

The Weak Spectroscopy Game to Characterize Behavioral Equivalences

Lisa A. Barthel^{1,2}, Leonard M. Hübner¹, Caroline Lemke^{1,3}, Karl P. P. Mattes¹,
Lenard Mollenkopf¹, and Benjamin Bisping^{1,4}

¹Technische Universität Berlin, Germany

²Technische Universität Ilmenau, Germany

³Carl von Ossietzky Universität Oldenburg, Germany

⁴Télécom SudParis, Institut Polytechnique de Paris, France

December 26, 2025

Abstract

We provide an Isabelle/HOL formalization of Bisping and Jansen’s weak spectroscopy game [4], which can be used to simultaneously characterize and decide a hierarchy of behavioral equivalences for systems with internal behavior. This is valuable for applications in concurrency theory and formal verification where equivalences and distinctions of the “linear-time-branching-time spectrum” are a recurring topic.

This entry contains a game characterization of most behavioral equivalences from stability-respecting branching bisimilarity to weak trace equivalence. Technically, the results link distinguishing sublanguages of Hennessy–Milner logic to winning attacker budgets in an energy game through an eight-dimensional measurement of syntactic features appearing in formulas.

Overview. This formalization provides theoretical underpinnings of <https://equiv.io>, a tool to *decide all behavioral equivalences at once*. By phrasing *equivalences as energy games*, one obtains a uniform way to handle a wide range of equivalences in van Glabbeek’s *linear-time-branching-time spectrum* [6, 7]. In particular, we treat systems with *silent* τ -steps, which usually arise because of abstraction from internal behavior, for instance, when modeling communication protocols or distributed systems using transition systems.

This formalization follows Bisping and Jansen’s *weak spectroscopy game* [4], respectively the proofs from the arXiv version [3].

- Section 1 provides some basics on transition systems with internal behavior.
- Sections 2 and 3 define a version of Hennessy–Milner logic for systems with internal behavior and a syntactic metric to select sublanguages of it through coordinates.
- Sections 4 to 6 prove certain coordinates to correspond to weak trace equivalence, η -bisimilarity, η -similarity and branching bisimilarity as well as their stable variants. (As the relationship is established through modal logics, the results can be understood as Hennessy–Milner theorems [5].)
- Sections 7 to 9 introduce the weak spectroscopy game and prove that winning attacker energies in the game correspond to coordinates of distinguishing formulas according to the syntactic expressiveness metric.

The broader project of *deciding all equivalences at once* is outlined in Bisping’s PhD thesis [2]. There, one can also find more gentle introductions to the topic and to the game-theoretic approach in general. The energy game approach is due to [1].

Acknowledgments. Several proofs in this document follow pen-and-paper proofs by David N. Jansen.

Contents

1	Labeled Transition Systems	4
1.1	Base LTS	4
1.2	Labeled Transition Systems with Silent Steps	4
1.3	Modal Logics on LTS	8
1.4	Preorders and Equivalences on Processes Derived from Formula Sets	10
2	Hennessy–Milner Logic for Stability-Respecting Branching Bisimilarity	11
2.1	Semantics of HML_{SRBB} Formulas	11
2.2	Distinguishing Formulas	12
2.3	HML_{SRBB} Implication and Equivalence	13
2.4	Substitution and Congruence	14
2.5	Trivial and Equivalent Formulas	14
3	Expressiveness Prices	20
3.1	Comparing and Subtracting Energies	20
3.2	Minimum Updates	22
3.3	Components of Expressiveness Prices	25
3.4	Properties of Price Components	28
3.5	Expressiveness Price Function	29
3.6	Prices of Certain Formulas	30
3.7	Characterizing Equivalence by Energy Coordinates	38
3.8	Relational Effects of Prices	39
4	Weak Traces	43
4.1	Weak Traces as Modal Constructs	43
4.2	Weak Trace Observations through Coordinates	43
5	η-Bisimilarity and η-Similarity	48
5.1	Definition and Properties of η -(Bi-)Similarity	48
5.2	Logical Characterization of η -Bisimilarity through Expressiveness Price	49
5.3	η -Similarity	55
6	Branching Bisimilarity	61
6.1	Definitions of (Stability-Respecting) Branching Bisimilarity	61
6.2	Properties of Branching Bisimulation Equivalences	61
6.3	hml_srbb as Modal Characterization of Stability-Respecting Branching Bisimilarity	65
7	Energy Games	72
7.1	Fundamentals	72
7.2	Winning Budgets	72
8	Weak Spectroscopy Game	74
8.1	Game Rules	74

8.2	Energy Game Properties	75
9	Correctness	80
9.1	Distinction Implies Winning Budgets	80
9.2	Strategy Formulas	95
9.3	Correctness Theorem	111

1 Labeled Transition Systems

```
theory Labeled_Transition_Systems
  imports Main
begin
```

1.1 Base LTS

The locale **LTS** represents a labeled transition system consisting of a set of states $\mathcal{P}$, a set of actions Σ , and a transition relation $\mapsto \subseteq \mathcal{P} \times \Sigma \times \mathcal{P}$. We formalize the sets of states and actions by the type variables 's and 'a. An LTS is then determined by the transition relation **step**.

```
locale lts =
  fixes step :: '<'s => 'a => 's => bool> (<_ mapsto _ _> [70,70,70] 80)
begin
```

One may lift **step** to sets of states, written as $P \mapsto S \alpha Q$.

```
abbreviation step_setp (<_ mapstoS _ _> [70,70,70] 80) where
  <P mapstoS alpha Q <=> (<forall q in Q. exists p in P. p mapsto alpha q>) & (<forall p in P. forall q. p mapsto alpha q -> q in Q>)>
```

The set of α -derivatives for a set of states P .

```
definition step_set :: '<'s set => 'a => 's set> where
  <step_set P alpha <=> { q . exists p in P. p mapsto alpha q }>
```

The set of possible α -steps for a set of states P is an instance of **step** lifted to sets of steps.

```
lemma step_set_is_step_set: <P mapstoS alpha (step_set P alpha)>
  using step_set_def by force
```

The lifted **step_setp** ($P \mapsto S \alpha Q$) is therefore this set Q .

```
lemma step_set_eq:
  assumes <P mapstoS alpha Q>
  shows <Q = step_set P alpha>
  using assms step_set_is_step_set by fastforce
```

end — of locale **lts**

1.2 Labeled Transition Systems with Silent Steps

We formalize labeled transition systems with silent steps as an extension of ordinary labeled transition systems with a fixed internal action τ .

```
locale lts_tau =
  lts step
  for step :: '<'s => 'a => 's => bool> (<_ mapsto _ _> [70,70,70] 80) +
  fixes tau :: 'a
begin
```

The paper [3] introduces a transition $p \xrightarrow{(\alpha)} p'$ if $p \xrightarrow{\alpha} p'$, or if $\alpha = \tau$ and $p = p'$. We define **soft_step** analogously and provide the notation $p \mapsto a \alpha p'$.

```
abbreviation soft_step (<_ mapsto_a _ _> [70,70,70] 80) where
  <p mapsto_a alpha q <=> p mapsto alpha q <ve> (alpha = tau & p = q)>
```

```
inductive silent_reachable :: '<'s => 's => bool> (infix <->> 80)
  where
    refl: <p ->> p> |
    step: <p ->> p''> if <p mapsto tau p'> and <p' ->> p''>
```

If p' is silent-reachable from p and there is a τ -transition from p' to p'' then p'' is silent reachable from p .

```

lemma silent_reachable_append_τ: <p → p' ⇒ p' ↦ τ p'' ⇒ p → p''>
proof (induct rule: silent_reachable.induct)
  case (refl p)
  then show ?case using silent_reachable.intros by blast
next
  case (step p p' p'')
  then show ?case using silent_reachable.intros by blast
qed

```

The relation $(\rightarrow)$ is transitive.

```

lemma silent_reachable_trans:
  assumes
    <p → p'>
    <p' → p''>
  shows
    <p → p''>
using assms silent_reachable.intros(2)
by (induct, blast+)

```

The relation `silent_reachable_loopless` is a variation of $(\rightarrow)$ that does not use self-loops.

```

inductive silent_reachable_loopless :: <'s ⇒ 's ⇒ bool> (infix <→L> 80)
where
  <p →L p> |
  <p →L p''> if <p ↦ τ p'> and <p' →L p''> and <p ≠ p'>

```

If a state p' is $(\rightarrow)$ from p it is also $(\rightarrowL)$.

```

lemma silent_reachable_impl_loopless:
  assumes <p → p'>
  shows <p →L p'>
using assms
proof (induct rule: silent_reachable.induct)
  case (refl p)
  thus ?case by (rule silent_reachable_loopless.intros(1))
next
  case (step p p' p'')
  thus ?case proof (cases <p = p'>)
    case True
    thus ?thesis using step.hyps(3) by auto
  next
    case False
    thus ?thesis using step.hyps silent_reachable_loopless.intros(2) by blast
  qed
qed

```

```

lemma tau_chain_reachabilty:
  assumes <∀ i < length pp - 1. pp!i ↦ τ pp!(Suc i)>
  shows <∀ j < length pp. ∀ i ≤ j. pp!i → pp!j>
proof safe
  fix j i
  assume <j < length pp> <i ≤ j>
  thus <pp!i → pp!j>
  proof (induct j)
    case 0
    then show ?case
      using silent_reachable.refl by blast
  next
    case (Suc j)
    then show ?case
    proof (induct i)
      case 0

```

```

    then show ?case using assms silent_reachable_append_τ
    by (metis Suc_lessD Suc_lessE bot_nat_0.extremum diff_Suc_1)
  next
    case (Suc i)
    then show ?case using silent_reachable.refl assms silent_reachable_append_τ
    by (metis Suc_lessD Suc_lessE diff_Suc_1 le_SucE)
  qed
qed
qed

```

A state p can reach p' weakly by performing an α -transition, possibly proceeded and followed by any number of τ -transitions.

```

definition weak_step (<_  $\Rightarrow$  _> [70, 70, 70] 80) where
  <p  $\Rightarrow$  α p'  $\equiv$  if α = τ
    then p  $\Rightarrow$  p'
    else  $\exists p_1 p_2. p \Rightarrow p_1 \wedge p_1 \Rightarrow \alpha p_2 \wedge p_2 \Rightarrow p'$ 

```

```

lemma silent_prepend_weak_step: <p  $\Rightarrow$  p'  $\implies$  p'  $\Rightarrow$  α p''  $\implies$  p  $\Rightarrow$  α p''>
  unfolding weak_step_def using silent_reachable_trans[of p p'] by fastforce

```

A sequence of `weak_steps` from one state p to another p' .

```

inductive weak_step_sequence :: <'s  $\Rightarrow$  'a list  $\Rightarrow$  's  $\Rightarrow$  bool> (<_  $\Rightarrow$  _> [70,70,70]
80) where
  <p  $\Rightarrow$  [] p'> if <p  $\Rightarrow$  p'> |
  <p  $\Rightarrow$  (α#rt) p''> if <p  $\Rightarrow$  α p'> <p'  $\Rightarrow$  rt p''>

```

```

lemma weak_step_sequence_trans:
  assumes <p  $\Rightarrow$  tr_1 p'> and <p'  $\Rightarrow$  tr_2 p''>
  shows <p  $\Rightarrow$  (tr_1 @ tr_2) p''>
  using assms weak_step_sequence.intros(2)
proof induct
  case (1 p p')
  then show ?case
    by (metis weak_step_sequence.simps append_Nil silent_prepend_weak_step silent_reachable_trans)
next
  case (2 p α p' rt p'')
  then show ?case by fastforce
qed

```

The weak traces of a state are all possible sequences of weak transitions that can be performed.

```

abbreviation weak_traces :: <'s  $\Rightarrow$  'a list set>
  where <weak_traces p  $\equiv$  {tr.  $\exists p'. p \Rightarrow$  tr p'}>

```

The empty trace is in `weak_traces` for all states.

```

lemma empty_trace_allways_weak_trace:
  shows <[]  $\in$  weak_traces p>
  using silent_reachable.intros(1) weak_step_sequence.intros(1) by fastforce

```

τ can be prepended to any weak trace.

```

lemma prepend_τ_weak_trace:
  assumes <tr  $\in$  weak_traces p>
  shows <(τ # tr)  $\in$  weak_traces p>
  using assms silent_reachable.intros(1) mem_Collect_eq
  weak_step_sequence.intros(2) weak_step_def by fastforce

```

```

lemma silent_prepend_weak_traces:
  assumes
    <p  $\Rightarrow$  p'>
    <tr  $\in$  weak_traces p'>

```

```

shows
  <tr ∈ weak_traces p>
using assms
proof -
  assume <p → p'>
  and <tr ∈ weak_traces p'>
  hence <∃p''. p' →→→$ tr p''> by auto
  then obtain p'' where <p' →→→$ tr p''> by auto
  from <p' →→→$ tr p''>
  and <p → p'>
  have <p →→→$ tr p''>
  by (metis append_self_conv2 weak_step_sequence.intros(1) weak_step_sequence_trans)
  hence <∃p''. p →→→$ tr p''> by auto
  then show <tr ∈ weak_traces p>
  by blast
qed

```

If there is an α -transition from p to p' , and p' has a weak trace tr , then the sequence $(\alpha \# tr)$ is a valid (weak) trace of p .

```

lemma step_prepend_weak_traces:
  assumes
    <p → α p'>
    <tr ∈ weak_traces p'>
  shows
    <(α # tr) ∈ weak_traces p>
using assms
proof -
  from <tr ∈ weak_traces p'>
  have <∃p''. p' →→→$ tr p''> by auto
  then obtain p'' where <p' →→→$ tr p''> by auto
  with <p → α p'>
  have <p →→→$ (α # tr) p''>
  by (metis lts_tau.silent_reachable.intros(1) lts_tau.silent_reachable_append_τ
    lts_tau.weak_step_def lts_tau.weak_step_sequence.intros(2))
  then have <∃p''. p →→→$ (α # tr) p''> by auto
  then show <(α # tr) ∈ weak_traces p> by auto
qed

```

A state is weakly trace pre-ordered to another other, `weakly_trace_preordered` denoted by $\lesssim_{WT}$ if all its traces can also be observed from the second process.

```

definition weakly_trace_preordered (infix <≲WT> 60) where
  <p ≲WT q ≡ weak_traces p ⊆ weak_traces q>

```

```

definition weakly_trace_equivalent (infix <≃WT> 60) where
  <p ≃WT q ≡ p ≲WT q ∧ q ≲WT p>

```

Just like `step_setp`, one can lift $(\rightarrow)$ to sets of states.

```

abbreviation silent_reachable_setp (infix <→S> 80) where
  <P →S P' ≡ ((∀p' ∈ P'. ∃p ∈ P. p → p') ∧ (∀p ∈ P. ∀p'. p → p' → p' ∈ P'))>

```

```

definition silent_reachable_set :: <'s set ⇒ 's set> where
  <silent_reachable_set P ≡ { q . ∃p ∈ P. p → q }>

```

```

lemma sreachable_set_is_sreachable: <P →S S (silent_reachable_set P)>
  using silent_reachable_set_def by auto

```

```

lemma sreachable_set_eq:
  assumes <P →S Q>
  shows <Q = silent_reachable_set P>
  using sreachable_set_is_sreachable assms by fastforce

```

We likewise lift `soft_step` to sets of states.

```
abbreviation soft_step_setp (<_ ↦aS _ _> [70,70,70] 80) where
  <P ↦aS α Q ≡ (∀ q ∈ Q. ∃ p ∈ P. p ↦a α q) ∧ (∀ p ∈ P. ∀ q. p ↦a α q ⟶ q ∈ Q)>
```

```
definition soft_step_set :: <'s set ⇒ 'a ⇒ 's set> where
  <soft_step_set P α ≡ { q . ∃ p ∈ P. p ↦a α q }>
```

```
lemma soft_step_set_is_soft_step_set:
  <P ↦aS α (soft_step_set P α)>
  using soft_step_set_def by auto
```

```
lemma exactly_one_soft_step_set:
  <∃!Q. P ↦aS α Q>
```

```
proof -
  from soft_step_set_is_soft_step_set
  have <P ↦aS α (soft_step_set P α)>
    and <∧Q. P ↦aS α Q ⟹ Q = (soft_step_set P α)>
    by fastforce+
  show <∃!Q. P ↦aS α Q>
  proof
    from <P ↦aS α (soft_step_set P α)>
    show <P ↦aS α (soft_step_set P α)> .
  next
    from <∧Q. P ↦aS α Q ⟹ Q = (soft_step_set P α)>
    show <∧Q. P ↦aS α Q ⟹ Q = (soft_step_set P α)> .
  qed
qed
```

```
lemma soft_step_set_eq:
  assumes <P ↦aS α Q>
  shows <Q = soft_step_set P α>
  using exactly_one_soft_step_set soft_step_set_is_soft_step_set assms
  by fastforce
```

A state is stable if it cannot make any further internal steps.

```
abbreviation <stable_state p ≡ ∀p'. ¬(p ↦ τ p')>
```

```
lemma stable_state_stable:
  assumes <stable_state p> <p ⟶ p'>
  shows <p = p'>
  using assms(2,1) by (cases, blast+)
```

```
definition stability_respecting :: <('s ⇒ 's ⇒ bool) ⇒ bool> where
  <stability_respecting R ≡ ∀ p q. R p q ∧ stable_state p ⟶
    (∃ q'. q ⟶ q' ∧ R p q' ∧ stable_state q')>
```

```
end — of locale lts_tau
```

```
end
```

1.3 Modal Logics on LTS

We here supply abstract definitions that would work for all modal logics one might define over an LTS. In particular, this contains mechanisms to derive equivalences from sublogics.

```
theory LTS_Semantics
  imports
    Labeled_Transition_Systems
begin
```

```

locale lts_semantics = lts step
  for step :: <'s  $\Rightarrow$  'a  $\Rightarrow$  's  $\Rightarrow$  bool> (<_  $\mapsto$  _ > [70,70,70] 80) +
  fixes models :: <'s  $\Rightarrow$  'formula  $\Rightarrow$  bool>
begin

definition entails :: <'formula  $\Rightarrow$  'formula  $\Rightarrow$  bool> where
  entails_def[simp]: <entails  $\varphi_1$   $\varphi_r \equiv (\forall p. (\text{models } p \ \varphi_1) \longrightarrow (\text{models } p \ \varphi_r))$ >

definition logical_eq :: <'formula  $\Rightarrow$  'formula  $\Rightarrow$  bool> where
  logical_eq_def[simp]: <logical_eq  $\varphi_1$   $\varphi_r \equiv \text{entails } \varphi_1 \ \varphi_r \wedge \text{entails } \varphi_r \ \varphi_1$ >

```

Formula implication is a pre-order.

```

lemma entails_preord: <reflp (entails)> <transp (entails)>
  by (simp add: reflpI transp_def)+

```

```

lemma eq_equiv: <equivp logical_eq>
  using equivpI reflpI sympI transpI
  unfolding logical_eq_def entails_def
  by (smt (verit, del_insts))

```

Formula equivalence is a biimplication on the models predicate.

```

lemma eq_equality[simp]: <(logical_eq  $\varphi_1$   $\varphi_r) = (\forall p. \text{models } p \ \varphi_1 \longleftrightarrow \text{models } p \ \varphi_r)$ >
  by force

```

```

lemma logical_eqI[intro]:
  assumes
    < $\bigwedge s. \text{models } s \ \varphi_1 \implies \text{models } s \ \varphi_r$ >
    < $\bigwedge s. \text{models } s \ \varphi_r \implies \text{models } s \ \varphi_1$ >
  shows
    <logical_eq  $\varphi_1$   $\varphi_r$ >
  using assms by auto

```

```

definition distinguishes :: <'formula  $\Rightarrow$  's  $\Rightarrow$  's  $\Rightarrow$  bool> where
  distinguishes_def[simp]:
    <distinguishes  $\varphi$  p q  $\equiv \text{models } p \ \varphi \wedge \neg(\text{models } q \ \varphi)$ >

```

```

definition distinguishes_from :: <'formula  $\Rightarrow$  's  $\Rightarrow$  's set  $\Rightarrow$  bool> where
  distinguishes_from_def[simp]:
    <distinguishes_from  $\varphi$  p Q  $\equiv \text{models } p \ \varphi \wedge (\forall q \in Q. \neg(\text{models } q \ \varphi))$ >

```

```

lemma distinction_unlifting:
  assumes
    <distinguishes_from  $\varphi$  p Q>
  shows
    < $\forall q \in Q. \text{distinguishes } \varphi \ p \ q$ >
  using assms by simp

```

```

lemma no_distinction_fom_self:
  assumes
    <distinguishes  $\varphi$  p p>
  shows
    <False>
  using assms by simp

```

```

lemma dist_equal_dist:
  assumes <logical_eq  $\varphi_1$   $\varphi_r$ >
    and <distinguishes  $\varphi_1$  p q>
  shows <distinguishes  $\varphi_r$  p q>
  using assms
  by auto

```

```

abbreviation model_set :: <'formula  $\Rightarrow$  's set> where
  <model_set  $\varphi \equiv \{p. \text{models } p \ \varphi\}$ >

```

1.4 Preorders and Equivalences on Processes Derived from Formula Sets

A set of formulas pre-orders two processes p and q if, for all formulas in this set, the fact that p satisfies a formula means that q must also satisfy this formula.

```

definition preordered :: <'formula set  $\Rightarrow$  's  $\Rightarrow$  's  $\Rightarrow$  bool> where
  preordered_def[simp]:
    <preordered  $\varphi s \ p \ q \equiv \forall \varphi \in \varphi s. \text{models } p \ \varphi \longrightarrow \text{models } q \ \varphi$ >

```

If a set of formulas pre-orders two processes p and q , then no formula in that set may distinguish p from q .

```

lemma preordered_no_distinction:
  <preordered  $\varphi s \ p \ q \equiv (\forall \varphi \in \varphi s. \neg(\text{distinguishes } \varphi \ p \ q))$ >
  by simp

```

A formula set derived pre-order is a pre-order.

```

lemma preordered_preord:
  <reflp (preordered  $\varphi s$ )>
  <transp (preordered  $\varphi s$ )>
  unfolding reflp_def transp_def by auto

```

A set of formulas equates two processes if it pre-orders these two processes in both directions.

```

definition equivalent :: <'formula set  $\Rightarrow$  's  $\Rightarrow$  's  $\Rightarrow$  bool> where
  equivalent_def[simp]:
    <equivalent  $\varphi s \ p \ q \equiv \text{preordered } \varphi s \ p \ q \wedge \text{preordered } \varphi s \ q \ p$ >

```

If a set of formulas equates two processes, then no formula in that set may distinguish them in any direction.

```

lemma equivalent_no_distinction: <equivalent  $\varphi s \ p \ q$ 
  =  $(\forall \varphi \in \varphi s. \neg(\text{distinguishes } \varphi \ p \ q) \wedge \neg(\text{distinguishes } \varphi \ q \ p))$ >
  by auto

```

A formula-set-derived equivalence is an equivalence.

```

lemma equivalent_equiv: <equivp (equivalent  $\varphi s$ )>
proof (rule equivpI)
  show <reflp (equivalent  $\varphi s$ )>
    by (simp add: reflpI)
  show <symp (equivalent  $\varphi s$ )>
    unfolding equivalent_no_distinction symp_def
    by auto
  show <transp (equivalent  $\varphi s$ )>
    unfolding transp_def equivalent_def preordered_def
    by blast
qed

```

end — of context `lts_semantics`

end

2 Hennessy–Milner Logic for Stability-Respecting Branching Bisimilarity

```
theory HML_SRBB
  imports LTS_Semantics
begin
```

This section describes a variant of Hennessy–Milner logic that characterizes stability-respecting branching bisimilarity (SRBB).

