Safe Types in Untyped Contexts Avik Chaudhuri

Gradual types = **Static** types + **any**

$t \leq any$ $any \leq t'$

Strong reject!

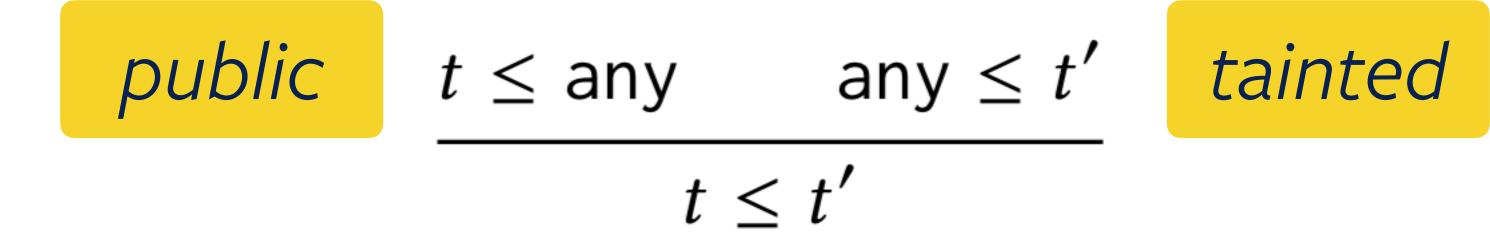
$\frac{t \le \text{any}}{t \le t'}$

Transitivity is key to subtyping

Subtyping models data flow



$\frac{t \le \text{any}}{t \le t'}$





Gradual types = Security* types!

Syntactic separation of types / safety

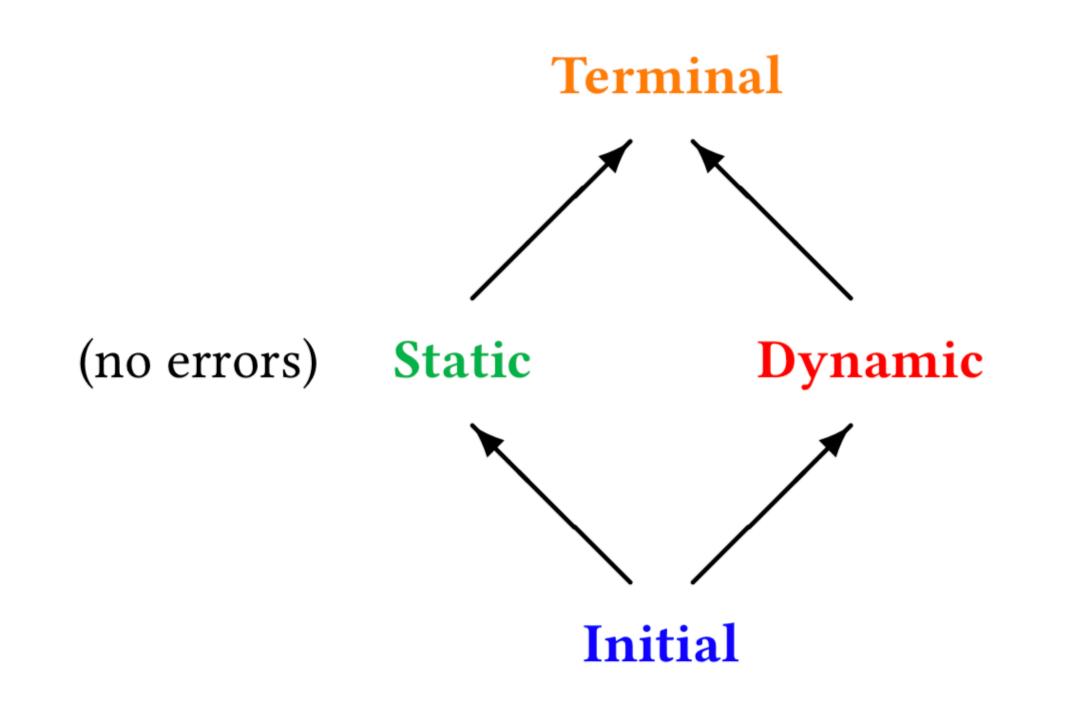
$\tau ::= \iota \mid t \to t' \mid \{\ell_1 : t_1, \dots, \ell_n : t_n\} \mid \& t$

