Supplementary materials

Appendix A. Semantics of Hoare triples for gene networks

We define the semantics of a trace specification *via* a binary relation between states and *sets* of states. This relation characterises all the possible realisations of the trace specification. The general ideas that motivate our definition are the following:

- Starting from an initial state η, a trace specification without existential or universal quantifier is either realised by associating with η another state η', or is not realisable and η' does not exist. For example, the atomic expression $v+$ associates η' with η (where $\forall u \neq v, \eta'(u) = \eta(u)$ and $\eta'(v) = \eta(v) + 1$) if and only if the transition $\eta \to \eta'$ exists in the state space. If, on the contrary, this transition does not exist, the trace specification is not realisable.

- Existential quantifiers open a sort of space of possibilities for η': According to the chosen trace specification under each existential quantifier one may get different associated states. Consequently, one cannot define the semantics as a partial function that associates a unique η' with η; a binary relation is a more suited mathematical object (denoted $\rightsquigarrow$ in the sequel).

- A universal quantifier induces a sort of unity/solidarity between all the states η' that can be obtained through each trace specification under its scope. All these states have to satisfy the postcondition (Definition Appendix A.2) . For this reason, we define a binary relation that associates a *set of states* E with the initial state η: "$\eta \rightsquigarrow E$". Such a set E can be understood as grouping together the states it contains in preparation for checking the forthcoming post condition.

- When the trace specification p contains both existential and universal quantifiers, we may consequently get several sets $E_1, \cdots, E_n$ such that $\eta \overset{p}{\rightsquigarrow} E_i$, each of the E_i being a *possibility* through the existential quantifiers of p and all the states belonging to a given E_i being together through the universal quantifiers of p. On the contrary, if p is not realisable, then there is no set E such that $\eta \overset{p}{\rightsquigarrow} E$ (not even the empty set).

Definition Appendix A.1. (Mathematical semantics of a trace specification). *Let $N = (V, M, E_V, E_M, \mathcal{K})$ be a* GRN*, let $\mathcal{S}$ be the state graph of N whose set of vertices is denoted S and let p be a trace specification for N. The binary relation $\overset{p}{\rightsquigarrow}$ is the smallest subset of $S \times \mathcal{P}(S)$ such that, for any state η:*

1. *If p is the atomic expression $v+$, then let us consider the state $\eta' = \eta[v \leftarrow (\eta(v)+1)]$: If $\eta \to \eta'$ is a transition of $\mathcal{S}$ then $\eta \overset{p}{\rightsquigarrow} \{\eta'\}$.*
2. *If p is the atomic expression $v-$, then let us consider the state $\eta' = \eta[v \leftarrow (\eta(v)-1)]$: If $\eta \to \eta'$ is a transition of $\mathcal{S}$ then $\eta \overset{p}{\rightsquigarrow} \{\eta'\}$.*
3. *If p is the atomic expression $v := i$, then $\eta \overset{p}{\rightsquigarrow} \{\eta[v \leftarrow i]\}$.*
4. *If p is of the form $assert(e)$, if $\eta \models_N e$, then $\eta \overset{p}{\rightsquigarrow} \{\eta\}$.*
5. *If p is of the form $\forall(p_1, p_2)$: If $\eta \overset{p_1}{\rightsquigarrow} E_1$ and $\eta \overset{p_2}{\rightsquigarrow} E_2$ then $\eta \overset{p}{\rightsquigarrow} (E_1 \cup E_2)$.*
6. *If p is of the form $\exists(p_1, p_2)$: If $\eta \overset{p_1}{\rightsquigarrow} E_1$ then $\eta \overset{p}{\rightsquigarrow} E_1$,* and *if $\eta \overset{p_2}{\rightsquigarrow} E_2$ then $\eta \overset{p}{\rightsquigarrow} E_2$.*
7. *If p is of the form $(p_1; p_2)$: If $\eta \overset{p_1}{\rightsquigarrow} F$ and if $\{E_e\}_{e \in F}$ is a F-indexed family of state sets such that $e \overset{p_2}{\rightsquigarrow} E_e$, then $\eta \overset{p}{\rightsquigarrow} (\bigcup_{e \in F} E_e)$.*
8. *If p is of the form $(while\ e\ with\ I\ do\ p_0)$:*
   - *If $\eta \not\models_N e$ then $\eta \overset{p}{\rightsquigarrow} \{\eta\}$.*
   - *If $\eta \models_N e$ and $\eta \overset{p_0;p}{\rightsquigarrow} E$ then $\eta \overset{p}{\rightsquigarrow} E$.*

This definition calls for several comments.

