Politecnico di Milano
Scuola di Ingegneria dell'Informazione
Corso di Laurea Magistrale in Ingegneria Informatica


Logica e Algebra 2

# Logica e Algebra 2

Appunti

Docente:
Prof. Alessandra Cherubini

Appunti di di:
**Edoardo Pasi** Matricola n. 805753
**Davide Tateo** Matricola n. 799311

Anno Accademico 2013-2014

# Indice

# Introduzione

Se voi signorine finirete questo corso, e se sopravviverete, sarete dispensatori di fbf, pregherete per fare model checking di sistemi assurdi con automi di Büchi ancora più assurdi, utilizzerete il teorema di Gödel per sconfiggere la logica inconsistente di satana e di altri esseri malvagi, esprimerete concetti che non si possono esprimere nella logica del prim'ordine. Ma fino a quel giorno non siete altro che buoni a nulla convinti che tutti i cretesi sono stupidi e forse mentono, che i barbieri si radono da soli leggendo il catalogo di tutti cataloghi che non includono sé stessi, che $1 \neq 0.\overline{9}$ e $0.\overline{8} * 10 \neq 8.\overline{8}$, e perderete inutilmente ore della vostra vita a dimostrare l'ipotesi del continuo con gli assiomi di Zermelo - Fraenkel.
Lasciate il formaggio fuori dall'aula.

***Leprotto Bisestile:*** *Comincia dal principio!*
***Cappellaio Matto:*** *Sì! E quando arrivi alla fine, fermati!*

Lewis Carroll

# 1 La Logica Modale

## 1.1 Perché usare la la logica modale

La logica proposizionale è una logica corretta, completa e decidibile, ma è poco espressiva, tutte le formule sono formate da concetti atomici che possono essere o veri o falsi, e da connettivi logici (di cui solo due, in realtà, sono necessari).
La logica del prim'ordine invece è estremamente espressiva, non ci limitiamo solo a concetti atomici ma a predicati che possono essere veri o falsi rispetto a delle variabili che possiamo quantificare esistenzialmente e universalmente. Tuttavia la logica del prim'ordine non è decidibile, e quindi non può essere usata per molte applicazioni pratiche, che richiedono una risposta certa riguardo la validità di una determinata formula.
Tra le logiche proposizionali e quelle del prim'ordine, si trovano le logiche modali, che sono logiche più espressive delle logiche proposizionali, ma restano decidibile.
Per avere maggiore espressività basta aggiungere due nuovi simboli:

- l'operatore box "$\Box$" che verrà letto d'ora in poi come necessariamente
- l'operatore diamond "$\diamond$" che verrà letto d'ora in poi come possibilmente

## 1.2 Sintassi delle logiche modali

### Alfabeto

Le logiche modali sono definite sul seguente alfabeto:

- A, B lettere proposizionali , chiamiamo l'insieme delle lettere proposizionali $\phi$

- $\neg$, $\wedge$, $\vee$, $\implies$, $\iff$
- $\Box$, $\diamond$
- ), (

L'unica differenza rispetto alla logica modale sono i due connettivi modali box e diamond.

### Formule ben formate

Le formule ben formate sono:

- Le lettere enunciative
- se a è una formula ben formata lo sono anche $\neg a$, $\Box a$, $\diamond a$
- se a e b sono formule ben formate lo sono anche $a \vee b$, $a \wedge b$, $a \implies b$, $a \iff b$
- nient'altro è una formula ben formata

### Priorità dei connettivi

i connettivi hanno la seguente priorità:

1. $\neg$, $\Box$, $\diamond$
2. $\wedge$
3. $\vee$
4. $\implies$
5. $\iff$

Dove 1 è la priorità maggiore (viene applicato prima) e 5 è la priorità minore. I connettivi con stessa priorità vengono applicati nell'ordine in cui si trovano.
Le parentesi possono essere usate per cambiare le priorità.

### Sottoformule

Sia a una formula qualsiasi
sottoformule(a) è l'insieme così definito:

- Se $a \in \phi$ allora $sottoformule(a) \equiv \{a\}$
- Se a è una formula del tipo $\neg b$, $\Box b$, $\diamond b$ allora $sottoformule(a) \equiv \{a\} \cup sottoformule(b)$
- Se ha è una formula del tipo $a \vee b$, $a \wedge b$, $a \implies b$, $a \iff b$ allora $sottoformule(a) \equiv \{a\} \cup sottoformule(b) \cup sottoformule(c)$

Si può costruire un albero con radice la formula a e come rami le sue sottoformule dirette. questo albero si chiama albero di struttura della formula.

## 1.3 Semantica di Kripke

### 1.3.1 La semantica dei mondi possibili

La semantica di Kripke, detta anche dei mondi possibili, considera che le lettere proposizionali possono essere vere o false a seconda del mondo in cui vengono valutate. Questi mondi sono poi collegati l'un l'altro con una relazione di raggiungibilità.
abbiamo quindi:

- S insieme dei mondi possibili, detti anche stati
- $R \subseteq S \times S$ relazione di raggiungibilità tra gli stati
- $F = (S, R)$ frame, un grafo orientati che ha come nodi i mondi e come archi le possibili transizioni tra un mondo e l'altro, ossia tra due mondi c'è un arco se e solo se il secondo mondo è raggiungibile dal primo.
- $V : \phi \longrightarrow \mathcal{P}(S)$ funzione di valutazione, che ad ogni lettera proposizionale, associa gli stati in cui è vera
- $\mu = (S, R, V)$ modello, ossia un frame con una funzione di valutazione per le lettere proposizionali.

### 1.3.2 Semantica delle logiche modali:

Diciamo che $a$ è vera nel mondo $\alpha$ del modello $\mu$, e scriviamo $\mu \models_\alpha a$, se:

- $\mu \models_\alpha A \implies \alpha \in V(A)$ con $A \in \phi$
- $\mu \models_\alpha b \vee c \iff \mu \models_\alpha b \vee \mu \models_\alpha c$
- $\mu \models_\alpha b \wedge c \iff \mu \models_\alpha b \wedge \mu \models_\alpha c$
- $\mu \models_\alpha (b \implies c) \iff \mu \not\models_\alpha b \vee \mu \models_\alpha c$
- $\mu \models_\alpha (b \iff c) \iff (\mu \not\models_\alpha b \wedge \mu \not\models_\alpha c) \vee (\mu \models_\alpha c \wedge \mu \models_\alpha c)$
- $\mu \models_\alpha \Box b \iff \forall \beta \in S : (\alpha, \beta) \in R\, \mu \models_\beta b$
- $\mu \models_\alpha \Diamond b \iff \exists \beta \in S : (\alpha, \beta) \in R\, \mu \models_\beta b$

Diciamo che a è vera nel modello $\mu$ se a è vera in ogni mondo del modello $\mu$, e scriviamo:
$\mu \models a$
Diciamo che a è valida su un frame F se è vera in tutti i modelli costruibili sul frame F, e scriviamo:
$F \models a$
Chiamiamo funzione di valutazione associata al mondo $V_\alpha(A)$ che è definita così:
$V_\alpha(A) = 0 \iff \alpha \notin V(A)$
Tutte le formule che cominciano coi connettivi modali sono dette formule semi atomiche.
Le tautologie nella logica modale sono quelle formule che sono vere per tutte le interpretazioni delle formule atomiche e semi atomiche.

*—Ma io non voglio andare fra i matti—, osservò Alice.*
*—Bè, non hai altra scelta—, disse il Gatto —Qui siamo tutti matti. Io sono matto. Tu sei matta.—*
*—Come lo sai che sono matta?— Disse Alice.*
*—Per forza,— disse il Gatto: —altrimenti non saresti venuta qui.—*

Lewis Carroll

# 2

# Formule di Logica modale e significato

## 2.1 Formule Valide in ogni frame

Le seguenti formule sono valide in ogni frame F
$\Box\top$ con $\top \equiv a \vee \neg a$
infatti $\top$è valida in ogni modello di ogni frame F, banalmente è valida $\Box\top$
Vale inoltre il seguente assioma, detto assioma K:
$\Box(a \implies b) \implies (\Box a \implies \Box b)$
infatti:
Se $M \nvDash_\alpha \Box(a \implies b)$ la formula è vera
Se $M \models_\alpha \Box(a \implies b)$ allora:

- Se $M \nvDash_\alpha \Box a$ allora $M \models_\alpha \Box a \implies \Box b$ è vera e la formula iniziale è vera
- se $M \models_\alpha \Box a$ allora $\forall \beta : (\alpha, \beta) \in R \; M \models_\beta a \implies b$, $M \models_\beta a$, $M \models_\beta b$

Esistono relazioni che non solo valide in ogni frame:
$\Box a \implies \diamond a$
Non è valida in ogni frame, infatti $\Box a$ implica che in tutti gli stati raggiungibili (ma potrebbero anche non esserci stati) da $\alpha$, a è vera. Mentre $\diamond a$ implica che esiste almeno uno stato raggiungibile da $\alpha$ in cui a è vero.

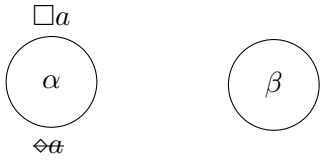
Tutte le tautologie sono valide in ogni frame

## 2.2 Relazione Seriale

Ip) Frame F con relazione R seriale
Ts) $\Box a \implies \diamond a$

Dimostrazione:
Se non vale: $\mu \models_\alpha \Box a$ allora immediatamente si ha la tesi in quanto l'antecedente è falso.
Se invece: $\mu \models_\alpha \Box a$ allora
$\forall \beta : \alpha R \beta \implies \mu \models_\beta a$ per definizione di box,
inoltre dato che R seriale per Ip si ha anche che $\exists \beta : (\alpha, \beta) \in R$
da cui: $\mu \models_\alpha \diamond a$ per definizione di diamond (esiste $\beta$ in relazione con $\alpha$ per la serialità e in $\alpha$ vale $a$ dato che $\mu \models_\alpha \Box a$ )

Ip) $\Box a \implies \diamond a$
Ts) Frame F con relazione R seriale

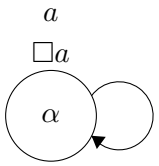



Per assurdo:
Suppongo di trovarmi in un mondo come quello in figura in cui $\mu \models_\alpha \Box a$ , e suppongo che la relazione R del frame NON sia seriale cioè $\not\exists \beta : (\alpha R \beta)$, se è così vale sicuramente $\mu \models_a \Box a$ (dato che $\alpha$ non ha successori) , d'altra parte per come è il mondo considerato, cioè si nega la tesi, assurdo.

## 2.3 Relazione Riflessiva

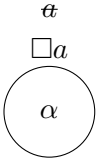
Ip) R riflessiva
Ts) $\Box a \implies a$

se l'antecedente è falso il teorema è dimostrato, consideriamo il caso in cui l'antecedente è vero:
$\mu \models_\alpha \Box a$
poiché il frame è riflessivo, abbiamo $\alpha R \alpha$, e quindi varrà:
$\mu \models_\alpha a$
e la tesi è dimostrata.



Ip) $\Box a \implies a$
Ts) R è riflessiva

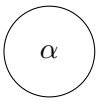
Supponiamo per assurdo che R non sia riflessiva, allora prendiamo uno stato $\alpha$ tale che $\nexists \beta : \alpha R \beta$. Allora si avrà che:
$\mu \models_\alpha \Box a \wedge \mu \not\models_\alpha a$
che è assurdo perché contraddice la tesi. La tesi allora è valida.



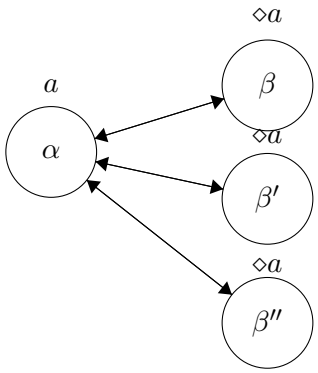

## 2.4 Relazione Simmetrica

Ip) R simmetrica
Ts) $a \implies \Box \diamond a$

Suppongo che $\mu \models_\alpha a$ (se no avrei già la tesi), due casi:
**Caso 1**: Da $\alpha$ non parte nessun arco, allora sicuramente $\mu \models_\alpha \Box x$ con $x$ qualsiasi e in particolare $\mu \models_\alpha \Box \diamond a$



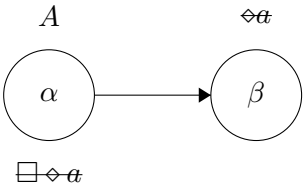

**Caso 2**: Esiste almeno un $\beta$ tale che $\alpha R \beta$.




Dato che la relazione è simmetrica se $\alpha R \beta$ allora $\beta R \alpha$**.** Dato che $\mu \models_\alpha a$, in ognuno di questi $\beta$, $\beta'$,$\beta''$ ecc. vale $\diamond a$ perché ognuno di loro è in relazione con $\alpha$.
Allora per ognuno di questi $\beta$ si ha $\mu \models_\beta \diamond a$, (esiste infatti un mondo, $\alpha$, in cui vale $a$) da cui: $\mu \models_\alpha \Box \diamond a$

Ip) $a \implies \Box \diamond a$
Ts) R simmetrica

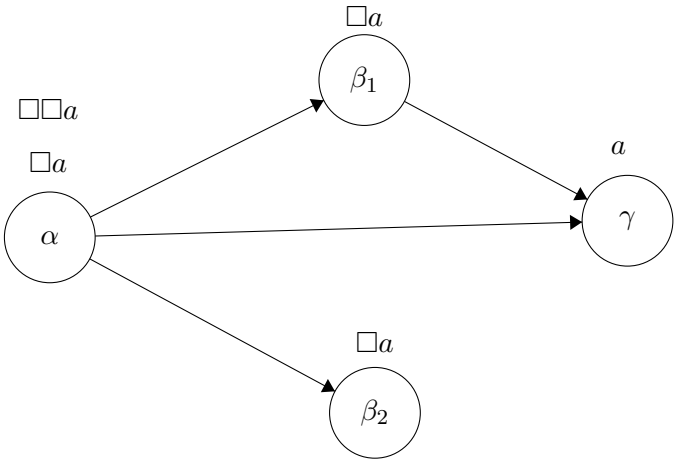
Per assurdo:
suppongo R non sia simmetrica e considero un frame con soli $\alpha$ e $\beta$ e in cui $R = \{(\alpha, \beta)\}$ . In questo frame considero un modello con funzione di verità tale che: $V(A) = \{\alpha\}$.
In $\beta$ non vale $\diamond a$ perché $\beta$ non è in relazione con nessun mondo, per questo: $\mu \nvDash_\alpha \Box \diamond a$




## 2.5 Relazione Transitiva

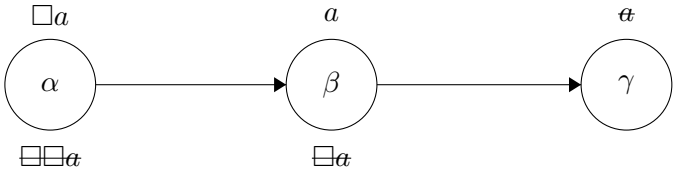
Ip) R relazione transitiva
Ts) $\Box a \implies \Box\Box a$

Se $\mu \nvDash_\alpha \Box a$ la tesi è dimostrata, consideriamo allora il caso in cui $\mu \models_\alpha \Box a$
per ipotesi:
$\exists \beta : (\alpha, \beta) \in R (\beta, \gamma) \in R$
allora abbiamo che:
$(\alpha, \gamma) \in R$
$\mu \models_\gamma a$
e quindi varrà ovviamente che:
$\mu \models_\beta a$
da cui segue:
$\mu \models_\alpha \Box\Box a$
e la tesi è dimostrata.



Ip) $\Box a \implies \Box\Box a$
Ts) R relazione transitiva

supponiamo per assurdo che esista uno stato$\alpha$ per cui non vale la proprietà transitiva consideriamo il caso in cui valga la seguente funzione di valutazione:
$V(a) = \{S \mid (\alpha, \delta) \in R\}$
Allora a sarà vera in $\beta$, ma non in $\gamma$. per cui in $\alpha$ sarà vera $\Box a$ ma non $\Box\Box a$




## 2.6 Funzione Parziale

| $\diamond a \implies \Box a$ | funzione parziale | $\forall \alpha : \alpha R\beta,\ \beta R\gamma \implies \beta = \gamma$ |
|---|---|---|

Funzione parziale, dimostrazione

Ip) funzione parziale
Ts) $\diamond a \implies \Box a$

$\diamond a$ falsa allora dato che l'antecedente è falso di ha $\diamond a \implies \Box a$
$\diamond a$ vera allora $\exists \beta$:$\alpha R\beta$ e$\in V(\beta)$, ma dato che la funzione è parziale questo $\beta$ è unico !
da cui $\mu \models \diamond a \implies \Box a$
Ip) $\diamond a \implies \Box a$
Ts) funzione parziale

Per assurdo: suppongo non che la funzione non sia parziale. Se è così $\exists \alpha : \alpha R\beta$, $\alpha R\gamma$, considero un modello in cui V(A) = $\{\beta\}$ , $\Box A$ non vale in $\alpha$ dato che A è falsa in $\gamma$, il che contraddice l'ipotesi (BAM!)

## 2.7 Funzione Totale

| $\diamond a \iff \Box a$ | funzione totale | $\forall \alpha \exists\, ! \, \beta : \alpha R\beta$ |
|---|---|---|

non ci sono "conti" da fare, R è seriale sse R è seriale $\Box a \implies \diamond a$ , e se R è una funzione parziale $\diamond a \implies \Box a$
quindi dato che l'implica prevede un and di implica da una parte e dall'altra per definizione abbiamo la tesi
.

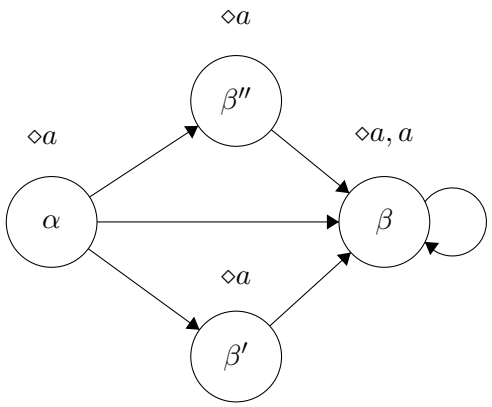
## 2.8 Relazione Euclidea

| $\diamond a \implies \Box \diamond a$ | relazione euclidea |
|---|---|

$\forall \alpha, \beta, \gamma : (\alpha R \beta,\ \alpha R \gamma) \implies \beta R \gamma$ da cui anche: $\beta \mathrm{R} \beta$, $\gamma R \gamma$, $\gamma \mathrm{R} \beta$

Ip) relazione euclidea
Ts) $\diamond a \implies \Box \diamond a$

Suppongo sia vero l'antecedente (se falso ho finito), quindi vale: $\diamond a$ da cui: $\mu \models \diamond a$
dato che $\diamond a$ si ha che esiste almeno un $\beta$ tale che in beta vale a
solo un beta: autoanello perché euclidea e quindi $\Box \diamond a$
diversi beta: ognuno dei vari $\beta'$, $\beta''$ , ecc. sono in relazione con $\beta$, dato che la relazione è euclidea, pertanto dato che in $\beta$ vale $a$, in ognuno di loro vale $\diamond a$




Ip)$\diamond a \implies \Box \diamond a$
Ts) relazione euclidea

Per assurdo, suppongo valga ip) ma non la tesi
Considero un Frame in cui: $\alpha R \beta$, $\alpha R \gamma$, $\beta R \gamma$ ma NON $\beta R \gamma$ cioè si ha un frammento in cui non vale l'euclidea. Poniamo che il modello sia tale che $V(A) = \{\gamma\}$
In queste ipotesi vale $\diamond a$ dato che in $\gamma$ vale $a$. In $\beta$ non vale $a$ e neppure $\diamond a$ perché non ha "uscite", da cui in $a$ non vale $\Box \diamond a$ contraddicendo così l'ipotesi (BAM!)

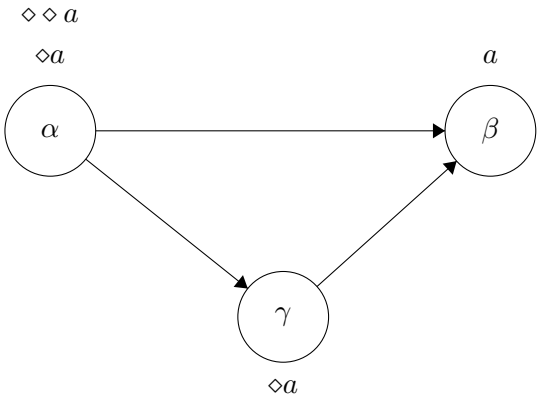
## 2.9 Relazione Debolmente Densa

| $\diamond a \implies \diamond \diamond a$ | relazione debolmente densa | $\forall \alpha, \beta : (\alpha R \beta) \implies \exists \gamma : (\alpha R \gamma \wedge \gamma R \beta)$ |
|---|---|---|

Ip) R debolmente densa
Ts) $\diamond a \implies \diamond \diamond a$

supponiamo che sia vero l'antecedente (se è falso la tesi è dimostrata) avremo quindi:

$\mu \models_\alpha \diamond a$
allora segue che:
$\exists \beta : \mu \models_\beta a$
ma poiché la relazione è debolmente densa, si avrà che:
$\exists \gamma : (\alpha R \gamma \wedge \gamma R \beta)$
poiché in $\beta$ è vera a, allora segue:
$\mu \models_\gamma \diamond a$
da cui segue:
$\mu \models_\alpha \diamond \diamond a$
e la tesi è dimostrata.




Ip) $\diamond a \implies \diamond \diamond a$
Ts) R debolmente densa

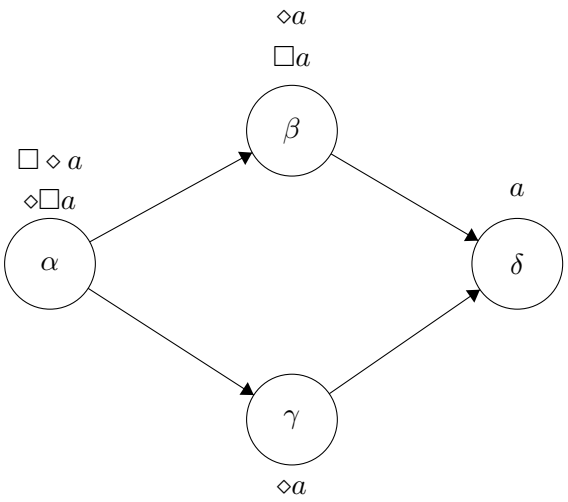
Supponiamo per assurdo che R non sia debolmente densa.
Supponiamo allora che esista uno stato $\beta$ pozzo e $\alpha R \beta$ in cui sia vera a
segue che:
$\mu \models_\alpha \diamond a$
ma avremo anche che:
$\mu \not\models_\beta \diamond a$
e allora otteniamo:
$\mu \not\models_\alpha \diamond \diamond a$
che è assurdo perché contraddice l'ipotesi, e quindi la tesi è dimostrata.


## 2.10 Relazione Diretta

| | | |
|---|---|---|
| $\diamond \Box a \implies \Box \diamond a$ | relazione diretta | $\forall \alpha, \beta, \gamma : (\alpha R \beta \wedge \alpha R \gamma) \implies \exists \delta : (\beta R \delta \wedge \gamma R \delta)$ |

Ip) R è diretta
Ts) $\diamond\Box a \implies \Box \diamond a$

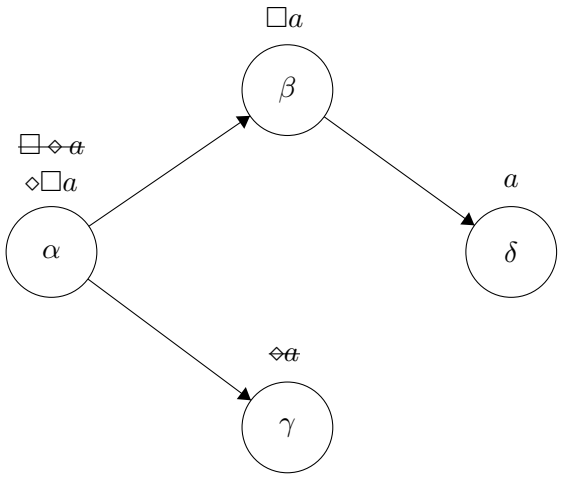
Se l'antecedente è falso, il teorema è dimostrato. poniamoci quindi nel caso:
$\mu \models_\alpha \diamond\Box a$
avremo allora che:
$\exists\beta : \alpha R\beta \wedge \mu \models_\beta \Box a$
allora necessariamente si avrà che:
$\exists\delta : \beta R\delta \wedge \mu \models_\delta a$
allora si avrà che:
$\mu \models_\beta \diamond a$
prendiamo ora un qualsiasi mondo$\gamma$ tale che $\alpha R\gamma$, poiché la relazione è diretta si avrà $\gamma R\delta$, e quindi:
$\mu \models_\gamma \diamond a$
e allora possiamo osservare che vale:
$\mu \models_\alpha \Box \diamond a$
e la tesi è dimostrata




Ip) $\diamond\Box a \implies \Box \diamond a$
Ts) R è diretta

Supponiamo per assurdo R non diretta.
Consideriamo la funzione di valutazione:
$V(a) = \{\delta | \beta R\delta\}$
supponiamo che:
$\exists\alpha : \alpha R\beta \wedge \mu \models_\alpha \diamond\Box a$
allora si avrà:
$\mu \models_\beta \Box a$
Prendiamo ora un qualsiasi mondo $\gamma$ tale che $\alpha R\gamma$, e supponiamo che:

$\nexists \eta : \gamma R \eta$
Si avrà dunque che
$\mu \not\models_\gamma \diamond a$
allora avremo che:
$\mu \not\models_\alpha \Box \diamond a$
che è assurdo, perché contraddice la tesi. La tesi è allora valida.



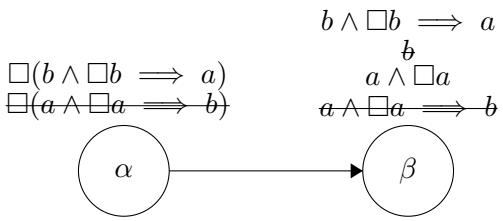

## 2.11 Relazione Debolmente Connessa

| $\Box(a \wedge \Box a \implies b) \vee \Box(b \wedge \Box b \implies a)$ | relazione debolmente connessa |
|---|---|

$\forall \alpha, \beta : (\alpha R \beta \wedge \alpha R \gamma) \implies (\beta R \gamma \vee \beta = \gamma \vee \gamma R \beta)$

Ip) R debolmente connessa
Ts) $\Box(a \wedge \Box a \implies b) \vee \Box(b \wedge \Box b \implies a)$

Se il primo termine è vero, il teorema è verificato. allora supponiamo che:
$\mu \not\models_\alpha \Box(a \wedge \Box a \implies b)$
ne consegue che:
$\mu \not\models_\beta a \wedge \Box a \implies b$
che si ha solo se valgono:
$\mu \not\models_\beta b$
$\mu \models_\beta a \wedge \Box a$
Dobbiamo allora verificare 3 casi:
**Caso 1**
se da $\alpha$ non esco in altri stati, poiché è falsa b, allora:
$\mu \models_\beta b \wedge \Box b \implies a$
da cui segue che:
$\mu \models_\alpha \Box(b \wedge \Box b \implies a)$
E la tesi è verificata.




**Caso 2**

Se da $\alpha$ vado in un altro mondo $\gamma$ raggiungibile da $\beta$:

$\mu \models_\gamma a$

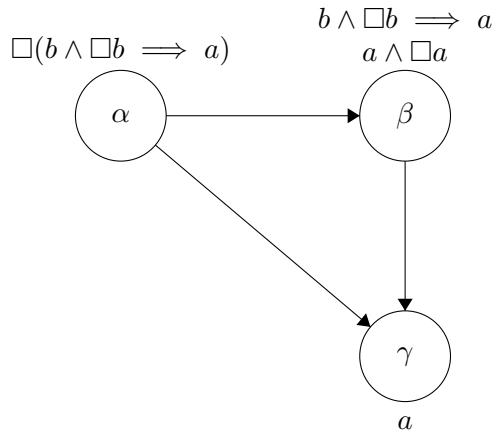
e quindi:

$\mu \models_\beta b \wedge \Box b \implies a$

da cui segue che:

$\mu \models_\alpha \Box(b \wedge \Box b \implies a)$

E la tesi è verificata.




