μ-Calculus Model Checking

Giovanna D'Agostino e Angelo Montanari

Dipartimento di Matematica e Informatica
Università di Udine

Outline

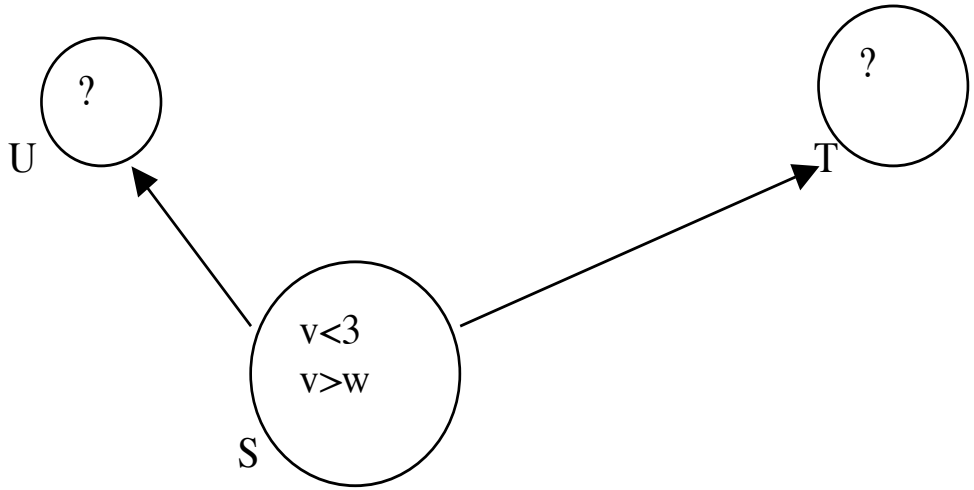
μ-calculus

Il μ-calculus proposizionale è un **frammento** della logica monadica al second'ordine *MSO* che **estende** la logica modale (temporale) *LM*:

$$LM \subseteq \mu\text{-calculus} \subseteq MSO$$

Viene utilizzato nell'ambito della verifica di sistemi informatici, in particolare, dei sistemi reattivi, nei quali la concorrenza svolge un ruolo fondamentale.

Logica Proposizionale

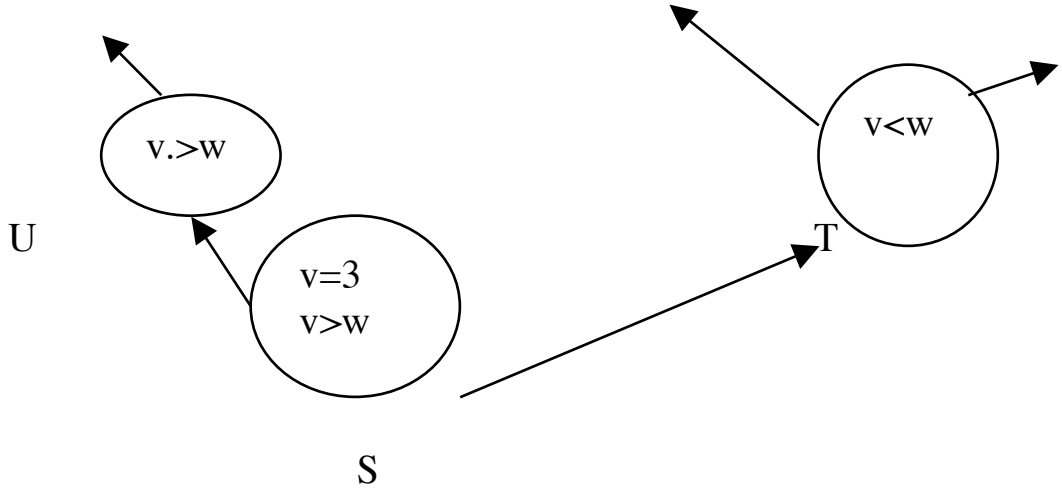


La Logica Proposizionale esprime proprietà dello stato corrente.

Ad esempio, possiamo chiederci se nello stato S vale

$(v=3) \rightarrow \neg(v>w) \vee (v<3)$

Logica Modale



La Logica Modale esprime proprietà di stati raggiungibili dallo stato corrente tramite gli operatori

[] P (in tutti i successori dello stato corrente vale P)
$\Diamond$ P (esiste un successore dello stato corrente in cui vale P)

Possiamo chiederci se in S vale (v=3) $\rightarrow\Diamond$ (v>w) ma non possiamo chiederci se esiste una computazione che porta in uno stato in cui vale v=4.

Logiche Temporali

A partire dagli anni ’70, vengono sviluppate logiche più espressive, in grado di esprimere in modo naturale proprietà di

liveness (vitalità),

safety (sicurezza) e

fairness (equità):

LTL, *PDL*, *CTL*, *ACTL*, *CTL**, . . .

μ-calculus: sintassi e semantica

Sintassi del μ-calculus:

logica modale + $\mu X\ F(X), \nu X\ F(X)$, con F positiva in X

Esempio:

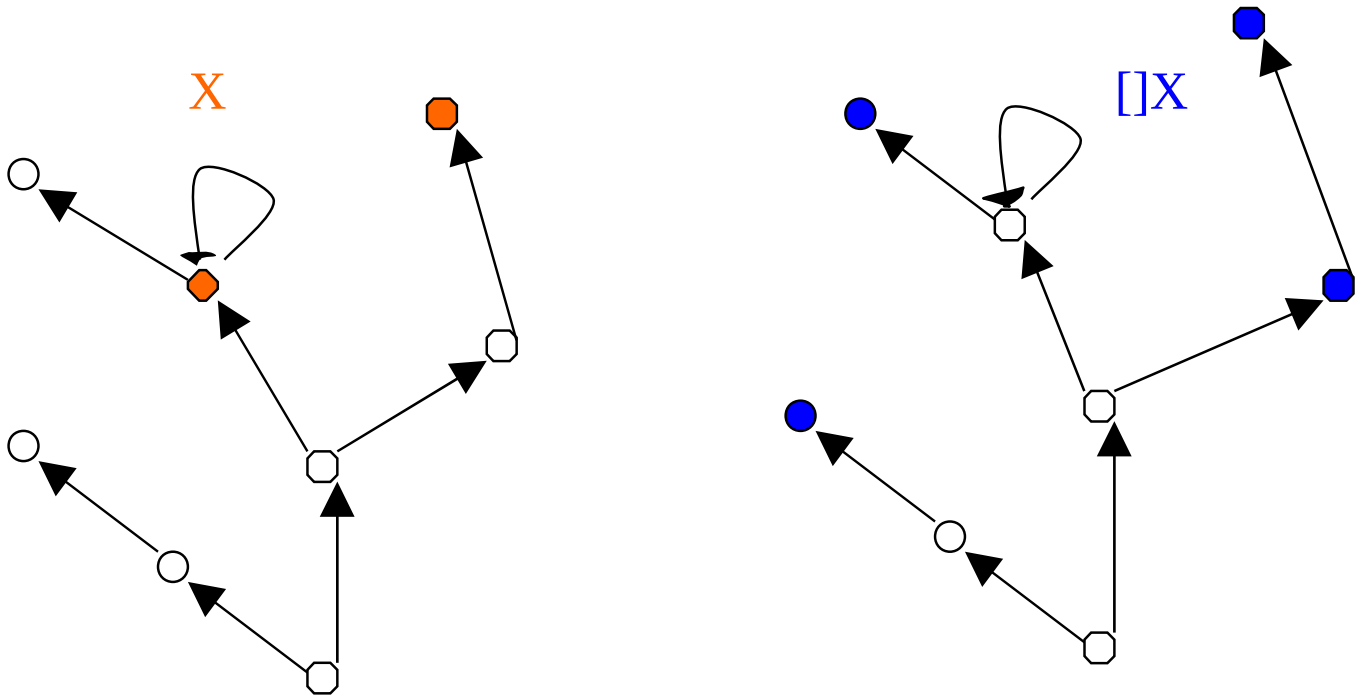
$$\mu X \Diamond (X \wedge \nu Y \Box Y)$$

μ sta per minimo punto fisso

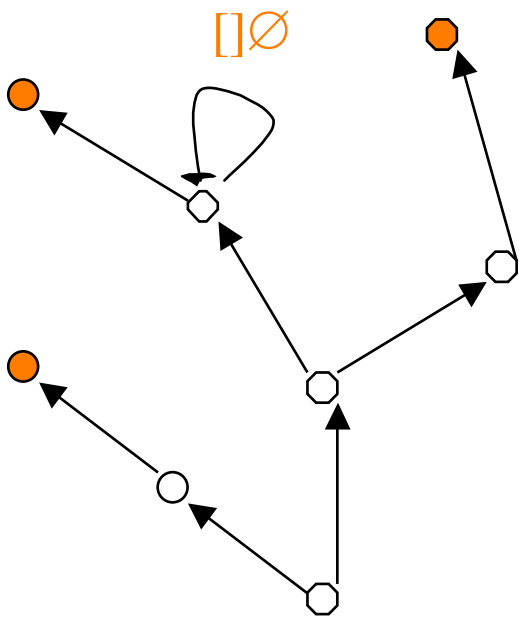
ν sta per massimo punto fisso

Semantica di $\mu X \Box X$

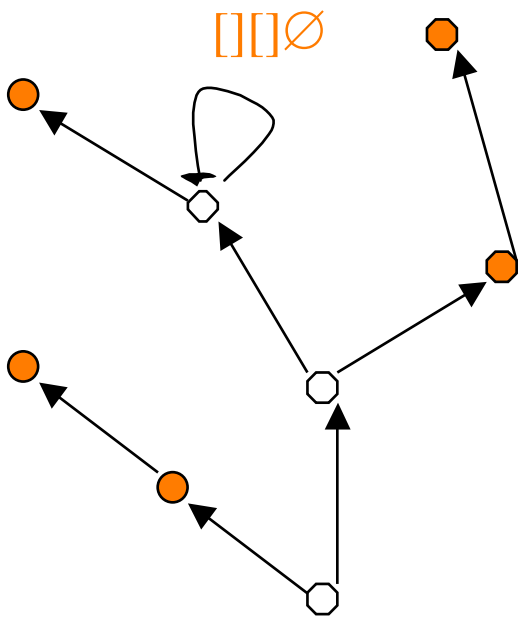
[] : Pow(W) --> Pow(W)
X → []X



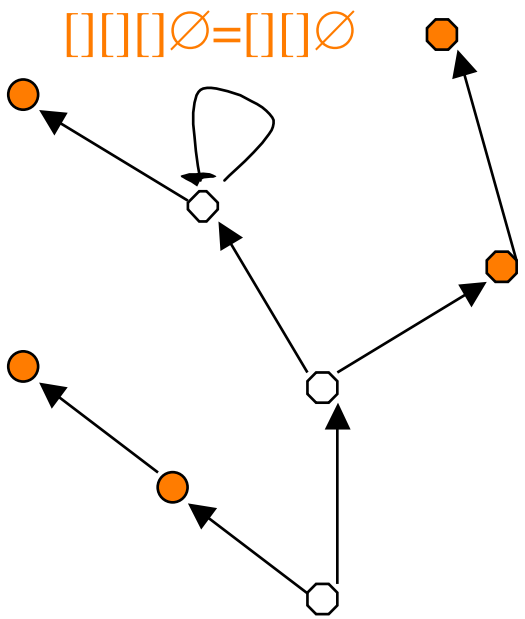
Semantica di $\mu X \Box X$



Semantica di $\mu X \Box X$



Semantica di $\mu X \Box X$



se A= [][]∅
[]A=A:
A è un punto fisso della funzione
[] : Pow(W) --> Pow(W)

