Exceptions

Syntax

- `throw` e

  Jinja: e can be of any class

  Java: e must be of a subclass of `Throwable`

- `try` e_1 `catch` $(C\ V)\ e_2$

Example:

`try throw` (`new` C) `catch` $(C\ V)$ `Var` V
behaves like `new` C

System exceptions

System exception classes:

$$\mathit{NullPointer}, \mathit{ClassCast}, \mathit{OutOfMemory} :: \mathit{cname}$$

Simplification: System exceptions are allocated *statically* not created *dynamically*:

$$\mathit{addr\text{-}of\text{-}sys\text{-}xcpt} :: \mathit{cname} \Rightarrow \mathit{addr}$$

Abbreviations:

$$\texttt{Throw}\ a \equiv \texttt{throw}(\mathit{addr}\ a)$$
$$\texttt{THROW}\ C \equiv \texttt{Throw}(\mathit{addr\text{-}of\text{-}sys\text{-}xcpt}\ C)$$

Extension of big step semantics

Variable access

$$I\,V = \lfloor v \rfloor \Longrightarrow$$
$$P \vdash \langle \mathtt{Var}\ V, (h, l) \rangle \Rightarrow \langle \mathtt{Val}\ v, (h, l) \rangle$$

Uninitialized variables cannot be evaluated

Field access

$$[\![P \vdash \langle e, s_0\rangle \Rightarrow \langle \mathit{addr}\ a, (h, l)\rangle; h\ a = \lfloor (C, \mathit{fs})\rfloor; \mathit{fs}\ (F, D) = \lfloor v\rfloor]\!]$$
$$\Longrightarrow P \vdash \langle e.F\{D\}, s_0\rangle \Rightarrow \langle \mathtt{Val}\ v, (h, l)\rangle$$

Exception creation:

$$P \vdash \langle e, s_0\rangle \Rightarrow \langle \mathit{null}, s_1\rangle \Longrightarrow$$
$$P \vdash \langle e.F\{D\}, s_0\rangle \Rightarrow \langle \mathtt{THROW}\ \mathit{NullPointer}, s_1\rangle$$

Exception propagation:

$$P \vdash \langle e, s_0\rangle \Rightarrow \langle \mathtt{throw}\ e', s_1\rangle \Longrightarrow$$
$$P \vdash \langle e.F\{D\}, s_0\rangle \Rightarrow \langle \mathtt{throw}\ e', s_1\rangle$$

Binary operations

$$[\![P \vdash \langle e_1,s_0\rangle \Rightarrow \langle \texttt{Val}\ v_1,s_1\rangle; P \vdash \langle e_2,s_1\rangle \Rightarrow \langle \texttt{Val}\ v_2,s_2\rangle;$$
$$\mathit{binop}\ (\mathit{bop}, v_1, v_2) = \lfloor v \rfloor]\!]$$
$$\Longrightarrow P \vdash \langle e_1 \ll \mathit{bop} \gg e_2,s_0\rangle \Rightarrow \langle \texttt{Val}\ v,s_2\rangle$$

Exception propagation:

$$P \vdash \langle e_1,s_0\rangle \Rightarrow \langle \texttt{throw}\ e,s_1\rangle \Longrightarrow$$
$$P \vdash \langle e_1 \ll \mathit{bop} \gg e_2,s_0\rangle \Rightarrow \langle \texttt{throw}\ e,s_1\rangle$$

$$[\![P \vdash \langle e_1,s_0\rangle \Rightarrow \langle \texttt{Val}\ v_1,s_1\rangle;$$
$$P \vdash \langle e_2,s_1\rangle \Rightarrow \langle \texttt{throw}\ e,s_2\rangle]\!]$$
$$\Longrightarrow P \vdash \langle e_1 \ll \mathit{bop} \gg e_2,s_0\rangle \Rightarrow \langle \texttt{throw}\ e,s_2\rangle$$

new

$$[\![\mathit{new\text{-}Addr}\ h = \lfloor a \rfloor;\ P \vdash C\ \mathit{has\text{-}fields}\ \mathit{FDTs};$$
$$h' = h(a \mapsto (C, \mathit{init\text{-}fields}\ \mathit{FDTs}))]\!]$$
$$\Longrightarrow P \vdash \langle \mathsf{new}\ C, (h, l)\rangle \Rightarrow \langle \mathit{addr}\ a, (h', l)\rangle$$

