Strategies as Knowledge Trees for Reasoning About Information Flow

Sebastian Hunt

City University London

The 19th CREST Open Workshop, April-May 2012

Work In Progress

Outline

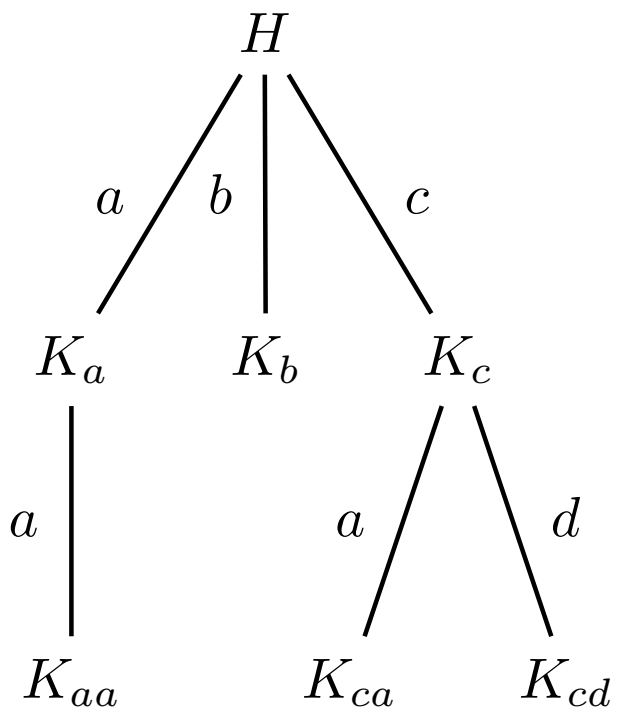
1 Knowledge Trees

2 Strategies

Knowledge Trees

- Consider a system $P(I, h)$ taking a Low and a High input and producing a sequence of outputs.
- Let $\text{ran}\ P(I)$ be $s \in A^*$ such that $P(I, h)$ can emit emit s for some h.
- For $s \in \text{ran}\ P(I)$, define:

$$K_s = \{h \in H \mid P(I, h) \text{ can emit } s\}$$



Termination-Insensitive Non-Interference

- Non-Interference (NI):

$$\forall I.\forall s \in \text{ran } P(I).\ K_s = H$$

- Termination-Insensitive Non-Interference (TINI):

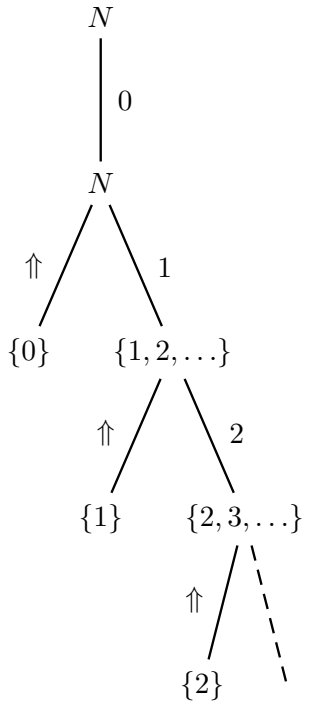
$$\forall I.\forall sa, sb \in \text{ran } P(I).\ K_s a = K_s b$$

- If we see sa we know that P had not diverged at s:
  - NI $\Rightarrow$ we learn nothing about h from this fact
  - TINI $\Rightarrow$ we may rule out some values of h
- TINI is a popular choice of non-interference condition because it can be checked by Denning-style static analysis.

TINI Leaks More Than Just a Bit [ESORICS 2008]

```
for i = 0 to maxNat {
    output i on public_channel
    if (i = secret) then (while true do skip)
}
```

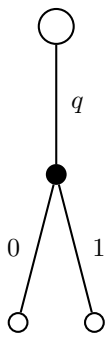
- TINI only allows the secret to affect termination behaviour.
- But programs with incremental output can use termination behaviour to leak an entire secret . . .
- . . . but not in polynomial time.



What about *interactive* systems?