The relation $\overset{p}{\rightsquigarrow}$ exists because (i) the set of all relations that satisfy the properties 1–8 of the definition is not empty (the relation which links all states to all sets of states satisfies the properties) and (ii) the intersection of all the relations that satisfy the properties 1–8, also satisfies the properties.

A simple atomic expression such as $v+$ may be not realisable in a state η (if $\eta \to \eta'$ is not a transition of $\mathcal{S}$). In this case, there is no set E such that $\eta \overset{v+}{\rightsquigarrow} E$. The same situation happens when the trace specification is an assertion that is not satisfied at the current state η.

Universal quantifiers propagate non-realisable trace specifications: If one of the p_i is not realisable then $\forall(p_1, \cdots, p_n)$ is not realisable. *It is not the case for existential quantifiers*: If $\eta \overset{p_i}{\rightsquigarrow} E_i$ for one of the p_i then $\eta \overset{\exists(p_1 \cdots p_n)}{\rightsquigarrow} E_i$ even if one of the p_j is not realisable.

When a *while* loop does not terminate, there is no set E such that $\eta \overset{while\ldots}{\rightsquigarrow} E$. This is due to the minimality of the binary relation $\overset{p}{\rightsquigarrow}$. On

the contrary, when the *while* loop terminates, it is equivalent to a trace specification containing a finite number of occurrences of the sub-trace p_0 in sequence, starting from η.

The semantics of sequential composition may seem unclear for readers not familiar with commutations of quantifiers. We give an example to explain the construction of $\overset{p_1;p_2}{\rightsquigarrow}$ (see Figure A.5):

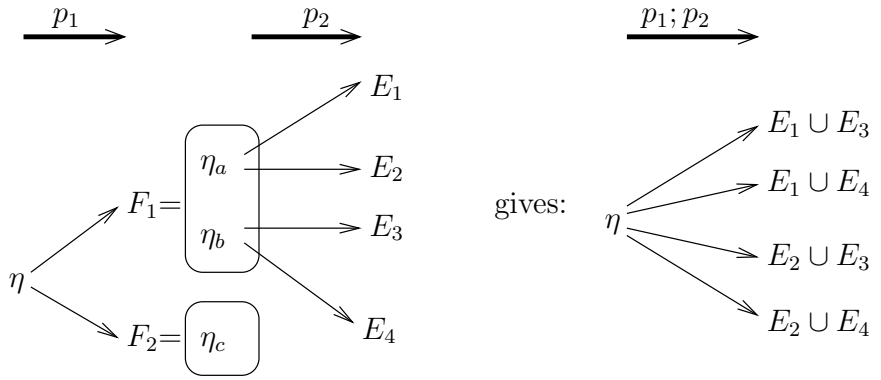

Figure A.5: An example for the semantics of sequential composition

- Let us assume that starting from state η, two sets of states are possible *via* p_1: $\eta \overset{p_1}{\rightsquigarrow} F_1 = \{\eta_a, \eta_b\}$ and $\eta \overset{p_1}{\rightsquigarrow} F_2 = \{\eta_c\}$. It intuitively means that p_1 permits a choice between F_1 and F_2 through some existential quantifier and that the trace specification leading to F_1 contains a universal quantifier grouping together η_a and η_b.
- Let us also assume that
  - starting from the state η_a, two sets of states are possible *via* p_2: $\eta_a \overset{p_2}{\rightsquigarrow} E_1$ and $\eta_a \overset{p_2}{\rightsquigarrow} E_2$,
  - starting from the state η_b, two sets of states are possible *via* p_2: $\eta_b \overset{p_2}{\rightsquigarrow} E_3$ and $\eta_b \overset{p_2}{\rightsquigarrow} E_4$,
  - and there are no set E such that $\eta_c \overset{p_2}{\rightsquigarrow} E$.