The following mutually-recursive datatype family describes a grammar of `HML_SRBB` formulas.

```
datatype
  ('act, 'i) hml_srbb =
    TT |
    Internal <('act, 'i) hml_srbb_inner> |
    ImmConj <'i set> <'i  $\Rightarrow$  ('act, 'i) hml_srbb_conjunct>
and
  ('act, 'i) hml_srbb_inner =
    Obs 'act <('act, 'i) hml_srbb> |
    Conj <'i set> <'i  $\Rightarrow$  ('act, 'i) hml_srbb_conjunct> |
    StableConj <'i set> <'i  $\Rightarrow$  ('act, 'i) hml_srbb_conjunct> |
    BranchConj 'act <('act, 'i) hml_srbb>
      <'i set> <'i  $\Rightarrow$  ('act, 'i) hml_srbb_conjunct>
and
  ('act, 'i) hml_srbb_conjunct =
    Pos <('act, 'i) hml_srbb_inner> |
    Neg <('act, 'i) hml_srbb_inner>
```

The constructors correspond to more conventional notation of HML as follows:

- `hml_srbb` (members usually referred to as φ):
 - `TT` encodes $\top$
 - `Internal  $\chi$` encodes $\langle \varepsilon \rangle \chi$
 - `ImmConj  $I \ \psi s$` encodes $\bigwedge_{i \in I} \psi s(i)$
- `hml_srbb_inner` (usually χ):
 - `Obs  $\alpha \ \varphi$` encodes $(\alpha) \varphi$
 - `Conj  $I \ \psi s$` encodes $\bigwedge_{i \in I} \psi s(i)$
 - `StableConj  $I \ \psi s$` encodes $\neg \langle \tau \rangle \top \wedge \bigwedge_{i \in I} \psi s(i)$
 - `BranchConj  $\alpha \ \varphi \ I \ \psi s$` encodes $(\alpha) \varphi \wedge \bigwedge_{i \in I} \psi s(i)$
- `hml_srbb_conjunct` (usually ψ):
 - `Pos  $\chi$` encodes $\langle \varepsilon \rangle \chi$
 - `Neg  $\chi$` encodes $\neg \langle \varepsilon \rangle \chi$

2.1 Semantics of `HMLSRBB` Formulas

This section describes how semantic meaning is assigned to `HMLSRBB` formulas in the context of a LTS. We define what it means for a process `p` to satisfy an `HMLSRBB` formula φ , written as `p  $\models_{\text{SRBB}}$   $\varphi$` .

```
context lts_tau
begin
```

```

primrec
  hml_srbb_models :: <'s  $\Rightarrow$  ('a, 's) hml_srbb  $\Rightarrow$  bool> (infix1 <|=SRBB> 60)
and hml_srbb_inner_models :: <'s  $\Rightarrow$  ('a, 's) hml_srbb_inner  $\Rightarrow$  bool>
and hml_srbb_conjunct_models :: <'s  $\Rightarrow$  ('a, 's) hml_srbb_conjunct  $\Rightarrow$  bool> where
  <hml_srbb_models state TT =
    True> |
  <hml_srbb_models state (Internal  $\chi$ ) =
    ( $\exists p'. \text{state} \Rightarrow p' \wedge (\text{hml\_srbb\_inner\_models } p' \chi)$ )> |
  <hml_srbb_models state (ImmConj I  $\psi$ s) =
    ( $\forall i \in I. \text{hml\_srbb\_conjunct\_models state } (\psi s \ i)$ )> |

  <hml_srbb_inner_models state (Obs a  $\varphi$ ) =
    ( $(\exists p'. \text{state} \mapsto a \ p' \wedge \text{hml\_srbb\_models } p' \ \varphi) \vee a = \tau \wedge \text{hml\_srbb\_models state } \varphi$ )> |
  <hml_srbb_inner_models state (Conj I  $\psi$ s) =
    ( $\forall i \in I. \text{hml\_srbb\_conjunct\_models state } (\psi s \ i)$ )> |
  <hml_srbb_inner_models state (StableConj I  $\psi$ s) =
    ( $(\#p'. \text{state} \mapsto \tau \ p') \wedge (\forall i \in I. \text{hml\_srbb\_conjunct\_models state } (\psi s \ i))$ )> |
  <hml_srbb_inner_models state (BranchConj a  $\varphi$  I  $\psi$ s) =
    ( $((\exists p'. \text{state} \mapsto a \ p' \wedge \text{hml\_srbb\_models } p' \ \varphi) \vee a = \tau \wedge \text{hml\_srbb\_models state } \varphi) \wedge (\forall i \in I. \text{hml\_srbb\_conjunct\_models state } (\psi s \ i))$ )> |

  <hml_srbb_conjunct_models state (Pos  $\chi$ ) =
    ( $\exists p'. \text{state} \Rightarrow p' \wedge \text{hml\_srbb\_inner\_models } p' \ \chi$ )> |
  <hml_srbb_conjunct_models state (Neg  $\chi$ ) =
    ( $\#p'. \text{state} \Rightarrow p' \wedge \text{hml\_srbb\_inner\_models } p' \ \chi$ )>

sublocale lts_semantics <step> <hml_srbb_models> .
sublocale hml_srbb_inner: lts_semantics where models = hml_srbb_inner_models .
sublocale hml_srbb_conj: lts_semantics where models = hml_srbb_conjunct_models .

```

2.2 Distinguishing Formulas

```

lemma verum_never_distinguishes:
  < $\neg$  distinguishes TT p q>
by simp

```

If $\bigwedge_{i \in I} \psi s(i)$ distinguishes p from q, then there must be at least one conjunct in this conjunction that distinguishes p from q.

```

lemma srbb_dist_imm_conjunction_implies_dist_conjunct:
  assumes <distinguishes (ImmConj I  $\psi$ s) p q>
  shows < $\exists i \in I. \text{hml\_srbb\_conj. distinguishes } (\psi s \ i) \ p \ q$ >
using assms by auto

```

```

lemma srbb_dist_conjunction_implies_dist_conjunct:
  assumes <hml_srbb_inner.distinguishes (Conj I  $\psi$ s) p q>
  shows < $\exists i \in I. \text{hml\_srbb\_conj. distinguishes } (\psi s \ i) \ p \ q$ >
using assms by auto

```

```

lemma srbb_dist_branch_conjunction_implies_dist_conjunct_or_branch:
  assumes
    <hml_srbb_inner.distinguishes (BranchConj  $\alpha$   $\varphi$  I  $\psi$ s) p q>
  shows
    <( $\exists i \in I. \text{hml\_srbb\_conj. distinguishes } (\psi s \ i) \ p \ q$ )
       $\vee$  hml_srbb_inner.distinguishes (Obs  $\alpha$   $\varphi$ ) p q>
using assms by force

```

```

lemma srbb_dist_conjunct_implies_dist_imm_conjunction:
  assumes
    <i  $\in$  I>
    <hml_srbb_conj.distinguishes  $(\psi s \ i) \ p \ q$ >

```

```

    <∀i∈I. hml_srbb_conjunct_models p (ψs i)>
  shows
    <distinguishes (ImmConj I ψs) p q>
  using assms by auto

lemma srbb_dist_conjunct_implies_dist_conjunction:
  assumes
    <i∈I>
    <hml_srbb_conj.distinguishes (ψs i) p q>
    <∀i∈I. hml_srbb_conjunct_models p (ψs i)>
  shows
    <hml_srbb_inner.distinguishes (Conj I ψs) p q>
  using assms by auto

lemma srbb_dist_conjunct_or_branch_implies_dist_branch_conjunction:
  assumes
    <∀i ∈ I. hml_srbb_conjunct_models p (ψs i)>
    <hml_srbb_inner_models p (Obs α φ)>
    <(i∈I ∧ hml_srbb_conj.distinguishes (ψs i) p q)
      ∨ (hml_srbb_inner.distinguishes (Obs α φ) p q)>
  shows
    <hml_srbb_inner.distinguishes (BranchConj α φ I ψs) p q>
  using assms by force

```

2.3 HML_{SRBB} Implication and Equivalence

```

abbreviation hml_srbb_impl
  :: <('a, 's) hml_srbb ⇒ ('a, 's) hml_srbb ⇒ bool>  (infixr <⇒> 70)
where
  <hml_srbb_impl ≡ entails>

abbreviation
  hml_srbb_impl_inner
  :: <('a, 's) hml_srbb_inner ⇒ ('a, 's) hml_srbb_inner ⇒ bool>
  (infix <χ⇒> 70)
where
  <(χ⇒) ≡ hml_srbb_inner.entails>

abbreviation
  hml_srbb_impl_conjunct
  :: <('a, 's) hml_srbb_conjunct ⇒ ('a, 's) hml_srbb_conjunct ⇒ bool>
  (infix <ψ⇒> 70)
where
  <(ψ⇒) ≡ hml_srbb_conj.entails>

abbreviation
  hml_srbb_eq
  :: <('a, 's) hml_srbb ⇒ ('a, 's) hml_srbb ⇒ bool>
  (infix <⇐srbb⇒> 70)
where
  <(⇐srbb⇒) ≡ logical_eq>

abbreviation
  hml_srbb_eq_inner
  :: <('a, 's) hml_srbb_inner ⇒ ('a, 's) hml_srbb_inner ⇒ bool>
  (infix <⇐χ⇒> 70)
where
  <(⇐χ⇒) ≡ hml_srbb_inner.logical_eq>

abbreviation
  hml_srbb_eq_conjunct

```

```

:: <('a, 's) hml_srbb_conjunct  $\Rightarrow$  ('a, 's) hml_srbb_conjunct  $\Rightarrow$  bool>
(infix <math>\Leftarrow\psi\Rightarrow> 70)
where
  <math>\Leftarrow\psi\Rightarrow>  $\equiv$  hml_srbb_conj.logical_eq>

```

2.4 Substitution and Congruence

lemma srbb_internal_subst:

```

  assumes
    <math>\chi l \Leftarrow\chi\Rightarrow \chi r>
    <math>\varphi \Leftarrow\text{srbb}\Rightarrow (\text{Internal } \chi l)>
  shows
    <math>\varphi \Leftarrow\text{srbb}\Rightarrow (\text{Internal } \chi r)>
  using assms by force

```

lemma internal_srbb_cong:

```

  assumes <math>\chi l \Leftarrow\chi\Rightarrow \chi r>
  shows <math>(\text{Internal } \chi l) \Leftarrow\text{srbb}\Rightarrow (\text{Internal } \chi r)>
  using assms by auto

```

lemma immconj_cong:

```

  assumes
    <math>\psi_{sl} \text{ ' I } = \psi_{sr} \text{ ' I}>
    <math>\psi_{sl} s \Leftarrow\psi\Rightarrow \psi_{sr} s>
  shows
    <math>\text{ImmConj } (I \cup \{s\}) \psi_{sl} \Leftarrow\text{srbb}\Rightarrow \text{ImmConj } (I \cup \{s\}) \psi_{sr}>
  using assms
  by (auto) (metis (mono_tags, lifting) image_iff)+

```

lemma obs_srbb_cong:

```

  assumes <math>\varphi l \Leftarrow\text{srbb}\Rightarrow \varphi r>
  shows <math>(\text{Obs } \alpha \varphi l) \Leftarrow\chi\Rightarrow (\text{Obs } \alpha \varphi r)>
  using assms by auto

```

2.5 Trivial and Equivalent Formulas

lemma empty_conj_trivial[simp]:

```

  <math>\text{state} \models \text{SRBB ImmConj } \{\} \psi s>
  <math>\text{hml\_srbb\_inner\_models state (Conj } \{\} \psi s)>
  <math>\text{hml\_srbb\_inner\_models state (Obs } \tau \text{ TT)}>
  by simp+

```

lemma empty_branch_conj_tau:

```

  <math>\text{hml\_srbb\_inner\_models state (BranchConj } \tau \text{ TT } \{\} \psi s)>
  by auto

```

lemma stable_conj_parts:

```

  assumes
    <math>\text{hml\_srbb\_inner\_models p (StableConj I } \Psi)>
    <math>i \in I>
  shows
    <math>\text{hml\_srbb\_conjunct\_models p } (\Psi i)>
  using assms by auto

```

lemma branching_conj_parts:

```

  assumes
    <math>\text{hml\_srbb\_inner\_models p (BranchConj } \alpha \varphi I \Psi)>
    <math>i \in I>
  shows
    <math>\text{hml\_srbb\_conjunct\_models p } (\Psi i)>

```

```

using assms by auto

lemma branching_conj_obs:
  assumes <hml_srbbs_inner_models p (BranchConj  $\alpha$   $\varphi$  I  $\Psi$ )>
  shows <hml_srbbs_inner_models p (Obs  $\alpha$   $\varphi$ )>
  using assms by auto

lemma srbbs_obs_ $\tau$ _is_ $\chi$ TT: <Obs  $\tau$  TT  $\Leftarrow \chi \Rightarrow$  Conj {}  $\psi$ s>
  by simp

lemma srbbs_obs_is_empty_branch_conj: <Obs  $\alpha$   $\varphi$   $\Leftarrow \chi \Rightarrow$  BranchConj  $\alpha$   $\varphi$  {}  $\psi$ s>
  by auto

lemma srbbs_TT_is_ $\chi$ TT: <TT  $\Leftarrow$  srbbs  $\Rightarrow$  Internal (Conj {}  $\psi$ s)>
  using lts_tau.refl by force

lemma srbbs_TT_is_empty_conj: <TT  $\Leftarrow$  srbbs  $\Rightarrow$  ImmConj {}  $\psi$ s>
  by simp

```

Positive conjuncts in stable conjunctions can be replaced by negative ones.

```

lemma srbbs_stable_Neg_normalizable:
  assumes
    <i  $\in$  I> < $\Psi$  i = Pos  $\chi$ >
    < $\Psi'$  =  $\Psi$ (i := Neg (StableConj {left} ( $\lambda$ _. Neg  $\chi$ )))>
  shows
    <Internal (StableConj I  $\Psi$ )  $\Leftarrow$  srbbs  $\Rightarrow$  Internal (StableConj I  $\Psi'$ )>
proof (rule logical_eqI)
  fix p
  assume <p  $\models$  SRBB Internal (StableConj I  $\Psi$ )>
  then obtain p' where p'_spec: <p  $\Rightarrow$  p'> <hml_srbbs_inner_models p' (StableConj I  $\Psi$ )> by auto
  hence <stable_state p'> by auto
  from p'_spec have < $\exists$  p''. p'  $\Rightarrow$  p''  $\wedge$  hml_srbbs_inner_models p''  $\chi$ >
  using assms(1,2) by auto
  with <stable_state p'> have <hml_srbbs_inner_models p'  $\chi$ >
  using stable_state_stable by blast
  hence <hml_srbbs_conjunct_models p' (Neg (StableConj {left} ( $\lambda$ _. Neg  $\chi$ )))>
  using <stable_state p'> stable_state_stable by (auto, blast)
  hence <hml_srbbs_inner_models p' (StableConj I  $\Psi'$ )>
  unfolding assms(3) using p'_spec by auto
  thus <p  $\models$  SRBB hml_srbbs.Internal (StableConj I  $\Psi'$ )>
  using <p  $\Rightarrow$  p'> by auto
next
  fix p
  assume <p  $\models$  SRBB Internal (StableConj I  $\Psi'$ )>
  then obtain p' where p'_spec: <p  $\Rightarrow$  p'> <hml_srbbs_inner_models p' (StableConj I  $\Psi'$ )> by
auto
  hence <stable_state p'> by auto
  from p'_spec(2) have other_conjuncts: < $\forall j \in I. i \neq j \longrightarrow$  hml_srbbs_conjunct_models p' ( $\Psi$  j)>
  using assms stable_conj_parts fun_upd_apply by metis
  from p'_spec(2) have <hml_srbbs_conjunct_models p' ( $\Psi'$  i)>
  using assms(1) stable_conj_parts by blast
  hence <hml_srbbs_conjunct_models p' (Neg (StableConj {left} ( $\lambda$ _. Neg  $\chi$ )))>
  unfolding assms(3) by auto
  with <stable_state p'> have <hml_srbbs_inner_models p'  $\chi$ >
  using stable_state_stable by (auto, metis silent_reachable.simps)
  then have <hml_srbbs_conjunct_models p' (Pos  $\chi$ )>
  using lts_tau.refl by fastforce
  hence <hml_srbbs_inner_models p' (StableConj I  $\Psi$ )>
  using p'_spec assms other_conjuncts by auto
  thus <p  $\models$  SRBB hml_srbbs.Internal (StableConj I  $\Psi$ )>
  using p'_spec(1) by auto

```

qed

All positive conjuncts in stable conjunctions can be replaced by negative ones at once.

lemma srbb_stable_Neg_normalizable_set:

```

  assumes
    <Ψ' = (λi. case (Ψ i) of
      Pos χ ⇒ Neg (StableConj {left} (λ_. Neg χ)) |
      Neg χ ⇒ Neg χ)>
  shows
    <Internal (StableConj I Ψ) ⇐srbb⇒ Internal (StableConj I Ψ')>
proof (rule logical_eqI)
  fix p
  assume <p ⊨SRBB Internal (StableConj I Ψ)>
  then obtain p' where p'_spec: <p ⇒ p'> <hml_srbb_inner_models p' (StableConj I Ψ)> by auto
  hence <stable_state p'> by auto
  from p'_spec have
    <∀χ i. i∈I ∧ Ψ i = Pos χ ⟶ (∃p''. p' ⇒ p'' ∧ hml_srbb_inner_models p'' χ)>
  by fastforce
  with <stable_state p'> have <∀χ i. i∈I ∧ Ψ i = Pos χ ⟶ hml_srbb_inner_models p' χ>
  using stable_state_stable by blast
  hence pos_rewrite: <∀χ i. i∈I ∧ Ψ i = Pos χ ⟶
    hml_srbb_conjunct_models p' (Neg (StableConj {left} (λ_. Neg χ)))>
  using <stable_state p'> stable_state_stable by (auto, blast)
  hence <hml_srbb_inner_models p' (StableConj I Ψ')>
  unfolding assms using p'_spec
  by (auto, metis (no_types, lifting) hml_srbb_conjunct.exhaust hml_srbb_conjunct.simps(5,6)
    pos_rewrite)
  thus <p ⊨SRBB Internal (StableConj I Ψ')>
  using <p ⇒ p'> by auto
next
  fix p
  assume <p ⊨SRBB Internal (StableConj I Ψ')>
  then obtain p' where p'_spec: <p ⇒ p'> <hml_srbb_inner_models p' (StableConj I Ψ')> by
  auto
  hence <stable_state p'> by auto
  from p'_spec(2) have other_conjuncts:
    <∀χ i. i∈I ∧ Ψ i = Neg χ ⟶ hml_srbb_conjunct_models p' (Ψ i)>
  using assms stable_conj_parts by (metis hml_srbb_conjunct.simps(6))
  from p'_spec(2) have <∀χ i. i∈I ∧ Ψ i = Pos χ ⟶ hml_srbb_conjunct_models p' (Ψ' i)>
  using assms(1) stable_conj_parts by blast
  hence <∀χ i. i∈I ∧ Ψ i = Pos χ ⟶
    hml_srbb_conjunct_models p' (Neg (StableConj {left} (λ_. Neg χ)))>
  unfolding assms by auto
  with <stable_state p'> have <∀χ i. i∈I ∧ Ψ i = Pos χ ⟶ hml_srbb_inner_models p' χ>
  using stable_state_stable by (auto, metis silent_reachable.simps)
  then have pos_conjuncts:
    <∀χ i. i∈I ∧ Ψ i = Pos χ ⟶ hml_srbb_conjunct_models p' (Pos χ)>
  using hml_srbb_conjunct_models.simps(1) silent_reachable.simps by blast
  hence <hml_srbb_inner_models p' (StableConj I Ψ)>
  using p'_spec assms other_conjuncts
  by (auto, metis other_conjuncts pos_conjuncts hml_srbb_conjunct.exhaust)
  thus <p ⊨SRBB Internal (StableConj I Ψ)>
  using p'_spec(1) by auto
qed

