Analisi del Software

Alessio Gjergji

Indice

1 Analisi **3**
- 1.1 Teorema di Rice . . . 4
  - 1.1.1 Definizione Formale . . . 4
  - 1.1.2 Conseguenze . . . 4
- 1.2 Approssimazione . . . 5
  - 1.2.1 Confronto tra analisi statica e analisi dinamica nella verifica delle specifiche dei programmi . . . 6
  - 1.2.2 Classificazione delle tecniche di analisi in base alle caratteristiche rinunciate per superare la non decidibilità . . . 7

2 Modelliamo programmi **8**
- 2.1 Un semplice linguaggio imperativo `IMP` . . . 8
  - 2.1.1 La semantica di `IMP` . . . 8
  - 2.1.2 Lo stato della memoria . . . 9
  - 2.1.3 Semantica delle transizioni di stato . . . 9
  - 2.1.4 Semantica delle espressioni . . . 10
  - 2.1.5 Semantica dei comandi . . . 10
- 2.2 Semantica Transazionale . . . 11
- 2.3 Semantica come punto fisso . . . 13
  - 2.3.1 Punto fisso inferiore . . . 13
  - 2.3.2 Punto fisso superiore . . . 14
  - 2.3.3 Semantica dei comandi come punto fisso . . . 15
- 2.4 Il Control Flow Graph . . . 15
  - 2.4.1 Blocchi di base . . . 16
  - 2.4.2 Identificare i blocchi di base . . . 16
  - 2.4.3 Esempio . . . 17
- 2.5 Il linguaggio `imp-CFG` . . . 19
  - 2.5.1 Semantica del linguaggio `imp-CFG` . . . 20
  - 2.5.2 Computazione del linguaggio `imp-CFG` . . . 21

3 Significato di approssimare **22**
- 3.1 L'idea di approssimazione . . . 22
  - 3.1.1 Astrazione della semantica . . . 23

3.1.2 Oggetti 23
3.1.3 Proprietà 24
3.2 Approssimazione dei dati 25
3.2.1 Approssimazione dal basso 25
3.2.2 Approssimazione dall'alto 26
3.2.3 Minima astrazione 26
3.2.4 Miglior astrazione 27
3.2.5 Esempio: `Sign` 27
3.3 Astrazione delle computazioni 28
3.3.1 Computazione di insiemi 29
3.3.2 Collecting semantics 29
3.3.3 Computazioni sulle proprietà 33

Capitolo 1

Analisi

L'analisi può essere costruita sia mediante l'elaborazione del codice sorgente che basandosi sul modello del programma. La scelta tra questi approcci dipende dalla situazione specifica.

Il Concetto di `CFG` (*Control Flow Graph, Grafo di Flusso di Controllo*) è affidabile per l'analisi statica, ma la sua precisione può variare a seconda di come viene costruito il modello del programma.

Ecco una panoramica delle due principali modalità di analisi:

- **Analisi Statica** (*senza esecuzione del codice*): Questo tipo di analisi è basato sulla struttura del codice sorgente e non richiede l'esecuzione del programma. Tuttavia, la sua principale limitazione è la precisione. L'analisi statica può fornire risultati decisi in modo certamente, ma può non essere completamente accurata nel catturare il comportamento reale del programma. È un'analisi basata sulla "visione teorica" del codice.
- **Analisi Dinamica** (*basata sull'esecuzione del codice*): In questo caso, l'analisi si basa sull'esecuzione effettiva del programma. Ciò fornisce una visione più accurata del comportamento, ma presenta sfide legate alla non terminazione e alla limitazione nell'eseguire tutti gli input possibili. L'analisi dinamica è solitamente basata su una serie limitata di input e non può garantire una copertura completa del comportamento del programma.

Entrambi gli approcci hanno limitazioni dovute al concetto di "non decidibilità" (**teorema di Rice**), che impedisce di ottenere risposte certe per alcune proprietà semantiche dei programmi.

L'obiettivo ideale dell'analisi sarebbe avere un sistema in grado di analizzare automaticamente qualsiasi programma in un linguaggio Turing completo come $\mathcal{L}$, fornendo risposte certe per tutte le proprietà semantiche in un tempo finito. Tuttavia, per ottenere un'analisi realistica, spesso è necessario fare delle compromissioni:

- **Automazione limitata**: Talvolta, per rendere l'analisi fattibile, è necessario rinunciare all'automazione completa e utilizzare un analizzatore solo su una classe limitata di programmi.

- **Accettazione dell'imprecisione controllata**: In alternativa, è possibile accettare un certo grado di imprecisione controllata nell'analisi, astrazione del risultato. Questo può essere fatto in modo completamente automatizzato ed è una caratteristica comune dell'analisi statica.

Tuttavia, è importante notare che togliendo l'automazione si perde la garanzia di rilevare tutti gli errori e le imprecisioni nell'analisi. Accettando l'imprecisione controllata, è comunque possibile ottenere risultati utili nell'ambito dell'analisi statica.

1.1 Teorema di Rice

Il Teorema di Rice è un importante risultato nella teoria della calcolabilità che dimostra le limitazioni fondamentali della verifica delle proprietà dei programmi. Il teorema afferma che, per qualsiasi proprietà non banale π di programmi, non esiste un algoritmo generale che possa determinare in modo decidibile se un programma p soddisfa la proprietà π. In altre parole, non è possibile costruire un analizzatore che, dato un programma p, determini in modo decidibile se p soddisfa π.

1.1.1 Definizione Formale

Per comprendere meglio il Teorema di Rice, introduciamo una definizione formale:

Sia $\mathcal{L}$ un linguaggio di programmazione e consideriamo l'insieme $\mathcal{P}$ di tutti i programmi validi scritti in $\mathcal{L}$. Ogni programma p in $\mathcal{P}$ è rappresentato da un numero naturale che funge da codifica univoca.

Definiamo una "proprietà di programma" π come un sottoinsieme di $\mathcal{P}$. In altre parole, π è un insieme di programmi che soddisfano una certa caratteristica o comportamento specifico.

Il Teorema di Rice afferma che, per ogni proprietà non banale π (ovvero, π non è vuota e $\pi \neq \mathcal{P}$), l'insieme $p \in \mathcal{P}, |, p$ soddisfa π è indecidibile.

Teorema di Rice

Sia $\mathcal{L}$ un linguaggio di programmazione Turing completo e sia π una proprietà non banale di programmi in $\mathcal{L}$. Allora, l'insieme $p \in \mathcal{L}$, p soddisfa π è indecidibile.

$$\forall \pi \text{ non banale } \exists \mathcal{L} \text{ Turing completo t.c. } \{p \in \mathcal{L} \mid p \text{ soddisfa } \pi\} \text{ è indecidibile}$$

Questo significa che non esiste un algoritmo generale che, dato un programma p, possa decidere in modo algoritmico se p appartiene all'insieme dei programmi che soddisfano la proprietà π.

1.1.2 Conseguenze

Il Teorema di Rice ha importanti conseguenze nella teoria della calcolabilità e nella verifica dei programmi. Dimostra che molte domande sulla correttezza o sul comportamento dei programmi non possono essere risolte in modo algoritmico generale. In altre parole, esistono

limitazioni intrinseche alla capacità di analizzare automaticamente i programmi per determinate proprietà. Questo teorema sottolinea l'importanza delle restrizioni sulle classi di problemi che possono essere risolti da algoritmi generici.

1.2 Approssimazione

L'approssimazione in analisi implica che una risposta non completamente accurata può ancora essere accettabile, a condizione che l'errore sia riconosciuto e possa essere descritto in modo controllato. Quindi, è importante distinguere tra l'inaccuratezza, che indica una leggera deviazione dalla precisione, e l'errore, che rappresenta una violazione significativa delle aspettative. π proprietà di analizzare, p programma, quindi Analisi$_\pi(p)$.

Nel contesto dell'analisi, consideriamo una proprietà π da analizzare su un programma p, che denotiamo come Analisi$\pi(p)$. Questo significa che per ogni programma p nel linguaggio $\mathcal{L}$, l'output dell'analisi, ovvero Analisi$\pi(p)$, sarà "true" solo se il programma p soddisfa la proprietà π. In altre parole, l'analisi ci dice se un programma rispetta la proprietà o meno.

$$\forall p \in \mathcal{L} \qquad Analisi_\pi(p) = true \Leftrightarrow p\, soddisfa\, \pi$$

Tuttavia, è importante notare che non sempre è possibile ottenere una bi-implicazione perfetta tra l'analisi e la proprietà. Ciò significa che, in alcuni casi, l'analisi potrebbe non essere in grado di fornire una risposta definitiva riguardo alla proprietà π, ma può comunque essere utilizzata per valutare in modo approssimativo e controllato l'aderenza del programma alla proprietà. Questo compromesso tra completezza e precisione è spesso necessario nell'ambito dell'analisi statica per rendere l'analisi praticamente realizzabile.

Soundness (*Correttezza*)

La correttezza (*o soundness*) dell'analisi implica che se l'output dell'analisi, cioè $Analisi_\pi(p)$, è "true," allora il programma p deve effettivamente soddisfare la proprietà π.

$$Analisi_\pi(p) = true \Rightarrow p\, soddisfa\, \pi$$

In altre parole, se l'analisi dice che un programma soddisfa la proprietà, questa affermazione è accurata. Tuttavia, è importante notare che se l'analisi restituisce "false," l'analizzatore potrebbe sovrastimare i programmi che non soddisfano la proprietà, includendo programmi che in realtà potrebbero soddisfarla. In termini pratici, ciò significa che l'analisi potrebbe essere conservativa nel rifiutare alcuni programmi.

Completezza

La completezza implica che se un programma p soddisfa effettivamente la proprietà π, allora l'output dell'analisi, cioè $Analisi_\pi(p)$, deve essere "true."

$$Analisi_\pi(p) = true \Leftarrow p\, soddisfa\, \pi$$

quindi

$$p\, soddisfa\, \pi \Rightarrow Analisi_\pi(p) = true$$

In altre parole, se un programma rispetta la proprietà, l'analisi dovrebbe essere in grado di riconoscerlo come tale e restituire una risposta positiva. Questo garantisce che l'analisi non dia risultati falsi negativi, ossia non manchi di riconoscere programmi che soddisfano la proprietà.