Semantica per i minimi punti fissi

Se $F(X)$ è positiva in X (tutte le occorrenze di X in $F(X)$ cadono sotto un numero pari di negazioni), allora $F(X)$ è monotona (come funzione su $Pow(W)$):

$$A \subseteq B \Rightarrow F(A) \subseteq F(B)$$

Ne segue che, in ogni modello, ha un minimo punto fisso $fix_F \subseteq W$:

$$F(fix_F) = fix_F \quad \text{e se } F(B) = B, \text{ allora } fix_F \subseteq B.$$

$$S \models \mu X\ F(X) \Leftrightarrow S \in fix_F$$

per ogni $S \in W$

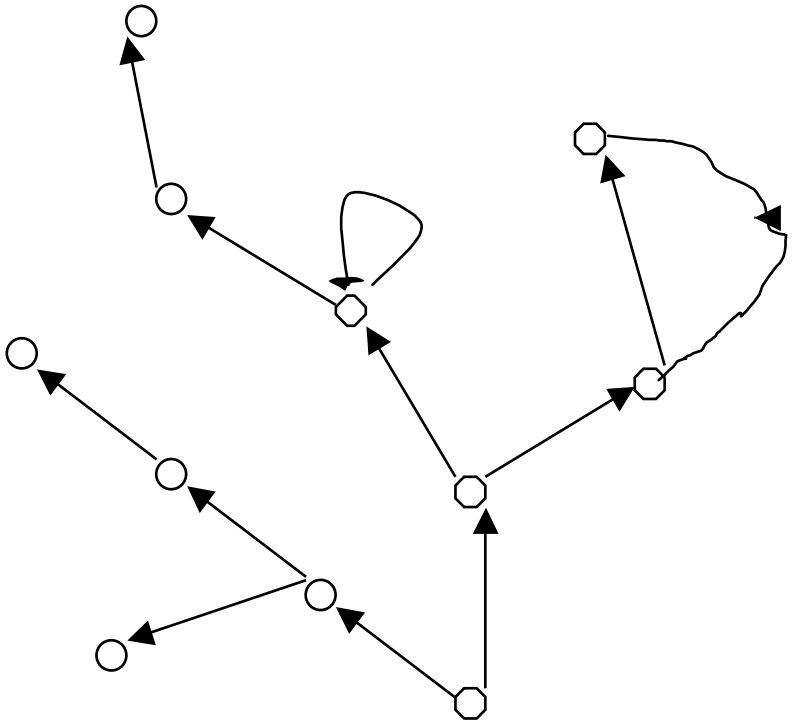
Come trovare i minimi punti fissi

Dalla monotonia di F segue che:

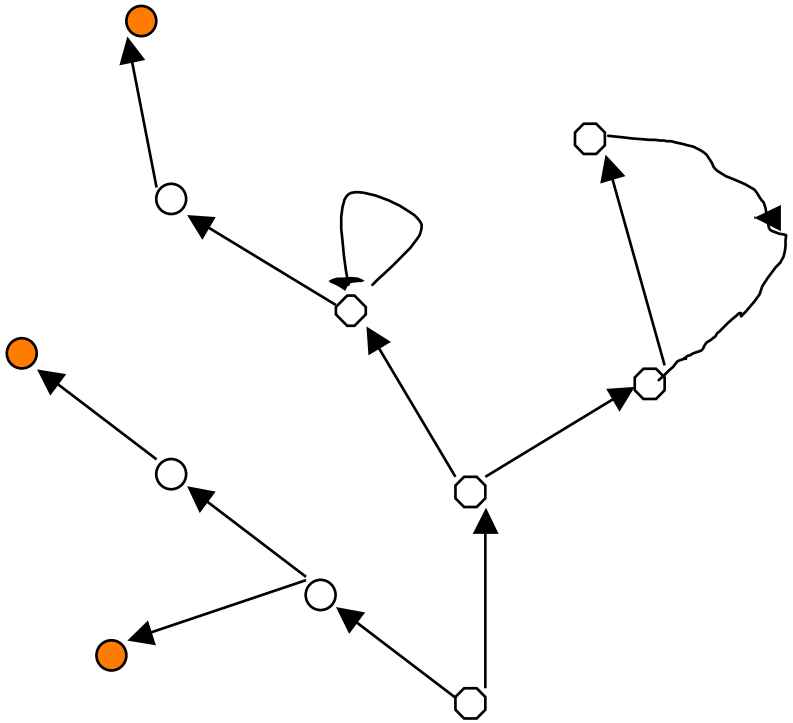
$$\emptyset \subseteq F(\emptyset) \subseteq F(F(\emptyset)) \subseteq \ldots \subseteq F^n(\emptyset) \subseteq \ldots$$

Se F è continua rispetto all'unione (tale è nel caso dei modelli finiti):

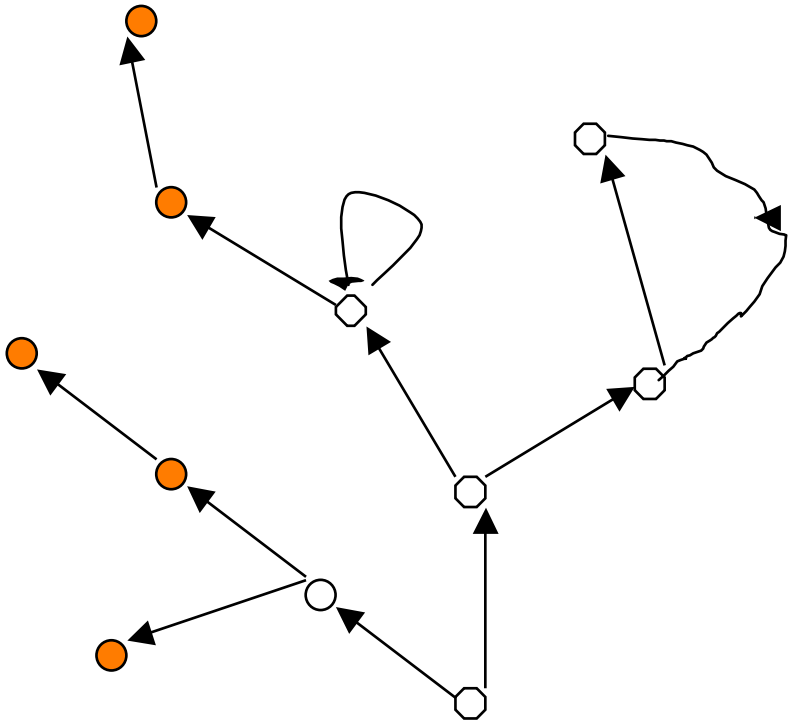
$$\mu X\ F(X) = fix_F = \bigcup_{n \in \omega} F^n(\emptyset).$$