```

definition conjunctify_distinctions ::

```

  <('s ⇒ ('a, 's) hml_srbb) ⇒ 's ⇒ ('s ⇒ ('a, 's) hml_srbb_conjunct)> where
  <conjunctify_distinctions Φ p ≡ λq.
    case (Φ q) of
      TT ⇒ undefined
    | Internal χ ⇒ Pos χ

```

```

| ImmConj I  $\Psi \Rightarrow \Psi$  (SOME i. i  $\in$  I  $\wedge$  hml_srbb_conj.distinguishes ( $\Psi$  i) p q)>

lemma distinction_conjunctification:
  assumes
    < $\forall q \in I$ . distinguishes ( $\Phi$  q) p q>
  shows
    < $\forall q \in I$ . hml_srbb_conj.distinguishes ((conjunctify_distinctions  $\Phi$  p) q) p q>
  unfolding conjunctify_distinctions_def
proof
  fix q
  assume q_I: <q  $\in$  I>
  show <hml_srbb_conj.distinguishes
    (case  $\Phi$  q of hml_srbb.Internal x  $\Rightarrow$  hml_srbb_conjunct.Pos x
    | ImmConj I  $\Psi \Rightarrow \Psi$  (SOME i. i  $\in$  I  $\wedge$  hml_srbb_conj.distinguishes ( $\Psi$  i) p q))
    p q>
  proof (cases < $\Phi$  q>)
    case TT
    then show ?thesis using assms q_I by fastforce
  next
    case (Internal  $\chi$ )
    then show ?thesis using assms q_I by auto
  next
    case (ImmConj J  $\Psi$ )
    then have < $\exists i \in J$ . hml_srbb_conj.distinguishes ( $\Psi$  i) p q>
      using assms q_I by auto
    then show ?thesis
      by (metis (mono_tags, lifting) ImmConj hml_srbb.simps(11) someI)
  qed
qed

lemma distinction_combination:
  fixes p q
  defines
    < $Q\alpha \equiv \{q'. q \twoheadrightarrow q' \wedge (\nexists \varphi. \text{distinguishes } \varphi \text{ p } q')\}$ >
  assumes
    <p  $\mapsto_a \alpha$  p'>
    < $\forall q' \in Q\alpha$ .
       $\forall q''. q' \mapsto_a \alpha q'' \longrightarrow (\text{distinguishes } (\Phi q'') \text{ p' } q'')$ >
  shows
    < $\forall q' \in Q\alpha$ .
      hml_srbb_inner.distinguishes (Obs  $\alpha$  (ImmConj {q''.  $\exists q''' \in Q\alpha. q''' \mapsto_a \alpha q''$ }
      (conjunctify_distinctions  $\Phi$  p')))) p q'>
proof -
  have < $\forall q' \in Q\alpha. \forall q'' \in \{q''. q' \mapsto_a \alpha q''\}$ .
    hml_srbb_conj.distinguishes ((conjunctify_distinctions  $\Phi$  p') q'') p' q''>
  proof clarify
    fix q' q''
    assume <q'  $\in Q\alpha$ > <q'  $\mapsto_a \alpha$  q''>
    thus <hml_srbb_conj.distinguishes (conjunctify_distinctions  $\Phi$  p' q'') p' q''>
      using distinction_conjunctification assms(3)
      by (metis mem_Collect_eq)
  qed
  hence < $\forall q' \in Q\alpha. \forall q'' \in \{q''. \exists q_1' \in Q\alpha. q_1' \mapsto_a \alpha q''\}$ .
    hml_srbb_conj.distinguishes ((conjunctify_distinctions  $\Phi$  p') q'') p' q''> by blast
  hence < $\forall q' \in Q\alpha. \forall q''. q' \mapsto_a \alpha q''$ 
     $\longrightarrow \text{distinguishes } (\text{ImmConj } \{q''. \exists q_1' \in Q\alpha. q_1' \mapsto_a \alpha q''\}$ 
    (conjunctify_distinctions  $\Phi$  p')) p' q''> by auto
  thus < $\forall q' \in Q\alpha$ .
    hml_srbb_inner.distinguishes (Obs  $\alpha$  (ImmConj {q''.  $\exists q''' \in Q\alpha. q''' \mapsto_a \alpha q''$ }
    (conjunctify_distinctions  $\Phi$  p')))) p q'>
  by (auto) (metis assms(2))+

```

qed

```

definition conjunctify_distinctions_dual ::
  <('s  $\Rightarrow$  ('a, 's) hml_srbb)  $\Rightarrow$  's  $\Rightarrow$  ('s  $\Rightarrow$  ('a, 's) hml_srbb_conjunct)> where
  <conjunctify_distinctions_dual  $\Phi$  p  $\equiv$   $\lambda$ q.
    case ( $\Phi$  q) of
      TT  $\Rightarrow$  undefined
    | Internal  $\chi$   $\Rightarrow$  Neg  $\chi$ 
    | ImmConj I  $\Psi$   $\Rightarrow$ 
      (case  $\Psi$  (SOME i. i  $\in$  I  $\wedge$  hml_srbb_conj.distinguishes ( $\Psi$  i) q p) of
        Pos  $\chi$   $\Rightarrow$  Neg  $\chi$  | Neg  $\chi$   $\Rightarrow$  Pos  $\chi$ )>

```

```

lemma dual_conjunct:
  assumes
    <hml_srbb_conj.distinguishes  $\psi$  p q>
  shows
    <hml_srbb_conj.distinguishes (case  $\psi$  of
      hml_srbb_conjunct.Pos  $\chi$   $\Rightarrow$  hml_srbb_conjunct.Neg  $\chi$ 
    | hml_srbb_conjunct.Neg  $\chi$   $\Rightarrow$  hml_srbb_conjunct.Pos  $\chi$ ) q p>
  using assms
  by (cases  $\psi$ , auto)

```

```

lemma distinction_conjunctification_dual:
  assumes
    < $\forall$ q $\in$ I. distinguishes ( $\Phi$  q) q p>
  shows
    < $\forall$ q $\in$ I. hml_srbb_conj.distinguishes (conjunctify_distinctions_dual  $\Phi$  p q) p q>
  unfolding conjunctify_distinctions_dual_def

```

proof

```

  fix q
  assume q_I: <q $\in$ I>
  show <hml_srbb_conj.distinguishes
    (case  $\Phi$  q of hml_srbb.Internal x  $\Rightarrow$  hml_srbb_conjunct.Neg x
    | ImmConj I  $\Psi$   $\Rightarrow$ 
      ( case  $\Psi$  (SOME i. i  $\in$  I  $\wedge$  hml_srbb_conj.distinguishes ( $\Psi$  i) q p) of
        hml_srbb_conjunct.Pos x  $\Rightarrow$  hml_srbb_conjunct.Neg x
      | hml_srbb_conjunct.Neg x  $\Rightarrow$  hml_srbb_conjunct.Pos x))
    p q>
  proof (cases < $\Phi$  q>)
    case TT
    then show ?thesis using assms q_I by fastforce
  next
    case (Internal  $\chi$ )
    then show ?thesis using assms q_I by auto
  next
    case (ImmConj J  $\Psi$ )
    then have < $\exists$ i  $\in$  J. hml_srbb_conj.distinguishes ( $\Psi$  i) q p>
      using assms q_I by auto
    hence <hml_srbb_conj.distinguishes (case  $\Psi$ 
      (SOME i. i  $\in$  J  $\wedge$  hml_srbb_conj.distinguishes ( $\Psi$  i) q p) of
        hml_srbb_conjunct.Pos x  $\Rightarrow$  hml_srbb_conjunct.Neg x
      | hml_srbb_conjunct.Neg x  $\Rightarrow$  hml_srbb_conjunct.Pos x) p q>
      by (metis (no_types, lifting) dual_conjunct someI_ex)
    then show ?thesis unfolding ImmConj by auto
  qed

```

qed

qed

```

lemma distinction_conjunctification_two_way:
  fixes  $\Phi$  p I
  defines
    <conjfy q  $\equiv$ 

```

```

      (if distinguishes ( $\Phi$  q) p q
       then conjunctify_distinctions  $\Phi$ 
       else conjunctify_distinctions_dual  $\Phi$ ) p q>
    assumes
      < $\forall q \in I. \text{distinguishes } (\Phi \text{ } q) \text{ } p \text{ } q \vee \text{distinguishes } (\Phi \text{ } q) \text{ } q \text{ } p$ >
    shows
      < $\forall q \in I. \text{hml\_srbb\_conj.distinguishes } (\text{conjfy } q) \text{ } p \text{ } q$ >
  proof safe
    fix q
    assume < $q \in I$ >
    then consider <distinguishes ( $\Phi$  q) p q>
      | <distinguishes ( $\Phi$  q) q p> using assms by blast
    thus <hml_srbb_conj.distinguishes (conjfy q) p q>
  proof cases
    case 1
    then show ?thesis using distinction_conjunctification conjfy_def
      by (smt (verit) singleton_iff)
  next
    case 2
    then show ?thesis using distinction_conjunctification_dual singleton_iff
      unfolding distinguishes_def conjfy_def
      by (smt (verit, ccfv_threshold))
  qed
qed
end — of lts_tau
end

```

3 Expressiveness Prices

```
theory Energy
  imports "HOL-Library.Extended_Nat"
begin
```

We intend to work on eight-dimensional vectors in an energy game. The dimensions will encode expressiveness prices to HML_{SRBB} formulas. This price is supposed to capture syntactic features needed to describe a certain property and will later be used to select sublogics of specific expressiveness to characterize behavioural equivalences.

The eight dimensions are intended to measure the following properties of formulas:

1. Modal depth (of observations $\langle \alpha \rangle$, (α)),
2. Depth of branching conjunctions (with one observation clause not starting with $\langle \varepsilon \rangle$),
3. Depth of stable conjunctions (that do enforce stability by a $\neg\langle \tau \rangle \top$ -conjunction),
4. Depth of unstable conjunctions (that do not enforce stability by a $\neg\langle \tau \rangle \top$ -conjunction),
5. Depth of immediate conjunctions (that are not preceded by $\langle \varepsilon \rangle$),
6. Maximal modal depth of positive clauses in conjunctions,
7. Maximal modal depth of negative clauses in conjunctions,
8. Depth of negations

```
datatype energy =
  E (modal_depth: <enat>) (br_conj_depth: <enat>) (conj_depth: <enat>)
    (st_conj_depth: <enat>) (imm_conj_depth: <enat>)
    (pos_conjuncts: <enat>) (neg_conjuncts: <enat>) (neg_depth: <enat>)
```

3.1 Comparing and Subtracting Energies

In order to define subtraction on energies, we first lift the orderings $\leq$ and $<$ from `enat` to `energy`.

```
instantiation energy :: order begin
```

```
definition <e1 ≤ e2 ≡
  (case e1 of E a1 b1 c1 d1 e1 f1 g1 h1 ⇒ (
    case e2 of E a2 b2 c2 d2 e2 f2 g2 h2 ⇒
      (a1 ≤ a2 ∧ b1 ≤ b2 ∧ c1 ≤ c2 ∧ d1 ≤ d2 ∧ e1 ≤ e2 ∧ f1 ≤ f2 ∧ g1 ≤ g2 ∧ h1 ≤ h2)
  ))>
```

```
definition <(x::energy) < y = (x ≤ y ∧ ¬ y ≤ x)>
```

```
instance proof
  fix e1 e2 e3 :: energy
  show <e1 ≤ e1> unfolding less_eq_energy_def by (simp add: energy.case_eq_if)
  show <e1 ≤ e2 ⇒ e2 ≤ e3 ⇒ e1 ≤ e3> unfolding less_eq_energy_def
    by (smt (z3) energy.case_eq_if order_trans)
  show <e1 < e2 = (e1 ≤ e2 ∧ ¬ e2 ≤ e1)> using less_energy_def .
  show <e1 ≤ e2 ⇒ e2 ≤ e1 ⇒ e1 = e2> unfolding less_eq_energy_def
    by (smt (z3) energy.case_eq_if energy.expand nle_le)
qed
```

```
lemma leq_components[simp]:
  shows <e1 ≤ e2 ≡
    (modal_depth e1 ≤ modal_depth e2 ∧ br_conj_depth e1 ≤ br_conj_depth e2
     ∧ conj_depth e1 ≤ conj_depth e2 ∧ st_conj_depth e1 ≤ st_conj_depth e2
```

```

     $\wedge$  imm_conj_depth e1  $\leq$  imm_conj_depth e2  $\wedge$  pos_conjuncts e1  $\leq$  pos_conjuncts e2
     $\wedge$  neg_conjuncts e1  $\leq$  neg_conjuncts e2  $\wedge$  neg_depth e1  $\leq$  neg_depth e2) >
  unfolding less_eq_energy_def by (simp add: energy.case_eq_if)

lemma energy_leq_cases:
  assumes
    <modal_depth e1  $\leq$  modal_depth e2> <br_conj_depth e1  $\leq$  br_conj_depth e2>
    <conj_depth e1  $\leq$  conj_depth e2> <st_conj_depth e1  $\leq$  st_conj_depth e2>
    <imm_conj_depth e1  $\leq$  imm_conj_depth e2> <pos_conjuncts e1  $\leq$  pos_conjuncts e2>
    <neg_conjuncts e1  $\leq$  neg_conjuncts e2> <neg_depth e1  $\leq$  neg_depth e2>
  shows
    <e1  $\leq$  e2>
  using assms unfolding leq_components by blast

end

abbreviation somewhere_larger where <somewhere_larger e1 e2  $\equiv$   $\neg$ (e1  $\geq$  e2)>

lemma somewhere_larger_eq:
  assumes
    <somewhere_larger e1 e2>
  shows
    <modal_depth e1 < modal_depth e2  $\vee$  br_conj_depth e1 < br_conj_depth e2
     $\vee$  conj_depth e1 < conj_depth e2  $\vee$  st_conj_depth e1 < st_conj_depth e2
     $\vee$  imm_conj_depth e1 < imm_conj_depth e2  $\vee$  pos_conjuncts e1 < pos_conjuncts e2
     $\vee$  neg_conjuncts e1 < neg_conjuncts e2  $\vee$  neg_depth e1 < neg_depth e2>
  by (smt (z3) assms energy.case_eq_if less_eq_energy_def linorder_le_less_linear)

instantiation energy :: minus
begin

definition minus_energy_def[simp]: <e1 - e2  $\equiv$  E
  ((modal_depth e1) - (modal_depth e2))
  ((br_conj_depth e1) - (br_conj_depth e2))
  ((conj_depth e1) - (conj_depth e2))
  ((st_conj_depth e1) - (st_conj_depth e2))
  ((imm_conj_depth e1) - (imm_conj_depth e2))
  ((pos_conjuncts e1) - (pos_conjuncts e2))
  ((neg_conjuncts e1) - (neg_conjuncts e2))
  ((neg_depth e1) - (neg_depth e2))>

instance ..

end

```

Some lemmas to ease the manipulation of expressions using subtraction on energies.

```

lemma energy_minus[simp]:
  shows <E a1 b1 c1 d1 e1 f1 g1 h1 - E a2 b2 c2 d2 e2 f2 g2 h2
    = E (a1 - a2) (b1 - b2) (c1 - c2) (d1 - d2)
      (e1 - e2) (f1 - f2) (g1 - g2) (h1 - h2)>
  unfolding minus_energy_def somewhere_larger_eq by simp

lemma minus_component_leq:
  assumes
    <s  $\leq$  x>
    <x  $\leq$  y>
  shows
    <modal_depth (x - s)  $\leq$  modal_depth (y - s)>
    <br_conj_depth (x - s)  $\leq$  br_conj_depth (y - s)>
    <conj_depth (x - s)  $\leq$  conj_depth (y - s)>
    <st_conj_depth (x - s)  $\leq$  st_conj_depth (y - s)>

```

```

    <imm_conj_depth (x - s) ≤ imm_conj_depth (y - s)>
    <pos_conjuncts (x - s) ≤ pos_conjuncts (y - s)>
    <neg_conjuncts (x - s) ≤ neg_conjuncts (y - s)>
    <neg_depth (x - s) ≤ neg_depth (y - s)>
  using assms by (simp_all) (metis add.commute add_diff_assoc_enat le_iff_add)+

lemma enat_diff_mono:
  assumes <(i::enat) ≤ j>
  shows <i - k ≤ j - k>
proof (cases i)
  case (enat iN)
  show ?thesis
  proof (cases j)
    case (enat jN)
    then show ?thesis
    using assms enat_ile by (cases k, fastforce+)
  next
    case infinity
    then show ?thesis using assms by auto
  qed
next
  case infinity
  hence <j = ∞>
  using assms by auto
  then show ?thesis by auto
qed

```

We further show that the subtraction of energies is decreasing.

```

lemma energy_diff_mono:
  fixes s :: energy
  shows <mono_on UNIV (λx. x - s)>
  unfolding mono_on_def
  by (auto simp add: enat_diff_mono)

lemma gets_smaller:
  fixes s :: energy
  shows <(λx. x - s) x ≤ x>
  by (auto)
  (metis add.commute add_diff_cancel_enat enat_diff_mono idiff_infinity idiff_infinity_right
    le_iff_add not_infinity_eq zero_le)+

lemma mono_subtract:
  assumes <x ≤ x'>
  shows <(λx. x - (E a b c d e f g h)) x ≤ (λx. x - (E a b c d e f g h)) x'>
  using assms enat_diff_mono by force

```

Abbreviations for performing subtraction in the energy games.

```

abbreviation <subtract_fn a b c d e f g h ≡
  (λx. if somewhere_larger x (E a b c d e f g h) then None else Some (x - (E a b c d e f g h)))>

abbreviation <subtract a b c d e f g h ≡ Some (subtract_fn a b c d e f g h)>

```

3.2 Minimum Updates

Two energy updates that replace the first component with the minimum of two other components.

```

definition <min1_6 e ≡ case e of E a b c d e f g h ⇒ Some (E (min a f) b c d e f g h)>
definition <min1_7 e ≡ case e of E a b c d e f g h ⇒ Some (E (min a g) b c d e f g h)>

```

Abbreviations for identity update.

```
abbreviation <id_up ≡ Some Some>
```

lift order to options

```
instantiation option :: (order) order
begin
```

```
definition less_eq_option_def[simp]:
  <less_eq_option (optA :: 'a option) optB ≡
    case optA of
      (Some a) ⇒
        (case optB of
          (Some b) ⇒ a ≤ b |
          None ⇒ False) |
      None ⇒ True>
```

```
definition less_option_def[simp]:
  <less_option (optA :: 'a option) optB ≡ (optA ≤ optB ∧ ¬ optB ≤ optA)>
```

```
instance proof standard
  fix x y :: <'a option>
  show <(x < y) = (x ≤ y ∧ ¬ y ≤ x)> by simp
next
  fix x :: <'a option>
  show <x ≤ x>
    by (simp add: option.case_eq_if)
next
  fix x y z :: <'a option>
  assume <x ≤ y> <y ≤ z>
  thus <x ≤ z>
    unfolding less_eq_option_def
    by (metis option.case_eq_if order_trans)
next
  fix x y :: <'a option>
  assume <x ≤ y> <y ≤ x>
  thus <x = y>
    unfolding less_eq_option_def
    by (smt (z3) inf.absorb_iff2 le_boolD option.case_eq_if option.split_sel order_antisym)
qed

end
```