When focusing on the traces of $(p_1; p_2)$ that encounter F_1 after p_1, the traces such that p_1 leads to η_a must be grouped together with the ones that lead to η_b. Nevertheless, for each of them, p_2 permits a choice of possibilities:

between E_1 or E_2 for η_a and between E_3 or E_4 for η_b. Consequently, when grouping together the possible futures of η_a and η_b, one needs to consider the four possible combinations: $\eta \overset{p_1;p_2}{\rightsquigarrow} (E_1 \cup E_3)$, $\eta \overset{p_1;p_2}{\rightsquigarrow} (E_1 \cup E_4)$ $\eta \overset{p_1;p_2}{\rightsquigarrow} (E_2 \cup E_3)$ and $\eta \overset{p_1;p_2}{\rightsquigarrow} (E_2 \cup E_4)$.
Lastly, when focusing on the traces of $(p_1; p_2)$ that encounter F_2 after p_1, since η_c has no future *via* p_2, there is no family indexed by F_2 as mentioned in the definition and consequently it adds no relation into $\overset{p_1;p_2}{\rightsquigarrow}$.

Let us remark that, if $\eta \overset{p}{\rightsquigarrow} E$ then E cannot be empty; it always contains at least one state. The proof is easy by structural induction of the trace specification p (using the fact that a *while* loop which terminates is equivalent to a trace specification containing a finite number of occurrences of the sub-trace p_0).

Definition Appendix A.2. (Semantics of a Hoare triple). *Given a* GRN $N = (V, M, E_V, E_M, \mathcal{K})$*, let* $\mathcal{S}$ *be the state graph of* N *whose set of vertices is denoted* S*. A Hoare triple* $\{P\}\ p\ \{Q\}$ *is satisfied if and only if:*

For all $\eta \in S$ *satisfying* P*, there exists* E *such that* $\eta \overset{p}{\rightsquigarrow} E$ *and for all* $\eta' \in E$*,* η' *satisfies* Q*.*

The previous definition implies the consistency of the trace specification p with the state graph: If the specification p is not realisable starting from one of the states satisfying pre-condition P, then the Hoare triple cannot be satisfied. For instance if some $v+$ is required by the trace specification p but the increasing of v is not possible according to the state graph, then the Hoare triple is not satisfied.
As an example, let us consider the GRN in Figure A.6 and its state graph.

1. The Hoare triple $\{(a = 0) \wedge (b = 0)\}\ a+; a+; b+\ \{(a = 2) \wedge (b = 1)\}$ is satisfied, because
   - for all states that do not satisfy the pre-condition, the Hoare triple is satisfied by definition,
   - there is, in this example, a unique state satisfying the precondition $(a = 0) \wedge (b = 0)$ and from *this* state, the trace specification $a+; a+; b+$ is possible and leads to the state $(2, 1)$ and
   - the state $(2, 1)$ satisfies the postcondition $(a = 2) \wedge (b = 1)$.
2. The Hoare triple $\{(a = 2) \wedge (b = 0)\}\ b+; a-; a-\ \{(a = 0) \wedge (b = 1)\}$ is not satisfied because from the state satisfying the precondition, the first

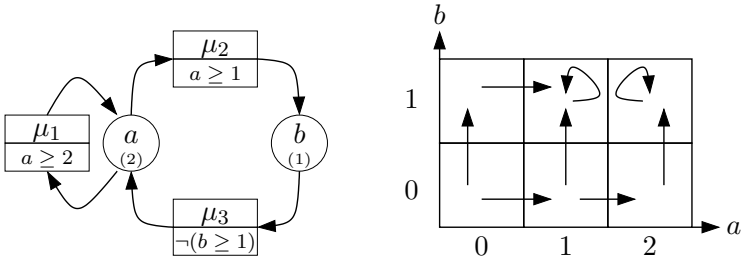

Figure A.6: **(Left)** The graphical representation of the GRN $N = (V, M, E_V, E_M, \mathcal{K})$ with $V = \{a, b\}$, the bounds of a and b are respectively 2 and 1, $M = \{\mu_1, \mu_2, \mu_3\}$, φ_{μ_1} is $(a \geqslant 2)$, φ_{μ_2} is $(a \geqslant 1)$, φ_{μ_3} is $\neg(b \geqslant 1)$. Finally the family of integers is $\{K_a = 1, K_{a,\mu_1} = 2, K_{a,\mu_3} = 2, K_{a,\mu_1\mu_3} = 2, K_b = 1, K_{b,\mu_2} = 1\}$. **(Right)** Representation of its state graph.

expression $b+$ is realisable and necessarily leads to the state $(2, 1)$ from which the next expression $a-$ is not consistent with the state graph.