Exception creation:

$$\mathit{new\text{-}Addr}\ h = \mathit{None} \Longrightarrow$$
$$P \vdash \langle \mathsf{new}\ C, (h, l)\rangle \Rightarrow \langle \mathsf{THROW}\ \mathit{OutOfMemory}, (h, l)\rangle$$

Cast

$$[\![P \vdash \langle e,s_0\rangle \Rightarrow \langle \mathit{addr}\ a,(h,l)\rangle; h\ a = \lfloor(D,fs)\rfloor; P \vdash D \preceq^* C]\!]$$
$$\Longrightarrow P \vdash \langle \texttt{Cast}\ C\ e,s_0\rangle \Rightarrow \langle \mathit{addr}\ a,(h,l)\rangle$$

Exception creation:

$$[\![P \vdash \langle e,s_0\rangle \Rightarrow \langle \mathit{addr}\ a,(h,l)\rangle; h\ a = \lfloor(D,fs)\rfloor; \neg\, P \vdash D \preceq^* C]\!]$$
$$\Longrightarrow P \vdash \langle \texttt{Cast}\ C\ e,s_0\rangle \Rightarrow \langle \texttt{THROW}\ \mathit{ClassCast},(h,l)\rangle$$

Exception propagation:

$$P \vdash \langle e,s_0\rangle \Rightarrow \langle \texttt{throw}\ e',s_1\rangle \Longrightarrow$$
$$P \vdash \langle \texttt{Cast}\ C\ e,s_0\rangle \Rightarrow \langle \texttt{throw}\ e',s_1\rangle$$

Variable assignment

$$[\![P \vdash \langle e, s_0 \rangle \Rightarrow \langle \texttt{Val}\ v, (h, l) \rangle; l' = l(V \mapsto v)]\!]$$
$$\Longrightarrow P \vdash \langle V := e, s_0 \rangle \Rightarrow \langle \mathit{unit}, (h, l') \rangle$$

Exception propagation:

$$P \vdash \langle e, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_1 \rangle \Longrightarrow$$
$$P \vdash \langle V := e, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_1 \rangle$$

Field assignment (1)

$$[\![P \vdash \langle e_1, s_0\rangle \Rightarrow \langle \mathit{addr}\ a, s_1\rangle;\ P \vdash \langle e_2, s_1\rangle \Rightarrow \langle \mathtt{Val}\ v, (h_2, l_2)\rangle;$$
$$h_2\ a = \lfloor (C, fs)\rfloor;\ fs' = fs((F, D) \mapsto v);\ h_2' = h_2(a \mapsto (C, fs'))]\!]$$
$$\Longrightarrow P \vdash \langle e_1.F\{D\} := e_2, s_0\rangle \Rightarrow \langle \mathit{unit}, (h_2', l_2)\rangle$$

Exception creation:

$$[\![P \vdash \langle e_1, s_0\rangle \Rightarrow \langle \mathit{null}, s_1\rangle;\ P \vdash \langle e_2, s_1\rangle \Rightarrow \langle \mathtt{Val}\ v, s_2\rangle]\!]$$
$$\Longrightarrow P \vdash \langle e_1.F\{D\} := e_2, s_0\rangle \Rightarrow \langle \mathtt{THROW}\ \mathit{NullPointer}, s_2\rangle$$

Principles:

- Evaluate all arguments before throwing an exception.
- Propagate exceptions immediately.

Field assignment (2)

Exception propagation:

$$P \vdash \langle e_1, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_1 \rangle \Longrightarrow$$
$$P \vdash \langle e_1.F\{D\} := e_2, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_1 \rangle$$

$$[\![P \vdash \langle e_1, s_0 \rangle \Rightarrow \langle \texttt{Val}\ v, s_1 \rangle;$$
$$P \vdash \langle e_2, s_1 \rangle \Rightarrow \langle \texttt{throw}\ e', s_2 \rangle]\!]$$
$$\Longrightarrow P \vdash \langle e_1.F\{D\} := e_2, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_2 \rangle$$

Method call

Exception creation:

$$[\![P \vdash \langle e,s_0\rangle \Rightarrow \langle \mathit{null},s_1\rangle;\ P \vdash \langle \mathit{ps},s_1\rangle\ [\Rightarrow]\ \langle \mathit{map}\ \mathtt{Val}\ \mathit{vs},s_2\rangle]\!]$$
$$\Longrightarrow P \vdash \langle e.M(\mathit{ps}),s_0\rangle \Rightarrow \langle \mathtt{THROW}\ \mathit{NullPointer},s_2\rangle$$