**Caso 3**

Se da $\alpha$ vado in un altro mondo $\delta$ che raggiunge $\beta$:

$\mu \not\models_\delta \Box b$

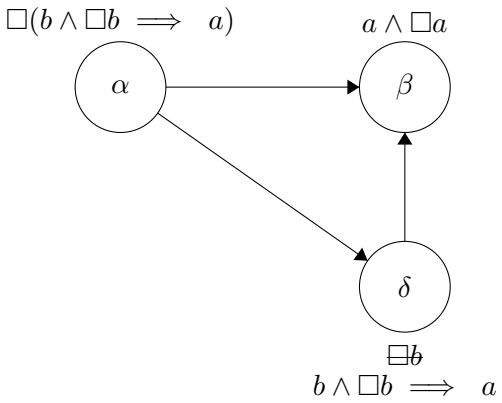
e quindi, poiché è falso l'antecedente, dovrà essere:

$\mu \models_\delta b \wedge \Box b \implies a$

da cui segue che:

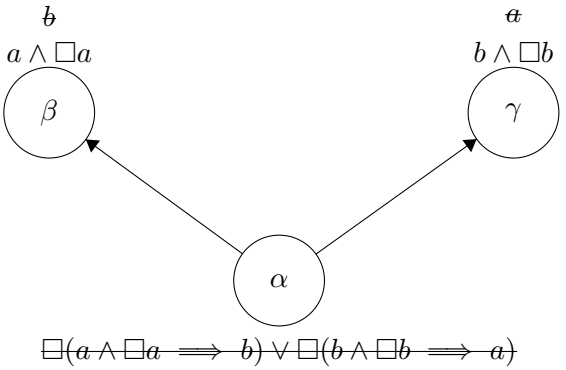
$\mu \models_\alpha \Box(b \wedge \Box b \implies a)$

E la tesi è verificata.




Ip) $\Box(a \wedge \Box a \implies b) \vee \Box(b \wedge \Box b \implies a)$
Ts) R debolmente connessa

Supponiamo per assurdo che R non sia debolmente connessa.
Consideriamo il caso in cui dallo stato $\alpha$ si raggiungano due stati $\beta$ e $\gamma$, tali che $\nexists \delta$ : $\beta R \delta \vee \gamma R \delta$. Supponiamo inoltre che:
$\mu \models_\beta a \wedge \neg b$
$\mu \models_\gamma b \wedge \neg a$
avremo allora:
$\mu \models_\beta a \wedge \Box a$
$\mu \models_\gamma b \wedge \Box b$
ma, poiché l'antecedente è vero e il conseguente no, avremo anche:
$\mu \not\models_\beta a \wedge \Box a \implies b$
$\mu \not\models_\gamma b \wedge \Box b \implies a$
allora:
$\mu \not\models_\alpha \Box(a \wedge \Box a \implies b) \vee \Box(b \wedge \Box b \implies a)$
che è assurdo, perché va contro l'ipotesi. La tesi allora deve essere valida.



# 3

# Assiomatizzazione delle logiche Modali

## 3.1 Formule equivalenti

$a \equiv b$ cioè a è semanticamente equivalente a b, se:

- $\forall F\, F \models b \iff F \models a$
- $\forall \mu\, \mu \models b \iff \mu \models a$
- $\forall s \in S\, \mu \models_s a \iff \mu \models_s b$

Si può anche dire che due formule sono semanticamente equivalenti se:
$a \models b \vee b \models a$
Oppure infine se è valida in ogni frame:
$\models a \iff b$

## 3.2 Insieme di connettivi minimi

Per ogni formula possiamo scriverne una equivalente che usa solo tre connettivi: $\neg$, $\Longrightarrow$ , $\Box$.
Infatti come è ben noto tutti i connettivi proposizionali si possono esprimere in funzione della negazione e dell'implicazione, mentre per quanto riguarda il connettivo diamond:
$\diamond a \equiv \neg\Box\neg a$
Infatti:
se $\mu \models_\alpha \diamond a$ allora
$\exists \beta : \alpha R \beta$ e $\mu \models_\beta a$ da cui:

$\mu \nvDash_\beta \neg a$
per questo in $\alpha$ non vale $\Box\neg a$ (perché non vale $\neg a$ in $\beta$)
allora in $\alpha$ vale $\neg\Box\neg a$ cioè $\mu \models_\alpha \neg\Box\neg a$ cioè la tesi.
Similmente si dimostra l'altro verso dell'equivalenza.

## 3.3 Logiche

### 3.3.1 Logica $\Lambda$

Una logica $\Lambda$ su L è un insieme di fbf su L che:

- contiene tutte le tautologie
- è chiusa rispetto al Modus Ponens

Ad esempio $PL(\phi)$ cioè i teoremi della logica proposizionale
Altro esempio $\Lambda_C = \{a \mid F \models a \; per \; ogni \; F \in C\}$
infatti:

- contiene tutte le tautologie perché sono vere mondo per mondo dappertutto
- MP : suppongo che in un mondo $\alpha$ accada che: $\mu \nvDash_\alpha b$ , $\mu \models_\alpha a$ . Se vale anche $\mu \models_\alpha a \implies b$ ... l'antecedente è vero, quindi dato che l'implicazione è vera, deve essere vero anche il conseguente da cui non può che essere $\mu \models_\alpha b$

Una logica si dice **uniforme** se è chiusa rispetto a sostituzioni uniformi cioè se sostituendo a una lettere uguali formule uguali in una tautologia, ottengo una tautologia.
Es. $\Lambda_C = \{a \mid F \models a \; per \; ogni \; F \in C\}$ NON è uniforme infatti se considero $V(A) = S$, dove S sono tutti gli stati possibili (mondi), vale anche $\mu \models_\alpha A$, e cioè A è una tautologia, se al posto di A sostituisco $B \wedge \neg B$ (falsa in ogni modello e mondo) non ottengo una tautologia.

### 3.3.2 Logiche modali normali

Le logiche normali sono logiche che contengono lo schema K
$K : \Box(a \implies b) \implies (\Box a \implies \Box b)$
E sono chiuse rispetto alla regola di necessitazione:
$RN : \dfrac{a}{\Box a}$
La logica normale ha i seguenti assiomi:
$A1 : a \implies (b \implies a)$
$A2 : (a \implies (b \implies c)) \implies ((a \implies b) \implies (a \implies c))$
$A3 : (\neg a \implies \neg b) \implies ((\neg a \implies b) \implies a)$
$K : \Box(a \implies b) \implies (\Box a \implies \Box b)$
$MP : \dfrac{a,\; a \implies b}{b}$
$RN : \dfrac{a}{\Box a}$

L'intersezione di tutte le logiche normali, è una logica normale (ed è la minima ) che non ha altri assiomi.
I teoremi sono le ultime formule della dimostrazione, ossia le formule che ottengo dopo un numero finito di applicazione degli assiomi oppure utilizzando la regola di necessitazione o il modus ponens.
La minima logica normale viene chiamata logica K.

### 3.3.3 Teorema

Sono equivalenti:

1. $\Lambda$ è normale
2. per ogni intero n $\geq 0$,
   $\vdash_\Lambda a1 \wedge a2 \wedge ... \wedge an \implies a$ implica $\vdash_\Lambda \Box a1 \wedge \Box a2 \wedge ... \wedge \Box an \implies \Box a$
3. valgono:
   (a) $\vdash_\Lambda \Box T$
   (b) $\vdash_\Lambda \Box a \wedge \Box b \implies \Box(a \wedge b)$
   (c) $\vdash_\Lambda a \implies b$ implica $\vdash_\Lambda \Box a \implies \Box b$

Dimostrazione
$1 \implies 2$
per induzione.
se n = 0 allora $\vdash_\Lambda a$ allora $\vdash_\Lambda \Box a$ per la regola RN che vale in $\Lambda$ per ipotesi
se n > 0 (passo induttivo) suppongo valga l'antecedente, altrimenti 2 vale senz'altro;
si può dimostrare quindi nel seguente modo:
$\vdash_\Lambda a_1 \wedge a_2 \wedge ... \wedge a_n n \implies a$
$\vdash_\Lambda a_1 \wedge a_2 \wedge ... \wedge a_{n-1} \implies (a_n \implies a)$
$\vdash_\Lambda \Box a_1 \wedge \Box a_2 \wedge ... \wedge \Box a_{n-1} \implies \Box(a_n \implies a)$ – per ipotesi di induzione
$\vdash_\Lambda \Box a_1 \wedge \Box a_2 \wedge ... \wedge \Box a_{n-1} \implies (\Box a_n \implies \Box a)$ – per K
$\vdash_\Lambda \Box a_1 \wedge \Box a_2 \wedge ... \wedge \Box a_{n-1} \wedge \Box a_n \implies \Box a$
E la tesi è dimostrata.
$2 \implies 1$
$\vdash_\Lambda (a \wedge (a \implies b)) \implies b$ – per MP
$\vdash_\Lambda (\Box a \wedge \Box(a \implies b)) \implies \Box b$ – per enunciato 2
$\vdash_\Lambda \Box(a \implies b) \implies \Box a \implies \Box b$ – che è K
Abbiamo ricavato usando solo il modus ponens e l'enunciato 2, l'assioma K. segue quindi la tesi.
$1 \implies 3$
$\vdash_\Lambda \top$
$\vdash_\Lambda \Box\top$– per RN
$\vdash_\Lambda a \wedge b \implies a \wedge b$ – per tautologia $(a \implies a)$

$\vdash_\Lambda \Box a \wedge \Box b \implies \Box(a \wedge b)$ – per proposizione 2
$\vdash_\Lambda a \implies b$ – per ipotesi
$\vdash_\Lambda \Box(a \implies b)$ – per RN
$\vdash_\Lambda \Box(a \implies b) \implies (\Box a \implies \Box b)$ – per K
$\vdash_\Lambda \Box a \implies \Box b$ – per MP
La tesi allora è verificata.
$3 \implies 1$
dimostriamo due tesi: che la 3 è chiusa rispetto alla necessitazione e che implica l'assioma K.
$\vdash_\Lambda a$
$\vdash_\Lambda a \implies (\top \implies a)$ – per A1
$\vdash_\Lambda \top \implies a$ – per MP
$\vdash_\Lambda \Box\top \implies \Box a$ – per 3.c
$\vdash_\Lambda \Box a$ – per 3.a e MP
abbiamo così dimostrato la chiusura secondo la necessitazione.
$\vdash_\Lambda a \wedge b \implies c$
$\vdash_\Lambda \Box(a \wedge b) \implies \Box c$ – per 3.c
$\vdash_\Lambda \Box a \wedge \Box b \implies \Box(a \wedge b)$ – per 3.b
$\vdash_\Lambda \Box a \wedge \Box b \implies \Box c$ – per la combinazione delle due implicazioni precedenti
$\vdash_\Lambda a \wedge (a \implies b) \implies b$ – per tautologia
$\vdash_\Lambda \Box a \wedge \Box(a \implies b) \implies \Box b$ – per applicazione dello schema $\Box a \wedge \Box b \implies \Box c$ dimostrato precedentemente
$\vdash_\Lambda \Box(a \implies b) \implies (\Box a \implies \Box b)$
e così è dimostrato che K è implicato da 3. Il teorema dunque è dimostrato.

## 3.4 Decidibilità di una formula

Una formula a si dice deducibile da un insieme di formule $\Gamma$ in una logica $\Lambda$ e si scrive:
$\Gamma \vdash_\Lambda a$
se e solo se:
$\vdash_\Lambda a_1 \wedge \ldots \wedge a_n \implies a$
con $a_1, \ldots, a_n \in \Gamma$
Cioè, una formula a si dice deducibile da un insieme di formule $\Gamma$ se e solo se la congiunzione di formule che formano $\Gamma$ implica la formula a
si noti che:
$\Gamma \vdash_\Lambda a \implies \{\Box b \,|\, b \in \Gamma\} \vdash_\Lambda \Box a$

*Senza dubbio questo era un piano eccellente, semplice e davvero ben congegnato. C'era solo una difficoltà: che Alice non aveva la più piccola idea di come realizzarlo.*

Lewis Carroll

# 4

# Verso la decidibilità - Logica determinata

## 4.1 Insieme $\Lambda$ consistente e sue proprietà

Sia $\Lambda$ una logica (cioè ha tutte le tautologie ed è chiusa rispetto al Modus Ponens)
$\Gamma$ si dice $\Lambda$-consistente se: $\Gamma \nvdash_\Lambda \bot$, dove $\bot = A \wedge \neg A$
$\Delta$ si dice $\Lambda$-consistente massimale se per ogni fbf $a$ $a \in \Delta$ oppure $\neg a \in \Delta$

**Proprietà:**

1. Se $\Gamma \vdash_\Lambda a$ e $\Gamma \subseteq \Delta$ allora $\Delta \vdash_\Lambda a$. Ovvero se alcune premesse non mi servono posso comunque metterle per dedurre una formula

2. Se $\Gamma \vdash_\Lambda a$ e $\Lambda \subseteq \Lambda'$ allora $\Gamma \vdash_{\Lambda'} a$. Ovvero quello che posso dedurre in una logica più scarna (es. PL) lo posso dedurre anche in una più ricca che la contiene (es. Modale)

3. se $a \in \Gamma$ allora $\Gamma \vdash_\Lambda a$ .
   Infatti $\vdash_\Lambda a \implies a$ è un teorema dato che $a \implies a$ è una tautologia

4. $\{a | \Gamma \vdash_\Lambda a\}$ è la minima logica che contiene $\Gamma \cup \Lambda$. Infatti posso dedurre tutte le tautologie da $\Gamma$, anche se non userò nessuna formula di $\Gamma$ ma solo quelle che già sono nella logica $\Lambda$

5. Se $\Gamma \vdash_\Lambda a$ e $\{a\} \vdash_\Lambda b$ allora $\Gamma \vdash_\Lambda b$
   Infatti: per dedurre $a$ uso regole di inferenza, formule di $\Gamma$, assiomi di $\Lambda$. Per arrivare in $b$ uso assiomi di $\Lambda$ e regole di inferenza, quindi posso arrivare da $\Gamma$ direttamente in $b$ usando formule di $\Gamma$, regole di inf. e assiomi di $\Lambda$

6. Se $\Gamma \vdash_\Lambda a$ e $\Gamma \vdash_\Lambda a \implies b$ allora $\Gamma \vdash_\Lambda b$, dato che $\Lambda$ è chiusa rispetto al MP

7. $\Gamma \cup \{a\} \vdash_\Lambda b$ se e solo se $\Gamma \vdash_\Lambda a \implies b$
   **Andata**: $\vdash_\Lambda a_1 \wedge ... \wedge a \wedge ... \wedge a_n \implies b$ (per definizione di teorema), si può portare $a$ alla destra dell'implicazione $\vdash_\Lambda a_1 \wedge ... \wedge a_n \implies (a \implies b)$
   **Ritorno**: $\vdash_\Lambda a_1 \wedge ... \wedge a_n \implies (a \implies b)$, basta portare $a$ tra le and.

8. $\Gamma \vdash_\Lambda a$ se e solo se $\Gamma \cup \{\neg a\}$ non è $\Lambda$-consistente

   **Andata**: $\Gamma \vdash_\Lambda a$, $\Gamma \vdash_\Lambda \neg a$, posso dedurre $\perp$ che è contro la definizione di $\Lambda$-consistenza
   **Ritorno**: Se$\Gamma \cup \{\neg a\}$ non è $\Lambda$-consistente, allora $\Gamma \cup \{\neg a\} \vdash_\Lambda \perp$ da cui per 7.
   $\Gamma \vdash_\Lambda \neg a \implies \perp$ (sposto $\neg a$ a destra e metto l'implica),
   Dato che $(\neg a \implies \perp) \implies a$ è una tautologia, per MP ottengo
   $a$

9. $\Gamma$ è $\Lambda - consistente$ se e solo se $\exists \beta : \Gamma \nvdash_\Lambda \beta$
   **Andata**: Basta prendere $\neg a \wedge a$
   **Ritorno**: Se deducessi tutte le formule ($\neg \exists \beta : \Gamma \nvdash_\Lambda \beta$ significa $\forall \beta : \Gamma \vdash_\Lambda \beta$) , potrei dedurre anche $\perp$, da cui la non consistenza

10. $\Gamma$ è $\Lambda - consistente$ se per ogni $a$
    $\Gamma \cup \{a\}$ o $\Gamma \cup \{\neg a\}$ è $\Lambda - consistente$
    se $\Gamma \vdash_\Lambda a$ allora $\Gamma \cup \{\neg a\}$ non è consistente perché con $a$ e $\neg a$ posso dedurre $\perp$, ma $\Gamma \cup \{a\}$ lo è
    se $\Gamma \vdash_\Lambda \neg a$ allora $\Gamma \cup \{\neg a\}$ è consistente ma non $\Gamma \cup \{a\}$

11. $\perp \notin \Gamma$ se $\Gamma$ è $\Lambda - consistente$ (altrimenti potrei dedurlo per il 3.)

12. Se $\Delta$è $\Lambda - consistente\, massimale$ e $\Delta \vdash_\Lambda a$ allora $a \in \Delta$
    se $a \notin \Delta$ allora $\neg a \in \Delta$ (dato che $\Delta$è massimale)
    ma se $\Delta$ contiene $\neg a$ allora per il 2.)
    $\Delta \vdash_\Lambda \neg a$ , che insieme a $\Delta \vdash_\Lambda a$ mi da $\Delta \vdash_\Lambda \perp$

13. Se $\Delta$ è $\Lambda - consistente\, massimale$ e $a \in \Delta$. $a \implies b \in \Delta$ allora $b \in \Delta$.
    Lo si vede subito usando 2.) se tutti e tre, e poi 6.) (deduco $a$, $a \implies b$, allora deduco anche $b$)

## 4.2 Insieme $\Lambda$ consistente massimale

### 4.2.1 Lemma di Lindenbaum

Una logica consistente ammette sempre un insieme $\Lambda$- consistente massimale. Infatti il lemma di Lindenbaum afferma:
$(\Gamma\, \Lambda - consistente) \implies \exists \Delta \supseteq \Gamma \wedge (\Delta\, \Lambda - consistente\, massimale)$
Ip) $\Gamma$ è $\Lambda - consistente$

Ts) $\exists \Delta \supseteq \Gamma$ e $\Delta$ è $\Lambda -$ *consistente massimale*

Considero tutte le formule b1, b2, b3 della logica $\Lambda$ (posso farlo perché sono una infinità numerabile)
Chiamo $\Gamma_0$ un insieme che contiene una sola formula (ad esempio una tautologia)
Dopodiché iterativamente, per ogni formula mi chiedo

$$\Gamma_0 \vdash_\Lambda b1 \ ? \begin{cases} si: & \Gamma_1 = \Gamma_0 \cup b1 \\ no: & \Gamma_1 = \Gamma_0 \cup \neg b1 \end{cases}$$

$$\Gamma_1 \vdash_\Lambda b2 \ ? \begin{cases} si: & \Gamma_2 = \Gamma_1 \cup b2 \\ no: & \Gamma_2 = \Gamma_1 \cup \neg b2 \end{cases}$$

$\Delta = \bigcup_{n \geq 0} \Gamma$ (nota, questa unione è infinita)

$\Delta$ è consistente massimale infatti:

1. Massimale in quanto contiene $a$ oppure $\neg a$ per costruzione

2. Consistente. Per assurdo se non lo fosse avrei: $\Delta \vdash_\Lambda \bot$
   cioè esiste un numero finito di formule di $\Delta$ da cui deduco il falso,
   dato che è un numero finito di formule, sta in $\Gamma_i$ , cioè esiste un $\Gamma_i$ non consistente,
   assurdo perché lo sono tutti per costruzione $\lightning$

*Nota:*

- Non sappiamo costruire $\Delta$ perché nasce da unione infinita

- Non è unico, infatti se considero formule in ordine diverse potrei "dire" si o no in modo diverso
  es. $a,\ a \implies b,\ b$ (allora $\Delta$ contiene $b$)
  es. $b,\ c$ (allora $\Delta$ contiene $\neg b$)

### 4.2.2 Teorema

$\Gamma \vdash_\Lambda a$ se e solo se $a \in$ a tutti i quei $\Delta$ $\Lambda -$ *consistenti massimali* tali che: $\Gamma \subseteq \Delta$

**Andata:**
$\Gamma \vdash_\Lambda a$, anche $\Delta \vdash_\Lambda a$ per la 1.)
**Ritorno:**
Per assurdo, se $\Gamma \nvdash_\Lambda a$ allora $\Gamma \cup \{\neg a\}$ è $\Lambda -$ *consistente* (per la 8.)
da cui per Lindellman esiste $\Delta'$ che contiene $\Gamma \cup \{\neg a\}$ consistente massimale
data la consistenza $\Delta'$ non contiene $a$, il che è contro l'ipotesi $\lightning$

## 4.3 Lemma di Verità

Sia $M^\Lambda(S^\Lambda, R^\Lambda, V^\Lambda)$ il modello canonico di $\Lambda$
$M^\Lambda \models_\alpha a$ se e solo se $a \in \alpha$

Ip) $M^\Lambda \models_\alpha a$
TS) $a \in \alpha$

Dimostrazione per **induzione** sul numero n dei connettivi della formula $a$
n=0 cioè $a$ è del tipo $A$ (lettera enunciativa) da cui $M^\Lambda \models_\alpha a$ se e solo se $\alpha \in V^\Lambda(A)$ se e solo se $A \in \alpha$
Ipotesi di Induzione $a$ con n connettivi, può essere dei seguenti tipi:

1. $\neg b$
2. $b \implies c$
3. $\Box b$

**Caso 1:** $M^\Lambda \models_\alpha a$ se e solo se $M^\Lambda \models_\alpha \neg b$ se e solo se $M^\Lambda \nvDash_\alpha b$

$b$ ha $n-1$ connettivi (dato che $b$) ne ha $n$, quindi vale l'ipotesi di induzione da cui:
$b \notin \alpha$, d'altra parte $\alpha$ è $\Lambda - consistente\ massimale$ (per come è definito $S^\Lambda$) da cui:
$b \notin \alpha$ se e solo se $\neg b \in \alpha$ cioè se:
$a \in \alpha$
**Caso** 2: $M^\Lambda \models_\alpha a$ se e solo se
Caso 21: $M^\Lambda \nvDash_\alpha b$
Caso 22: $\models c$

**Caso 21**: $M^\Lambda \nvDash_\alpha b$

Il numero di connettivi di $b$ e di $c$ sommati dà $n-1$
quindi per ipotesi induttiva $M^\Lambda \nvDash_\alpha b$ se e solo se $b \notin \alpha$
se e solo se $\neg b \in \alpha$ (per la compattezza max di $\Lambda$) **(*)**
D'altra parte $\neg b \implies (b \implies c)$ è una tautologia della PL e quindi è un teorema di $\Lambda$ (perché un logica contiene tutte le tautologie)
e quindi $\neg b \implies (b \implies c) \in \alpha$ **(**)**
da cui per MP con **(*)** e **(**)** si ha che $b \implies c$ appartiene ad $\alpha$

**Caso 22**: $M^\Lambda \models_\alpha c$

Vale l'ipotesi di induzione da cui:
quindi per ipotesi induttiva $\models c$ se e solo se $c \in \alpha$ **(*)**
D'altra parte $c \implies (b \implies c)$ è una tautologia della PL e quindi è un teorema di $\Lambda$ (perché un logica contiene tutte le tautologie)

e quindi $c \implies (b \implies c) \in \alpha$ **(**)**
MP **(*)** e **(**)** ci dà $b \implies c$ appartiene ad $\alpha$

**Caso 3**: $a$ è del tipo $\Box b$

Ip)$M^\Lambda \models_\alpha \Box b$
Ts)$\Box b \in \alpha$

Dall'ipotesi segue che $\forall \beta : (\alpha, \beta) \in R^\Lambda$ si ha: $M^\Lambda \models_\beta b$ (questo per la definizione di $\Box x$)
$b$ ha $n-1$ connettivi quindi vale per lei l'ipotesi di induzione:
$b \in \beta$

$(\alpha, \beta) \in R^\Lambda$ se e solo se: $\{a \mid \Box a \in \alpha\} \subseteq \beta$
$\alpha \in V^\Lambda(A)$ se e solo se: $A \in \alpha$

Ognuno dei $\beta$ con cui $\alpha$ è in relazione è $\Lambda -$ *consistente massimale* (per come sono definiti gli stati del modello canonico) e ognuno contiene l'insieme $\{a \mid \Box a \in \alpha\}$ (per come è definita la relazione $R^\Lambda$)
$\Gamma \vdash_\Lambda a$ se e solo se $a$ appartiene a tutti i $\Delta_i$ $\Lambda -$ *consistente massimale* con $\Gamma \subseteq \Delta_i$
$\beta \vdash_\Lambda b$ se e solo se $b$ appartiene a tutti i $\Delta_i$ $\Lambda -$ *consistente massimale* con $\beta \subseteq \Delta_i$
$\{a \mid \Box a \in \alpha\}$ è consistente massimale ed è contenuto in $\beta$ e quindi
$b \in \{a \mid \Box a \in \alpha\}$ da cui per la proprietà 3. di insieme consistente si ha anche
$\{a \mid \Box a \in \alpha\} \vdash_\Lambda b$, inoltre, per la 2. definizione equivalente di Logica Normale "aggiungo $\Box$ ad entrambi i lati" da cui:
$\{\Box a \mid \Box a \in \alpha\} \vdash_\Lambda \Box b$, dato che $\{\Box a \mid \Box a \in \alpha\}$ è consistente massimale. per la 12. delle proprietà di consistenza si ha anche
$\Box b \in \{a \mid \Box a \in \alpha\}$ da cui, a maggior ragione $\Box b \in \alpha$

Ip) $\Box b \in \alpha$
TS) $M^\Lambda \models_\alpha \Box b$

Se $\Box b \in \alpha$ per definizione di $R^\Lambda$ per ogni mondo $\beta$ con $(\alpha, \beta) \in R^\Lambda$ si ha $b \in \beta$
Notiamo che $b$ ha $n-1$ connettivi, quindi vale l'ipotesi di induzione e quindi:
$b \in \beta$ se e solo se $M^\Lambda \models_\beta b$
Dato che questo vale per ogni $\beta$ in relazione con $\alpha$, si ha: $M^\Lambda \models \beta \Box b$

## 4.4 Correttezza e completezza della logica K rispetto a tutti i Frame

Dimostriamo che la logica K (minima logica modale normale) è corretta e completa
Ip) $\vdash_K a$
Ts)$F \models a$

A1, A2, A3 sono tautologie e quindi valide su tutti i frame
MP, sia la regola di necessitazione (RN) fanno passare da formule valide su un frame a formule valide su quello stesso frame.
Essendo $a$ l'ultima formula di una sequenza finita di fbf che o sono istanze degli assiomi A1, A2, A3, K o sono ottenute da fbf precedenti tramite MP o RN, è una fbf valida su ogni frame.

Ip) $F \models a$
Ts)$\vdash_K a$

Supponiamo $\nvdash_K a$, allora per il corollario del lemma di verità

Per ogni formula $a$, sia $\Lambda$ una logica, si ha $M^\Lambda \models a$ se e solo se $\vdash_\Lambda a$, dove $M^\Lambda$ è il modello canonico

Si avrebbe: $M^K \not\models a$ da cui anche
$F^K \not\models a$, cioè $a$ non valida sul frame su cui $M^K$ è costruito quindi:
$F \not\models a$ (infatti esiste almeno un frame, $F^K$, in cui non è valida $a$) il che però è contro l'ipotesi $\lightning$.

## 4.5 Correttezza e completezza della logica K4 rispetto ai Frame transitivi

Nota: K4 è costruita a partire dalla logica K a cui si aggiunge l'assioma della transitività
$\Box a \implies \Box\Box a$
Ip)$\vdash_{K4} a$
Ts) $F \models a$ con F frame transitivo

Simile al caso precedente in cui anche 4 è valido in quando il frame è transitivo

Ip) $F \models a$ con F frame transitivo (cioè la cui relazione è transitiva)
Ts)$\vdash_{K4} a$

Per procedere con una dimostrazione sulla falsa riga della precedente abbiamo bisogno di dimostrare la transitività di $R^{K4}$
cioè della relazione $R^{K4}$ del modello canonico $M^{K4} = (S^{K4}, R^{K4}, V^{K4})$, servirà ragionando per assurdo.

