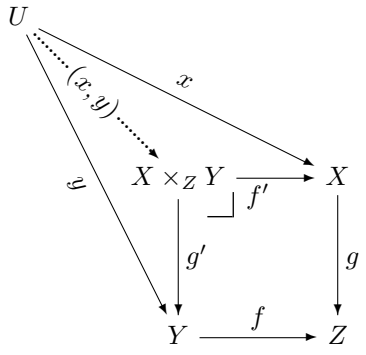
e scriviamo $X \overset{f}{\rightarrowtail} Y$.
Il concetto duale è l'*epimorfismo* (o *epic*), scritto $X \overset{f}{\twoheadrightarrow} Y$.

Teorema:

- Ogni equalizer è monic.
- Se $X \overset{f}{\to} Y$ ha un'inversa sinistra g, allora f è un equalizer.

14.8 Pullback

Un *pullback*, o prodotto fibrato, di una coppia di frecce con codominio Z è un oggetto $X \times_Z Y$ tale che il diagramma commuta:



Quando Z è l'oggetto terminale, il pullback diventa un prodotto.
Teorema: se $\mathbf{C}$ è una categoria con un terminale $\mathbf{1}$ allora $\mathbf{C}$ ha pullbacks (per ogni coppia di mappe convergenti) sse ha prodotti (per ogni coppia di oggetti) e equalizers (per ogni coppia di morfismi paralleli).

14.9 Limiti

Data una categoria I (la categoria *indice*), una categoria A e un funtore $\Gamma : I \to A$ (un I-diagramma), un *limite* di Γ è dato da un oggetto terminale nella categoria delle coppie (A, t) con a oggetto di A e $t : K(a) \to \Gamma$ trasformazione naturale, dove $K(a) : I \to A$ è il funtore con valore costante a. I limiti sono pullback, e possono essere costruiti da prodotti ed equalizer. Casi speciali di limiti sono i terminali, i prodotti, gli equalizers, i pullbacks.
Se I è un poset i limiti sono detti *proiettivi* (o *inversi*), mentre i colimiti sono detti *induttivi* (o *diretti*). Il limite di Γ si denota spesso con $\lim_{\leftarrow} \Gamma$ e il colimite con $\lim_{\rightarrow} \Gamma$.

Th: se $F : A \to B$ ha aggiunto destro $U : B \to A$, allora U preserva i limiti e F i colimiti.

Un funtore che preserva limiti finiti è detto *left exact*, uno che preserva colimiti finiti è detto *right exact*.

14.10 Monadi (o triple)

La nozione di *monade* è la generalizzazione categoriale del concetto di chiusura per un preordine (vedi sez. 14.1).

Una *monade* (T, η, μ) su una categoria A consiste di un funtore $T : A \to A$ e trasformazioni naturali $\nu : 1_A \to T$ e $\mu : T^2 \to T$ tali che:

- $\mu \circ T\nu = 1_T = \mu \circ \nu T$ (unità)
- $\mu \circ \mu T = \mu \circ T\mu$ (associativa)

Esempio: si consideri come monade T il funtore powerset (covariante) che a ogni oggetto a in A associa $\mathbb{P}(a) = \{X \mid X \subseteq a\}$ e a ogni freccia $f : a \to b$ e ogni $X \subseteq a$ associa $\mathbb{P}(f)(X) = \{f(x) \mid x \in X\}$. ν e μ saranno i mappings $\nu(a) : a \to \mathbb{P}(a)$ e $\mu(a) : \mathbb{P}(\mathbb{P}(a)) \to \mathbb{P}(a)$ definite da (per ogni insieme a, ogni elemento $a' \in A$ e insieme χ di sottoinsiemi di a):

- $\nu(a)(a') \equiv \{a'\}$
- $\mu(a)(\chi) \equiv \bigcup \chi \equiv \bigcup_{X \in \chi} X$

Th: se $F : A \to B$ ha aggiunto destro $U : B \to A$ con aggiunzioni $\nu : 1_A \to UF$ e $\epsilon : FU \to 1_B$ allora $(UF, \nu, U\epsilon F)$ è una monade su A. Anche l'inverso è vero: ogni monade si genera da un'aggiunzione. Vediamo come.

