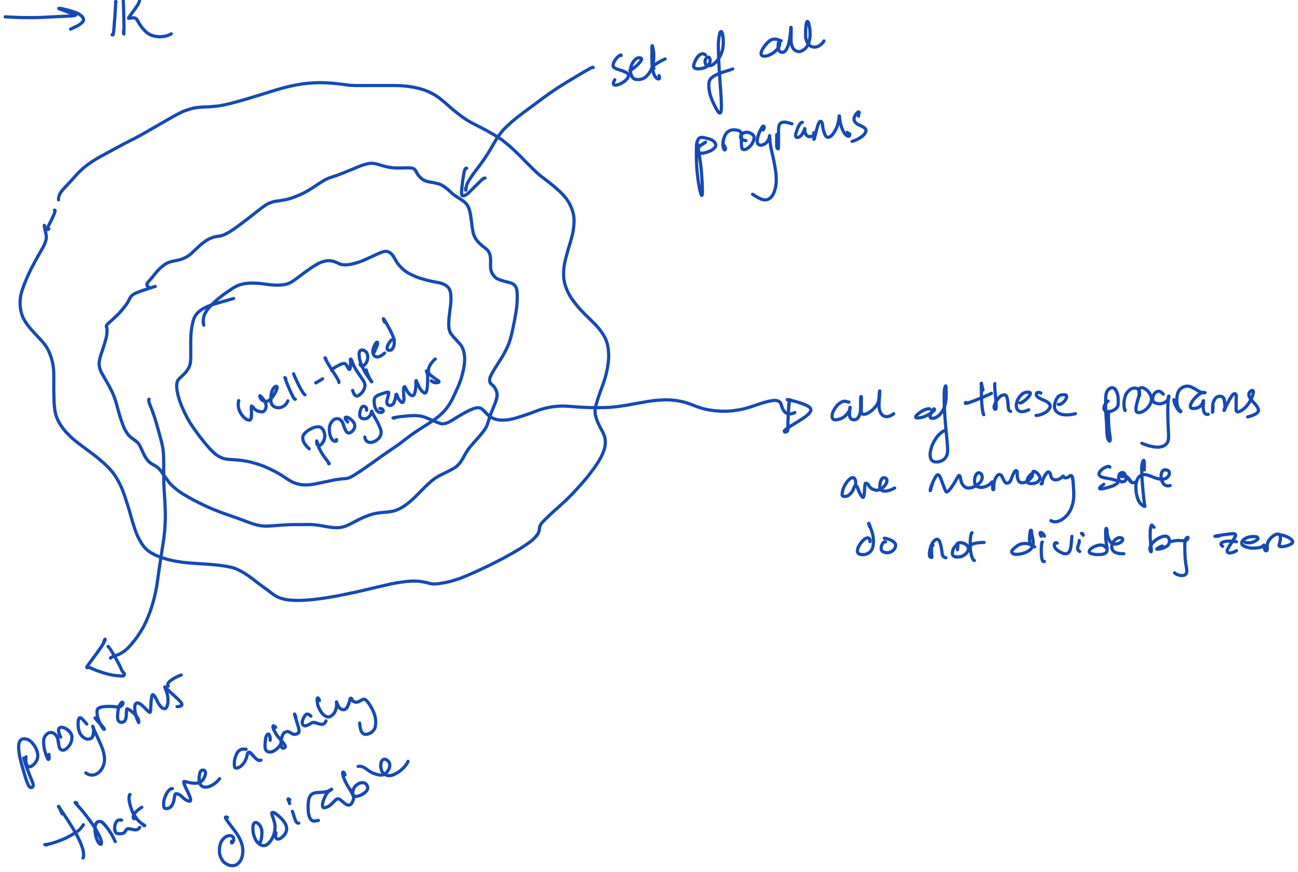
TYPES!

$f : \mathbb{R} \to \mathbb{R}$



Type checking : program P, type T $\xrightarrow{\text{check}}$ P has type T ?