Again, we prove some lemmas to ease the manipulation of expressions using minimum updates.

```
lemma min_1_6_simps[simp]:
  shows <modal_depth (the (min1_6 e)) = min (modal_depth e) (pos_conjuncts e)>
    <br_conj_depth (the (min1_6 e)) = br_conj_depth e>
    <conj_depth (the (min1_6 e)) = conj_depth e>
    <st_conj_depth (the (min1_6 e)) = st_conj_depth e>
    <imm_conj_depth (the (min1_6 e)) = imm_conj_depth e>
    <pos_conjuncts (the (min1_6 e)) = pos_conjuncts e>
    <neg_conjuncts (the (min1_6 e)) = neg_conjuncts e>
    <neg_depth (the (min1_6 e)) = neg_depth e>
  unfolding min1_6_def by (simp_all add: energy.case_eq_if)
```

```
lemma min_1_7_simps[simp]:
  shows <modal_depth (the (min1_7 e)) = min (modal_depth e) (neg_conjuncts e)>
    <br_conj_depth (the (min1_7 e)) = br_conj_depth e>
    <conj_depth (the (min1_7 e)) = conj_depth e>
    <st_conj_depth (the (min1_7 e)) = st_conj_depth e>
    <imm_conj_depth (the (min1_7 e)) = imm_conj_depth e>
    <pos_conjuncts (the (min1_7 e)) = pos_conjuncts e>
```

```

    <neg_conjuncts (the (min1_7 e)) = neg_conjuncts e>
    <neg_depth (the (min1_7 e)) = neg_depth e>
  unfolding min1_7_def by (simp_all add: energy.case_eq_if)

lemma min_1_6_some:
  shows <min1_6 e ≠ None>
  unfolding min1_6_def
  using energy.case_eq_if by blast

lemma min_1_7_some:
  shows <min1_7 e ≠ None>
  unfolding min1_7_def
  using energy.case_eq_if by blast

lemma min_1_7_lower_end:
  assumes <(Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7) = None>
  shows <neg_depth e = 0>
  using assms
  by (smt (verit, ccfv_threshold) bind.bind_lunit energy.sel ileI1
    leq_components min_1_7_some not_gr_zero one_eSuc zero_le)

lemma min_1_7_subtr_simp:
  shows <(Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7)
    = (if neg_depth e = 0 then None
      else Some (E (min (modal_depth e) (neg_conjuncts e)) (br_conj_depth e) (conj_depth e)
        (st_conj_depth e) (imm_conj_depth e) (pos_conjuncts e)
        (neg_conjuncts e) (neg_depth e - 1)))>
  using min_1_7_lower_end
  by (auto simp add: min1_7_def)

lemma min_1_7_subtr_mono:
  shows <mono (λe. Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7)>
proof
  fix e1 e2 :: energy
  assume <e1 ≤ e2>
  thus <(λe. Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7) e1
    ≤ (λe. Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7) e2>
  unfolding min_1_7_subtr_simp
  by (auto simp add: min.coboundedI1 min.coboundedI2 enat_diff_mono)
qed

lemma min_1_6_subtr_simp:
  shows <(Option.bind ((subtract_fn 0 1 1 0 0 0 0 0) e) min1_6)
    = (if br_conj_depth e = 0 ∨ conj_depth e = 0 then None
      else Some (E (min (modal_depth e) (pos_conjuncts e)) (br_conj_depth e - 1)
        (conj_depth e - 1) (st_conj_depth e) (imm_conj_depth e)
        (pos_conjuncts e) (neg_conjuncts e) (neg_depth e)))>
  by (auto simp add: min1_6_def ileI1 one_eSuc)

instantiation energy :: Sup
begin

definition <Sup ee ≡ E
  (Sup (modal_depth ' ee)) (Sup (br_conj_depth ' ee)) (Sup (conj_depth ' ee))
  (Sup (st_conj_depth ' ee)) (Sup (imm_conj_depth ' ee)) (Sup (pos_conjuncts ' ee))
  (Sup (neg_conjuncts ' ee)) (Sup (neg_depth ' ee))>

instance ..
end

```

end

3.3 Components of Expressiveness Prices

```
theory Expressiveness_Price
  imports HML_SRBB Energy
begin
```

The (maximal) modal depth (of observations $\langle \alpha \rangle$, (α)) is increased on each Obs and BranchConj.

```
primrec
  modal_depth_srbb :: <('act, 'i) hml_srbb  $\Rightarrow$  enat>
  and modal_depth_srbb_inner :: <('act, 'i) hml_srbb_inner  $\Rightarrow$  enat>
  and modal_depth_srbb_conjunct :: <('act, 'i) hml_srbb_conjunct  $\Rightarrow$  enat> where
  <modal_depth_srbb TT = 0> |
  <modal_depth_srbb (Internal  $\chi$ ) = modal_depth_srbb_inner  $\chi$ > |
  <modal_depth_srbb (ImmConj I  $\psi$ s) = Sup ((modal_depth_srbb_conjunct  $\circ$   $\psi$ s) ' I)> |

  <modal_depth_srbb_inner (Obs  $\alpha$   $\varphi$ ) = 1 + modal_depth_srbb  $\varphi$ > |
  <modal_depth_srbb_inner (Conj I  $\psi$ s) =
    Sup ((modal_depth_srbb_conjunct  $\circ$   $\psi$ s) ' I)> |
  <modal_depth_srbb_inner (StableConj I  $\psi$ s) =
    Sup ((modal_depth_srbb_conjunct  $\circ$   $\psi$ s) ' I)> |
  <modal_depth_srbb_inner (BranchConj a  $\varphi$  I  $\psi$ s) =
    Sup ({1 + modal_depth_srbb  $\varphi$ }  $\cup$  ((modal_depth_srbb_conjunct  $\circ$   $\psi$ s) ' I))> |

  <modal_depth_srbb_conjunct (Pos  $\chi$ ) = modal_depth_srbb_inner  $\chi$ > |
  <modal_depth_srbb_conjunct (Neg  $\chi$ ) = modal_depth_srbb_inner  $\chi$ >
```

The depth of branching conjunctions (with one observation clause not starting with $\langle \varepsilon \rangle$) is increased on each: BranchConj.

```
primrec
  branching_conjunction_depth :: <('a, 's) hml_srbb  $\Rightarrow$  enat>
  and branch_conj_depth_inner :: <('a, 's) hml_srbb_inner  $\Rightarrow$  enat>
  and branch_conj_depth_conjunct :: <('a, 's) hml_srbb_conjunct  $\Rightarrow$  enat> where
  <branching_conjunction_depth TT = 0> |
  <branching_conjunction_depth (Internal  $\chi$ ) = branch_conj_depth_inner  $\chi$ > |
  <branching_conjunction_depth (ImmConj I  $\psi$ s) =
    Sup ((branch_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)> |

  <branch_conj_depth_inner (Obs _  $\varphi$ ) = branching_conjunction_depth  $\varphi$ > |
  <branch_conj_depth_inner (Conj I  $\psi$ s) = Sup ((branch_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)> |
  <branch_conj_depth_inner (StableConj I  $\psi$ s) =
    Sup ((branch_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)> |
  <branch_conj_depth_inner (BranchConj _  $\varphi$  I  $\psi$ s) =
    1 + Sup ({branching_conjunction_depth  $\varphi$ }  $\cup$  ((branch_conj_depth_conjunct  $\circ$   $\psi$ s) ' I))> |

  <branch_conj_depth_conjunct (Pos  $\chi$ ) = branch_conj_depth_inner  $\chi$ > |
  <branch_conj_depth_conjunct (Neg  $\chi$ ) = branch_conj_depth_inner  $\chi$ >
```

The depth of stable conjunctions (that do enforce stability by a $\neg\langle \tau \rangle \top$ -conjunct) is increased on each StableConj. Note that if the StableConj is empty (has no other conjuncts), it is still counted.

```
primrec
  stable_conjunction_depth :: <('a, 's) hml_srbb  $\Rightarrow$  enat>
  and st_conj_depth_inner :: <('a, 's) hml_srbb_inner  $\Rightarrow$  enat>
  and st_conj_depth_conjunct :: <('a, 's) hml_srbb_conjunct  $\Rightarrow$  enat> where
  <stable_conjunction_depth TT = 0> |
  <stable_conjunction_depth (Internal  $\chi$ ) = st_conj_depth_inner  $\chi$ > |
  <stable_conjunction_depth (ImmConj I  $\psi$ s) = Sup ((st_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)> |

  <st_conj_depth_inner (Obs _  $\varphi$ ) = stable_conjunction_depth  $\varphi$ > |
```

```

<st_conj_depth_inner (Conj I  $\psi$ s) = Sup ((st_conj_depth_conjunct  $\circ \psi$ s) ' I)> |
<st_conj_depth_inner (StableConj I  $\psi$ s) = 1 + Sup ((st_conj_depth_conjunct  $\circ \psi$ s) ' I)> |
<st_conj_depth_inner (BranchConj _  $\varphi$  I  $\psi$ s) =
  Sup ({stable_conjunction_depth  $\varphi$ }  $\cup$  ((st_conj_depth_conjunct  $\circ \psi$ s) ' I))> |

<st_conj_depth_conjunct (Pos  $\chi$ ) = st_conj_depth_inner  $\chi$ > |
<st_conj_depth_conjunct (Neg  $\chi$ ) = st_conj_depth_inner  $\chi$ >

```

The depth of unstable conjunctions (that do not enforce stability by a $\neg\langle\tau\rangle\top$ -conjunction) is increased on each:

- ImmConj if there are conjuncts (i.e. $\bigwedge\{\}$ is not counted)
- Conj if there are conjuncts, (i.e. the conjunction is not empty)
- BranchConj.

primrec

```

unstable_conjunction_depth :: <('a, 's) hml_srbb  $\Rightarrow$  enat>
and inst_conj_depth_inner :: <('a, 's) hml_srbb_inner  $\Rightarrow$  enat>
and inst_conj_depth_conjunct :: <('a, 's) hml_srbb_conjunct  $\Rightarrow$  enat> where
<unstable_conjunction_depth TT = 0> |
<unstable_conjunction_depth (Internal  $\chi$ ) = inst_conj_depth_inner  $\chi$ > |
<unstable_conjunction_depth (ImmConj I  $\psi$ s) =
  (if I = {}
    then 0
    else 1 + Sup ((inst_conj_depth_conjunct  $\circ \psi$ s) ' I))> |

<inst_conj_depth_inner (Obs _  $\varphi$ ) = unstable_conjunction_depth  $\varphi$ > |
<inst_conj_depth_inner (Conj I  $\psi$ s) =
  (if I = {}
    then 0
    else 1 + Sup ((inst_conj_depth_conjunct  $\circ \psi$ s) ' I))> |
<inst_conj_depth_inner (StableConj I  $\psi$ s) =
  Sup ((inst_conj_depth_conjunct  $\circ \psi$ s) ' I)> |
<inst_conj_depth_inner (BranchConj _  $\varphi$  I  $\psi$ s) =
  1 + Sup ({unstable_conjunction_depth  $\varphi$ }  $\cup$  ((inst_conj_depth_conjunct  $\circ \psi$ s) ' I))> |

<inst_conj_depth_conjunct (Pos  $\chi$ ) = inst_conj_depth_inner  $\chi$ > |
<inst_conj_depth_conjunct (Neg  $\chi$ ) = inst_conj_depth_inner  $\chi$ >

```

The depth of immediate conjunctions (that are not preceded by $\langle\varepsilon\rangle$) is increased on each ImmConj if there are conjuncts (i.e. $\bigwedge\{\}$ is not counted).

primrec

```

immediate_conjunction_depth :: <('a, 's) hml_srbb  $\Rightarrow$  enat>
and imm_conj_depth_inner :: <('a, 's) hml_srbb_inner  $\Rightarrow$  enat>
and imm_conj_depth_conjunct :: <('a, 's) hml_srbb_conjunct  $\Rightarrow$  enat> where
<immediate_conjunction_depth TT = 0> |
<immediate_conjunction_depth (Internal  $\chi$ ) = imm_conj_depth_inner  $\chi$ > |
<immediate_conjunction_depth (ImmConj I  $\psi$ s) =
  (if I = {}
    then 0
    else 1 + Sup ((imm_conj_depth_conjunct  $\circ \psi$ s) ' I))> |

<imm_conj_depth_inner (Obs _  $\varphi$ ) = immediate_conjunction_depth  $\varphi$ > |
<imm_conj_depth_inner (Conj I  $\psi$ s) = Sup ((imm_conj_depth_conjunct  $\circ \psi$ s) ' I)> |
<imm_conj_depth_inner (StableConj I  $\psi$ s) = Sup ((imm_conj_depth_conjunct  $\circ \psi$ s) ' I)> |
<imm_conj_depth_inner (BranchConj _  $\varphi$  I  $\psi$ s) =
  Sup ({immediate_conjunction_depth  $\varphi$ }  $\cup$  ((imm_conj_depth_conjunct  $\circ \psi$ s) ' I))> |

```

```

<imm_conj_depth_conjunct (Pos  $\chi$ ) = imm_conj_depth_inner  $\chi$ > |
<imm_conj_depth_conjunct (Neg  $\chi$ ) = imm_conj_depth_inner  $\chi$ >

```

The maximal modal depth of positive clauses in conjunctions calculates the modal depth for every positive clause in a conjunction (Pos χ).

primrec

```

max_positive_conjunct_depth :: <('a, 's) hml_srbbs ⇒ enat>
and max_pos_conj_depth_inner :: <('a, 's) hml_srbbs_inner ⇒ enat>
and max_pos_conj_depth_conjunct :: <('a, 's) hml_srbbs_conjunct ⇒ enat> where
<max_positive_conjunct_depth TT = 0> |
<max_positive_conjunct_depth (Internal  $\chi$ ) = max_pos_conj_depth_inner  $\chi$ > |
<max_positive_conjunct_depth (ImmConj I  $\psi$ s) =
  Sup ((max_pos_conj_depth_conjunct ∘  $\psi$ s) ' I)> |

<max_pos_conj_depth_inner (Obs _  $\varphi$ ) = max_positive_conjunct_depth  $\varphi$ > |
<max_pos_conj_depth_inner (Conj I  $\psi$ s) =
  Sup ((max_pos_conj_depth_conjunct ∘  $\psi$ s) ' I)> |
<max_pos_conj_depth_inner (StableConj I  $\psi$ s) =
  Sup ((max_pos_conj_depth_conjunct ∘  $\psi$ s) ' I)> |
<max_pos_conj_depth_inner (BranchConj _  $\varphi$  I  $\psi$ s) =
  Sup ({1 + modal_depth_srbbs  $\varphi$ , max_positive_conjunct_depth  $\varphi$ }
    ∪ ((max_pos_conj_depth_conjunct ∘  $\psi$ s) ' I))> |

<max_pos_conj_depth_conjunct (Pos  $\chi$ ) = modal_depth_srbbs_inner  $\chi$ > |
<max_pos_conj_depth_conjunct (Neg  $\chi$ ) = max_pos_conj_depth_inner  $\chi$ >

```

The maximal modal depth of negative clauses in conjunctions calculates the modal depth for every negative clause in a conjunction (Neg χ).

primrec

```

max_negative_conjunct_depth :: <('a, 's) hml_srbbs ⇒ enat>
and max_neg_conj_depth_inner :: <('a, 's) hml_srbbs_inner ⇒ enat>
and max_neg_conj_depth_conjunct :: <('a, 's) hml_srbbs_conjunct ⇒ enat> where
<max_negative_conjunct_depth TT = 0> |
<max_negative_conjunct_depth (Internal  $\chi$ ) = max_neg_conj_depth_inner  $\chi$ > |
<max_negative_conjunct_depth (ImmConj I  $\psi$ s) =
  Sup ((max_neg_conj_depth_conjunct ∘  $\psi$ s) ' I)> |

<max_neg_conj_depth_inner (Obs _  $\varphi$ ) = max_negative_conjunct_depth  $\varphi$ > |
<max_neg_conj_depth_inner (Conj I  $\psi$ s) =
  Sup ((max_neg_conj_depth_conjunct ∘  $\psi$ s) ' I)> |
<max_neg_conj_depth_inner (StableConj I  $\psi$ s) =
  Sup ((max_neg_conj_depth_conjunct ∘  $\psi$ s) ' I)> |
<max_neg_conj_depth_inner (BranchConj _  $\varphi$  I  $\psi$ s) =
  Sup ({max_negative_conjunct_depth  $\varphi$ } ∪ ((max_neg_conj_depth_conjunct ∘  $\psi$ s) ' I))> |

<max_neg_conj_depth_conjunct (Pos  $\chi$ ) = max_neg_conj_depth_inner  $\chi$ > |
<max_neg_conj_depth_conjunct (Neg  $\chi$ ) = modal_depth_srbbs_inner  $\chi$ >

```

The depth of negations on a path of the syntax tree) is increased on each Neg χ .

primrec

```

negation_depth :: <('a, 's) hml_srbbs ⇒ enat>
and neg_depth_inner :: <('a, 's) hml_srbbs_inner ⇒ enat>
and neg_depth_conjunct :: <('a, 's) hml_srbbs_conjunct ⇒ enat> where
<negation_depth TT = 0> |
<negation_depth (Internal  $\chi$ ) = neg_depth_inner  $\chi$ > |
<negation_depth (ImmConj I  $\psi$ s) = Sup ((neg_depth_conjunct ∘  $\psi$ s) ' I)> |

<neg_depth_inner (Obs _  $\varphi$ ) = negation_depth  $\varphi$ > |
<neg_depth_inner (Conj I  $\psi$ s) = Sup ((neg_depth_conjunct ∘  $\psi$ s) ' I)> |
<neg_depth_inner (StableConj I  $\psi$ s) = Sup ((neg_depth_conjunct ∘  $\psi$ s) ' I)> |

```

```

<neg_depth_inner (BranchConj _  $\varphi$  I  $\psi$ s) =
  Sup ({negation_depth  $\varphi$ }  $\cup$  ((neg_depth_conjunct  $\circ \psi$ s) ' I))> |

<neg_depth_conjunct (Pos  $\chi$ ) = neg_depth_inner  $\chi$ > |
<neg_depth_conjunct (Neg  $\chi$ ) = 1 + neg_depth_inner  $\chi$ >

```

3.4 Properties of Price Components

```

lemma <modal_depth_srbb TT = 0>
  using Sup_enat_def by simp

lemma <modal_depth_srbb (Internal (Obs  $\alpha$  (Internal (BranchConj  $\beta$  TT {}  $\psi$ s2)))) = 2>
  using Sup_enat_def by simp

fun observe_n_alphas :: <'a  $\Rightarrow$  nat  $\Rightarrow$  ('a, nat) hml_srbb> where
  <observe_n_alphas  $\alpha$  0 = TT> |
  <observe_n_alphas  $\alpha$  (Suc n) = Internal (Obs  $\alpha$  (observe_n_alphas  $\alpha$  n))>

lemma obs_n_ $\alpha$ _depth_n: <modal_depth_srbb (observe_n_alphas  $\alpha$  n) = n>
proof (induct n)
  case 0
  show ?case unfolding observe_n_alphas.simps(1) and modal_depth_srbb.simps(2)
    using zero_enat_def and Sup_enat_def by force
next
  case (Suc n)
  then show ?case
    using eSuc_enat plus_1_eSuc(1) by auto
qed

lemma sup_nats_in_enats_infinite: <(SUP x $\in$ N. enat x) =  $\infty$ >
  by (metis Nats_infinite Sup_enat_def enat.inject finite.emptyI finite_imageD inj_on_def)

lemma sucs_of_nats_in_enats_sup_infinite: <(SUP x $\in$ N. 1 + enat x) =  $\infty$ >
  using sup_nats_in_enats_infinite
  by (metis Sup.SUP_cong eSuc_Sup eSuc_infinity image_image image_is_empty plus_1_eSuc(1))

lemma <modal_depth_srbb (ImmConj N ( $\lambda$ n. Pos (Obs  $\alpha$  (observe_n_alphas  $\alpha$  n)))) =  $\infty$ >
  unfolding modal_depth_srbb.simps(3)
  and o_def
  and modal_depth_srbb_conjunct.simps(1)
  and modal_depth_srbb_inner.simps(1)
  and obs_n_ $\alpha$ _depth_n
  by (metis sucs_of_nats_in_enats_sup_infinite)

lemma modal_depth_dominates_pos_conjuncts:
  fixes
     $\varphi$ ::<'a, 's> hml_srbb> and
     $\chi$ ::<'a, 's> hml_srbb_inner> and
     $\psi$ ::<'a, 's> hml_srbb_conjunct>
  shows
    <(max_positive_conjunct_depth  $\varphi$   $\leq$  modal_depth_srbb  $\varphi$ )
     $\wedge$  (max_pos_conj_depth_inner  $\chi$   $\leq$  modal_depth_srbb_inner  $\chi$ )
     $\wedge$  (max_pos_conj_depth_conjunct  $\psi$   $\leq$  modal_depth_srbb_conjunct  $\psi$ )>
  using hml_srbb_hml_srbb_inner_hml_srbb_conjunct.induct[of
    < $\lambda \varphi$ ::<'a, 's> hml_srbb. max_positive_conjunct_depth  $\varphi$   $\leq$  modal_depth_srbb  $\varphi$ >
    < $\lambda \chi$ . max_pos_conj_depth_inner  $\chi$   $\leq$  modal_depth_srbb_inner  $\chi$ >
    < $\lambda \psi$ . max_pos_conj_depth_conjunct  $\psi$   $\leq$  modal_depth_srbb_conjunct  $\psi$ >]
  by (auto simp add: SUP_mono' add_increasing sup.coboundedI1 sup.coboundedI2)

lemma modal_depth_dominates_neg_conjuncts:
  fixes