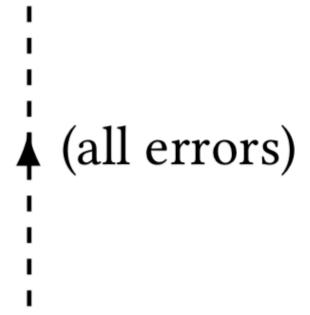
 $t ::= \tau \# \theta \mid any$

"Safety qualifiers" $\theta ::= src \gg dst$



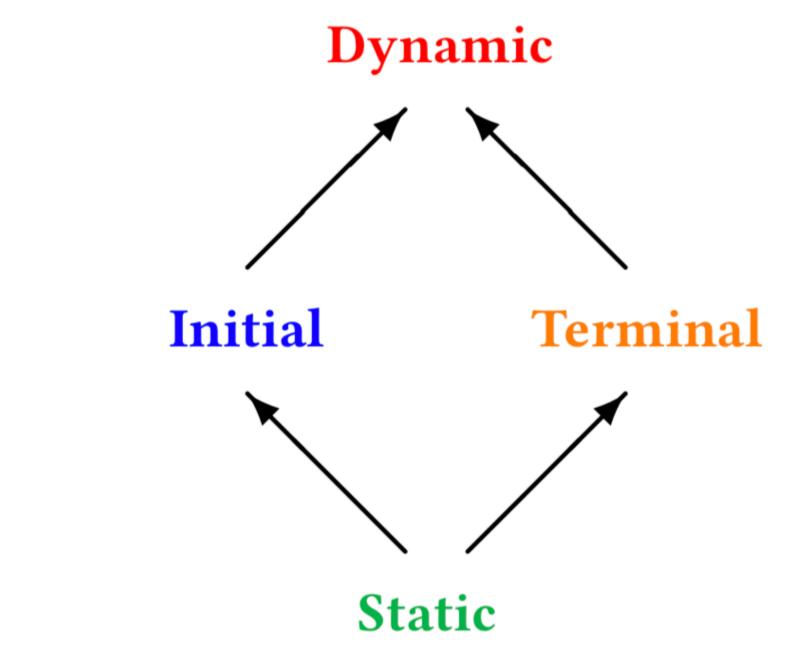
$\operatorname{src}' \subseteq \operatorname{src} \quad \operatorname{dst} \subseteq \operatorname{dst}'$ $src \gg dst \leq src' \gg dst'$







$\operatorname{src}' \subseteq \operatorname{src} \quad \operatorname{dst}' \subseteq \operatorname{dst}$ $\operatorname{src} \operatorname{*} \operatorname{dst} \sqsupseteq \operatorname{src}' \operatorname{*} \operatorname{dst}'$





Types

$$\frac{t_1' \le t_1 \quad t_2 \le t_2'}{t_1 \to t_2 \le t_1' \to t_2'}$$

$$\frac{m \le n \quad t_1 \le t_1' \quad \dots \quad t_n}{\{\ell_1 : t_1, \dots, \ell_n : t_n\} \le \{\ell_1 : t_1', \dots, \frac{t' \le t \quad t \le t'}{\& t \le \& t'}}$$

$$\frac{\tau \le \tau' \quad \theta \le \theta'}{\tau \# \theta \le \tau' \# \theta'} \quad \frac{\tau \le \tau' \quad \theta \le \theta'}{\mathsf{any} \le \mathsf{any} t \mathsf{any} \le \mathsf{any} \le \mathsf{any} \mathsf{any} \le \mathsf{any} \le \mathsf{any} \le \mathsf{any} \le \mathsf{any} \le \mathsf{any} \le \mathsf{any} \mathsf{an$$

 $t_m \le t'_m$ $\ldots, \ell_m : t'_m \}$

≤ any

 $\begin{array}{ll} \theta \leq \mathbf{Dynamic} & \mathbf{Dynamic} \leq \theta \\ & & \\ public \ \theta & & \\ tainted \ \theta \end{array}$

public θ

tainted θ

au # $heta \leq any$

any $\leq \tau \# \theta$

θ # θ

- $\iota^{\bullet} = \iota$ $(t_1 \rightarrow t_2)^{\bullet} = \text{any} \rightarrow \text{any}$ Type tags $\{\ell_1 : t_1, \ldots, \ell_n : t_n\}^{\bullet} = \{\ell_1 : any, \ldots, \ell_n : any\}$ $(\& t)^{\bullet} = \& any$
 - $\tau \leq \tau^{\bullet}$ $\tau^{\bullet} \leq \tau$ public τ tainted τ

Well-formed types / safety



Hint: this is the most important slide in this talk!