14.11 Categorie Eilenberg-Moore

Data una monade (T, μ, ν) su una categoria $\mathscr{A}$, la sua categoria di Eilenberg-Moore $\mathscr{A}^T$ è definita come segue:

- i suoi oggetti sono *algebre*, ossia coppie (A, ϕ) dove $\phi : T(A) \to A$ è una freccia di $\mathscr{A}$ tale che $\phi\nu(A) = 1_A$ e $\phi\mu(A) = \phi T(\phi)$ per ogni oggetto A di $\mathscr{A}$;

- le sue frecce sono *omomorfismi*, ossia frecce $\alpha : (A, \phi) \mapsto (A', \phi')$ di $\mathscr{A}$ tali che $\phi' T(\alpha) = \alpha\phi$

Esempio: le algebre della monade powerset di $\mathbb{S}et$ sono reticoli inf-completi e gli omomorfismi sono mappings che preservano gli inf.

Molte categorie di interesse si possono quindi vedere come categorie Eilenberg-Moore di monadi su categorie familiari.

14.12 Kleisli categories

Data una monade (T, ν, μ) su una categoria $\mathscr{A}$, la sua categoria di Kleisli $\mathscr{A}_T$ è definita come segue:

- i suoi oggetti sono gli oggetti di $\mathscr{A}$
- le sue frecce sono, per ogni freccia $A \to A'$ di $\mathscr{A}$, frecce $A \to T(A')$

La composizione di due frecce $f : A \to T(A')$ e $g : A' \to T(A'')$ è:

$$g \circledast f \equiv \mu(a'')T(g)f$$

L'identità è data da $\nu(A) : A \to T(A)$.

Esempio: la categoria Kleisli della monade powerset ha come frecce le frecce $A \to \mathbb{P}(B)$, che sono relazioni $R \subseteq A \times B$.

14.13 CCCs

Una *cartesian closed category* $\mathscr{C}$ è una categoria con prodotti finiti (e quindi oggetto terminale) tali che per ogni oggetto B, il funtore $(-) \times B : \mathscr{C} \to \mathscr{C}$ ha aggiunto destro $(-)^B : \mathscr{C} \to \mathscr{C}$.
Nota:

- per ogni categoria piccola C, la categoria funtore $\mathbb{S}et^C$ è cartesiana chiusa
- $\mathbb{C}at$ è cartesiana chiusa
- le algebre di Heyting, viste come categorie, sono (bi)cartesiane chiuse (ossia chiuse anche per coprodotti)

La categoria del λ-calcolo tipato con *surjective pairing* è equivalente alla categoria delle CCC. L'equivalenza rimane aggiungendo a entrambi i frameworks un oggetto dei numeri naturali.

Questo risultato è dovuto alla completezza funzionale delle CCC, e questa è relata al teorema di deduzione del calcolo proposizionale intuizionista, o meglio, a un'istanza della transitività:

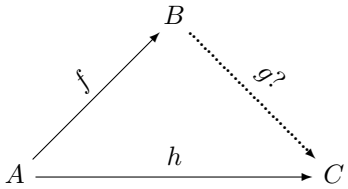
$$\frac{T \vdash A \quad A \vdash B}{T \vdash B}$$

Le *cartesian closed categories* **degenerate** sono quelle che non distinguono i morfismi (sono preordini). La logica classica è degenerata. Una logica, vista come categoria, è classica quando è equivalente alla sua opposta.

14.14 Sezioni e ritrazioni

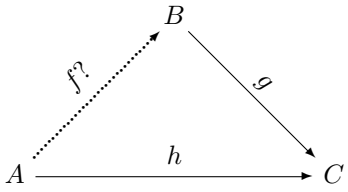
Problemi di divisione per mappe:

- *determinazione* (o "estensione"): date f e h con stesso dominio, trovare le g tali che $h = g \circ f$:



  Si dice che g è una determinazione di h attraverso f, o che h dipende solo da f, o che h è funzione di f.

- *scelta* (o lifting): date g e h con stesso codominio, trovare le f tali che $h = g \circ f$:



Se h è l'identità, determinazione e scelta diventano *retrazione* e *sezione*.
Se $A \xrightarrow{f} B$:

- una *retrazione* per f è una mappa $B \xrightarrow{r} A$ tale che $r \circ f = 1_A$
- una *sezione* per f è una mappa $B \xrightarrow{s} A$ tale che $f \circ s = 1_B$

14.15 Sotto-oggetti

Un'*inclusione*, o *mono*, in una categoria è una mappa $S \xrightarrow{i} X$, tale che per ogni oggetto T e ogni coppia di mappe s_1, s_2 da T a S:

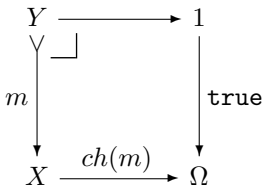
$$i(s_1) = i(s_2) \text{ implica } s_1 = s_2$$

Denotiamo un mono i da A a B con $A \xhookrightarrow{i} B$.

