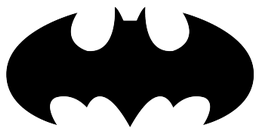


Safe Types in Untyped Contexts

Avik Chaudhuri

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

$$t \leq \text{any} \qquad \text{any} \leq t'$$

Strong reject!

$$\frac{t \leq \text{any} \qquad \text{any} \leq t'}{t \leq t'}$$

Transitivity is key to subtyping

Subtyping models data flow

Strong accept!

$$\frac{t \leq \text{any} \qquad \text{any} \leq t'}{t \leq t'}$$

public

$$\frac{t \leq \text{any} \qquad \text{any} \leq t'}{t \leq t'}$$

tainted

Gradual types = Security* types!

Syntactic separation of types / safety

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

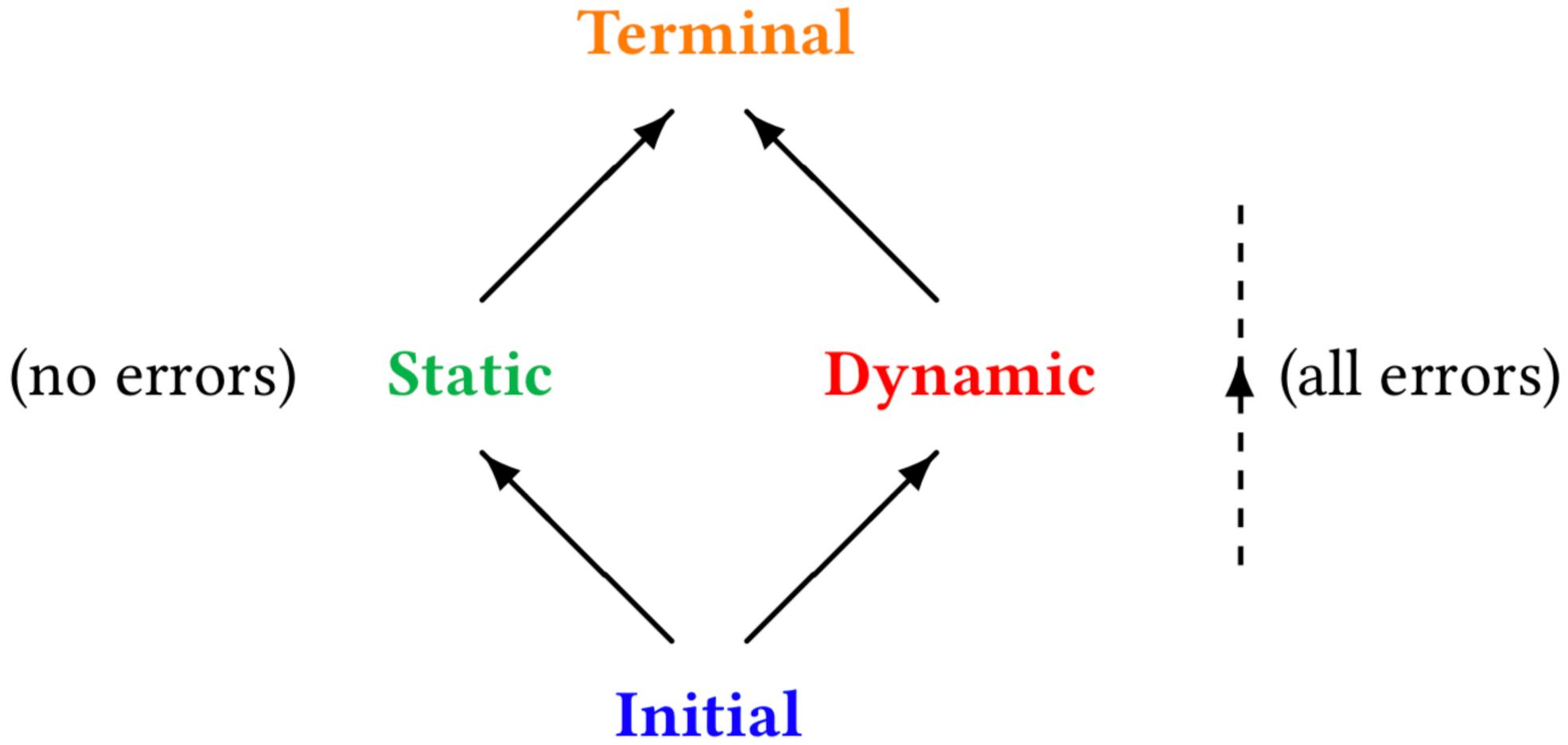
$$t \quad ::= \quad \tau \# \theta \mid \text{any}$$

