



# CS 515: Failures, Divergences, and Infinite Traces

Stefan D. Bruda

Winter 2019

- We continue to record the stable failures of a process, but we also perform other observations
- **Divergent process:**  $P \uparrow = \exists (P_i)_{i \in \mathbb{N}} : P = P_0 \wedge \forall i \in \mathbb{N} : P_i \xrightarrow{\tau} P_{i+1}$ 
  - The process might reach stable state but there is no guarantee that this will happen
  - Worse possible behaviour
- A **divergent trace**  $tr$  of a process  $P$  is a trace that leads to a divergent state:  $P \xrightarrow{tr} P' \wedge P' \uparrow$
- **Infinite traces:**  $u = \langle a_1, a_2, a_3, \dots \rangle$  is an infinite trace of  $P$  whenever  $\exists (P_i)_{i \in \mathbb{N}} : P = P_0 \wedge \forall i \in \mathbb{N} : P_i \xrightarrow{\langle a_i \rangle} P_{i+1}$ 
  - **ITRACE:** set of all possible infinite traces over  $\Sigma$
  - Note that an infinite trace cannot contain  $\surd$

## SEMANTIC MODEL



- The failure, divergences, and infinite trace (FDI) model identifies a process with the three sets of stable failures, divergent, and infinite traces
- **Consistency conditions for failures:**
  - 1  $(\langle \rangle, \{\}) \in F$  (there is always at least one observation)
  - 2  $(tr, X) \in F \wedge tr' \leq tr \implies (tr', \{\}) \in F$  (closure under prefix for traces)
  - 3  $(tr, X) \in F \wedge X' \subseteq X \implies (tr, X') \in F$  (subset closure for refusals)
  - 4  $(tr, X) \in F \wedge \forall a \in X' : (tr \frown \langle a \rangle, \{\}) \notin F \implies (tr, X \cup X') \in F$  (an event is either refused or permitted)
- **Consistency conditions for divergent traces:**
  - 1  $tr \in D \wedge tr \leq tr' \implies tr' \in D$  (we have a divergent trace no matter how much we continue past the divergence – pessimistic approach)
  - 2  $tr \in D \wedge X \subseteq \Sigma^\surd \implies (tr, X) \in F$  (any possible divergence is associated with any possible set of refusals)
  - 3  $tr \in D \wedge tr \leq u \implies u \in I$  (once a process has diverged nothing can be ruled out)
  - 4  $tr \frown \langle \surd \rangle \in D \implies tr \in D$  (if a process is divergent upon termination it means that it was already divergent)

## SEMANTIC MODEL (CONT'D)



- **FDI determinism:**
  - A process is deterministic whenever  $\forall tr, A : (tr \frown \langle a \rangle, \{\}) \in F \implies (tr, \{a\}) \notin F$
  - No divergent process can be deterministic (since after divergence all failures are possible)
  - Deterministic processes can be completely characterized by their traces: For the set  $T$  of traces,
 
$$F_T = \{(tr, X) : tr \in T \wedge \forall a \in X : tr \frown \langle a \rangle \notin T\}$$

$$D_T = \{\}$$

$$I_T = \{u : \forall tr \leq u : \#tr \in \mathbb{N} \implies tr \in T\}$$
  - **Closure:**  $\overline{(F, D, I)} = (F, S, \{u : \forall tr \leq u : (tr, \{\}) \in F\})$ 
    - A set  $(F, D, I)$  is closed whenever  $(F, D, I) = \overline{(F, D, I)}$
  - **Finitely nondeterministic processes:** internal choice only between finitely many alternatives; always closed
- **Consistency for infinite traces:**
  - 1  $u \in I \wedge tr < u \implies (tr, \{\}) \in F$  (finite prefixes of infinite traces must appear in  $F$ )
  - 2  $\forall (tr, X) \in F : \exists T : \{(tr \frown tr', X') : (tr', X') \in F_T\} \subseteq F \wedge \{tr \frown u : u \in I_T\} \subseteq I$  (deterministic refinement)



- Each process  $P$  associated three sets  $\mathcal{F}[P]$  (failures),  $\mathcal{D}[P]$  (divergent traces) and  $\mathcal{I}[P]$  (infinite traces)
- Special properties for divergence-free processes:

$$\begin{aligned} \mathcal{D}[P] = \{\} &\implies \{tr : (tr, \{\}) \in \mathcal{F}[P]\} = \text{traces}(P) \\ \mathcal{D}[P] = \{\} &\implies \mathcal{F}[P] = \mathcal{SF}[P] \end{aligned}$$