3. The following Hoare triple contains two existential quantifiers and a universal one:
$\{(a = 0) \wedge (b = 0)\}\ \forall(a+, b+); \exists(a+, b+); \exists(\varepsilon, b+)\ \{(b = 1)\}$ (remember that ε denotes the empty trace and is an abbreviation for $assert(\top)$ where $\top$ stands for a tautology).

   - We have clearly $(0,0) \overset{\forall(a+,b+)}{\rightsquigarrow} \{(1,0),(0,1)\}$
   - Since we have $(1,0) \overset{\exists(a+,b+)}{\rightsquigarrow} \{(2,0)\}$ and $(1,0) \overset{\exists(a+,b+)}{\rightsquigarrow} \{(1,1)\}$ and $(0,1) \overset{\exists(a+,b+)}{\rightsquigarrow} \{(1,1)\}$, we deduce $(0,0) \overset{\forall(a+,b+);\exists(a+,b+)}{\rightsquigarrow} \{(1,1),(2,0)\}$ and $(0,0) \overset{\forall(a+,b+);\exists(a+,b+)}{\rightsquigarrow} \{(1,1)\}$.
   - We have trivially $(1,1) \overset{\exists(\varepsilon,b+)}{\rightsquigarrow} \{(1,1)\}$
   - Moreover we have both $(2,0) \overset{\exists(\varepsilon,b+)}{\rightsquigarrow} \{(2,0)\}$ and $(2,0) \overset{\exists(\varepsilon,b+)}{\rightsquigarrow} \{(2,1)\}$
   - We deduce that the considered trace specification p can lead to 3 different sets of states: $(0,0) \overset{p}{\rightsquigarrow} \{(1,1),(2,0)\}$, $(0,0) \overset{p}{\rightsquigarrow} \{(1,1)\}$ and $(0,0) \overset{p}{\rightsquigarrow} \{(1,1),(2,1)\}$.

   Because the postcondition is satisfied in both states $(1, 1)$ and $(2, 1)$, the two last sets of states which are in relation with $(0, 0)$, satisfy the postcondition. Consequently although the first set does not, one can deduce that the Hoare triple is satisfied.

Appendix B. Soundness and Completeness

As usual in Hoare logic, The soundness and completeness of the logic can only ensure a *partial* correctness of the Hoare triples because the *while* loops of the trace specifications do not necessarily terminate.

Appendix B.1. Soundness

The soundness of our modified Hoare logic means that: Given a network $N = (V, M, E_V, E_M, \mathcal{K})$, if $\vdash \{P\}\ p\ \{Q\}$ according to the inference rules of Section 5 (and after substituting the symbols $K_{...}$ by their value in N), then for all states η that satisfies P, if there is a set E such that $\eta \overset{p}{\rightsquigarrow} E$, then there is at least a set E' such that $\eta \overset{p}{\rightsquigarrow} E'$ and $\forall \eta' \in E', \eta' \models_N Q$.

The proof is made as usual by induction on the proof tree of $\vdash \{P\}\ p\ \{Q\}$. Hence, we have to prove that each rule of Section 5 is sound. Here we develop only the *Increase* rule and the *Sequential composition* rule since the soundness of the other inference rules is either similar (*Decrease* rule), trivial (*Assert* rule, *Quantifier rules*, *Assignment* rule, *Empty trace* rule and *Boundary axioms*) or standard in Hoare logic (*Iteration* rule). Let us note that the soundness of the *Sequential composition* rule is not trivial because its semantics is enriched to cope with the quantifiers.

Let η be any state of N.

Increase rule: $\dfrac{}{\{\ \Phi_v^+ \wedge Q[v{\leftarrow}v{+}1]\ \}\ v{+}\ \{Q\}}$ (where v is a variable of N)

From Definition Appendix A.2, the hypothesis is

$\boxed{H}\ \eta \models_N \Phi_v^+$ and $\eta \models_N Q[v \leftarrow v+1]$

and we have to prove the conclusion

$\boxed{C}$ there exists $E \subset S$ such that $\eta \overset{v+}{\rightsquigarrow} E$ and $\forall \eta' \in E,\ \eta' \models_N Q$