```

```

 $\varphi :: \langle ('a, 's) \text{ hml\_srbb} \rangle \text{ and}$ 
 $\chi :: \langle ('a, 's) \text{ hml\_srbb\_inner} \rangle \text{ and}$ 
 $\psi :: \langle ('a, 's) \text{ hml\_srbb\_conjunct} \rangle$ 
shows
   $\langle (\text{max\_negative\_conjunct\_depth } \varphi \leq \text{modal\_depth\_srbb } \varphi)$ 
   $\wedge (\text{max\_neg\_conj\_depth\_inner } \chi \leq \text{modal\_depth\_srbb\_inner } \chi)$ 
   $\wedge (\text{max\_neg\_conj\_depth\_conjunct } \psi \leq \text{modal\_depth\_srbb\_conjunct } \psi) \rangle$ 
using hml_srbb_hml_srbb_inner_hml_srbb_conjunct.induct[of
   $\langle \lambda \varphi :: ('a, 's) \text{ hml\_srbb}. \text{max\_negative\_conjunct\_depth } \varphi \leq \text{modal\_depth\_srbb } \varphi$ 
   $\langle \lambda \chi. \text{max\_neg\_conj\_depth\_inner } \chi \leq \text{modal\_depth\_srbb\_inner } \chi \rangle$ 
   $\langle \lambda \psi. \text{max\_neg\_conj\_depth\_conjunct } \psi \leq \text{modal\_depth\_srbb\_conjunct } \psi \rangle]$ 
by (auto simp add: SUP_mono' add_increasing sup.coboundedI1 sup.coboundedI2)

```

3.5 Expressiveness Price Function

The `expressiveness_price` function combines the eight component functions into one.

```

fun expressiveness_price ::  $\langle ('a, 's) \text{ hml\_srbb} \Rightarrow \text{energy} \rangle$  where
   $\langle \text{expressiveness\_price } \varphi =$ 
    E (modal_depth_srbb  $\varphi$ )
      (branching_conjunction_depth  $\varphi$ )
      (unstable_conjunction_depth  $\varphi$ )
      (stable_conjunction_depth  $\varphi$ )
      (immediate_conjunction_depth  $\varphi$ )
      (max_positive_conjunct_depth  $\varphi$ )
      (max_negative_conjunct_depth  $\varphi$ )
      (negation_depth  $\varphi$ )  $\rangle$ 

```

Here, we can see the decomposed price of an immediate conjunction:

```

lemma expressiveness_price_ImmConj_def:
  shows  $\langle \text{expressiveness\_price } (\text{ImmConj } I \ \psi) = \text{E}$ 
    (Sup ((modal_depth_srbb_conjunct  $\circ \psi$ ) ' I))
    (Sup ((branch_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (if I = {} then 0 else 1 + Sup ((inst_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (Sup ((st_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (if I = {} then 0 else 1 + Sup ((imm_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (Sup ((max_pos_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (Sup ((max_neg_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (Sup ((neg_depth_conjunct  $\circ \psi$ ) ' I))  $\rangle$  by simp

```

```

lemma expressiveness_price_ImmConj_non_empty_def:
  assumes  $\langle I \neq \{\} \rangle$ 
  shows  $\langle \text{expressiveness\_price } (\text{ImmConj } I \ \psi) = \text{E}$ 
    (Sup ((modal_depth_srbb_conjunct  $\circ \psi$ ) ' I))
    (Sup ((branch_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (1 + Sup ((inst_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (Sup ((st_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (1 + Sup ((imm_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (Sup ((max_pos_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (Sup ((max_neg_conj_depth_conjunct  $\circ \psi$ ) ' I))
    (Sup ((neg_depth_conjunct  $\circ \psi$ ) ' I))  $\rangle$  using assms by simp

```

```

lemma expressiveness_price_ImmConj_empty_def:
  assumes  $\langle I = \{\} \rangle$ 
  shows  $\langle \text{expressiveness\_price } (\text{ImmConj } I \ \psi) = \text{E } 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \rangle$  using assms
  unfolding expressiveness_price_ImmConj_def by (simp add: bot_enat_def)

```

Formalizing `HMLSRBB` by mutually recursive data types leads to expressiveness price functions of these other types and corresponding definitions and lemmas.

```

fun expr_pr_inner ::  $\langle ('a, 's) \text{ hml\_srbb\_inner} \Rightarrow \text{energy} \rangle$  where

```

```

<expr_pr_inner  $\chi$  =
  E (modal_depth_srbb_inner  $\chi$ )
    (branch_conj_depth_inner  $\chi$ )
    (inst_conj_depth_inner  $\chi$ )
    (st_conj_depth_inner  $\chi$ )
    (imm_conj_depth_inner  $\chi$ )
    (max_pos_conj_depth_inner  $\chi$ )
    (max_neg_conj_depth_inner  $\chi$ )
    (neg_depth_inner  $\chi$ )>

fun expr_pr_conjunct :: <('a, 's) hml_srbb_conjunct  $\Rightarrow$  energy> where
  <expr_pr_conjunct  $\psi$  =
    E (modal_depth_srbb_conjunct  $\psi$ )
      (branch_conj_depth_conjunct  $\psi$ )
      (inst_conj_depth_conjunct  $\psi$ )
      (st_conj_depth_conjunct  $\psi$ )
      (imm_conj_depth_conjunct  $\psi$ )
      (max_pos_conj_depth_conjunct  $\psi$ )
      (max_neg_conj_depth_conjunct  $\psi$ )
      (neg_depth_conjunct  $\psi$ )>

```

3.6 Prices of Certain Formulas

```

context lts_tau
begin

```

For example, here, we establish that the expressiveness price of `Internal  $\chi$` is equal to the expressiveness price of χ .

```

lemma expr_internal_eq:
  shows <expressiveness_price (Internal  $\chi$ ) = expr_pr_inner  $\chi$ >
  by auto

lemma expr_pos:
  assumes <expr_pr_inner  $\chi \leq$  the (min1_6 e)>
  shows <expr_pr_conjunct (Pos  $\chi$ )  $\leq$  e>
  using assms by auto

lemma expr_neg:
  assumes
    <expr_pr_inner  $\chi \leq$  e'>
    <(Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7) = Some e'>
  shows <expr_pr_conjunct (Neg  $\chi$ )  $\leq$  e>
proof -
  have expr_neg: <expr_pr_conjunct (Neg  $\chi$ ) =
    E (modal_depth_srbb_conjunct (Neg  $\chi$ ))
      (branch_conj_depth_conjunct (Neg  $\chi$ ))
      (inst_conj_depth_conjunct (Neg  $\chi$ ))
      (st_conj_depth_conjunct (Neg  $\chi$ ))
      (imm_conj_depth_conjunct (Neg  $\chi$ ))
      (max_pos_conj_depth_conjunct (Neg  $\chi$ ))
      (max_neg_conj_depth_conjunct (Neg  $\chi$ ))
      (neg_depth_conjunct (Neg  $\chi$ ))>
  using expr_pr_conjunct.simps by blast
  have neg_ups:
    <modal_depth_srbb_conjunct (Neg  $\chi$ ) = modal_depth_srbb_inner  $\chi$ >
    <(branch_conj_depth_conjunct (Neg  $\chi$ )) = branch_conj_depth_inner  $\chi$ >
    <inst_conj_depth_conjunct (Neg  $\chi$ ) = inst_conj_depth_inner  $\chi$ >
    <st_conj_depth_conjunct (Neg  $\chi$ ) = st_conj_depth_inner  $\chi$ >
    <imm_conj_depth_conjunct (Neg  $\chi$ ) = imm_conj_depth_inner  $\chi$ >
    <max_pos_conj_depth_conjunct (Neg  $\chi$ ) = max_pos_conj_depth_inner  $\chi$ >
    <max_neg_conj_depth_conjunct (Neg  $\chi$ ) = modal_depth_srbb_inner  $\chi$ >

```

```

    <neg_depth_conjunct (Neg  $\chi$ ) = 1 + neg_depth_inner  $\chi$ >
  by simp+
obtain e1 e2 e3 e4 e5 e6 e7 e8 where e_def: <e = E e1 e2 e3 e4 e5 e6 e7 e8>
  by (metis energy.exhaust_sel)
hence is_some: <(subtract_fn 0 0 0 0 0 0 0 1 e = Some (E e1 e2 e3 e4 e5 e6 e7 (e8-1)))>
  using assms bind_eq_None_conv by fastforce
hence <modal_depth_srbb_inner  $\chi \leq (\min e1 e7)$ >
  using assms expr_pr_inner.simps leq_components min_1_7_subtr_simp e_def
  by (metis energy.sel(1) energy.sel(7) option.discI option.inject)
moreover have <neg_depth_inner  $\chi \leq (e8-1)$ >
  using e_def is_some energy_minus leq_components min_1_7_simps assms
  by (smt (verit, ccfv_threshold) bind.bind_lunit energy.sel(8) expr_pr_inner.simps option.sel)
moreover hence <neg_depth_conjunct (Neg  $\chi$ )  $\leq e8$ >
  using <neg_depth_conjunct (Neg  $\chi$ ) = 1 + neg_depth_inner  $\chi$ >
  by (metis is_some add_diff_assoc_enat add_diff_cancel_enat e_def enat.simps(3)
    enat_defs(2) enat_diff_mono energy.sel(8) leq_components linorder_not_less
    option.distinct(1) order_le_less)
ultimately show <expr_pr_conjunct (Neg  $\chi$ )  $\leq e$ >
  using expr_neg e_def is_some assms neg_ups assms leq_components min_1_7_subtr_simp
  by (metis energy.sel expr_pr_inner.simps min.bounded_iff option.distinct(1) option.inject)
qed

lemma expr_obs:
  assumes
    <expressiveness_price  $\varphi \leq e'$ >
    <subtract_fn 1 0 0 0 0 0 0 0 e = Some e'>
  shows <expr_pr_inner (Obs  $\alpha$   $\varphi$ )  $\leq e$ >
  using assms
  by (simp) (metis add_diff_cancel_enat add_mono_thms_linordered_semiring(1)
    enat.simps(3) enat_defs(2) energy.sel idiff_0_right
    le_iff_add le_numeral_extra(4) minus_energy_def option.discI
    option.inject)

lemma expr_st_conj:
  assumes
    <subtract_fn 0 0 0 1 0 0 0 0 e = Some e'>
    <I  $\neq \{\}$ >
    < $\forall q \in I. \text{expr\_pr\_conjunct } (\psi s \ q) \leq e'$ >
  shows
    <expr_pr_inner (StableConj I  $\psi s$ )  $\leq e$ >
proof -
  have st_conj_upds:
    <modal_depth_srbb_inner (StableConj I  $\psi s$ ) = Sup ((modal_depth_srbb_conjunct  $\circ \psi s$ ) ' I)>
    <branch_conj_depth_inner (StableConj I  $\psi s$ ) = Sup ((branch_conj_depth_conjunct  $\circ \psi s$ ) ' I)>
    <inst_conj_depth_inner (StableConj I  $\psi s$ ) = Sup ((inst_conj_depth_conjunct  $\circ \psi s$ ) ' I)>
    <st_conj_depth_inner (StableConj I  $\psi s$ ) = 1 + Sup ((st_conj_depth_conjunct  $\circ \psi s$ ) ' I)>
    <imm_conj_depth_inner (StableConj I  $\psi s$ ) = Sup ((imm_conj_depth_conjunct  $\circ \psi s$ ) ' I)>
    <max_pos_conj_depth_inner (StableConj I  $\psi s$ ) = Sup ((max_pos_conj_depth_conjunct  $\circ \psi s$ ) ' I)>
    <max_neg_conj_depth_inner (StableConj I  $\psi s$ ) = Sup ((max_neg_conj_depth_conjunct  $\circ \psi s$ ) ' I)>
    <neg_depth_inner (StableConj I  $\psi s$ ) = Sup ((neg_depth_conjunct  $\circ \psi s$ ) ' I)>
  by force+
obtain e1 e2 e3 e4 e5 e6 e7 e8 where e_def: <e = E e1 e2 e3 e4 e5 e6 e7 e8>
  using energy.exhaust_sel by blast
hence is_some: <subtract_fn 0 0 0 1 0 0 0 0 e = Some (E e1 e2 e3 (e4-1) e5 e6 e7 e8)>
  using assms minus_energy_def
  by (smt (verit, del_insts) energy_minus idiff_0_right option.distinct(1))
hence
  < $\forall i \in I. \text{modal\_depth\_srbb\_conjunct } (\psi s \ i) \leq e1$ >
  < $\forall i \in I. \text{branch\_conj\_depth\_conjunct } (\psi s \ i) \leq e2$ >
  < $\forall i \in I. \text{inst\_conj\_depth\_conjunct } (\psi s \ i) \leq e3$ >
  < $\forall i \in I. \text{st\_conj\_depth\_conjunct } (\psi s \ i) \leq (e4 - 1)$ >

```

```

    <∀i ∈ I. imm_conj_depth_conjunct (ψs i) ≤ e5>
    <∀i ∈ I. max_pos_conj_depth_conjunct (ψs i) ≤ e6>
    <∀i ∈ I. max_neg_conj_depth_conjunct (ψs i) ≤ e7>
    <∀i ∈ I. neg_depth_conjunct (ψs i) ≤ e8>
    using assms unfolding leq_components by auto
  hence sups:
    <Sup ((modal_depth_srbb_conjunct ∘ ψs) ' I) ≤ e1>
    <Sup ((branch_conj_depth_conjunct ∘ ψs) ' I) ≤ e2>
    <Sup ((inst_conj_depth_conjunct ∘ ψs) ' I) ≤ e3>
    <Sup ((st_conj_depth_conjunct ∘ ψs) ' I) ≤ (e4 - 1)>
    <Sup ((imm_conj_depth_conjunct ∘ ψs) ' I) ≤ e5>
    <Sup ((max_pos_conj_depth_conjunct ∘ ψs) ' I) ≤ e6>
    <Sup ((max_neg_conj_depth_conjunct ∘ ψs) ' I) ≤ e7>
    <Sup ((neg_depth_conjunct ∘ ψs) ' I) ≤ e8>
    by (simp add: Sup_le_iff)+
  hence <st_conj_depth_inner (StableConj I ψs) ≤ e4>
    using e_def is_some minus_energy_def leq_components st_conj_upds(4)
    by (metis add_diff_cancel_enat add_left_mono enat.simps(3) enat_defs(2) energy.sel(4)
        le_iff_add option.distinct(1))
  then show ?thesis
    using st_conj_upds sups
    by (simp add: e_def)
qed

lemma expr_imm_conj:
  assumes
    <subtract_fn 0 0 0 0 1 0 0 0 e = Some e'>
    <I ≠ {}>
    <expr_pr_inner (Conj I ψs) ≤ e'>
  shows <expressiveness_price (ImmConj I ψs) ≤ e>
proof -
  have conj_upds:
    <modal_depth_srbb_inner (Conj I ψs) = Sup ((modal_depth_srbb_conjunct ∘ ψs) ' I)>
    <branch_conj_depth_inner (Conj I ψs) = Sup ((branch_conj_depth_conjunct ∘ ψs) ' I)>
    <inst_conj_depth_inner (Conj I ψs) = 1 + Sup ((inst_conj_depth_conjunct ∘ ψs) ' I)>
    <st_conj_depth_inner (Conj I ψs) = Sup ((st_conj_depth_conjunct ∘ ψs) ' I)>
    <imm_conj_depth_inner (Conj I ψs) = Sup ((imm_conj_depth_conjunct ∘ ψs) ' I)>
    <max_pos_conj_depth_inner (Conj I ψs) = Sup ((max_pos_conj_depth_conjunct ∘ ψs) ' I)>
    <max_neg_conj_depth_inner (Conj I ψs) = Sup ((max_neg_conj_depth_conjunct ∘ ψs) ' I)>
    <neg_depth_inner (Conj I ψs) = Sup ((neg_depth_conjunct ∘ ψs) ' I)>
    using assms
    by force+
  have imm_conj_upds:
    <modal_depth_srbb (ImmConj I ψs) = Sup ((modal_depth_srbb_conjunct ∘ ψs) ' I)>
    <branching_conjunction_depth (ImmConj I ψs) = Sup ((branch_conj_depth_conjunct ∘ ψs) ' I)>
    <unstable_conjunction_depth (ImmConj I ψs) = 1 + Sup ((inst_conj_depth_conjunct ∘ ψs) ' I)>
    <stable_conjunction_depth (ImmConj I ψs) = Sup ((st_conj_depth_conjunct ∘ ψs) ' I)>
    <immediate_conjunction_depth (ImmConj I ψs) = 1 + Sup ((imm_conj_depth_conjunct ∘ ψs) ' I)>
    <max_positive_conjunct_depth (ImmConj I ψs) = Sup ((max_pos_conj_depth_conjunct ∘ ψs) ' I)>
    <max_negative_conjunct_depth (ImmConj I ψs) = Sup ((max_neg_conj_depth_conjunct ∘ ψs) ' I)>
    <negation_depth (ImmConj I ψs) = Sup ((neg_depth_conjunct ∘ ψs) ' I)>
    using assms
    by force+
  obtain e1 e2 e3 e4 e5 e6 e7 e8 where e_def: <e = E e1 e2 e3 e4 e5 e6 e7 e8>
    using assms by (metis energy.exhaust_sel)
  hence is_some: <(e - (E 0 0 0 0 1 0 0 0)) = (E e1 e2 e3 e4 (e5-1) e6 e7 e8)>
    using minus_energy_def
    by simp
  hence <e5>0 using assms(1) e_def leq_components by auto
  have
    <E (modal_depth_srbb_inner (Conj I ψs))

```

```

      (branch_conj_depth_inner (Conj I  $\psi$ s))
      (inst_conj_depth_inner (Conj I  $\psi$ s))
      (st_conj_depth_inner (Conj I  $\psi$ s))
      (imm_conj_depth_inner (Conj I  $\psi$ s))
      (max_pos_conj_depth_inner (Conj I  $\psi$ s))
      (max_neg_conj_depth_inner (Conj I  $\psi$ s))
      (neg_depth_inner (Conj I  $\psi$ s))  $\leq$  (E e1 e2 e3 e4 (e5-1) e6 e7 e8) >
    using is_some assms
    by (metis expr_pr_inner.simps option.discI option.inject)
  hence
    <(modal_depth_srbb_inner (Conj I  $\psi$ s))  $\leq$  e1>
    <(branch_conj_depth_inner (Conj I  $\psi$ s))  $\leq$  e2>
    <(inst_conj_depth_inner (Conj I  $\psi$ s))  $\leq$  e3>
    <(st_conj_depth_inner (Conj I  $\psi$ s))  $\leq$  e4>
    <(imm_conj_depth_inner (Conj I  $\psi$ s))  $\leq$  (e5-1)>
    <(max_pos_conj_depth_inner (Conj I  $\psi$ s))  $\leq$  e6>
    <(max_neg_conj_depth_inner (Conj I  $\psi$ s))  $\leq$  e7>
    <(neg_depth_inner (Conj I  $\psi$ s))  $\leq$  e8>
  by auto
  hence E:
    <Sup ((modal_depth_srbb_conjunct  $\circ$   $\psi$ s) ' I)  $\leq$  e1>
    <Sup ((branch_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)  $\leq$  e2>
    <1 + Sup ((inst_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)  $\leq$  e3>
    <Sup ((st_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)  $\leq$  e4>
    <Sup ((imm_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)  $\leq$  (e5-1)>
    <Sup ((max_pos_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)  $\leq$  e6>
    <Sup ((max_neg_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)  $\leq$  e7>
    <Sup ((neg_depth_conjunct  $\circ$   $\psi$ s) ' I)  $\leq$  e8>
  using conj_upds by force+
  from this(5) have <(1 + Sup ((imm_conj_depth_conjunct  $\circ$   $\psi$ s) ' I))  $\leq$  e5>
  using assms(1) <e5>0> is_some e_def add.right_neutral
    add_diff_cancel_enat enat_add_left_cancel_le ileI1 le_iff_add plus_1_eSuc(1)
  by metis
  thus <expressiveness_price (ImmConj I  $\psi$ s)  $\leq$  e> using imm_conj_upds E
  by (metis e_def energy.sel expressiveness_price.elims leD somewhere_larger_eq)
qed

lemma expr_conj:
  assumes
    <subtract_fn 0 0 1 0 0 0 0 0 e = Some e'>
    <I  $\neq$  {}>
    < $\forall q \in I. \text{expr\_pr\_conjunct } (\psi \text{ } q) \leq e'$ >
  shows <expr_pr_inner (Conj I  $\psi$ s)  $\leq$  e>
proof -
  have conj_upds:
    <modal_depth_srbb_inner (Conj I  $\psi$ s) = Sup ((modal_depth_srbb_conjunct  $\circ$   $\psi$ s) ' I)>
    <branch_conj_depth_inner (Conj I  $\psi$ s) = Sup ((branch_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)>
    <inst_conj_depth_inner (Conj I  $\psi$ s) = 1 + Sup ((inst_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)>
    <st_conj_depth_inner (Conj I  $\psi$ s) = Sup ((st_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)>
    <imm_conj_depth_inner (Conj I  $\psi$ s) = Sup ((imm_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)>
    <max_pos_conj_depth_inner (Conj I  $\psi$ s) = Sup ((max_pos_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)>
    <max_neg_conj_depth_inner (Conj I  $\psi$ s) = Sup ((max_neg_conj_depth_conjunct  $\circ$   $\psi$ s) ' I)>
    <neg_depth_inner (Conj I  $\psi$ s) = Sup ((neg_depth_conjunct  $\circ$   $\psi$ s) ' I)>
  using assms by force+
  obtain e1 e2 e3 e4 e5 e6 e7 e8 where e_def: <e = E e1 e2 e3 e4 e5 e6 e7 e8>
  using energy.exhaust_sel by metis
  hence is_some: <e - (E 0 0 1 0 0 0 0 0) = E e1 e2 (e3-1) e4 e5 e6 e7 e8>
  using minus_energy_def by simp
  hence <e3>0> using assms(1) e_def leq_components by auto
  hence
    < $\forall i \in I. \text{modal\_depth\_srbb\_conjunct } (\psi \text{ } i) \leq e1$ >