- $\mathcal{F}[STOP] = \{(\langle \rangle, X) : X \subseteq \Sigma^\vee\}$ ;  $\mathcal{D}[STOP] = \mathcal{I}[STOP] = \{\}$
- $\mathcal{F}[SKIP] = \{(\langle \rangle, X) : \checkmark \notin X\} \cup \{(\langle \checkmark \rangle, X) : X \subseteq \Sigma^\vee\}$ ;  
 $\mathcal{D}[SKIP] = \mathcal{I}[SKIP] = \{\}$
- $\mathcal{F}[DIV] = \{(tr, X) : tr \in TRACE \wedge X \subseteq \Sigma^\vee\}$ ;  $\mathcal{D}[DIV] = TRACE$ ;  
 $\mathcal{I}[DIV] = ITRACE$  (all possible failures, divergences, and traces)
- $\mathcal{F}[CHAOS] = \{(tr, X) : tr \in TRACE \wedge X \subseteq \Sigma^\vee\}$ ;  $\mathcal{D}[CHAOS] = \{\}$ ;  
 $\mathcal{I}[CHAOS] = ITRACE$  (can do anything but diverge)
- $\mathcal{F}[RUN] = \{(tr, X) : X = \{\} \vee \checkmark \in \sigma(tr)\}$ ;  $\mathcal{D}[RUN] = \{\}$ ;  
 $\mathcal{I}[RUN] = ITRACE$ ; similar for  $RUN_A$



- $\mathcal{F}[a \rightarrow P] = \{(\langle \rangle, X) : a \notin X\} \cup \{(\langle a \rangle \frown tr, X) : (tr, X) \in \mathcal{F}[P]\}$   
 $\mathcal{D}[a \rightarrow P] = \{(\langle a \rangle \frown tr : tr \in \mathcal{D}[P])\}$   
 $\mathcal{I}[a \rightarrow P] = \{(\langle a \rangle \frown tr : tr \in \mathcal{I}[P])\}$
- $\mathcal{F}[x : A \rightarrow P] = \{(\langle \rangle, X) : A \cap X = \{\}\} \cup$   
 $\{(\langle a \rangle \frown tr, X) : a \in A \wedge (tr, X) \in \mathcal{F}[P(a)]\}$   
 $\mathcal{D}[x : A \rightarrow P] = \{(\langle a \rangle \frown tr : a \in A \wedge tr \in \mathcal{D}[P(a)]\}$   
 $\mathcal{I}[x : A \rightarrow P] = \{(\langle a \rangle \frown tr : a \in A \wedge tr \in \mathcal{I}[P(a)]\}$
- $\mathcal{F}[P_1 \sqcap P_2] = \{(\langle \rangle, X) : (\langle \rangle, X) \in \mathcal{F}[P_1] \cap \mathcal{F}[P_2] \vee \langle \rangle \in \mathcal{D}[P_1 \sqcap P_2]\} \cup$   
 $\{(tr, X) : tr \neq \{\} \wedge (tr, X) \in \mathcal{F}[P_1] \cup \mathcal{F}[P_2]\}$   
 $\mathcal{D}[P_1 \sqcap P_2] = \mathcal{D}[P_1] \cup \mathcal{D}[P_2]$   
 $\mathcal{I}[P_1 \sqcap P_2] = \mathcal{I}[P_1] \cup \mathcal{I}[P_2]$ 
  - Idempotence, associativity, commutativity laws still hold,  $STOP$  is still a unit,  $DIV$  is a zero
- $\mathcal{F}[P_1 \sqcap P_2] = \mathcal{F}[P_1] \cup \mathcal{F}[P_2]$   
 $\mathcal{D}[P_1 \sqcap P_2] = \mathcal{D}[P_1] \cup \mathcal{D}[P_2]$   
 $\mathcal{I}[P_1 \sqcap P_2] = \mathcal{I}[P_1] \cup \mathcal{I}[P_2]$



