unI vostri valori astratti incorporano la componente relativa alla qualità q (che io pensavo legata alla tamperability, ovvero tamperable/tamperable+sensitive = scarsamente affidabile, ma questo non è un problema). In particolare, per i valori astratti relativi a nomi e variabili avete creato una funzione \tau' e un operatore di combinazione che tiene conto dei tag di qualità, sullo stile visto a lezione. Entrambi vengono usati nelle clausole della CFA che controllano variabili (assegnamento e input).

Avete introdotto una funzione di combinazione che tiene conto dei tag di qualità già in fase di propagazione: &_\exists \tau(f,(v1,…,vr))
In alternativa si poteva propagare nel senso più "sicuro", ovvero una goccia di Li rende Li le eventuali aggregazioni e successivamente vedere se rispetto al predicato di qualità scelto, che diventerebbe così un parametro della proprietà, si può avere la proprietà dinamica o meno.

Avrei due questioni su cui vi chiederei di commentare prima di venerdì.

1) Cosa succede con predicati più complessi e composti? Come quelli indicati nella specifica dell'Homework.

Resilience Analysis a là Quality The above taint analysis can be further pushed in order to consider resilience issues, by answering to question like "Given an aggregation function, how many values must be correct for giving the right answer?" The aim is to ensure a certain level of reliability of actuations even in the presence of unreliable data. For instance, consider the check whether the given temperature average, used to trigger the fire suppression system, is greater than a certain threshold, and suppose that the temperature sensors in the room now are eight.

$$gt(avg(1_{E_{11}}, 1_{E_{21}}, 1_{E_{31}}, 1_{E_{41}}, 1_{E_{51}}, 1_{E_{61}}, 1_{E_{71}}, 1_{E_{81}}), T_{RT})$$

A possible detailed question here may be: "What if $1_{E_{11}}$ and $1_{E_{61}}$, give the wrong results?" and "Does the overall result amortise these weaknesses?" Maybe it does, but "what does it happen if additionally, also $1_{E_{41}}$ fails?

Risposta:
Nella definizione dell'operazione di join i valori restituiti dall'operazione sono due (taint, min(q,q')) dove q e q' sono i valori di quality dei due operandi.
Min(q,q') viene calcolato sulla base della proprieta' di ordinamento lo<hi.
Di conseguenza ogni aggregazione standard propaga sempre il valore minimo di quality.

Esempio 1:

$$gt(\ \&_{\exists}(\ avg(1_{E_{11}}, 1_{E_{21}}, 1_{E_{31}}, 1_{E_{41}}\ ,\ 1_{E_{51}}, 1_{E_{61}}, 1_{E_{71}}, 1_{E_{81}})\ )\ , T_{RT})$$

In questo esempio consideriamo di applicare il costrutto &_E e la relativa regola di propagazione a tutto l'insieme di valori. Questo permette di propagare solamente i valori Hi.

Esempio 2:

$$gt(avg(1_{E_{11}}, 1_{E_{21}}, \&_{\exists}(avg(1_{E_{31}}, 1_{E_{41}}\ )), 1_{E_{51}}, 1_{E_{61}}, 1_{E_{71}}, 1_{E_{81}}), T_{RT})$$

Nel nostro esempio se tra E31 ed E41 ci fossero valori Hi verrebbero considerati nella media solo loro e propagato localmente al valore &_E il tag "hi" (applicando il filtro). Diversamente verrebbe propagato il tag "lo" e la media verrebbe eseguita normalmente su entrambi i valori (senza filtri).

Quello che volevamo garantire era che il sistema fosse equivalente al precedente nel caso in cui tutti sensori fossero valutati “hi”.

Esempio 3 (senza &_E):

$$gt(avg(1_{E_{11}}, 1_{E_{21}}, 1_{E_{31}}, 1_{E_{41}}, 1_{E_{51}}, 1_{E_{61}}, 1_{E_{71}}, 1_{E_{81}}), T_{RT})$$

La regola di propagazione che viene utilizzata e’

$$F_\tau(f, \hat{v}_1, \ldots, \hat{v}_r) = \otimes(\hat{v}_{1\downarrow_2}, \ldots, \hat{v}_{r\downarrow_2})$$

Ci rendiamo conto che nella definizione della propagazione &_E_tau potrebbe essere stato omesso, per estrema sintesi, il caso senza funzione:

$$\&_{(\exists\tau)}(\hat{v}_1, \ldots \hat{v}_r) = \begin{cases} \otimes(\hat{v}_{1\downarrow(2,3)}, \ldots, \hat{v}_{i\downarrow(2,3)}) & \forall \hat{v}_{i\downarrow 3} = hi \text{ if } \exists \hat{v}_{j\downarrow 3} = hi \mid 1 \le j, i \le r \\ \otimes(\hat{v}_{1\downarrow(2,3)}, \ldots, \hat{v}_{r\downarrow(2,3)}) & o.w. \end{cases}$$

2) L’ultima parte mi pare scritta un po’ in fretta. Non mi è chiarissima la definizione di validità e come usa i valori astratti. Dovrebbe contenere la definizione della proprietà statica e dinamica e come si legano tra loro.

<u>Risposta:</u>
La definizione di validita’ e’ stata pensata come segue:

$$\frac{\forall\, l_c \in L_c : (x)_{\downarrow 3} \in \{\text{ hi }\} \forall x \in \Sigma_{l_c}}{(\hat{\Sigma}, k, \Theta) \models N}$$

Le proprieta’ statiche di tainteness e quality vengono propagate fino ai nodi critici Lc.
Il nodo critico e’ considerato valido solo se tutti i valori presenti nello store sono di qualita’ alta.
La rete di Nodi e’ considerata valida se tutti i nodi critici sono validi per la proprieta’ sopra espressa.

Esempio: durante l’analisi di qualita’ vengono propagati solamente i valori (v,b,q) dei sensori con livello di q = hi e la relativa taintness.

Per quanto riguarda il legame tra valore astratto e propagazione abbiamo cercato di esplicitarlo nella risposta precedente.