- Model sequential interaction via *strategies* (Game Semantics).
- A type (*arena*) A is defined by tuple (M, λ, P) where
  - M is the set of moves,
  - λ labels each move as Player or Opponent
  - $P \subseteq M^*$, a non-empty, prefix-closed set of *plays* where each $s \in P$ starts with an Opponent move and strictly alternates between Opponent and Player
- A strategy σ of type A is a non-empty set of even-length plays closed under even-length prefix: $sa \in \sigma$ means a is the move chosen by σ at position s

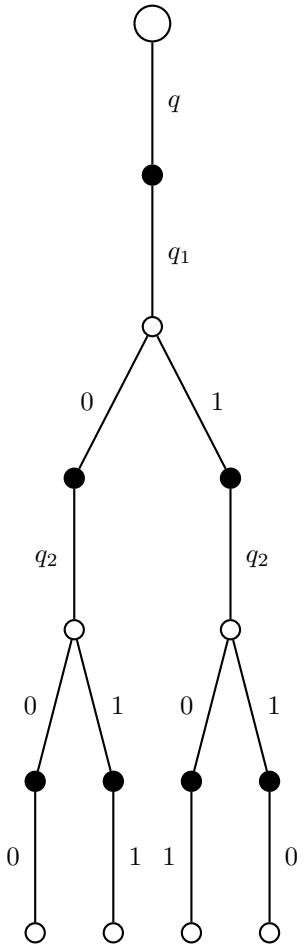
Example: XOR (left-first)

- $\mathcal{B} =$ 

- XOR : $\mathcal{B}_1 \otimes \mathcal{B}_2 \multimap \mathcal{B}$
- $A \otimes B$ is the disjoint sum of A and B:

$$P_{A \otimes B} = \{s \mid s \upharpoonright A \in P_A, s \upharpoonright B \in P_B\}$$

- $A \multimap B$ is like $A \otimes B$ but with Player/Opponent reversed in A.



Composition of Strategies

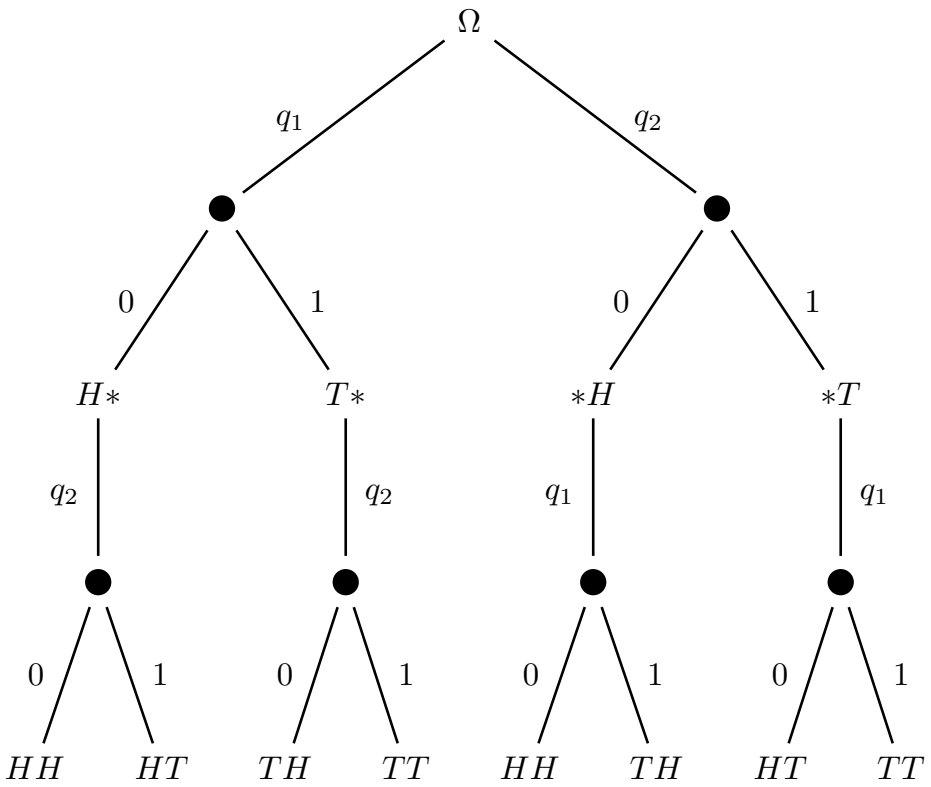
- $\sigma : A \multimap B$ and $\tau : B \multimap C$
- $\sigma;\tau : A \multimap C$
- $\sigma||\tau = \{u \in (M_A + M_B + M_C)^* \mid u \upharpoonright A, B \in \sigma, u \upharpoonright B, C \in \tau\}$
- $\sigma;\tau = \{u \upharpoonright A, C \mid u \in (\sigma||\tau)\}$
  - The *witnesses* for $s \in \sigma;\tau$ are those $u \in (\sigma||\tau)$ such that $u \upharpoonright A, C = s$.