“Safety qualifiers”

$$\theta \quad ::= \quad \mathbf{src} \gg \mathbf{dst}$$

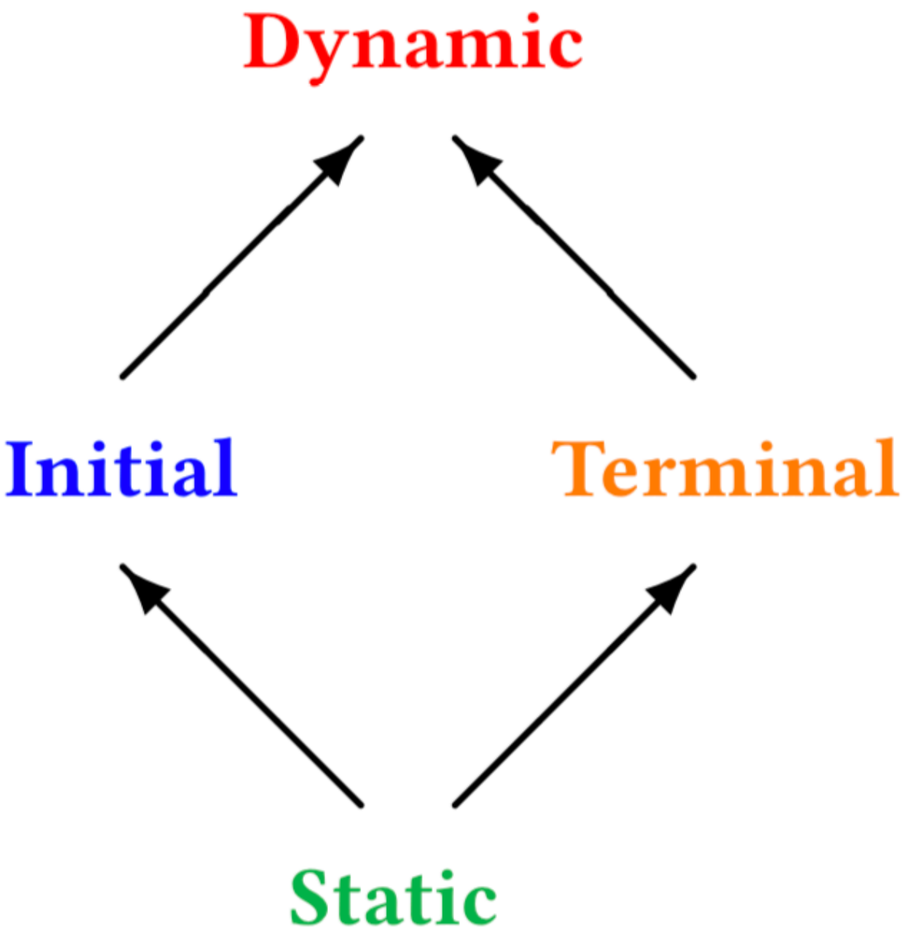
Safety lattice

$$\frac{\mathbf{src}' \subseteq \mathbf{src} \qquad \mathbf{dst} \subseteq \mathbf{dst}'}{\mathbf{src} \gg \mathbf{dst} \leq \mathbf{src}' \gg \mathbf{dst}'}$$


Terminal
(no errors)
Static
Dynamic
(all errors)
Initial

Precision lattice

$$\frac{\mathbf{src}' \subseteq \mathbf{src} \qquad \mathbf{dst}' \subseteq \mathbf{dst}}{\mathbf{src} \gg \mathbf{dst} \sqsupseteq \mathbf{src}' \gg \mathbf{dst}'}$$


Dynamic
Initial
Terminal
Static

Types

$$\frac{}{\iota \leq \iota}$$

$$\frac{t_1' \leq t_1 \qquad t_2 \leq t_2'}{t_1 \to t_2 \leq t_1' \to t_2'}$$

$$\frac{m \leq n \qquad t_1 \leq t_1' \qquad \ldots \qquad t_m \leq t_m'}{\{\ell_1 : t_1, \ldots, \ell_n : t_n\} \leq \{\ell_1 : t_1', \ldots, \ell_m : t_m'\}}$$

$$\frac{t' \leq t \qquad t \leq t'}{\& \, t \leq \& \, t'}$$

Safety

$$\frac{\tau \leq \tau' \qquad \theta \leq \theta'}{\tau \,\#\, \theta \leq \tau' \,\#\, \theta'} \qquad \frac{}{\text{any} \leq \text{any}}$$

$$\frac{\theta \leq \textbf{Dynamic}}{\text{public } \theta} \qquad \frac{\textbf{Dynamic} \leq \theta}{\text{tainted } \theta}$$

$$\frac{\text{public } \theta}{\tau \ \# \ \theta \leq \text{any}} \qquad \frac{\text{tainted } \theta}{\text{any} \leq \tau \ \# \ \theta}$$

