Liveness:

<u>Assumption</u>: • The temporal correctness specification is given by

  • a liveness property Ψ and
  • a fairness property Φ.

• Both are encoded by a Büchi automaton $A_{\Phi,\Psi}$ whose language consists of exactly the infinite Φ-fair sequences of program states that do <u>not</u> satisfy Ψ.

<u>Definition</u>:

The set of program states W forms the alphabet.

A <u>Büchi automaton</u> (over W) is a tuple

$$(Q, Q_0, \Delta, F)$$

with

Q = a possibly infinite set of states,

$Q_0 \subseteq Q$ = the starting states,

$\Delta \subseteq Q \times W \times Q$ = the transition relation,

$F \subseteq Q$ = the final states.

A <u>run</u> of $A_{\Phi,\Psi}$ on the word $s_1 s_2 \ldots$ is a sequence of automaton states $q_1, q_2, \ldots$ so that $q_1 \in Q_0$ and (q_i, s_i, q_{i+1}) for all i.

It is <u>accepting</u>, if $q_i \in F$ for infinitely many i.

Program P satisfies the liveness property φ
under the fairness assumption Φ,

if all computations of P are rejected by $A_{\Phi,\varphi}$.

We export the program computations to the automaton
by a parallel composition.

<u>Definition</u>:
Let $P = (W, I, R)$ and $A_{\Phi,\varphi} = (Q, Q_0, \Delta, F)$.

Then

$$P_{\Phi,\varphi} = (\underbrace{W_Q}_{= W \times Q}, I \times Q_0, \Delta_\times, \underbrace{W_F}_{= W \times F})$$

with

$$((s,q),(s',q')) \in \Delta_\times, \text{ if } (s,s') \in R \text{ and } (q,s,q') \in \Delta.$$

A computation $(s_1\, q_1)(s_2\, q_2) \dots$ of $P_{\Phi,\varphi}$ is <u>fair</u>,
if $(s_i, q_i) \in W_F$ for infinitely many i.

Program P is <u>correct</u> w.r.t. φ under fairness condition Φ,
if all infinite computations of $P_{\Phi,\varphi}$ are not fair.

We also say $P_{\Phi,\varphi}$ is fair <u>terminating</u>.

<u>Theorem (Liveness)</u>:
Program P satisfies the liveness property φ
under the fairness condition Φ

iff there is a transition invariant T for $P_{\Phi,\varphi}$
so that $T \cap (W_F \times W_F)$ is disjunctively well-founded.

Proof:

"⇐" Consider

$$T = T_1 \cup \ldots \cup T_n$$

so that $T_i \cap (W_F \times W_F)$ is well-founded for all i

and this is a transition invariant for $P_{\Phi,\Psi}$.

Assume $P_{\Phi,\Psi}$ has an infinite fair computation.

$$\sigma = s_1 s_2 \ldots$$

Let

$$\pi = s^1 s^2 \ldots$$

be the subsequence of states in W_F.

Now very similar to the proof of the termination theorem,

there is an infinite subsequence of π

and a relation T_i

so that every pair of elements in the subsequence

belongs to T_i, and hence

$$T_i \cap (W_F \times W_F).$$

$\lightning$ to the fact that $T_i \cap (W_F \times W_F)$ is well-founded.

"⇒" Assume $P_{\Phi,\Psi}$ is fair terminating.

Let

$$T_1 = R^+ \cap ((Acc \cap W_F) \times Acc)$$

$$T_2 = R^+ \cap ((Acc \setminus W_F) \times Acc)$$

Then

$$T = T_1 \cup T_2 \quad \text{is a transition invariant.}$$

 We prove well-foundedness of the relations.

Assume $\sigma = s^1 s^2 \ldots$ is an infinite sequence of states so that $(s^i, s^{i+1}) \in T_1$ for all i.

Since s^1 is accessible and, for all i, there is a computation segment leading from s^i to s^{i+1}, there is an infinite fair computation

$$s_1 \ldots s^1 \ldots s^2 \ldots$$

This contradicts the assumption that $P_{\Phi,\psi}$ is fair terminating. Hence, T_1 has to be well-founded.