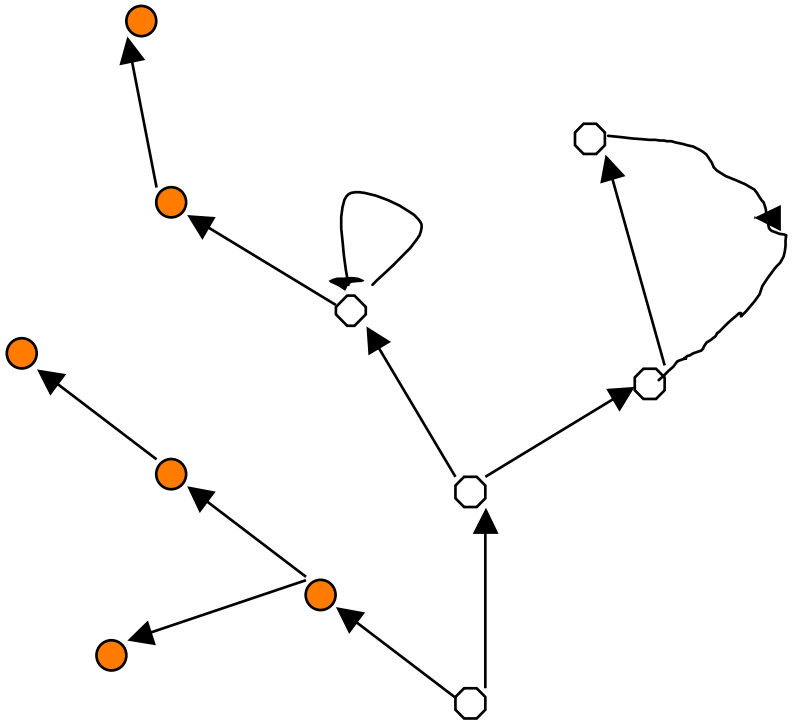
$\varnothing$



$[]\varnothing$

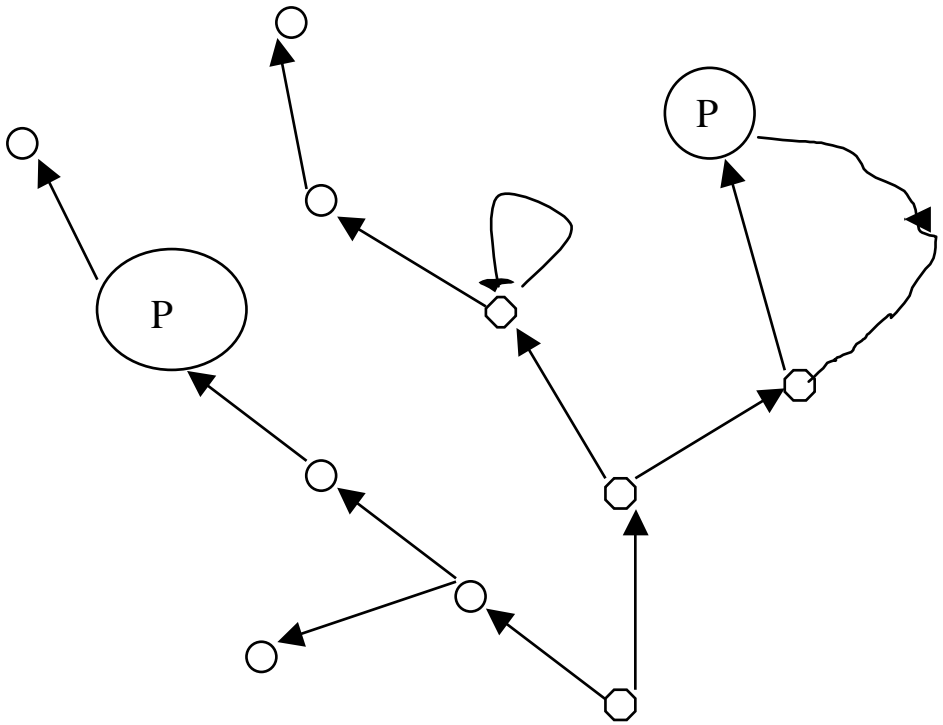


$[][]\varnothing$



$[][][]\ \varnothing = \mu\ X\ []\ X$

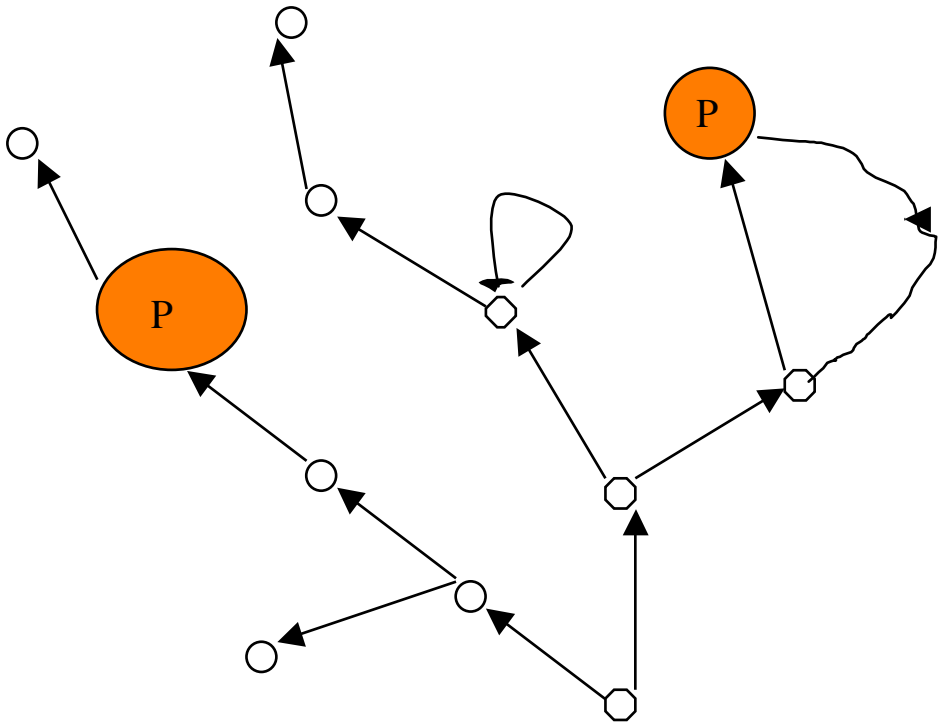
Un altro esempio: $\mu X(P \vee \Diamond X)$



IN QUALI PUNTI VALE

μx (Pv◊ X)?

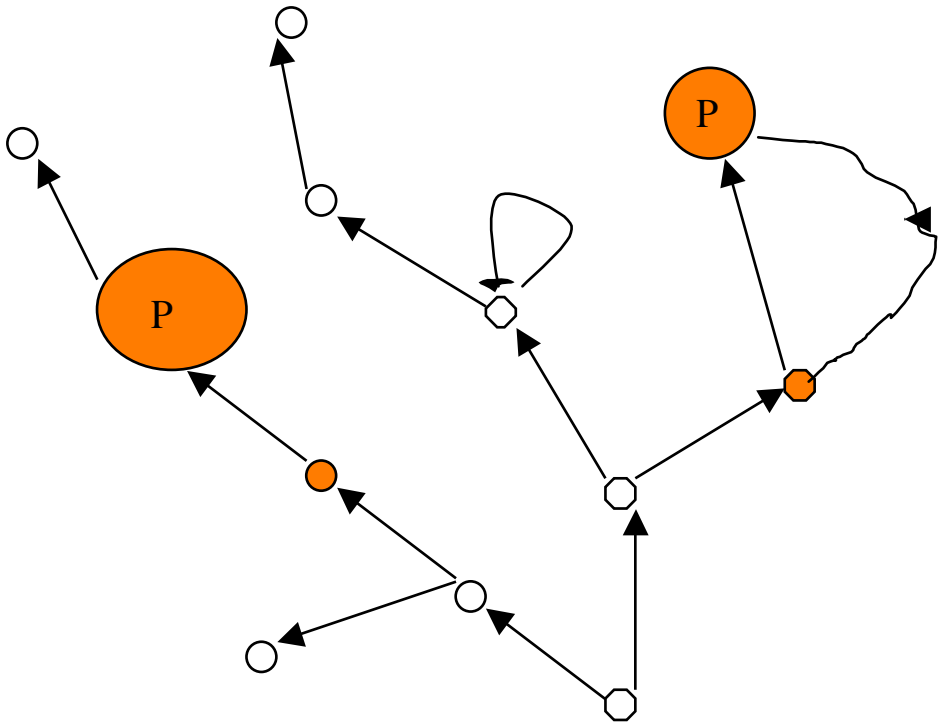
Un altro esempio: $\mu X(P \vee \Diamond X)$



μx (Pv◊ X):

Pv◊ ∅=P

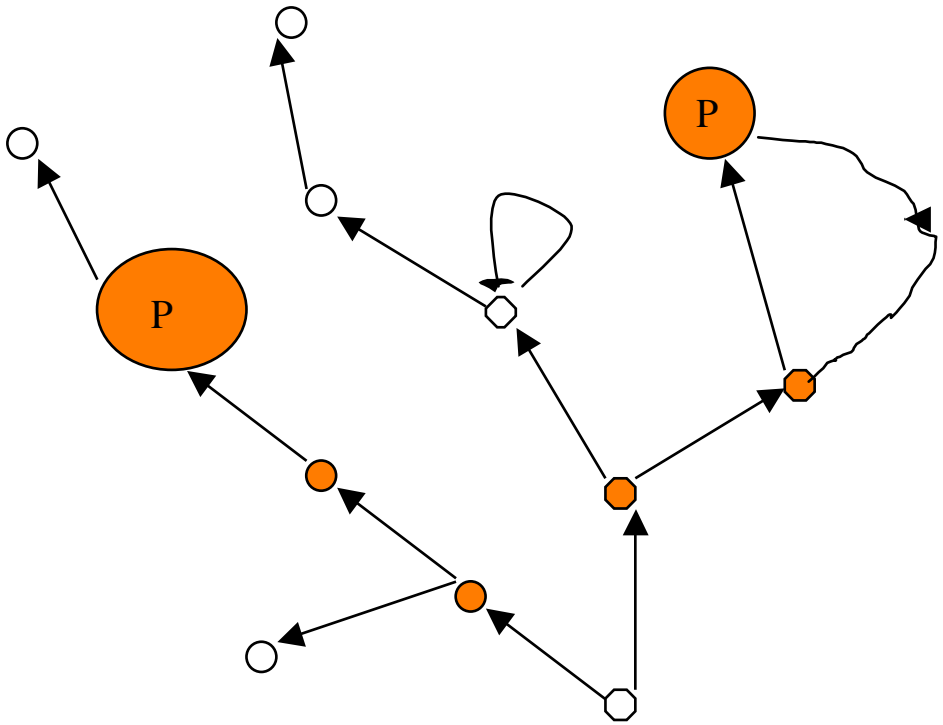
Un altro esempio: $\mu X(P \vee \Diamond X)$



μx (Pv◊ X):

Pv◊ P

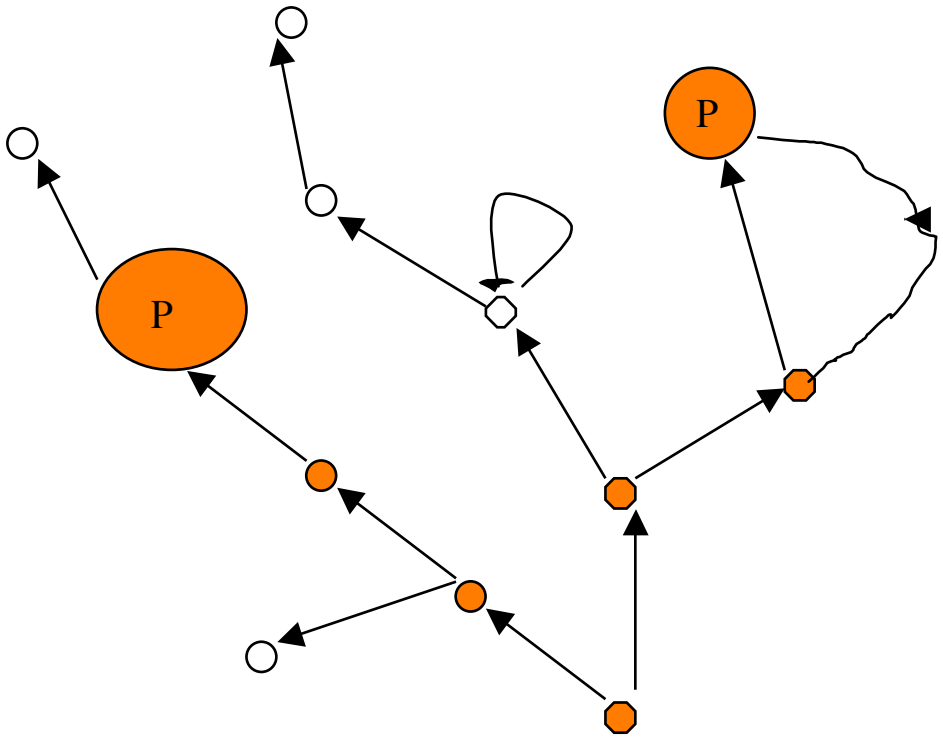
Un altro esempio: $\mu X(P \vee \Diamond X)$



μx (Pv◊ X):

Pv◊ (Pv◊ P)