public $\theta \Rightarrow$ public τ

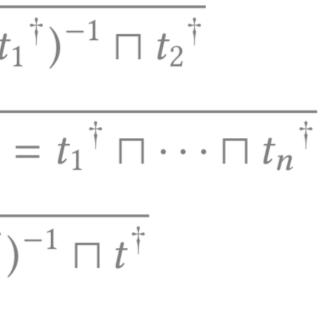


tainted $\theta \Rightarrow$ tainted τ

Polarities
$$\checkmark$$

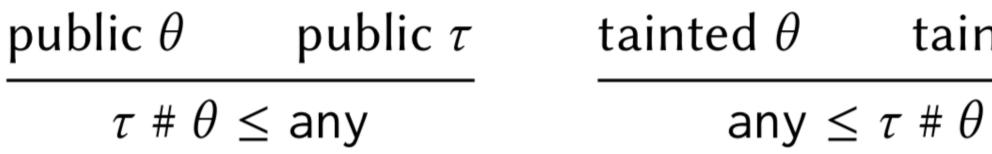
 $\overline{t^{\dagger} = \mathbf{Dynar}}$
 $\overline{(t_1 \to t_2)^{\dagger} = (t_1^{\dagger})^{\dagger}}$
 $\overline{(t_1 : t_1, \dots, \ell_n : t_n)^{\dagger} = (t^{\dagger})^{-1}}$
 $\overline{(k t)^{\dagger} = (t^{\dagger})^{-1}}$
 $\overline{(k t)^{\dagger} = (t^{\dagger})^{-1}}$
 $\overline{(t t^{\dagger} = t^{\dagger})^{\dagger}}$
 $\overline{(t t^{\dagger} = t^{\dagger})^{\dagger}} = t^{\dagger}$





 $= \theta$







tainted τ

$t_{\text{unsafe}} = \{\ell : (\& (\{\} \# \text{Initial})) \# \text{Initial}\} \# \text{Initial}\}$

Mutability + Subtyping = 💭



Well-formed = Sound

"I'll be fine, thank you!" $t_{safe(1)} = \{\ell : (\& (\{\} # Dynamic)) # Initial\} # Initial \}$

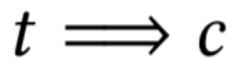
"Help me please!" $t_{safe(2)} = \{\ell : (\& (\{\} # Initial)) # Initial\} # Static$

Applications

Well-typed programs can be optimized



- **METERCE** $\Gamma \vdash e : t \Longrightarrow c$
- **Dynamic Checking** $\Gamma \vdash e : \tau \uparrow c$
 - Static checking $\Gamma \vdash e : t \longleftarrow c$



Insert dynamic checks for tainted types...

$\Gamma \vdash e : any \Longrightarrow c$ $\Gamma \vdash e : \tau^{\bullet} \Uparrow \langle \tau^{\bullet} \rangle c$

 $\Gamma \vdash e : \tau \# \theta \Longrightarrow c$ tainted θ

 $\Gamma \vdash e : \tau \Uparrow \langle \tau^{\bullet} \rangle c$



Remove dynamic checks for trusted types!

$\Gamma \vdash e : \tau \# \theta \Longrightarrow c \quad \text{trusted } \theta$

$$\Gamma \vdash e : \tau \uparrow c$$

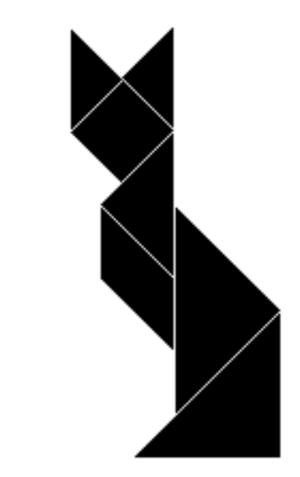


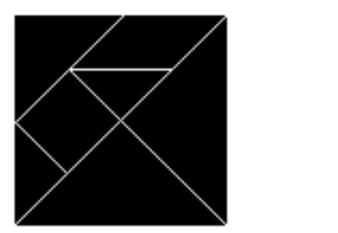
AISO, "Subtyping models data flow"

 $\Gamma \vdash e : t' \Longrightarrow c \qquad t' \leq t$

 $\Gamma \vdash e : t \iff c$

Well-typed programs can't be blamed





"Encouraging discovery!"

s happy to have another friend, his former captain and perpetual apologist. sent on the committee. Apparently, he could trust

sibility and a selfish obses sion with how he was being portrayed by the media that will be remembered. he Funny people, folk.