Con l'inclusione abbiamo la nozione di *parte* S di un insieme X, $S \hookrightarrow X$. Data una parte $S \xhookrightarrow{i} X$, la sua mappa corrispondente $X \xrightarrow{\phi_S} \mathbf{2}$ è detta *mappa caratteristica* di S, i, perché caratterizza gli elementi di S come gli elementi x tali che $\phi_S(x) = true$.

14.16 Classificatore di sotto-oggetti

Un *classificatore di sotto-oggetti* consiste di un oggetto Ω e una freccia $\texttt{true} : 1 \rightarrowtail \Omega$ tali che per ogni mono $m : Y \rightarrowtail X$ c'è un'unica mappa $ch(m) : X \to \Omega$ (la funzione caratteristica del sotto-oggetto Y) che produce un pullback:



In $\mathbb{S}et$ $ch(m)$ è la funzione caratteristica di m.

14.17 Topos

Una categoria **E** è un *topos* se:

- ha limiti finiti
- è cartesiana chiusa
- ha classificatore di sotto-oggetti

15 Tipi

15.1 Setoidi

Un *setoide* $X = (\underline{X}, =_X)$ è un *tipo* $\underline{X}$ con una relazione di equivalenza $=_X$ su X[11].

$$x \in X \triangleq x : \underline{X}$$

15.2 Funzioni

Una *funzione* f tra insiemi X e Y è una coppia $(\underline{f}, ext_f)$ con $\underline{f} : \underline{X} \to \underline{Y}$ è un'operazione t.c.:

$$(ext_f abp) : \underline{f}a =_Y \underline{f}b(a, b : \underline{X}, p : a =_X b)$$

Definiamo $f(a) \triangleq \underline{f}a$.
Una mappa tra setoidi $A = (\underline{A}, =_A)$ e $B = (\underline{B}, =_B)$ è una funzione $f : \underline{A} \to \underline{B}$ tale che sia estensionale, ossia:

$$a_1 =_A a_2 \Rightarrow f(a_1) =_B f(a_2)$$

Otteniamo una categoria dicendo che $f, g : (\underline{A}, =_A) \to (\underline{B}, =_B)$ sono uguali sse $\Pi a : A.f(a) =_B g(a)$.
Nota:

- f è mono sse $f(a_1) =_B f(a_2) \Rightarrow a_1 =_A a_2$
- f è epi sse $\Pi b : B.\Sigma a : A.b =_B f(a)$

[11] I setoidi sono anche chiamati $E - sets$ dai categoristi, *extensional sets* da Martin-Löf, e *sets* da Bishop, che chiama *presets* gli $\underline{X}$.

Le funzioni da A in B formano un insieme B^A definito dal tipo:

$$\Sigma f : \underline{A} \to \underline{B}.\forall x, y : \underline{A}.(x =_A y \Rightarrow f(x) =_B f(y))$$

con la relazione di equivalenza:

$$(f, p) =_{B^A} (g, q) \triangleq \forall x : \underline{A}.f(x) =_B g(x)$$

La valutazione $ev_{A,B} : B^A \times A \to B$:

$$ev_{A,B}((f, p), a) = f(a)$$

15.3 Setoidi discreti

Un setoide X è detto *discreto* se, per ogni $x, y \in X$:

$$(x =_X y) \vee \neg(x =_X y)$$

In teoria degli insiemi classica tutti gli insiemi sono discreti, mentre nelle teorie costruttive non è così. Ma $\mathbf{1}$ e l'insieme dei numeri naturali $\mathbb{N}$ sono discreti, e il prodotto e il coprodotto mantengono la proprietà di discretezza degli insiemi.