Let us choose $E = \{\eta'\}$ with $\eta' = \eta[v \leftarrow \eta(v) + 1]$. From Notation 5.1, the hypothesis $\eta \models_N \Phi_v^+$ is equivalent to $(\eta \rightarrow \eta') \in \mathcal{S}$, which in turn, according to Definition 4.4, implies $\eta \overset{v+}{\rightsquigarrow} \{\eta'\}$. Hence, it only remains to prove that $\eta' \models_N Q$, which results from the hypothesis $\eta \models_N Q[v \leftarrow v+1]$. □

Sequential composition rule: $\dfrac{\{P_1\}\ p_1\ \{P_2\} \qquad \{P_2\}\ p_2\ \{Q\}}{\{P_1\}\ p_1;p_2\ \{Q\}}$

From Definition Appendix A.2, we consider the following three hypotheses:

$\boxed{H_1}$ for all $\eta_1 \in S$ such that $\eta_1 \models_N P_1$ there exists E_1 such that $\eta_1 \overset{p_1}{\rightsquigarrow} E_1$ and $\forall \eta' \in E_1,\ \eta' \models_N P_2$

$\boxed{H_2}$ for all $\eta_2 \in S$ such that $\eta_2 \models_N P_2$ there exists E_2 such that $\eta_2 \overset{p_2}{\rightsquigarrow} E_2$ and $\forall \eta'' \in E_2,\ \eta'' \models_N Q$

$\boxed{H_3}$ $\eta \models_N P_1$

and we have to prove the conclusion:

$\boxed{C}$ there exists $E \subset S$ such that $\eta \overset{p_1;p_2}{\rightsquigarrow} E$ and $\forall \eta'' \in E,\ \eta'' \models_N Q$

Let us arbitrarily choose a set E_1 such that $\eta \overset{p_1}{\rightsquigarrow} E_1$ and $\forall \eta' \in E_1,\ \eta' \models_N P_2$ (we know that E_1 exists from $\boxed{H_1}$ and $\boxed{H_3}$).

For each $\eta' \in E_1$, we similarly choose a set $E_2^{\eta'}$ such that:
$\eta' \overset{p_2}{\rightsquigarrow} E_2^{\eta'}$ and $\forall \eta'' \in E_2^{\eta'},\ \eta'' \models_N Q$ (we know that the family $\{E_2^{\eta'}\}_{\eta' \in E_1}$ exists from $\boxed{H_2}$ and the fact that $\eta' \models_N P_2$ for all $\eta' \in E_1$)

Let $E = (\bigcup_{\eta' \in E_1} E_2^{\eta'})$, we have: $\eta \overset{p_1;p_2}{\rightsquigarrow} E$ from Definition 4.4 and $\forall \eta'' \in E,\ \eta'' \models_N Q$ (from the way the union is built). □

Appendix B.2. Completeness and weakest precondition

Completeness of Hoare logic is defined as follows. Given a network $N = (V, M, E_V, E_M, \mathcal{K})$, if the Hoare triple $\{P\}\ p\ \{Q\}$ is satisfied in N (according to Definition Appendix A.2) then $\vdash \{P\}\ p\ \{Q\}$ (using the inference rules of Section 5 and after substituting the symbols $K_{...}$ by their value in N). We prove the completeness by establishing that one can compute the weakest invariants of all *while* loops and that the backward strategy gives a proof of $\{P\}\ p\ \{Q\}$.

The main difference with respect to the classical completeness proof is that we navigate into a finite state space, so that we will not have to care about the incompleteness of arithmetic or restrictions about weakest loop invariants. In the following proposition, we see that one can compute the weakest invariant for each *while* occurrence in the trace specification. Only

practical reasons in order to facilitate proofs justify to ask the specifier to include loop invariants into trace specifications: Often, a slightly non minimal invariant considerably simplifies the proof tree.