In sintesi, la correttezza ci assicura che l'analisi non dia risultati falsi positivi, mentre la completezza ci assicura che l'analisi non dia risultati falsi negativi. Tuttavia, spesso è difficile ottenere sia la completa correttezza che la completa completezza in un'analisi, e quindi si deve trovare un equilibrio tra queste due proprietà.

Supponiamo di avere un programma p nel linguaggio $\mathcal{L}$ e desideriamo determinare se una determinata proprietà π vale su di esso. In generale, non è sempre possibile condurre un'analisi diretta su p a causa della complessità del codice. Per affrontare questa sfida, trasformiamo il nostro codice in un modello astratto su cui possiamo applicare strumenti automatici come grafi di flusso di controllo (`CFG`), automi, e così via. Su questi modelli, spesso disponiamo di tecniche algoritmiche decidibili per stabilire se una versione adattata della proprietà π, denotata come π', vale sul programma p. Questa trasformazione del codice in un modello astratto consente di sfruttare strumenti automatizzati per ottenere informazioni sulla proprietà π'.

La perdita di precisione si verifica quando la risposta definitiva ottenuta dal modello astratto non si traduce in modo accurato nella risposta ottenuta direttamente dal programma originale. La precisione si perde nella transizione dall'affermazione:

$$\pi' \text{ vale sul modello di } p \Longrightarrow \pi \text{ vale su } p$$

In altre parole, non sempre possiamo garantire che se la proprietà π' vale sul modello astratto di p, allora la proprietà π vale direttamente sul programma p senza errori o imprecisioni.

1.2.1 Confronto tra analisi statica e analisi dinamica nella verifica delle specifiche dei programmi

Immaginiamo di avere un programma e una specifica, rappresentata dalla proprietà π, che vogliamo verificare. Nell'analisi statica, esaminiamo la proprietà π direttamente nel codice sorgente del programma senza eseguirlo. In altre parole, effettuiamo un'analisi basata solo sulla struttura e sulla sintassi del codice.

D'altra parte, l'analisi dinamica prende in input il programma e valuta la relazione tra gli input forniti e gli output generati durante l'esecuzione del programma. In questo caso, l'analisi

dinamica può non avere conoscenza completa del codice sorgente, ma si concentra sulla valutazione del comportamento effettivo del programma attraverso l'esecuzione (*questo approccio è spesso chiamato "testing"*).

Quindi, mentre l'analisi statica si basa sull'analisi del codice sorgente aperto per determinare se la proprietà π è verificata, l'analisi dinamica si concentra sull'esecuzione del programma e sull'osservazione del comportamento in relazione agli input dati.

1.2.2 Classificazione delle tecniche di analisi in base alle caratteristiche rinunciate per superare la non decidibilità

Per affrontare le limitazioni imposte dal Teorema di Rice, le tecniche di analisi possono rinunciare a alcune caratteristiche chiave. Queste caratteristiche includono:

- **Automatico**: La capacità di eseguire l'analisi senza intervento umano.
- $\forall p \in \mathcal{L}$: La capacità di analizzare qualsiasi programma nel linguaggio $\mathcal{L}$.
- **Corretto**: La capacità di fornire risultati accurati e privi di errori.
- **Completo**: La capacità di coprire tutti i possibili casi e fornire risposte definitive.

A seconda delle caratteristiche a cui si rinuncia, emergono diverse classi di analisi:

- Verifica (*Model checking*): Questa tecnica si basa su insiemi finiti di stati o comportamenti del sistema. Rinuncia alla possibilità di analizzare tutti i programmi, ma rimane automatica ed è corretta e completa all'interno del modello specifico.
- Analisi Conservative (*Statiche*): Le analisi conservative cercano di estrarre informazioni in modo statico dal programma. Forniscono una semantica approssimata ma conservativa del programma, il che significa che le proprietà approssimate implicano le proprietà concrete. Questa tecnica è automatica, lavora su programmi rappresentabili finitamente ed è corretta ma non completa (*operando solo su specifiche proprietà*).
- Bug finding (*Debugging*): Il debugging è una tecnica di supporto per gli sviluppatori che può fornire risposte con perdita sia di correttezza che di completezza. È principalmente utilizzato per identificare e risolvere errori durante lo sviluppo del software.
- Testing: Il testing è una tecnica dinamica che comporta l'esecuzione del programma su un insieme selezionato di input. Non ha limitazioni sul tipo di programmi che può analizzare, ma rinuncia alla correttezza, intesa come copertura completa degli input. Quando un test rileva una violazione della proprietà, si può concludere che la proprietà non è soddisfatta.

Queste diverse classi di analisi offrono trade-off tra automazione, capacità di analisi, precisione e completezza, e vengono utilizzate in base alle esigenze specifiche di verifica e analisi dei programmi.

Capitolo 2

Modelliamo programmi

2.1 Un semplice linguaggio imperativo `IMP`

Definiamo il linguaggio $\mathcal{L}$ dove:

$$\mathbb{V} = \mathbb{Z}$$
$$\mathbb{X} = \texttt{Var}$$

$$\begin{aligned}
\textit{Exp}\ \mathbb{E} &::= n \in \mathbb{V} \mid x \in \mathbb{X} \mid \mathbb{E} \oplus \mathbb{E} \\
\textit{Bool}\ \mathbb{B} &::= \texttt{true} \mid \texttt{false} \mid \mathbb{E} \oplus \mathbb{E} \\
\textit{Com}\ \mathbb{C} &::= \texttt{skip} \mid \mathbb{X} := \mathbb{E} \mid \mathbb{C}; \mathbb{C} \mid \texttt{if}\ \mathbb{B}\ \texttt{then}\ \mathbb{C}\ \texttt{else}\ \mathbb{C} \\
&\quad \mid \texttt{while}\ \mathbb{B} \mid \texttt{input(x)} \\
\textit{Programma}\ \mathbb{P} &::= \mathbb{C}
\end{aligned}$$

2.1.1 La semantica di `IMP`

La semantica è uno strumento formale che permette di dare significato ai programmi.

Semantica operazionale

La semantica operazionale è uno strumento formale che fornisce significato ai programmi attraverso la descrizione del comportamento passo dopo passo dell'interprete. Questo significa che il significato di un programma è descritto dalla sequenza dei singoli passi di computazione che esso compie.

Semantica denotazionale

La semantica denotazionale attribuisce significato ai programmi tramite una funzione che associa a ciascun programma un valore. In termini matematici, possiamo rappresentare questa idea come segue:

$$\texttt{intput} \xrightarrow[\text{semantica}]{} \texttt{output}$$

In altre parole, esiste una funzione $[\![.]\!]$ che mappa l'input del programma all'output. Questa approccio è composito, il che significa che possiamo definire il significato di programmi composti in termini dei loro componenti, come segue:

$$[\![.]\!] : \texttt{intput} \to \texttt{output}$$

$$[\![P_1; P_2]\!] = [\![P_2]\!] \oplus [\![P_1]\!]$$

Queste due forme di semantica, operazionale e denotazionale, sono strumenti utili per comprendere il significato dei programmi in modo dettagliato e matematico.

2.1.2 Lo stato della memoria

Nel contesto della programmazione, lo "stato" rappresenta una fotografia istantanea della configurazione della macchina (*astratta*) su cui viene eseguito un programma. Questo stato descrive l'associazione tra le variabili del programma e i valori che contengono. Formalmente, possiamo rappresentare lo stato come una funzione $\mathbb{M}$ che mappa le variabili ($\mathbb{X}$) ai loro valori ($\mathbb{V}$), come segue:

$$\mathbb{M} : \mathbb{X} \to \mathbb{V}$$

Durante l'esecuzione di un programma, viene generata una sequenza di stati che riflettono come il programma modifica lo stato della memoria nel corso del tempo. Questa sequenza di stati è essenziale per comprendere come il programma funziona e come influisce sullo stato della macchina. Nel contesto della modellazione formale, spesso ci riferiamo a questo processo come "esecuzione".

Per descrivere l'evoluzione di uno stato durante l'esecuzione di un programma, utilizziamo un modello chiamato "sistema di transizione", che è rappresentato da una coppia $\langle \Sigma, \to \rangle$. In questa coppia, Σ rappresenta l'insieme degli stati possibili e $\to$ rappresenta la relazione che specifica come un determinato stato può transizionare in un altro stato a seguito dell'esecuzione di un'azione del programma. Questo modello è fondamentale per analizzare il comportamento dinamico di un programma e comprendere come le modifiche di stato si verificano nel corso dell'esecuzione.

2.1.3 Semantica delle transizioni di stato

La semantica è definita come l'insieme di tutte le possibili sequenze di transizioni di stato (*eventualmente infinite*) a partire dagli stati iniziali, ovvero le esecuzioni delle istruzioni di un programma, indicate da sequenze di stati nel sistema di transizione.

Fornisce il significato dei programmi attraverso l'esecuzione delle loro istruzioni su un interprete (*cioè componendo gli effetti delle istruzioni*).

Il modello matematico si basa sull'utilizzo delle tracce in un sistema di transizione.

2.1.4 Semantica delle espressioni

La semantica delle espressioni è definita come segue:

$$[\![E]\!] : \mathbb{M} \to \mathbb{V}$$

a partire dalla memoria in $\mathbb{M}$ restituisce:

Valori

Il valore in $\mathbb{V}$ rappresentato da e. In altre parole:

$$m \in \mathbb{M} \quad , n \in \mathbb{V}$$

$$[\![n]\!](m) = n$$

$$[\![x]\!](m) = m(x)$$

Quindi, per un'espressione composta:

$$[\![e_1 \oplus e_2]\!](m) = f_{\oplus}([\![e_1]\!](m), [\![e_2]\!](m))$$

Dove il simbolo $\oplus$ è il simbolo sintattico e $f_{\oplus}$ è la funzione semantica.