```

```

    <∀i ∈ I. branch_conj_depth_conjunct (ψs i) ≤ e2>
    <∀i ∈ I. inst_conj_depth_conjunct (ψs i) ≤ (e3-1)>
    <∀i ∈ I. st_conj_depth_conjunct (ψs i) ≤ e4>
    <∀i ∈ I. imm_conj_depth_conjunct (ψs i) ≤ e5>
    <∀i ∈ I. max_pos_conj_depth_conjunct (ψs i) ≤ e6>
    <∀i ∈ I. max_neg_conj_depth_conjunct (ψs i) ≤ e7>
    <∀i ∈ I. neg_depth_conjunct (ψs i) ≤ e8>
    using assms is_some energy.sel leq_components
    by (metis expr_pr_conjunct.elims option.distinct(1) option.inject)+
  hence sups:
    <Sup ((modal_depth_srbb_conjunct ∘ ψs) ' I) ≤ e1>
    <Sup ((branch_conj_depth_conjunct ∘ ψs) ' I) ≤ e2>
    <Sup ((inst_conj_depth_conjunct ∘ ψs) ' I) ≤ (e3-1)>
    <Sup ((st_conj_depth_conjunct ∘ ψs) ' I) ≤ e4>
    <Sup ((imm_conj_depth_conjunct ∘ ψs) ' I) ≤ e5>
    <Sup ((max_pos_conj_depth_conjunct ∘ ψs) ' I) ≤ e6>
    <Sup ((max_neg_conj_depth_conjunct ∘ ψs) ' I) ≤ e7>
    <Sup ((neg_depth_conjunct ∘ ψs) ' I) ≤ e8>
    by (simp add: Sup_le_iff)+
  hence <inst_conj_depth_inner (Conj I ψs) ≤ e3>
    using <e3>0> is_some e_def
    unfolding conj_upds(3)
    by (metis add.right_neutral add_diff_cancel_enat enat_add_left_cancel_le ileI1
      le_iff_add plus_1_eSuc(1))
  then show ?thesis
    using conj_upds sups
    by (simp add: e_def)
qed

lemma expr_br_conj:
  assumes
    <subtract_fn 0 1 1 0 0 0 0 0 e = Some e'>
    <min1_6 e' = Some e''>
    <subtract_fn 1 0 0 0 0 0 0 0 e'' = Some e'''>
    <expressiveness_price φ ≤ e'''>
    <∀q ∈ Q. expr_pr_conjunct (Φ q) ≤ e'>
    <1 + modal_depth_srbb φ ≤ pos_conjuncts e>
  shows <expr_pr_inner (BranchConj α φ Q Φ) ≤ e>
proof -
  obtain e1 e2 e3 e4 e5 e6 e7 e8 where e_def: <e = E e1 e2 e3 e4 e5 e6 e7 e8>
    by (smt (z3) energy.exhaust)
  hence e'''_def: <e''' = (E ((min e1 e6)-1) (e2-1) (e3-1) e4 e5 e6 e7 e8)>
    using minus_energy_def
    by (smt (z3) assms energy.sel idiff_0_right min_1_6_simps option.distinct(1) option.sel)
  hence min_vals: <the (min1_6 (e - E 0 1 1 0 0 0 0 0)) - (E 1 0 0 0 0 0 0 0)
    = (E ((min e1 e6)-1) (e2-1) (e3-1) e4 e5 e6 e7 e8)>
    using assms
    by (metis not_Some_eq option.sel)
  hence <0 < e1> <0 < e2> <0 < e3> <0 < e6>
    using assms energy.sel min_1_6_simps
    unfolding e_def minus_energy_def leq_components
    by (metis (no_types, lifting) gr_zeroI idiff_0_right min_enat_simps(3)
      not_one_le_zero option.distinct(1) option.sel, auto)
  have e_comp: <e - (E 0 1 1 0 0 0 0 0) = E e1 (e2-1) (e3-1) e4 e5 e6 e7 e8> using e_def
    by simp
  have conj:
    <E (modal_depth_srbb φ)
      (branching_conjunction_depth φ)
      (unstable_conjunction_depth φ)
      (stable_conjunction_depth φ)
      (immediate_conjunction_depth φ)

```

```

      (max_positive_conjunct_depth  $\varphi$ )
      (max_negative_conjunct_depth  $\varphi$ )
      (negation_depth  $\varphi$ )
       $\leq ((E ((\min e1\ e6)-1) (e2-1) (e3-1) e4\ e5\ e6\ e7\ e8)))$ 
    using assms e''_def by force
  hence conj_single:
    <modal_depth_srbb  $\varphi \leq ((\min e1\ e6)-1)$ >
    <branching_conjunction_depth  $\varphi \leq e2 - 1$ >
    <(unstable_conjunction_depth  $\varphi \leq e3 - 1$ >
    <(stable_conjunction_depth  $\varphi \leq e4$ >
    <(immediate_conjunction_depth  $\varphi \leq e5$ >
    <(max_positive_conjunct_depth  $\varphi \leq e6$ >
    <(max_negative_conjunct_depth  $\varphi \leq e7$ >
    <(negation_depth  $\varphi \leq e8$ >
    using leq_components by auto
  have <0 < (min e1 e6)> using <0 < e1> <0 < e6>
    using min_less_iff_conj by blast
  hence <1 + modal_depth_srbb  $\varphi \leq (\min e1\ e6)$ >
    using conj_single add.commute add_diff_assoc_enat add_diff_cancel_enat
      add_right_mono conj_single(2) i1_ne_infinity ileI1 one_eSuc
    by (metis (no_types, lifting))
  hence <1 + modal_depth_srbb  $\varphi \leq e1$ > <1 + modal_depth_srbb  $\varphi \leq e6$ >
    using min.bounded_iff by blast+
  from conj have <1 + branching_conjunction_depth  $\varphi \leq e2$ >
    by (metis <0 < e2> add.commute add_diff_assoc_enat add_diff_cancel_enat
      add_right_mono conj_single(2) i1_ne_infinity ileI1 one_eSuc)
  from conj_single have <1 + unstable_conjunction_depth  $\varphi \leq e3$ >
    using <0 < e3> add.commute add_diff_assoc_enat add_diff_cancel_enat
      add_right_mono conj_single(2) i1_ne_infinity ileI1 one_eSuc
    by (metis (no_types, lifting))
  have branch: < $\forall q \in Q.$ 
    E (modal_depth_srbb_conjunct ( $\Phi\ q$ ))
      (branch_conj_depth_conjunct ( $\Phi\ q$ ))
      (inst_conj_depth_conjunct ( $\Phi\ q$ ))
      (st_conj_depth_conjunct ( $\Phi\ q$ ))
      (imm_conj_depth_conjunct ( $\Phi\ q$ ))
      (max_pos_conj_depth_conjunct ( $\Phi\ q$ ))
      (max_neg_conj_depth_conjunct ( $\Phi\ q$ ))
      (neg_depth_conjunct ( $\Phi\ q$ ))
     $\leq (E\ e1\ (e2-1)\ (e3-1)\ e4\ e5\ e6\ e7\ e8)$ >
    using assms e_def e_comp
    by (metis expr_pr_conjunct.simps option.distinct(1) option.sel)
  hence branch_single:
    < $\forall q \in Q.$  (modal_depth_srbb_conjunct ( $\Phi\ q$ ))  $\leq e1$ >
    < $\forall q \in Q.$  (branch_conj_depth_conjunct ( $\Phi\ q$ ))  $\leq (e2-1)$ >
    < $\forall q \in Q.$  (inst_conj_depth_conjunct ( $\Phi\ q$ ))  $\leq (e3-1)$ >
    < $\forall q \in Q.$  (st_conj_depth_conjunct ( $\Phi\ q$ ))  $\leq e4$ >
    < $\forall q \in Q.$  (imm_conj_depth_conjunct ( $\Phi\ q$ ))  $\leq e5$ >
    < $\forall q \in Q.$  (max_pos_conj_depth_conjunct ( $\Phi\ q$ ))  $\leq e6$ >
    < $\forall q \in Q.$  (max_neg_conj_depth_conjunct ( $\Phi\ q$ ))  $\leq e7$ >
    < $\forall q \in Q.$  (neg_depth_conjunct ( $\Phi\ q$ ))  $\leq e8$ >
    by auto
  hence < $\forall q \in Q.$  (1 + branch_conj_depth_conjunct ( $\Phi\ q$ ))  $\leq e2$ >
    by (metis <0 < e2> add.commute add_diff_assoc_enat add_diff_cancel_enat
      add_right_mono i1_ne_infinity ileI1 one_eSuc)
  from branch_single have < $\forall q \in Q.$  (1 + inst_conj_depth_conjunct ( $\Phi\ q$ ))  $\leq e3$ >
    using <0 < e3>
    by (metis add.commute add_diff_assoc_enat add_diff_cancel_enat add_right_mono
      i1_ne_infinity ileI1 one_eSuc)
  have
    <expr_pr_inner (BranchConj  $\alpha\ \varphi\ Q\ \Phi$ )

```

```

= E (modal_depth_srbb_inner (BranchConj  $\alpha$   $\varphi$   $Q$   $\Phi$ ))
  (branch_conj_depth_inner (BranchConj  $\alpha$   $\varphi$   $Q$   $\Phi$ ))
  (inst_conj_depth_inner (BranchConj  $\alpha$   $\varphi$   $Q$   $\Phi$ ))
  (st_conj_depth_inner (BranchConj  $\alpha$   $\varphi$   $Q$   $\Phi$ ))
  (imm_conj_depth_inner (BranchConj  $\alpha$   $\varphi$   $Q$   $\Phi$ ))
  (max_pos_conj_depth_inner (BranchConj  $\alpha$   $\varphi$   $Q$   $\Phi$ ))
  (max_neg_conj_depth_inner (BranchConj  $\alpha$   $\varphi$   $Q$   $\Phi$ ))
  (neg_depth_inner (BranchConj  $\alpha$   $\varphi$   $Q$   $\Phi$ ))> by simp
hence expr:
  <expr_pr_inner (BranchConj  $\alpha$   $\varphi$   $Q$   $\Phi$ )
  = E (Sup ({1 + modal_depth_srbb  $\varphi$ }  $\cup$  ((modal_depth_srbb_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))
    (1 + Sup ({branching_conjunction_depth  $\varphi$ }  $\cup$  ((branch_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))
    (1 + Sup ({unstable_conjunction_depth  $\varphi$ }  $\cup$  ((inst_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))
    (Sup ({stable_conjunction_depth  $\varphi$ }  $\cup$  ((st_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))
    (Sup ({immediate_conjunction_depth  $\varphi$ }  $\cup$  ((imm_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))
    (Sup ({1 + modal_depth_srbb  $\varphi$ , max_positive_conjunct_depth  $\varphi$ }
       $\cup$  ((max_pos_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))
    (Sup ({max_negative_conjunct_depth  $\varphi$ }  $\cup$  ((max_neg_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))
    (Sup ({negation_depth  $\varphi$ }  $\cup$  ((neg_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))> by auto
from branch_single <1 + modal_depth_srbb  $\varphi$   $\leq$  e1>
  have < $\forall x \in$  ({1 + modal_depth_srbb  $\varphi$ }  $\cup$  ((modal_depth_srbb_conjunct  $\circ$   $\Phi$ ) '  $Q$ )).  $x \leq$  e1>
  by fastforce
hence e1_le:
  <(Sup ({1 + modal_depth_srbb  $\varphi$ }  $\cup$  ((modal_depth_srbb_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))  $\leq$  e1>
  using Sup_least by blast
have < $\forall x \in$  {branching_conjunction_depth  $\varphi$ }  $\cup$  ((branch_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )).
   $x \leq$  e2 - 1>
  using branch_single conj_single comp_apply image_iff insertE by auto
hence e2_le:
  <1 + Sup ({branching_conjunction_depth  $\varphi$ }
     $\cup$  ((branch_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ ))  $\leq$  e2>
  using Sup_least
  by (metis Un_insert_left <0 < e2> add.commute eSuc_minus_1 enat_add_left_cancel_le
    ileI1 le_iff_add one_eSuc plus_1_eSuc(2) sup_bot_left)
have < $\forall x \in$  ({unstable_conjunction_depth  $\varphi$ }  $\cup$  ((inst_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )).
   $x \leq$  e3-1>
  using conj_single branch_single
  using comp_apply image_iff insertE by auto
hence e3_le:
  <1 + Sup ({unstable_conjunction_depth  $\varphi$ }  $\cup$  ((inst_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ ))  $\leq$  e3>
  using Un_insert_left <0<e3> add.commute eSuc_minus_1 enat_add_left_cancel_le ileI1
    le_iff_add one_eSuc plus_1_eSuc(2) sup_bot_left
  by (metis Sup_least)
have fa:
  < $\forall x \in$  ({stable_conjunction_depth  $\varphi$ }  $\cup$  ((st_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )).  $x \leq$  e4>
  < $\forall x \in$  ({immediate_conjunction_depth  $\varphi$ }  $\cup$  ((imm_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )).  $x \leq$  e5>
  < $\forall x \in$  ({1 + modal_depth_srbb  $\varphi$ , max_positive_conjunct_depth  $\varphi$ }
     $\cup$  ((max_pos_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )).  $x \leq$  e6>
  < $\forall x \in$  ({max_negative_conjunct_depth  $\varphi$ }
     $\cup$  ((max_neg_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )).  $x \leq$  e7>
  < $\forall x \in$  ({negation_depth  $\varphi$ }  $\cup$  ((neg_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )).  $x \leq$  e8>
  using conj_single branch_single <1 + modal_depth_srbb  $\varphi$   $\leq$  e6> by auto
hence
  <(Sup ({stable_conjunction_depth  $\varphi$ }  $\cup$  ((st_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))  $\leq$  e4>
  <(Sup ({immediate_conjunction_depth  $\varphi$ }  $\cup$  ((imm_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))  $\leq$  e5>
  <(Sup ({1 + modal_depth_srbb  $\varphi$ , max_positive_conjunct_depth  $\varphi$ }
     $\cup$  ((max_pos_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))  $\leq$  e6>
  <(Sup ({max_negative_conjunct_depth  $\varphi$ }  $\cup$  ((max_neg_conj_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))  $\leq$  e7>
  <(Sup ({negation_depth  $\varphi$ }  $\cup$  ((neg_depth_conjunct  $\circ$   $\Phi$ ) '  $Q$ )))  $\leq$  e8>
  using Sup_least
  by metis+

```

```

thus <expr_pr_inner (BranchConj  $\alpha$   $\varphi$   $Q$   $\Phi$ )  $\leq$  e>
  using expr e3_le e2_le e1_le e_def energy.sel leq_components by presburger
qed

lemma expressiveness_price_ImmConj_geq_parts:
  assumes <i  $\in$  I>
  shows <expressiveness_price (ImmConj I  $\psi$ s) - E 0 0 1 0 1 0 0 0  $\geq$  expr_pr_conjunct ( $\psi$ s i)>
proof -
  from assms have <I  $\neq$  {}> by blast
  from expressiveness_price_ImmConj_non_empty_def[OF <I  $\neq$  {}>]
  have <expressiveness_price (ImmConj I  $\psi$ s)  $\geq$  E 0 0 1 0 1 0 0 0>
    using energy_leq_cases by force
  hence
    <expressiveness_price (ImmConj I  $\psi$ s) - E 0 0 1 0 1 0 0 0 = E
      (Sup ((modal_depth_srbb_conjunct  $\circ$   $\psi$ s) ' I))
      (Sup ((branch_conj_depth_conjunct  $\circ$   $\psi$ s) ' I))
      (Sup ((inst_conj_depth_conjunct  $\circ$   $\psi$ s) ' I))
      (Sup ((st_conj_depth_conjunct  $\circ$   $\psi$ s) ' I))
      (Sup ((imm_conj_depth_conjunct  $\circ$   $\psi$ s) ' I))
      (Sup ((max_pos_conj_depth_conjunct  $\circ$   $\psi$ s) ' I))
      (Sup ((max_neg_conj_depth_conjunct  $\circ$   $\psi$ s) ' I))
      (Sup ((neg_depth_conjunct  $\circ$   $\psi$ s) ' I))>
    unfolding expressiveness_price_ImmConj_non_empty_def[OF <I  $\neq$  {}>]
    by simp
  also have <...  $\geq$  expr_pr_conjunct ( $\psi$ s i)>
    using assms <I  $\neq$  {}> SUP_upper unfolding leq_components by fastforce
  finally show ?thesis .
qed

lemma expressiveness_price_ImmConj_geq_parts':
  assumes <i  $\in$  I>
  shows
    <(expressiveness_price (ImmConj I  $\psi$ s) - E 0 0 0 0 1 0 0 0) - E 0 0 1 0 0 0 0 0
       $\geq$  expr_pr_conjunct ( $\psi$ s i)>
  using expressiveness_price_ImmConj_geq_parts[OF assms]
    less_eq_energy_def minus_energy_def
  by (smt (z3) energy.sel idiff_0_right)

```

Here, we show the prices for some specific formulas.

```

lemma example_φ_cp:
  fixes op a b :: <'a> and left right :: <'s>
  defines <φ  $\equiv$ 
    (Internal
      (Obs op
        (Internal
          (Conj {left, right}
            (λi. (if i = left
                  then (Pos (Obs a TT))
                  else if i = right
                  then (Pos (Obs b TT))
                  else undefined))))))>
  shows
    <modal_depth_srbb φ = 2>
    <branching_conjunction_depth φ = 0>
    <unstable_conjunction_depth φ = 1>
    <stable_conjunction_depth φ = 0>
    <immediate_conjunction_depth φ = 0>
    <max_positive_conjunct_depth φ = 1>
    <max_negative_conjunct_depth φ = 0>
    <negation_depth φ = 0>
  unfolding φ_def by simp+

```

```

lemma <expressiveness_price (Internal
  (Obs op
    (Internal
      (Conj {left, right}
        (λi. (if i = left
          then (Pos (Obs a TT))
          else if i = right
            then (Pos (Obs b TT))
            else undefined)))))) = E 2 0 1 0 0 1 0 0>

by simp

lemma <expressiveness_price TT = E 0 0 0 0 0 0 0 0>
by simp

lemma <expressiveness_price (ImmConj {} ψs) = E 0 0 0 0 0 0 0 0>
by (simp add: Sup_enat_def)

lemma <expressiveness_price (Internal (Conj {} ψs)) = E 0 0 0 0 0 0 0 0>
by (simp add: Sup_enat_def)

lemma <expressiveness_price (Internal (BranchConj α TT {} ψs)) = E 1 1 1 0 0 1 0 0>
by (simp add: Sup_enat_def)

lemma expr_obs_phi:
  <subtract_fn 1 0 0 0 0 0 0 0 (expr_pr_inner (Obs α φ)) = Some (expressiveness_price φ)>
by simp

end — pause lts_tau context

```

3.7 Characterizing Equivalence by Energy Coordinates

We can now define a sublanguage of Hennessy–Milner Logic $\mathcal{O}$ by the set of formulas with prices below an energy coordinate.

```

definition  $\mathcal{O} :: \langle \text{energy} \Rightarrow (('a, 's) \text{hml\_srbb}) \text{set} \rangle$  where
  < $\mathcal{O} \text{ energy} \equiv \{\varphi . \text{expressiveness\_price } \varphi \leq \text{energy}\}$ >

lemma  $\mathcal{O}_{\text{sup}}$ : <UNIV =  $\mathcal{O} (E \infty \infty \infty \infty \infty \infty \infty \infty)$ > unfolding  $\mathcal{O}_{\text{def}}$  by auto

lemma price_hierarchy_entails_modal_hierarchy:
  assumes < $e1 \leq e2$ >
  shows < $\mathcal{O} e1 \subseteq \mathcal{O} e2$ >
  using assms unfolding  $\mathcal{O}_{\text{def}}$  by auto

definition  $\mathcal{O}_{\text{inner}} :: \langle \text{energy} \Rightarrow (('a, 's) \text{hml\_srbb\_inner}) \text{set} \rangle$  where
  < $\mathcal{O}_{\text{inner}} \text{ energy} \equiv \{\chi . \text{expr\_pr\_inner } \chi \leq \text{energy}\}$ >

definition  $\mathcal{O}_{\text{conjunct}} :: \langle \text{energy} \Rightarrow (('a, 's) \text{hml\_srbb\_conjunct}) \text{set} \rangle$  where
  < $\mathcal{O}_{\text{conjunct}} \text{ energy} \equiv \{\chi . \text{expr\_pr\_conjunct } \chi \leq \text{energy}\}$ >

context lts_tau
begin