**Transitività di $R^{K4}$**
se $(\alpha, \beta) \in R^{K4}$, $(\beta, \gamma) \in R^{K4}$ allora $(\alpha, \gamma) \in R^{K4}$
cioè deve avvenire che: $\{a \mid \Box a \in \alpha\} \subseteq \gamma$ (definizione di essere in relazione $\alpha R^{K4} \gamma$ del modello canonico)
se $\Box a \in \alpha$ , ricordando che:

$\alpha$ è un insieme $K4 - \textit{consistente massimale}$,
4 è un teorema della logica
i teoremi di una logica appartengono a tutti gli insiemi consistenti massimali rispetto a quella logica quindi
$\alpha$, così come ogni insieme $K4 - \textit{consistente massimale}$, contiene anche $\Box a \implies \Box\Box a$ (4) da cui
$\Box\Box a \in \alpha$.
$\{a \mid \Box a \in \alpha\} \subseteq \beta$ (per ipotesi $\alpha R^{K4} \beta$)
ma per ogni formula $\Box a \in \alpha$ si ha che $\Box\Box a \in \alpha$ e quindi: $\{\Box a \mid \Box\Box a \in \alpha\} \subseteq \beta$ da cui $\{\Box a \mid \Box a \in \alpha\} \subseteq \beta$
$\{a \mid \Box a \in \beta\} \subseteq \gamma$ (per ipotesi $\beta R^{K4} \gamma$), ma le formule del tipo $\Box a$ contenute in $\beta$ sono le stesse contenute in $\alpha$, quindi si ha anche:
$\{a \mid \Box a \in \alpha\} \subseteq \gamma$ cioè $(\alpha, \gamma) \in R^{K4}$

A questo punto possiamo usare in modo proficuo il corollario del lemma di verità.
Dimostriamo la tesi per assurdo: supponiamo che $\nvdash_{K4} a$
allora per il corollario del teorema di verità si avrebbe anche $M^{K4} \not\models a$
e in particolare si avrebbe $F^{K4} \not\models a$, cioè si avrebbe un Frame transitivo (infatti $R^{K4}$ è transitiva) nel quale non è valida $a$
ma ciò contraddice l'ipotesi $F \models a$ (con $F$ transitivo) $\lightning$

## 4.6 Teorema di Raggiungibilità

$(\alpha, \beta) \in R^{\Lambda}$ se e solo se $\{a \mid \Box a \in \alpha\} \subseteq \beta$ se e solo se $\{\diamond b \mid b \in \beta\} \subseteq \alpha$
Ip)$\{a \mid \Box a \in \alpha\} \subseteq \beta$
Ts)$\{\diamond b \mid b \in \beta\} \subseteq \alpha$

**Per** assurdo supponiamo che

$b \in \beta$ e che $\diamond b \notin \alpha$,
$\neg \diamond b \in \alpha$ (dato che $\alpha$) è $\Lambda - \textit{consistente massimale}$
$\Box \neg b \in \alpha$ (equivalenza $\Box \neg a \equiv \neg \diamond a$) da cui
$\neg b \in \beta$ (definizione di $\Box x$ e considerato $\alpha R^{\Lambda} \beta$)
il che è assurdo perché $b \in \beta$, e $\beta$ è $\Lambda - \textit{consistente massimale}$ $\lightning$

Ip)$\{\diamond b \mid b \in \beta\} \subseteq \alpha$
Ts)$\{a \mid \Box a \in \alpha\} \subseteq \beta$
Per assurdo supponiamo cioè che
$\Box a \in \alpha$ e $a \notin \beta$
$\neg a \in \beta$ (dato che $\beta$ è $\Lambda - \textit{consistente massimale}$)
$\diamond \neg a \in \alpha$ (infatti $\alpha R^{\Lambda} \beta$ e in $\beta$ è vera $\neg a$, quindi $a$ ha almeno un successore nel quale $\neg a$ è vera)

$\neg\Box a \in \alpha$ contro l'ipotesi della consistenza e massimalità di $\alpha$↯

*Se io avessi un mondo come piace a me, là tutto sarebbe assurdo: niente sarebbe com'è, perché tutto sarebbe come non è, e viceversa! Ciò che è, non sarebbe e ciò che non è, sarebbe!*

Lewis Carroll

# 5 Logiche modali particolari e Determinatezza

Per il teorema di correttezza e completezza abbiamo che $\vdash_\Lambda a$ se e solo se $M^\Lambda \models a$
Il problema di $M^\Lambda \models a$ è che non so costruire a livello "pratico" il modello canonico dato che i suoi mondi sono infiniti.
Provo quindi a vedere se $\vdash_\Lambda a$ se e solo se $F^\Lambda \models a$ possa valere almeno per particolari classi di frame.

**Nota:** Per dimostrare la determinatezza di una logica rispetto a una classe di frame con una proprietà si può mostrare che la relazione del Frame canonico costruito da quella logica gode della stessa proprietà.
Con questa chiave di lettura diamo alcune dimostrazioni di determinatezza.

## 5.1 Serialità del frame canonico di KD

$R^{KD}$ è seriale se: $\forall \alpha \in S^{KD} \exists \beta : (\alpha, \beta) \in R^{KD}$
TS) $\vdash_{KD} a$ se e solo se $R^{KD}$ è seriale
$\{a \mid \Box a \in \alpha\} \subseteq \beta$ se e solo se $\alpha$ e $\beta$ sono in relazione.
Vogliamo quindi provare che per ogni insieme $\{a \mid \Box a \in \alpha\}$ esiste un $\beta$ che sia $KD-$ *consistente massimale* che lo contiene,
per farlo mi basta mostrare che esiste un insieme $\beta_0$ consistente che lo contiene, poi per il teorema di Lindelmann saprò anche che ne esiste uno consistente massimale.

$\beta_0 = \{a \mid \Box a \in \alpha\}$ , dimostro che $\beta_0$ è consistente.
Se per assurdo non lo fosse
$\vdash_{KD} a_1 \wedge ... \wedge a_n \implies \bot$, dove $a_1, a_2, ..., a_n$ sono formule di $\beta_0$
(da cui spostando $a_n$ dopo l'implica)
$\vdash_{KD} a_1 \wedge ... \wedge a_{n-1} \implies \neg a_n$ (uso la definizione 2. di logica normale)
$\vdash_{KD} \Box a_1 \wedge \cdots \wedge \Box a_n \implies \Box \neg a_n$
$\Box a_1 \wedge \cdots \wedge \Box a_n \implies \Box \neg a_n \in \alpha$ (dato che $\alpha$ è $KD - \textit{consistente massimale}$ contiene tutti i teoremi di $KD$)
$\Box a_1 \wedge \cdots \wedge \Box a_n \in \alpha$ per costruzione di $\beta_0$ (in $\beta_0$ valgono tutto le $\Box x$ se $x$ vale in $\alpha$)
$\Box \neg a_n \in \alpha$ (per MP dalle due precedenti)
$\neg \Diamond a_n \in \alpha$
$\Box a_n \in \alpha$ **(*)**
$\Box a_n \implies \Diamond a_n$ (schema seriale) **(**)**
Per MP fra **(*)** e **(**)** si ha $\Diamond a_n \in \alpha$

Da cui $\alpha$ non consistente, assurdo. $\lightning$

## 5.2 Debole densità del frame canonico di K$X\Diamond$

$R$ è debolmente densa se: $\forall \alpha, \beta : (\alpha R \beta) \implies \exists \gamma : (\alpha R \gamma \wedge \gamma R \beta)$

Chiamiamo K$X\Diamond$ una logica costruita a partire dalla logica $K$ aggiungendo lo schema $X\Diamond$: $\Diamond a \implies \Diamond \Diamond a$
La partenza del ragionamento è simile a quello del precedente in cui come insieme considero:
$\gamma_0 = \{a \mid a \in \alpha\} \cup \{\Diamond b \mid b \in \beta\}$

Per assurdo:
$\vdash_{KX\Diamond} a_1 \wedge ... \wedge a_n \wedge \Diamond b_1 \wedge ... \wedge \Diamond b_n \implies \bot$
dove $a_1, ..., a_n$ sono formule di $\alpha$, e $b_1, ..., b_n$ sono formule di $\beta$
$\vdash_{KX\Diamond} a_1 \wedge ... \wedge a_n \implies \neg(\Diamond b_1 \wedge ... \wedge \Diamond b_n)$
pongo $b = b_1 \wedge ... \wedge b_n$

**Teorema al volo:**
$\vdash_{KX\Diamond} \neg(\Diamond c \wedge \Diamond d) \implies \neg \Diamond (c \wedge d)$, cioè:
$\vdash_{KX\Diamond} \Diamond(c \wedge d) \implies \Diamond c \wedge \Diamond d$
infatti, sono tautologie della logica proposizionale: $\neg c \implies \neg c \vee \neg d$
e $\neg d \implies \neg c \vee \neg d$,
queste sono anche teoremi di $\Lambda$
dato che $\Lambda$ è normale si ha $\Box \neg c \implies \Box \neg c \vee \neg d$ (definizione 3.3 di logica normale)
e lo stesso vale per la seconda $\Box \neg d \implies \Box \neg c \vee \neg d$
dato che il conseguente si ha per due antecedenti diversi allora:
$\Box \neg c \vee \Box \neg d \implies \Box \neg c \vee \neg d$ da cui negando e scambiando antecedente e conseguente:

$\neg(\Box\neg c \vee \neg d) \implies \neg(\Box\neg c \vee \Box\neg d)$, sviluppo il $\neg$
$\diamond(c \wedge d) \implies \diamond c \wedge \diamond d$

Uso il teorema ottenendo (in un certo senso "portiamo fuori" il $\diamond$)
$\vdash_{KX\diamond} a_1 \wedge ... \wedge a_n \implies \neg \diamond (b_1 \wedge ... \wedge \diamond b_n)$ cioè (per come ho posto b)
$\vdash_{KX\diamond} a_1 \wedge ... \wedge a_n \implies \neg \diamond b$
Uso la definizione 2. di logica normale e riscrivo:
$\vdash_{KX\diamond} \Box a_1 \wedge \cdots \wedge \Box a_n \implies \Box\neg \diamond b$
$\vdash_{KX\diamond} \Box a_1 \wedge \cdots \wedge \Box a_n \implies \neg \diamond \diamond b$
dato che $\Box a_1 \wedge \cdots \wedge \Box a_n \implies \neg \diamond \diamond b \in \alpha$
e che: $\Box a_1 \wedge \cdots \wedge \Box a_n \in \alpha$
anche $\neg \diamond \diamond b \in \alpha$ (MP dalle due precedenti)
dato che $\diamond b \in \alpha$ anche $\diamond \diamond b \in \alpha$ per lo schema delle relazioni debolmente dense
il che ci porterebbe alla non massimalità di $\alpha$ contro l'ipotesi. ↯

## 5.3 Riflessività del frame canonico di KT

$R^{KT}$ è riflessiva se: $\forall\alpha$, $\alpha R^{KT}\alpha$
Vogliamo dimostrare che l'insieme $\{a \,|\, \Box a \in \alpha\}$ di formule è contenuto in $\alpha$
Se $\Box a \in \alpha$ cioè se $\vdash_{KT} \Box a$ allora
$\vdash_{KT} x$ dato che $\Box a \implies a$ è uno schema della logica $KT$ e quindi:
$a \in \alpha$.
Per questi motivi $\{a \,|\, \Box a \in \alpha\}$ è in effetti contenuto in $\alpha$
Da cui segue la tesi.

## 5.4 Simmetria del frame canonico di KB

$R^{KB}$è simmetrica se $\forall\alpha, \beta\, \alpha R^{KB}\beta \implies \beta R^{KB}\alpha$
Se $\beta R^{K4}\alpha$ allora:
$\{\diamond b \,|\, b \in \alpha\} \subseteq \beta$
per definizione di R del modello canonico.
Dal momento che vale l'assioma B: $a \implies \Box \diamond a$,
per ogni formula $b \in \alpha$ si ha che:
$\Box \diamond b \in \alpha$,
D'altra parte ogni volta che $b \in \alpha$, $\diamond b \in \beta$ dato che $\beta R^{K4}\alpha$ e quindi:
$\{a \mid \Box a \in \alpha\} \subseteq \beta$ cioè $\alpha R\beta$

## 5.5 Correttezza e completezza di KD

La logica KD è corretta e completa rispetto alla classe dei Frame seriali
Dimostrazione
Ip) $F \models a$ con F seriale

Ts) $\vdash_{KD} a$

Se a è un teorema di KD, è ricavato da una serie di formule che possono essere applicazioni degli schemi A1, A2, A3, K, D oppure applicazioni del modus ponens o della regola di necessitazione.
Supponiamo per assurdo che:
$\nvdash_{KD} a$
allora avremo che:
$\mu^{KD} \not\models a$
e quindi:
$F^{KD} \not\models a$
Poiché a non è vera nel frame canonico, non può essere vera in alcun frame seriale, ma questo va contro l'ipotesi, assurdo. Allora la tesi deve essere valida.

*No, Impassabile. Nulla è impossibile.*

Lewis Carroll

# 6 Decidibilità Delle Logiche Modali

## 6.1 Filtrazione

Dato una logica $\Lambda$ e una formula a, si può garantire che esiste un modello $\mu$, con un numero di mondi limitato da f(n), con n numero di sottoformule di a tale che:
$\vdash_\Lambda a \iff \mu \models a$
Dimostrazione.
Ip) $a \in \Gamma \implies sottoformule(a) \subseteq \Gamma$
Ts) $\exists \mu : \vdash_\Lambda a \iff \mu \models a$
sia $\mu$=(S,R,V), consideriamo la seguente relazione:
$\sim_\Gamma \subseteq S \times S$
che gode della seguente proprietà:
$\Gamma_\alpha = \{a \in \Gamma \mid \mu \models_\alpha a\}$
$\alpha \sim_\Gamma \beta \iff \Gamma_\alpha = \Gamma_\beta$
Si può notare che $\sim_\Gamma$ è una relazione di equivalenza, Infatti:

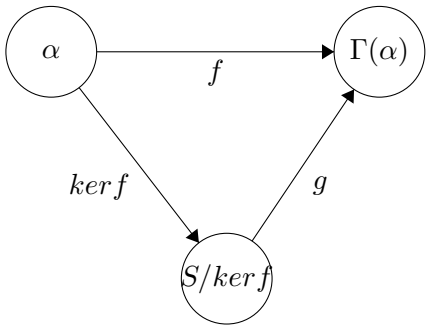
1. è simmetrica
   $\alpha \sim_\Gamma \alpha \iff \Gamma_\alpha = \Gamma_\alpha$

2. è riflessiva
   $\alpha \sim_\Gamma \beta \iff \Gamma_\alpha = \Gamma_\beta \iff \beta \sim_\Gamma \alpha$

3. è transitiva:
   $\alpha \sim_\Gamma \beta \wedge \alpha \sim_\Gamma \gamma \iff \Gamma_\alpha = \Gamma_\beta = \Gamma_\gamma \iff \gamma \sim_\Gamma \beta$

Posso allora considerare l'insieme quoziente:

$S_\Gamma = S/\sim_\Gamma$
Si può dimostrare con il teorema di fattorizzazione delle applicazioni che:
$|S_\Gamma| \leq 2^{|\Gamma|}$




Per dimostrarlo basta prendere:
$f : S \to \mathcal{P}(\Gamma)$ che associa $f(\alpha) = \Gamma_\alpha$
risulta banale verificare che:
$ker\, f \equiv\sim_\Gamma$ (due stati $\alpha,\ \beta$ appartengono al kernel se hanno la stessa immagine cioè se $f(\alpha) = \Gamma_\alpha = \Gamma_\beta = f(\beta)$, se ciò avviene sono anche in relazione tramite $\sim_\Gamma$)
e quindi, ricordando che $g$ è iniettiva, risulta banale che:
$|S/\sim_\Gamma| \leq |\mathcal{P}(\Gamma)|$
$|\mathcal{P}(\Gamma)| = 2^{|\Gamma|}$
Allora possiamo prendere il modello:
$M^\Gamma = (S^\Gamma, R', V^\Gamma)$
$R' \subseteq S^\Gamma \times S^\Gamma$
con R' che soddisfi le seguenti proprietà:
F1) $(\alpha, \beta) \in R \implies ([\alpha], [\beta]) \in R'$
F2) $([\alpha], [\beta]) \in R' \implies \forall \Box b \in \Gamma,\ \mu \models_\alpha \Box b \implies \mu \models_\beta b$
Una relazione che gode delle proprietà F1 e F2 si chiama Γ-filtrazione della relazione R.
Prendiamo infine:
$V^\Gamma : \Phi \cap \Gamma \to \mathcal{P}(S^\Gamma)$
che gode della seguente proprietà:
presa una formula atomica $A \in \Phi \cap \Gamma$
$\alpha \in V^\Gamma(A) \iff \alpha \in V(A)$

### 6.1.1 Teorema

Esiste almeno una relazione che gode delle proprietà F1 e F2:
$R^\sigma \subseteq S^\Gamma \times S^\Gamma$
così definita:
$([\alpha], [\beta]) \in R^\sigma \iff \exists \delta \in [\alpha], \eta \in [\beta] : (\delta, \eta) \in R$
La proprietà F1 è dimostrata banalmente.
Dimostriamo F2
Ip) $([\alpha], [\beta]) \in R^\sigma, \Box b \in \Gamma, \mu \models_\alpha \Box b$

Ts) $R^{\delta}$gode della proprietà F2

Supponiamo che:
$\exists \delta, \eta : \delta R \eta \wedge \delta \in [\alpha] \wedge \eta \in [\beta]$
avremo che:
$\mu \models_{\delta} \Box b$
$\mu \models_{\eta} b$
e quindi:
$\mu \models_{\beta} b$

## 6.2 Lemma di Filtrazione

Dato un insieme $\Gamma$ chiuso rispetto alle sottoformule di $a$, con $a \in \Gamma$
$\mu \models_{\alpha} a \iff \mu^{\Gamma} \models_{\alpha} a$
per ogni $\mu^{\Gamma}\Gamma$-filtrazione di $\mu$
Dimostrazione:
Ip) $\mu^{\Gamma}\Gamma$-filtrazione di $\mu$
Ts) $\mu \models_{\alpha} a \iff \mu^{\Gamma} \models_{[\alpha]} a$

Per induzione sul numero di connettivi di a
Caso Base, $n = 0$:
$a$ non ha connettivi, allora $a \equiv A$
$\mu \models_{\alpha} A \iff \alpha \in V(A) \iff \alpha \in V^{\Gamma}(A) \iff \mu^{\Gamma} \models_{[\alpha]} a$
Ipotesi di induzione: il teorema vale per ogni formula di $\Gamma$ con m<n connettivi.
a può essere:

1. $\neg b$
2. $b \implies c$
3. $\Box b$

**Caso 1:**
$\mu \models_{\alpha} \neg b \iff \mu \not\models_{\alpha} b \iff \mu^{\Gamma} \not\models_{[\alpha]} b \iff \mu^{\Gamma} \models_{[\alpha]} \neg b$

**Caso 2:**
$\mu \models_{\alpha} b \implies c$ se e solo se $\mu \not\models_{\alpha} b$ oppure $\mu \models_{\alpha} c$
quindi si può affermare
$\mu \not\models_{\alpha} b \iff \mu^{\Gamma} \not\models_{[\alpha]} b$
$\mu \models_{\alpha} c \iff \mu^{\Gamma} \models_{[\alpha]} c$
ma vale almeno una delle due se e solo se
$\mu^{\Gamma} \models_{[\alpha]} b \implies c$

**Caso 3:**
Ip) $\mu \models_\alpha \Box b$
Ts) $\mu^\Gamma \models_{[\alpha]} \Box b$

Consideriamo la reazione R' avente le proprietà F1 e F2
$\forall[\beta] : ([\alpha], [\beta]) \in R' \implies \mu \models_\beta b$ – per F2
e per ipotesi induttiva anche: $\mu^\Gamma \models_{[\beta]} b$
allora si può affermare che:
$\mu \models_\beta b \implies \mu^\Gamma \models_{[\beta]} b \implies \mu^\Gamma \models_{[\alpha]} \Box b$

Ip)$\mu^\Gamma \models_{[\alpha]} \Box b$
Ts)$\mu \models_\alpha \Box b$

$\forall[\beta] : (\alpha, \beta) \in R, ([\alpha], [\beta]) \in R'$ –per F1
allora si può affermare che:
$\mu^\Gamma \models_{[\beta]} b \implies \mu \models_\beta b \implies \mu \models_\alpha \Box b$

## 6.3 Determinatezza di K dai Frame Finiti

La minima logica normale K è determinata dalla classe di tutti i frame finiti.
Se $a$ ha n sottoformule $a$ è un teorema di K se e solo se A è valida in tutti i frame con meno di $2^n$ mondi.
$\vdash_K a$ se e solo se $F \models a$.

Ip)$\vdash_K a$
Ts)$F \models a$

Se $a$ è un teorema di K allora $a$ è valida in tutti i frame (infatti K è determinata rispetto alla classe di tutti i frame) è a maggior ragione valida in tutti i frame finiti ed in tutti i frame con meno di $2^n$ mondi.

Ip)$F \models a$
Ts)$\vdash_K a$

Suppongo per assurdo che $\nvdash_K a$ se e solo se $M^K \not\models a$ se e solo se (per il lemma di filtrazione) $(M^K)^\Gamma \not\models a$ il che implica che
in particolare $(F^K)^\Gamma \not\models a$ dove $(F^K)^\Gamma$ è il Frame su cui è costruita la filtrazione del modello canonico costruito rispetto alla logica $K$
Si noti che $(M^K)^\Gamma$ ha al più $2^n$ mondi.

## 6.4 Determinatezza di KD dai Frame seriali finiti

Per seguire lo stesso ragionamento della dimostrazione appena fatta, dobbiamo solo mostrare che se $R$ è seriale allora $R^\sigma$ lo è.

**Nota:** $R^\sigma \subseteq S^\Gamma \times S^\Gamma$
così definita:
$([\alpha],[\beta]) \in R^\sigma \iff \exists \delta \in [\alpha], \eta \in [\beta] \,:\, (\delta,\, \eta) \in R$

Sia $[\alpha] \in S^\Gamma$

Se $R^{KD}$ è seriale allora $\forall \delta \in S^{KD} \exists \eta \in S^{KD} :\ (\delta, \eta) \in R^{KD}$

In particolare esiste $\delta$ appartiene alla classe di equivalenza $[\alpha]$ (di cui al limite potrebbe essere l'unico elemento con $\alpha = \delta$)

Dalla serialità abbiamo che esiste $\eta$ appartiene alla classe di equivalenza $[\beta]$

Da cui $([\alpha],[\beta]) \in R^\sigma$

## 6.5 Determinatezza di K4 dai Frame transitivi finiti

L'aspetto interessante di questa dimostrazione sta nel fatto che non possiamo usare la relazione "classica" $R^\sigma$ come $\Gamma$-filtrazione ma dobbiamo costruirne una ad hoc, dato che se $R^{K4}$ è transitiva la sua filtrazione standard non è detto che lo sia

Definiamo quindi $R^\tau$così:

$([\alpha],[\beta]) \in R^\tau$ se se e solo se per ogni fbf $b$, $\Box b \in \Gamma$ e $M \models_\alpha \Box b$ implicano $M \models_\beta b \wedge \Box b$

dimostriamo che $R^\tau$ è una $\Gamma$-filtrazione transitiva

$R^\tau$è una $\Gamma$-filtrazione

F2) $([\alpha],[\beta]) \in R^\tau$ se e solo se$M \models_\alpha \Box b$ implicano $M \models_\beta b \wedge \Box b$ da cui: $\{b \mid \Box b \in \alpha\} \subseteq \beta$ e quindi $\alpha, \beta \in R^{K4}$

F1) $(\alpha, \beta) \in R^{K4}$per ogni $\Box b \in \Gamma$, se $M \models_\alpha \Box b$ allora anche (schema 4) $M \models_\alpha \Box\Box b$

dato che $(\alpha, \beta) \in R^{K4}$ , anche:

$M \models_\beta b$ e $M \models_\beta \Box b$ e quindi:

$M \models_\beta b \wedge \Box b$

$R^\tau$ è transitiva

Sia $([\alpha],[\beta]) \in R^\tau$, $([\beta],[\gamma]) \in R^\tau$ ora la prima implica che per ogni fbf $b$, da $\Box b \in \Gamma$ e $M \models_\alpha \Box b$ segua $M \models_\beta \Box b \wedge b$, e da questa essendo $([\alpha],[\beta]) \in R^\tau$, segue anche $M \models_\gamma \Box b \wedge b$, cioè $([\beta],[\gamma]) \in R^\tau$

## 6.6 Tableaux

I Tableaux sono un metodo efficiente per dimostrare la verità, falsità e soddisfacibilità di una formula
Il metodo consiste nel partire dalla formula che si vuole considerare, negandola.
Dopodiché si procede passo passo alla costruzione di un albero seguendo delle regole di espansione che aggiungono uno o più nodi o rami all'albero.
Le regole con la virgola aggiungono un nodo allo stesso ramo, mentre le regole con il pipe sdoppiano il ramo.
Se espando una formula, devo aggiungere coerentemente l'espansione a tutti i sotto-rami, e non posso più espanderla.
Se un cammino contiene sia una formula che la sua negazione il cammino si chiude.
Se esiste almeno un cammino chiuso, la formula di partenza è soddisfacibile, se tutti i cammini sono chiusi, la formula è logicamente valida, altrimenti la formula è falsa.

### 6.6.1 Tableaux per la logica proposizionale

Le regole Per applicare l'algoritmo dei tableaux nella logica proposizionale sono le seguenti:

- Radice dell'albero

  $$\neg a$$

- Regola del $\neg$

  $$\frac{\neg\neg a}{a}$$

- Regole di tipo $\alpha$

  $$\frac{a \wedge b}{a,\ b} \qquad \frac{\neg(a \vee b)}{\neg a,\ \neg b} \qquad \frac{\neg(a \implies b)}{a,\ \neg b}$$

- Regole di tipo $\beta$

  $$\frac{a \vee b}{a \mid b} \qquad \frac{\neg(a \wedge b)}{\neg a \mid \neg b} \qquad \frac{a \implies b}{\neg a \mid b}$$

- Regole di tipo $\iff$

  $$\frac{a \iff b}{a,\ b \mid \neg a,\ \neg b} \qquad \frac{\neg(a \iff b)}{a,\ \neg b \mid \neg a,\ b}$$

### 6.6.2 Tableaux per le logiche modali

Per le logiche modali, si può modificare l'algoritmo già usato per le logiche proposizionali, aggiungendo le regole per la necessitazione e considerando che ogni regola deve essere vera in un mondo.

Per fare ciò devo aggiungere l'indice del mondo a tutte le regole, e si potrà chiudere un ramo solo se si trova la regola e il suo negato nello stesso mondo.
Le regole dei tableaux per le logiche modali saranno:

- Radice dell'albero

  $1.\neg a$

- Regola del $\neg$

  $$\frac{\delta\, \neg\neg a}{\delta a}$$

- Regole di tipo $\alpha$

  $$\frac{\delta\, a \wedge b}{\delta\, a,\, \delta\, b} \qquad \frac{\delta\, \neg(a \vee b)}{\delta\, \neg a,\, \delta\, \neg b} \qquad \frac{\delta\, \neg(a \implies b)}{\delta\, a,\, \delta\, \neg b}$$

- Regole di tipo $\beta$

  $$\frac{\delta\, a \vee b}{\delta\, a | \delta\, b} \qquad \frac{\delta\, \neg(a \wedge b)}{\delta\, \neg a | \delta\, \neg b} \qquad \frac{\delta\, a \implies b}{\delta\, \neg a | \delta\, b}$$

- Regole di tipo $\iff$

  $$\frac{\delta\, a \iff b}{\delta\, a,\, \delta\, b | \delta\, \neg a,\, \delta\, \neg b} \qquad \frac{\delta\, \neg(a \iff b)}{\delta\, a,\, \delta\, \neg b | \delta\, \neg a,\, \delta\, b}$$

- Regole di necessitazione

  $$\frac{\sigma\, \Box a}{\sigma_n\, a} \qquad \frac{\sigma\, \neg \Diamond a}{\sigma_n\, \neg a}$$ – con $\sigma_n$ già presente nei nodi precedenti

  $$\frac{\sigma\, \neg \Box a}{\sigma_n\, \neg a} \qquad \frac{\sigma\, \Diamond a}{\sigma_n\, a}$$ – con $\sigma_n$ non presente nei nodi precedenti

Tuttavia queste regole non sono sufficienti se vogliamo usare una regola modale differente da K.
Per lavorare su regole con proprietà dei frame particolari, devo necessariamente cambiare le regole di necessitazione aggiungendo dei vincoli alla generazione di nuovi mondi in modo tale che rispettino le proprietà del frame.