Type inference : program P $\xrightarrow{\text{infer}}$ P has type T

$\lambda x.\ x + \boxed{10}$

int $\to$ int

λ calc subset

0, succ 0, isZero n, tru, fls, pred

if ___ then ___ else ___

isZero tru

$\boxed{\text{undefined behavior}}$

Operational semantics ≡ β reduction

pred 0 → 0

isZero 0 → tru

isZero (succ n) → fls

pred (succ n) → n

if tru then t_1 else t_2 → t_1

if fls then t_1 else t_2 → t_2

congruence rule for pred

$$\frac{t \to t'}{\text{succ } t \to \text{succ } t'}$$

pred (pred 0)

↓

pred 0

↓

0

if t_1 then t_2 else t_3 → if t_1' then t_2 else t_3

assuming $t_1 \to t_1'$

$$\frac{t_1 \to t_1'}{\text{if } t_1 \text{ then } t_2 \text{ else } t_3 \to \text{if } t_1' \text{ then } t_2 \text{ else } t_3}$$

T := Bool | Nat

t : T OR t ∈ T

Base case:

tru ∈ Bool

fls ∈ Bool

0 ∈ Nat

$$\frac{t \in \text{Nat}}{\text{isZero } t \in \text{Bool}} \; T_{\text{isZero}}$$

$$\frac{t \in \text{Nat}}{\text{succ } t \in \text{Nat}} \; T_{\text{succ}}$$

$$\frac{t \in \text{Nat}}{\text{pred } t \in \text{Nat}}$$

$$\dfrac{t_1 \in Bool \qquad t_2, t_3 \in \overset{\text{any type}}{T}}{\text{if } t_1 \text{ then } t_2 \text{ else } t_3 \in T} \; T\text{-if}$$

A term t is typable if there is a type T s.t.
OR well-typed

$$\underbrace{t \in T}_{\text{typing relation}}$$

smallest binary relation satisfying the typing rules

$$\dfrac{\dfrac{\overset{BC}{0 \in Nat}}{\text{isZero } 0 \in Bool} \qquad \overset{BC}{0 \in Nat} \qquad \dfrac{\overset{BC}{0 \in Nat}}{\text{pred } 0 \in Nat}}{\text{if } \underbrace{\text{isZero } 0}_{t_1} \text{ then } \underbrace{0}_{t_2} \text{ else } \underbrace{\text{pred } 0}_{t_3} \in \underbrace{Nat}_{T}}$$

Theorem : Each term t has at most a single type T s.t. $t \in T$ (uniqueness)

Proof : Base cases

$0 \in Nat$, $tru \in Bool$, $fls \in Bool$

hypothesis

any term of size $\leq n$ has at most 1 type

inductive step

take term of size $n+1$

assume term has type T

case 1 $\quad$ $succ\ t_1 \in T$

$$\frac{t_1 \in Nat}{succ\ t_1 \in Nat}$$

t_1 has at most 1 type

$\therefore T = Nat$

case 2 $\quad$ $if\ t_1\ then\ t_2\ else\ t_3 \in T$

$$\frac{t_1 \in Bool \qquad t_2, t_3 \in T}{if\ t_1\ then\ t_2\ else\ t_3 \in T}$$

Safety = progress + preservation

well-typed terms "don't get stuck"

pred tm

progress: A well-typed term is not stuck (either it's a value or can go one more step)

preservation: if a well-typed term takes a step of execution/evaluation (per operational semantics) then the result is well-typed

Thm (progress)

Suppose $t \in T$. Then either t is $\underbrace{\text{a value}}_{0,\ tru,\ fls,\ succ(\cdots 0)}$ or $t \to t'$

Thm (preservation)

if $t \in T$ and $t \to t'$, then $t' \in T$

$$\frac{BC \quad BC \quad BC}{t \in T}$$

Base case

$t =$ true / fls / 0

then $t \not\to t'$ and the theorem holds vacuously

Induction

$$\frac{t_1 \in Bool \qquad t_2, t_3 \in T}{\text{if } t_1 \text{ then } t_2 \text{ else } t_3 \in T}$$

Case 1 $t_1 = true$

then $t' = t_2$

we know $t_2 \in T$ $\therefore$ $t' \in T$

Case 2 $t_1 = fls$

same argument

Case 3 $\quad t_1 \longrightarrow t_1'$ $\quad$ By inductive hypothesis $t_1' \in$ Bool

$$\text{if } t_1 \text{ then } t_2 \text{ else } t_3$$

$$\longrightarrow \text{if } t_1' \text{ then } t_2 \text{ else } t_3$$