- $\mathcal{F}[P \parallel_B Q] = \{(tr, X) : \exists X_P, X_Q \in 2^{\Sigma^\vee} :$   
 $X \cap (A \cup B)^\vee = (X_P \cap A^\vee) \cup (X_Q \cap B^\vee) \wedge$   
 $(tr \upharpoonright A^\vee, X_P) \in \mathcal{F}[P] \wedge (tr \upharpoonright B^\vee, X_Q) \in \mathcal{F}[Q] \wedge$   
 $\sigma(tr) \subseteq (A \cup B)^\vee\} \cup$   
 $\{(tr, X) : tr \in \mathcal{D}[P \parallel_B Q]\}$
- $\mathcal{D}[P \parallel_B Q] = \{tr \frown tr' : \sigma(tr) \subseteq (A \cup B)^\vee \wedge tr' \in TRACE \wedge$   
 $(tr \upharpoonright A^\vee \in \mathcal{D}[P] \wedge (tr \upharpoonright B^\vee, \{\}) \in \mathcal{F}[Q] \vee$   
 $tr \upharpoonright B^\vee \in \mathcal{D}[Q] \wedge (tr \upharpoonright A^\vee, \{\}) \in \mathcal{F}[P])\}$
- $\mathcal{I}[P \parallel_B Q] = \{u : \sigma(u) \subseteq A \cup B \wedge$   
 $u \downarrow A = |\mathbb{N}| \implies u \upharpoonright A \in \mathcal{I}[P] \wedge$   
 $u \downarrow A \in \mathbb{N} \implies (u \upharpoonright A, \{\}) \in \mathcal{F}[P] \wedge$   
 $u \downarrow B = |\mathbb{N}| \implies u \upharpoonright B \in \mathcal{I}[Q] \wedge$   
 $u \downarrow B \in \mathbb{N} \implies (u \upharpoonright B, \{\}) \in \mathcal{F}[Q]\}$   
 $\{tr \frown u : tr \in \mathcal{D}[P \parallel_B Q]\}$
- All the previous laws except  $\parallel$ -idempotence continue to be valid



- $\mathcal{F}[P \parallel\parallel Q] = \{(tr, X_P \cup X_Q) : \exists tr_P, tr_Q : tr \text{ interleaves } tr_P, tr_Q \wedge$   
 $X_P \upharpoonright \Sigma = X_Q \upharpoonright \Sigma \wedge (tr_P, X_P) \in \mathcal{F}[P] \wedge (tr_Q, X_Q) \in \mathcal{F}[Q]\} \cup$   
 $\{(tr, X) : tr \in \mathcal{D}[P \parallel\parallel Q]\}$
- $\mathcal{D}[P \parallel\parallel Q] = \{tr \frown tr' : \exists tr_P, tr_Q : tr \text{ interleaves } tr_P, tr_Q \wedge$   
 $(tr_P \in \mathcal{D}[P] \wedge (tr_Q, \{\}) \in \mathcal{F}[Q] \vee$   
 $tr_Q \in \mathcal{D}[Q] \wedge (tr_P, \{\}) \in \mathcal{F}[P])\}$
- $\mathcal{I}[P \parallel\parallel Q] =$   
 $\{u : \exists u_P, u_Q : u \text{ interleaves } u_P, u_Q \wedge u_P \in \mathcal{I}[P] \wedge u_Q \in \mathcal{I}[Q] \vee$   
 $\exists u_P, tr_Q : u \text{ interleaves } u_P, tr_Q \wedge u_P \in \mathcal{I}[P] \wedge (tr_Q, \{\}) \in \mathcal{F}[Q] \vee$   
 $\exists tr_P, u_Q : u \text{ interleaves } tr_P, u_Q \wedge (tr_P, \{\}) \in \mathcal{F}[P] \wedge u_Q \in \mathcal{I}[Q]\} \cup$   
 $\{tr \frown u : tr \in \mathcal{D}[P \parallel\parallel Q]\}$
- All the original laws continue to hold except that  $DIV$  is a zero