## 6.7 Logiche notevoli

Abbiamo visto K essere la logica modale minima, a partire da questa logica ne possiamo ottenere altre aggiungendo ad essa alcuni schemi di assiomi:

- D : $\Box a \implies \diamond a$ (seriale)
- T: $\Box a \implies a$ (riflessiva)
- B: $a \implies \Box \diamond a$ (simmetrica)
- 4:$\Box a \implies \Box\Box a$ (transitiva)
- 5: $\diamond a \implies \Box \diamond a$ (euclidea)

Per ognuno di questi schemi di assiomi (X) ne esiste il cosiddetto duale (X$\diamond$), cioè lo schema che si ottiene invertendo antecedente e conseguente e negando $\Box a$ con $\diamond a$

### 6.7.1 Teorema: validità del duale

M sia una sequenza di connettivi $\Box$, $\diamond$ ed M' il suo duale.
Idem per N ed N'.

Ip) $Ma \implies Nb$
Ts) $N'b \implies M'a$

Se vale lo schema d'assiomi $Ma$ deve valere anche $M\neg a$ dato che appunto è uno schema.
Riscrivo l'ipotesi come:
$M\neg a \implies N\neg b$
Considero la tautologia della PL: $(C \implies D) \implies (\neg D \implies \neg C)$
la applico all'ipotesi ottenendo:
$(M\neg a \implies N\neg b) \implies (\neg(N\neg b) \implies \neg(M\neg a))$
Da cui per MP con l'ipotesi (riscritta) ottengo:
$\neg(N\neg b) \implies \neg(M\neg a)$
Usando ripetutamente le equivalenze tra$\Box$ e $\diamond$ ottengo:
$N'\neg\neg b \implies M'\neg\neg a$ semplificando:
$N'b \implies M'a$
La dimostrazione nell'altro senso è del tutto simmetrica dato che le operazioni effettuate sono valide in entrambe le direzioni

### 6.7.2 Esempio validità del duale: schema 5

Ip) $\diamond a \implies \Box \diamond a$
Ts)$\diamond\Box a \implies \Box a$

Riscrivo l'ipotesi come:
$\diamond\neg a \implies \Box \diamond \neg a$
Considero la tautologia della PL: $(C \implies D) \implies (\neg D \implies \neg C)$
$(\diamond\neg a \implies \Box \diamond \neg a) \implies (\neg\Box \diamond \neg a \implies \neg \diamond \neg a)$
Semplifico il conseguente :$\neg\Box \diamond \neg a \implies \neg \diamond \neg a$ diventa
$\diamond\Box\neg\neg a \implies \Box\neg\neg a$ , semplificando i $\neg$:

$\diamond\Box a \implies \Box a$
Cioè la tesi.

Vogliamo ora mostrare come alcune notazione della forma KX denotino la stessa logica. Ricordiamo che con KX intendiamo la logica K a cui abbiamo aggiunto il generico assioma X
KB4 = K + assioma B + assioma 4

### 6.7.3 Inclusione di KD in KT

Pare ovvio che una logica riflessiva sia anche seriale (se parlo da solo parlo con qualcuno), ma dimostriamolo comunque.

Ip) KT
Ts) KD
Se vale T:
$\Box a \implies a$ (riflessiva)
allora vale anche il suo duale $T\diamond$:
$a \implies \diamond a$
Per la catena di implicazioni ($a \implies b,\ b \implies c,\ a \implies c$) abbiamo:
$\Box a \implies \diamond a$
Cioè lo schema D

**Lemma implica in KB:**
IP)$\vdash_{KB} \diamond C \implies D$
TS) $\vdash_{KB} C \implies \Box D$

Per Ip) $\diamond C \implies D$ e quindi, dato che è un teorema della logica KB, (che è una logica normale)
posso usare la definizione 3 equivalente di logica normale ottenendo:
$\Box \diamond C \implies \Box D$
Inoltre vale lo schema B
$C \implies \Box \diamond C$
Leggendo i due schemi appena scritti dal secondo al primo riconosciamo la catena di implicazioni ($a \implies b,\ b \implies c,\ a \implies c$)
Da cui: $C \implies \Box D$

### 6.7.4 Equivalenza KB4, KB5

**Da KB4 a KB5**
Valendo 4 vale anche 4$\diamond$:
$\diamond(\diamond a) \implies (\diamond a)$, e tenendo conto del precedente lemma
(dove $C$ è $\diamond a$ e $B$ è $\diamond a$),

abbiamo $\diamond a \implies \Box \diamond a$ cioè lo schema5.

**Da KB5 a KB4**

Da 5 infatti deduciamo 5$\diamond$: $\diamond(\Box a) \implies (\Box a)$

Tenuto conto della prima osservazione (con$C$ e$B$ uguali ad $a$)

abbiamo $\Box a \implies \Box\Box a$.

### 6.7.5 Equivalenza KDB4. KDB5, KDB45, KTB4, KT5

**KDB4 = KDB5 = KD45**, infatti aggiungendo l'assioma D a due logiche equivalenti (KB4, KB5) continuano a rimanere equivalenti;

aggiungere 4 a KDB5 non produce alcun effetto perché lo contiene già.

Inoltre notiamo che: **KDB4⊆KTB4** in quanto KT contiene KD

e **KT5⊆KTB4** in quando KT4B contiene KT4 che coincide con KT5.

Mostriamo che **KTB4⊆KDB4** così da arrivare a KTB4 = KDB4

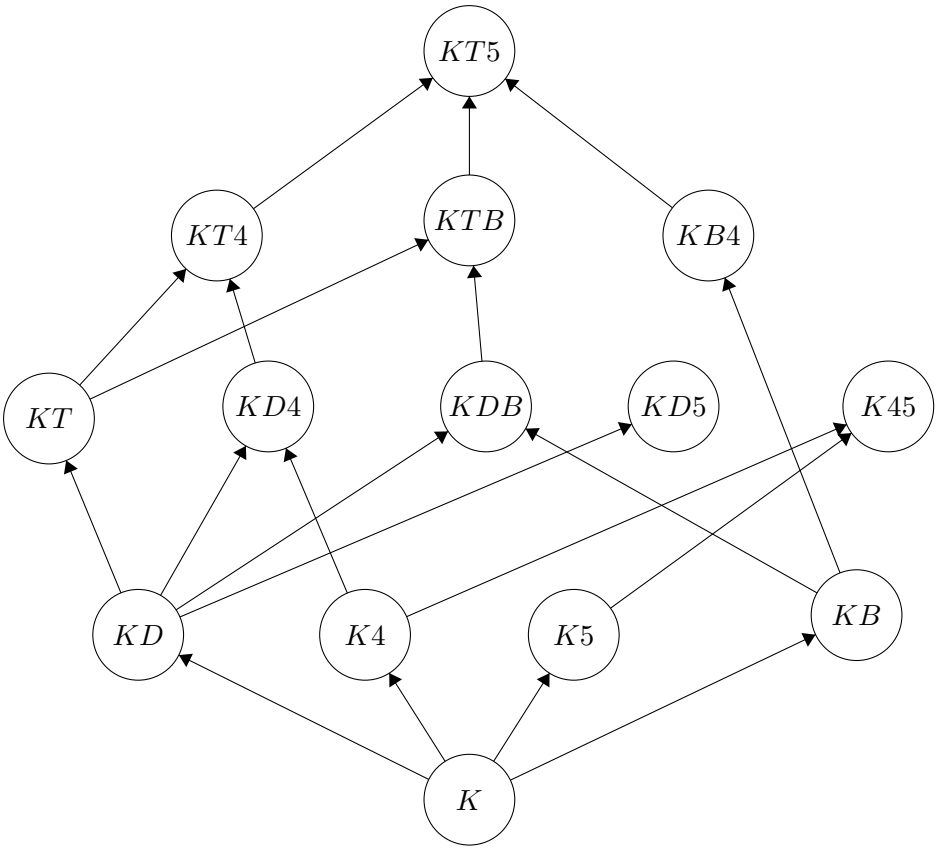
Cioè mostriamo che nella logica K, dall'assioma T, con B e 4 posso dedurre l'assioma D

Dall'assioma T deduciamo l'assioma T$\diamond$ cioè $a \implies \diamond a$

Dato che vale 5: $\diamond a \implies \Box \diamond a$, sfruttando la catena di implicazioni delle due precedenti abbiamo:

$a \implies \Box \diamond a$ cioè B.

### 6.7.6 Reticolo delle logiche




### Somma diretta di Frame

S5 è determinata dalla classe dei frame d' equivalenza (cioè frame in cui la relazione di accessibilità è una relazione di equivalenza), S5 = KT5 = KTB4 (riflessiva, simmetrica, transitiva)
S5 è determinata dalla classe dei frame universali (cioè frame in cui la relazione di accessibilità è la relazione universale).
Mostriamo (almeno argomentiamo) la seconda affermazione.

Data una collezione di frame con insiemi di mondi a due a due disgiunti, si dice somma diretta di questi frame il frame che ha come insieme dei mondi l'unione dell'insieme dei mondi dei frame della collezione e come relazione la unione delle relazioni dei frame della collezione.
$F = (S, R)$
$F1 = (S1, R1),\ F2 = (S2, R2)$
$F = F1 \oplus F2$ se e solo se $F = (S1 \cup S2,\ R1 \cup R2)$
Si dimostra che $F \models a$ se e solo se $F1 \models a$ e $F2 \models a$

Dato che una relazione di equivalenza forma una partizione sull'insieme su cui è definita, e che in ogni classe di equivalenza è una relazione universale, possiamo vedere una relazione di equivalenza come somma di relazioni universali e il suo insieme come somma disgiunta di insiemi; la somma diretta pertanto ci mostra quindi che S5 è determinata dai frame universali.

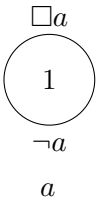
### 6.7.7 Tableaux rivisitato per KT, KB

Se una logica contiene l'assioma T devo aggiungere alle regole del Tableaux

- Regole di necessitazione

$$\frac{\sigma\,\Box a}{\sigma_n\,a} \qquad \frac{\sigma\,\neg\,\Diamond\,a}{\sigma_n\,\neg a}$$ – con $\sigma_n$ già presente nei nodi precedenti, oppure $\sigma_n$ **nodo corrente**

es. Si provi che la formula: $(\Box a \implies a)$ è un teorema in KT
1: $\neg(\Box a \implies a)$
1: $\Box a$
1: $\neg a$
**1**: $a$




Dove nell'ultimo passaggio ho usato proprio la regola appena introdotta, avendo ottenuto $a$ e $\neg a$ nello stesso stato (mondo) deduco che negare $a$ mi porta a un assurdo e quindi deve per forza essere un teorema.
Se una logica contiene l'assioma B devo aggiungere alle regole del Tableaux

- Regole di necessitazione

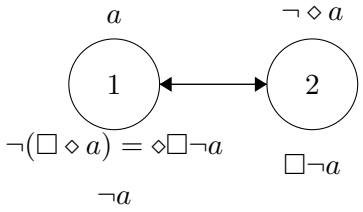
$$\frac{\sigma\,\Box a}{\sigma_n\,a}$$
$$\frac{\sigma\,\neg\,\Diamond\,a}{\sigma_n\,\neg a}$$

con $\sigma_n$ già presente nei nodi precedenti, oppure $\sigma_n$ **nodo prefisso del nodo corrente**

(es 11 è prefisso di 111)

es. Si provi che la formula $(a \implies \Box\,\Diamond\,a)$ è un teorema in KB
1:$\neg(a \implies \Box\,\Diamond\,a)$
1:$a$

1:$\neg(\Box \diamond a)$
1: $\diamond\Box\neg a$
11: $\Box\neg a$
**1:** $\neg a$



*Be'! Naturale che tu sia in ritardo!*
*Questo cipollone è esattamente due*
*giorni indietro!*

Lewis Carroll

# 7 Logica temporale

## 7.1 Sottomodello generato da $\alpha$

Presa una logica $\Lambda$ e un modello $\mu = (S, R, V)$, prendiamo un qualunque $\alpha \in S$
Si dice sottomodello generato da $\alpha$ il modello:
$\mu^\alpha = (S^\alpha, R^\alpha, V^\alpha)$
con:
$S^\alpha = \{\beta \mid \alpha R^* \beta\}$ dove $R^*$ è la chiusura riflessiva e transitiva di R
$R^\alpha \subseteq S^\alpha \times S^\alpha$
$R^\alpha = R \cap S^\alpha \times S^\alpha$
e la valutazione tale che:
$\beta \in V^\alpha(A) \iff \beta \in S^\alpha \wedge \beta \in V(A)$

### 7.1.1 Lemma

Ip) $\beta \in S^\alpha$
Ts) $\mu \models_\beta a \iff \mu^\alpha \models_\beta a$
Dimostrazione per induzione sulla complessità di a:
Caso base: $a \in \Phi$
$\beta \in V(a) \implies \beta \in V^\alpha(a)$
Ipotesi di induzione: il teorema vale per formule con un numero di connettivi minore di n.
Bisogna dimostrare 3 casi:
1) $\neg b$
2) $b \implies c$

3) $\Box b$
I primi due casi sono banali, come negli altri casi. Dimostriamo l'ultimo.
Ip) $\mu^\alpha \models_\beta \Box b$
Ts) $\mu \models_\beta \Box b$

$\mu^\alpha \models_\beta \Box b \iff \mu^\alpha \models_\gamma b$, per ogni $\gamma$ tale che $\beta R^\alpha \gamma$
ma per ipotesi di induzione:
$\mu^\alpha \models_\gamma b \iff \mu \models_\gamma b \iff \mu \models_\beta \Box b$
Ip) $\mu \models_\beta \Box b$
Ts) $\mu^\alpha \models_\beta \Box b$

Per ogni $\delta$ tale che $\beta R^\alpha \delta$
si ha che $\beta R \delta$
infatti $R^\alpha = R \cap S^\alpha \times S^\alpha$ e quindi se $(\beta, \delta) \in R^\alpha$ deve essere anche $(\beta, \delta) \in R$
Dall'ipotesi $\mu \models_\beta \Box b$, sappiamo che $b$ è vera in tutti i $\gamma$ tali che $(\beta, \gamma) \in R$ cioè $\mu \models_\gamma b$, ma per ipotesi induttiva si ha anche $\mu^\alpha \models_\gamma b$
Da cui la tesi.

### 7.1.2 Corollario

Valgono le seguenti:
$\mu \models a \implies \mu^\alpha \models a$
$\mu \models a \iff \mu^\alpha \models a \, \forall \alpha \in S$
$F \models a \iff F^\alpha \models a \, \forall \alpha \in S$

## 7.2 p-Morfismo

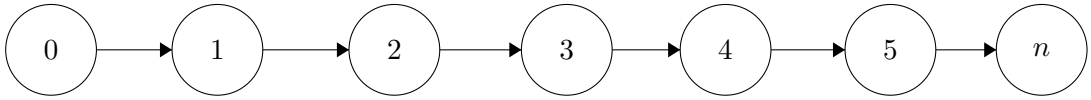
Siano $F_1(S_1, R_1)$, $F_2(S_2, R_2)$ frame.
C'è un p-morfismo (pseudo-morfismo) tra $F_1$ e $F_2$ se esiste una applicazione che gode delle seguenti proprietà:
1) $(\alpha, \beta) \in R_1 \implies (f(\alpha), f(\beta)) \in R_2$
2) $(f(\alpha), \eta) \in R_2 \implies \exists \beta \in S_1 : f(\beta) = \eta \wedge (\alpha, \beta) \in R_1$
Considerati poi due modelli $M_1(F_1, V_1)$, $M_2(F_2, V_2)$, esiste un p-morfismo tra $M_1$ e $M_2$se vale la proprietà:
3) $\alpha \in V_1(A) \iff f(\alpha) \in V_2(A)$
se f è suriettiva, allora il p-morfismo si dice suriettivo

### 7.2.1 Lemma

Siano $\mu_1$ e $\mu_2$ due modelli e f un p-morfismo di $\mu_1$ su $\mu_2$, allora:
$\mu_1 \models_\alpha a \iff \mu_2 \models_{f(\alpha)} a$
Siano $F_1$e $F_2$ due frame e f un p-morfismo suriettivo di $F_1$su $F_2$, allora:
$F_1 \models a \implies F_2 \models a$

## 7.3 Frame ($\omega$, $<$)

Il frame ($\omega$, $<$) è il frame che rappresenta la retta dei numeri naturali.
E' adatto a rappresentare il tempo discreto con un istante iniziale.
La logica che rappresenta questo frame è la logica K4DLZ, che è corretta e completa rispetto a ($\omega$, $<$)




## 7.4 La logica K4DLZ

La logica K4DLZ, detta anche logica $\Omega$ è la logica che ha, oltre all'assioma K, i seguenti assiomi:

- 4: $\Box a \implies \Box\Box a$ –> transitività
- D: $\Box a \implies \diamond a$ –> serialità
- L: $\Box(a \wedge \Box a \implies b) \vee \Box(b \wedge \Box b \implies a)$ –> debole connessione
- Z: $\Box(\Box a \implies a) \implies (\diamond\Box a \implies \Box a)$

L'assioma Z, non ha alcuna interpretazione preso a se stante, ma in combinazione con gli altri implica che tra due mondi connessi c'è solo un numero finito di mondi, a due a due connessi.

## 7.5 Correttezza di K4DLZ

Ip) $\vdash_\Omega a$
Ts) $(\omega, <) \models a$

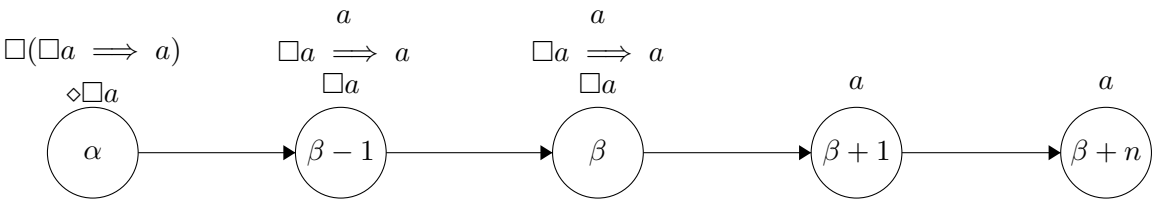
Per dimostrare questo teorema dobbiamo dimostrare che ogni teorema di K4DLZ è una formula valida. Poiché ogni teorema di $\Omega$ è una serie di applicazioni degli assiomi o delle regole di inferenza, dobbiamo assicurare che:

1. Modus Ponens e la regola di necessitazione fanno passare da formule valide a formule valide. Come abbiamo dimostrato, questo è sempre vero.
2. Gli assiomi siano formule valide:

- A1, A2, A3, K sono validi su ogni frame, e quindi sono validi anche su ($\omega$, $<$)
- 4 è valido su ogni frame transitivo, e quindi è valido anche su ($\omega$, $<$) essendo transitivo

- D è valido su ogni frame seriale, e quindi è valido anche su $(\omega, <)$ essendo seriale.
- L è valido su ogni frame debolmente connesso, e quindi è valido anche su $(\omega, <)$ essendo debolmente connesso.

Dobbiamo quindi dimostrare solo la validità di Z.
Z è l'assioma $\Box(\Box a \implies a) \implies (\diamond\Box a \implies \Box a)$, per dimostrare che è valido basta considerare il caso in cui gli antecedenti delle implicazioni siano validi
supponiamo dunque che esistano due mondi $\alpha$ e $\beta$ con $\alpha < \beta$ tali che
$(\omega, <) \models_\alpha \Box(\Box a \implies a)$
$(\omega, <) \models_\alpha \diamond\Box a$
$(\omega, <) \models_\beta \Box a$
allora da quest'ultima, viste le altre proprietà del frame, $\forall \eta > \beta$ avremo:
$(\omega, <) \models_\eta a$
dalla prima invece abbiamo:
$(\omega, <) \models_\beta \Box a \implies a$
e allora, applicando il modus ponens
$(\omega, <) \models_\beta a$
Ma, allora possiamo applicare lo stesso ragionamento per $\beta - 1$, poiché:
$(\omega, <) \models_{\beta-1} \Box a$




Ma, siccome esiste un numero finito di mondi tra $\alpha$ e $\beta$, arriveremo a un certo punto a provare che:
$(\omega, <) \models_{\alpha+1} a$
e quindi:
$(\omega, <) \models_\alpha \Box a$


e la tesi è dimostrata.

## 7.6 Completezza di K4DLZ

Ip) $(\omega, <) \models a$

Ts)$\vdash_\Omega a$

Questa dimostrazione è così lunga da essere suddivisa per convenienza in punti

**1)**

Per assurdo supponiamo che non valga la tesi, cioè che

$\nvdash_\Omega a$, per il lemma di verità si ha anche $M^\Omega \not\models a$, $M^\Omega = M_1$

$M_1$è seriale, transitivo e debolmente connesso, infatti queste proprietà si conservano quando si passa dalla logica al modello canonico.

Dato che $M^\Omega \not\models a$, in particolare esiste un mondo $\alpha$ in cui $M_1 \not\models_\alpha a$

**2)**

$M_2 = M_1^\alpha$, dove $M_1^\alpha$ è il sottomodello generato da $\alpha$.

$M_2$ è seriale, transitivo e connesso. La serialità e la transitività vengono direttamente da $M_1$, esaminiamo la connessione.

$M_2 = (S_2, R_2, V_2)$ se $\delta \in S_2$e $\gamma \in S_2$ allora $(\alpha, \gamma) \in R_1^*$ e $(\alpha, \delta) \in R_1^*$

Dato che $R_1$è già transitiva(vedi punto 1) la sua chiusura riflessiva e transitiva si limita a unire la relazione identica (cioè aggiunge gli autoanelli ai mondi)

Dal momento che $R_1$ è debolmente connessa, $R_1^*$, avendo anche la riflessività è connessa e lo stesso vale quindi per $R_2$.

Inoltre $M_2 \not\models a$, infatti sappiamo che se $M \models a$ allora $M^\alpha \models a$ per ogni mondo $\alpha$ di $M$

**3)**

$M^3$ =$\Gamma$-filtrazione di $M_2$, con $\Gamma = Stf(a)$

dove come $\Gamma$-filtrazione delle relazione di raggiungibilità di $M_2$ si prende la filtrazione transitiva.

$M^3$ è ancora seriale e connesso ed è transitivo per costruzione, inoltre il suo insieme di mondi ha cardinalità limitata superiormente da $2^{|Sfm(A)|}$

Inoltre $M_3 \not\models a$

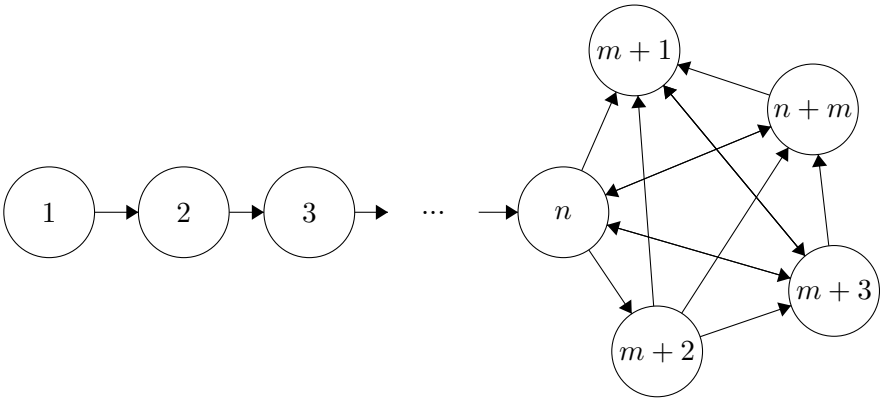
**4-pre)**

Diciamo palloncino un frame $(T, \rho)$ dove

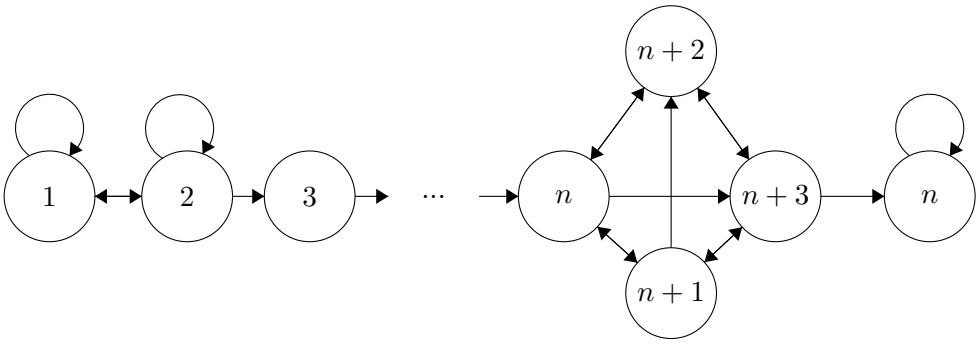
$T = \{\alpha_1, \alpha_2, ..., \alpha_n, \alpha_{n+1}, ..., \alpha_{n+m}\}$ e

$i.j \in \rho \iff i < j$ *oppure* $i, j \geq n$

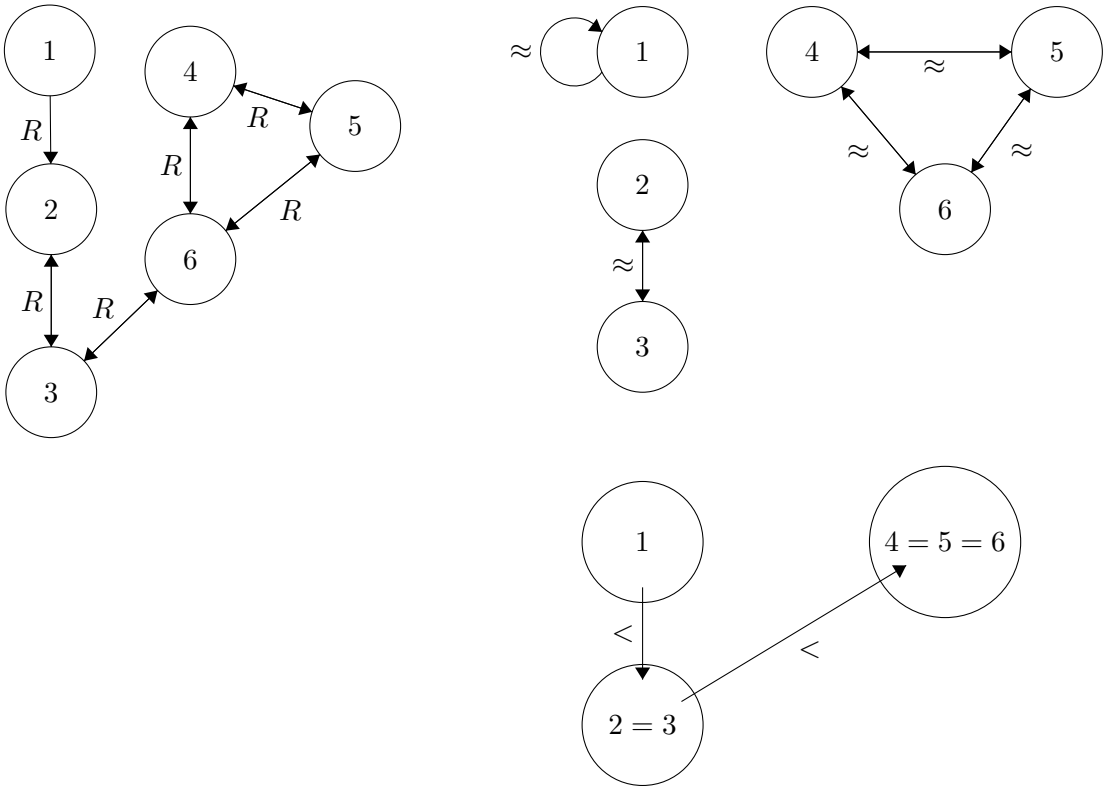
Sostanzialmente il grafo di $\rho$ si presenta nella seguente forma (a meno degli archi che esprimono il fatto che $\rho$ è transitiva).