Proposition Appendix B.1. (Existence of the weakest loop invariant). *Given a* GRN $N = (V, M, E_V, E_M, \mathcal{K})$*, let us consider two assertions* Q *and* e*, and a trace specification* p*. There exists a weakest loop invariant* I *such that the Hoare triple* $\{I\}$ *while* e *with* I *do* p $\{Q\}$ *is partially correct.*

The following proof is constructive and gives a way to compute I (see remark Appendix B.4).
Proof:

1. In the first step of the proof, we build a set $\mathcal{D}$ as a countable union.
   - Let $q_0 = \{\eta \in S \mid \eta \models_N Q \wedge \neg e\}$ be the set of all states that satisfy Q without entering the *while* loop.
   - given q_i, let $q_{i+1} = \{\eta \in S \mid \eta \models_N e$ and $\exists E \subset S, \eta \overset{p}{\rightsquigarrow} E$ and $E \subset q_i\}$. From Definition Appendix A.2, for each i, q_i is the set of states that induce exactly i *while* loops and such that the resulting states satisfy Q.
   - Let $\mathcal{D}_n = \bigcup_{i=0}^{n} q_i$. The sequence of $\mathcal{D}_n$ is increasing and because S is finite, it is stationary. So $\mathcal{D} = \bigcup_{i=0}^{\infty} q_i$ exists and can be inductively computed.
2. In the second step of the proof, we show that the characteristic formula of $\mathcal{D}$ is a loop invariant.
   - Because $\mathcal{D}$ is finite, there is a formula I such that $\eta \models_N I$ iff $\eta \in \mathcal{D}$: $I \equiv \bigvee_{\eta \in \mathcal{D}} \mathbb{1}_\eta$ where $\mathbb{1}_\eta \equiv \bigwedge_{v \in V} v = \eta(v)$
   - I is a loop invariant because for each state η that satisfies I, there is an integer i such that $\eta \in q_i$.
     - If $i > 0$, then η satisfies $I \wedge e$ and by definition, there is a set E such that $\eta \overset{p}{\rightsquigarrow} E$ and $E \subset q_{i-1}$, consequently E satisfies I because every state of q_{i-1} satisfies I.
     - If $i = 0$, then $\eta \models_N \neg e$, thus $\eta \not\models_N e \wedge I$, which implies that $\{e \wedge I\}$ p $\{I\}$ is satisfied for η, according to Definition Appendix A.2 and elementary truth tables.

3. In the last step of the proof, we show that each state of $\mathcal{D}$ satisfies any minimal loop invariant.
   - Let J be a minimal loop invariant. Assume that there is a state $\eta \in \mathcal{D}$ that does not satisfy J. Then $J \vee \mathbb{1}_\eta$ (where $\mathbb{1}_\eta$ is the formula characterizing the state η), is strictly weaker than J. But it is also an invariant since after i iterations of the *while* loop from η, one of the resulting sets of states E satisfies Q. This contradicts the minimality of J.
   - Consequently I is the weakest loop invariant. □

Theorem Appendix B.2. (Completeness theorem on the genetically modified Hoare logic). *Given a* GRN N*, a trace specification* p *and a post-condition* Q*, the backward strategy defined at the end of Section 2, with the inference rules of Section 5, computes after steps 1 and 2 the* weakest precondition P_0 *such that* $\{P_0\}\ p\ \{Q\}$ *is satisfied. In other words, for any assertion* P*, if* $\{P\}\ p\ \{Q\}$ *is satisfied, then* $P \Rightarrow P_0$ *is satisfied (that is, the third step of the backward strategy).*

This theorem has an obvious corollary.

Corollary Appendix B.3. *Given a* GRN N*, our modified Hoare logic is complete.*

Proof of the corollary: if $\{P\}\ p\ \{Q\}$ is satisfied, then, from the theorem above, there is a proof tree that infers the Hoare triple if there is a proof tree for the property $P \Rightarrow P_0$ (which is semantically satisfied because P_0 is the weakest precondition). First order logic being complete and the number of possible substitutions being finite (the state space being finite), the proof tree for $P \Rightarrow P_0$ exists. □

Proof of the completeness theorem:
Under the following two hypotheses

$\boxed{H_1}$ the Hoare triple $\{P\}\ p\ \{Q\}$ is satisfied, i.e., for all η satisfying P, there exists E such that $\eta \overset{p}{\rightsquigarrow} E$ and for all $\eta' \in E$, η' satisfies Q,

$\boxed{H_2}$ for all *while* statements of p, the corresponding loop invariant I is the weakest one (Proposition Appendix B.1),

one has to prove the conclusion:

$\boxed{C}$ $P \Rightarrow P_0$ is satisfied, where P_0 is the precondition computed from p and Q by the steps 1 and 2 of the backward strategy with the inference rules of Section 5.

The proof is done by structural induction according to the backward strategy on p.