- $\mathcal{F}[P \setminus A] = \{(tr \setminus A, X) : (tr, X \cup A) \in \mathcal{F}[P]\} \cup \{(tr, X) : tr \in \mathcal{D}[P \setminus A]\}$   
 $\mathcal{D}[P \setminus A] = \{(tr \setminus A) \hat{\sim} tr' : tr \in \mathcal{D}[P]\} \cup \{(u \setminus A) \hat{\sim} tr' : u \in \mathcal{I}[P] \wedge \#(u \setminus A) \in \mathbb{N}\}$   
 $\mathcal{I}[P \setminus A] = \{u \setminus A : u \in \mathcal{I}[P] \wedge \#(u \setminus A) = |\mathbb{N}|\}$
- $\mathcal{F}[f(P)] = \{(f(tr), X) : (tr, f^{-1}(X)) \in \mathcal{F}[P]\} \cup \{(tr, X) : tr \in \mathcal{D}[f(P)]\}$   
 $\mathcal{D}[f(P)] = \{f(tr) \hat{\sim} tr' : tr \in \mathcal{D}[P]\}$   
 $\mathcal{I}[f(P)] = \{f(u) : u \in \mathcal{I}[P]\} \cup \{tr \hat{\sim} u : tr \in \mathcal{D}[f(P)]\}$
- $\mathcal{F}[f^{-1}(P)] = \{(tr, X) : (f(tr), f(X)) \in \mathcal{F}[P]\} \cup \{(tr, X) : tr \in \mathcal{D}[f^{-1}(P)]\}$   
 $\mathcal{D}[f^{-1}(P)] = \{tr : f(tr) \in \mathcal{D}[P]\}$   
 $\mathcal{I}[f^{-1}(P)] = \{u : f(u) \in \mathcal{I}[P]\}$



- $\mathcal{F}[P; Q] = \{(tr, X) : (tr, X \cup \{\checkmark\}) \in \mathcal{F}[P]\} \cup$   
 $\{(tr_1 \hat{\sim} tr_2, X) : (tr_1 \hat{\sim} \langle \checkmark \rangle, \{\}) \in \mathcal{F}[P] \wedge (tr_2, X) \in \mathcal{F}[Q]\} \cup$   
 $\{(tr, X) : tr \in \mathcal{D}[P; Q]\}$   
 $\mathcal{D}[P; Q] = \mathcal{D}[P] \cup \{tr \hat{\sim} tr' : (tr \hat{\sim} \langle \checkmark \rangle, \{\}) \in \mathcal{F}[P] \wedge tr' \in \mathcal{D}[Q]\}$   
 $\mathcal{I}[P; Q] = \mathcal{I}[P] \cup \{tr \hat{\sim} u : (tr \hat{\sim} \langle \checkmark \rangle, \{\}) \in \mathcal{F}[P] \wedge u \in \mathcal{I}[Q]\}$
- $\mathcal{F}[P \triangle Q] = \{(tr, X) : (tr, X) \in \mathcal{F}[P] \wedge$   
 $(\checkmark \in \sigma(tr) \vee (\langle \rangle, X) \in \mathcal{F}[Q])\} \cup$   
 $\{(tr_1 \hat{\sim} tr_2, X) : (tr_1, \{\}) \in \mathcal{F}[P] \wedge \checkmark \notin \sigma(tr_1) \wedge$   
 $(tr_2, X) \in \mathcal{F}[Q] \wedge tr_2 \neq \langle \rangle\} \cup$   
 $\{(tr, X) : tr \in \mathcal{D}[P \triangle Q]\}$   
 $\mathcal{D}[P \triangle Q] = \mathcal{D}[P] \cup \{tr_1 \hat{\sim} tr_2 : (tr_1, \{\}) \in \mathcal{F}[P] \wedge \checkmark \notin \sigma(tr_1) \wedge tr_2 \in \mathcal{D}[Q]\}$   
 $\mathcal{I}[P \triangle Q] = \mathcal{I}[P] \cup \{tr_1 \hat{\sim} tr_2 : (tr_1, \{\}) \in \mathcal{F}[P] \wedge \checkmark \notin \sigma(tr_1) \wedge tr_2 \in \mathcal{I}[Q]\}$
- The laws of sequential composition and interrupt from the stable failure model continue to hold



- Recursion needs same operational semantics as for stable failures namely, it unwinds through an internal action
- We can base the recursion semantics on a the refinement relation  $(F_1, D_1, I_1) \sqsubseteq_{FDI} (F_2, D_2, I_2)$  iff  $F_2 \subseteq F_1 \wedge D_2 \subseteq D_1 \wedge I_2 \subseteq I_1$ 
  - Refinement reduces nondeterminism ( $P \sqsubseteq_{FDI} Q$  iff  $P =_{FDI} P \sqcap Q$ )
  - It follows that the minimal process is *DIV* and the maximal process is a deterministic process (cannot be further refined)
- Each recursive equation has at least one (minimal) solution, refined by all the other solutions
  - In the FDI model approximations start from the most behaviours and start excluding behaviours as the recursion is unfolded:
- In the absence of infinite nondeterminism (infinite internal choice) the sequence of approximations  $F^n(DIV)$  will give the fixed point:

$$DIV \sqsubseteq_{FDI} N \quad F^n(DIV) \sqsubseteq_{FDI} N \implies F^{n+1}(DIV) \sqsubseteq_{DIV} N$$

$$\left( \bigcap_{n \in \mathbb{N}} \mathcal{F}[F^n(DIV)] \right), \left( \bigcap_{n \in \mathbb{N}} \mathcal{D}[F^n(DIV)] \right), \left( \bigcap_{n \in \mathbb{N}} \mathcal{I}[F^n(DIV)] \right)$$