15.4 Predicati

Una *proprietà estensionale*, o *predicato*, P su un setoide X è una famiglia di proposizioni $P(x)(x \in X)$ con:

$$x =_X y, P(x) \Rightarrow P(y)$$

Una *relazione* R tra insiemi X e Y è una famiglia di proposizioni $R(x, y)(x \in X, y \in Y)$ con:

$$x =_X x', y =_Y y', R(x, y) \Rightarrow R(x', y')$$

15.5 Equivalenze

Una relazione di equivalenza $\sim$ è *più fine* di una r.d.e. $\approx$ su un tipo $\underline{A}$ se per ogni $x, y : A$:

$$x \sim y \Rightarrow x \approx y$$

Se esiste la più fine r.d.e. $=_A$ su un tipo $\underline{A}$, il setoide $A = (\underline{A}, =_A)$ ha la *proprietà di sostituzione* (per ogni predicato P sul tipo $\underline{A}$):

$$x =_A y \Rightarrow (P(x) \iff P(y))$$

Raramente i setoidi sono sostitutivi, e la nozione non si conserva tra isomorfismi. Si può però costruire un setoide sostitutivo A per ogni tipo $\underline{A}$ grazie alla costruzione identità $Id(\underline{A})$.

16 Calcoli

16.1 Hilbert

- 3 assiomi

  (A1) $A \to (B \to A)$
  (A2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
  (A3) $(\neg A \to \neg B) \to (B \to A)$

- 1 regola

$$\frac{A \quad A \to B}{B}\ (mp)$$

L'estensione al primo ordine si ha aggiungendo:

- 2 assiomi

  (A4) $\forall x.(A(x) \to A[x/t])$
  (A5) $A(t) \to \exists x.A(x)$

- 2 regole

$$\frac{X \to A(t)}{X \to \forall x(A(x))}\ (\forall r)$$

$$\frac{A(t) \to X}{\exists x(A(x)) \to X}\ (\exists l)$$

con t non libero in X né in A(x).

16.2 Deduzione naturale intuizionista

Vedi figura 1. Vedi figura 2

$$\frac{A \quad B}{A \wedge B}\ \wedge\text{-}I \qquad \frac{A \wedge B}{A}\ \wedge\text{-}EL \qquad \frac{A \wedge B}{B}\ \wedge\text{-}ER$$

$$\frac{A}{A \vee B}\ \vee\text{-}IL \qquad \frac{B}{A \vee B}\ \vee\text{-}IR \qquad \frac{A \vee B \quad \begin{matrix}[A]\\ \vdots \\ C\end{matrix} \quad \begin{matrix}[B]\\ \vdots \\ C\end{matrix}}{C}\ \vee\text{-}E$$

$$\frac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \to B}\ \to\text{-}I \qquad \frac{A \to B \quad A}{B}\ \to\text{-}E \qquad \frac{\bot}{A}\ \bot\text{-}E$$

Tabella 1: Deduzione naturale senza regole classiche.

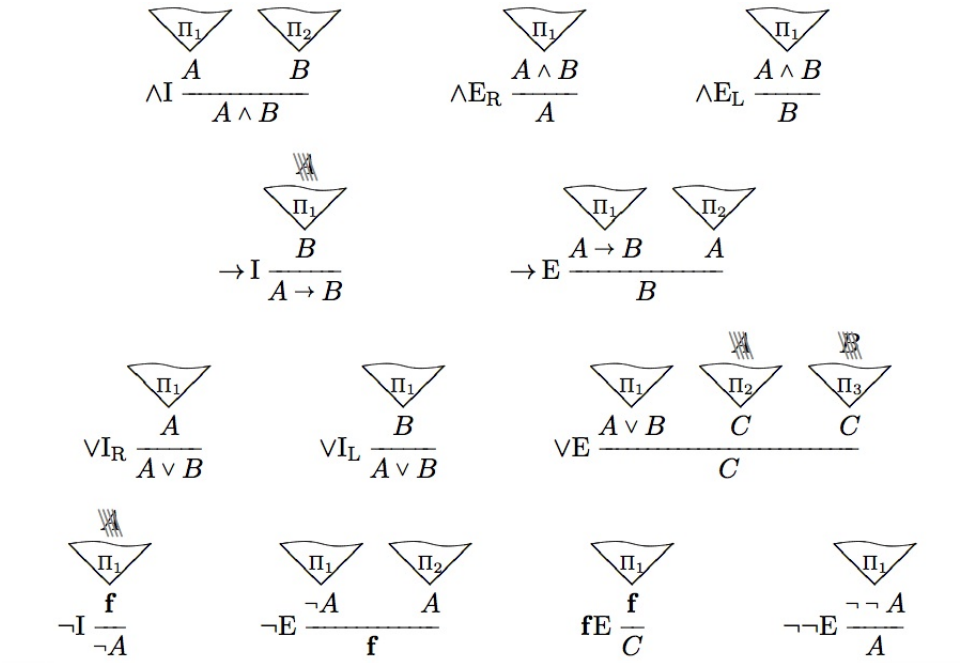


Tabella 2: Deduzione naturale classica.