**4)**
Si vuole trovare un modello a palloncino $P$ che sia modello di $\Omega$, in cui $P \not\models a$, e tale che $P$ abbia tutte le proprietà di $M_3$
$M_3$ potrebbe presentare dei "grovigli" di questo tipo:



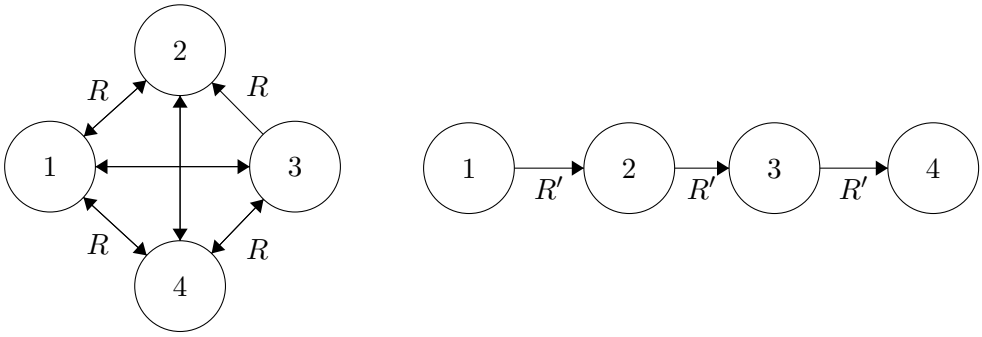

L'idea di questo punto 4 è "sciogliere" questi grovigli.
Sia $M_3 = (S, R, V)$, introduciamo una relazione $\approx \subseteq S \times S$
$\alpha \approx \beta$ se e solo se: $(\alpha R \beta)$ *e* $(\beta R \alpha)$ *oppure* $\alpha = \beta$
$\approx$è una relazione di equivalenza infatti:
è riflessiva per costruzione
è simmetrica infatti: $\alpha \approx \beta$ $(\alpha \neq \beta)$se e solo se: $(\alpha R \beta)$ *e* $(\beta R \alpha)$ se e solo se $\beta \approx \alpha$
è transitiva infatti: $\alpha \approx \beta$, $\beta \approx \gamma$ se e solo se: $(\alpha R \beta)$ *e* $(\beta R \alpha)$ e $(\gamma R \beta)$ *e* $(\beta R \gamma)$, per la transitività di $R$ si ha anche $(\alpha R \gamma)$, $(\gamma R \alpha)$ da cui: $\alpha \approx \gamma$
Per questi motivi $\approx$ è una relazione d'equivalenza, e come tale partiziona l'insieme $S$ e ne definisce un insieme quoziente $S/\approx$
Chiamiamo R-cluster la classe di equivalenza $C_\alpha$ di $\alpha$, e definiamo in modo abbastanza naturale la relazione di $\leq$nel modo seguente:
$C_\alpha \leq C_\beta$ se e solo se: $\alpha R \beta$ oppure $C_\alpha = C_\beta$
$C_\alpha < C_\beta$ se e solo se: $\alpha R \beta$ e $C_\alpha \neq C_\beta$



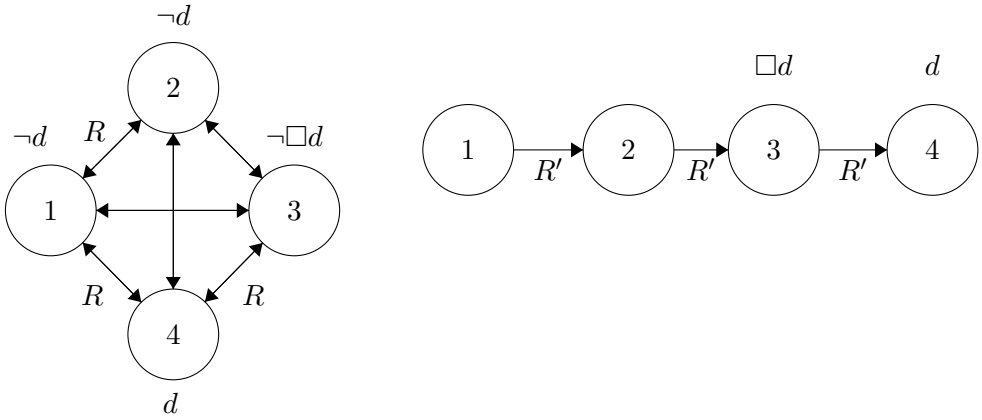

Se un R-cluster C contiene più di un elemento, la relazione R è riflessiva su $C$ e si ha $C \leq C$, infatti detti $\alpha$ e $\beta$ due elementi di $C$ si ha $\alpha R \beta$ e $\beta R \alpha$ quindi, per la transitività di $R$ $\alpha R \alpha$,
inoltre $C = C_\alpha \leq C\alpha = C$.
Se non è $C \leq C$, l'R-cluster $C$ si dice degenere ed è formato da un unico elemento $\alpha$ per il quale non risulta $\alpha R \alpha$
Un palloncino può essere visto come una sequenza finita di cluster di cui solo l'ultimo è non degenere. Ma nel nostro modello possono esserci, oltre all'ultimo R-cluster $C_\alpha$, altri R-cluster non degeneri.
Per ricondurmi a un palloncino, a partire da $M_3$ considero la relazione $R'$ che ordina in modo arbitrario i mondi appartenenti a uno stesso R-cluster che non sia l'ultimo.
$R'$ è così definita:

- Se $\alpha, \beta$ appartengono a cluster diversi allora $(\alpha, \beta) \in R'$ se e solo se $(\alpha, \beta) \in R$
- Se $\alpha, \beta$ appartengono all'ultimo cluster $(\alpha, \beta) \in R'$
- Se $\alpha, \beta$ appartengono allo stesso cluster, e non è l'ultimo, detti $\gamma_1, \gamma_2, \ldots, \gamma_n$, si pone $\gamma_i R' \gamma_j$ se e solo se $i < j$.
- $(\alpha, \alpha) \notin R'$ (tolgo gli autoanelli)

A questo punto abbiamo un palloncino $P$ costruito su $S$,$R'$, $V$, ed è lecito chiedersi se $M_3 \models a$ se e solo se $P \models a$.
Questo è ovviamente vero se $a$ non presenta connettivi modali.
Supponiamo allora che $a$ sia del tipo $\Box d$.
Dato che$R' \subseteq R$,




se $\Box d$ è vera in un mondo $\beta$ di $M_3$, $\Box d$ è vera anche nel mondo $\beta$ di $M$' ($R'$ ha meno archi quindi è più facile per $\Box x$ essere soddisfatta)
Sia allora $\Box d$ vera in un mondo $\beta$ di $M$' e supponiamo che $\Box d$ non sia vera nel mondo $\beta$ di $M_3$.
Se è così, $d$ dovrà allora risultare falsa in un mondo $\gamma$ tale che $(\beta, \gamma) \in R$ mentre $(\beta, \gamma) \notin R$'.




Ovviamente se $(\beta, \gamma) \in R$ ma $(\beta, \gamma) \notin R$', i mondi $\beta, \gamma$ devono appartenere ad uno stesso R- cluster che non è l'ultimo. (infatti se $(\beta, \gamma) \in R$ allora sono nello stesso cluster, che viene "sciolto" in R')
Si può ora far uso dello Z-lemma che garantisce l'esistenza di un mondo $\delta$ in un R-cluster $C_\delta$ tale che $C_\beta < C_\delta$ in cui $d$ non è vera (lo Z-lemma sarà enunciato e dimostrato nel seguito).
Ma $C_\beta < C_\delta$ implica $(\beta, \delta) \in R$' e dunque $\Box d$ non sarebbe vera nel mondo $\beta$ del modello M', contro la nostra supposizione.

Dunque avendo dimostrato nel passo 3 che $a$ non è vera nel mondo $\alpha$ del modello $M_3$, abbiamo che $a$ non è vera nel mondo $\alpha$ del modello $M$', costruito su un palloncino e quindi $a$ non è valida su ogni palloncino.
**5)** Esiste un p-morfismo suriettivo da $(\omega, <)$ a un palloncino P.
Sia P : $(T, \rho)$ dove
$T = \{\alpha_1, \alpha_2, ..., \alpha_n, \alpha_{n+1}, ..., \alpha_{n+m}\}$ e
$i.j \in \rho \iff i < j$ *oppure* $i, j \geq n$
L'idea è di fare un p-morfismo la cui funzione f : manda i primi $n$ mondi di $\omega$ nel "gambo" e i mondi da $n+1$ in poi nella parte "tonda" del palloncino contando modulo $m$.
Pertanto definiamo $f : \omega \to T$ (ricordando che i mondi sono numerati, sia in $\omega$ che in $T$)
$f(i) = i$ *se* $i \leq n$
$f(i) = n + ((i - n)\ mod\ m)$ *se* $i > n$
$f$ è suriettiva (tutto il codominio $T$ è raggiunto)
Infatti ogni elemento $i \in T$ ha almeno controimmagine $i \in \omega$ (gli elementi nella parte "tonda" del palloncino ne avranno altre)

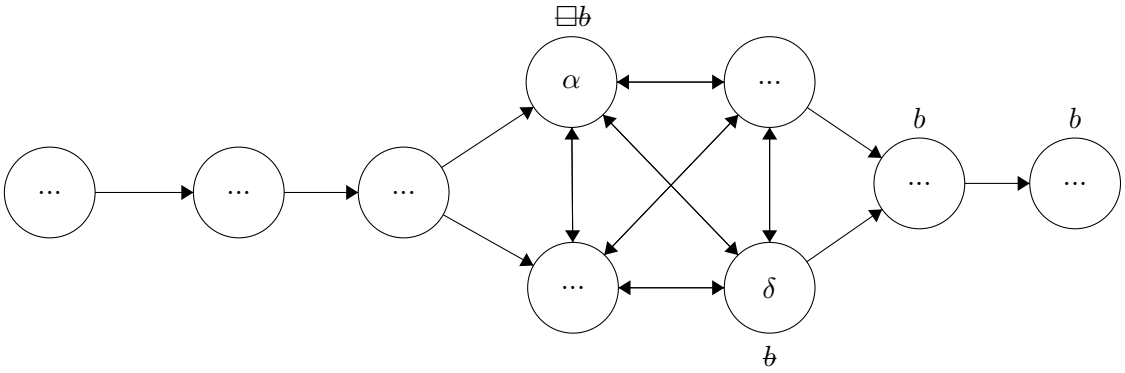
| Proprietà di un p-morfismo |
|---|
| 1) $(\alpha, \beta) \in R_1 \implies (f(\alpha), f(\beta)) \in R_2$ |
| 2) $(f(\alpha), \eta) \in R_2 \implies \exists \beta \in S_1 : f(\beta) = \eta \wedge (\alpha, \beta) \in R_1$ |

1) Se $\alpha, \beta < n$ si ha banalmente $f(\alpha), f(\beta)$ per come è definita $f$ ;
Se$f(\alpha), f(\beta)$ sono nella parte "tonda" la 1) vale perché $f(\alpha), f(\beta)$ in relazione di equivalenza
Se $\alpha$ nel gambo e $\beta$ nella parte "tonda", comunque vale la 1) ricordando la transitività di $\rho$
2) Se $f(\alpha) < \eta$ basta prendere come $\beta$ proprio $\eta$ da $\omega$ e quindi avere $\alpha < \eta$
Se $f(\alpha) > \eta$ posso comunque trovare $\beta$ opportuno sfruttando l'aritmetica modulare.
Quindi se $a$ non è valida su ogni palloncino non è valida su $(\omega, <)$, contro l'ipotesi, pertanto $a$ deve essere un teorema di $\Omega$.

## 7.7 Z-Lemma

Preso un modello $\mu$ finito, seriale, transitivo, connesso, su cui è vero l'assioma Z, se la formula $\Box b$ è falsa in un mondo $\alpha$ che non appartenga all'ultimo R-cluster allora esiste $\beta$ in un cluster successivo a $C_\alpha$ in cui b è falsa.
Ip) $\mu$ finito, seriale, transitivo, connesso e in cui vale Z. In un cluster $C_\alpha$ esiste un mondo $\alpha$ in cui non vale $\Box b$
Ts) Esiste un mondo $\beta$ appartenente ad un R-cluster $C_\beta$ tale che $C_\alpha < C_\beta$ nel quale $b$ è falsa

Per assurdo, supponiamo:
$\mu \models_\beta b$ per ogni $\beta$ appartenente ai cluster successivi a $C_\alpha$
allora deve valere
$\mu \not\models_\delta b$ in qualche mondo $\delta$ tale che $C_\alpha = C_\delta$




allora, poiché la relazione è transitiva e connessa, abbiamo che $\forall\gamma : \ \gamma R\delta$ (cioè i mondi in $C_\alpha$ e nei cluster precedenti) si ha
$\mu \not\models_\gamma \Box b$
e per questo possiamo dire che vale:
$\mu \models_\gamma \Box b \implies b$
per ogni cluster precedente a $C_\alpha$ e in $C_\alpha$stesso, essendo falso l'antecedente.
Poiché in tutti i mondi successivi è vera $b$, allora in tutti i mondi del modello è vera:
$\mu \models \Box(\Box b \implies b)$
Però applicando a questo punto il modus ponens all'assioma Z e alla precedente abbiamo che vale:
$\mu \models \Diamond\Box b \implies \Box b$
Poiché per tutti i mondi dopo $C_\alpha$ è vera $b$, allora è vera anche $\Box b$
Ma allora in $\alpha$ vale:
$\mu \models_\alpha \Diamond\Box b$
poiché esistono dei mondi raggiungibili in cui è vera $\Box b$
ma allora per Modus Ponens, è vale anche:
$\mu \models_\alpha \Box b$
Assurdo! La tesi allora deve essere valida.

## 7.8 Altre logiche temporali

Ci sono altre due logiche temporali interessanti:

1. K4DLDum, corretta e completa sul frame $(\omega, \leq)$
2. K4DLX corretta e completa sui frame $(\mathbb{Q},<)$ e $(\mathbb{R},<)$

Dove all'assioma Z vengono sostituiti rispettivamente:

- Dum: $\Box(\Box a \implies a) \implies (\Diamond\Box a \implies \Box a)$
- X: $\Box\Box a \implies \Box a$

Come si può notare non si può distinguere un tempo numerabile da un tempo continuo.

*—Marty, non stai pensando quadridimensionalmente!—*

Emmett Brown

*—Sono in ritardo! In arciritardissimo!—*

Bianconiglio

# 8

# Logica Multimodale - Back To The Future

## 8.1 Logiche multimodali

una logica multimodale è una logica che definisce oltre ai normali operatori della logica proposizionale gli operatori:
$[i]$ con $i \in I$
$< i > \equiv \neg[i]\neg$
definita sul frame:
$F = (S, \{R_i \mid i \in I\})$
La semantica di una logica multimodale è la stessa della logica proposizionale per gli operatori comuni, mentre gli operatori box hanno la seguente semantica:
$\mu \models_\alpha [i]a \iff \mu \models_\beta a \forall \beta : (\alpha, \beta) \in R_i$
Chiamiamo assioma $K_i$ la seguente formula:
$K_i$: $[i](a \implies b) \implies ([i]a \implies [i]b)$
Tutte le logiche multimodali normali devono contenere:
gli assiomi $K_i$ $\forall i \in I$
le regole di necessitazione:
$RN_i : \dfrac{a}{[i]a}$ $\forall i \in I$

## 8.2 Futuro e Passato

Possiamo applicare le logiche multimodali al concetto di tempo, per farlo consideriamo il frame:
$F = (S, \{R_P, R_F\})$

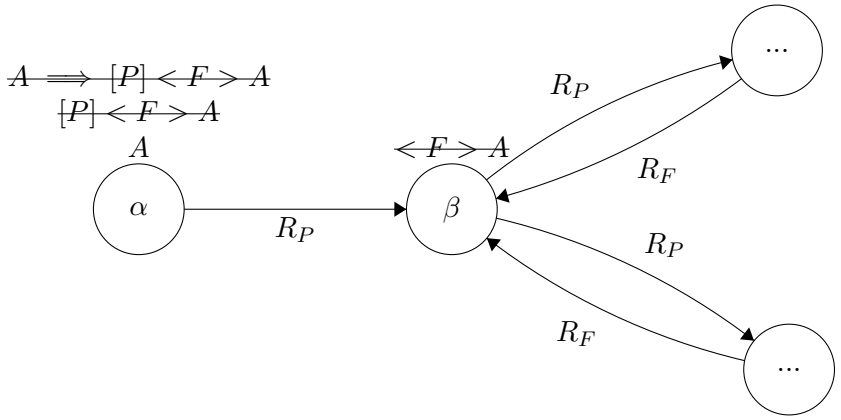
da cui possiamo ricavare gli operatori modali:
$[P]$ e $[F]$
ricordiamo che:
$< P > \equiv \neg[P]\neg$
$< F > \equiv \neg[F]\neg$
Perché le due relazioni rappresentino il tempo che scorre una deve essere l'opposta dell'altra, in modo che la prima relazione rappresenti il futuro, la seconda il passato:
$\alpha R_P \beta \iff \beta R_F \alpha$
$R_p = R_f^{-1}$
Questa proprietà si può dimostrare equivalente ai due assiomi:
$B_{PF} : a \implies [P] < F > a$
$B_{FP} : a \implies [F] < P > a$

### 8.2.1 Dimostrazione

Ip) $\mu \models_\alpha a$ e $\forall \beta : (\alpha, \beta) \in R_P \iff (\beta, \alpha) \in R_F$
Ts) $\mu \models_\alpha a \implies [P] < F > a$

Ogni mondo $\beta$ raggiunge $\alpha$ tramite $R_F$, e quindi:
$\mu \models_\beta < F > a$
allora, usando la regola di necessitazione nel passato, possiamo scrivere:
$\mu \models_\alpha [P] < F > a$
ma poiché per ipotesi in $\alpha$ è vera a:
$\mu \models_\alpha [P] < F > a$
poiché abbiamo preso un $\alpha$ generico, la tesi è dimostrata.
Ip) $\mu \models_\alpha a \implies [P] < F > a$
Ts) $R_F = R_P^{-1}$

per assurdo $R_F \neq R_p^{-1}$
prendiamo allora un mondo $\alpha$ in cui a $R_P$ non corrisponda l'arco inverso nella relazione $R_F$
$V(A) = \{\alpha\}$
allora in $\beta$ poiché non si raggiunge tramite $R_P$ il mondo $\alpha$ vale:
$\mu \not\models_\beta < F > A$
ma poiché $\beta$ è raggiungibile da $\alpha$ tramite $R_P$ abbiamo:
$\mu \not\models_\alpha [P] < F > A$
Ma allora, poiché in $\alpha$ è vera A:
$\mu \not\models_\alpha A \implies [P] < F > A$
Assurdo! allora la tesi è dimostrata.




## 8.3 Frame Temporale

Un frame temporale è un frame così composto:
$F = (S, R_F)$
con $R_F = R_p^{-1}$ e $R_F$ transitiva.
In un frame temporale devono valere gli assiomi:
A1, A2, A3, $K_P$, $K_F$, $4_P$, $4_F$, $B_{FP}$, $B_{PF}$
dove gli assiomi che esprimono la transitività sono:
$4_P$: $[F]a \implies [F][F]a$
$4_F$: $[P]a \implies [P][P]a$
$B_{PF} : a \implies [P] < F > a$
$B_{FP} : a \implies [F] < P > a$

Una logica temporale è una logica normale multimodale nei connettivi modali [F] e [P] che contiene gli schemi $B_{FP}$ $B_{PF}4_P$ $4_F$.
Si dice logica lineare temporale ogni logica normale che contiene la minima logica normale temporale $Kt$
$Kt$ si assiomatizza con $A1,\ A2,\ A3,\ MP,\ K_P,\ K_F,\ B_{PF},\ B_{FP},\ 4_P,\ 4_F,\ RN_P,\ RN_F$

## 8.4 Correttezza, completezza e decidibilità nelle logiche multimodali

Possiamo seguire lo stesso schema di dimostrazioni usato nella logica unimodale per dimostrare la correttezza, completezza e decidibilità delle logiche multimodali. Bisogna tuttavia ridefinire alcuni dettagli, ossia il teorema di raggiungibilità e la Γ-Filtrazione

### 8.4.1 Teorema di Raggiungibilità

$(\alpha, \beta) \in R^\Lambda$
è equivalente a:

$\{a \,|\, [F]a \in \alpha\} \subseteq \beta$
oppure:
$\{< F > b \,|\, b \in \beta\} \subseteq \alpha$

### 8.4.2 Γ-Filtrazione

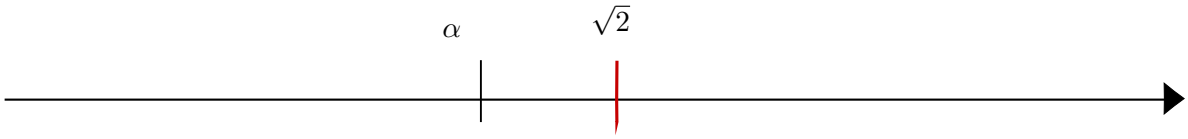
Bisogna, nel caso delle logiche multimodali, ridefinire il concetto di relazione filtrata R'. R' infatti dovrà ora soddisfare le tre seguenti proprietà:
F1) $(\alpha, \beta) \in R \implies ([\alpha], [\beta]) \in R'$
F2) $([\alpha], [\beta]) \in R' \implies (\forall [F]b \in \Gamma\, \mu \models_\alpha [F]b \implies \mu \models_\beta b)$
F3) $([\alpha], [\beta]) \in R' \implies (\forall [P]b \in \Gamma\, \mu \models_\beta [P]b \implies \mu \models_\alpha b)$

## 8.5 Distinzione tra $(\mathbb{Q}, <)$ e $(\mathbb{R}, <)$

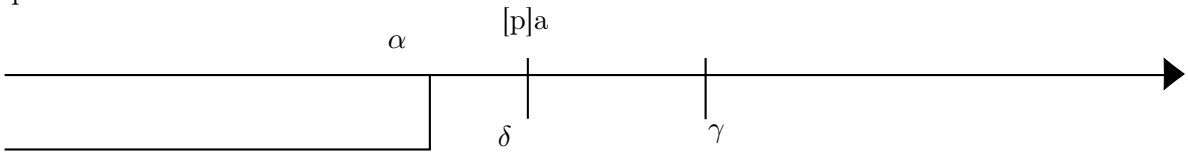
Nella logica unimodale non siamo in grado di distinguere i frame $(\mathbb{Q}, <)$ e $(\mathbb{R}, <)$, entrambi sono espressi dalla logica K4DLX
Per convenzione poniamo:
$\Box a \equiv [P]a \wedge a \wedge [F]a$
L'assioma che esprime la continuità della relazione è il seguente:
Cont: $\Box([P]a \implies < F > [P]a) \implies ([P]a \implies [F]a)$
Si dimostra che:
$(\mathbb{Q}, <) \nvDash Cont$
$(\mathbb{R}, <) \models Cont$

Ip) $V(A) = \{q \in \mathbb{Q} \,|\, q < \sqrt{2}\}$
Ts) $(\mathbb{Q}, <) \nvDash Cont$

Preso $\alpha < \sqrt{2}$, varranno:
$\mu \models_\alpha [P]A$
$\mu \nvDash_\alpha [F]A$
e quindi possiamo scrivere $\forall \alpha < \sqrt{2}$
$\mu \nvDash_\alpha [P]A \implies [F]A$
Tuttavia l'antecedente di Cont è vero, infatti $\forall \alpha < \sqrt{2}$:
$\mu \models_\alpha < F > [P]A$
e quindi l'antecedente di Cont è vero
mentre $\forall \alpha > \sqrt{2}$ vale:
$\mu \nvDash_\alpha [P]A$
e quindi l'antecedente di Cont è ancora vero.
Poiché l'antecedente di Cont è sempre vero, mentre la conseguenza no, allora:
$(\mathbb{Q}, <) \nvDash Cont$
e la tesi è dimostrata.




Ip) $\delta = \max_{\eta \in \mathbb{R}}(\mu \models_\eta A\, \eta < \delta)$
Ts) $(\mathbb{R}, <) \models Cont$
$\forall \alpha > \delta$:
$\mu \not\models [P]A$ da cui $\mu \models$ [P]A $\implies$ [F]A da cui $\mu \models Cont$ dato che il conseguente è vero e quindi non devo controllare l'antecedente.
$\forall \alpha < \delta$ possiamo scrivere:
$\mu \models_\alpha [P]A$
$\mu \not\models_\alpha [F]A$
Tuttavia l'antecedente di Cont è falso, infatti:
$\mu \models_\delta [P]A$
ma poiché non può esistere nessun mondo $\xi > \delta$ in cui sia vera A, essendo $\delta$ massimo, avremo che:
$\mu \not\models_\delta < F > [P]A$
e quindi non potrà che essere che:
$\mu \not\models_\delta [P]A \implies < F > [P]A$
Poiché $\delta$ è raggiungibile da $\alpha$ avremo che:
$\mu \not\models_\alpha \Box([P]A \implies < F > [P]A)$
e quindi $\mu \models_\alpha Cont$, inoltre $Cont$ è vero in $\delta$ dato che l'antecedente è falso perché se $\mu \not\models_\delta [P]A \implies < F > [P]A$, allora anche $\mu \not\models_\delta \Box[P]A \implies < F > [P]A$
allora avremo che in $\alpha$ l'antecedente di Cont è falso solo quando è falso il conseguente, e quindi il teorema è dimostrato.




Questo significa che esiste una differente potenza espressiva tra la logica unimodale e la logica multimodale.

## 8.6 Logica della concorrenza

Una logica che si presta bene a descrivere la concorrenza, cioè un insieme di n diversi processi che agiscono in parallelo, condividendo la memoria, in modo che ogni processo

può alterare i valori di variabili usate anche dagli altri, è la logica nota sotto il nome di LTL (linear temporal logic) o di logica delle concorrenza.
Si introducono l'operatore unario $\circ$ e l'operatore binario $U$
La semantica di questa logica è espressa tramite il frame detto **sequenza di stati** che è costituito da una coppia (S,$\sigma$) dove S è al solito un insieme di stati e $\sigma$ è una funzione suriettiva da $\omega$ ad S e enumera gli stati di S disponendoli in sequenza (con eventuali elementi ripetuti)
La funzione di valutazione V si da in modo consueto, tranne che per i seguenti:
$M \models_j \circ a$, se e solo se $M \models_{j+1} a$
$M \models_j \Box a$, se e solo se $M \models_k a$ per ogni $k \geq j$,
$M \models_j aUb$, se e solo se $M \models_k b$ per qualche $k \geq j$ e $M \models_i a$ per ogni i con$j \leq i < k$.

Questa logica si può assiomatizzare con i seguenti:

$K_\Box : \Box(a \implies b) \implies (\Box a \implies \Box b)$
$K_\circ : \circ(a \implies b) \implies (\circ a \implies \circ b)$
$Fun : \circ\neg a \iff \neg \circ a$
$Mix : \Box a \implies a \wedge \circ\Box a$
$Ind : \Box(a \implies \circ a) \implies (a \implies \Box a)$
$U1 : aUb \implies \Diamond b$
$U2 : aUb \iff b \vee (a \wedge \circ(aUb))$

Si dimostra che LTL è determinata dai frame sequenza di stati.

### 8.6.1 Correttezza di LTL

Gli assiomi A1, A2, A3, $K_\circ$, $K_\Box$ sono validi su tutti i frame, e quindi portano formule vere a formule vere.
L'assioma Fun vale solo se la relazione di raggiungibilità a un passo è una funzione: infatti se non ho stati raggiungibili da uno stato, abbiamo che non vale $\circ a$, e quindi vale $\neg \circ a$, ma $\circ\neg a$ non può valere perché non ci sono stati raggiungibili. Mentre se abbiamo più di uno stato raggiungibile $\circ a$ è falso anche se solo in uno degli stati vale $\neg a$, e quindi $\circ\neg a$ non può essere vero, perché $\neg a$ è vero solo in un successore. Ma per definizione la raggiungibilità a un passo è una funzione.
Mix implica immediatamente lo schema T e quindi la riflessività.
4: $\Box a \implies \Box\Box a$
Per provare la presenza di 4, notiamo che se vale
Mix, vale anche: $\Box a \implies \circ\Box a$ (se vale l'and vale anche uno solo delle due parti)
Per $RN_\Box : \Box(\Box a \implies \circ\Box a)$
Scrivendo Ind (con $\Box a$ come $a$): $\Box(\Box a \implies \circ\Box a) \implies (\Box a \implies \Box\Box a)$
Per MP dalle due precedenti: $\Box a \implies \Box\Box a$
Si può inoltre dimostrare che sono validi gli assiomi:
$L1 : \Box(\Box a \implies b) \vee \Box(\Box b \implies a)$ di cui L è una banale estensione, che indica la debole connessione del frame.