Booleani

Per i valori booleani:

$$b \in \mathbb{B} \qquad [\![tt]\!](m) = tt \qquad [\![ff]\!](m) = ff$$

$$[\![b_1 \oplus b_2]\!](m) = f_{\oplus}([\![b_1]\!](m), [\![b_2]\!](m))$$

2.1.5 Semantica dei comandi

La semantica dei comandi è definita come segue:

$$c \in \mathbb{C}. \quad [\![c]\!] : \mathbb{M} \to \mathbb{M}$$

`skip`

L'istruzione `skip` rappresenta un comando nullo che non modifica lo stato della memoria.

$$[\![\texttt{skip}]\!](m) = m$$

Composizione

La composizione di due comandi c_1 e c_2 esegue prima c_1 e poi c_2. La semantica della composizione è data da:

$$[\![c_1; c_2]\!](m) = [\![c_2]\!]([\![c_1]\!](m)) = [\![c_2]\!] \oplus [\![c_1]\!](m)$$

Assegnamento

L'assegnamento dell'espressione e alla variabile x modifica lo stato della memoria mappando x al valore di e in m.

$$[\![x := e]\!](m) = m[x \mapsto [\![e]\!](m)]$$

`input`

L'istruzione `input(x)` rappresenta l'input di un valore n nella variabile x all'interno dello stato della memoria m.

$$[\![\texttt{input(x)}]\!](m) = m[x \mapsto n] \quad n \in \mathbb{V}$$

If-then-else

L'istruzione condizionale `if b then c_1 else c_2` esegue c_1 se la condizione b è vera, altrimenti esegue c_2.

$$[\![\texttt{if} \quad b \quad \texttt{then} \quad c_1 \quad \texttt{else} \quad c_2]\!](m) = \begin{cases} [\![c_1]\!](m) & \text{se } [\![b]\!](m) = \texttt{true} \\ [\![c_2]\!](m) & \text{se } [\![b]\!](m) = \texttt{false} \end{cases}$$

While

L'istruzione `while b do c` rappresenta un ciclo che continua a eseguire c fintanto che la condizione b è vera. La semantica di `while` è definita come segue:

$$[\![\texttt{while} \quad b \quad \texttt{do} \quad c]\!](m) = \begin{cases} [\![\texttt{while} \quad b \quad \texttt{do} \quad c]\!]([\![c]\!](m)) & \text{se } [\![b]\!](m) = \texttt{true} \\ m & \text{se } [\![b]\!](m) = \texttt{false} \end{cases}$$

Il while può comportare un ciclo infinito. Per gestire questa eventualità, si utilizza il concetto di traccia del programma e il punto di programma, raccogliendo gli stati raggiunti fino a quel punto. Questo permette di lavorare con proprietà degli input invece di manipolare singoli valori, affrontando problemi legati all'infinito.

2.2 Semantica Transazionale

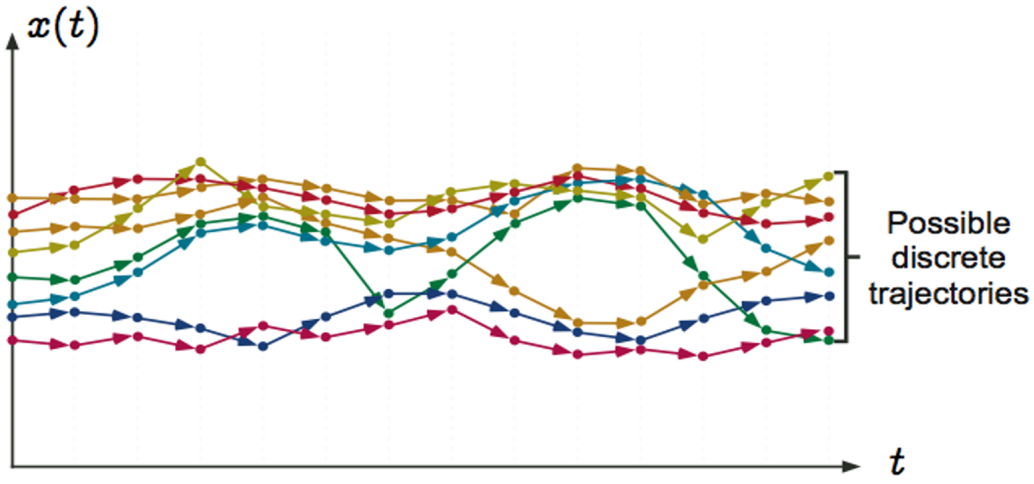
La semantica transazionale è un approccio alla comprensione del comportamento dei programmi attraverso la raccolta e l'analisi delle tracce di esecuzione. Questo approccio considera l'insieme di tutte le tracce di esecuzione possibili, partendo dagli stati iniziali del programma.

Questa raccolta di tracce è nota come "program trace semantics" (*semantica delle tracce di programma*).

Le tracce di programma forniscono una visione dettagliata dell'evoluzione del programma nel tempo, inclusi gli stati intermedi e le transizioni tra di essi. Questa analisi delle tracce è preziosa per comprendere come il programma risponde a diverse condizioni e input, e può rivelare informazioni importanti sul suo comportamento dinamico.

La semantica transazionale è particolarmente utile per affrontare problemi legati all'infinito, in quanto consente di lavorare con tracce e punti di programma invece di manipolare singoli valori. Questo approccio facilita la gestione delle esecuzioni potenzialmente infinite, fornendo una base solida per l'analisi formale dei programmi.

Nel complesso, la semantica transazionale fornisce uno strumento potente per la comprensione approfondita del comportamento dei programmi, evidenziando le variazioni nello stato della memoria nel corso dell'esecuzione e consentendo l'analisi delle proprietà attraverso l'osservazione delle tracce di programma.



2.3 Semantica come punto fisso

Semantica a punto fisso

Dato un dominio D di stati e una funzione F:

- D è un ordine parziale, cioè $\langle D, \leq \rangle$ è un *po-set*, dove D soddisfa le seguenti proprietà:
  - Riflessività: $\forall x \in D : x \leq x$.
  - Antisimmetria: $\forall x, y \in D : (x \leq y \land y \leq x) \Rightarrow x = y$.
  - Transitività: $\forall x, y, z \in D : (x \leq y \land y \leq z) \Rightarrow x \leq z$.
- $F : D \to D$ è una funzione totale e monotona, il che significa che per ogni x e y in D se $x \leq y$, allora $F(x) \leq F(y)$. Inoltre, la funzione F è iterabile, cioè può essere composta con se stessa più volte, ottenendo $F^n(x) = F(F(F(\ldots F(x)))$.

Un sistema di transizione è una coppia $\langle \Sigma, \tau \rangle$, dove Σ è un insieme non vuoto di stati e τ è una relazione di transizione che collega gli stati. In altre parole, un sistema di transizione rappresenta un insieme di stati e le relazioni tra di essi, ed è utilizzato per descrivere il comportamento di sistemi o programmi.

2.3.1 Punto fisso inferiore

- Il punto rosso $\odot$ rappresenta un stato bloccato.
- Il punto blu $\bullet$ rappresenta uno stato non bloccato.

Quindi, possiamo rappresentare l'evoluzione del sistema attraverso iterazioni. Iniziamo con un insieme vuoto di stati X^0: Nella prima iterazione, otteniamo l'insieme X^1 contenente uno stato bloccato:

$$X^0 = \varnothing$$

Nella prima iterazione, otteniamo l'insieme X^1 contenente uno stato bloccato:

$$X^1 = \{\odot\}$$

Nella seconda iterazione, aggiungiamo uno stato non bloccato con una transizione τ dall'insieme X^1 all'insieme X^2:

$$X^2 = \{\odot, \bullet \xrightarrow{\tau} \odot\} \qquad \text{dove } \{\odot\} \cup \bullet \xrightarrow{\tau} \{\odot\}$$

In questa iterazione, uno stato non bloccato può avanzare diventando uno stato bloccato. La notazione $\bullet \xrightarrow{\tau}$ indica una transizione che può verificarsi. Nella terza iterazione, continuiamo ad aggiungere stati e transizioni: Qui vediamo che gli stati non bloccati possono ancora avanzare tramite transizioni τ, ma alla fine possono diventare stati bloccati.

Tutti gli stati contenuti in X^3 rappresentano gli stati terminati del sistema, ossia quegli stati in cui il sistema non può avanzare ulteriormente.

Qui vediamo che gli stati non bloccati possono ancora avanzare tramite transizioni τ, ma alla fine possono diventare stati bloccati.

Tutti gli stati contenuti in X^3 rappresentano gli stati terminati del sistema, ossia quelli in cui il sistema non può avanzare ulteriormente.

La notazione finale, $lfp^{\subseteq}_{\varnothing} F^+$, rappresenta il calcolo del punto fisso inferiore di una funzione o di un operatore F in questo contesto. In questo calcolo, stiamo cercando il più piccolo insieme di stati che rimane invariato quando applichiamo l'operatore F iterativamente a partire da un insieme vuoto. Questo è fondamentale per identificare gli stati stabili o terminali in un sistema o un processo.

2.3.2 Punto fisso superiore

- Il punto rosso $\odot$ rappresenta uno stato bloccato.
- Il punto blu $\bullet$ rappresenta uno stato non bloccato.
- Il punto arancione $\bullet$ rappresenta uno stato non bloccato che può avanzare e diventare uno stato bloccato.