Clearly, $T_2 \cap (W_F \times W_F) = \emptyset$. $\square$

Example:

The liveness property ψ is termination, for all examples.

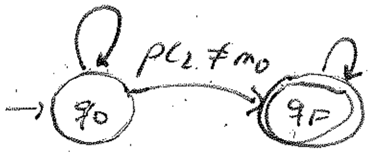
ANY-DOWN:

$x = 1,\ y = 0$

```
l0 : while x = 1 do          ||   m0 : x := 0
       l1 : y = y+1;          ||   m1
l2 : while y > 0 do           ||
       l3 : y = y-1;          ||
```

Fairness assumption: eventually Thread 2 leaves m_0, $F(pc_2 \neq m_0)$

$A_{\Phi,\psi}$:



The union of the following relations is a transition invariant:

// Loops in Büchi accepting state and l_2

// Different states at Büchi automaton or program

state of the automaton

T_1 $pc_Q = q_F \wedge y > 0 \wedge y' < y$

T_2 $pc_Q \neq q_F$ // Loop at l_0

T_3 $pc_Q = q_0 \wedge pc_Q' = q_F$

T_4 $pc_2 = m_0 \wedge pc_2' = m_1$

T_{ij} $pc_1 = l_i \wedge pc_1' = l_j$, $i \neq j \in \{0, \ldots, 3\}$.

CONC-WHILES:

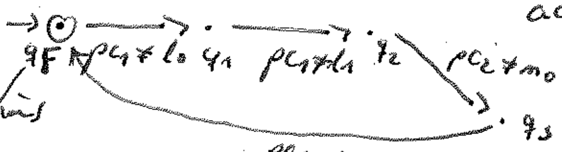
$x>0,\ y>0$

l_0: **while** $x>0$ **do**	m_0: **while** $y>0$ **do**
$\quad l_1$: $y = x-1$	$\quad m_1$: $x = y-1$;
l_2 $y=0$	m_2: $x=0$.

Fairness: No process can wait forever: always eventually

$$GF(pc_1 \neq l_0) \wedge GF(pc_1 \neq l_1)$$
$$\wedge\ GF(pc_2 \neq m_0) \wedge GF(pc_2 \neq m_1)$$

The Büchi automaton has states $\{q_0, q_1, q_2, q_F\}$. accepting.



The union of the following relations is a transition invariant for $P_{\bar{q},\varphi}$:

T_1: $pc_Q = q_F \wedge x>0 \wedge x'<x$ // Both threads move, loop in Büchi accepting state.

T_2: $pc_Q = q_F \wedge y>0 \wedge y'<y$

T_3: $pc_Q \neq q_F$ // One thread does not cycle.

$T_{4,i,j}$: $pc_Q = q_i \wedge pc_Q' = q_j$, $i \neq j \in \{0,1,2\}$

$T_{5,i,j}$: $pc_1 = l_i \wedge pc_1' = l_j$, $i \neq j \in \{0,1,2\}$

$T_{6,i,j}$: $pc_2 = m_i \wedge pc_2' = m_j$, $i \neq j \in \{0,1,2\}$. // No loops, in either the Büchi automaton or one of the threads.

Inductiveness:

Definition: Let $P=(W,I,R)$.
A relation $T \subseteq W \times W$ is *inductive*, if

$$R \cup T \circ R \subseteq T.$$

Remark:

$R \cup R \circ T \subseteq T$ yields an equivalent notion.

$R \cap (Acc \times Acc) \cup T \circ R \cap (Acc \times Acc) \subseteq T$

is weaker.

Remark:

- The inductive relation for program P $\boxed{\text{is a transition invariant for } P}$, called an inductive transition invariant.
- Even inductive transition invariants are not closed under composition with themselves:

$$T \circ T \not\subseteq T.$$

Corollary:

A finite union $T = T_1 \cup \ldots \cup T_n$ of well-founded relations is well-founded, if it is closed under composition with itself, $T \circ T \subseteq T$.