16.3 Gentzen intuizionista

Vedi figura 3. x non deve comparire nella seconda regola del $\forall$ e nella prima del $\exists$.

17 Metateoria

Assiomatizzabilità Una teoria elementare T è assiomatizzata sse l'insieme dei suoi assiomi è decidibile (ad esempio quando è finito, in tal caso T è *finitamente assiomatizzata*.

Una teoria T è assiomatizzabile sse esiste una teoria elementare assiomatizzata ad essa equivalente[12].

Una teoria T è *finitamente assiomatizzabile* se esiste una teoria equivalente che sia finitamente assiomatizzata.

Coerenza Una teoria elementare T è contraddittoria sse esiste una fbf chiusa A del suo linguaggio tale che $T \vdash A$ e $T \vdash \neg A$.

Completezza sintattica Una teoria elementare T è sintatticamente completa sse, data una fbf chiusa A del suo linguaggio, o $T \vdash A$ o $T \vdash \neg A$[13].

[12] Due teorie sono equivalenti se hanno stesso linguaggio e stesso insieme di teoremi. Possono differire per gli assiomi.

[13] Ci aspetteremmo di saper decidere, data una teoria T e una formula A, se $T \vdash A$ o $T \vdash \neg A$. Ciò non è vero in generale. Infatti, per il primo teorema di incompletezza (sintattica)

(axioms)	$\dfrac{}{\Gamma, A \vdash A}$	$\dfrac{\Gamma, \top \vdash A}{\Gamma \vdash A} \quad \dfrac{}{\Gamma, \bot \vdash A}$
(and)	$\dfrac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}$	$\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$
(or)	$\dfrac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$	$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \quad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$
(implication)	$\dfrac{\Gamma \vdash A \quad \Gamma, B \vdash C}{\Gamma, A \to B \vdash C}$	$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}$
(univ. quant.)	$\dfrac{\Gamma, A[x := t] \vdash C}{\Gamma, \forall x.A \vdash C}$	$\dfrac{\Gamma \vdash A}{\Gamma \vdash \forall x.A}$
(exist. quant.)	$\dfrac{\Gamma, A \vdash C}{\Gamma, \exists x.A \vdash C}$	$\dfrac{\Gamma \vdash A[x := t]}{\Gamma \vdash \exists x.A}$

Tabella 3: Il calcolo dei sequenti intuizionista

Per il lemma di Lindembaum ogni teoria coerente ha un'estensione coerente e sintatticamente completa; tuttavia tale estensione può non essere assiomatizzata o assiomatizzabile.

Una teoria si dice *essenzialmente incompleta* sse ogni sua soprateoria coerente e assiomatizzabile è sintatticamente incompleta.

Nota:
Data una formula atomica A in logica proposizionale si ha che $\{\} \nvdash A$ e $\{\} \nvdash \neg A$. Tuttavia $\{A, B\} \vdash A$. L'aritmetica formalizzata al primo ordine è invece *essenzialmente* incompleta (primo teorema di incompletezza).

Decidibilità Una teoria è decidibile sse è decidibile l'insieme dei suoi teoremi.
Ogni teoria non assiomatizzabile è indecidibile.
Dal fatto che il teorema di Church vale già usando l'alfabeto dell'aritmetica di Robinson, si ha che l'aritmetica ricorsiva è indecidibile.
Una teoria indecidibile può avere estensioni che sono decidibili (ossia: non tutte le teorie indecidibili lo sono essenzialmente).
Ci sono teorie elementari decidibili: le teorie degli ordinamenti totali e densi, dell'identità, dell'aritmetica additiva, dei gruppi abeliani.

Teorema: se una teoria elementare coerente è assiomatizzata e sintatticamente completa allora è decidibile.

