Analisi del Software

Alessio Gjergji

Indice

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.