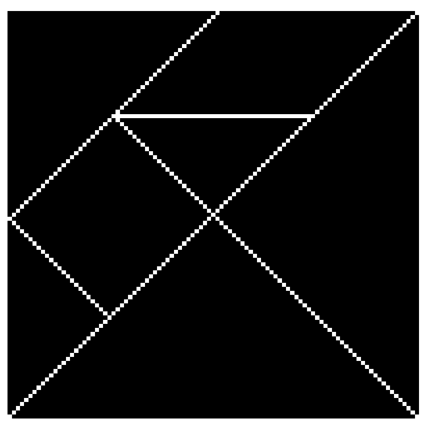
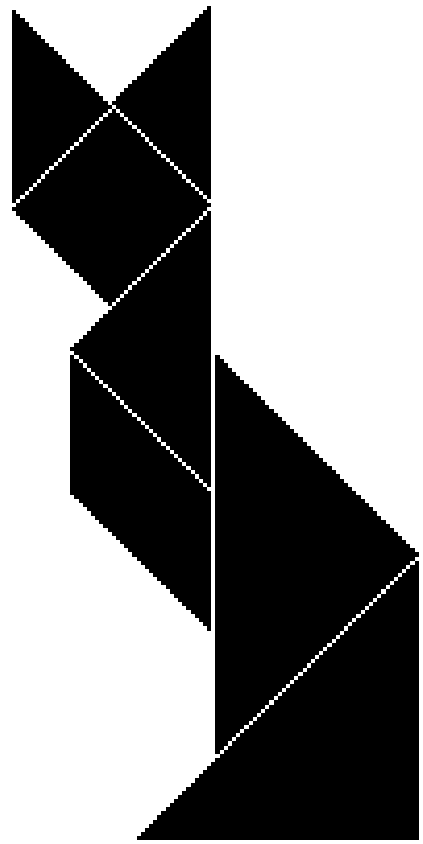
Blame for All

Amal Ahmed, Indiana University
Robert Bruce Findler, Northwestern University
Jacob Matthews, Google
Philip Wadler, University of Edinburgh





A repeated theme

Henglein (1994):
Dynamic typing

Findler and Felleisen (2002):
Contracts

Siek and Taha (2006):
Gradual types

Tobin-Hochstadt and Felleisen (2006):
Migratory types

Flanagan (2006):
Hybrid types

A repeated theme

Javascript 4.0

Perl 6.0

C# 4.0

Visual Basic 9.0

Part I

Blame

Syntax

base type	B		
type	S, T	$::=$	$B \mid S \to T \mid \star$
cast	C, D	$::=$	$B \mid C \to D \mid \star$
ground	G, H	$::=$	$B \mid \star \to \star$
blame label	p, q		
term	s, t, u	$::=$	$x \mid \lambda x : S.\, t \mid t\ s \mid \langle D \Leftarrow C \rangle^p\ s$

Typing

$\boxed{\Gamma \vdash t : T}$

$$\frac{\Gamma \vdash s : S \qquad S \sim T}{\Gamma \vdash \langle T \Leftarrow S \rangle^{p}\, s : T}$$

Compatibility

$\boxed{S \sim T}$

$$\frac{}{S \sim \star} \qquad \frac{}{\star \sim T} \qquad \frac{}{B \sim B}$$

$$\frac{S \sim S' \qquad T \sim T'}{S \to T \sim S' \to T'}$$

Typing

$$\boxed{\Gamma \vdash t : T}$$

$$\frac{\Gamma \vdash s : |C| \qquad C \lhd D}{\Gamma \vdash \langle D \Leftarrow C \rangle^p \, s : |D|}$$

Compatibility

$$\boxed{C \lhd D}$$

$$\frac{}{C \lhd \star} \qquad \frac{}{\star \lhd D} \qquad \frac{}{B \lhd B}$$

$$\frac{C' \lhd C \qquad D \lhd D'}{C \to D \lhd C' \to D'}$$

Erasure

$$\boxed{|C| = T}$$

$$\begin{aligned} |B| &= B \\ |C \to D| &= |C| \to |D| \\ |\star| &= \star \end{aligned}$$

Syntax

$$
\begin{array}{llll}
\text{ground} & G, H & ::= & B \mid \star \to \star \\
\text{value} & v, w & ::= & \lambda x.\, t \mid \langle \star \Leftarrow G \rangle^p\, v
\end{array}
$$