$Dum : (\Box a \implies a) \implies (\diamond\Box a \implies \Box a)$ che svolge lo stesso ruolo di Z per la relazione $\leq$sul frame $\omega$

### 8.6.2 CTL

In questa logica si cerca di modellizzare l'esecuzione di più programmi lanciati in parallelo, e quindi di fatto descrive un frame in cui ogni nodo ha al massimo n figli.
CTL usa i seguenti operatori modali:
in cui $F$ sta per "finally" cioè "prima o poi", $G$ sta per "generally" cioè "sempre" e $X$ sta per "next"" cioè nello stato successivo
$[\forall F]a$: su ogni possibile sequenza di stati successivi all'attuale ce n'è uno in cui $a$ è vera,
$[\exists F]a$: esiste almeno uno stato in una sequenza di stati successivi all'attuale in cui $a$ è vera,
$[\forall G]a$: a vale in tutti gli stati dell'albero
$[\exists G]a$: esiste una sequenza di stati successivi all'attuale tale che $a$ è vero in ogni stato di tale sequenza
$[\forall X]a$: in tutte le esecuzioni, nello stato successivo vale a
$[\exists X]a$: c'è uno stato successivo in cui vale a
$\forall(a\mathcal{U}b)$: in tutte le sequenze di stati successive all'attuale vale $a\mathcal{U}b$
$\exists(a\mathcal{U}b)$: in almeno una sequenza di stati successiva all'attuale in cui vale $a\mathcal{U}b$
Tuttavia sono necessari solo tre operatori, mentre tutti gli altri si possono ricavare, quelli indispensabili sono:
$[\forall X]a$
$\forall(a\mathcal{U}b)$
$\exists(a\mathcal{U}b)$
E infatti si dimostra facilmente che:
$[\forall F]a \equiv \forall(\top\mathcal{U}a)$
$[\exists F]a \equiv \exists(\top\mathcal{U}a)$
$[\forall G]a \equiv \neg\exists(\top\mathcal{U}\neg a)$
$[\exists G]a \equiv \neg\forall(\top\mathcal{U}\neg a)$
$[\exists X]a \equiv \neg[\forall X]\neg a$
Si può ora assiomatizzare ctl usando solo gli operatori normali nel seguente modo:
A1, A2, A3, MP
$K_{\forall x} : [\forall X](a \implies b) \implies ([\forall X]a \implies [\forall X]b)$
$D_{\forall x} : [\exists X]\top$
$\exists U : \exists(a\mathcal{U}b) \iff b \vee (a \wedge [\exists X]\exists(a\mathcal{U}b))$
$\forall U : \forall(a\mathcal{U}b) \iff b \vee (a \wedge [\forall X]\forall(a\mathcal{U}b))$
$RN_{\forall x} : \dfrac{a}{[\forall x]a}$
$\exists - Ind : \dfrac{b \vee (a \wedge [\exists x]c) \implies c}{\exists(a\mathcal{U}b) \implies c}$
$\forall - Ind : \dfrac{b \vee (a \wedge [\forall x]c) \implies c}{\forall(a\mathcal{U}b) \implies c}$

## 8.7 Logica Dinamica

### 8.7.1 Definizione della logica dinamica

La logica dinamica è una logica che si occupa di descrivere le proprietà di un programma.
L'idea è di associare a ogni istruzione $\alpha$ del programma un operatore modale $[\alpha]a$ con il significato "dopo ogni esecuzione di $\alpha$ a è vera".
L'operatore duale $< \alpha > a$ significa invece "esiste una esecuzione di $\alpha$, dopo la quale a è vera".
quindi vale come al solito:
$< \alpha > \equiv \neg[\alpha]\neg$
Le logiche dinamiche si definiscono sul particolare modello:
$\mu = (S, \{R_\alpha \mid \alpha \in Programmi\}, V)$
Definiamo gli insiemi:
$\phi$: insieme delle formule atomiche
$\pi$: insieme dei programmi elementari
Le formule ben formate sono definite come al solito:

- $a \in \phi$
- $\neg a$, $[\alpha]a$, $< \alpha > a$ con $\alpha$ programma
- $a \wedge b$, $a \vee b$, $a \implies b$, $a \iff b$
- null'altro è una formula ben formata.

I programmi sono definiti come:

- $\alpha \in \pi$
- $\alpha; \beta$ ossia la concatenazione di due programmi
- $\alpha \cup \beta$ ossia non-deterministicamente $\alpha$ oppure $\beta$
- $\alpha^*$ossia la ripetizione di $\alpha$
- $a?$ ossia il test di $\alpha$

Le relazioni che descrivono il comportamento dei programmi composti sono espressi dalle seguenti equivalenze:
$R_{\alpha;\beta} \equiv R_\alpha \circ R_\beta$
$R_{\alpha \cup \beta} \equiv R_\alpha \cup R_\beta$
$R_{\alpha^*} \equiv \bigcup_{n \geq 0} R_\alpha^n$
$R_{a?} \equiv \{(s, s) \mid \mu \models_s a\}$

### 8.7.2 Assiomatizzazione della logica dinamica

La logica dinamica modale può essere assiomatizzata aggiungendo agli schemi della logica multimodale normale, ossia gli assiomi A1, A2, A3, $K_{[\alpha]}$ i seguenti assiomi:

Comp: $[\alpha;\beta]a \iff [\alpha][\beta]a$

Union: $[\alpha \cup \beta]a \iff [\alpha] \wedge [\beta]a$

Mix: $[\alpha^*]a \iff a \wedge [\alpha][\alpha^*]a$

Ind: $[\alpha^*](a \implies [\alpha]a) \implies (a \implies [\alpha^*]a)$

Test: $[a?]b \iff (a \implies b)$

### 8.7.3 Logica dinamica concorrente proposizionale

Si può estendere la logica dinamica, normalmente utilizzata per programmi sequenziali, ai programmi concorrenti, aggiungendo l'operatore $[\alpha \cap \beta]a$ che significa "dopo aver eseguito parallelamente $\alpha$ e $\beta$ è vera a".

Per farlo tuttavia, dobbiamo modificare le relazioni del modello, per poter gestire i casi con la concorrenza, e quindi abbiamo che:

$R_\alpha \subseteq S \times \mathcal{P}(S)$

E' quindi necessario cambiare pure la semantica della logica:

$\mu \models_s [\alpha]a \iff \forall T \subseteq S : (s, T) \in R_\alpha \wedge \forall t \in T\, \mu \models_t a$

$\mu \models_s < \alpha > a \iff \exists T \subseteq S : (s, T) \in R_\alpha \wedge \forall t \in T\, \mu \models_t a$

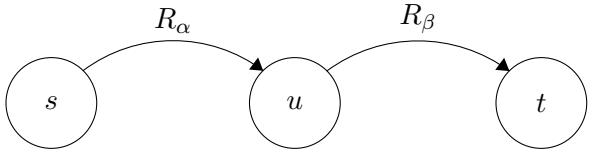
Si nota quindi che:

$[\alpha] \not\equiv \neg < \alpha > \neg$

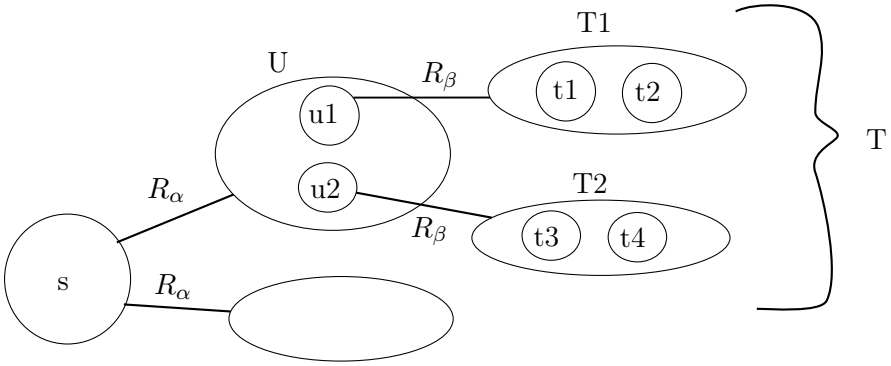
Allora è necessario ridefinire il prodotto tra relazioni:

$(s, T) \in R_\alpha \circ R_\beta \iff \exists U \subseteq \mathcal{P}(S) \wedge (s, U) \in R_\alpha \wedge \forall u \in U \exists T_u : (u, T_u) \in R_\beta \wedge T = \bigcup_{u \in U} T_u$

Il prodotto di relazioni è quindi cambiato, passando dal seguente grafo:




Al seguente grafo:




Bisogna cambiare anche la Relazione di iterazione nel seguente modo:
$R_{\alpha^*} \equiv \bigcup_{n \geq 0} R_\alpha^n$ con $R_\alpha^0 = \{(s, \{s\}) \,|\, s \in S\}$ e $R_\alpha^n = R_\alpha \circ R_\alpha^{n-1}$
Inoltre si introduce la relazione di combinazione, ossia quella che traduce il parallelismo (l'operatore intersezione):
$(s, T) \in R_\alpha \otimes R_\beta \iff T = U \cup V \wedge (s, U) \in R_\alpha \wedge (s, V) \in R_\beta$
Tutto il resto è definito allo stesso modo di prima, a meno di stare attenti agli insiemi di stati, anziché agli stati.

*—Allora dovresti dire quello a cui credi—, riprese la Lepre Marzolina.*
*—È quello che faccio—, rispose subito Alice;*
*—almeno credo a quello che dico, che poi è la stessa cosa.—*
*—Non è affatto la stessa cosa!— disse il Cappellaio.*
*—Scusa, è come se tu dicessi che vedo quello che mangio è la stessa cosa di mangio quello che vedo!—*

Lewis Carroll

# 9 Logica Multimodale Classica

## 9.1 Necessità di una interpretazione differente

Nella logica modale, come l'abbiamo descritta nei precedenti capitoli, sono possibili interpretazioni talvolta sgradite quando si danno significati particolari agli operatori modali.

- $\Box\top$ (schema **N**)

Sembra inappuntabile se $\Box$ si legge come "è possibile"
Ma diventa già discutibile se $\Box$ si legge come "è dimostrabile", infatti il teorema di goedel asserisce che non tutto ciò che è vero è dimostrabile

- $\Box(a \wedge b) \implies \Box a \wedge \Box b$ (schema **M**)

Se diamo a $\Box$ il significato di "non so" notiamo che questa formula non è necessariamente significativa
es. io non so se tizio sia allegro E un astronauta però so che è allegro e quindi il conseguente in questo caso non è vero.

- $\Box a \wedge \Box b \implies \Box(a \wedge b)$ (schema **C**)

Analogo al precedente con "vedo" come $\Box$

## 9.2 Frame Minimali

A questo proposito si definisce diversamente il concetto di frame:

$F = (S, N)$
$S$ sia un insieme di stati
$N : S \to \mathcal{P}(\mathcal{P}(S))$
e in modo naturale il modello $M = (S, N.V)$ che fissa una funzione di verità
Si definisce insieme di verità di $a$ il seguente: $\|a\|^\mu = \{\alpha : \ M \models_\alpha a\}$
Frame e modelli di questo tipo si definiscono minimali
Inoltre diciamo che:
$M \models_\alpha \Box a$ se e solo se: $\|a\|^\mu \in N(\alpha)$
$M \models_\alpha \Diamond a$ se e solo se: $(S - \|a\|^\mu) \notin N(\alpha)$

### 9.2.1 Negazione di N

Ts) $F \not\models \Box T$

Consideriamo un frame con due stati$F(\{\alpha, \beta\}, N)$
$N(\alpha) = \{\{\beta\}\}$
$N(\beta) = \{\{\alpha\}, \{\beta\}, \{\alpha, \beta\}\}$ (solo un esempio, qualunque $N(\beta)$ va bene per la dimostrazione)
$\|T\|^\mu = \{\alpha, \beta\}$ infatti $T$ è vero in ogni mondo, ma $M \not\models_\alpha \Box T$
infatti $\|T\|^\mu \notin N(\alpha)$

### 9.2.2 Validità di N

$F \models \Box \top$ se e solo se $S \in N(\alpha) \, \forall \alpha \in S$
Un frame in cui vale l'assioma N si dice frame con unità.

### 9.2.3 Negazione di M

Ts) $F \not\models \Box(a \wedge b) \implies \Box a \wedge \Box b$

Considero un frame in cui vale l'antecedente:
$S = \{\alpha, \beta\}$
$N(\alpha) = \emptyset$
$N(\beta) = \{\{\alpha, \beta\}\}$
$V(A) = \alpha$, $V(B) = \beta$
Con queste ipotesi si ha: $M \models_\alpha \Box(A \wedge B)$
infatti $\|A \wedge B\|^\mu = \{\gamma : \ M \models_\gamma A \wedge B\} = \emptyset$ perché in nessuno mondo è vera sia A che B e quindi: $\|A \wedge B\|^\mu \in N(\alpha)$
Ora mostro che non vale il conseguente:
$\|A\|^\mu = \{\alpha\}$ e palesemente $\{\alpha\} \notin N(\alpha) = \emptyset$ da cui $M \not\models_\alpha \Box A$ da qui quindi neppure:
$M \not\models_\alpha \Box A \wedge \Box B$

### 9.2.4 Validità di M

Ip)$F \models \Box(a \wedge b) \implies \Box a \wedge \Box b$
Ts)$\forall X, Y$ *Se* $X \cap Y \in N(\alpha)$ *allora* $X \in N(\alpha),\ Y \in N(\beta)$

Considero un frame generico F che abbia $\alpha$ come stato
Siano $X, Y$ due insiemi di stati tali che
$X \cap Y \in N(\alpha)$.
$V(A) = \{s \mid s \in X\}$
$V(B) = \{s \mid s \in Y\}$
Dato che $X \cap Y \in N(\alpha)$
si ha che$\|A \wedge B\|^\mu \in N(\alpha)$, infatti $\|A \wedge B\|^\mu = \{\gamma \ : \ M \models_\gamma A \wedge B\} = \{s \ : \ s \in X \ e \ s \in Y\} = \{s \ : \ s \in X \cap Y\} = X \cap Y$
cioè gli stati in cui è vera $A \wedge B$ sono gli stati in cui vale sia $A$ che $B$ cioè quelli che appartengono sia a $X$ che a $Y$
Si ha quindi $M \models_\alpha \Box(A \wedge B)$ da cui per ipotesi:
$M \models_\alpha \Box a \wedge \Box b$ e cioè: $M \models_\alpha \Box a$ e $M \models_\alpha \Box b$ da cui:
$\|A\|^\mu = \{\alpha : \ M \models_\alpha A\} = X \in N(\alpha)$
$\|B\|^\mu = \{\alpha : \ M \models_\alpha B\} = Y \in N(\alpha)$

Ip)$\forall X, Y$ *Se* $X \cap Y \in N(\alpha)$ *allora* $X \in N(\alpha),\ Y \in N(\beta)$
Ts)$F \models \Box(a \wedge b) \implies \Box a \wedge \Box b$

Supponiamo valga $M \models_\alpha \Box(a \wedge b)$ allora:
$\|a \wedge b\|^\mu \in N(\alpha)$ (per definizione di $\Box$), da cui:
$\|a\|^\mu \cap \|b\|^\mu \in N(\alpha)$, se chiamo $X$ e $Y$ questi insiemi di verità allora ho per ipotesi
$\|a\|^\mu \in N(\alpha)$ e $\|b\|^\mu \in N(\alpha)$,
dalla prima, per definizione di $\Box$ ottengo $M \models_\alpha \Box a$
dalla seconda ottengo $M \models_\alpha \Box b$
quindi complessivamente $M \models_\alpha \Box a \wedge \Box b$

Un frame in cui valga l'assioma M si dice frame supplementato.

### 9.2.5 Negazione di C

Ts) $F \models \Box a \wedge \Box b \implies \Box(a \wedge b)$

Consideriamo un frame con due stati $F(\{\alpha, \beta\}, N)$ e la seguente valutazione:
$N(\alpha) = \{\{\beta\}, \{\alpha\}\}$
$V(A) = \{\beta\}$
$V(B) = \{\alpha\}$
avremo dunque che:
$\mu \models_\alpha \Box a$
$\mu \models_\alpha \Box b$

ma non vale:
$\mu \nvDash_\alpha \Box(A \wedge B)$
infatti:
$\emptyset \nsubseteq N(\alpha)$

### 9.2.6 Validità di C

Ip) $F \models \Box a \wedge \Box b \implies \Box(a \wedge b)$
Ts) $\forall \alpha \in S, \forall X, Y \subseteq S :$ *se* $X \in N(\alpha)$ *e* $Y \in N(\alpha)$ *allora* $X \cap Y \in N(\alpha)$

Poiché vale l'assioma C possiamo scrivere:
$F \models \Box A \wedge \Box B \implies \Box(A \wedge B)$
supponiamo valga l'antecedente, allora supponendo:
$V(A) = \{s \mid s \in X\}$
$V(B) = \{s \mid s \in Y\}$
Avremo che:
$\|A\|^\mu = X$
$\|B\|^\mu = Y$
Ma per modus ponens vale il conseguente, e quindi:
$\mu \models_\alpha \Box(A \wedge B)$
e quindi l'insieme di verità:
$\|A \wedge B\|^\mu \in N(\alpha)$
da cui segue:
$(X \cap Y) \in N(\alpha)$
e la tesi è dimostrata.
Ip) $\forall \alpha \in S, \forall X, Y \subseteq S : X \cap Y \in N(\alpha)$
Ts) $F \models C$

Se l'antecedente è falso, C è vero, per cui consideriamo il caso in cui valga la formula:
$\mu \models_\alpha \Box a \wedge \Box b$
avremo quindi che:
$\|A\|^\mu \in N(\alpha)$
$\|B\|^\mu \in N(\alpha)$
allora possiamo scrivere:
$\|A\|^\mu \cap \|B\|^\mu \equiv \|A \wedge B\|^\mu \in N(\alpha)$

Un frame in cui valga l'assioma C si dice chiuso rispetto all'intersezione.

### 9.2.7 Proprietà dei frame

Un frame si quasi filtro se:

1. È supplementato
2. È chiuso rispetto all'intersezione

Un frame si dice filtro se:

1. È un quasi filtro
2. È un frame con unità

## 9.3 Logiche Classiche

Le logiche classiche sono tutte le logiche valide sui frame minimali. La minima logica classica è la Logica E.
La logica E è definita come la logica che:

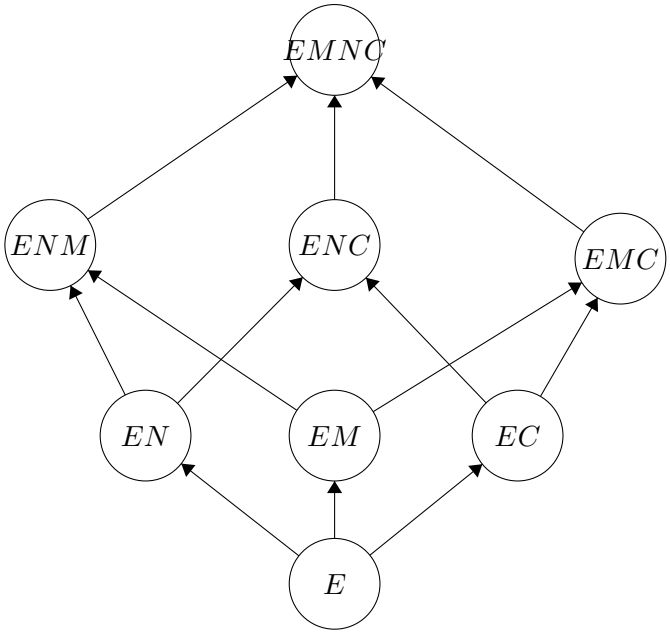
- Contiene tutte le tautologie
- È chiusa rispetto al Modus Ponens
- È chiusa rispetto alla regola RE

**RE**: $\dfrac{a \iff b}{\Box a \iff \Box b}$

Le logiche Monotone sono logiche classiche in cui vale anche la regola RM:
**RM**: $\dfrac{a \implies b}{\Box a \implies \Box b}$

Le logiche Regolari sono logiche classiche in cui vale la regola RR:
**RR**: $\dfrac{a \wedge b \implies c}{\Box a \wedge \Box b \implies \Box c}$

### 9.3.1 Reticolo delle logiche classiche



EM è la minima logica monotona
EMC è la minima logica regolare
$EMNC \equiv K$ è la minima logica normale

**Teorema**

Le logiche normali sono regolari, le logiche regolari sono monotone, le logiche monotone sono classiche.
Ip) Vale K
Ts) la logica è regolare

$\vdash_K a \wedge b \implies c$ – per ipotesi
$\vdash_K \Box(a \wedge b) \implies \Box c$ –definizione 3.c di logica normale
$\vdash_K \Box a \wedge \Box b \implies \Box(a \wedge b)$ – perché è una logica nomale (definizione 3.b)
$\vdash_K \Box a \wedge \Box b \implies \Box c$ – per catena di implicazioni fra le due precedenti
Poiché vale RR, ogni logica normale è regolare
Ip) Vale la regola RR
Ts) Vale la regola RM

$\vdash_\Lambda a \implies b$ – per ipotesi
$\vdash_\Lambda a \wedge a \implies b$ – tautologia
$\vdash_\Lambda \Box a \wedge \Box a \implies \Box b$ – per RR
$\vdash_\Lambda \Box a \implies \Box b$
Poiché vale RM, ogni logica regolare è monotona
Ip) Vale RM
Ts) Vale RE

$\vdash_\Lambda a \iff b$ – per ipotesi
$\vdash_\Lambda a \implies b$
$\vdash_\Lambda b \implies a$
$\vdash_\Lambda \Box a \implies \Box b$ – per RM
$\vdash_\Lambda \Box b \implies \Box a$ – per RM
$\vdash_\Lambda \Box a \iff \Box b$
Poiché vale RE, ogni logica monotona è classica

### 9.3.2 Minima logica monotona

La minima logica monotona è EM, ossia la logica E con l'aggiunta dell'assioma M
Ip) valgono RE e M
Ts) vale RM

$\vdash_\Lambda a \implies b$ – per ipotesi
$\vdash_\Lambda (a \implies b) \implies (a \iff (a \wedge b))$ – per tautologia
$\vdash_\Lambda a \iff (a \wedge b)$ – per MP

$\vdash_\Lambda \Box a \iff \Box(a \wedge b)$ – per RE
$\vdash_\Lambda \Box(a \wedge b) \implies \Box a \wedge \Box b$ – schema M
$\vdash_\Lambda \Box a \implies \Box a \wedge \Box b$ – per catena implicazioni dalle due precedenti
$\vdash_\Lambda \Box a \implies \Box b$ – perché se $x \implies y \wedge z$ vale anche $x \implies y$
E il teorema è dimostrato
Ip) vale RM
Ts) Vale M

$\vdash_\Lambda a \wedge b \implies a$ – per tautologia
$\vdash_\Lambda a \wedge b \implies b$ – per tautologia
$\vdash_\Lambda \Box(a \wedge b) \implies \Box a$ – per RM
$\vdash_\Lambda \Box(a \wedge b) \implies \Box b$ – per RM
$\vdash_\Lambda \Box(a \wedge b) \implies \Box a \wedge \Box b$
Che è lo schema M, e la tesi è dimostrata

### 9.3.3 Minima logica regolare

La minima logica regolare è EMC, ossia la logica E con l'aggiunta degli assiomi M e C
Ip) valgono RE, M e C
Ts) vale RR

Sappiamo già che da RE e M ottengo RM.
$\vdash_\Lambda a \wedge b \implies c$ – per ipotesi
$\vdash_\Lambda \Box(a \wedge b) \implies \Box c$ – per RM
$\vdash_\Lambda \Box a \wedge \Box b \implies \Box(a \wedge b)$ – schema C
$\vdash_\Lambda \Box a \wedge \Box b \implies \Box c$ – per catena di implicazioni dalle due precedenti
Poiché vale RR, la tesi è dimostrata.
Ip) vale RR
Ts) valgono M e C

Poiché abbiamo RR, sappiamo che vale RM, ma allora sappiamo già che vale RE e l'assioma M.
$\vdash_\Lambda a \wedge b \implies a \wedge c$ – per tautologia
$\vdash_\Lambda \Box a \wedge \Box b \implies \Box a \wedge c$ – per RR
Abbiamo trovalo lo schema C, quindi la tesi è dimostrata.

### 9.3.4 Minima logica normale

La minima logica normale è EMCN, ossia la logica E con l'aggiunta dei tre assiomi M, C e N.
Questa logica è equivalente alle logiche normali, ossia i tre assiomi insieme sono equivalenti alla logica K.
Ip) valgono RE, M, C, N

Ts) vale la logica K

Possiamo notare che, per definizione della logica K, devono valere:

- N
- C
- $(a \implies b) \implies (\Box a \implies \Box b)$

Resta soltanto l'ultima affermazione da dimostrare.
Sappiamo già che con RE e M otteniamo RM, e quindi:
$\vdash_\Lambda a \implies b$ – per ipotesi
$\vdash_\Lambda \Box a \implies \Box b$ – per RM
Ip) vale K
Ts) vale RE, M, C e N.

Poiché siamo in una logica normale vale RR e quindi valgono RE, M e C.
N vale per punto 1 della definizione di logica normale.
La tesi è quindi dimostrata.

## 9.4 Relazione Tra Frame Minimali E Standard

Poiché le logiche classiche contengono le logiche normali, è possibile delineare la relazione tra i frame minimali e i frame standard.

### 9.4.1 Frame Aumentato

Si dice frame aumentato, un frame F supplementato tale che:
$\forall \alpha \in S \, sia \; Z \equiv \bigcap_{Y \in N(\alpha)} Y \; allora \; Z \in N(\alpha)$
Un frame aumentato è un filtro:

1. è supplementato
2. è chiuso rispetto all'intersezione
3. non è vuoto (c'è sempre almeno il vuoto)

### 9.4.2 Teorema

Per ogni modello minimale aumentato $\mu^a = (S, N, V)$ esiste un modello standard $\mu^s = (S, R, V)$ tale che, $\forall \alpha \in S$ e $\forall a \in f.b.f$
$\mu^a \models_\alpha a \iff \mu^s \models_\alpha a$
Questo teorema è banalmente vero per le formule che non utilizzano i connettivi modali, poiché S e V sono identiche. Dobbiamo dimostrarlo solo nel caso di utilizzo dei connettivi

modali, e poi per induzione sulla complessità della formula, si può verificare che il teorema è valido in generale.
Ip) $\mu^a \models_\alpha a$
Ts) $\exists \mu^s : \mu^s \models_\alpha a \iff \mu^a \models_\alpha a$

Supponiamo di scegliere R tale che:
$(\alpha, \beta) \in R \iff \beta \in \bigcap_{Y \in N(\alpha)} Y$
abbiamo che:
$\mu^a \models_\alpha \Box b \iff \|b\|^\mu \in N(\alpha)$
ma:
$\|b\|^\mu \supseteq \bigcap_{Y \in N(\alpha)} Y$
allora possiamo affermare che:
$\forall \beta : (\alpha, \beta) \in R, \mu^s \models_\beta b$
e quindi vale:
$\mu^s \models_\alpha \Box \beta$
viceversa, se è vero:
$\mu^s \models_\alpha \Box b$
allora avremo che:
$\mu^s \models_\beta b, \forall \beta : (\alpha, \beta) \in R$
ma per definizione:
$\{\beta \,|\, (\alpha, \beta) \in R\} = \bigcap_{Y \in N(\alpha)} Y$
e allora:
$\|b\|^{\mu^s} = \|b\|^{\mu^a} \supseteq \bigcap_{Y \in N(\alpha)} Y$
e dunque:
$\mu^a \models_\alpha a$
Ip) $\mu^s \models_\alpha a$
Ts) $\exists \mu^a : \mu^a \models_\alpha a \iff \mu^s \models_\alpha a$

Supponiamo di scegliere N tale che:
$X \in N(\alpha) \iff X \supseteq \{\beta \,|\, (\alpha, \beta) \in R\}$
supponiamo che valga:
$\mu^s \models_\alpha \Box b$
e quindi:
$\mu^s \models_\beta b$
ma allora abbiamo che:
$\|b\|^{\mu^s} \supseteq \{\beta \,|\, (\alpha, \beta) \in R\}$
ma allora abbiamo, per come abbiamo definito N:
$\|b\|^{\mu^a} \in N(\alpha)$
e quindi:
$\mu^a \models_\alpha \Box b$
viceversa, supponiamo di avere:

$\mu^a \models_\alpha \Box b$
allora per definizione avremo che:
$\|b\|^{\mu^a} \in N(\alpha)$
ma per come abbiamo definito N, si ha che:
$\|b\|^{\mu^a} \supseteq \{\beta \,|\, (\alpha, \beta) \in R\}$
ma allora abbiamo che:
$\|b\|^{\mu^a} = \|b\|^{\mu^s}$
da cui si ricavano banalmente:
$\mu^s \models_\beta b$
$\mu^s \models_\alpha \Box b$
e la tesi è dimostrata.