- Unique fixed point: For any  $P_1, P_2$  finitely nondeterministic and any guarded  $F$ :  $F(P_1) =_{FDI} P_1 \wedge F(P_2) =_{FDI} P_2 \implies P_1 =_{FDI} P_2$



- A specification will consist of three parts:
 
$$P \text{ sat } (S_F(tr, X), S_D(tr), S_I(u)) \text{ iff } \forall (tr, X) \in \mathcal{F}[P] : S_F(tr, X) \wedge$$

$$\forall tr \in \mathcal{D}[P] : S_D(tr) \wedge$$

$$\forall u \in \mathcal{I}[P] : S_I(u)$$
- Most interesting specification in the FDI model:
 
$$\text{divergence-free} = (\text{true}(tr, X), \text{false}(tr), \text{true}(u))$$
  - Relationship with stable failures:  $\mathcal{SF}[P] = \mathcal{F}[P]$  for any divergence-free process  $P$
  - Relationship with traces: for any divergence-free  $P$  and with  $S_F(tr, X)$  the equivalent of  $S_T(tr)$  in the stable failure model,  $P \text{ sat } S_T(tr) \implies P \text{ sat } (S_F(tr, X), \text{false}(tr), \text{true}(u))$
- Specifications on infinite traces normally specify progress requirements or fairness constraints
  - Other than this properties on infinite traces can typically be stated in terms of the finite prefixes of those infinite traces
  - Such a specification  $(S_F(tr, X), S_D(tr), \text{true}(u))$  is called an **admissible specification**



- Can set up a proof system as before
- However, in practice FDI verification is only concerned with divergence freedom
  - Once this is established we can just use the stable failure model
- The only operators that can introduce divergence are *DIV*, hiding, and recursion
- *DIV* is divergent by definition and should not be used
- *Hiding* must be prevented from hiding any set of events that occur infinitely often in a trace
  - In order to avoid this we establish a bound for the length of the resulting trace:

$$\frac{P \text{ sat divergence-free} \quad P \text{ sat } \#tr \leq \beta(tr \setminus A)}{p \setminus A \text{ sat divergence-free}}$$

- The actual bounding function does not matter, all it matters is that it exists
- *Recursion* does not introduce divergence if the recursive definition is guarded:

$$\frac{\forall Y : Y \text{ sat divergence-free} \implies F(Y) \text{ sat divergence-free}}{N \text{ sat divergence-free}} \quad \left[ \begin{array}{l} N = F(N) \\ F \text{ guarded} \end{array} \right]$$



- The refinement relation  $\sqsubseteq_{FDI}$  already defined
  - $SPEC \sqsubseteq_{FDI} IMP$  means that all the possible behaviours of *IMP* are allowed by *SPEC*
  - Specification for divergence freedom: *CHAOS* (permits any non-divergent behaviour but does not allow divergence)
- **Must testing** requires that all the maximal runs are successful
  - Maximal runs cannot be extended (because they have reached a deadlock or they are infinite)
  - $P \text{ must } T$  iff **all** the traces of the maximal runs of  $(P \parallel_{\Sigma} T) \setminus \Sigma$  contain  $\omega$
  - $P_1 \sqsubseteq_{\text{must}} P_2$  iff  $\forall T : P_1 \text{ must } T \implies P_2 \text{ must } T$
  - $P_1 \equiv_{\text{must}} P_2$  iff  $P_1 \sqsubseteq_{\text{must}} P_2 \wedge P_2 \sqsubseteq_{\text{must}} P_1$
  - $P_1 \sqsubseteq_{\text{must}} P_2$  iff  $P_1 \sqsubseteq_{FDI} P_2$
  - Note that must testing regards divergence as catastrophic: if a divergent behaviour is possible then that behaviour causes all tests to fail