Exception propagation:

$$P \vdash \langle e,s_0\rangle \Rightarrow \langle \mathtt{throw}\ e',s_1\rangle \Longrightarrow$$
$$P \vdash \langle e.M(\mathit{ps}),s_0\rangle \Rightarrow \langle \mathtt{throw}\ e',s_1\rangle$$

$$[\![P \vdash \langle e,s_0\rangle \Rightarrow \langle \mathtt{Val}\ v,s_1\rangle;$$
$$P \vdash \langle \mathit{es},s_1\rangle\ [\Rightarrow]\ \langle \mathit{map}\ \mathtt{Val}\ \mathit{vs} @ (\mathtt{throw}\ \mathit{ex} \cdot \mathit{es}'),s_2\rangle]\!]$$
$$\Longrightarrow P \vdash \langle e.M(\mathit{es}),s_0\rangle \Rightarrow \langle \mathtt{throw}\ \mathit{ex},s_2\rangle$$

Expression list

$[\![P \vdash \langle e, s_0\rangle \Rightarrow \langle \mathtt{Val}\ v, s_1\rangle; P \vdash \langle es, s_1\rangle\ [\Rightarrow]\ \langle es', s_2\rangle]\!]$
$\Longrightarrow P \vdash \langle e \cdot es, s_0\rangle\ [\Rightarrow]\ \langle \mathtt{Val}\ v \cdot es', s_2\rangle$

Exception propagation:

$P \vdash \langle e, s_0\rangle \Rightarrow \langle \mathtt{throw}\ e', s_1\rangle \Longrightarrow$
$P \vdash \langle e \cdot es, s_0\rangle\ [\Rightarrow]\ \langle \mathtt{throw}\ e' \cdot es, s_1\rangle$

Sequential composition

$$[\![P \vdash \langle e_0, s_0\rangle \Rightarrow \langle \texttt{Val}\ v, s_1\rangle; P \vdash \langle e_1, s_1\rangle \Rightarrow \langle e_2, s_2\rangle]\!]$$
$$\Longrightarrow P \vdash \langle e_0\texttt{;}\ e_1, s_0\rangle \Rightarrow \langle e_2, s_2\rangle$$

Exception propagation:

$$P \vdash \langle e_0, s_0\rangle \Rightarrow \langle \texttt{throw}\ e, s_1\rangle \Longrightarrow$$
$$P \vdash \langle e_0\texttt{;}\ e_1, s_0\rangle \Rightarrow \langle \texttt{throw}\ e, s_1\rangle$$

if

Exception propagation:

$$P \vdash \langle e, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_1 \rangle \Longrightarrow$$

$$P \vdash \langle \texttt{if}\ (e)\ e_1\ \texttt{else}\ e_2, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_1 \rangle$$

while

Exception propagation:

$$P \vdash \langle e, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_1 \rangle \Longrightarrow$$
$$P \vdash \langle \texttt{while}\ (e)\ c, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_1 \rangle$$

$$[\![P \vdash \langle e, s_0 \rangle \Rightarrow \langle \mathit{true}, s_1 \rangle ; P \vdash \langle c, s_1 \rangle \Rightarrow \langle \texttt{throw}\ e', s_2 \rangle]\!]$$
$$\Longrightarrow P \vdash \langle \texttt{while}\ (e)\ c, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_2 \rangle$$

throw

$$P \vdash \langle e, s_0 \rangle \Rightarrow \langle \mathit{addr}\ a, s_1 \rangle \Longrightarrow$$
$$P \vdash \langle \texttt{throw}\ e, s_0 \rangle \Rightarrow \langle \texttt{Throw}\ a, s_1 \rangle$$

Exception creation:

$$P \vdash \langle e, s_0 \rangle \Rightarrow \langle \mathit{null}, s_1 \rangle \Longrightarrow$$
$$P \vdash \langle \texttt{throw}\ e, s_0 \rangle \Rightarrow \langle \texttt{THROW}\ \mathit{NullPointer}, s_1 \rangle$$

Exception propagation:

$$P \vdash \langle e, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_1 \rangle \Longrightarrow$$
$$P \vdash \langle \texttt{throw}\ e, s_0 \rangle \Rightarrow \langle \texttt{throw}\ e', s_1 \rangle$$