---

di Gödel: per una teoria T coerente e in grado di esprimere l'aritmetica ricorsiva, esiste una formula A tale che $T \nvdash A$ e $T \nvdash \neg A$.
Prendendo come T l'aritmetica di Robinson si mostra immediatamente che il calcolo del primo ordine è indecidibile (già limitandosi a un alfabeto limitato).

Completezza semantica Teorema: ogni teoria elementare è semanticamente completa, nel senso che ogni fbf chiusa A vera in tutti i modelli della teoria è teorema della teoria.

Compattezza Due formulazioni equivalenti (data teoria T e suo linguaggio L_T):

1. Una fbf chiusa A di L_T è conseguenza logica di T (degli assiomi di T) sse è già conseguenza logica di un insieme finito di assiomi di T[14].
2. Una teoria elementare ha modello sse ogni sua sottoteoria finitamente assiomatizzata ha modello.

Dal teorema di compattezza segue:

- Teorema: non esiste alcuna fbf chiusa A di $FOL_=$ valida sse il dominio è infinito.
- Teorema: non esiste alcun insieme X di fbf chiuse di $FOL_=$ valido sse il dominio è finito[15].

Categoricità Una teoria elementare è categorica se tutti i suoi modelli sono isomorfi.
Teorema: se una teoria elementare T ha un modello di dominio infinito, non è categorica[16]. Se non è presente l'identità, nessuna teoria elementare è categorica.

Incompletezza Per il primo teorema di incompletezza di Gödel, la teoria elementare N dell'aritmetica, se è coerente, è sintatticamente incompleta[17].
La proposizione di Gödel è vera nel modello standard ma non dimostrabile (né refutabile).
Il risultato sorprendente non è questo, ma il fatto che ogni soprateoria di teorie complete, se coerente e assiomatizzabile, è sintatticamente incompleta.
Si dimostra che, se sono coerenti, sistemi come N e l'aritmetica di Robinson sono indecidibili, e lo sono essenzialmente.
Ne segue il teorema di Church per FOL[18]. Date correttezza e completezza, segue che è indecidibile il problema della validità per formule FOL.
Se una teoria è sintatticamente completa, allora è decidibile (ma la conversa non vale in generale; la teoria vuota ad esempio è sintatticamente incompleta ma decidibile nel calcolo proposizionale).

Secondo ordine Teorema: non esiste un calcolo corretto per la logica del secondo ordine che sia completo.
Ne segue che al secondo ordine non vale il teorema di compattezza.
Ne segue che al secondo ordine non vale il teorema di Löwenheim-Skolem.

[14] Ossia sse è conseguenza logica di una teoria finitamente assiomatizzata di T.
[15] Anche se si può esprimere che il dominio contenga esattamente n elementi per n qualunque.
[16] Ciò segue dai teoremi di Löwenheim-Skolem.
[17] Il risultato vale già per l'aritmetica di Robinson.
[18] Se il calcolo fosse decidibile potremmo decidere se $\mathbf{AR} \vdash_{FOL} A$ decidendo $\vdash_{FOL} \mathbf{AR} \rightarrow A$, il che è impossibile per quanto detto prima.

Al secondo ordine è definibile l'identità, quindi tutte le teorie formulate al secondo ordine (come N^2) sono dotate di identità.

Teorema (Dedekind): N^2 è categorica.

Dato che N^2 è categorica, essa possiede una proprietà di completezza semantica: data una proposizione A, o A o $\neg A$ è vera nel modello standard[19], quindi è vera in tutti i modelli.

Tuttavia per N^2 vale il teorema di Gödel, per cui se è coerente allora è indecidibile e sintatticamente incompleta. Combinando la completezza semantica con l'incompletezza sintattica si ha una (ulteriore) prova dell'incompletezza dei calcoli per il secondo ordine.

Osservazioni Ha senso parlare di decidibilità per teorie elementari finitamente assiomatizzabili. L'aritmetica di Robinson **AR** è finitamente assiomatizzabile. Per essa vale il teorema di Gödel, quindi esiste una formula non dimostrabile né refutabile in **AR**. Quindi **AR** è indecidibile. **AR** è una teoria del primo ordine, quindi ne segue che a maggior ragione il calcolo del primo ordine è in generale indecidibile (sono decidibili suoi frammenti di alfabeto limitato, ad esempio l'aritmetica additiva).

Essendo il calcolo corretto e (semanticamente) completo, per ogni teoria elementare le formule valide in ogni modello sono dimostrabili.

[19] Che è l'unico modello, a meno di isomorfismi.