*—Non so spiegarlo chiaramente,*
*perchè non è chiaro neanche a me—*

Alice

# 10 Logiche Descrittive

## 10.1 Introduzione - Logica $\mathcal{AL}$

Le DL sono una famiglia di logiche per la rappresentazione della conoscenza che possono essere utilizzate per rappresentare conoscenza terminologica, dando ad essa una semantica formale ben definita.
Un sistema di rappresentazione della conoscenza (KR) fornisce i mezzi per definire, gestire, manipolare e ragionare su basi di conoscenza (KB).
In una KB ci sono T-Box e A-Box
I TBox descrivono la terminologia della KB (concetti, ruoli atomici e concetti composti), gli ABox sono asserzioni su individui della KB
TBox es. $Madre \equiv Donna \sqcap Genitore$
ABox es. $Donna(Paola)$

La famiglia di logiche descrittive più utilizzata è la famiglia $\mathcal{AL}$ (Attributive Language).
Nella logica $\mathcal{AL}$ (logica descrittiva tra le più semplici) ci sono:

**A,B,C** concetti

**R** ruoli

$\neg$ negazione (solo di concetti atomici)

$\sqcap$ di concetti

I concetti sono:

- Concetti atomici A,B
- $\top$, $\bot$
- negazione di concetti atomici: $\neg A$
- and di concetti: $C \sqcap D$
- quantificazioni: $\forall R.C$, $\exists R.\top$

Un'interpretazione I di una base di conoscenza´e una coppia $I =< \Delta^i, \cdot^I >$ composta da un dominio di interpretazione $\Delta$I, detto dominio di I e da una funzione di interpretazione $\cdot^I$ che associa:
ad ogni **nome** di individuo un elemento:
$a^I \in \Delta^I$
ad ogni **concetto** C un sottoinsieme di $\Delta^I$
$I:\ C \to C^I \subseteq \Delta^I$
e ad ogni **ruolo** un sottoinsieme di $\Delta$I $\times$ $\Delta$I :
$R:\ R^I \subseteq \Delta^I \times \Delta^I$
I rouli sono quindi relazioni binarie, una volta interpretati
es. $(Peter,\ Chris)^I \in HaFiglio^I$
Inoltre:
$\bot^I = \emptyset$, $\top^I = \Delta^I$
$(C \sqcap D)^I = C^I \cap D^I$
$(\forall R.C)^I = \{a^I \in \Delta^I :\ (a^I, b^I) \in R^I \implies b^I \in C^I\}$
es. $\forall Possiede.Cosa$ cioè se a possiede un oggetto del dominio quello deve essere una cosa (slavery is bad)
$(\exists R.C)^I = \{a^I \in \Delta^I :\ \exists b \in \Delta^I :\ (a^I, b^I) \in R^I \wedge b^I \in C^I\}$

es. $\exists HaFiglio.Femmina$ cioè l'insieme dei genitori con una figlia femmina

### 10.1.1 Varianti di $\mathcal{AL}$

Indebolendo la logica $\mathcal{AL}$ si ottengono le logiche poco descrittive della famiglia $\mathcal{FL}$:

- $\mathcal{FL}$- è ottenuta da $\mathcal{AL}$ eliminando la negazione atomica •
- $\mathcal{FL}_0$è ottenuta da $\mathcal{FL}-$ eliminando anche la quantificazione esistenziale

La logica $\mathcal{AL}$ può essere estesa aggiungendo alcuni costruttori:

- costrutto $\mathcal{U}$ disgiunzione dei concetti $C \sqcup D$
- costrutto $\mathcal{E}$ quantificazione esistenziale qualificata $\exists R.C$
- costrutto $\mathcal{C}$ complemento di concetti complessi $\neg C$

- costrutto $\mathcal{N}$ cardinalità di un ruolo

$(\leq nR)^I = \{a^I : \|\{b^I : (a^I, b^I) \in R^I\}\| < n\}$
es. $(\leq 2HaFiglio)^I$ è l'insieme delle persone un numero di figli minore o uguale a 2.

## 10.2 Confronti fra logiche

In modo analogo a quanto si era fatto con le logiche derivate da K, denotiamo con ALX la logica AL a cui si aggiunge il costrutto X

### 10.2.1 Equivalenza $\mathcal{ALUE}$ed $\mathcal{ALC}$

Dimostriamo che $\mathcal{ALUE} \equiv \mathcal{ALC}$

IP) $\mathcal{UE}$
Ts)$\mathcal{C}$

Si vuole mostrate che a partire in$\mathcal{ALUE}$ posso fare tutto ciò che faccio in $\mathcal{ALC}$, il che si riduce a mostrare che in $\mathcal{ALUE}$posso fare negazioni di concetti qualsiasi.
Questo è immediato per i concetti atomici la cui negazione è per definizione in $\mathcal{AL}$
$\neg\top \equiv \bot$, $\neg\bot \equiv \top$
Per negare l'and di due concetti:
$\neg(D \sqcap E) \equiv \neg D \sqcup \neg E$ che sono concetti più semplici di cui ricorsivamente posso costruire la negazione
$\neg\forall R.C \equiv \exists R.\neg C$
Con queste semplici trasformazioni posso rendere ricorsivamente più semplice una qualsiasi formula di $\mathcal{ALC}$ fino a portarla in una formula di $\mathcal{ALUE}$

IP) $\mathcal{C}$
Ts)$\mathcal{UE}$

Sfruttando De Morgan possiamo scrivere:
$D \sqcup E \equiv \neg(\neg D \sqcap \neg E)$
$\exists R.C \equiv \neg(\forall R.\neg C)$

### 10.2.2 Confronto con logica del prim'ordine

È possibile vedere le logiche $\mathcal{AL}$,$\mathcal{ALC}$,$\mathcal{ALN}$, (deve essere con identità nel caso di $\mathcal{N}$)

- A è un concetto: $a(x)$
- R è un ruolo: $R(x, y)$
- $a$ è un individuo: $a$ è una costante

Notiamo che ci sono due sole variabili libere e il dominio è fissato (controllare) la logica del prim'ordine è decidibile.

$\neg C$**:** $\neg C(x)$

$C \sqcap D$: $C(x) \vee D(x)$

$\forall R.C$**:** $\forall y : (R(x,y) \implies C(y))$

$\exists R.C$ : $\exists y : (R(x,y) \implies C(y))$

$\leq nR,$ la logica deve essere con unità cioè avere un predicato di uguaglianza E

$\exists x_1,\ x_2, ...,\ x_{n+1}(R(x,x_1) \wedge R(x,x_2) \wedge \ldots R(x,x_n)$

$\implies E(x_1,x_2) \vee E(x_1,x_2) \vee ..... \bigvee_{1 \leq i \leq j \leq n+1} E(x_i,x_j)$

### 10.2.3 Confronto con logica multimodale

L'espressività di ALC è la stessa di $K_n$
Infatti ogni ruolo $R_i$ si può mettere in corrispondenza con $[R_i]c$

## 10.3 Terminologia

- Definizione:

Una definizione associa a un concetto atomico un concetto complesso (non atomico) es. $Parent \equiv Father \sqcup Mather$, il concetto atomico viene detto anche simbolo nominale

- Simbolo di base (o nominale):

I ruoli e i concetti che appaiono solo nelle parti destre delle definizioni

- Interpretazione di base:

Un'interpretazione di una T-Box che interpreta solo i simboli di base

- Aciclico:

Nessun simbolo nominale usa sé stesso

- T-Box definitorio:

La sua interpretazione si estende in modo unico a una interpretazione di tutto il t-box (estesa)
Un T-Box è definitorio se è possibile costruirne uno equivalente ma aciclico

Non sono definitorie alcune T cicliche es.
$Human \equiv Animal \sqcap \forall hasParent.Human$

Ma alcune T cicliche sono definitorie es.
$A \equiv B \sqcap \exists R.(A \sqcap \neg A)$ che è equivalente a:
$A \equiv B \sqcap \exists R.(\bot)$

## 10.4 Terminologia generalizzata

A volte è possibile aggiungere nuovi operatori qua descritti.
**Inclusione**
Si possono usare T-Box del tipo:
$A \sqsubseteq B$ che vale se e solo se $A^I \subseteq B^I$
Una terminologia T generalizzata (cioè che contiene assiomi di inclusione) può essere tradotta in una forma T normalizzata sostituendo le forme del tipo:
$Woman \sqsubseteq Person$ con $Woman \equiv \underline{Woman} \sqcap Person$ dove $\underline{Woman}$ è un nuovo simbolo base (che denota qualità specifiche)
In termini di espressività, le due forme sono equivalenti
Ogni modello di $T$ è anche modello di $\underline{T}$
Qualsiasi interpretazione base di un modello di $T$ è anche interpretazione base di un modello di $\underline{T}$
Così facendo si ha che: $Woman^I \subseteq Person^I$ e quindi $Woman^I \equiv Person \cap (\underline{Woman})^I$
**Set**
$Set{a_1, a_2, \ldots, a_n}^I = \{a_1^I, a_2^I, \ldots, a_n^I\}$
**Fills**
$Fills\ r\ c$ sono gli individui che sono in relazione tramite $r$ agli individui identificati da $c$
es. $FILLS\ :\ Child\ Chris$ sono tutti gli individui con figlio "Chris"
$(Fills\ R : a)^I = \{b \in \Delta^I\ :\ (a^I, b^I) \in R^I\}$

### 10.4.1 Note

$\exists R.C$ si può sostituire con $\exists R.Set(a)$
Posso pensare i T-Box come composti solo di definizioni
Il T-Box può essere tolto del tutto specificando completamente le definizioni nell'A-Box
Normalmente nelle Logiche Descrittive si fa l'UNA: l'unicity name assunction cioè si assume che se si usano due nomi come a, b, allora $a^I \neq b^I$

## 10.5 Servizi di Reasoning

I servizi di reasoning si propongono di risolvono quattro tipi di problemi
**Soddifisfacibilità:** Un concetto C si dice soddisfacibile rispetto al T-Box T se esiste un modello di T tale che $C^I$ non è vuoto
**Sussunzione:** Un concetto C è sussunto da un concetto D, in T se $C^I \subseteq D^I$ per ogni modello di T
**Equivalenze:** Due concetti C e D si dicono equivalenti rispetto a T se $C^I = D^I$per ogni modello di T
**Disgiunzione:** Due concetti C e D sono disgiunti rispetto a T se $C^I \cap D^I = \emptyset$ per ogni modello di T
Mostriamo che una KB che fornisce il servizio di sussunzione risolve anche gli altri tre problemi, infatti:

$C$ è insoddisfacibile se e solo se $\bot \sqsubseteq C$
$C, D$sono equivalenti se $C \sqsubseteq D$ e $D \sqsubseteq C$
$C, D$sono disgiunti se $C \sqcap D \sqsubseteq \bot$

## 10.6 Feauture Logic

Le logiche descrittive più semplici appartengono alla famiglia della features logics ($\mathcal{FL}$ in breve) e sono ottenute indebolendo la più´famosa logica $\mathcal{AL}$ inibendo i costruttori di concetto più complessi.
La più semplice di queste è $\mathcal{FL}_0$ che si ottiene da $\mathcal{AL}$ togliendo $\bot$ e $\exists$
Un concetto in **forma normale** è del tipo:
$A_1 \sqcap A_2 \sqcap \ldots A_n \forall R_1.C_1 \sqcap \forall \dot{R}_2.C_2 \cdots \sqcap \forall R_m.C_m$
dove $C_j$ sono concetti in forma normale e $R_j$ sono ruoli atomici

Posso scrivere qualsiasi concetto in questo modo con l'accortezza di:
togliere i duplicati: $A_i \neq A_j$
"sciogliere" i ruoli con intersezioni:
$\forall R.(C \sqcap D) \equiv \forall R.C \sqcap \forall R.D$
Siano C e D due concetti $FL_0$ in forma normale:

$C \equiv A_1 \sqcap \cdots \sqcap A_m \sqcap \forall R1.C1 \sqcap \forall Rn.Cn$
$D \equiv B1 \sqcap \cdots \sqcap Bk \sqcap \forall S1.D1 \sqcap \forall Sl.Dl$

allora $C \sqsubseteq D$ se e solo se

1. per ogni i, $1 \leq i \leq k$ esiste un j, $1 \leq j \leq m$ per il quale $Bi = Aj$.
2. per ogni i, $1 \leq i \leq l$ esiste un j, $1 \leq j \leq n$ per il quale $Si = Rj$ e$Cj \sqsubseteq Di$.

### 10.6.1 Varianti

Ad $\mathcal{AL}_0$può essere aggiunto il concetto $\bot$, ottenendo $\mathcal{AL}_\bot$e la forma normale viene a essere la stessa di prima a cui si aggiunge l'opportunità per un concetto di essere o$\bot$
Notiamo che $\bot \sqsubseteq C$, per ogni $C$
Ad $AL_0$ si può aggiungere la negazione di concetti atomici ottenendo $\mathcal{AL}_\neg$
Notiamo che $\bot \equiv A \wedge \neg A$, quindi $\mathcal{AL}_\neg$contiene strettamente$\mathcal{AL}_0$
In $ALC$ per verificare se $C \sqsubseteq D$ possiamo controllare che $C \sqcap \neg D$ si insoddisfacibile
Per controllare $C \equiv D$ possiamo quindi testare $C \sqcap \neg D$ e $D \sqcap \neg C$.

## 10.7 A-Box Reasoning

I servizi di reasoning di A-Box sono:
**Consistenza**: Un A-Box è consistente in un modello T-Box T se c'è un'interpreatzione che sia modello sia di T che di A

**Instance Checking**: Un individuo è istanza di un concetto C rispetto a un A-Box A se è membro dell'insieme C. $A \models C(a)$ il che vale se e solo se $A \cup \{\neg C(a)\}$ è insoddisfacibile
**Instance Retrivial**: Trova tutti gli individui che sono istanze di una data descrizione
**Problema di Realizzazione**: Trova il concetto più specifico a cui un individuo appartiene

### 10.7.1 Variante

T-Box ed A-Box si possono arricchire con $C \implies D$ cioè: per ogni individuo $a$ cui è noto $C(a)$ si ha anche $D(a)$.
Notiamo che NON vale $\neg D \implies \neg C$

*—Bu-burro, certo, ci vuole un po'*
*di burro! Buuuurro!—*
*—Bu-bu-burro? Eccolo!—*
*—Oh, grazie! Burro! Benissimo!—*
Lewis Carroll

# 11 Logica Modale Del Prim'Ordine

## 11.1 La Sintassi delle Logiche Modali del Prim'Ordine

Una logica modale del prim'ordine è definita sul seguente alfabeto:

- Costanti $(k_1, ..., k_n)$
- Variabili $(x_1, ..., x_n)$
- Lettere predicative $A_i^j$
- Connettivi logici: $\neg$, $\wedge$, $\vee$, $\implies$, $\iff$
- Quantificatori universali ed esistenziali: $\forall x_i$, $\exists x_i$
- Connettivi modali $\Box$, $\diamond$
- Parentesi ), (

Si chiamano termini le costanti e le lettere predicative, gli indichiamo come $t_i$
Si chiamano formule atomiche, le formule del tipo:
$A_i^n(t_1, ..., t_n)$
Le formule ben formate sono definite come al solito:

- Le formule atomiche sono formule ben formate
- $a$, $\neg a$, $(\forall x)a$, $(\exists x)a$, $\Box a$, $\diamond a$ sono furmule ben formate
- $a$, $b$, $(a \wedge b)$, $(a \vee b)$, $(a \implies b)$, $(a \iff b)$ sono formule ben formate
- Null'altro è una formula ben formata.

## 11.2 Semantica della Logica Modale del Prim'Ordine

### 11.2.1 Frame e modello

Definiamo un frame della logica modale del prim'ordine il seguente:
F = (S, R, D)
in cui:

- S è insieme dei possibili stati
- R è la relazione di raggiungibilità tra gli stati
- D è la funzione che associa a ogni stato il suo dominio.

Chiamiamo modello il seguente:
$\mu = (S, R, D, I)$
dove I è la funzione di interpretazione, che può essere vista come l'unione di due funzioni separate:

- $I_c$ è la funzione di interpretazione delle costanti, ossia che in ogni stato associa al valore di una costante un valore del dominio in quello stato
- $I_P$ è la funzione di interpretazione dei predicati, che associa a un predicato una relazione n-aria tra gli elementi del dominio

### 11.2.2 Tipi di dominio

I domini nella logica modale del pr'imordine possono essere visti in verie maniere differenti, a seconda che gli stati abbiano domini uguali o diversi tra loro.
In generale, infatti ogni stato potrebbe avere domini a piacere differenti.
Si dicono domini costanti quei domini per cui vale:
$\forall \alpha, \beta \in S \, D_\alpha = D_\beta$
Si dicono domini variabili monotoni i domini per cui vale:
$\forall \alpha, \beta \in S \, D_\alpha \subseteq D_\beta$
Si dicono domini variabili antimonotoni i domini per cui vale:
$\forall \alpha, \beta \in S \, D_\alpha \supseteq D_\beta$
I domini monotoni sono i domini in cui "nulla si crea", mentre i domini antimonotoni sono quelli in cui "nulla si distrugge". Un dominio costante è sia monotono che antimonotono, per cui gli elementi dell'insieme rimangono immutabili.
Se chiamiamo P l'insieme dei predicati, C l'insieme delle costanti, e $R_D$ l'insieme di tutte le possibili relazioni sui domini D, possiamo definire l'interpretazione I come:
$I_c : C \times S \longrightarrow D$
$I_P : P \times S \longrightarrow R_D$
In questo caso si parla di logica a designatori non rigidi.
Se invece consideriamo una logica a designatori non rigidi abbiamo I definita come:
$I_c : C \longrightarrow D$
$I_P : P \longrightarrow R_D$

### 11.2.3 Semantica

Chiamiamo s la funzione di assegnamento, posto V l'insieme delle variabili ossia la funzione, è la seguente:
$s : V \times S \longrightarrow D$
è possibile estendere s ad s*, e se chiamiamo T l'insieme di tutti i possibili termini, abbiamo che:
$s* : T \times S \longrightarrow D$
che è così definita:
$s * (x_i) = s(x_i)$
$s * (k_i) = I(k_i)$
Indichiamo che una formula è vera in un modello $\mu$, rispetto all'assegnamento s, in un mondo $\alpha$ nel seguente modo:
$\mu, s \models_\alpha a$
La verità di una formula è definita per induzione sui connettivi minimi:

- $\mu, s \models_\alpha A_i^n(t_1, ..., t_n) \iff (s * (t_1), ..., s * (t_n)) \in I_P(A_i^n, \alpha)$
- $\mu, s \models_\alpha \neg b \iff \mu, s \not\models_\alpha b$
- $\mu, s \models_\alpha b \implies c \iff \mu, s \models_\alpha c \vee \mu, s \not\models_\alpha b$
- $\mu, s \models_\alpha (\forall x)b \iff (\forall s' : s'(x) \neq s(x) \wedge s'(x_i) = s(x_i))\, \mu, s \models_\alpha (\forall x)b$
- $\mu, s \models_\alpha \Box b \iff \forall \beta : (\alpha, \beta) \in R\, \mu, s \models_\beta b$

Una formula M è vera in un mondo se ogni assegnamento la soddisfa, insoddisfacibile se nessuno la sofddisfa e sodisfacibile se è vera per alcuni assegnamenti.
Una formula si dice vera in un modello se è vera in tutti i mondi del modello
Una formula si dice valida in un frame se è vera in tutti i modelli costruiti su quel frame.

## 11.3 Assiomatizzazzione della Logica Modale del Prim'Ordine

### 11.3.1 Gli Assiomi della logica del prim'ordine

Gli assiomi della logica del prim'ordine sono:

- A1: $a \implies (b \implies a)$
- A2: $(a \implies (b \implies c)) \implies ((a \implies b) \implies (a \implies c))$
- A3: $(\neg a \implies \neg b) \implies ((\neg a \implies b) \implies a)$
- A4: $(\forall x)a(x) \implies a[t/x]$, dove t è un termine libero per x in A(x)
- A5: $(\forall x)(a \implies b) \implies (a \implies (\forall x)b)$, purchè non ci siano occorrenze libere di x in A

Inoltre valgono le due regole di inferenza:

- MP: $\dfrac{a,\ a \implies b}{b}$
- Gen: $\dfrac{a}{(\forall x)a}$

### 11.3.2 Formula di Barcan

Si chiama formula di barcan la seguente formula:
$(\forall x)\Box a \implies \Box(\forall x)a$
o equivalentemente la sua duale:
$\diamond(\exists x)a \implies (\exists x) \diamond a$
Si chiama formula di barcan inversa la formula:
$\Box(\forall x)a \implies (\forall x)\Box a$
o equivalentemente la sua duale:
$(\exists x) \diamond a \implies \diamond(\exists x)a$
La formula di barcan vale se e solo se il modello è antimonotono, la formula di barcan inversa vale se e solo se il modello è monotono.
Quindi in un modello a designatori costanti vale la formula di barcan inversa.

### 11.3.3 Minima logica modale del prim'ordine

Se consideriamo la logica che usa tutti gli assiomi della logica modale e quella del prim'ordine, ossia una logica che usa i seguenti assiomi:

- A1, A2, A3
- A4, A5
- K

E le seguenti regole di inferenza:

- MP
- Gen
- RN

Otteniamo la minima logica modale del prim'ordine.
Si può dimostrare che in questa logica vale la formula di Barcan inversa:
$\vdash_\Lambda (\forall x)a \implies a$ – per A4, t = x
$\vdash_\Lambda \Box((\forall x)a \implies a)$ – per RN
$\vdash_\Lambda \Box((\forall x)a \implies a) \implies (\Box(\forall x)a \implies \Box a)$ – per K
$\vdash_\Lambda \Box(\forall x)a \implies \Box a$ – per MP
$\vdash_\Lambda (\forall x)(\Box(\forall x)a \implies \Box a)$ – per Gen

$\vdash_\Lambda (\forall x)(\Box(\forall x)a \implies \Box a) \implies (\Box(\forall x)a \implies (\forall x)\Box a)$ – per A5
$\vdash_\Lambda \Box(\forall x)a \implies (\forall x)\Box a$ – per MP
che è la formula di barcan inversa.
Allo stesso modo si può dimostrare che aggiungendo lo schema:
B: $a \implies \Box \diamond a$
Dalla minima logica modale del prim'ordine si ricava anche la formula di Barcan. Questo è vero intuitivamente perchè se ho una relazione simmetrica monotona, allora deve anche essere antimonotona, e questo può essere vero solo se ci troviamo nel caso a domini costanti.
Si può usare, anzichè la logica normale, una logica classica, e si possono ricavare logiche in cui le due formule di Barcan non valgano.

# 12
# Bisimulazione

## 12.1 Definizione di bisimulazione

Siano $\mu = (S, R, V)$ e $\mu' = (S', R', V')$ due modelli e siano $s \in S$, e $t \in S'$ due stati
Si dice che le coppie $(\mu, s)$ e $(\mu', s)$ sono in bisimulazione tra loro, ossia:
$(\mu, s) \leftrightarroweq (\mu', s)$
Se esiste una relazione $E : S \times S$ tale che

1. $(s, t) \in E$

2. se $(x, y) \in E$ allora:
   a)$\forall P \in \phi\, x \in V(P) \iff y \in V'(P)$
   b1)$(x, z) \in R \implies \exists u \in S' : (y, u) \in R' \wedge (z, u) \in E$
   b2)$(y, u) \in R' \implies \exists z \in S : (x, z) \in R \wedge (z, u) \in E$

Due frame sono in bisimulazione se soddisfano le condizioni 1, b1 e b2.

### 12.1.1 Teorema

se $(\mu, s) \leftrightarroweq (\mu', s)$
allora:
$\forall \varphi \in \phi\, \mu \models_s \varphi \iff \mu' \models_t \varphi$

## 12.2 Esempi di bisimulazione

### 12.2.1 Alberi binari e Retta

Consideriamo il frame rappresentante la lettera dei numeri naturali:

$N = (\mathbb{N}, successivo)$

E il frame che rappresenta un albero binario a dimensione infinita:

$B = (w = \{0, 1\}*, \rho)$

Supponiamo che V su B sia:

$V(P) = \{w \in \{0, 1\}* : |w| = 2n\}$

Allora esiste una unica valutazione V' su N tale che $(B, V, 0) \leftrightarrows (N, V', \epsilon)$, ed è:

$V'(P) = \mathbb{P}$ (l'insieme dei numeri pari)

Dimostriamolo per induzione:

$(n, w) \in E \iff |w| = n$

il caso base si dimostra banalmente:

$|\epsilon| = 0$

$(\epsilon, 0) \in E$

per definizione. Per il passo induttivo abbiamo:

$|w| = n$

$(w, n) \in E$

sia w per ipotesi tale che $|w| = n + 1$

allora:

$w = ua$, $|u| = n$, $a \in \{0, 1\}$

per la condizione 1 di bisimulazione:

$(u, w) \in \rho$ e $(u, n) \in E$

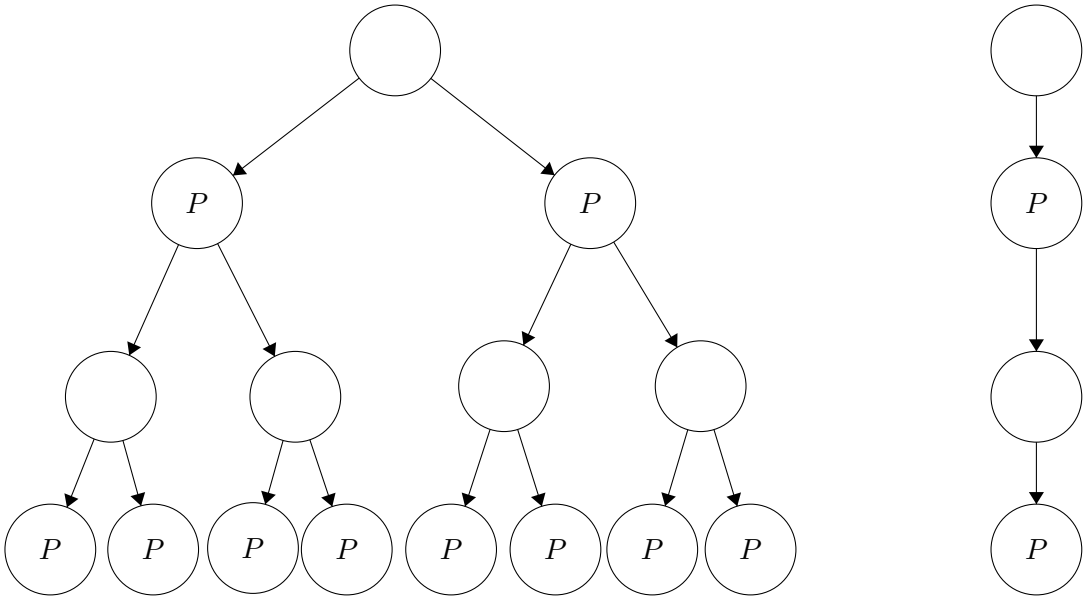
per la condizione b1 invece:

$\exists m \in \mathbb{N} : m = n + 1 \wedge (w, n + 1) \in E$

e quindi si deduce facilmente che:

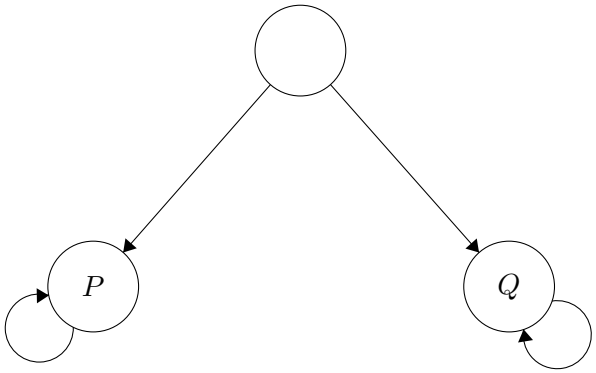
$|w| = |ua| = n + 1$

e quindi la valutazione non può che essere la sola V', perché è quella che si ricava imponendo la condizione di bisimulazione, e che rispetta anche la condizione 2.