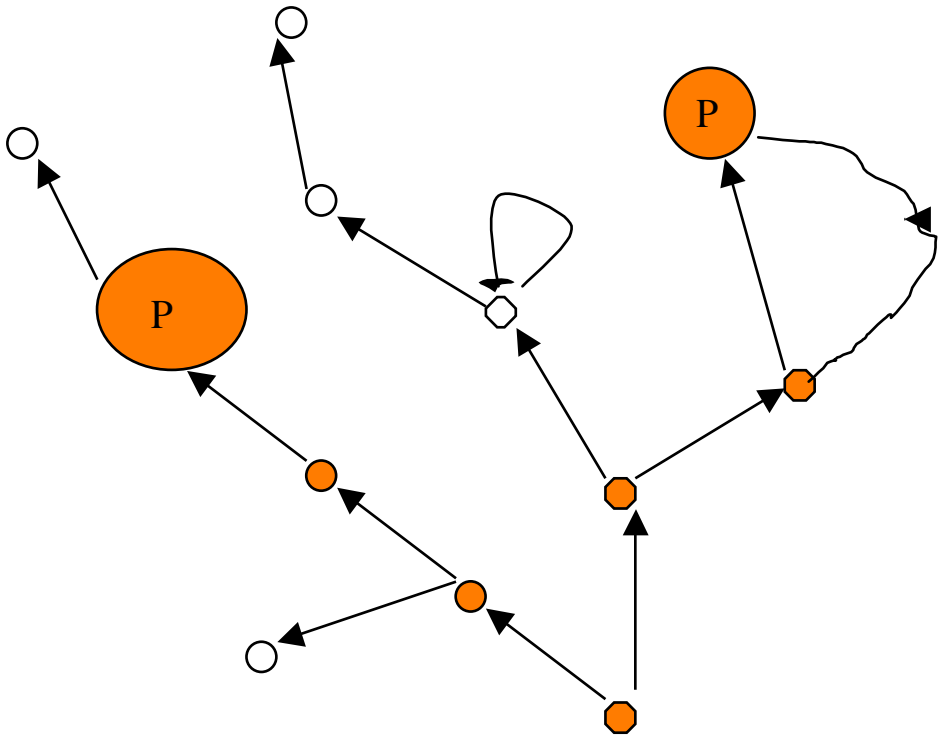
Un altro esempio: $\mu X(P \vee \Diamond X)$



μx (Pv◊ X):

Pv◊ (Pv◊ (Pv◊ P))

Un altro esempio: $\mu X(P \vee \Diamond X)$



μx (Pv◊ X) è vera se p è raggiungibile in un numero finito di passi.

Semantica per i massimi punti fissi

Se $F(X)$ è positiva in X, allora $F(X)$ ha un massimo punto fisso FIX_F:

$$F(FIX_F) = FIX_F \quad \text{e se } F(B) = B, \text{ allora } B \subseteq FIX_F.$$

$$S \models \nu X\ F(X) \Leftrightarrow S \in FIX_F$$

per ogni $S \in W$.

Come trovare i massimi punti fissi

Se F è positiva, allora

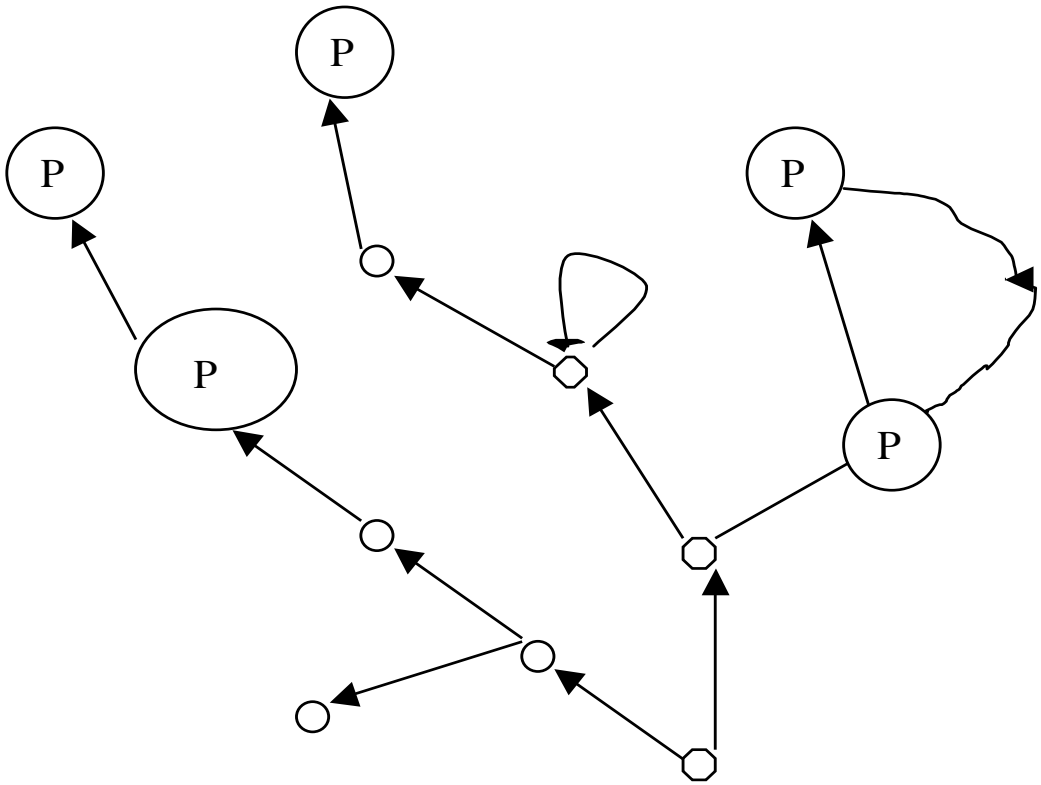
$$W \supseteq F(W) \supseteq F(F(W)) \supseteq \ldots \supseteq F^n(W) \supseteq \ldots$$

Se F è continua rispetto all'intersezione (tale è nel caso dei modelli finiti):

$$\nu X\ F(X) = FIX_F = \bigcap_{n \in \omega} F^n(W).$$

Un esempio: $\nu X(P \wedge \Diamond X)$

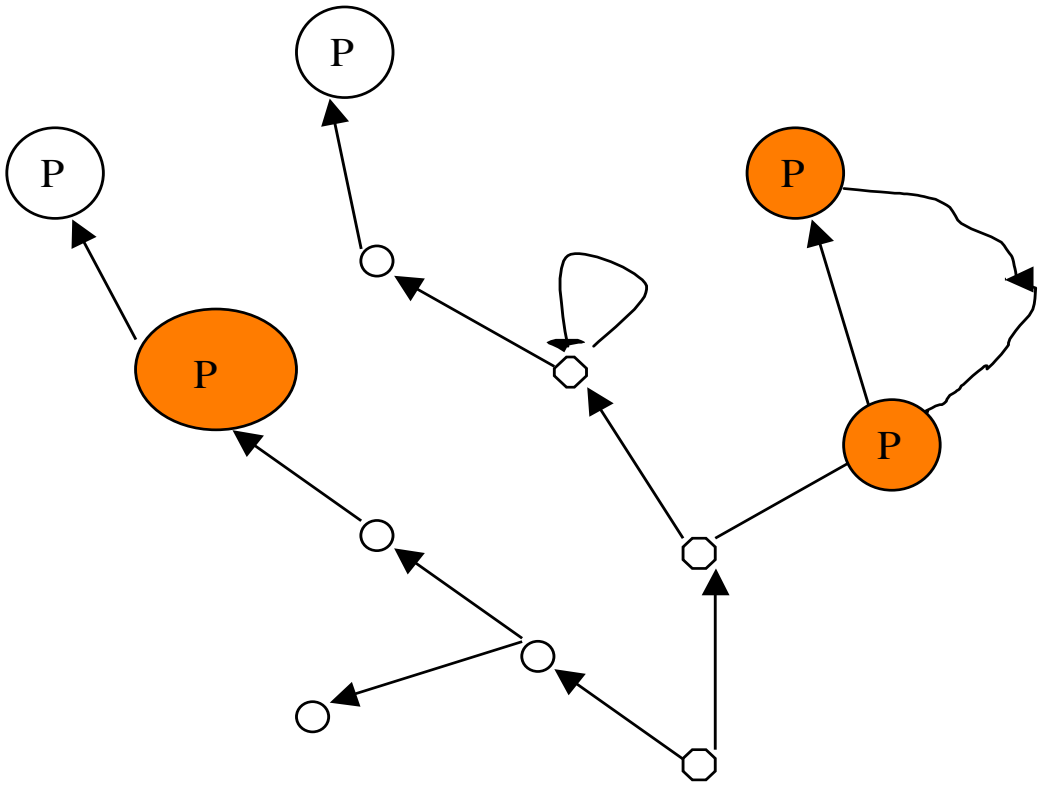
Un esempio: $\nu X(P \wedge \Diamond X)$



IN QUALI PUNTI VALE

$\nu x\ (P \wedge \Diamond\ X)$?

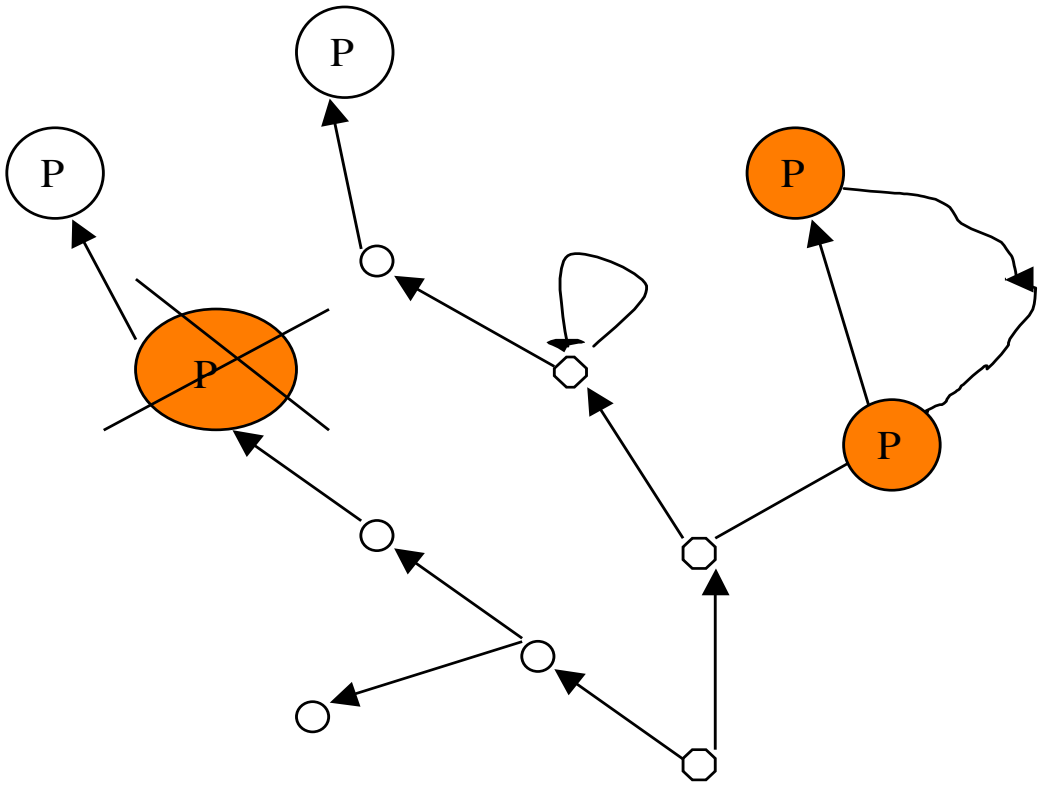
Un esempio: $\nu X(P \wedge \Diamond X)$