Reductions

$s \longrightarrow t$

$$
\begin{array}{rcl}
(\lambda x.\, t)\; v & \longrightarrow & t[x := v] \\
\langle C' {\to} D' \Leftarrow C {\to} D \rangle^p\; v & \longrightarrow & \lambda x.\, \langle D' \Leftarrow D \rangle^p\; v\; (\langle C \Leftarrow C' \rangle^{\bar{p}}\; x) \\
\langle \star \Leftarrow \star \rangle^p\; v & \longrightarrow & v \\
\langle B \Leftarrow B \rangle^p\; v & \longrightarrow & v \\
\langle \star \Leftarrow C {\to} D \rangle^p\; v & \longrightarrow & \langle \star \Leftarrow \star {\to} \star \rangle^p\; \langle \star {\to} \star \Leftarrow C {\to} D \rangle^p\; v \\
\langle C {\to} D \Leftarrow \star \rangle^p\; v & \longrightarrow & \langle C {\to} D \Leftarrow \star {\to} \star \rangle^p\; \langle \star {\to} \star \Leftarrow \star \rangle^p\; v \\
\langle G \Leftarrow \star \rangle^q \langle \star \Leftarrow G \rangle^p\; v & \longrightarrow & v \\
\langle H \Leftarrow \star \rangle^q \langle \star \Leftarrow G \rangle^p\; v & \longrightarrow & \texttt{blame}\; q, \quad \text{if } G \neq H
\end{array}
$$

Part II

Blame for all

Syntax

base type	B		
type	S, T	$::=$	$B \mid S \to T \mid \star \mid X \mid \forall X. T$
cast	C, D	$::=$	$B \mid C \to D \mid \star \mid X \mid \forall X. C \mid k(T)$
ground	G, H	$::=$	$B \mid \star \to \star \mid k(T)$
term	s, t, u	$::=$	$x \mid \lambda x : S. t \mid t\ s \mid \langle D \Leftarrow C \rangle^p\ s$
			$\lambda X. t \mid t\ S \mid s\ \mathtt{is}^p\ G$

Typing

$$\boxed{\Gamma \vdash t : T}$$

$$\frac{\Gamma \vdash s : |C| \qquad C \lhd D}{\Gamma \vdash \langle D \Leftarrow C \rangle^{p}\, s : |D|}$$

Compatibility

$$\boxed{C \lhd D}$$

$$\frac{}{X \lhd X} \qquad \frac{}{k(T) \lhd k(T)}$$

$$\frac{C[X := \star] \lhd D}{\forall X.\, C \lhd D} \qquad \frac{C \lhd D}{C \lhd \forall X.\, D}\; X \notin C$$

Erasure

$$\boxed{|C| = T}$$

$$\begin{aligned} |X| &= X \\ |\forall X.\, C| &= \forall X.\, |C| \\ |k(T)| &= T \end{aligned}$$

Compatibility is reflexive

$$\dfrac{\dfrac{\dfrac{C \lhd D}{C[X := \star] \lhd D}}{\forall X.\, C \lhd D}}{\forall X.\, C \lhd \forall X.\, D}\; X \notin \forall X.\, C$$

Reduction

$$\boxed{K; s \longrightarrow t; K'}$$

$$\begin{array}{rcl}
K;\ (\Lambda X.\, t)\ S & \longrightarrow & t[X := k(S)];\ K \cup \{k\}, \quad \textbf{if } k \notin K \\
\langle D \Leftarrow \forall X.\, C \rangle^{p}\ v & \longrightarrow & \langle D \Leftarrow C[X := \star] \rangle^{p}\ (v\ \star) \\
\langle \forall X.\, D \Leftarrow C \rangle^{p}\ v & \longrightarrow & \Lambda X.\, \langle D \Leftarrow C \rangle^{p}\ v, \quad \textbf{if } X \notin C, v
\end{array}$$

Reduction, continued

$$
\begin{array}{rcl}
(\langle \star \Leftarrow G\rangle^p\, v)\ \mathtt{is}^q\, G & \longrightarrow & \mathtt{true}, \quad \textbf{if}\ G \neq k(T) \\
(\langle \star \Leftarrow G\rangle^p\, v)\ \mathtt{is}^q\, H & \longrightarrow & \mathtt{false}, \quad \textbf{if}\ G \neq H, k(T) \\
(\langle \star \Leftarrow k(T)\rangle^p\, v)\ \mathtt{is}^q\, H & \longrightarrow & \mathtt{blame}\, q
\end{array}
$$

Part III

Subtyping

Subtype

$$\boxed{C <: D}$$

$$\frac{C <: G}{C <: \star} \qquad \frac{}{\star <: \star} \qquad \frac{}{B <: B} \qquad \frac{C' <: C \qquad D <: D'}{C \to D <: C' \to D'}$$

Positive subtype

$$\boxed{C <:^{+} D}$$

$$\frac{}{C <:^{+} \star} \qquad \frac{}{B <:^{+} B} \qquad \frac{C' <:^{-} C \qquad D <:^{+} D'}{C \to D <:^{+} C' \to D'}$$