Ora, possiamo rappresentare l'evoluzione del sistema attraverso iterazioni. Iniziamo con un insieme iniziale X^0 che contiene uno stato non bloccato che può avanzare e diventare uno stato bloccato, con un numero di passi non definito:

$$X^0 = \{\bullet, \bullet \xrightarrow{?} \bullet, \bullet \xrightarrow{?} \bullet \xrightarrow{?} \bullet, \ldots, \bullet \xrightarrow{?} \bullet \ldots \bullet \xrightarrow{?} \bullet, \ldots\}$$

Nella prima iterazione, otteniamo l'insieme X^1, che include uno stato bloccato e uno stato non bloccato che può avanzare tramite una transizione τ:

$$X^1 = \{\odot, \bullet \xrightarrow{\tau} \bullet, \bullet \xrightarrow{\tau} \bullet \xrightarrow{?} \bullet, \ldots, \bullet \xrightarrow{\tau} \bullet \ldots \bullet \xrightarrow{?} \bullet, \ldots\}$$

Nella seconda iterazione, otteniamo l'insieme X^2, che include uno stato bloccato, uno stato non bloccato che può avanzare tramite una transizione τ, e uno stato non bloccato che può continuare a evolversi:

$$X^2 = \{\odot, \bullet \xrightarrow{\tau} \odot, \bullet \xrightarrow{\tau} \bullet \xrightarrow{\tau} \bullet, \ldots, \bullet \xrightarrow{\tau} \bullet \xrightarrow{\tau} \bullet \ldots \bullet \xrightarrow{?} \bullet, \ldots\}$$

Qui vediamo che gli stati non bloccati possono avanzare tramite transizioni τ, ma alla fine possono diventare stati bloccati.

L'insieme $\{\odot\} \cup \bullet \xrightarrow{\tau} \Sigma^+$ rappresenta il punto fisso superiore (*gfp*) in questo contesto. Il *gfp* rappresenta il più grande insieme di stati che rimane invariato quando applichiamo l'operatore Σ^+ iterativamente a partire da un insieme vuoto. In altre parole, è l'insieme più grande in cui gli stati non bloccati possono continuare a evolversi. Il *gfp* è fondamentale per identificare gli stati stabili o terminali in un sistema o un processo.

$$gfp^{\subseteq}_{\Sigma^\omega} F^\omega$$

2.3.3 Semantica dei comandi come punto fisso

La semantica dei comandi mappa un insieme di input in un insieme di stati.

$$[\![\mathbb{C}]\!]_{\wp} : \wp P(\mathbb{M}) \to \wp(\mathbb{M})$$

$$[\![\texttt{skip}]\!]_{\wp}(M) = M$$

$$[\![C_0; C_1]\!]_{\wp}(M) = [\![C_1]\!]_{\wp}([\![C_0]\!]_{\wp}(M))$$

$$[\![\texttt{x:= E}]\!]_{\wp}(M) = \{m[x \mapsto [\![E]\!]_M(m)] \mid m \in M\}$$

$$[\![\texttt{input(x)}]\!]_{\wp}(M) = \{m[x \mapsto n] \mid m \in M, n \in \mathbb{V}\}$$

$$[\![\texttt{if B then C else C'}]\!]_{\wp}(M) = [\![C_0]\!]_{\wp}(\mathcal{F}_B(M)) \cup [\![C_1]\!]_{\wp}(\mathcal{F}_{\neg B}(M))$$

$$[\![\texttt{while B do C}]\!]_{\wp}(M) = \mathcal{F}_{\neg B}\left(\bigcup_{i\geq 0}([\![C]\!]_{\wp} \circ \mathcal{F}_B)^i(M)\right)$$

Dove:

$$\mathcal{F}_B(M) = \{m \in M | [\![B]\!](m) = \texttt{true}\}$$

Semantica del ciclo

Dobbiamo partizionare l'esecuzione basandola sul numero di iterazioni che il ciclo esegue prima di uscire. L'insieme degli output è l'infinita unione della famiglia di insiemi M_i che denotano gli stati prodotti dal programma in esecuzione.

$$M_i = \mathcal{F}_{\neg B}\left(([\![C]\!]_{\wp} \circ \mathcal{F}_B)^i(M)\right)$$

Dove:

$$\bigcup_{i\geq 0} M_i = \bigcup_{i\geq 0} \mathcal{F}_{\neg B}\left(([\![C]\!]_{\wp} \circ \mathcal{F}_B)^i(M)\right) = \mathcal{F}_{\neg B}\left(\bigcup_{i\geq 0}([\![C]\!]_{\wp} \circ \mathcal{F}_B)^i(M)\right)$$

Notiamo che:

$$\mathcal{F}_{\neg B}(lfp_M F) \ \textit{dove}\ F : M' \mapsto M \cup [\![C]\!]_{\wp} \circ (\mathcal{F}_B(M'))$$

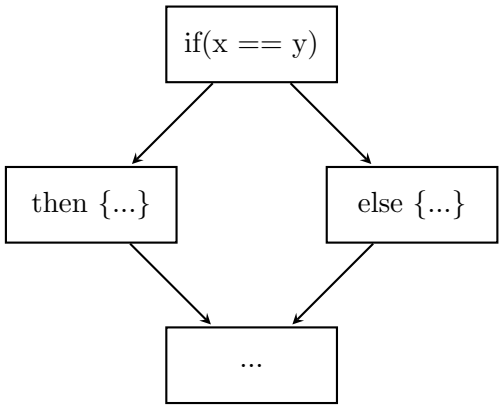
2.4 Il Control Flow Graph

Il *Control Flow Graph* (CFG) è un grafo diretto che rappresenta il flusso di controllo di un programma. Il grafo è generato dalla sintassi del programma. Lo scopo principale di tale grafo è quello di permettere di capire facilmente la struttura del codice rilevando codice morto, cicli infiniti, e altre caratteristiche del programma. È quindi utile per l'analisi statica del codice.

Il `CFG` è un grafo diretto $G = (N, E)$ dove:

- un nodo $n \in N$ rappresenta un blocco di codice, ovvero è una sequenza massimale di istruzioni con un singolo punto di ingresso, un singolo punto di uscita e senza diramazioni interne. Per semplicità, assumiamo un unico nodo d'ingresso n_0 e un unico nodo di uscita n_f.

- Un arco $e = (n_i, n_j) \in E$ rappresenta un possibile flusso di controllo tra due blocchi di codice.



(a) Esempio di CFG

```
if(x == y)
    then
        ...
    else
        ...
...
```

Figura 2.4.1: La figura generale

2.4.1 Blocchi di base

Blocco di base

Un blocco di base è la massima sequenza consecutiva di istruzioni senza diramazioni interne, con un singolo punto di ingresso, un singolo punto di uscita e senza salti all'interno del blocco.

Si tratta dell'unità di base per la costruzione del `CFG` e per l'analisi del flusso.

Le ottimizzazioni che è possibile attuare includono l'eliminazione della ridondanza e l'allocazione dei registri.

2.4.2 Identificare i blocchi di base

Questo è un processo di analisi del flusso di controllo per identificare i blocchi di base. Di seguito è riportata una spiegazione dettagliata basata sull'input fornito:

Identificazione dei leader:

- Il primo statement nella sequenza (*punto di ingresso*) è un leader.
- Ogni statement "s" che è la destinazione di un salto (*condizionale o incondizionale*) è un leader (*cioè esiste un "goto s"*).
- Ogni statement immediatamente successivo a un salto (*condizionale o incondizionale*) o a un return è un leader.

Creazione dei blocchi di base:

- Per ogni leader identificato, il suo blocco di base include il leader stesso e tutte le istruzioni fino al prossimo leader (*senza includerlo*) o fino alla fine del programma.

Questo processo consente di identificare i blocchi di base e di definire il flusso di controllo all'interno del programma.

2.4.3 Esempio

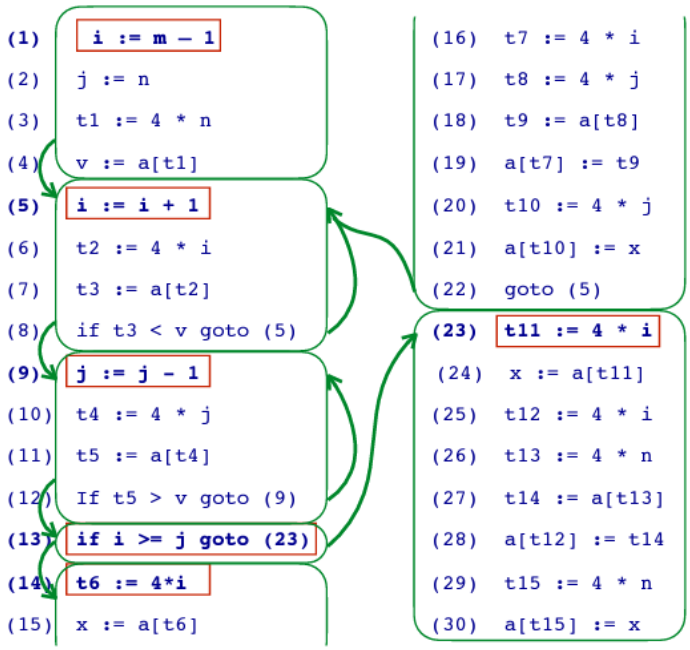
```
1. i := m - 1
2. j := n
3. t1 := 4 * n
4. v := a[t1]
5. i := m + 1
6. t2 := 4 * i
7. t3 := a[t2]
8. if t3 < v goto (5)
9. j:= j - 1
10. t4 := 4 * j
11. t5 := a[t4]
12. if t5 > v goto (9)
13. if i >= j goto (23)
14. t6 := 4 * i
15. x := a[t6]
16. t7 := 4 * i
17. t8 := 4 * j
18. t9 := a[t8]
19. a[t7] := t9
20. t10 := 4 * j
21. a[t10] := x
22. goto (5)
23. t11 := 4 * i
24. x := a[t11]
25. t12 := 4 * i
26. t13 := 4 * n
27. t14 := a[t13]
28. a[t12] := t14
29. t15 := 4 * n
30. a[t15] := x
```

```
1. i := m - 1
2. j := n
3. t1 := 4 * n
4. v := a[t1]
5. i := m + 1
6. t2 := 4 * i
7. t3 := a[t2]
8. if t3 < v goto (5)
9. j:= j - 1
10. t4 := 4 * j
11. t5 := a[t4]
12. if t5 > v goto (9)
13. if i >= j goto (23)
14. t6 := 4 * i
15. x := a[t6]
16. t7 := 4 * i
17. t8 := 4 * j
18. t9 := a[t8]
19. a[t7] := t9
20. t10 := 4 * j
21. a[t10] := x
22. goto (5)
23. t11 := 4 * i
24. x := a[t11]
25. t12 := 4 * i
26. t13 := 4 * n
27. t14 := a[t13]
28. a[t12] := t14
29. t15 := 4 * n
30. a[t15] := x
```

La partizione del codice intermedio in blocchi di base coinvolge diversi passaggi importanti per rappresentare il flusso di controllo in un programma. I passaggi chiave sono i seguenti:

- Aggiunta di archi corrispondenti ai flussi di controllo tra i blocchi.
- Trattamento dei costrutti come:
  - **Goto incondizionale**: Questo genera un collegamento diretto a un blocco specifico.
  - **Branch condizionale**: Può generare più archi uscenti da un blocco, a seconda delle possibili condizioni.
  - **Flusso sequenziale**: Se non ci sono ramificazioni alla fine di un blocco, il controllo passa semplicemente al blocco successivo.
- Aggiunta di nodi finti e archi, se necessario, per rappresentare i nodi di ingresso e di uscita nel caso in cui non siano unici.
- L'obiettivo è di semplificare al massimo gli algoritmi di analisi e trasformazione, assicurando che non ci siano archi che entrano nel nodo di ingresso n_0 o che escono dal nodo di uscita n_f.