$\nu x\ (P \wedge \Diamond\ X)$:

$P \wedge \Diamond\ T$

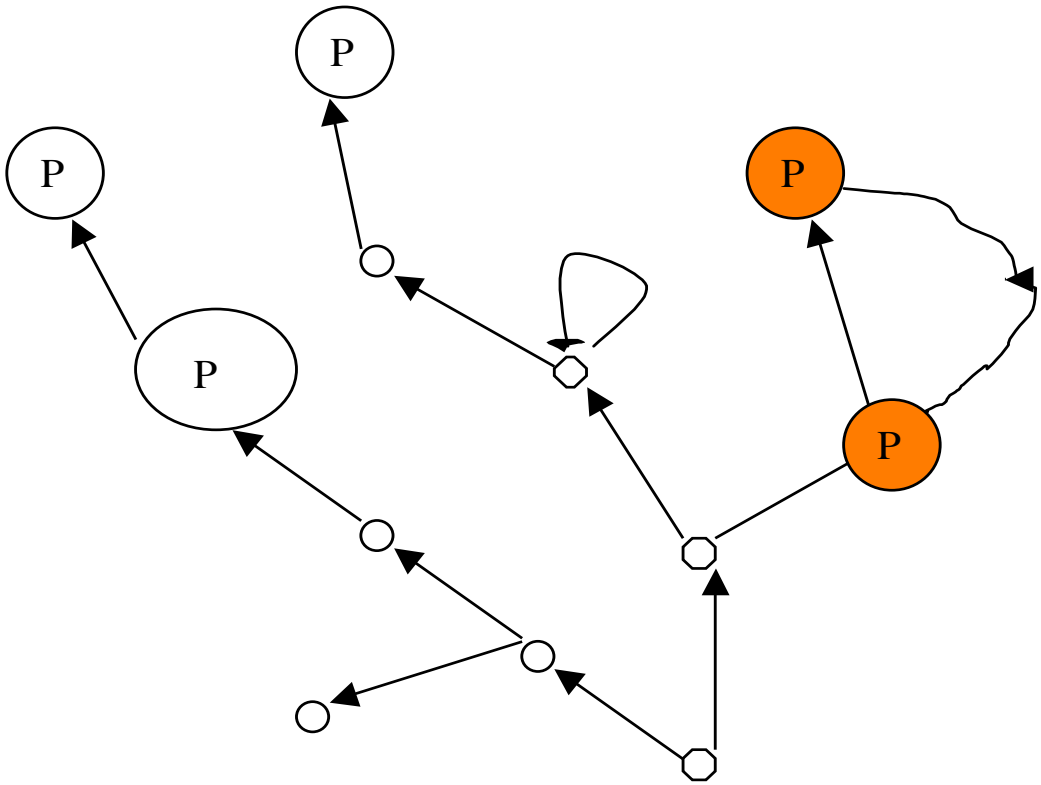
Un esempio: $\nu X(P \wedge \Diamond X)$



$\nu x\ (P \wedge \Diamond\ X)$:

$P \wedge \Diamond\ (P \wedge \Diamond\ T)$

Un esempio: $\nu X(P \wedge \Diamond X)$



$\nu x\ (P \wedge \Diamond\ X)$:
parte un cammino infinito dove vale sempre P

Massimi e minimi punti fissi

Minimi punti fissi:

- $\mu X \Box X \equiv$ non parte alcun cammino infinito;
- $\mu X(p \vee \Diamond X) \equiv$ si raggiunge in un numero finito di passi un nodo dove vale p;

Massimi punti fissi:

- $\nu X \Diamond X \equiv$ parte un cammino infinito;
- $\nu X \Box(X \wedge p) \equiv$ in ogni punto raggiungibile vale p;

Confronto con la logica classica

Sia M un modello e sia $w \in M$.
Le proprietà degli stati di M esprimibili con formule modali sono esprimibili in logica al prim'ordine (FO):

$$w \models \Diamond p \qquad \Leftrightarrow \qquad M \models \exists y(wRy \wedge p(y))$$

$$w \models \Box p \qquad \Leftrightarrow \qquad M \models \forall y(wRy \rightarrow p(y))$$

Il μ-calculus, invece, è un frammento della logica monadica al second'ordine (MSO):

$$\nu X \Diamond(X) = FIX_{\Diamond} = \bigcup \{X : X \subseteq \Diamond(X)\}$$

$$w \models \nu X \Diamond X \qquad \Leftrightarrow \qquad \exists X(w \in X \wedge X \subseteq \Diamond(X))$$

Completezza Modulo Bisimulazione

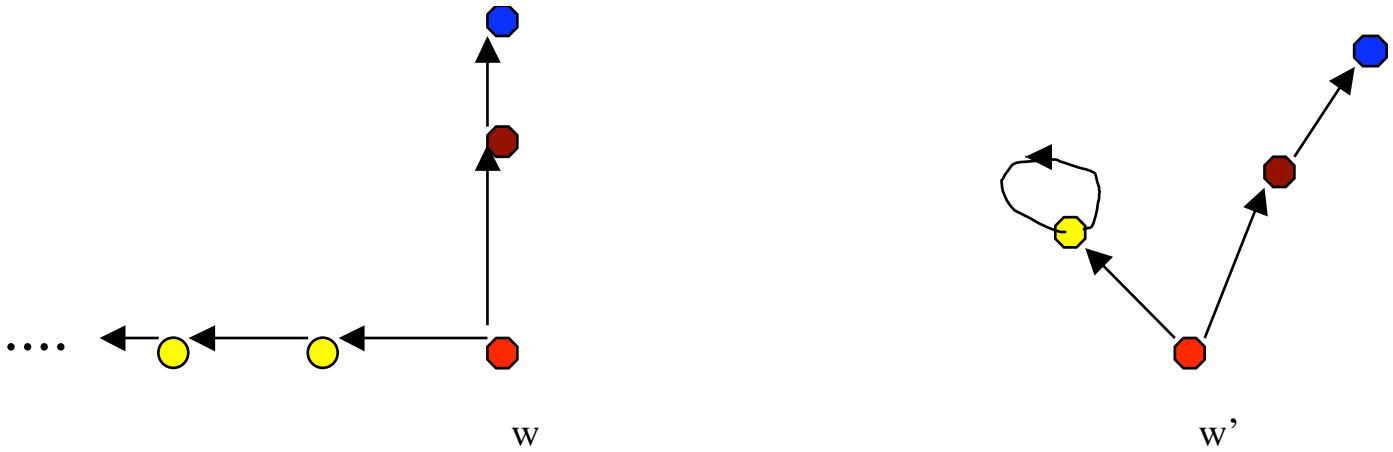
Logica Modale $\subseteq$ FO

μ-calculus $\subseteq$ MSO

Cosa perdiamo?

i nodi con lo stesso colore rappresentano lo stesso processo

w e w' sono "bisimili"



Le proprietà che ci interessano sono quelle che non distinguono fra w e w'

$F(x)$ è invariante per bisimulazione se, dati w e w' bisimili, vale

$$F(w) \Leftrightarrow F(w')$$

Le proprietà della logica modale e del μ-calculus sono invarianti per bisimulazione.

Teorema [van Benthem '70, Janin e Walukievicz 1999]

logica modale = frammento di FO invariante per bisimulazione

μ-calculus = frammento di MSO invariante per bisimulazione

La formula di FO:

$$\exists y(wRy \wedge yRy) \text{ non è invariante per bisimulazione;}$$

La formula di MSO (che esprime la proprietà "*dal nodo parte un cammino dove p vale infinite volte*"):

$$\nu X \mu Y[(P \wedge \Diamond X) \vee \Diamond Y] \text{ è invariante per bisimulazione.}$$

Il significato di una formula del μ-calculus con punti fissi annidati è molto difficile da comprendere . . .

Arena: un modello di Kripke M ed una formula F in un data logica.
Due giocatori: I, II
I e II giocano seguendo regole che dipendono dalla logica.

Una posizione del gioco è data da una coppia $[v, G]$, dove v è un punto in M e G è una *sottoformula* di F.

Dalla posizione iniziale $[w, F]$,
I vuole provare che F è falsa in w (falsifier);
II vuole provare che F è vera in w (verifier).

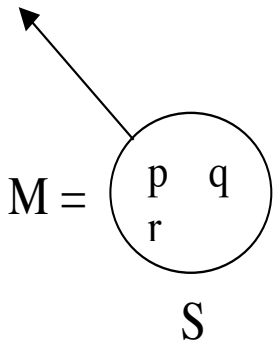
Gioco Proposizionale

$$G = G_1 \vee G_2 \mid G_1 \wedge G_2 \mid p \mid \neg p$$

Nel caso proposizionale, il gioco non si sposta mai da w (le posizioni del gioco sono sempre di tipo $[w, G]$).

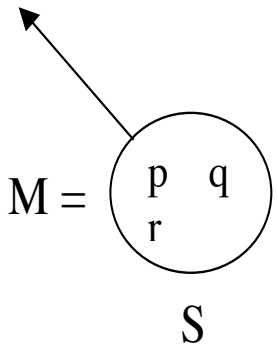
- se $G = G_1 \wedge G_2$, tocca ad I che sceglie una sottoformula G_i; il gioco riprende da $[w, G_i]$;
- se $G = G_1 \vee G_2$, tocca a II che sceglie una sottoformula G_i; il gioco riprende da $[w, G_i]$;
- arrivati ad un letterale ℓ ($\ell = p$ o $\ell = \neg p$), I vince se $w \not\models \ell$, II vince se $w \models \ell$.