Effectively, it is a genuine reflection of his character. In the chapter dealing

with the exhilarating Grand Prix, for example, and his spat with his dangerous team-mate, his driving is so

Nears its actual tax paid British Virgin Islands. Over the last

SEL DOTTO AND AND MANY DESCRIPTION OF

Government focused on the 100,000 British prisoners released every an advisor added "It gives tota

The various pieces of fresh fruit are placed

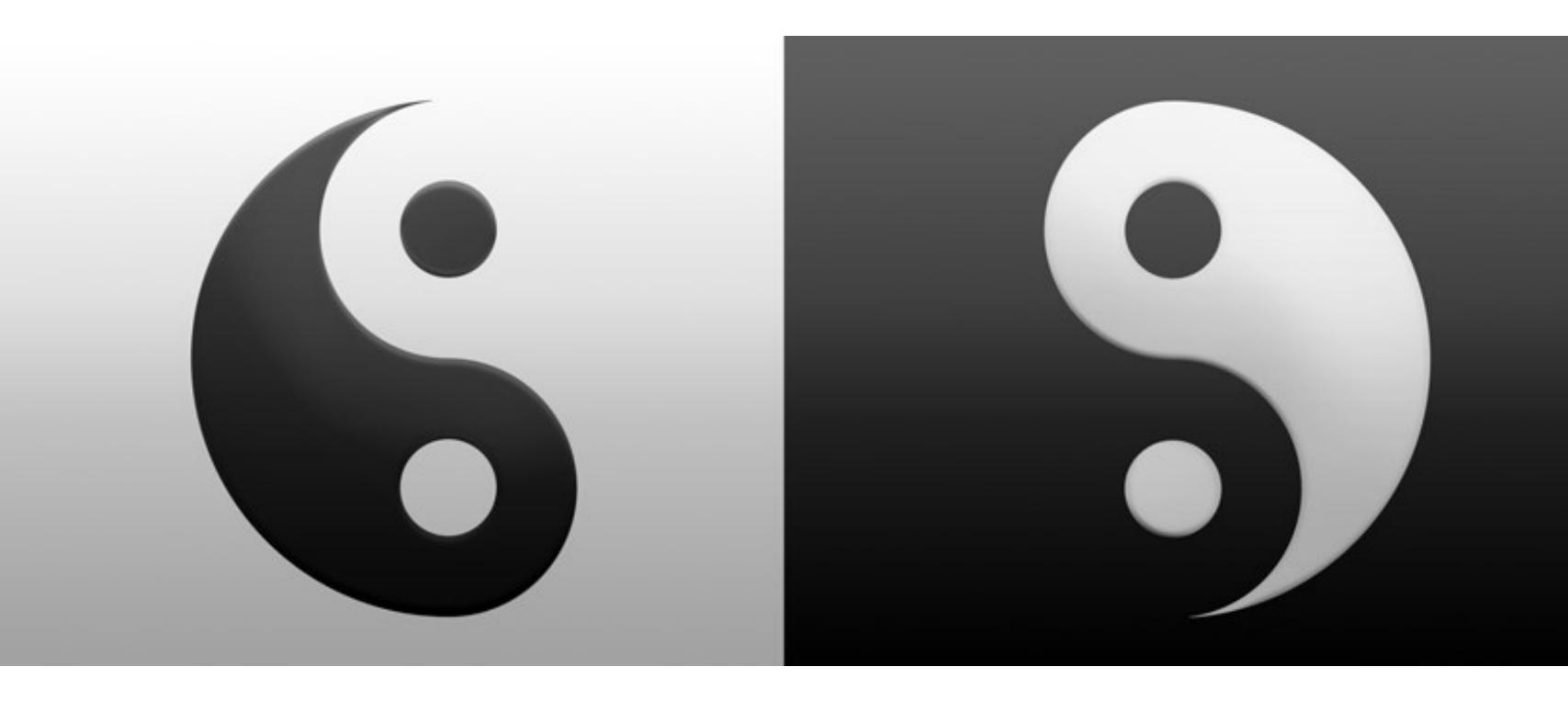
"Disappointing reception"





$t \leq t'$ iff $t \leq^+ t'$ and $t \leq^- t'$. Safety

Precision $t \sqsupseteq t'$ iff $t \leq^+ t'$ and $t' \leq^- t$



Symmetric rules, Asymmetric encoding

Tainted types = any Trusted types = Static types

"IT'S NOT WHO I AM UNDERNEATH BUT WHAT I DO THAT DEFINES ME"