Negative subtype

$$\boxed{C <:^{-} D}$$

$$\frac{C <:^{-} G}{C <:^{-} D} \qquad \frac{}{\star <:^{-} D} \qquad \frac{}{B <:^{-} B} \qquad \frac{C' <:^{+} C \qquad D <:^{-} D'}{C \to D <:^{-} C' \to D'}$$

Naive subtype

$$\boxed{C <:_{n} D}$$

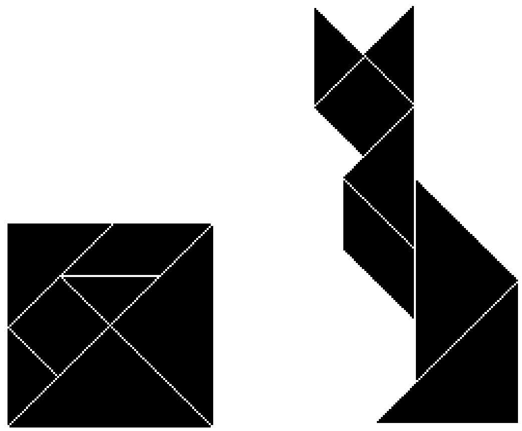
$$\frac{}{C <:_{n} \star} \qquad \frac{}{B <:_{n} B} \qquad \frac{C <:_{n} C' \qquad D <:_{n} D'}{C \to D <:_{n} C' \to D'}$$

Examples

$$\star \longrightarrow \mathtt{I} <: \mathtt{I} \longrightarrow \star$$

$$\mathtt{I} \longrightarrow \mathtt{I} <:_n \star \longrightarrow \star$$

Tangram theorems



$$C <: D \text{ iff } C <:^{+} D \text{ and } C <:^{-} D$$

$$C <:_{n} D \text{ iff } C <:^{+} D \text{ and } D <:^{-} C$$

Safety

$$\frac{C <:^{+} D \qquad s \text{ sf } p}{\langle D \Leftarrow C \rangle^{p}\, s \text{ sf } p} \qquad \frac{C <:^{-} D \qquad s \text{ sf } p}{\langle D \Leftarrow C \rangle^{\bar{p}}\, s \text{ sf } p} \qquad \frac{q \neq p, \bar{p} \qquad s \text{ sf } p}{\langle D \Leftarrow C \rangle^{q}\, s \text{ sf } p}$$

$$\frac{}{x \text{ sf } p} \qquad \frac{t \text{ sf } p}{\lambda x.\, t \text{ sf } p} \qquad \frac{t \text{ sf } p \qquad s \text{ sf } p}{t\ s \text{ sf } p}$$

Blame theorem

Preservation

If s sf p and $s \longrightarrow t$ then t sf p

Progress

If t sf p then $t \not\longrightarrow \texttt{blame}\ p$

Part IV

Subtyping for all

Subtype

$\boxed{C <: D}$

$$\frac{}{X <: X} \qquad \frac{}{k(T) <: k(T)}$$

Positive subtype

$\boxed{C <:^{+} D}$

$$\frac{}{X <:^{+} X} \qquad \frac{}{k(T) <:^{+} k(T)}$$

Negative subtype

$\boxed{C <:^{-} D}$

$$\frac{}{X <:^{-} X} \qquad \frac{}{k(T) <:^{-} k(T)}$$

Naive subtype

$\boxed{C <:_{n} D}$

$$\frac{}{X <:_{n} X} \qquad \frac{}{k(T) <:_{n} k(T)}$$

Subtype

$\boxed{C <: D}$

$$\frac{C[X := \star] <: D}{\forall X.\, C <: D} \qquad \frac{C <: D}{C <: \forall X.\, D}\; X \notin C$$

Positive subtype

$\boxed{C <:^{+} D}$

$$\frac{C[X := \star] <:^{+} D}{\forall X.\, C <:^{+} D} \qquad \frac{C <:^{+} D}{C <:^{+} \forall X.\, D}\; X \notin C$$

Negative subtype

$\boxed{C <:^{-} D}$

$$\frac{C[X := \star] <:^{-} D}{\forall X.\, C <:^{-} D} \qquad \frac{C <:^{-} D}{C <:^{-} \forall X.\, D}\; X \notin C$$

Naive subtype

$\boxed{C <:_{n} D}$

$$\frac{C[X := \star] <:_{n} D}{\forall X.\, C <:_{n} D} \qquad \frac{C <:_{n} D}{C <:_{n} \forall X.\, D}\; X \notin C$$

Subtyping is *not* reflexive

$$\dfrac{\dfrac{\dfrac{C <: D}{C[X := \star] <: D}\ \textit{incorrect!}}{\forall X.\, C <: D}}{\forall X.\, C <: \forall X.\, D}\ X \notin \forall X.\, C$$