Type tags

$$\iota^\bullet = \iota$$
$$(t_1 \to t_2)^\bullet = \text{any} \to \text{any}$$
$$\{\ell_1 : t_1, \ldots, \ell_n : t_n\}^\bullet = \{\ell_1 : \text{any}, \ldots, \ell_n : \text{any}\}$$
$$(\&\ t)^\bullet = \&\ \text{any}$$

$$\frac{\tau \leq \tau^\bullet}{\text{public } \tau} \qquad \frac{\tau^\bullet \leq \tau}{\text{tainted } \tau}$$

Well-formed types / safety

Hint: this is

the most important slide

in this talk!

$$\text{public}\ \theta \Rightarrow \text{public}\ \tau \qquad \text{tainted}\ \theta \Rightarrow \text{tainted}\ \tau$$

Polarities 💓

$$\frac{}{\iota^{\dagger} = \mathbf{Dynamic}}$$

$$\frac{}{(t_1 \to t_2)^{\dagger} = (t_1{}^{\dagger})^{-1} \sqcap t_2{}^{\dagger}}$$

$$\frac{}{\{\ell_1 : t_1, \ldots, \ell_n : t_n\}^{\dagger} = t_1{}^{\dagger} \sqcap \cdots \sqcap t_n{}^{\dagger}}$$

$$\frac{}{(\& \; t)^{\dagger} = (t^{\dagger})^{-1} \sqcap t^{\dagger}}$$

$$\frac{}{\mathsf{any}^{\dagger} = \mathbf{Dynamic}}$$

$$\frac{\theta \sqsupseteq \tau^{\dagger}}{(\tau \; \# \; \theta)^{\dagger} = \theta}$$


CAUTION
THIS IS SPARTA

$$\frac{\text{public } \theta \qquad \text{public } \tau}{\tau \ \# \ \theta \leq \text{any}} \qquad \frac{\text{tainted } \theta \qquad \text{tainted } \tau}{\text{any} \leq \tau \ \# \ \theta}$$

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

Mutability + Subtyping = ☠️

Well-formed = Sound

"I'll be fine, thank you!"

$$t_{\mathrm{safe}(1)} = \{\ell : (\&\ (\{\}\ \#\ \mathbf{Dynamic}))\ \#\ \mathbf{Initial}\}\ \#\ \mathbf{Initial}$$

"Help me please!"

$$t_{\mathrm{safe}(2)} = \{\ell : (\&\ (\{\}\ \#\ \mathbf{Initial}))\ \#\ \mathbf{Initial}\}\ \#\ \mathbf{Static}$$

Applications

Well-typed programs can be optimized

Inference $\Gamma \vdash e : t \Longrightarrow c$

Dynamic checking $\Gamma \vdash e : \tau \Uparrow c$

Static checking $\Gamma \vdash e : t \Longleftarrow c$

Insert dynamic checks for tainted types...

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

$$\frac{\Gamma \vdash e : \tau \,\#\, \theta \Longrightarrow c \qquad \mathsf{tainted}\ \theta}{\Gamma \vdash e : \tau \Uparrow \langle \tau^{\bullet} \rangle\, c}$$

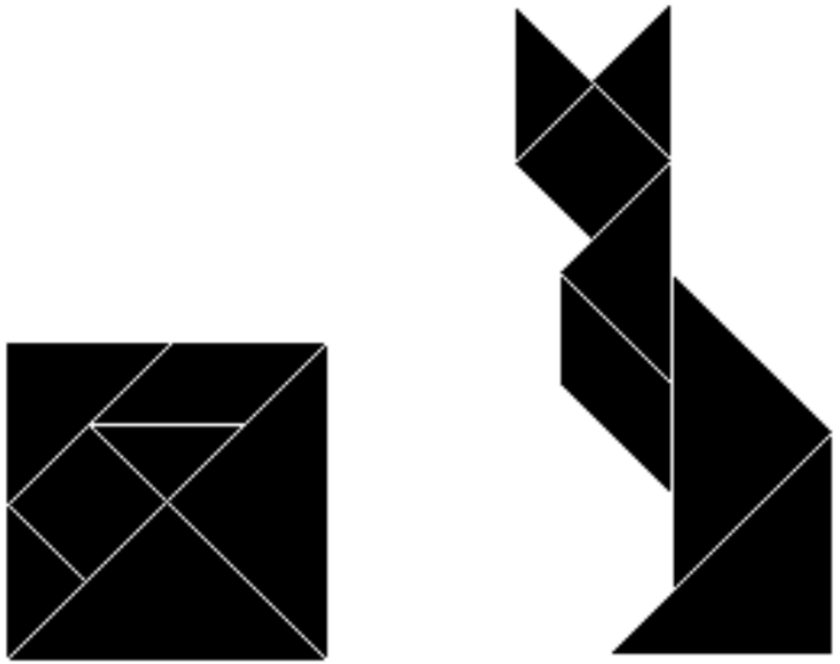
Remove dynamic checks for trusted types!