Questi passaggi sono cruciali per modellare accuratamente il flusso di controllo all'interno di un programma e facilitare ulteriori analisi e ottimizzazioni.



Dato un `CFG` $= \langle N, E \rangle$, è definito come un insieme di nodi e archi, dove ogni arco rappresenta il flusso di controllo tra due nodi. Nel contesto di un `CFG` $=< N, E >$:

- Se esiste un arco $n_i \to n_j \in E$:
  - n_i è un predecessore di n_j
  - n_j è un successore di n_i
- Per qualsiasi nodo $n \in N$:
  - `Pred(n)`: l'insieme dei predecessori di n
  - `Succ(n)`: l'insieme dei successori di n
  - Un nodo di diramazione (`branch node`) è un nodo che ha più di un successore
  - Un nodo di unione, (`join node`) è un nodo che ha più di un predecessore

2.5 Il linguaggio `imp-CFG`

Spostando la caratteristica di controllo sulla struttura del grafo, il linguaggio non è più `IMP`, ma una versione leggermente modificata:

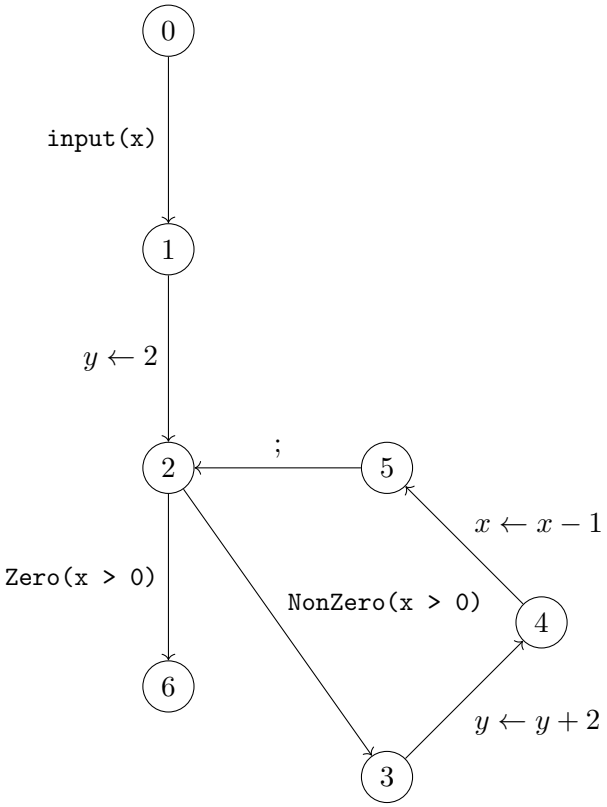
- I vertici corrispondono ai punti del programma
- Gli archi sono passi del calcolo etichettati con l'azione del programma corrispondente

- Le etichette delle istruzioni diventano etichette dei nodi

test:	`NonZero(e)` or `Zero(e)`
assignment:	$x \leftarrow e$
empty statement:	;
input:	`input(x)`

Esempio

```
input(x);
y := 2;
while(x > 0) {
  y := y + 2;
  x := x - 1;
}
```



Una dichiarazione condizionale o un ciclo all'interno di un grafo di flusso di controllo presenta due archi corrispondenti: l'arco etichettato con `NonZero` viene percorso se la condizione "e" è verificata (cioè se "e" viene valutata come un valore diverso da 0). L'arco etichettato con `Zero`, invece, viene percorso se la condizione non è soddisfatta.

Un arco è definito come $k = (u, \texttt{lab}, v)$, dove u rappresenta il vertice di partenza, v rappresenta il vertice di destinazione e `lab` rappresenta l'etichetta dell'arco. Questo arco rappresenta l'effetto della dichiarazione, ovvero la trasformazione dello stato prima dell'esecuzione dell'azione di etichettatura in uno stato successivo: **effetto dell'arco**.

2.5.1 Semantica del linguaggio `imp-CFG`

La semantica del linguaggio descrive la trasformazione dello stato prima e dopo l'esecuzione di un'azione del linguaggio, che viene riflessa nell'effetto complessivo della dichiarazione

all'interno del programma.

$$\begin{array}{lcll} [\![;]\!](m) & = & m & \\ [\![\texttt{NonZero(e)}]\!](m) & = & m & \textit{if } [\![e]\!](m) = \texttt{true} \\ [\![\texttt{Zero(e)}]\!](m) & = & m & \textit{if } [\![e]\!](m) = \texttt{false} \\ [\![x \leftarrow e]\!](m) & = & m[x \mapsto [\![e]\!](m)] & \\ [\![\texttt{input(x)}]\!](m) & = & m[x \mapsto m(x)] & \end{array}$$

2.5.2 Computazione del linguaggio `imp-CFG`

Una computazione è un percorso nel grafo di flusso di controllo, ovvero una sequenza di archi che iniziano dal nodo iniziale u e terminano in un nodo finale v. Il percorso è quindi una sequenza di archi:

$$\pi = k_1, k_2, \ldots, k_n = (u_i, \texttt{lab}_i, u_{i+1}), i = 1, \ldots, n-1, u = u_1, v = v_n$$

La trasformazione di stato corrispondente alle computazioni ottenuta dalla composizione degli effetti degli archi della computazione:

$$[\![\pi]\!] = [\![k_n]\!] \circ \cdots \circ [\![k_1]\!]$$

Capitolo 3

Significato di approssimare

3.1 L'idea di approssimazione

Immagina di avere due insiemi di oggetti: uno di questi, chiamiamolo $[\![P]\!]$, ha una caratteristica speciale che chiameremo Q. Ora, il punto cruciale è che non possiamo dire con certezza se un determinato oggetto appartiene a Q o meno. È come se avessimo un mucchio di oggetti e non riuscissimo a dire se uno specifico oggetto appartiene a un gruppo particolare o meno.

Quello che dobbiamo fare è trovare un modo per approssimare l'insieme $[\![P]\!]$ in modo da poter prendere decisioni più facili su Q. In altre parole, dobbiamo trovare un altro insieme, $[\![P]\!]^{\#}$, che contiene la maggior parte degli oggetti di $[\![P]\!]$, ma che sia più facile da analizzare. Questo insieme deve avere due caratteristiche importanti: tutti gli oggetti di $[\![P]\!]$ devono essere anche in $[\![P]\!]^{\#}$, e l'insieme $[\![P]\!]^{\#}$ deve essere tale che possiamo dire con certezza se un oggetto appartiene a Q o meno.

Quando abbiamo questo insieme $[\![P]\!]^{\#}$, possiamo utilizzarlo per fare deduzioni su Q. Se tutti gli oggetti in $[\![P]\!]^{\#}$ appartengono a Q, allora possiamo dire con sicurezza che tutti gli oggetti in $[\![P]\!]$ devono appartenere a Q. Ma se non tutti gli oggetti in $[\![P]\!]^{\#}$ appartengono a Q, non possiamo essere certi se gli oggetti in $[\![P]\!]$ appartengono o meno a Q.

In sostanza, il nostro obiettivo è rendere più facile prendere decisioni su questi oggetti, anche se non possiamo dire con certezza assoluta se un oggetto specifico appartiene a Q. Questo approccio ci consente di ragionare in modo più chiaro su questi insiemi e di trarre conclusioni ragionevoli su di essi.

La correttezza ci consente di sfruttare la decidibilità dell'approssimazione:

$$[\![P]\!] \subseteq Q \implies [\![P]\!]^{\#} \subseteq Q$$

Altrimenti, non possiamo saperlo con certezza!

3.1.1 Astrazione della semantica

Vediamo come costruire l'insieme $[\![P]\!]^{\#}$ a partire da $[\![P]\!]$. Specificheremo la semantica come una coppia: una funzione f (*con punto fisso*) e un dominio di calcolo D (*ordinato*).

- Astrazione del dominio di calcolo e delle relazioni tra oggetti concreti e astratti, ovvero l'osservazione astratta dei dati e come questi si relazionano tra loro.
- Astrazione del calcolo, con particolare attenzione all'astrazione del punto fisso, come la semantica manipola questi risultati astratti.

L'astrazione è il processo di sostituire qualcosa di concreto con una descrizione che considera alcune proprietà (*generalmente non tutte*), definita come modello astratto. Può descrivere alcune proprietà in modo preciso, ma non tutte.

Un'astrazione $\wp(\Sigma)$ di oggetti in Σ è $A \subseteq \wp(\Sigma)$ tale che:

- Gli elementi presenti nell'insieme A sono quelli descritti precisamente dall'astrazione, senza perdita di precisione.
- Gli elementi non presenti nell'insieme A devono essere rappresentati da altri elementi dell'insieme, con una perdita di precisione.

3.1.2 Oggetti

Nell'analisi/verifica dei programmi dobbiamo considerare oggetti che rappresentano parti dello stato di calcolo:

- Valori: Booleani, Interi,... $\mathcal{V}$
- Nomi di variabili $\mathbb{X}$
- Ambienti $\mathbb{X} \to \mathcal{V}$
- Stacks
- ...