Determined Non-Determinism

- Allow non-deterministic strategies but enrich with knowledge sets.
- Fix some "sample space" Ω: knowledge sets will be subsets of Ω.
- Enrich strategy σ with $K_\sigma : \sigma \to \mathcal{P}(\Omega)$ satisfying:
  - $K(\epsilon) = \Omega$
  - $K(sab) \subseteq K(s)$
  - $b_1 \neq b_2 \Rightarrow K(sab_1) \cap K(sab_2) = \emptyset$
- The knowledge sets "explain" the non-determinism (hidden variable).

Example: Pair of Coins

- $\Omega = \{H, T\} \times \{H, T\}$
- Write $H*$ for $\{H\} \times \{H, T\}$, write $T*$ for $\{T\} \times \{H, T\}$, etc

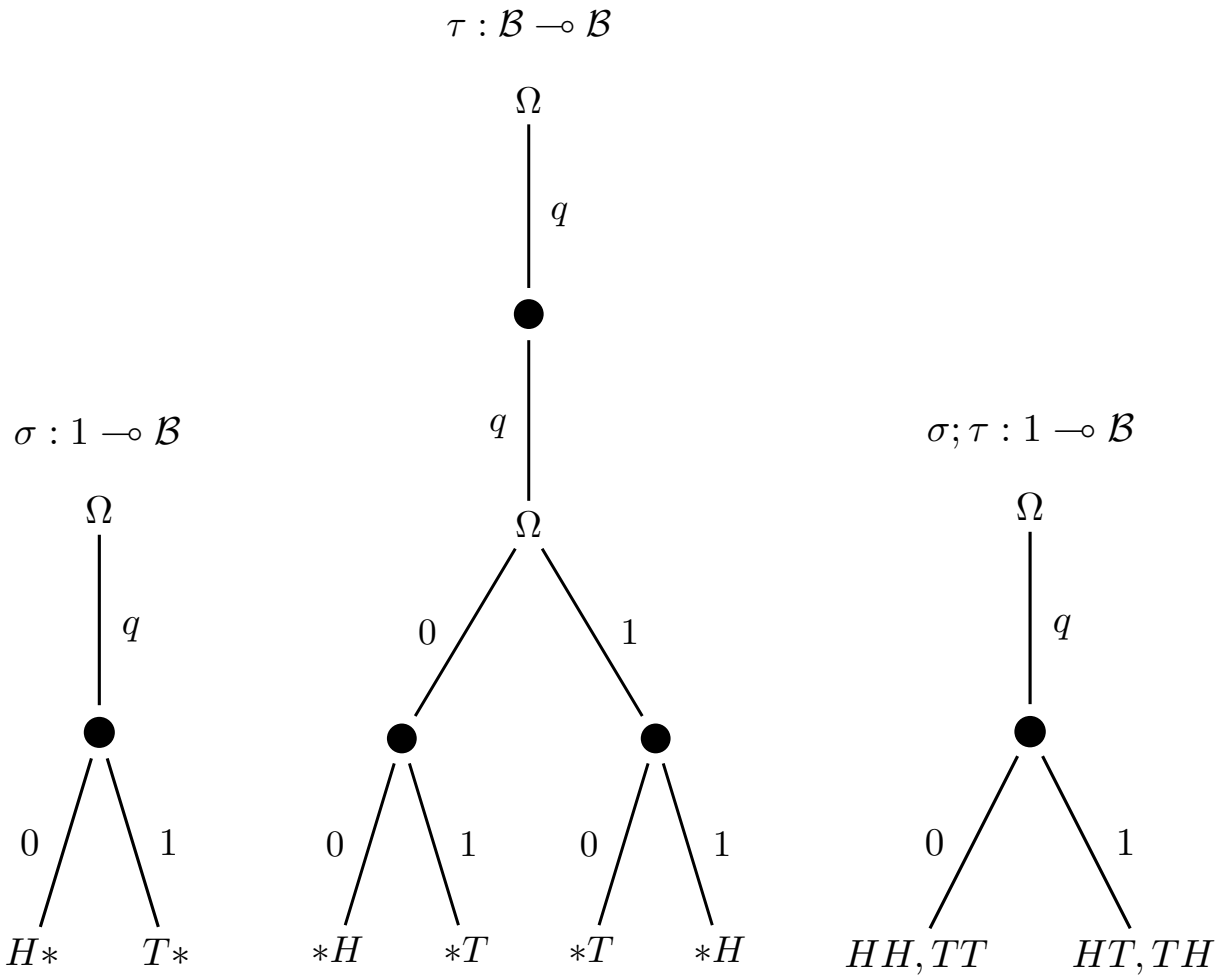


Composition of Enriched Strategies

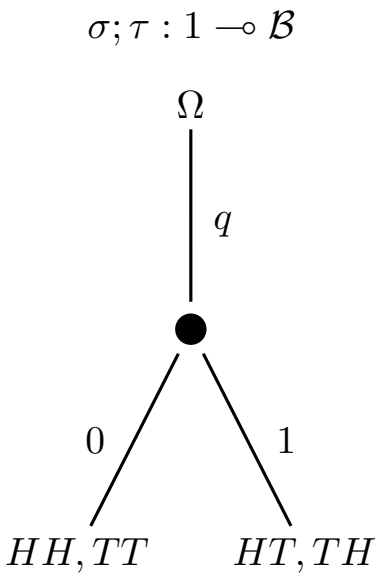
- $\sigma : A \multimap B$ and $\tau : B \multimap C$
- $\sigma;\tau : A \multimap C$
- $\sigma||\tau = \{s \in (M_A + M_B + M_C)^* \mid s \upharpoonright A, B \in \sigma, s \upharpoonright B, C \in \tau\}$
- $\sigma;\tau = \{s \upharpoonright A, C \mid s \in (\sigma||\tau)\}$
- $K_{\sigma;\tau}(s) =$

$$\bigcup\{K_\sigma(u \upharpoonright A, B) \cap K_\tau(u \upharpoonright B, C) \mid u \text{ is a witness for } s\}$$

Example: One-Bit Perfect Encryption



Can You Keep a Secret?



- Whether the secret (first coin) is preserved depends on what an adversary knows about the second coin.
- If we assume adversary cannot predict the second coin, check for security by projecting onto the first coin, giving $\{H, T\}$: Good.
- If adversary may know second coin, quantify over it's possible values and project for each one, giving $\{H\}, \{T\}$: Bad.

Universal Knowledge

- Given arena A define the maximally non-deterministic strategy $\mu_A : 1 \multimap A$ as $\{s \in P_A \mid s \text{ has even length}\}$.
- Choose sample space $\Omega = \mu_A$.
- Define $K_\mu : \mu_A \to \mu_A$ by $K(s) = \uparrow s$.
- Conjecture: all enriched strategies for A can (in some suitable sense) be factored through this one.
- Let $\sigma : H \multimap L$. Say that σ is NI iff $K(s) = \mu_H$ for all $s \in \mu_H; \sigma$
- *No* σ which makes *any* move in H can be NI.
- TINI may be the more appropriate notion of NI for sequential systems, regardless of the ease or difficulty of analysis.

Future Work

And now for the Doomsday Device . . .