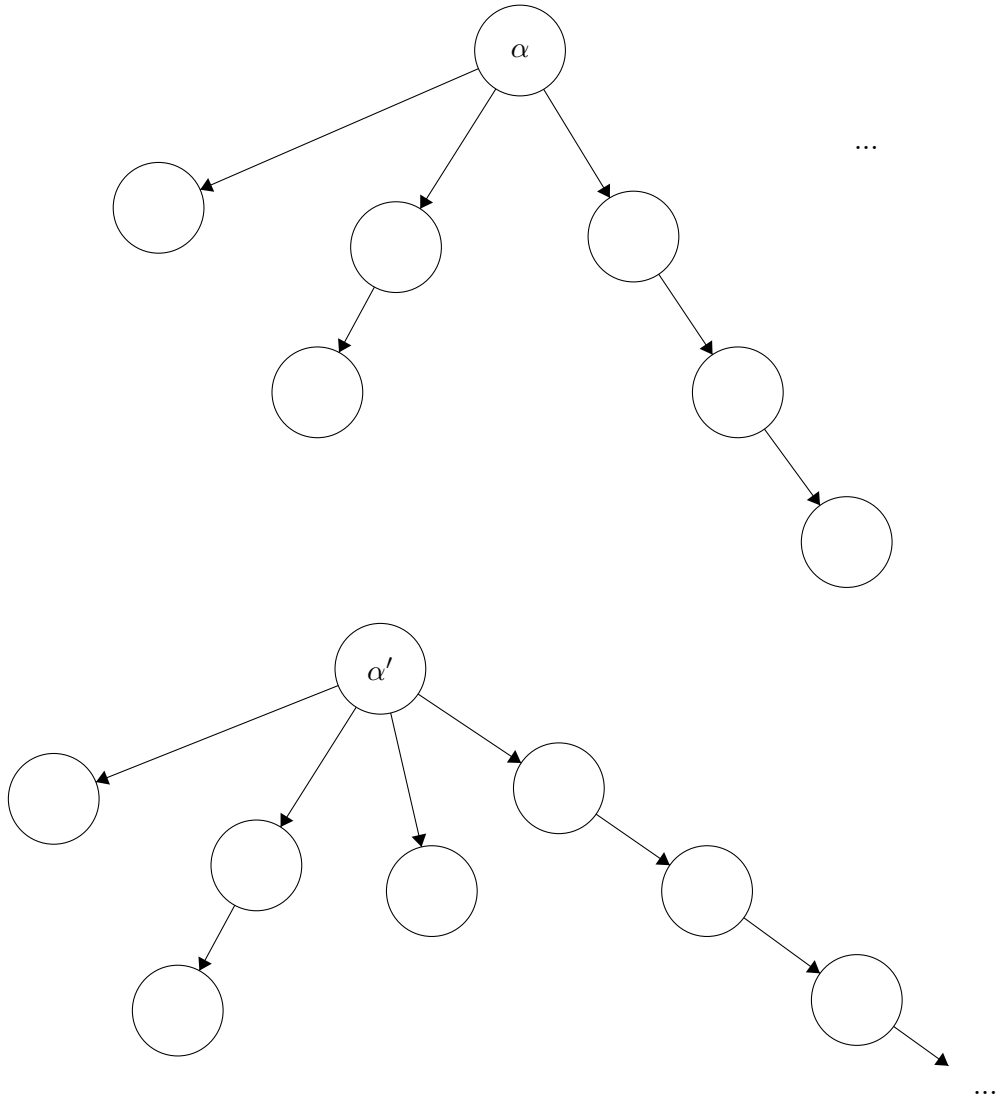

### 12.2.2 Alberi binari e frame finito

Supponiamo di prendere su un frame binario B la seguente funzione di valutazione:
$V(P) = \{0w \mid w \in \{0,1\}*\}$
$V(Q) = \{1w \mid w \in \{0,1\}*\}$
In questo frame Q è vera su tutto il sotto-albero destro, mentre P sul scotolassero sinistro.
è evidente che non può esistere alcuna V' su N tale che $(B, V, 0) \leftrightarrows (N, V', \epsilon)$, perché dovrebbero esistere due insiemi di stati non in relazione tra loro per cui in uno valga P e nell'altro Q. Ma questo non è possibile, poiché il frame N è una retta di elementi connessi a uno a uno. Tuttavia esiste un frame molto più semplice e finito che bisimula l'albero, di soli 3 stati, uno per lo stato $\epsilon$, uno per lo stato in qui vale P, e uno per lo stato in cui vale Q. Si può vedere come l'automa che riconosce se la stringa è "etichettata" P o Q.



### 12.2.3 Infiniti cammini vs Cammino infinito

Consideriamo due frame, il primo tale che da un nodo $\alpha$ partono infiniti percorsi, e l'altro che ha un solo percorso di lunghezza infinita.




Si dimostra che non esiste una bisimulazione tra i due frame:
$(F, \alpha) \not\leftrightarrows (F', \alpha')$
Dimostriamolo per assurdo, e supponiamo esista una bisimulazione tra i due frame:
$(F, \alpha) \leftrightarrows (F', \alpha')$
supponiamo inoltre w accessibile da $\alpha'$ sul ramo infinito.
Poiché sono in condizione di bisimulazione vale la condizione b2:
$(\alpha', u) \in R' \implies \exists \beta \in F : (\alpha, \beta) \in R \wedge (\beta, w) \in E$
Ma poiché $\beta$ appartiene al primo frame, esso sta su un ramo di lunghezza finita n.

Ma allora si ha che:
$F \not\models_\beta \diamond^n \top$
Tuttavia abbiamo anche che:
$\forall n \in \mathbb{N}$, $F' \models_\beta \diamond^n \top$
ma non può essere perché i due frame sono in bisimulazione, assurdo!
quindi non può esistere una bisimulazione tra i due frame.

### 12.2.4 Irriflessività e logica modale e temporale

Non esiste alcuna formula modale temporale per esprimere l'irriflessività, infatti siano:
$Z = (\mathbb{Z}, <)$
$F = (W, R)$
con $R = \{(a, a)\}$ e $W = \{a\}$
Sia $V_F$ una generica valutazione su F, esiste sempre una $V_Z$ su Z tale che:
$(Z, V_Z, 0) \leftrightarrows (F, V_F, a)$
Infatti $\forall P \in \phi$ e $\forall n \in \mathbb{Z}$ sia:
$V_Z(P, N) = V_F(P, a)$
o meglio:
$V_F(P) = \{a\} \implies V_Z(P) = \mathbb{Z}$
E' facile provare che i due modelli sono in bisimulazione:
1) $E \subseteq \mathbb{Z} \times W$, $\forall n \in \mathbb{Z}\,(n, a) \in E$
b1) $n < m \implies (m, a) \in E \wedge (a, a) \in R$
b2) $(a, a) \in R \implies (n + 1, a) \in E \wedge n < n + 1$
Ma, poiché il frame Z è irriflessivo, se esistesse una formula che esprime l'irriflessività, allora non sarebbe valida su F, ma ciò è impossibile, perché è in bisimulazione con Z, e quindi tutte le formule vere su F sono vere su Z e viceversa.

# 13 Model Checking

## 13.1 Frame Temporale

chiamiamo frame temporale un generico frame
$\tau = (T, <)$
dove $<$ è una relazione irriflessiva e transitiva.
Posto V una funzione di valutazione, un modello su un frame temporale è:
$\mu = (\tau, V)$
Le logiche basate sui frame temporali si chiamano logiche (modali) temporali.
Il frame temporale può avere alcune proprietà, infatti si dice:

- Lineare a destra: $\forall x, y, z((x < y \land x < z) \implies (y < z \lor z < y \lor y = z))$
- Lineare a sinistra: $\forall x, y, z((x > y \land x > z) \implies (y > z \lor z > y \lor y = z))$
- Ramificato a destra: se non è lineare a destra
- Ramificato a sinistra: se non è lineare a sinistra
- Discreto: $\forall x, y(x < y \implies \exists z(x < z \land \neg\exists u(x < u \land u < z)))$
- Denso: $\forall x, y(x < y \implies \exists z(x < z < y))$

## 13.2 Logica LTL

### 13.2.1 Notazione modena

La logica LTL ha una notazione più nuova rispetto a quella inizialmente formulata con gli operatori $\Box$, $\diamond$, $\circ$:

- $\mathcal{G} \equiv [F]$ chiamato "globally"
- $\mathcal{F} \equiv < F >$ chiamato "eventaully"
- $\mathcal{X} \equiv \circ$ chiamato next
- $\mathcal{U}$ chiamato until
- $\mathcal{R}$ chiamato release

### 13.2.2 Operatori modali ed espressività della logica

Dimostriamo Ora alcune proprietà degli operatori di LTL:

1. $\mathcal{X}$ può essere espresso da $\mathcal{U}$
2. $\mathcal{G}$ può essere espresso tramite il solo operatore $\mathcal{U}$
3. $\mathcal{F}$ può essere espresso tramite il solo operatore $\mathcal{U}$
4. $\mathcal{X}$ non può essere espresso con $\mathcal{G}$ e $\mathcal{F}$

Si dimostra abbastanza facilmente:
1) ricordando che next ha il significato seguente:
$\mu \models_s \mathcal{X}a \iff \mu \models_{s+1} a$
consideriamo la seguente formula:
$\mu \models_n \bot \mathcal{U} a$
è vera se e solo se vale la seguente:
$\exists m > n(\mu \models_m a \wedge \forall k(n < k < m \implies \mu \models_k \bot))$
poichè $\mu \models_k \bot$ è falsa in ogni mondo, deve essere falso l'antecedente dell'implicazione, quindi non deve esistere nessun k tale che $n < k < m$
Allora avremo che:
$m = n + 1$
e quindi
$\mu \models_n \bot \mathcal{U} a \iff \mu \models_n \mathcal{X}a$
2 e 3) Possiamo esprimere l'eventually (e quindi il globally) facilmente come:
$\mathcal{F}a \equiv \top \mathcal{U} a$
e quindi:
$\neg \mathcal{G} \neg a \equiv \top \mathcal{U} a$
$\mathcal{G}a \equiv \neg(\top \mathcal{U} \neg a)$
infatti:

$\mu \models_s \top \mathcal{U} a \iff \exists t(s < t \wedge \mu \models_t a \wedge \forall k(s < k < t \implies \mu \models_k \top)$
ma poichè $\forall k(s < k < t \implies \mu \models_k \top)$ è sempre vera, perchè il conseguente è sempre vero, allora abbiamo:
$\exists t(s < t \wedge \mu \models_t a)$
che è la definizione di eventually.
4) Supponiamo per assurdo che si possa esprimere l'operatore next in funzione di globally e eventually.
allora prendiamo il frame:
$N = (\mathbb{N}, <)$
e usiamo la seguente valutazione:
$V(P) = \{3n \mid n \in \mathbb{N}\}$
quindi il modello sarà:
$\mu = (N, V)$
allora, per ogni formula ben formata si ha che:
$\mu \models_n a \iff \mu \models_{n+3} a$
e
$\mu \models_1 a \iff \mu \models_2 a$
Per dimostrarlo, uso la bisimulazione:

- $(\mu, n) \leftrightarrows (\mu, n + 3)$
- $(\mu, 1) \leftrightarrows (\mu, 2)$

Nel primo caso, costruisco E tale che:
$(n, m) \in E \iff m = n + 3$
<<MANCA! non ci ho capito molto, pessimi appunti...>>

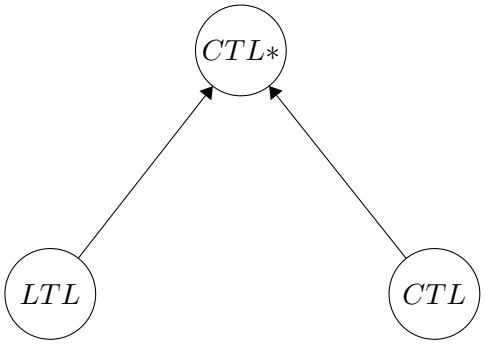
## 13.3 Logiche per il model checking

### 13.3.1 Logiche per il model checking e semantica

le principali logiche usate nel Model Checking sono 3:

- LTL, linear temporal logic (proposta da Pnueli nel 1977)
- CTL, computational tree logic (proposta da clarkee emerson nel 1981)
- CTL* (proposta da Emerson e Holpem nel 1986)

Le re logiche sono in relazione tra loro nel modo seguente:




La semantica di queste logiche è basata sulle strutture di Kripke, ossia
$\mu = (S, I, \tau \subseteq S \times S, L : S \longrightarrow 2^{\phi}, F)$
dove:

- S è l'insieme degli stati
- $I \subseteq S$ è l'insieme degli stati iniziali
- $\tau$ è una relazione tra gli stati totale a sinistra, ossia: $\forall s \in S \, \exists s' \in S \, : \, (s, s') \in \tau$ che significa che esistono sempre percorsi di lunghezza infinita.
- L è la funzione di labelling, che associa ad ogni stato un insieme di lettere proposizionali, quelle vere nello stato
- F è l'insieme di stati finali, ovvero l'insieme di stati per cui una sequenza accettata passa infinitamente spesso

### 13.3.2 Grammatica di LTL

La sintassi di LTL è la più semplice:
una formula ben formata è generata dalla seguente grammatica:
$\varphi \rightarrow P|\neg\varphi|\varphi \wedge \varphi|\varphi \vee \varphi|\varphi \implies \varphi|\varphi \iff \varphi|\mathcal{X}\varphi|\mathcal{F}\varphi|\mathcal{G}\varphi|\varphi\mathcal{U}\varphi|\varphi\mathcal{R}\varphi$

### 13.3.3 Grammatica di CTL

la grammatica di CTL è più complessa, e contiene anche i quantificatori di cammino, che sono degli operatori che esprimono la verità di una formula su almeno uno o tutti i cammini, e sono l'operatore E e A rispettivamente.
i quantificatori di cammino sono vincolati a delle sottoformule specifiche e non possono essere usati liberamente.
una formula ben formata è generata dalla seguente grammatica:
$\varphi \rightarrow P|\neg\varphi|\varphi \wedge \varphi|\varphi \vee \varphi|\varphi \implies \varphi|\varphi \iff \varphi$
$\varphi \rightarrow A\mathcal{X}\varphi|E\mathcal{X}\varphi|A\mathcal{F}\varphi|E\mathcal{F}\varphi|A\mathcal{G}\varphi|E\mathcal{G}\varphi|A(\varphi\mathcal{U}\varphi)|E(\varphi\mathcal{U}\varphi)|A(\varphi\mathcal{R}\varphi)|E(\varphi\mathcal{R}\varphi)$

### 13.3.4 Grammatica di CTL*

La logica CTL* è la logica più complessa e espressiva delle tre. La sua grammatica è quindi molto più complessa, e si descrive separando le formule di stato da quelle di cammino:
Sono formule di stato:
$\phi \to P|\neg\phi|\phi \wedge \phi|\phi \vee \phi|\phi \implies \phi|\phi \iff \phi|A\phi|E\phi$
Sono formule di cammino:
$\varphi \to \phi|\neg\varphi|\varphi \wedge \varphi|\varphi \vee \varphi|\varphi \implies \varphi|\varphi \iff \varphi|\mathcal{X}\varphi|\mathcal{F}\varphi|\mathcal{G}\varphi|\varphi\mathcal{U}\varphi|\varphi\mathcal{R}\varphi$
Le formule di cammino sono formule ben formate (e quindi, anche quelle di stato).

### 13.3.5 Semantica di CTL*

Per descrivere la semantica di CTL* fissiamo una notazione:
sia $\pi$ un cammino $\pi = s_0, s_1, s_2, ...$
mentre sia $\pi^i$ il suffisso $s_i, s_{i+1}, ...$
$\pi \in s^\omega$, ossia appartiene all'insieme delle stringhe infinite. Si ricordi che:
$s^\infty = s^* \cup s^\omega$
La semantica delle formule di stato è definita come:
$\mu, \pi^i \models P \iff P \in L(s_i)$
$\mu, \pi^i \models \neg\phi \iff \mu, \pi^i \not\models \phi$
$\mu, \pi^i \models \phi \wedge \psi \iff \mu, \pi^i \models \phi \wedge \mu, \pi^i \models \psi$
$\mu, \pi^i \models \phi \vee \psi \iff \mu, \pi^i \models \phi \vee \mu, \pi^i \models \psi$
$\mu, \pi^i \models \phi \implies \psi \iff \mu, \pi^i \not\models \phi \vee \mu, \pi^i \models \psi$
$\mu, \pi^i \models (\phi \iff \psi) \iff (\mu, \pi^i \models \phi \vee \mu, \pi^i \models \psi) \vee (\mu, \pi^i \not\models \phi \wedge \mu, \pi^i \not\models \psi)$
$\mu, \pi^i \models A\phi \iff \forall\overline{\pi}\,((\overline{\pi} = s_i, ...) \implies (\mu, \overline{\pi} \models \phi))$
$\mu, \pi^i \models A\phi \iff \exists\overline{\pi}\,((\overline{\pi} = s_i, ...) \implies (\mu, \overline{\pi} \models \phi))$
La semantica delle formule di cammino è la seguente:
$\mu, \pi^i \models \mathcal{X}\varphi \iff \mu, \pi^{i+1} \models \varphi$
$\mu, \pi^i \models \mathcal{F}\varphi \iff \exists j \geq i : \mu, \pi^j \models \varphi$
$\mu, \pi^i \models \mathcal{G}\varphi \iff \forall j \geq i : \mu, \pi^j \models \varphi$
$\mu, \pi^i \models \varphi\mathcal{U}\psi \iff \exists j \geq i : \mu, \pi^j \models \varphi \wedge \forall k : i < k < j\, \mu, \pi^k \models \psi$
$\mu, \pi^i \models \varphi\mathcal{U}\psi \iff \exists j \geq i : \mu, \pi^j \models \varphi \wedge \forall k : i < k < j\, \mu, \pi^k \models \psi$ <<sbagliati gli ultimi due, controllare>>

## 13.4 Model Checking

### 13.4.1 Definizione

Il model checking si occupa di risolvere il seguente problema:
Data una formula $\varphi$ e una struttura di Kripke $\mu$, dire se $\mu \models \phi$ per ogni cammino su $\mu$, ossia:
$\mu, \pi^0 \models A\varphi$

In caso contrario esibire un cammino $\pi$ tale che $\mu$, $\pi \not\models \phi$

Solitamente si verificano 3 tipi di proprietà:

- Safety: "non succede mai nulla di grave" ($\mathcal{G}\neg\varphi$)
- Liveness: "prima o poi avviene un evento desiderato" ($\mathcal{F}\varphi$)
- Fairness: "un evento desiderato avviene infinitamente spesso" ($\mathcal{GF}\varphi$)

Esistono sostanzialmente due tipologie di tecniche di model checking:

- Simboliche: basate su tableaux, deduzione formale e SMT solver
- Operazionali: Basate sulla manipolazione di automi a stati finiti

### 13.4.2 Model Checking operazionale

Il model checking operazionale si basa sulla manipolazione di particolari automi, detti automi di Büchi.
L'algoritmo alla base è il seguente:

1. Rappresento il modello $\mu$ con un automa di Büchi $A_\mu$
2. per verificare la proprietà $\varphi$, traduco la sua negazione in un automa di Büchi $A_{\neg\varphi}$
3. Costruisco l'automa prodotto che riconosce il linguaggio intersezione tra $L(A_\mu)$ e $L(A_{\neg\varphi})$
4. Controllo se $L(A_\mu \times A_{\neg\varphi}) = \emptyset$, in caso affermativo la proprietà è verificata.

### 13.4.3 Automi di Büchi

Gli automi di Büchi sono automi a stati finiti nondeterministici, che riconoscono linguaggi infiniti, e dove gli stati "finali" sono stati di ripetizione, ovvero stati che vengono raggiunti infinite volte durante il riconoscimento della stringa appartenente al linguaggio.
Gli automi di Büchi godono delle seguenti propietà:
Siano A, B automi di Büchi, allora esiste un automa che riconosce:

- $L(A) \cup L(B)$
- $L(A) \cap L(B)$
- $L(A)^c$
- $L(A)L(B)$ se A è un automa a stati finiti classico

### 13.4.4 Da formule di LTL ad automi di Büchi

Esiste un algoritmo per tradurre una formula di LTL in un automa di Büchi. Lo stesso algoritmo si può estendere, con le dovute accortezze e prestando attenzione ai sottocasi, alle formule di CTL e CTL*.
Sia $\varphi$ la formula e siano $P_1$, ..., $P_n$ le lettere predicative di $\varphi$
Si può trovare un automa di Büchi $A_\varphi = (S, I, \tau, L, F)$ con $L : S \longrightarrow 2^{\{P_1, ..., P_n\}}$tale che, se $\pi$ è un path che corrisponde ad una parola $\omega \in L(A_\varphi)$, allora $(S, \tau, L), \pi \models \varphi$
l'algoritmo è il seguente:

1. Porto la formula $\varphi$ in forma negata normale
2. elimino i globally ($\mathcal{G}$)
3. Costruisco l'automa locale $A_L$
4. altro che non abbiamo fatto

#### 13.4.4.1 Forma negata normale

Portare una formula in forma negata normale, consiste nel rendere una formula più "semplice", cioè in modo che contenga "pochi" connettivi e operatori modali diversi, avendo cura di portare le negazioni davanti alle lettere proposizionali.
Per farlo utilizzo le seguenti regole:
I) Le relazioni tra gli operatori modali

- $\neg\mathcal{G}a \equiv \mathcal{F}\neg a$
- $\neg\mathcal{F}a \equiv \mathcal{G}\neg a$
- $\neg(a\mathcal{U}b) \equiv (\neg a\mathcal{R}\neg b)$
- $\neg(a\mathcal{R}b) \equiv (\neg a\mathcal{U}\neg b)$

II) Le formule di De Morgan

- $\neg(a \wedge b) \equiv (\neg a) \vee (\neg b)$
- $\neg(a \vee b) \equiv (\neg a) \wedge (\neg b)$

La formula così trovata si dice in forma negata normale.
Si può a questo punto eliminare anche l'operatore globally, ricordando la seguante relazione:

- $\mathcal{G}a \equiv \bot\mathcal{R}a$

#### 13.4.4.2 Costruzione dell'automa locale

L'automa locale è un automa che riconosce sequenze di esecuzione che verificano la proprietà $\varphi$
l'algoritmo si articola in due passi:

1. Chiusura della formila $\varphi$: $cl(\varphi)$

   - $\varphi \in cl(\varphi)$
   - $\psi \in cl(\varphi) \implies \neg\psi \in cl(\varphi)$
   - $\psi \wedge \theta \in cl(\varphi) \implies \psi, \theta \in cl(\varphi)$
   - $\psi \vee \theta \in cl(\varphi) \implies \psi, \theta \in cl(\varphi)$
   - $\mathcal{X}\psi \in cl(\varphi) \implies \neg\psi \in cl(\varphi)$
   - $\mathcal{F}\psi \in cl(\varphi) \implies \neg\psi \in cl(\varphi)$
   - $\psi\mathcal{U}\theta \in cl(\varphi) \implies \psi, \theta \in cl(\varphi)$
   - $\psi\mathcal{R}\theta \in cl(\varphi) \implies \psi, \theta \in cl(\varphi)$

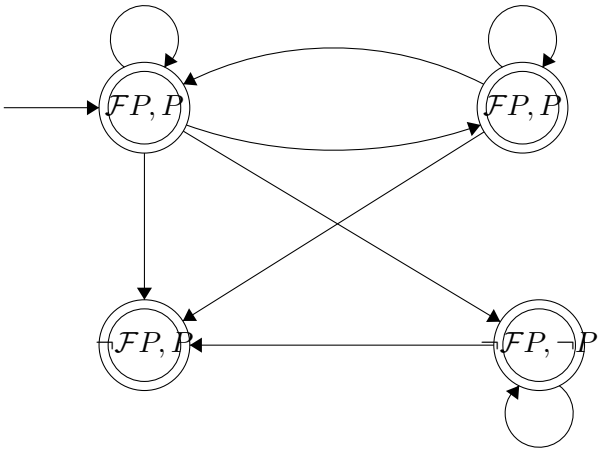
2. Automa locale $A_L = (\Sigma, S_L, I_L, \tau_L, F_L)$

   - $\Sigma = 2^{cl(\varphi)}$ ovvero $\Sigma \subseteq \mathcal{P}(cl(\varphi))$
   - $S_L$ formato da tutti gli elementi di $\Sigma$ consistenti ovvero $\psi \in S_L \iff \neg\psi \notin S_L$
   - $I_L = \{s \in S_L \,|\, \varphi \in s\}$
   - $F_L = S_L$ (ossia tutti gli stati sono finali)
   - $\tau_L$ tale che: siano $s, s' \in S_L$, $a \in \Sigma$ allora $(s, a, s') \in \tau_L$ se e solo se:
     (a) $a = s$
     (b) $\mathcal{X}\psi \in s \iff \psi \in s'$
     (c) $\mathcal{F}\psi \in s \iff \psi \in s' \vee \mathcal{F}\psi \in s'$ (infatti vale $\mathcal{F}\psi \equiv \mathcal{X}\psi \vee \mathcal{X}\mathcal{F}\psi$)
     (d) $\psi\mathcal{U}\theta \in s \iff \theta \in s' \vee (\psi \in s \wedge \psi\mathcal{U}\theta \in s')$ (infatti vale $\psi\mathcal{U}\theta \equiv \mathcal{X}\theta \vee (\psi \wedge \mathcal{X}(\psi\mathcal{U}\theta))$)
     (e) $\psi\mathcal{R}\theta \in s \iff \psi \wedge \theta \in s \vee (\theta \in s \wedge \psi\mathcal{R}\theta \in s')$

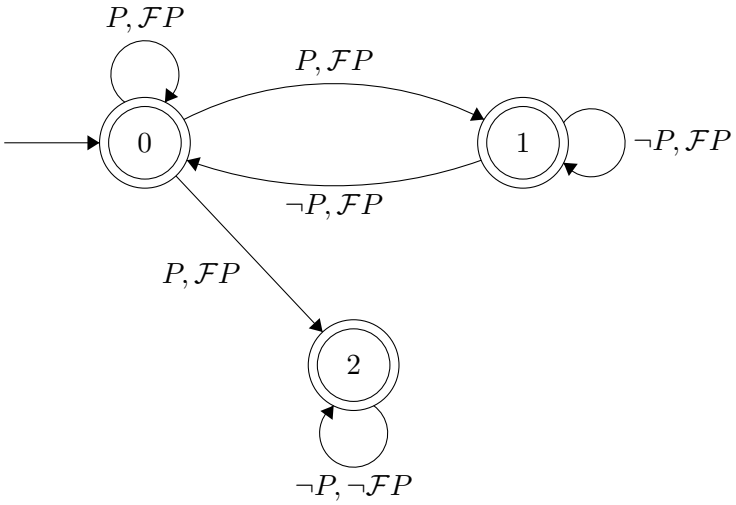
Una volta costruito l'automa in queosto modo, si deve minimizzare. L'automa minimo è l'automa locale di $\varphi$

**Esempio**

Costruiamo l'automa locale della formula:
$\varphi \equiv \mathcal{F}P$
Prima di tutto costruiamo la chiusura di $\varphi$
$cl(\mathcal{F}P) = \{\mathcal{F}P, P, \neg P, \neg\mathcal{F}P\}$
Ora l'automa locale costruito sarà:




Posso ora minimizzare l'automa locale, cancellando lo stato pozzo, ottenendo l'automa locale:




Si può notare chel'automa locale riconosce anche sequenze di esecuzione che non soddisfano $\varphi$, ad esempio:
$(\neg P)^\omega \in L(A_L)$