Proprietà

Le proprietà sono insiemi di oggetti (che hanno quella proprietà). Esempi:

- Numeri naturali dispari: $\{1, 3, 4, \ldots, 2n + 1, \ldots\}$
- Numeri interi pari: $\{2z \mid z \in \mathbb{Z}\}$
- Valori delle variabili intere: $\{x \mid x \in \mathbb{X} \wedge \texttt{minint} < x < \texttt{maxint}\}$
- Proprietà di invarianza: di un programma con stati: Γ

$$I \in \wp(\Sigma)$$

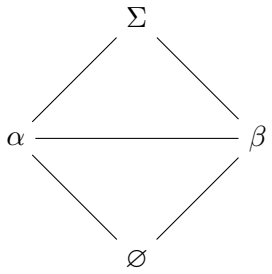
- ...

3.1.3 Proprietà

L'insieme delle proprietà di $\wp(\Sigma)$ degli oggetti in Σ è un reticolo distributivo completo,

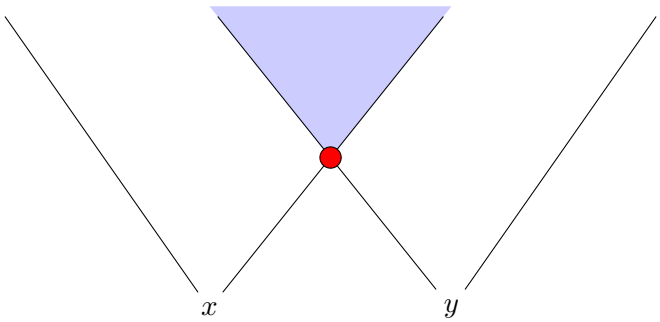
$$\langle \wp(\Sigma), \subseteq, \varnothing, \sigma, \Sigma, \cup, \cap, \neg \rangle$$

Nell'analisi di un sistema complesso, è essenziale considerare l'astrazione come un processo chiave per semplificare la comprensione. Quando si tratta di approssimare una proprietà concreta con un'astrazione, si aprono due possibili approcci. L'approccio di **approssimazione dal basso** implica che l'astrazione rappresenti un sottoinsieme della proprietà concreta, mentre l'approccio di **approssimazione dall'alto** (P) implica che l'astrazione rappresenti un sovrainsieme della proprietà concreta. Questi approcci possono essere visti come duali, sebbene l'analisi si concentri principalmente sull'approccio di approssimazione dall'alto, poiché trovare approssimazioni utili dal basso può essere più impegnativo e complesso.



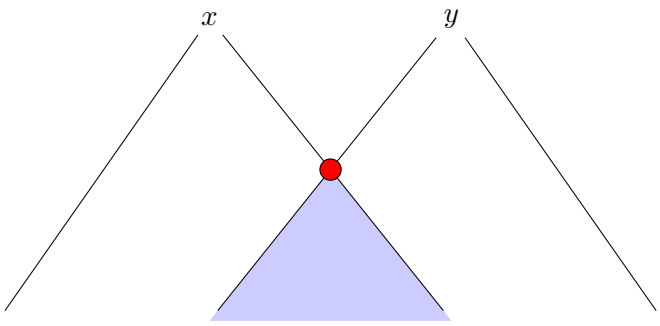
Least upper bound

Il least upper bound (`LUB`) di un insieme di elementi è il più piccolo elemento del reticolo che è maggiore o uguale a ciascun elemento dell'insieme ($X \vee Y$). Ovvero in $\wp(D)$ tale che $A \supseteq X$ e $A \supseteq Y$.



Greatest lower bound

Il greatest lower bound (`GLB`) di un insieme di elementi è il più grande elemento del reticolo che è minore o uguale a ciascun elemento dell'insieme ($X \wedge Y$). Ovvero in $\wp(D)$ tale che $A \subseteq X$ e $A \subseteq Y$.



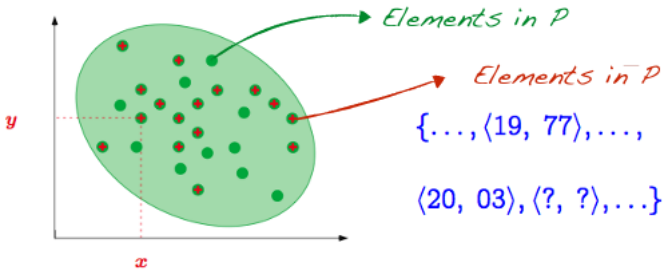
3.2 Approssimazione dei dati

Sia $P^{\#}$ una proprietà di D se e solo se $P^{\#}$ e $\wp(D)$. Vogliamo quindi capire la relazione tra gli elementi di D e $\wp(D)$ e poi, preso $D^{\#} \subseteq \wp(D)$ la relazione tra gli elementi di D e gli elementi di $D^{\#}$. Per approssimare D scegliamo un sottoinsieme $D^{\#}$ che fissa le proprietà che vogliamo osservare (*con precisione*). In generale $d \in D \implies d^{\#} \in D \subseteq \wp(D)$.

Potremmo quindi avere:

- $d \subseteq d^{\#}$ ovvero **over approximation**.
- $d \supseteq d^{\#}$ ovvero **under approximation**.

3.2.1 Approssimazione dal basso

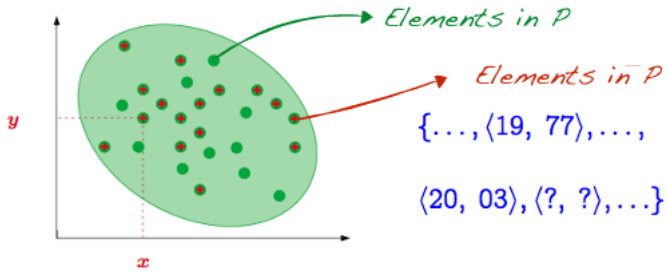


Per rispondere alla domanda $\langle x, y\rangle \in P$ utilizziamo un'astrazione $\bar{P}$, tale che $P \supseteq \bar{P}$.

- Se $\langle x, y\rangle \in \bar{P}$, quindi $d \subseteq d^{\#}$, allora $\langle x, y\rangle \in P$.
- Se $\langle x, y\rangle \notin \bar{P}$, quindi $d \supseteq d^{\#}$, allora non lo sappiamo.

In sintesi prendiamo un insieme più piccolo che comprende una sottoparte del nostro insieme di partenza e analizziamo tale insieme più piccolo. Se troviamo una risposta positiva allora abbiamo risposto alla domanda, altrimenti non lo sappiamo.

3.2.2 Approssimazione dall'alto



Per rispondere alla domanda $\langle x, y\rangle \in P$ utilizziamo un'astrazione $\bar{P}$, tale che $P \subseteq \bar{P}$.

- Se $\langle x, y\rangle \in \bar{P}$, quindi $d \supseteq d^{\#}$, allora non sappiamo rispondere.
- Se $\langle x, y\rangle \notin \bar{P}$, quindi $d \subseteq d^{\#}$, allora no.

In sintesi prendiamo un insieme più grande che comprende il nostro insieme di partenza e analizziamo tale insieme più grande. Più grande non è sinonimo di più complesso, ma spesso ricondurci a proprietà più generali potrebbe aiutarci nell'analisi, la rappresentazione estensionale potrebbe quindi risultare più semplice. Tale approccio ci permette di rispondere alla domanda solo che la proprietà non è soddisfatta per il nuovo insieme più grande, ovvero $P^{\#}$.

In sostanza:

Proprietà concrete

Le proprietà concrete sono un insieme di oggetti potenzialmente complessi, infiniti e non rappresentabili da un calcolatore.

Proprietà astratte

Le proprietà astratte sono un insieme più ampio di oggetti. A volte, l'ampiezza maggiore implica una maggiore estensibilità per la rappresentazione. Tuttavia, strutture più ampie ben scelte possono avere codifiche più semplici che possono essere sfruttate per la memorizzazione e il calcolo.

3.2.3 Minima astrazione

Assumendo che le proprietà astratte $P \in \wp(\Sigma)$ devono essere apporssimate dall'alto della proprietà astratta $\bar{P} \in A \subset \wp(\Sigma)$, tale che:

$$P \subseteq \bar{P}$$

Sappiamo che la più piccola proprietà $\bar{P}$ è la più precisa delle approssimazioni che possiamo avere. Ovviamente, la minima proprietà astratta potrebbe non non esistere per tutte le astrazioni A. Se questa minima approssimazione esiste è preferibile che sia il più precisa possibile,

se non esiste, può essere utilizzata una migliore alternativa che fornisce un'approssimazione più precisa.

3.2.4 Miglior astrazione

Una buona scelta per l'astrazione è quella che fornisce la miglior approssimazione per ogni proprietà concreta

$$P \subseteq \bar{P}$$

$$\forall \bar{P}' \in A.(P \subseteq \bar{P}') \implies (\bar{P} \subseteq \bar{P}')$$

Segue che la miglior approssimazione è la *greatest lower bound* di tutte le approssimazioni delle proprietà.

$$\bar{P} = \bigcap \{\bar{P}' \in A \mid P \subseteq \bar{P}'\} \in A$$

Tra tutti gli elementi più piccoli di quelli in X, è il più grande.

$$x = \texttt{glb}X \subseteq P \iff \forall l \in P.(\forall y \in X.l \leq y) \implies x \geq l$$

3.2.5 Esempio: `Sign`

Semantica concreta

Abbiamo a disposizione programmi che manipolano numeri interi: $f : \mathbb{Z} \to \mathbb{Z}$. Una delle proprietà osservate è quella di *sign*, ovvero che il risultato tra due numeri dipenderà dal segno dei due numeri. Dobbiamo indicare cosa inseriremo in $D^{\#}$ ovvero `Sign`.