Esempio di gioco proposizionale



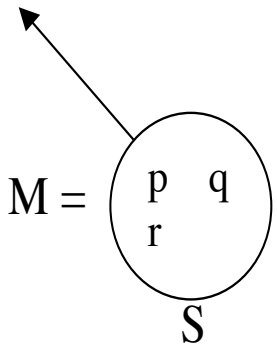
$$F = (\neg p \vee r) \wedge (\neg r \vee q)$$

Esempio di gioco proposizionale



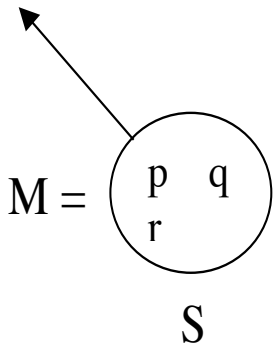
F = $(\neg p \vee r) \wedge (\neg r \vee q)$;
tocca ad I che sceglie $(\neg p \vee r)$;

Esempio di gioco proposizionale



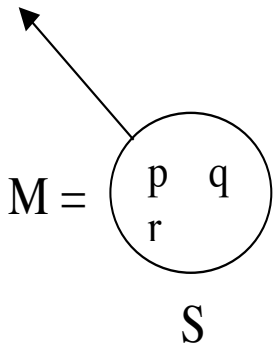
F = $(\neg p \vee r) \wedge (\neg r \vee q)$;
tocca ad I che sceglie $(\neg p \vee r)$;
tocca a II che sceglie r;

Esempio di gioco proposizionale



F = $(\neg p \vee r) \wedge (\neg r \vee q)$;
tocca ad I che sceglie $(\neg p \vee r)$;
tocca a II che sceglie r;
II vince perché r è vera in S

Esempio di gioco proposizionale



F = $(\neg p \vee r) \wedge (\neg r \vee q)$;
tocca ad I che sceglie $(\neg p \vee r)$;

NB se invece II scegliesse ¬p, perderebbe!

Strategie

- Una strategia vincente per II è una scelta delle mosse che permette a II di vincere qualsiasi cosa faccia I.
- Una strategia vincente per I è una scelta delle mosse che permette ad I di vincere qualsiasi cosa faccia II.

II ha una strategia vincente partendo da $[w, F] \Leftrightarrow w \models F$;

($\Leftarrow$: la strategia di *II* è: scegli sempre una sottoformula vera in $w \ldots$);

($\Rightarrow$: per induzione sulla complessità di F.)

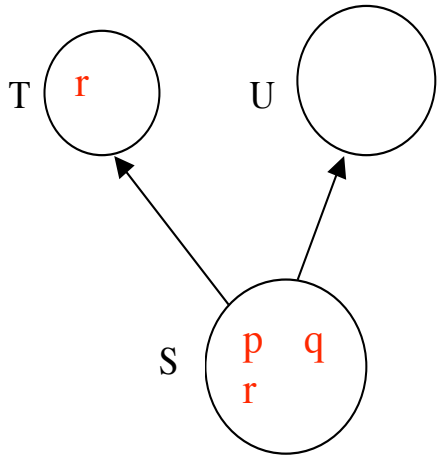
Gioco Modale

$$G = G_1 \vee G_2 \mid G_1 \wedge G_2 \mid \Box G \mid \Diamond G \mid p \mid \neg p$$

Al gioco si aggiungono le regole per gli operatori modali:

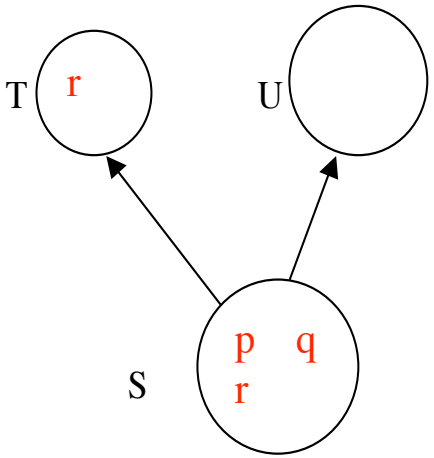
- dalla posizione $[w, \Box G']$ tocca ad I, che sceglie un successore w' di w; il gioco riprende dalla posizione $[w', G']$;
- dalla posizione $[w, \Diamond G']$ tocca a II che sceglie un successore w' di w; il gioco riprende dalla posizione $[w', G']$.

Esempio



Gioco (S,F)
con F= $\Diamond (p \vee r) \wedge r$

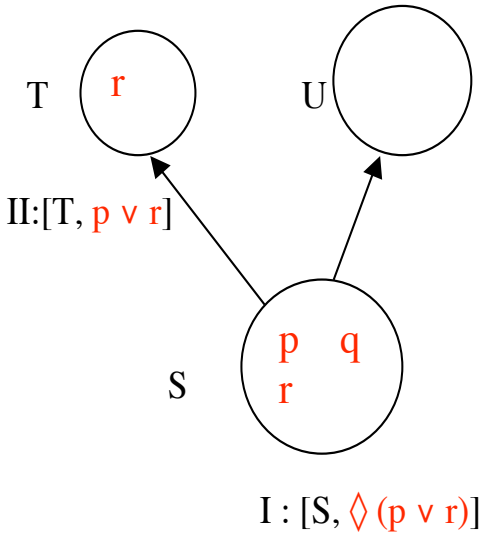
Esempio



I : [S, $\Diamond (p \vee r)$]

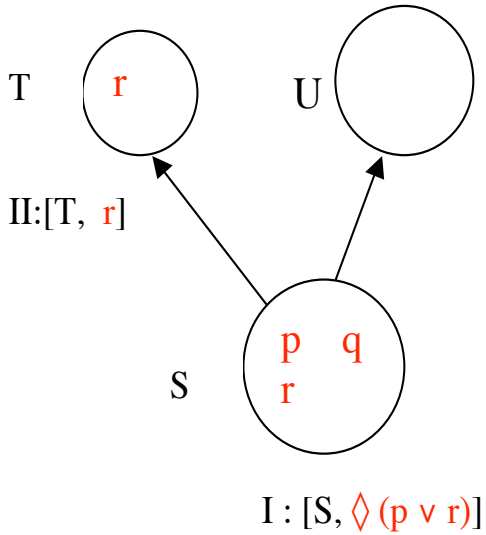
Gioco (S,F)
con F= $\Diamond (p \vee r) \wedge r$

Esempio



Gioco (S,F)
con F= $\Diamond (p \vee r) \wedge r$

Esempio



Gioco (S,F)
con F= $\Diamond (p \vee r) \wedge r$

II vince la partita

Giochi per il μ-calculus

I giochi visti finora sono *finiti*.
Se $F = \mu X G(X)$, quale mossa da una posizione $[w, F]$?
Siccome ha $G(F) = F$, le posizioni $[w, F]$ e $[w, G(F)]$ sono "equivalenti".
Gioco da posizione $[w, F]$ con F formula del μ-calculus:

- se $F = \mu X G$, $F = \nu X G$, si passa alla posizione $[w, G(F)]$;

ora le partite possono essere infinite e servono nuove condizioni di vittoria su queste partite in modo che

$$\text{II ha una strategia vincente a partire da } [w, F] \quad \Leftrightarrow w \models F$$

Un esempio di partita per $F = \mu X \Box X$

$$[w, F] \to [w, \Box F] \to^{I} [w', F] \to [w', \Box F] \to^{I} [w'', F] \to \dots$$

$$F = \mu X \Box X = \bigcup_{n} \Box^{n} \emptyset$$

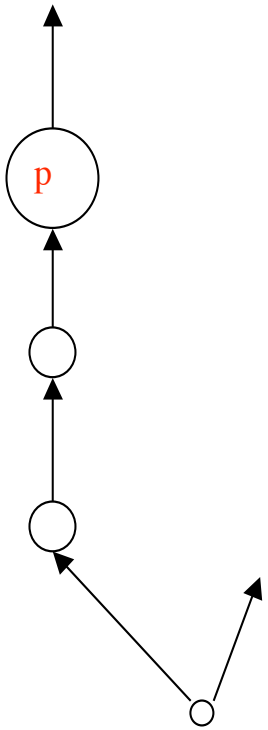
Quindi, se $M, w \models F$, esiste n tale che $w \in \Box^{n}\emptyset$ e la partita deve terminare
EX. se $w \models \Box^{2}\emptyset$: $\quad w \in F = \Box^{2}\emptyset, \quad w' \in \Box^{1}\emptyset, \quad w'' \in \emptyset.$
cioè: w' non ha successori e I non riesce a fare nessuna mossa, perdendo la partita.
Viceversa, se tutte le partite da $[w, F]$ terminano dopo un numero finito di passi, $w \models \mu X \Box X$.

$$w \models \mu X \Box X \Leftrightarrow \text{ tutte le partite da } [w, F] \text{ sono finite.}$$

Regole di vincita delle partite infinite: *I* vince tutte le partite infinite.

$$\textit{II} \text{ ha una strategia vincente da } [w, \mu X \Box X] \Leftrightarrow w \models \mu X \Box X$$

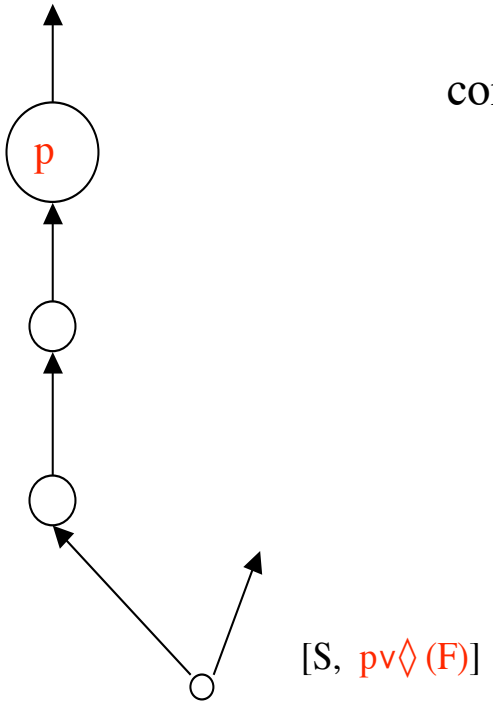
Un altro esempio: $\mu X(P \vee \Diamond X)$



Gioco (S,F)
con F= μ x (pv◊ (x))

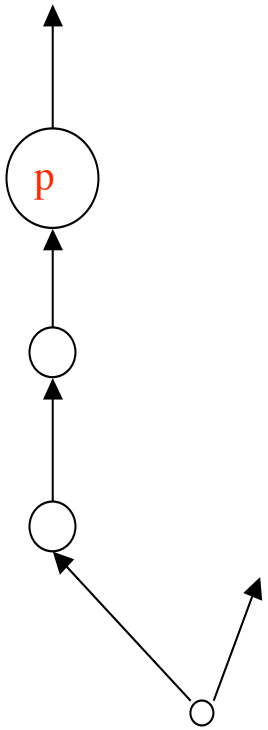
[S, μ x (pv◊ (x))]