`try catch` *(1)*

Normal evaluation:

$$P \vdash \langle e_1, s_0 \rangle \Rightarrow \langle \texttt{Val}\ v_1, s_1 \rangle \Longrightarrow$$

$$P \vdash \langle \texttt{try}\ e_1\ \texttt{catch}\ (C\ V)\ e_2, s_0 \rangle \Rightarrow \langle \texttt{Val}\ v_1, s_1 \rangle$$

try catch *(2)*

Exception handling:

$$[\![P \vdash \langle e_1, s_0\rangle \Rightarrow \langle \mathtt{Throw}\ a, (h_1, l_1)\rangle;\ h_1\ a = \lfloor (D, fs)\rfloor;$$
$$P \vdash D \preceq^* C;\ P \vdash \langle e_2, (h_1, l_1(V \mapsto Addr\ a))\rangle \Rightarrow \langle e_2', (h_2, l_2)\rangle]\!]$$
$$\Longrightarrow P \vdash \langle \mathtt{try}\ e_1\ \mathtt{catch}\ (C\ V)\ e_2, s_0\rangle \Rightarrow$$
$$\langle e_2', (h_2, l_2(V := l_1\ V))\rangle$$

Exception propagation:

$$[\![P \vdash \langle e_1, s_0\rangle \Rightarrow \langle \mathtt{Throw}\ a, (h_1, l_1)\rangle;\ h_1\ a = \lfloor (D, fs)\rfloor;$$
$$\neg\, P \vdash D \preceq^* C]\!]$$
$$\Longrightarrow P \vdash \langle \mathtt{try}\ e_1\ \mathtt{catch}\ (C\ V)\ e_2, s_0\rangle \Rightarrow \langle \mathtt{Throw}\ a, (h_1, l_1)\rangle$$

Final expressions redefined (exercise)

$final\ e \equiv (\exists v.\ e = \mathtt{Val}\ v) \vee (\exists a.\ e = \mathtt{Throw}\ a)$

$finals\ es \equiv ?$

Lemma If $P \vdash \langle e,s\rangle \Rightarrow \langle e',s'\rangle$ then $final\ e'$.
If $P \vdash \langle es,s\rangle\ [\Rightarrow]\ \langle es',s'\rangle$ then $finals\ es'$.

Proof by simultaneous rule induction.

Extension of small step semantics

Variable access

$$lcl\ s\ V = \lfloor v \rfloor \Longrightarrow P \vdash \langle \mathtt{Var}\ V, s \rangle \rightarrow \langle \mathtt{Val}\ v, s \rangle$$

$$lcl\ s\ V = None \Longrightarrow P \vdash \langle Var\ V, s \rangle \rightarrow ?$$

Uninitialized variables cannot be reduced

Ill-formed configuration — small step semantics is *stuck*

Field access

Exception creation:

$$P \vdash \langle \mathit{null}.F\{D\}, s\rangle \longrightarrow \langle \texttt{THROW}\ \mathit{NullPointer}, s\rangle$$

Exception propagation:

$$P \vdash \langle \texttt{throw}\ e.F\{D\}, s\rangle \longrightarrow \langle \texttt{throw}\ e, s\rangle$$

new

Exception creation:

$$\mathit{new\text{-}Addr}\ h = \mathit{None} \Longrightarrow$$

$$P \vdash \langle \mathsf{new}\ C, (h, l) \rangle \rightarrow \langle \mathsf{THROW}\ \mathit{OutOfMemory}, (h, l) \rangle$$

Cast

Exception creation:

$$[\![hp\ s\ a = \lfloor (D, fs) \rfloor; \neg\ P \vdash D \preceq^* C]\!]$$
$$\Longrightarrow P \vdash \langle \texttt{Cast}\ C\ (addr\ a), s \rangle \rightarrow \langle \texttt{THROW}\ ClassCast, s \rangle$$

Exception propagation:

$$P \vdash \langle \texttt{Cast}\ C\ (\texttt{throw}\ e), s \rangle \rightarrow \langle \texttt{throw}\ e, s \rangle$$

Variable assignment

Exception propagation:

$P \vdash \langle V := \texttt{throw}\, e, s \rangle \rightarrow \langle \texttt{throw}\, e, s \rangle$

Field assignment

Exception creation:

$$P \vdash \langle \mathit{null}.F\{D\} := \mathtt{Val}\ v, s\rangle \longrightarrow \langle \mathtt{THROW}\ \mathit{NullPointer}, s\rangle$$

Exception propagation:

$$P \vdash \langle \mathtt{throw}\ e.F\{D\} := e_2, s\rangle \longrightarrow \langle \mathtt{throw}\ e, s\rangle$$

$$P \vdash \langle \mathtt{Val}\ v.F\{D\} := \mathtt{throw}\ e, s\rangle \longrightarrow \langle \mathtt{throw}\ e, s\rangle$$