$$\frac{\Gamma \vdash e : \tau \,\#\, \theta \Longrightarrow c \qquad \text{trusted } \theta}{\Gamma \vdash e : \tau \Uparrow c}$$

Also,
“subtyping models data flow”

$$\frac{\Gamma \vdash e : t' \Longrightarrow c \qquad t' \leq t}{\Gamma \vdash e : t \Longleftarrow c}$$

Well-typed programs can’t be blamed

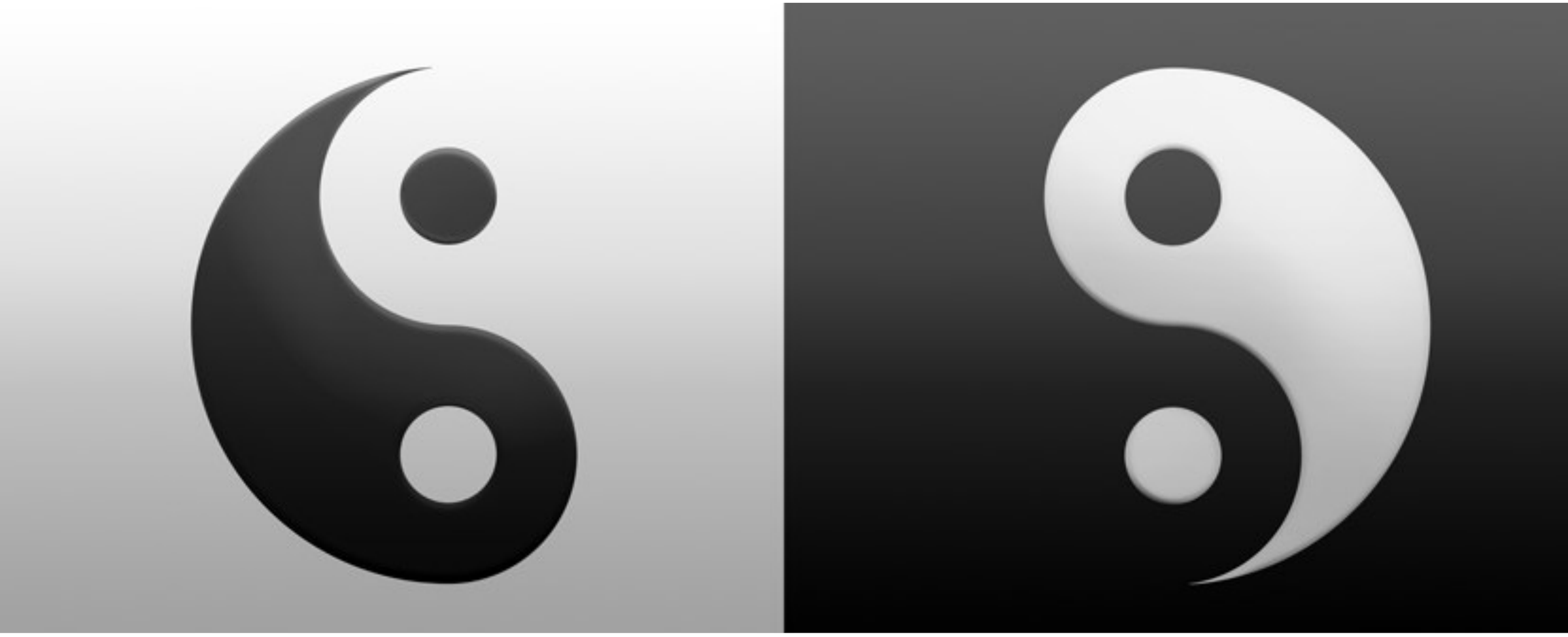


“Encouraging discovery!” 👍

“Disappointing reception” 👎

Safety $t \leq t' \text{ iff } t \leq^{+} t' \text{ and } t \leq^{-} t'$

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



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”