- $+ = \{n \mid n > 0\} \in \wp(\mathbb{Z})$
- $- = \{n \mid n < 0\} \in \wp(\mathbb{Z})$
- $0 = \{0\} \in \wp(\mathbb{Z})$

Quindi:

$$\{+, 0, -\} \subseteq \wp(\mathbb{Z})$$

Semantica astratta

Il dominio astratto, noto come `Sign`, viene utilizzato per approssimare l'insieme di interi manipolati dai programmi. La funzione $f^{\#}$ manipola quindi i segni.

$$D^{\#} = \{+, -, 0, \mathbb{Z}, \varnothing\} = \texttt{Sign}$$

In `Sign`, gli interi possono essere rappresentati come:

- $x \subseteq \mathbb{Z} \to x^{\#} \in D^{\#}$ è il più piccolo insieme in $D^{\#}$ che contiene x.
- $\{-, 5, 4\} \to \mathbb{Z}$
- $\{3\} \to + \equiv \mathbb{Z}$
- $\{7\} \to + \equiv \mathbb{Z}^{+}$

- $\{-5\} \to - \equiv \mathbb{Z}^-$
- $\{-5, -6\} \to - \equiv \mathbb{Z}^-$

	$\mathbb{Z}$	$\mathbb{Z}^+$	$\mathbb{Z}^0$	$\mathbb{Z}^-$	$\varnothing$
$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$
$\mathbb{Z}^+$	$\mathbb{Z}$	$\mathbb{Z}^+$	$\mathbb{Z}^+$	$\mathbb{Z}$	$\mathbb{Z}^+$
$\mathbb{Z}^0$	$\mathbb{Z}$	$\mathbb{Z}^+$	$\mathbb{Z}^0$	$\mathbb{Z}^-$	$\mathbb{Z}^0$
$\mathbb{Z}^-$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}^-$	$\mathbb{Z}^-$	$\mathbb{Z}^-$
$\varnothing$	$\mathbb{Z}$	$\mathbb{Z}^+$	$\mathbb{Z}^0$	$\mathbb{Z}^-$	$\varnothing$

Figura 3.2.1: Operazioni di `Sign` relative alla somma.

	$\mathbb{Z}$	$\mathbb{Z}^+$	$\mathbb{Z}^0$	$\mathbb{Z}^-$	$\varnothing$
$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$
$\mathbb{Z}^+$	$\mathbb{Z}$	$\mathbb{Z}^+$	$\mathbb{Z}^0$	$\mathbb{Z}^-$	$\mathbb{Z}^+$
$\mathbb{Z}^0$	$\mathbb{Z}$	$\mathbb{Z}^0$	$\mathbb{Z}^0$	$\mathbb{Z}^0$	$\mathbb{Z}^0$
$\mathbb{Z}^-$	$\mathbb{Z}$	$\mathbb{Z}^-$	$\mathbb{Z}^0$	$\mathbb{Z}^+$	$\mathbb{Z}^-$
$\varnothing$	$\mathbb{Z}$	$\mathbb{Z}^+$	$\mathbb{Z}^0$	$\mathbb{Z}^-$	$\varnothing$

Figura 3.2.2: Operazioni di `Sign` relative alla moltiplicazione.

Per quanto riguarda la somma perdiamo informazioni solamente nel caso in cui si abbia un'operazione tra un numero positivo e uno negativo, poiché perdiamo le informazioni relative ai valori. Per quanto riguarda la moltiplicazione, invece, non perdiamo informazioni guardando la proprietà `Sign`, poiché è precisa sulla moltiplicazione.

3.3 Astrazione delle computazioni

Si tratta di approssimare la semantica sul dominio delle osservazioni. Una volta fissate queste osservazioni, osserviamo come la semantica opera su di esse.

Abbiamo già visto il significato di computazione, che ripetiamo.

Computazione

Una computazione è una traccia nel tempo dello stato del programma durante l'esecuzione. Quindi lo stato delle memorie nei vari punti del programma. A partire da uno stato iniziale noi abbiamo le possibili traiettorie di esecuzione del programma, talvolta infinite poiché potenzialmente divergenti.

In realtà le possibili traiettorie non sono continue, ma sono discrete, poiché fissiamo degli step di tempo che tipicamente corrispondono alle singole istruzioni del programma e ogni traccia è spezzata in questa sequenza di evoluzione.

3.3.1 Computazione di insiemi

Quello che avviene ricerca della **decidibilità** è quello di osservare le proprietà di interesse. Per osservare le proprietà di interesse, necessitiamo dell'osservazione di insiemi. L'insieme infatti rappresenta una proprietà che descrive un invariante di tutti gli elementi in esso contenuti.

Trasformando l'insieme di tracce in un'unica computazione che avviene tra insiemi. I punti rimangono comunque concreti, quindi dal punto di vista di ciò che possiamo calcolare, ovvero degli stati raggiungibili ad ogni passo di computazione, non cambia nulla, perché non perdiamo informazioni sugli stati raggiunti.

Questo calcolo però non vogliamo eseguirlo con il calcolo diretto, perché l'infinità delle traiettorie non viene assolutamente alterata, quindi stiamo potenzialmente gestendo insiemi potenzialmente infiniti.

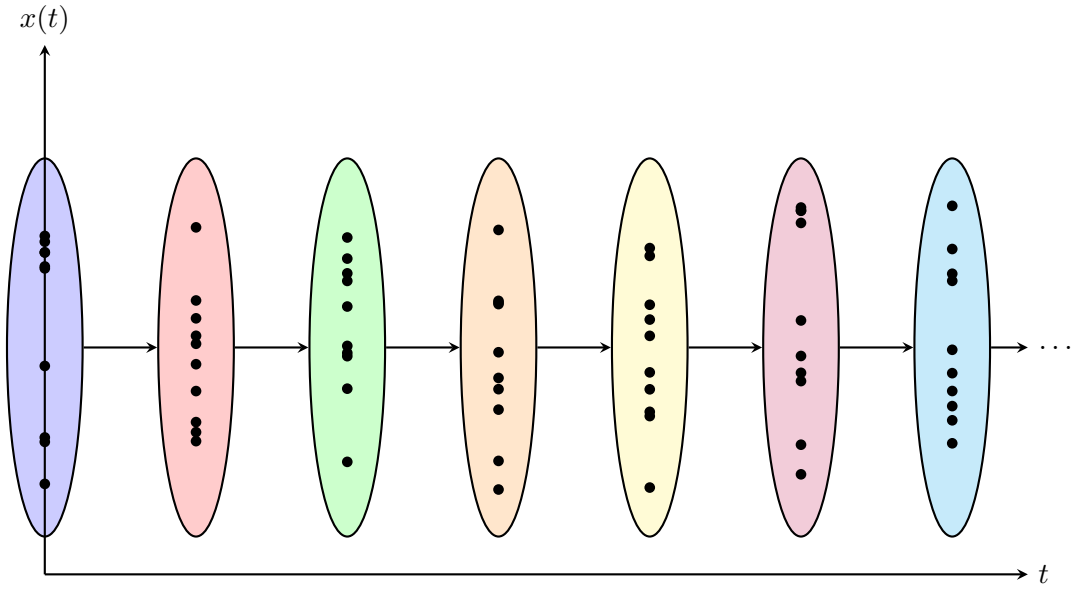
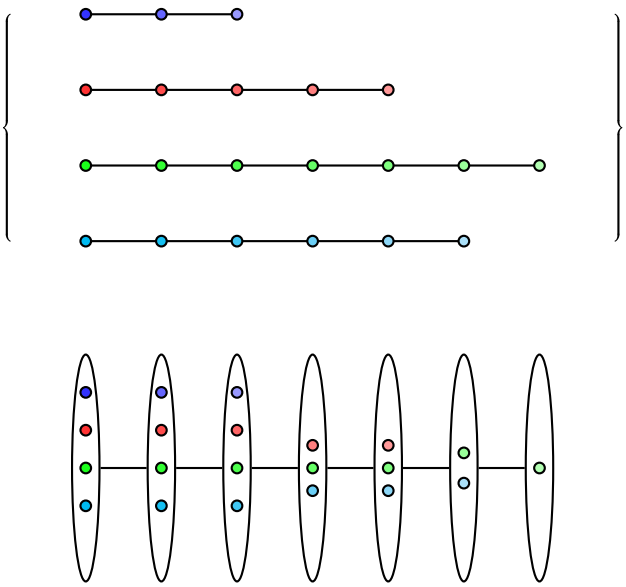


Figura 3.3.1: Traccia di una computazione di insiemi.

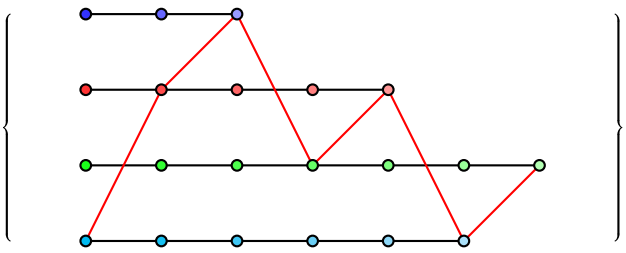
Il calcolo avviene quindi per punto fisso, partiamo quindi da un insieme di stati iniziali e andiamo via a via a collezionare tutti gli stati che raggiungiamo durante l'esecuzione, chiamato **reachability semantics** o **collecting semantics**.

3.3.2 Collecting semantics

Dal punto di vista della raggiungibilità degli stati, l'informazione è precisa, infatti l'insieme di stati raggiunti sono gli stessi che avremmo raggiunto con la semantica concreta. Di fatto, però, abbiamo una perdita di informazione dal punto di vista dell'insieme delle tracce che stiamo rappresentando.