```

A state p pre-orders another state q with respect to some energy e if and only if p HML pre-orders q with respect to the HML sublanguage $\mathcal{O} e$.

```

definition expr_preord :: <'s  $\Rightarrow$  energy  $\Rightarrow$  's  $\Rightarrow$  bool> (<_  $\preceq$  _ _> 60) where
  <(p  $\preceq$  e q)  $\equiv$  preordered ( $\mathcal{O} e$ ) p q>

```

Conversely, p and q are equivalent with respect to e if and only if they are equivalent with respect to that HML sublanguage $\mathcal{O} e$.

```

definition expr_equiv :: '<'s  $\Rightarrow$  energy  $\Rightarrow$  's  $\Rightarrow$  bool> (<_  $\sim$  _ _> 60) where
  <p  $\sim$  e q>  $\equiv$  equivalent ( $\mathcal{O}$  e) p q>

lemma price_hierarchy_preorder_dual:
  assumes
    <e1  $\leq$  e2>
    <p  $\preceq$  e2 q>
  shows
    <p  $\preceq$  e1 q>
  using assms price_hierarchy_entails_modal_hierarchy expr_preord_def by auto

```

3.8 Relational Effects of Prices

Certain properties of prices influence the preorder/equivalence relations that are characterized by price coordinates. (This will be important for some behavioral equivalences that we will prove to be characterized by specific prices.)

```

lemma distinction_combination_eta:
  fixes p q
  defines
    <Q $\alpha$   $\equiv$  {q'. q  $\rightarrow$  q'  $\wedge$  ( $\nexists \varphi. \varphi \in \mathcal{O}$  (E  $\infty \infty \infty$  0 0  $\infty$  0 0)  $\wedge$  distinguishes  $\varphi$  p q')}>
  assumes
    <p  $\mapsto_a$   $\alpha$  p'>
    < $\forall q' \in Q\alpha. \forall q'' q'''. q' \mapsto_a \alpha q'' \rightarrow q'' \twoheadrightarrow q''' \rightarrow$  distinguishes ( $\Phi$  q''') p' q'''>
  shows
    < $\forall q' \in Q\alpha. \text{hml\_srbb\_inner.distinguishes (Obs } \alpha \text{ (Internal (Conj$ 
      {q'''.  $\exists q' \in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \twoheadrightarrow q'''} \}$ 
      (conjoinctify_distinctions  $\Phi$  p')))) p q'>
proof -
  have <q'  $\in Q\alpha. \forall q'' q''' \in \{q'''. \exists q' \in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \twoheadrightarrow q'''} \}$ .
    hml_srbb_conj.distinguishes ((conjoinctify_distinctions  $\Phi$  p') q''') p' q''')>
  proof clarify
    fix q' q'' q'''
    assume <q'  $\in Q\alpha$ > <q'  $\mapsto_a$   $\alpha$  q''> <q''  $\twoheadrightarrow$  q'''>
    thus <hml_srbb_conj.distinguishes (conjoinctify_distinctions  $\Phi$  p' q''') p' q''')>
      using assms(3) distinction_conjoinctification by blast
  qed
  hence < $\forall q' \in Q\alpha. \forall q''. q' \mapsto_a \alpha q''$ 
     $\rightarrow$  distinguishes (Internal (Conj {q'''.  $\exists q' \in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \twoheadrightarrow q'''} \}$ 
      (conjoinctify_distinctions  $\Phi$  p')))) p' q''>
    using silent_reachable.refl unfolding Q $\alpha$ _def by fastforce
  thus < $\forall q' \in Q\alpha. \text{hml\_srbb\_inner.distinguishes (Obs } \alpha \text{ (Internal (Conj$ 
    {q'''.  $\exists q' \in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \twoheadrightarrow q'''} \}$ 
    (conjoinctify_distinctions  $\Phi$  p')))) p q'>
    using assms(2) by (auto) (metis silent_reachable.refl)+
qed

lemma distinction_conjoinctification_two_way_price:
  assumes
    < $\forall q \in I. \text{distinguishes } (\Phi \text{ } q) \text{ } p \text{ } q \vee \text{distinguishes } (\Phi \text{ } q) \text{ } q \text{ } p$ >
    < $\forall q \in I. \Phi \text{ } q \in \mathcal{O}$  (E  $\infty \infty \infty$  0 0  $\infty \infty \infty$ )>
  shows
    < $\forall q \in I. \text{(if distinguishes } (\Phi \text{ } q) \text{ } p \text{ } q$ 
      then conjoinctify_distinctions
      else conjoinctify_distinctions_dual
      )  $\Phi$  p q  $\in \mathcal{O}_{\text{conjoinct}}$  (E  $\infty \infty \infty$  0 0  $\infty \infty \infty$ )>
proof
  fix q

```

```

assume <q ∈ I>
show
  <(if distinguishes (Φ q) p q
    then conjunctify_distinctions
    else conjunctify_distinctions_dual
  ) Φ p q ∈ O_conjunct (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)>
proof (cases <Φ q>)
  case TT
  then show ?thesis
    using assms <q ∈ I>
    by fastforce
next
  case (Internal χ)
  then show ?thesis
    using assms <q ∈ I>
    unfolding conjunctify_distinctions_def conjunctify_distinctions_dual_def O_def O_conjunct_def
    by fastforce
next
  case (ImmConj J Ψ)
  hence <J = {}>
    using assms <q ∈ I> unfolding O_def
    by (simp, metis iadd_is_0 immediate_conjunction_depth.simps(3) zero_one_enat_neq(1))
  then show ?thesis
    using assms <q ∈ I> ImmConj by fastforce
qed
qed

lemma distinction_combination_eta_two_way:
  fixes p q p' Φ
  defines
    <Qα ≡ {q'. q → q' ∧ (∄φ. φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)
      ∧ (distinguishes φ p q' ∨ distinguishes φ q' p))}> and
    <Ψα ≡ λq'''. (
      if distinguishes (Φ q''') p' q'''
      then conjunctify_distinctions
      else conjunctify_distinctions_dual
    ) Φ p' q'''>
  assumes
    <p ↦a α p'>
    <∀q' ∈ Qα.
      ∀q'' q'''. q' ↦a α q'' → q'' → q'''
      → distinguishes (Φ q''') p' q''' ∨ distinguishes (Φ q''') q''' p'>
  shows
    <∀q' ∈ Qα. hml_srbb_inner.distinguishes (Obs α (Internal (Conj
      {q'''. ∃q' ∈ Qα. ∃q''. q' ↦a α q'' ∧ q'' → q'''}
      Ψα))) p q'>
proof -
  have <∀q' ∈ Qα. ∀q''' ∈ {q'''. ∃q' ∈ Qα. ∃q''. q' ↦a α q'' ∧ q'' → q'''}
    hml_srbb_conj.distinguishes (Ψα q''') p' q'''>
  proof clarify
    fix q' q'' q'''
    assume <q' ∈ Qα> <q' ↦a α q''> <q'' → q'''>
    thus <hml_srbb_conj.distinguishes (Ψα q''') p' q'''>
      using assms(4) Ψα_def distinction_conjunctification_two_way mem_Collect_eq
      by (smt (verit, best))
  qed
  hence <∀q' ∈ Qα. ∀q''' ∈ {q'''. ∃q' ∈ Qα. ∃q''. q' ↦a α q'' ∧ q'' → q'''}
    hml_srbb_inner.distinguishes (Conj {q'''. ∃q' ∈ Qα. ∃q''. q' ↦a α q'' ∧ q'' → q'''}
      Ψα) p' q'''>
  using srbb_dist_conjunct_implies_dist_conjunction
  unfolding lts_semantics.distinguishes_def

```

```

    by (metis (no_types, lifting))
  hence <∀q'∈Qα. ∀q'''. (∃q''. q' ↦a α q'' ∧ q'' ⇒ q''') ⇒>
    hml_srb_inner.distinguishes
      (Conj {q'''. ∃q'∈Qα. ∃q''. q' ↦a α q'' ∧ q'' ⇒ q'''} Ψα) p' q'''>
  by blast
  hence <∀q'∈Qα. ∀q''. q' ↦a α q'' ⇒ distinguishes
    (Internal (Conj {q'''. ∃q'∈Qα. ∃q''. q' ↦a α q'' ∧ q'' ⇒ q'''} Ψα)) p' q''>
  by (meson distinguishes_def hml_srb_inner.distinguishes_def
    hml_srb_models.simps(2) silent_reachable.refl)
  thus <∀q'∈Qα. hml_srb_inner.distinguishes
    (Obs α (Internal (Conj {q'''. ∃q'∈Qα. ∃q''. q' ↦a α q'' ∧ q'' ⇒ q'''} Ψα))) p q'>
  using assms(3)
  by auto (metis silent_reachable.refl)+
qed

lemma distinction_conjunctification_price:
  assumes
    <∀q∈I. distinguishes (Φ q) p q>
    <∀q∈I. Φ q ∈ O pr>
    <modal_depth pr ≤ pos_conjuncts pr>
  shows
    <∀q∈I. ((conjunctify_distinctions Φ p) q) ∈ O_conjunct pr>
proof
  fix q
  assume <q ∈ I>
  show <conjunctify_distinctions Φ p q ∈ O_conjunct pr>
  proof (cases <Φ q>)
    case TT
    then show ?thesis
      using assms <q ∈ I>
      by fastforce
  next
    case (Internal χ)
    then show ?thesis
      using assms <q ∈ I>
      unfolding conjunctify_distinctions_def O_def O_conjunct_def
      by fastforce
  next
    case (ImmConj J Ψ)
    hence <∃i. i∈J ∧ hml_srb_inner.distinguishes (Ψ i) p q>
      using <q ∈ I> assms(1) by fastforce
    moreover have <conjunctify_distinctions Φ p q
      = Ψ (SOME i. i∈J ∧ hml_srb_inner.distinguishes (Ψ i) p q)>
      unfolding ImmConj conjunctify_distinctions_def by simp
    ultimately have Ψ_i:
      <∃i∈J. hml_srb_inner.distinguishes (Ψ i) p q ∧ conjunctify_distinctions Φ p q = Ψ i>
      by (metis (no_types, lifting) some_eq_ex)
    hence <conjunctify_distinctions Φ p q ∈ Ψ'J>
      unfolding image_iff by blast
    hence
      <expr_pr_conjunct (conjunctify_distinctions Φ p q)
        ≤ expressiveness_price (ImmConj J Ψ)>
      by (smt (verit, best) Ψ_i dual_order.trans expressiveness_price_ImmConj_geq_parts
        gets_smaller)
    then show ?thesis
      using assms <q ∈ I> ImmConj unfolding O_def O_conjunct_def by auto
  qed
qed

```

```

lemma modal_stability_respecting:
  <stability_respecting (preordered (O (E e1 e2 e3 ∞ e5 ∞ e7 e8)))>

```

```

unfolding stability_respecting_def
proof safe
  fix p q
  assume p_stability:
    <preordered ( $\mathcal{O}$  (E e1 e2 e3  $\infty$  e5  $\infty$  e7 e8)) p q>
    <stable_state p>
  have < $\neg(\forall q'. q \Rightarrow q' \rightarrow \neg \text{preordered } (\mathcal{O} (E e1 e2 e3 \infty e5 \infty e7 e8)) p q' \vee \neg \text{stable\_state } q')$ >
  proof safe
    assume < $\forall q'. q \Rightarrow q' \rightarrow \neg \text{preordered } (\mathcal{O} (E e1 e2 e3 \infty e5 \infty e7 e8)) p q' \vee \neg \text{stable\_state } q'$ >
    hence < $\forall q'. q \Rightarrow q' \rightarrow \text{stable\_state } q' \rightarrow (\exists \varphi \in \mathcal{O} (E e1 e2 e3 \infty e5 \infty e7 e8). \text{distinguishes } \varphi p q')$ > by auto
    then obtain  $\Phi$  where  $\Phi\_def$ :
      < $\forall q' \in (\text{silent\_reachable\_set } \{q\}). \text{stable\_state } q' \rightarrow \text{distinguishes } (\Phi q') p q' \wedge \Phi q' \in \mathcal{O} (E e1 e2 e3 \infty e5 \infty e7 e8)$ >
      using singleton_iff sreachable_set_is_sreachable by metis
    hence distinctions:
      < $\forall q' \in (\text{silent\_reachable\_set } \{q\} \cap \{q'. \text{stable\_state } q'\}). \text{distinguishes } (\Phi q') p q'$ >
      < $\forall q' \in (\text{silent\_reachable\_set } \{q\} \cap \{q'. \text{stable\_state } q'\}). \Phi q' \in \mathcal{O} (E e1 e2 e3 \infty e5 \infty e7 e8)$ > by blast+
    from distinction_conjunctification_price[OF this] have
      < $\forall q' \in (\text{silent\_reachable\_set } \{q\} \cap \{q'. \text{stable\_state } q'\}). \text{conjunctify\_distinctions } \Phi p q' \in \mathcal{O\_conjunct} (E e1 e2 e3 \infty e5 \infty e7 e8)$ >
      by fastforce
    hence conj_price: <StableConj (silent_reachable_set {q}  $\cap$  {q'. stable_state q'})
      (conjunctify_distinctions  $\Phi$  p)  $\in \mathcal{O\_inner} (E e1 e2 e3 \infty e5 \infty e7 e8)$ >
      unfolding  $\mathcal{O\_inner\_def}$   $\mathcal{O\_conjunct\_def}$  using SUP_le_iff by fastforce
    from  $\Phi\_def$  have
      < $\forall q' \in (\text{silent\_reachable\_set } \{q\}). \text{stable\_state } q' \rightarrow \text{hml\_srbb\_conj.distinguishes } (\text{conjunctify\_distinctions } \Phi p q') p q'$ >
      using singleton_iff distinction_conjunctification by metis
    hence <hml_srbb_inner.distinguishes_from
      (StableConj (silent_reachable_set {q}  $\cap$  {q'. stable_state q'})
        (conjunctify_distinctions  $\Phi$  p)) p (silent_reachable_set {q})>
      using p_stability(2) by fastforce
    hence
      <distinguishes
        (Internal (StableConj (silent_reachable_set {q}  $\cap$  {q'. stable_state q'})
          (conjunctify_distinctions  $\Phi$  p))
        )
        p q>
      unfolding silent_reachable_set_def
      using silent_reachable.refl by auto
    moreover have
      <Internal (StableConj (silent_reachable_set {q}  $\cap$  {q'. stable_state q'})
        (conjunctify_distinctions  $\Phi$  p))  $\in \mathcal{O} (E e1 e2 e3 \infty e5 \infty e7 e8)$ >
      using conj_price unfolding  $\mathcal{O\_def}$   $\mathcal{O\_inner\_def}$  by simp
    ultimately show False
      using p_stability(1) preordered_no_distinction by blast
  qed
  thus < $\exists q'. q \Rightarrow q' \wedge \text{preordered } (\mathcal{O} (E e1 e2 e3 \infty e5 \infty e7 e8)) p q' \wedge \text{stable\_state } q'$ >
    by blast
qed
end
end

```

4 Weak Traces

```
theory Weak_Traces
  imports Main HML_SRBB Expressiveness_Price
begin
```

The point of this theory is to prove that the coordinate $E \infty 0 0 0 0 0 0 0$ precisely characterizes weak trace preorder and equivalence.

4.1 Weak Traces as Modal Constructs

```
inductive
  is_trace_formula :: <('act, 'i) hml_srbb  $\Rightarrow$  bool> and
  is_trace_formula_inner :: <('act, 'i) hml_srbb_inner  $\Rightarrow$  bool>
where
  <is_trace_formula TT> |
  <is_trace_formula (Internal  $\chi$ )> if <is_trace_formula_inner  $\chi$ > |
  <is_trace_formula (ImmConj I  $\psi$ s)> if <I = {}> |

  <is_trace_formula_inner (Obs  $\alpha$   $\varphi$ )> if <is_trace_formula  $\varphi$ > |
  <is_trace_formula_inner (Conj I  $\psi$ s)> if <I = {}>
```

We define a function that translates a (weak) trace tr to a formula φ such that a state $\mathbf{p}$ models φ , $\mathbf{p} \models \varphi$ if and only if tr is a (weak) trace of $\mathbf{p}$.

```
fun
  wtrace_to_srbb :: <'act list  $\Rightarrow$  ('act, 'i) hml_srbb> and
  wtrace_to_inner :: <'act list  $\Rightarrow$  ('act, 'i) hml_srbb_inner> and
  wtrace_to_conjunct :: <'act list  $\Rightarrow$  ('act, 'i) hml_srbb_conjunct>
where
  <wtrace_to_srbb [] = TT> |
  <wtrace_to_srbb tr = (Internal (wtrace_to_inner tr))> |

  <wtrace_to_inner [] = (Conj {} ( $\lambda$ _. undefined))> | — Should never happen
  <wtrace_to_inner ( $\alpha$  # tr) = (Obs  $\alpha$  (wtrace_to_srbb tr))> |

  <wtrace_to_conjunct tr = Pos (wtrace_to_inner tr)> — Should never happen

lemma trace_to_srbb_is_trace_formula:
  <is_trace_formula (wtrace_to_srbb trace)>
by (induct trace,
    auto simp add: is_trace_formula.simps is_trace_formula_is_trace_formula_inner.intros(1,4))
```

4.2 Weak Trace Observations through Coordinates

The following three lemmas show that the modal-logical characterization of weak traces corresponds to the sublanguage of HML_{SRBB} , obtain by the energy coordinates $(\infty, 0, 0, 0, 0, 0, 0, 0)$.

```
lemma trace_formula_to_expressiveness:
  fixes
     $\varphi$  :: <('act, 'i) hml_srbb> and
     $\chi$  :: <('act, 'i) hml_srbb_inner>
  shows <(is_trace_formula  $\varphi$   $\longrightarrow$  ( $\varphi \in \mathcal{O}$  ( $E \infty 0 0 0 0 0 0 0$ )))
     $\wedge$  (is_trace_formula_inner  $\chi$   $\longrightarrow$  ( $\chi \in \mathcal{O}_{\text{inner}}$  ( $E \infty 0 0 0 0 0 0 0$ )))>
by (rule is_trace_formula_is_trace_formula_inner.induct)
  (simp add: Sup_enat_def  $\mathcal{O}_{\text{def}}$   $\mathcal{O}_{\text{inner\_def}}$ )

lemma expressiveness_to_trace_formula:
  fixes
     $\varphi$  :: <('act, 'i) hml_srbb> and
     $\chi$  :: <('act, 'i) hml_srbb_inner>
```

```

shows <( $\varphi \in \mathcal{O} (E \infty 0 0 0 0 0 0 0) \rightarrow \text{is\_trace\_formula } \varphi$ )
       $\wedge (\chi \in \mathcal{O\_inner} (E \infty 0 0 0 0 0 0 0) \rightarrow \text{is\_trace\_formula\_inner } \chi)$ 
       $\wedge \text{True}$ >
proof (induct rule: hml_srbb_hml_srbb_inner_hml_srbb_conjunct.induct)
  case TT
  then show ?case
    using is_trace_formula_is_trace_formula_inner.intros(1) by blast
next
  case (Internal x)
  then show ?case
    by (simp add:  $\mathcal{O\_inner\_def}$   $\mathcal{O\_def}$  is_trace_formula_is_trace_formula_inner.intros(2))
next
  case (ImmConj x1 x2)
  then show ?case
    using  $\mathcal{O\_def}$  is_trace_formula_is_trace_formula_inner.intros(3)
    by (auto simp add:  $\mathcal{O\_def}$ )
next
  case (Obs x1 x2)
  then show ?case by (simp add:  $\mathcal{O\_def}$   $\mathcal{O\_inner\_def}$  is_trace_formula_is_trace_formula_inner.intros(4))
next
  case (Conj I  $\psi$ s)
  show ?case
  proof (rule impI)
    assume <Conj I  $\psi$ s  $\in \mathcal{O\_inner} (E \infty 0 0 0 0 0 0 0)$ >
    hence <I = {}>
      unfolding  $\mathcal{O\_inner\_def}$ 
      by (metis bot.extremum_uniqueI bot_enat_def energy.sel(3) expr_pr_inner.simps
        inst_conj_depth_inner.simps(2) le_iff_add leq_components
        mem_Collect_eq not_one_le_zero)
    then show <is_trace_formula_inner (Conj I  $\psi$ s)>
      by (simp add: is_trace_formula_is_trace_formula_inner.intros(5))
  qed
next
  case (StableConj I  $\psi$ s)
  show ?case
  proof (rule impI)
    assume <StableConj I  $\psi$ s  $\in \mathcal{O\_inner} (E \infty 0 0 0 0 0 0 0)$ >
    have <StableConj I  $\psi$ s  $\notin \mathcal{O\_inner} (E \infty 0 0 0 0 0 0 0)$ >
      by (simp add:  $\mathcal{O\_inner\_def}$ )
    with <StableConj I  $\psi$ s  $\in \mathcal{O\_inner} (E \infty 0 0 0 0 0 0 0)$ >
    show <is_trace_formula_inner (StableConj I  $\psi$ s)> by contradiction
  qed
next
  case (BranchConj  $\alpha$   $\varphi$  I  $\psi$ s)
  have <expr_pr_inner (BranchConj  $\alpha$   $\varphi$  I  $\psi$ s)  $\geq E 0 1 1 0 0 0 0 0$ >
    by simp
  hence <BranchConj  $\alpha$   $\varphi$  I  $\psi$ s  $\notin \mathcal{O\_inner} (E \infty 0 0 0 0 0 0 0)$ >
    unfolding  $\mathcal{O\_inner\_def}$  by simp
  thus ?case by blast
next
  case (Pos x)
  then show ?case by auto
next
  case (Neg x)
  then show ?case by auto
qed

lemma modal_depth_only_is_trace_form:
  <(is_trace_formula  $\varphi$ ) = ( $\varphi \in \mathcal{O} (E \infty 0 0 0 0 0 0 0)$ )>
  using expressiveness_to_trace_formula trace_formula_to_expressiveness by blast