Method call

Exception creation:

$$P \vdash \langle null.M(map\ \texttt{Val}\ vs), s\rangle \rightarrow \langle \texttt{THROW}\ NullPointer, s\rangle$$

Exception propagation:

$$P \vdash \langle \texttt{throw}\ e.M(es), s\rangle \rightarrow \langle \texttt{throw}\ e, s\rangle$$

$$P \vdash \langle \texttt{Val}\ v.M(map\ \texttt{Val}\ vs\ @\ (\texttt{throw}\ e \cdot es')), s\rangle \rightarrow \langle \texttt{throw}\ e, s\rangle$$

Expression list

$$P \vdash \langle e,s\rangle \rightarrow \langle e',s'\rangle \Longrightarrow$$
$$P \vdash \langle e \cdot es,s\rangle \; [\rightarrow] \; \langle e' \cdot es,s'\rangle$$

$$P \vdash \langle es,s\rangle \; [\rightarrow] \; \langle es',s'\rangle \Longrightarrow$$
$$P \vdash \langle \mathtt{Val}\, v \cdot es,s\rangle \; [\rightarrow] \; \langle \mathtt{Val}\, v \cdot es',s'\rangle$$

Sequential composition

$$P \vdash \langle e,s\rangle \rightarrow \langle e',s'\rangle \Longrightarrow$$
$$P \vdash \langle e;\ e_2,s\rangle \rightarrow \langle e';\ e_2,s'\rangle$$

$$P \vdash \langle \texttt{Val}\ v;\ e_2,s\rangle \rightarrow \langle e_2,s\rangle$$

Exception propagation:

$$P \vdash \langle \texttt{throw}\ e;\ e_2,s\rangle \rightarrow \langle \texttt{throw}\ e,s\rangle$$

`if`

Exception propagation:

$$P \vdash \langle \texttt{if}\ (\texttt{throw}\ e)\ e_1\ \texttt{else}\ e_2, s\rangle \longrightarrow \langle \texttt{throw}\ e, s\rangle$$

while

$$P \vdash \langle \texttt{while}\ (b)\ c, s \rangle \longrightarrow \langle \texttt{if}\ (b)\ (c; \texttt{while}\ (b)\ c)\ \texttt{else}\ \mathit{unit}, s \rangle$$

throw

$$P \vdash \langle e, s \rangle \rightarrow \langle e', s' \rangle \Longrightarrow$$
$$P \vdash \langle \texttt{throw}\, e, s \rangle \rightarrow \langle \texttt{throw}\, e', s' \rangle$$

Exception creation:

$$P \vdash \langle \texttt{throw}\, \mathit{null}, s \rangle \rightarrow \langle \texttt{THROW}\, \mathit{NullPointer}, s \rangle$$

Exception propagation:

$$P \vdash \langle \texttt{throw}\, (\texttt{throw}\, e), s \rangle \rightarrow \langle \texttt{throw}\, e, s \rangle$$

`try catch` *(1)*

$$P \vdash \langle e,s \rangle \rightarrow \langle e',s' \rangle \Longrightarrow$$
$$P \vdash \langle \texttt{try}\ e\ \texttt{catch}\ (C\ V)\ e_2,s \rangle \rightarrow$$
$$\langle \texttt{try}\ e'\ \texttt{catch}\ (C\ V)\ e_2,s' \rangle$$

Normal evaluation:

$$P \vdash \langle \texttt{try}\ \texttt{Val}\ v\ \texttt{catch}\ (C\ V)\ e_2,s \rangle \rightarrow \langle \texttt{Val}\ v,s \rangle$$

`try catch` *(2)*

Exception handling:

$$[\![hp\ s\ a = \lfloor (D, fs) \rfloor ; P \vdash D \preceq^* C]\!]$$
$$\Longrightarrow P \vdash \langle \texttt{try Throw}\ a\ \texttt{catch}\ (C\ V)\ e_2, s \rangle \rightarrow$$
$$\langle \{ V{:}Class\ C; V\ \texttt{:=}\ addr\ a\ \texttt{;}\ e_2 \}, s \rangle$$

$$[\![hp\ s\ a = \lfloor (D, fs) \rfloor ; \neg\, P \vdash D \preceq^* C]\!]$$
$$\Longrightarrow P \vdash \langle \texttt{try Throw}\ a\ \texttt{catch}\ (C\ V)\ e_2, s \rangle \rightarrow \langle \texttt{Throw}\ a, s \rangle$$