Blame theorem still holds

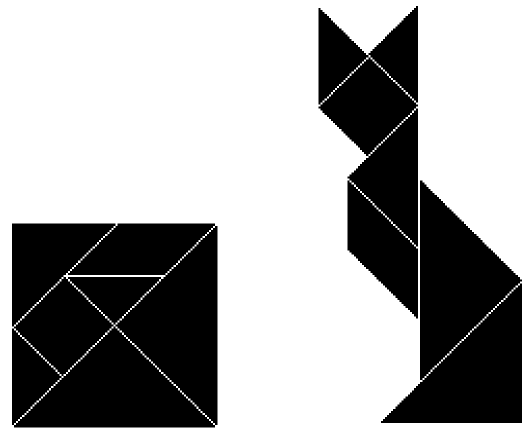
Preservation

If s sf p and $s \longrightarrow t$ then t sf p

Progress

If t sf p then $t \not\longrightarrow \mathtt{blame}\ p$

Tangram theorems still hold



$C <: D$ iff $C <:^{+} D$ and $C <:^{-} D$

$C <:_{n} D$ iff $C <:^{+} D$ and $D <:^{-} C$

Second Tangram Theorem requires two lemmas

Lemma 1:

Assume $X \notin D$

$D <:^{-} C[X := \star]$ iff $D <:^{-} C$

$C[X := \star] <:^{+} D$ iff $C <:^{+} D$

Lemma 2:

$C <:^{+} D$ and $X \notin C$ implies $X \notin D$

$C <:^{-} D$ and $X \notin D$ implies $X \notin C$

Better subtyping

$\boxed{C <:' D}$

$$\frac{C <:' G}{C <:' \star} \qquad \frac{}{\star <:' \star} \qquad \frac{}{B <:' B}$$

$$\frac{C' <:' C \qquad D <:' D'}{C \to D <:' C' \to D'}$$

$$\frac{}{X <:' X} \qquad \frac{}{k(T) <:' k(T)}$$

$$\frac{C[X := T] <:' D}{\forall X.\, C <:' D} \qquad \frac{C <:' D}{C <:' \forall X.\, D}\; X \notin C$$

Maybe ordinary subtyping is of some use after all . . .

The end

Bonus material

Counterexample

It is tempting to take

$$\frac{C[X := T] <:^{+} D}{\forall X.\, C <:^{+} D}$$

but that would be wrong, since

$$\frac{\dfrac{\star <:^{-} \mathtt{I} \qquad \mathtt{I} <:^{+} \mathtt{I}}{\mathtt{I} \rightarrow \mathtt{I} <:^{+} \star \rightarrow \mathtt{I}}}{\forall X.\, X \rightarrow X <:^{+} \star \rightarrow \mathtt{I}}$$

and

$$
\begin{array}{ll}
& ((\langle \star \to \mathtt{I} \Leftarrow \forall X.\, X \to X \rangle^p \; \mathit{id})\; \mathit{true} \\
\longrightarrow & \\
& ((\langle \star \to \mathtt{I} \Leftarrow \star \to \star \rangle^p \; \mathit{id}\; \star)\; \mathit{true} \\
\longrightarrow & \\
& \langle \mathtt{I} \Leftarrow \star \rangle^p \; \mathit{id}\; \star\; (\langle \star \Leftarrow \star \rangle^{\bar{p}}\; \mathit{true}) \\
\longrightarrow & \\
& \langle \mathtt{I} \Leftarrow \star \rangle^p \; \mathit{true} \\
\longrightarrow & \\
& \mathtt{blame}\, p
\end{array}
$$

Proof of tangram theorem (one case)

Assume $X \notin D$

$\forall X. C <:_n D$

iff (def'n subtyping, inversion)

$C[X := \star] <:_n D$

iff (inductive hypothesis)

$C[X := \star] <:^+ D$ and $D <:^- C[X := \star]$

iff (Lemma 1)

$C[X := \star] <:^+ D$ and $D <:^- C$

iff (def'n subtyping, inversion)

$\forall X. C <:^+ D$ and $D <:^- \forall X. C$

Proof of tangram theorem (another case)

Assume $X \notin C$

$C <:_n \forall X.\, D$

iff (def'n subtyping, inversion)

$C <:_n D$

iff (inductive hypothesis)

$C <:^+ D$ and $D <:^- C$

iff (Lemma 2, $X \notin D$ implies $D = D[X := \star]$)

$C <:^+ D$ and $D[X := \star] <:^- C$

iff (def'n subtyping, inversion)

$C <:^+ \forall X.\, D$ and $\forall X.\, D <:^- C$