Un altro esempio: $\mu X(P \vee \Diamond X)$



Gioco (S,F)
con F= μ x (pv◊ (x))

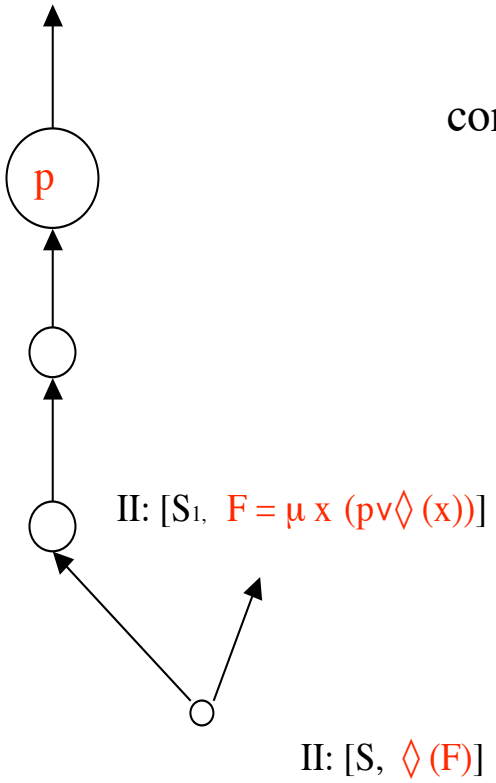
Un altro esempio: $\mu X(P \vee \Diamond X)$



Gioco (S,F)
con F= μ x (p∨◊ (x))

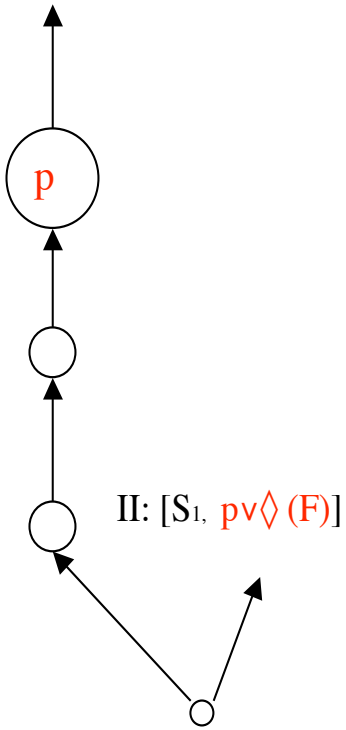
II: [S, ◊ (F)]

Un altro esempio: $\mu X(P \vee \Diamond X)$



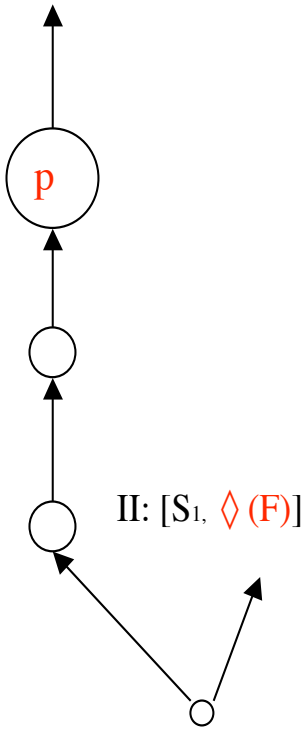
Gioco (S,F)
con F= μ x (pv◊ (x))

Un altro esempio: $\mu X(P \vee \Diamond X)$



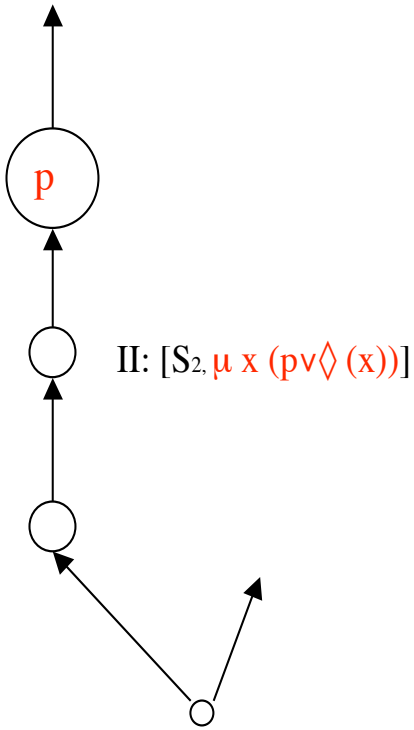
Gioco (S,F)
con F= μ x (pv◊ (x))

Un altro esempio: $\mu X(P \vee \Diamond X)$



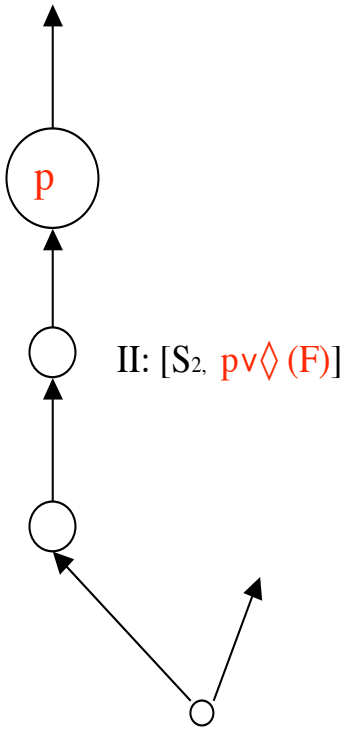
Gioco (S,F)
con F= μ x (p∨◊ (x))

Un altro esempio: $\mu X(P \vee \Diamond X)$



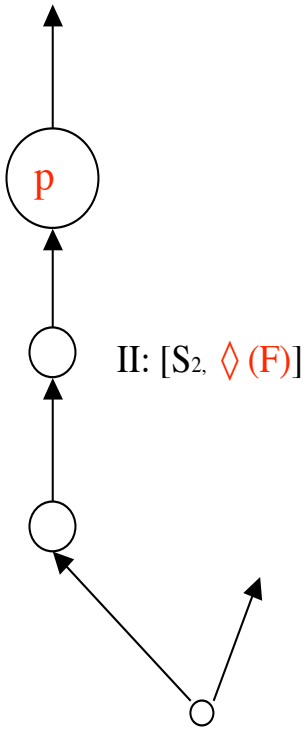
Gioco (S,F)
con F= μ x (pv◊ (x))

Un altro esempio: $\mu X(P \vee \Diamond X)$



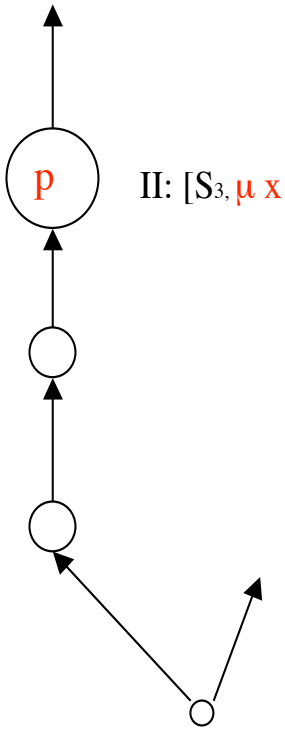
Gioco (S,F)
con F= μ x (pv◊ (x))

Un altro esempio: $\mu X(P \vee \Diamond X)$



Gioco (S,F)
con F= μ x (p∨◊ (x))

Un altro esempio: $\mu X(P \vee \Diamond X)$

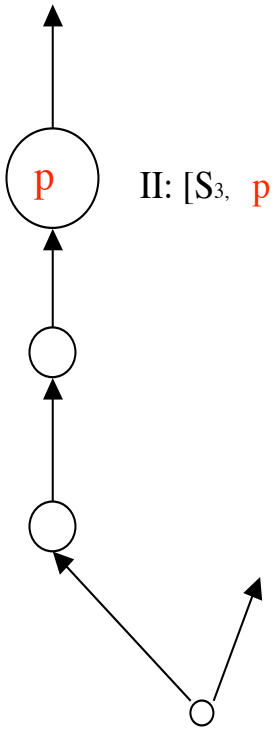


II: [S_3, μ x (pv◊ (x))]

Gioco (S,F)

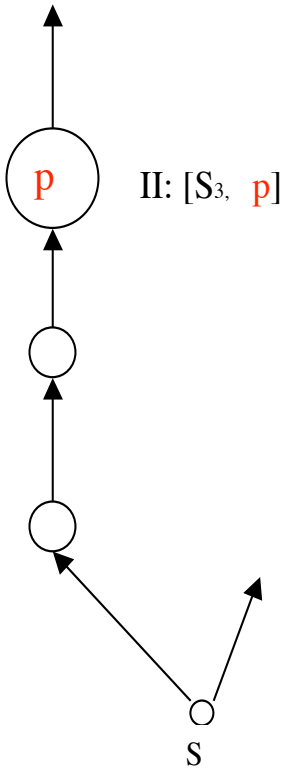
con F= μ x (pv◊ (x))

Un altro esempio: $\mu X(P \vee \Diamond X)$



Gioco (S,F)
con F= μ x (pv◊ (x))

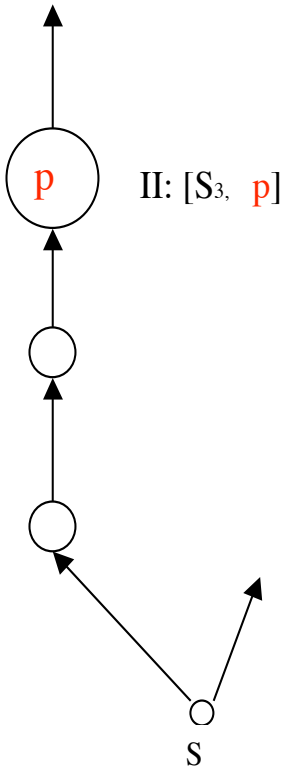
Un altro esempio: $\mu X(P \vee \Diamond X)$



Gioco (S,F)
con F= μ x (pv◊ (x))

se μ x (pv◊ (x)) è vera in S, II ha una strategia per vincere la partita

Un altro esempio: $\mu X(P \vee \Diamond X)$



Gioco (S,F)
con F= μ x (pv◊ (x))

se μ x (pv◊ (x)) è vera in S, II ha una strategia per vincere la partita

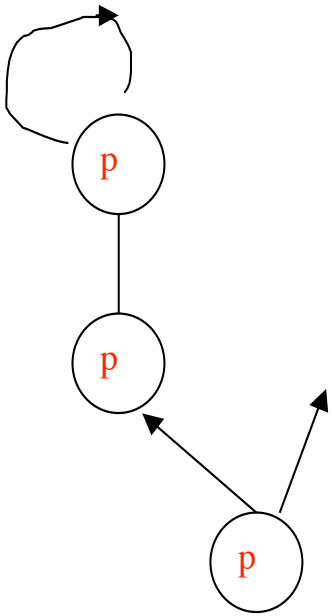
Vale anche il viceversa: se II ha una strategia vincente , allora μ x (pv◊ (x)) è vera in S

Più in generale:

- se $F = \mu X\ G$, con G modale, la regola di vincita è:
  I vince tutte le partite infinite,
- Dualmente, se $F = \nu X\ G$ (G modale), allora la regola di vincita è:
  II vince tutte le partite infinite.