Proof:

By the remark, T is a transition invariant for itself.

Since T is disjunctively well-founded,

it is well-founded by the termination theorem. □

The remark combined with the liveness theorem give us a proof rule for liveness.

Proof rule:

Program P
Liveness property ψ and fairness condition Φ given by $A_{\Phi,\psi}$
Parallel composition $P_{\Phi,\psi} = (W_Q, R, W_F)$
Relation $T \subseteq W_Q \times W_Q$

$$\begin{array}{ll} P1: & R \subseteq T \\ P2: & T \circ R \subseteq T \\ P3: & T \cap (W_F \times W_F) \text{ disjunctively well-founded} \\ \hline & P \text{ satisfies } \psi \text{ under } \Phi. \end{array}$$

// Inductiveness.

Remark:

- There is a similar rule for termination,
  simply use · as R the transition relation of the program
  and · replace $T \cap (W_F \times W_F)$ by T.

- We split the reasoning into inductiveness and
  disjunctive well-foundedness.

  One could make this explicit by requiring $T' \subseteq T$
  and asking P1 and P2 for T'.
  Then P3 will carry over to T'
  by downward closure of disjunctive well-foundedness.

Validating the Premises of the Proof Rule:

- The transition relation of the program
  can be seen as a finite union

$$R = R_1 \cup \ldots \cup R_m,$$

where each R_i models the transition relation
at some program point (over unprimed and primed variables).

If $T = T_1 \cup \ldots \cup T_n$, then

$$T \circ R = \bigcup_{\substack{i \in [1,n] \\ j \in [1,m]}} T_i \circ R_j$$

This means P1 and P2 are just entailment checks between assertions.

- For P3, one can use traditional methods to prove well-foundedness.
  In particular, a relation

  $g(\bar{x}) \wedge e(\bar{x}, \bar{x}')$ is well-founded

  iff

  <u>while</u> $g(\bar{x})$ <u>do</u>
  $e(\bar{x}, \bar{x}')$
  <u>od</u>
  terminates.

<u>Inductive Transition Invariants for the Examples:</u>

The transition invariants we have seen so far are not inductive.
We prove they are transition invariants by identifying a subrelation that is inductive.

<u>LOOPS:</u>

```
l0 : while x >= 0 do
     l1 : y = 1;
     l2 : while y < x do
          l3 : y = 2y
     l4 : x = x - 1
```

This is an inductive transition invariant

$pc = l_0 \wedge x \geq 0 \wedge x' \leq x \wedge pc' = l_2$

$pc = l_2 \wedge x' < x \wedge pc' = l_0$

$pc = l_2 \wedge x - y > 0 \wedge x' \leq x \wedge y' > y \wedge pc' = l_2$

$pc = l_0 \wedge x \geq 0 \wedge x' < x \wedge pc' = l_0$

$pc = l_2 \wedge x \geq 0 \wedge x' < x \wedge pc' = l_2$

Inductiveness is easy to check,
as an example consider the transition from l_2 to l_0:

$$pc = l_2 \wedge \underbrace{y \geq x}_{\text{leave loop}} \wedge x' = x - 1 \wedge y' = y \wedge pc' = l_0 .$$

Compose this transition with the first from the invariant:

$$pc = l_0 \wedge x \geq 0 \wedge x' \leq x - 1 \wedge pc' = l_0 .$$

This entails the fourth entry in our invariant.

<u>Theorem</u>

The proof rule for liveness is sound
and complete relative to first-order validity
and well-foundedness validity
of the relations that constitute
the transition invariant.

Proof:

Soundness: By the remark and the liveness theorem.

Relative completeness: We use the two relations
we have constructed in the proof
of the liveness theorem.
This is in fact an inductive transition invariant.

To establish completeness relative to assertion provability,
we need a first-order assertion
that expresses the two relations.
↳ This follows the relative completeness result for invariants,
needs Gödel's β-predicate, see Winskel's book.