- If p is of the form $v+$, then the only set E such that $\eta \overset{v+}{\rightsquigarrow} E$ is $E = \{\eta[v \leftarrow v+1]\}$. The hypothesis $\boxed{H_1}$ becomes:

  $\boxed{H_1}$ for all η satisfying P, $\eta' = \eta[v \leftarrow v+1]$ satisfies Q and $\eta \rightarrow \eta'$ is a transition of $\mathcal{S}$

  and from the *Increase* rule, the conclusion becomes:

  $\boxed{C}$ $P \Rightarrow (\Phi_v^+ \wedge Q[v \leftarrow v+1])$ is satisfied.

  So, $\boxed{H_1} \Rightarrow \boxed{C}$ straightforwardly results from the definition of Φ_{v^+} (Notation 5.1) and we do not use $\boxed{H_2}$.

- If p is of the form $p_1; p_2$, then we firstly inherit the two structural induction hypotheses:

  $\boxed{H_3}$ for all assertions P' and Q', if $\{P'\}\ p_1\ \{Q'\}$ is satisfied then $P' \Rightarrow P_1$ is satisfied, where P_1 is the precondition computed from Q' *via* the backward strategy

  $\boxed{H_4}$ for all assertions P'' and Q'', if $\{P''\}\ p_2\ \{Q''\}$ is satisfied then $P'' \Rightarrow P_2$ is satisfied, where P_2 is the precondition computed from Q'' *via* the backward strategy

  Moreover the hypothesis $\boxed{H_1}$ becomes (Definition 4.4):

  $\boxed{H_1}$ for all η satisfying P, there exists a family of state sets $\mathcal{F} = \{E_e\}_{e \in F}$ such that $\eta \overset{p_1}{\rightsquigarrow} F$ and $e \overset{p_2}{\rightsquigarrow} E_e$ for all $e \in F$ and for all $\eta' \in E = (\bigcup_{e \in F} E_e)$, η' satisfies Q

  Lastly, from the *Sequential composition* rule, the conclusion becomes:

  $\boxed{C}$ $P \Rightarrow P_1$ is satisfied, where P_1 is the weakest precondition of $\{\cdots\}\ p_1\ \{P_2\}$, P_2 being the weakest precondition of $\{\cdots\}\ p_2\ \{Q\}$.

From $\boxed{H_4}$ (with $Q'' = Q$) it results that all the states $e \in F$ of hypothesis $\boxed{H_1}$ satisfy P_2. Consequently $\{P\}\ p_1\ \{P_2\}$ is satisfied. Thus, from $\boxed{H_3}$ (with $Q' = P_2$ and $P' = P$) it comes $P \Rightarrow P_1$, which proves the conclusion.

- If p is of the form *while e with I do p'*, then, by construction of the backward strategy, applying the *Iteration* rule, we get $P_0 = I$, and the conclusion results immediately from $\boxed{H_2}$.
- Similarly to the soundness proof, we do not develop here the other cases of the structural induction. They are either similar to already developed cases (*Decrease* rule) or trivial (*Assert* rule, *Quantifier rules*, and *Assignment* rule).

This ends the proof. □

Remark Appendix B.4. *Soundness and completeness being now established, one can extend Proposition Appendix B.1 by giving a purely symbolic computation of the weakest loop invariant I of a while loop. Following the notations of the proof of Proposition Appendix B.1:*

- *The set of states q_0 is characterised by the formula $Q_0 \equiv \neg e \wedge Q$,*
- *In addition,* assuming that the trace specification p terminates*, the set of states q_{i+1} is inductively characterised by the weakest precondition Q_{i+1} obtained via the backward strategy of the proof of $\{Q_{i+1}\}\ p\ \{Q_i\}$ (this is due to the soundness and completeness of our calculus).*
- *From this construction, we deduce that the first integer n such that $q_{n+1} \subset \mathcal{D}_n$ (where $\mathcal{D}_n = \bigcup_{i=0}^{n} q_i$) is the first n such that $Q_{n+1} \Rightarrow \bigvee_{i=0}^{n} Q_i$. This implication is decidable because the set of possible substitutions is finite.*

Proposition Appendix B.1 implies that the integer n mentioned before exists. Consequently $I = \bigvee_{i=0}^{n} Q_i$ can be expressed in a purely symbolic way. And more importantly, this can be done from the solely knowledge *of the interaction graph. The assertion I is then a constraint on states and parameters $K_{\ldots}$, what we used in Section 6.*