Gioco per $\nu x(P \wedge \Diamond X)$

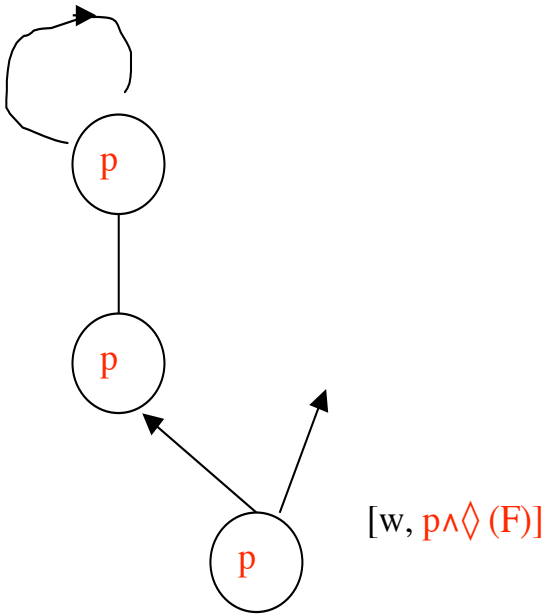
Gioco [w,F]
con F= ν x (p∧◊ (x))



[w, ν x (p∧◊ (x))]

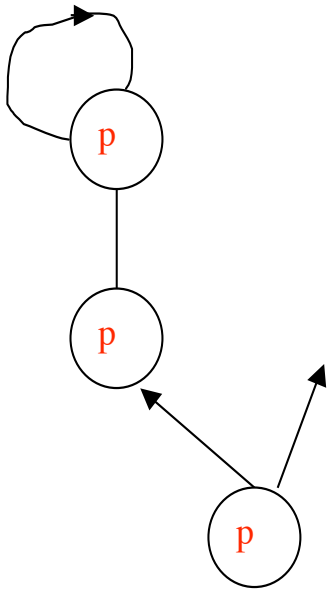
Gioco per $\nu x(P \wedge \Diamond X)$

Gioco [w,F]
con F= ν x ($p \wedge \Diamond$ (x))



Gioco per $\nu x(P \wedge \Diamond X)$

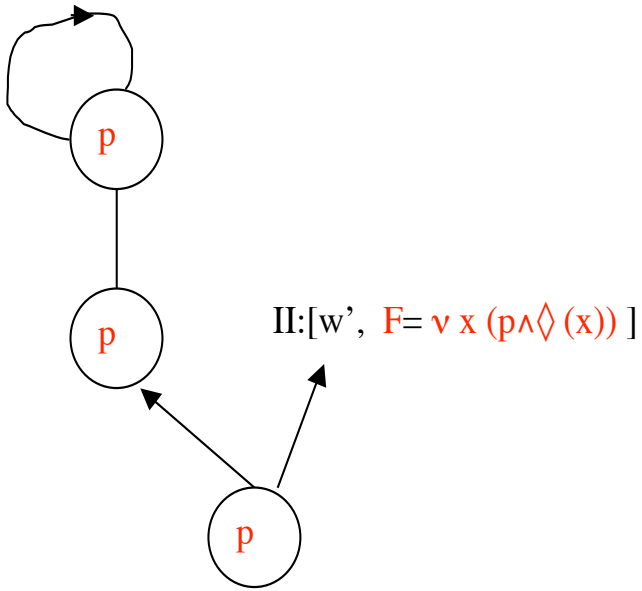
Gioco [w,F]
con F= ν x (p∧◊ (x))



I:[w, ◊ (F)]

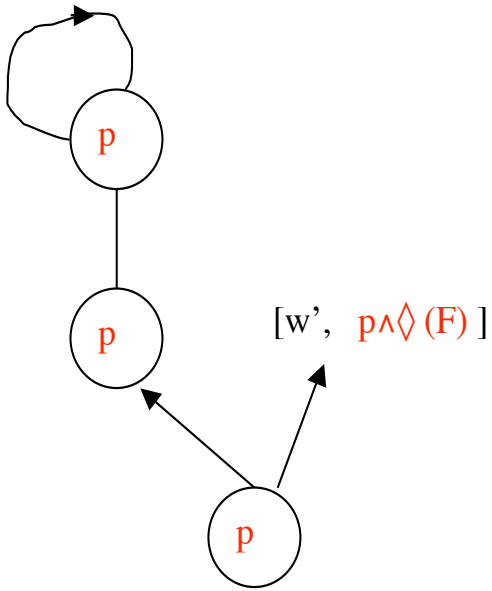
Gioco per $\nu x(P \wedge \Diamond X)$

Gioco [w,F]
con F= ν x (p∧◊ (x))



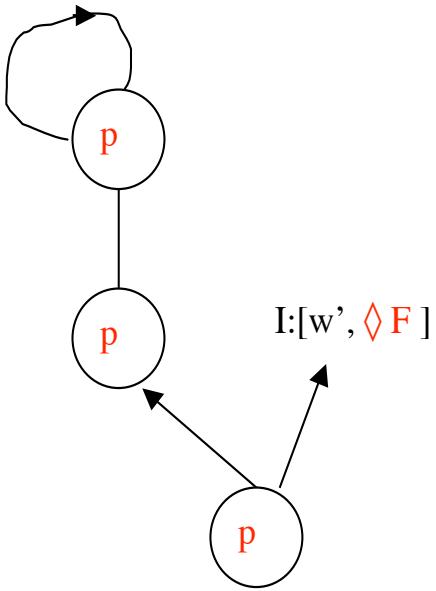
Gioco per $\nu x(P \wedge \Diamond X)$

Gioco [w,F]
con F= ν x (p∧◊ (x))



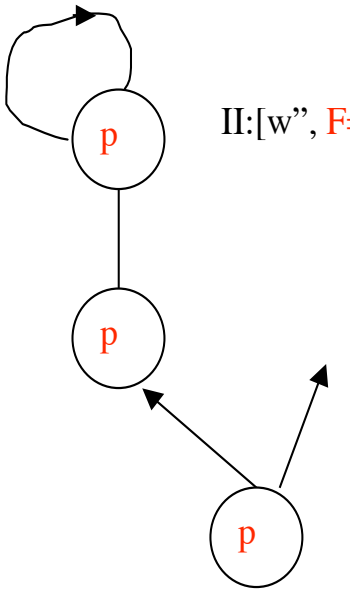
Gioco per $\nu x(P \wedge \Diamond X)$

Gioco [w,F]
con F= ν x (p∧◊ (x))



Gioco per $\nu x(P \wedge \Diamond X)$

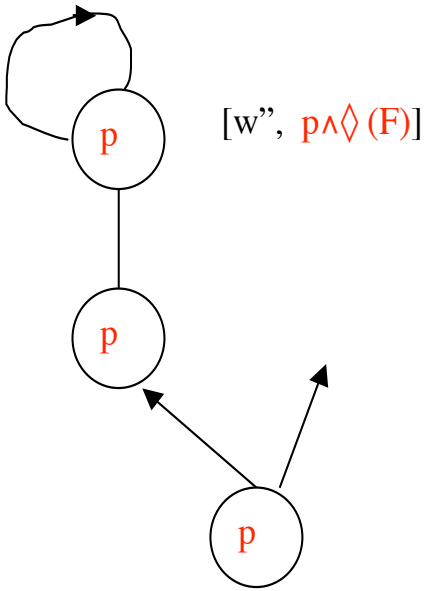
Gioco [w,F]
con F= ν x (p∧◊ (x))



II:[w", F=νx (p∧◊ (x))]

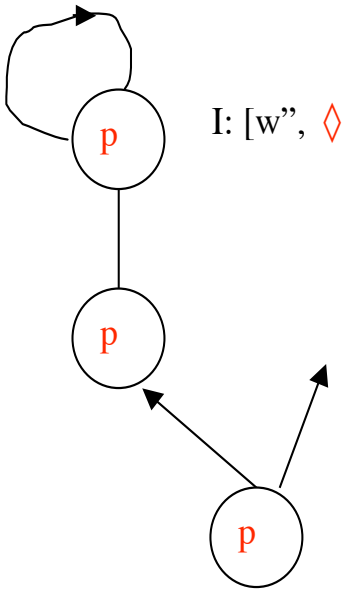
Gioco per $\nu x(P \wedge \Diamond X)$

Gioco [w,F]
con F= ν x (p∧◊ (x))



Gioco per $\nu x(P \wedge \Diamond X)$

Gioco [w,F]
con F= ν x (p∧◊ (x))



I: [w”, ◊ (F)] etc

I può decidere di terminare scegliendo p, ma perde
oppure di proseguire il gioco infinito ma perde lo stesso

Giochi di parità

Le regole si complicano se in F appaiono punti fissi annidati, come accade nella formula:

$$\nu X \mu Y[(P \wedge \Diamond X) \vee \Diamond Y]$$

che significa: dal nodo parte un cammino dove P vale infinite volte.
Dentro ν c'è un μ: a *Il* va bene ripercorrere ("rigenerare") infinite volte ν,
ma all'interno di ogni ciclo, deve ripercorrere (rigenerare) μ solo un numero finito di volte.
Soluzione: assegnare dei numeri naturali ai punti fissi, a seconda della posizione d'innesto (μ dispari, ν pari)

In generale, se $F = \nu x \mu y \nu z \mu u\ G$, con G modale, assegnamo gli indici così:

$$F = \nu^4 x \mu^3 y \nu^2 z \mu^1 u\ G.$$

Le partite infinite vengono vinte da II $\Leftrightarrow$ fra i punti fissi ripercorsi (rigenerati) infinite volte, l' indice maggiore è pari.
In una partita infinita, il punto fisso $\mu^3 y$ può essere ripercorso (rigenerato) infinite volte, ma solo se viene ripercorso (rigenerato) infinite volte anche $\nu^4 x$.

Ad ogni formula F del μ-calculus corrisponde un *gioco di parità* $G(\_, F)$ tale che, per ogni M, S vale:

$$M, S \models F \Leftrightarrow \textit{II} \text{ ha una strategia vincente in G(S,F).}$$

Viceversa, ad ogni gioco di parità corrisponde una formula del μ-calculus, che caratterizza le posizioni S vincenti per *II*.