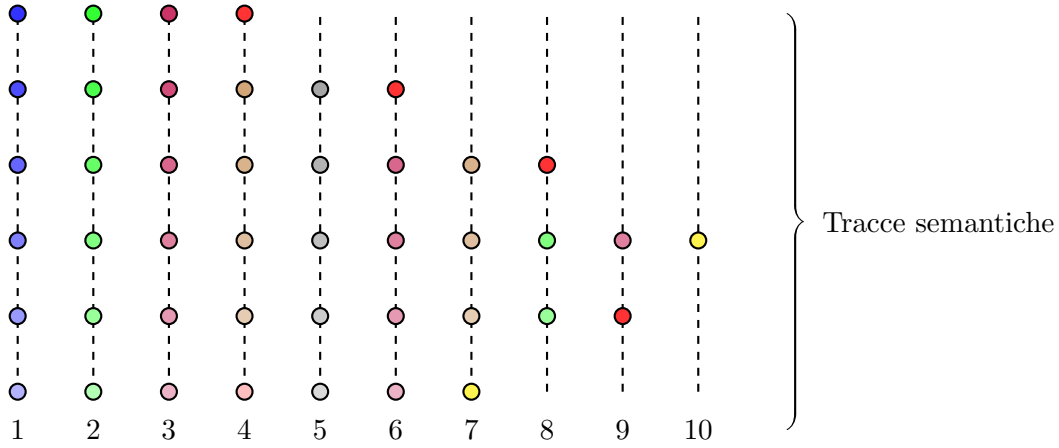


La semantica delle tracce mi colleziona l'insieme di tutte le tracce di computazione e la semantica delle collezioni invece considera per ogni passo di computazione l'insieme la proprietà raggiunta degli stati raggiunti. Abbiamo perso informazione rispetto alle tracce che rappresentiamo, in questo passaggio perdiamo la traccia che nello stato successivo raggiunge un determinato stato, poiché la traccia diventa unica.

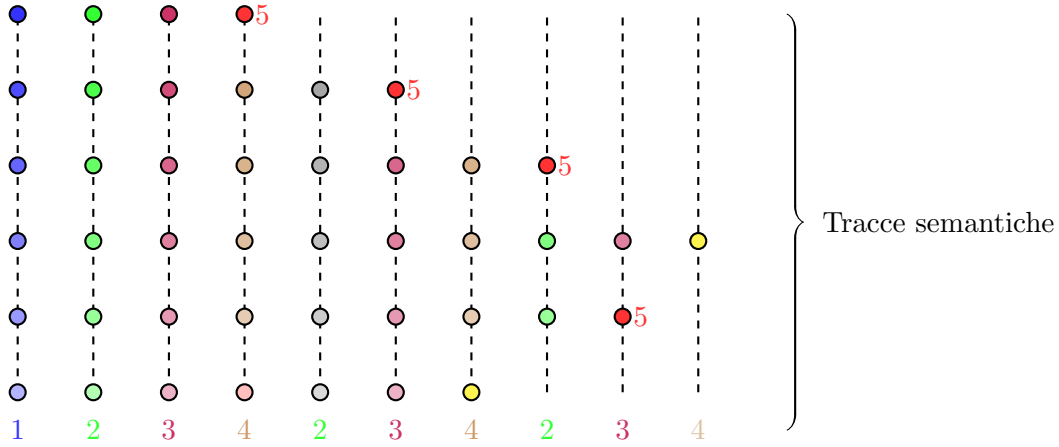


Abbiamo buttato via l'informazione che riguardava l'esatta transizione tra gli stati, aggiungendo tracce spurie.

La domanda che sporge spontanea è se ci stiamo muovendo nella direzione della decidibilità; di fatto no. Vediamo quindi un'altra rappresentazione che ci permette di comprendere la situazione.

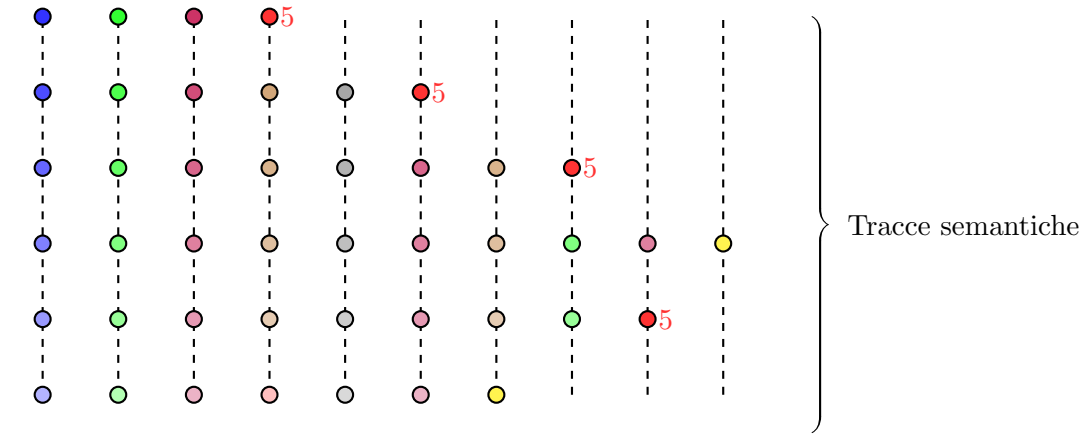


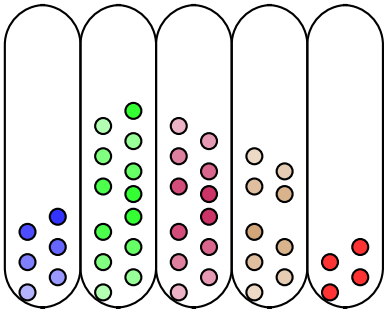
Ad ogni passo di computazione eseguiamo un istruzione in un **punto di programma**, possiamo quindi guardare il punto di programma che stiamo osservando.



Quello che osserviamo è che 5 è uno stato terminale, e che i punti 2 e 3 sono il corpo del ciclo, andando avanti nel tempo torniamo a visitate dei punti di programma.

Spostiamo la discretizzazione del punto di vista della traccia dal tempo ai punti di programma.





Quello che viene fatto è quello di collezionare gli elementi nei punti di programma che sono stati eseguiti. Di fatto per ogni punto di programma, l'insieme degli stati è sempre incrementale rispetto al punto di programma.

Potenzialmente anche questa rappresentazione sarà non terminante, poiché stiamo guardando ancora il mondo concreto, quindi gli stati raggiungibili sono ancora potenzialmente infiniti. Soprattutto in presenza di un ciclo `while` che calcola valori differenti ad ogni iterazione.

```
1 x ← 0
2 while x ≥ 0 do
3     x ← x + 1
```

L'insieme in questo caso continuerà ad espandersi all'infinito, poiché non c'è un limite e quindi non è possibile trovare un punto fisso. Il tentativo di raggiungere la terminazione è quello di trovare la stabilità di tali insiemi.

In alcuni casi la decidibilità è raggiungibile, ma nella maggior pate dei casi non è possibile.

```
1 x ← 0
2 while x ≥ 0 do
3     x ← x
```

In caso appena riportato l'insieme degli stati è sempre lo stesso, quindi è possibile trovare un punto fisso.

3.3.3 Computazioni sulle proprietà

Nella collecting semantics abbiamo quindi esecuzioni spurie, dovute al fatto che collezioniamo insiemi di stati, ma sono solo tra stati raggiungibili. Il fatto che manteniamo gli stati raggiungibili fa si che non vi sia perdita di informazione, ma dall'altra parte abbiamo esecuzioni potenzialmente infinite.

Dobbiamo ulteriormente raffinare la collecting semantics, per poter raggiungere la terminazione. Per farlo abbiamo bisogno dell'approssimazione, non più calcolando sugli insiemi di stati raggiungibili, ma su proprietà degli stati raggiungibili. Spostiamo quindi l'attenzione sugli sulle proprietà aggiungendo ulteriore rumore.

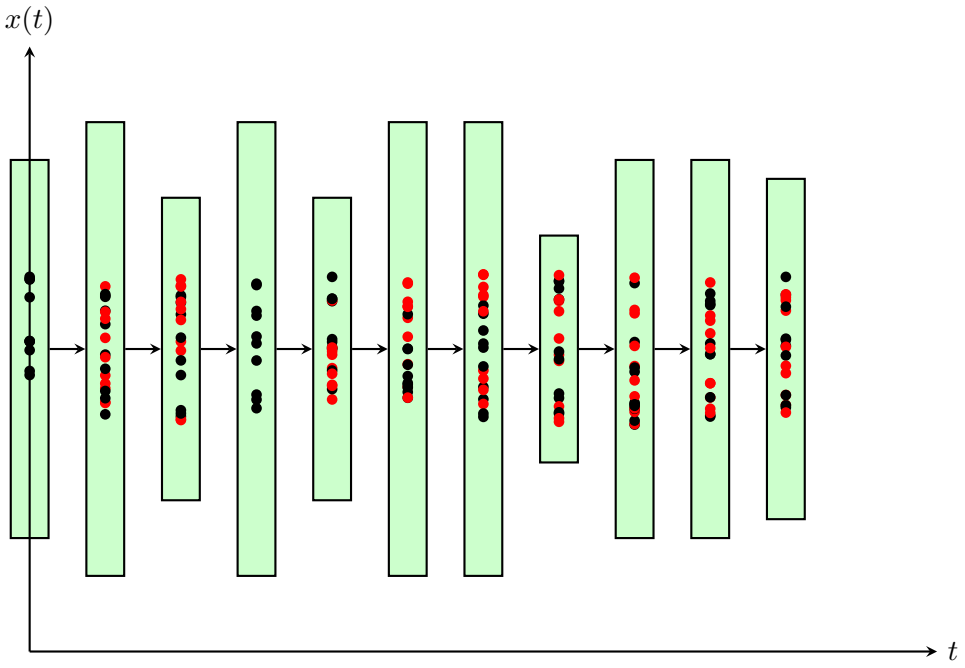


Figura 3.3.2: Traccia di una computazione sulle proprietà.

Non abbiamo solamente computazioni spurie dovute al fatto che ci muoviamo tra insiemi, ma abbiamo computazioni spurie che partono da stati che non vengono mai raggiunti nel concreto (*rappresentati dai pallini rossi nell'immagine* 3.3.2).

L'idea genera è quella di:

- Passare da l'insieme di tracce distinte ad una taccia di insiemi rappresentate (*che aggiunge rumore, mediante tracce spurie*).
- A questo punto è possibile approssimare la computazione guardando proprietà, utilizzando quindi la semantics collecting sulle proprietà, che possono agevolare la terminazione.