```

```

context lts_tau
begin

```

If a trace formula φ is satisfied by a state p then there exists a weak trace tr of p such that $wtrace_to_srbb\ tr$ is equivalent to φ .

```

lemma trace_formula_implies_trace:
  fixes
     $\psi :: \langle 'a, 's \rangle\ hml\_srbb\_conjunct$ 
  shows
     $\langle is\_trace\_formula\ \varphi \implies p \models SRBB\ \varphi \implies \exists tr \in weak\_traces\ p. wtrace\_to\_srbb\ tr \Leftarrow srbb \Rightarrow \varphi \rangle$ 
     $\langle is\_trace\_formula\_inner\ \chi \implies hml\_srbb\_inner\_models\ q\ \chi \implies \exists tr \in weak\_traces\ q. wtrace\_to\_inner\ tr \Leftarrow \chi \Rightarrow \chi \rangle$ 
    True
proof (induction  $\varphi$  and  $\chi$  and  $\psi$  arbitrary:  $p$  and  $q$ )
  case TT
  thus ?case
    using weak_step_sequence.intros(1) silent_reachable.intros(1) by fastforce
next
  case (Internal  $\chi$ )
  hence  $\langle is\_trace\_formula\_inner\ \chi \rangle$ 
  using is_trace_formula.cases by blast
  from  $\langle p \models SRBB\ Internal\ \chi \rangle$ 
  have  $\langle \exists p'. p \twoheadrightarrow p' \wedge hml\_srbb\_inner\_models\ p'\ \chi \rangle$ 
  unfolding hml_srbb_models.simps .
  then obtain  $p'$  where  $\langle p \twoheadrightarrow p' \rangle\ \langle hml\_srbb\_inner\_models\ p'\ \chi \rangle$  by auto
  hence  $\langle hml\_srbb\_inner\_models\ p'\ \chi \rangle$  by auto
  with  $\langle is\_trace\_formula\_inner\ \chi \rangle$ 
  have  $\langle \exists tr \in weak\_traces\ p'. wtrace\_to\_inner\ tr \Leftarrow \chi \Rightarrow \chi \rangle$ 
  using Internal by blast
  then obtain  $tr$  where  $tr\_spec:$ 
     $\langle tr \in weak\_traces\ p' \rangle\ \langle wtrace\_to\_inner\ tr \Leftarrow \chi \Rightarrow \chi \rangle$  by auto
  with  $\langle p \twoheadrightarrow p' \rangle$  have  $\langle tr \in weak\_traces\ p \rangle$ 
  using silent_prepend_weak_traces by auto
  moreover have  $\langle wtrace\_to\_srbb\ tr \Leftarrow srbb \Rightarrow Internal\ \chi \rangle$ 
  proof (cases  $tr$ )
    case Nil
    thus ?thesis
      using srbb_TT_is_ $\chi$ TT  $tr\_spec$  by auto
  next
    case (Cons  $a\ tr$ )
    thus ?thesis
      using  $tr\_spec$  internal_srbb_cong
      by (metis  $wtrace\_to\_srbb.simps(2)$ )
  qed
  ultimately show ?case by blast
next
  case (ImmConj  $I\ \psi s$ )
  from  $\langle is\_trace\_formula\ (ImmConj\ I\ \psi s) \rangle$ 
  have  $\langle I = \{\} \rangle$ 
  by (simp add: is_trace_formula.simps)
  have  $\langle [] \in weak\_traces\ p \rangle$ 
  using silent_reachable.intros(1) weak_step_sequence.intros(1) by auto
  have  $\langle wtrace\_to\_srbb\ [] \Leftarrow srbb \Rightarrow ImmConj\ I\ \psi s \rangle$ 
  using srbb_TT_is_empty_conj  $\langle I = \{\} \rangle$ 
  unfolding  $wtrace\_to\_srbb.simps$  by auto
  thus  $\langle \exists tr \in weak\_traces\ p. wtrace\_to\_srbb\ tr \Leftarrow srbb \Rightarrow ImmConj\ I\ \psi s \rangle$ 
  using  $\langle [] \in weak\_traces\ p \rangle$  by auto
next
  case (Obs  $\alpha\ \varphi$ )
  thus ?case

```

```

proof (cases < $\alpha = \tau$ >)
  case True
  with <hml_srbb_inner_models q (Obs  $\alpha$   $\varphi$ )> have <q  $\models$  SRBB  $\varphi$ >
    using Obs.premis(1) silent_reachable.step empty_conj_trivial(1)
    by (metis (no_types, lifting) hml_srbb_inner.distinct(1) hml_srbb_inner.inject(1)
      hml_srbb_inner_models.simps(1) hml_srbb_models.simps(1,2) is_trace_formula.cases
      is_trace_formula_inner.cases)
  moreover have <is_trace_formula  $\varphi$ >
    using <is_trace_formula_inner (Obs  $\alpha$   $\varphi$ )> is_trace_formula_inner.cases by auto
  ultimately show < $\exists$  tr  $\in$  weak_traces q. wtrace_to_inner tr  $\Leftarrow \chi \Rightarrow$  Obs  $\alpha$   $\varphi$ >
    using Obs.IH
    by (metis < $\alpha = \tau$ > obs_srbb_cong prepend_ $\tau$ _weak_trace wtrace_to_inner.simps(2))
next
  case False
  from <is_trace_formula_inner (Obs  $\alpha$   $\varphi$ )>
  have <is_trace_formula  $\varphi$ >
    by (simp add: is_trace_formula_inner.simps)
  from <hml_srbb_inner_models q (Obs  $\alpha$   $\varphi$ )> and < $\alpha \neq \tau$ >
  have < $\exists$  q'. q  $\mapsto$   $\alpha$  q'  $\wedge$  q'  $\models$  SRBB  $\varphi$ > by simp
  then obtain q' where <q  $\mapsto$   $\alpha$  q'> <q'  $\models$  SRBB  $\varphi$ > by auto
  hence < $\exists$  tr'  $\in$  weak_traces q'. wtrace_to_srbb tr'  $\Leftarrow$  srbb  $\Rightarrow$   $\varphi$ >
    using <is_trace_formula  $\varphi$ > Obs by auto
  then obtain tr' where <tr'  $\in$  weak_traces q'> <wtrace_to_srbb tr'  $\Leftarrow$  srbb  $\Rightarrow$   $\varphi$ > by auto
  have <( $\alpha$  # tr')  $\in$  weak_traces q>
    using <q  $\mapsto$   $\alpha$  q'> <tr'  $\in$  weak_traces q'> step_prepend_weak_traces by auto
  from <wtrace_to_srbb tr'  $\Leftarrow$  srbb  $\Rightarrow$   $\varphi$ >
  have <Obs  $\alpha$  (wtrace_to_srbb tr')  $\Leftarrow \chi \Rightarrow$  Obs  $\alpha$   $\varphi$ >
    using obs_srbb_cong by auto
  then have <wtrace_to_inner ( $\alpha$  # tr')  $\Leftarrow \chi \Rightarrow$  Obs  $\alpha$   $\varphi$ >
    unfolding wtrace_to_inner.simps.
  with <( $\alpha$  # tr')  $\in$  weak_traces q>
  show < $\exists$  tr  $\in$  weak_traces q. wtrace_to_inner tr  $\Leftarrow \chi \Rightarrow$  Obs  $\alpha$   $\varphi$ > by blast
qed
next
  case (Conj I  $\psi$ s)
  from <is_trace_formula_inner (Conj I  $\psi$ s)> have <I = {}>
    by (simp add: is_trace_formula_inner.simps)
  have <(Conj {} ( $\lambda$ _. undefined))  $\Leftarrow \chi \Rightarrow$  (Conj {}  $\psi$ s)>
    using srbb_obs_ $\tau$ _is_ $\chi$ TT by simp
  then have <(Conj {} ( $\lambda$ _. undefined))  $\Leftarrow \chi \Rightarrow$  (Conj I  $\psi$ s)>
    using <I = {}> by auto
  then have <wtrace_to_inner []  $\Leftarrow \chi \Rightarrow$  Conj I  $\psi$ s>
    unfolding wtrace_to_inner.simps.
  with empty_trace_always_weak_trace[of q] show ?case by auto
qed (auto simp add: is_trace_formula_inner.simps)

lemma trace_equals_trace_to_formula:
  <t  $\in$  weak_traces p  $\longleftrightarrow$  p  $\models$  SRBB (wtrace_to_srbb t)>
proof
  assume <t  $\in$  weak_traces p>
  show <p  $\models$  SRBB (wtrace_to_srbb t)>
    using <t  $\in$  weak_traces p>
  proof (induction t arbitrary: p)
    case Nil
    then show ?case
      by simp
  next
    case (Cons a tail)
    then obtain p'' p' where <p  $\Rightarrow \mapsto \Rightarrow$  a p''> <p''  $\Rightarrow \mapsto \Rightarrow$  $ tail p''>
      using weak_step_sequence.simps
      by (smt (verit, best) list.discI list.inject mem_Collect_eq)

```

```

with Cons(1) have IS: <p''  $\models$ SRBB wtrace_to_srbb tail>
  by blast
from Cons have <wtrace_to_srbb (a # tail) = (Internal (Obs a (wtrace_to_srbb tail)))>
  by simp
thus ?case
  by (smt (verit) Cons.IH IS lts_tau.hml_srbb_inner_models.simps(1)
      lts_tau.silent_reachable_trans <p  $\rightarrow$  $\mapsto$  $\rightarrow$  a p''> empty_trace_allways_weak_trace
      hml_srbb_models.simps(2) weak_step_def wtrace_to_srbb.elims)
qed
next
assume <p  $\models$ SRBB wtrace_to_srbb t>
then show <t  $\in$  weak_traces p>
proof(induction t arbitrary: p)
  case Nil
  then show ?case
    using weak_step_sequence.intros(1) silent_reachable.intros(1) by auto
next
  case (Cons a tail)
  hence <p  $\models$ SRBB (Internal (Obs a (wtrace_to_srbb tail)))>
    by simp
  thus ?case
    using Cons prepend_ $\tau$ _weak_trace silent_prepend_weak_traces step_prepend_weak_traces
    by fastforce
qed
qed

lemma expr_preorder_characterizes_relational_preorder_traces:
  <(p  $\lesssim$ WT q) = (p  $\preceq$  (E  $\infty$  0 0 0 0 0 0) q)>
  unfolding expr_preord_def preordered_def
proof
  assume <p  $\lesssim$ WT q>
  thus < $\forall \varphi \in \mathcal{O}$  (E  $\infty$  0 0 0 0 0 0). p  $\models$ SRBB  $\varphi \rightarrow$  q  $\models$ SRBB  $\varphi$ >
    using expressiveness_to_trace_formula trace_equals_trace_to_formula
    trace_formula_implies_trace
    unfolding weakly_trace_preordered_def
    by (metis (no_types, lifting) eq_equality in_mono)
next
  assume  $\varphi_{\text{eneg}}$ : < $\forall \varphi \in \mathcal{O}$  (E  $\infty$  0 0 0 0 0 0). p  $\models$ SRBB  $\varphi \rightarrow$  q  $\models$ SRBB  $\varphi$ >
  thus <p  $\lesssim$ WT q>
    unfolding weakly_trace_preordered_def
    using trace_equals_trace_to_formula trace_formula_to_expressiveness
    trace_to_srbb_is_trace_formula
    by fastforce
qed

Two states p and q are weakly trace equivalent if and only if they are equivalent with respect
to the coordinate ( $\infty$ , 0, 0, 0, 0, 0, 0, 0).

theorem weak_traces_coordinate: <(p  $\simeq$ WT q) = (p  $\sim$  (E  $\infty$  0 0 0 0 0 0) q)>
  using expr_preorder_characterizes_relational_preorder_traces
  unfolding weakly_trace_equivalent_def expr_equiv_def  $\mathcal{O}_{\text{def}}$  expr_preord_def
  by simp

end

end

```

5 η -Bisimilarity and η -Similarity

```
theory Eta_Bisimilarity
  imports Expressiveness_Price
begin
```

η -Bisimilarity and η -Similarity are comparably arcane notions of behavioral equivalence. We show that they are characterized by coordinates $E \infty \infty \infty 0 0 \infty \infty \infty$ and $E \infty \infty \infty 0 0 \infty 0 0$ as an illustration of how to connect coordinates and relational characterizations of equivalences.

5.1 Definition and Properties of η -(Bi-)Similarity

```
context lts_tau
begin
```

We characterize η -bisimilarity through symmetric η -simulations.

```
definition eta_simulation :: <'s  $\Rightarrow$  's  $\Rightarrow$  bool $\Rightarrow$  bool> where
  <eta_simulation R  $\equiv$   $\forall p \alpha p' q. R p q \longrightarrow p \mapsto \alpha p' \longrightarrow$ 
    ( $\alpha = \tau \wedge R p' q$ )
     $\vee (\exists q' q'' q'''. q \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge q'' \twoheadrightarrow q''' \wedge R p q' \wedge R p' q''')$ >
```

```
definition eta_bisimulated :: <'s  $\Rightarrow$  's  $\Rightarrow$  bool> (infix <~ $\eta$ > 40) where
  <p ~ $\eta$  q  $\equiv$   $\exists R. \text{eta\_simulation } R \wedge \text{symp } R \wedge R p q$ >
```

```
lemma eta_bisim_sim:
  shows <eta_simulation (~ $\eta$ )>
  unfolding eta_bisimulated_def eta_simulation_def by blast
```

```
lemma eta_bisim_sym:
  assumes <p ~ $\eta$  q>
  shows <q ~ $\eta$  p>
  using assms unfolding eta_bisimulated_def
  by (meson sympD)
```

```
lemma silence_retains_eta_sim:
  assumes
    <eta_simulation R>
    <R p q>
    <p  $\twoheadrightarrow$  p'>
  shows < $\exists q'. R p' q' \wedge q \twoheadrightarrow q'$ >
  using assms(3,2)
proof (induct arbitrary: q)
  case (refl p)
  then show ?case
    using silent_reachable.refl by blast
next
  case (step p p' p'')
  then obtain q' where <R p' q'> <q  $\twoheadrightarrow$  q'>
  using <eta_simulation R> silent_reachable.refl
    silent_reachable_append_ $\tau$  silent_reachable_trans
  unfolding eta_simulation_def by blast
  then obtain q'' where <R p'' q''> <q'  $\twoheadrightarrow$  q''> using step by blast
  then show ?case
    using <q  $\twoheadrightarrow$  q'> silent_reachable_trans by blast
qed
```

```
lemma eta_bisimulated_silently_retained:
  assumes
    <p ~ $\eta$  q>
    <p  $\twoheadrightarrow$  p'>
```

```

shows
  < $\exists q'. q \Rightarrow q' \wedge p' \sim_{\eta} q'$ > using assms(2,1)
using silence_retains_eta_sim unfolding eta_bisimulated_def by blast

```

5.2 Logical Characterization of η -Bisimilarity through Expressiveness Price

lemma logic_eta_bisim_invariant:

```

assumes
  <p0 ~ $\eta$  q0>
  < $\varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty)$ >
  <p0  $\models_{\text{SRBB}}$   $\varphi$ >
shows <q0  $\models_{\text{SRBB}}$   $\varphi$ >
proof -
  have < $\bigwedge \varphi \chi \psi.$ 
    ( $\forall p q. p \sim_{\eta} q \rightarrow \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty) \rightarrow p \models_{\text{SRBB}} \varphi \rightarrow q \models_{\text{SRBB}} \varphi$ )  $\wedge$ 
    ( $\forall p q. p \sim_{\eta} q \rightarrow \chi \in \mathcal{O}_{\text{inner}} (E \infty \infty \infty 0 0 \infty \infty \infty) \rightarrow$ 
       $\rightarrow \text{hml\_srbb\_inner\_models } p \chi \rightarrow (\exists q'. q \Rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \chi)) \wedge$ 
    ( $\forall p q. p \sim_{\eta} q \rightarrow \psi \in \mathcal{O}_{\text{conjunct}} (E \infty \infty \infty 0 0 \infty \infty \infty) \rightarrow$ 
       $\rightarrow \text{hml\_srbb\_conjunct\_models } p \psi \rightarrow \text{hml\_srbb\_conjunct\_models } q \psi$ )>
  proof -
    fix  $\varphi \chi \psi$ 
    show
      <( $\forall p q. p \sim_{\eta} q \rightarrow \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty) \rightarrow p \models_{\text{SRBB}} \varphi \rightarrow q \models_{\text{SRBB}} \varphi$ )  $\wedge$ 
      ( $\forall p q. p \sim_{\eta} q \rightarrow \chi \in \mathcal{O}_{\text{inner}} (E \infty \infty \infty 0 0 \infty \infty \infty) \rightarrow$ 
         $\rightarrow \text{hml\_srbb\_inner\_models } p \chi \rightarrow (\exists q'. q \Rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \chi)) \wedge$ 
      ( $\forall p q. p \sim_{\eta} q \rightarrow \psi \in \mathcal{O}_{\text{conjunct}} (E \infty \infty \infty 0 0 \infty \infty \infty) \rightarrow$ 
         $\rightarrow \text{hml\_srbb\_conjunct\_models } p \psi \rightarrow \text{hml\_srbb\_conjunct\_models } q \psi$ )>
  proof (induct rule: hml_srbb_hml_srbb_inner_hml_srbb_conjunct.induct)
    case TT
    then show ?case by simp
  next
    case (Internal  $\chi$ )
    show ?case
    proof safe
      fix p q
      assume case_assms:
        <p ~ $\eta$  q> <p  $\models_{\text{SRBB}}$  hml_srbb.Internal  $\chi$ > <Internal  $\chi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty)$ >
      then obtain p' where p'_spec: <p  $\Rightarrow$  p'> <hml_srbb_inner_models p'  $\chi$ > by auto
      have < $\chi \in \mathcal{O}_{\text{inner}} (E \infty \infty \infty 0 0 \infty \infty \infty)$ >
        using case_assms(3) unfolding  $\mathcal{O}_{\text{inner\_def}}$   $\mathcal{O}_{\text{def}}$  by auto
      hence < $\exists q'. q \Rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \chi$ >
        using Internal case_assms(1) p'_spec eta_bisimulated_silently_retained
        by (meson silent_reachable_trans)
      thus <q  $\models_{\text{SRBB}}$  hml_srbb.Internal  $\chi$ > by auto
    qed
  next
    case (ImmConj I  $\Psi$ )
    then show ?case unfolding  $\mathcal{O}_{\text{inner\_def}}$   $\mathcal{O}_{\text{def}}$  by auto
  next
    case (Obs  $\alpha \varphi$ )
    then show ?case
    proof (safe)
      fix p q
      assume case_assms:
        <p ~ $\eta$  q>
        <Obs  $\alpha \varphi \in \mathcal{O}_{\text{inner}} (E \infty \infty \infty 0 0 \infty \infty \infty)$ >
        <hml_srbb_inner_models p (hml_srbb_inner.Obs  $\alpha \varphi$ )>
      hence < $\varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty)$ > unfolding  $\mathcal{O}_{\text{inner\_def}}$   $\mathcal{O}_{\text{def}}$  by auto
      hence no_imm_conj: < $\nexists I \Psi. \varphi = \text{ImmConj } I \Psi \wedge I \neq \{\}$ > unfolding  $\mathcal{O}_{\text{def}}$  by force
      have back_step: < $\forall p0 p1. p1 \models_{\text{SRBB}} \varphi \rightarrow p0 \Rightarrow p1 \rightarrow p0 \models_{\text{SRBB}} \varphi$ >

```

```

proof (cases  $\varphi$ )
  case TT
  then show ?thesis by auto
next
  case (Internal _)
  then show ?thesis
    using silent_reachable_trans by auto
next
  case (ImmConj _ _)
  then show ?thesis using no_imm_conj by auto
qed
from case_assms obtain  $p'$  where  $\langle p \mapsto_a \alpha p' \rangle \langle p' \models_{\text{SRBB}} \varphi \rangle$  by auto
then obtain  $q' q'' q'''$  where  $\langle q \twoheadrightarrow q' \rangle \langle q' \mapsto_a \alpha q'' \rangle \langle q'' \twoheadrightarrow q''' \rangle \langle p' \sim_\eta q''' \rangle$ 
  using  $\langle p \sim_\eta q \rangle$  eta_bisim_sim unfolding eta_simulation_def
  using silent_reachable.refl by blast
hence  $\langle q''' \models_{\text{SRBB}} \varphi \rangle$ 
  using  $\langle p' \models_{\text{SRBB}} \varphi \rangle$  Obs  $\langle \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty) \rangle$  by blast
hence  $\langle \text{hml\_srbb\_inner\_models } q' (\text{hml\_srbb\_inner.Obs } \alpha \varphi) \rangle$ 
  using  $\langle q' \mapsto_a \alpha q'' \rangle \langle q'' \twoheadrightarrow q''' \rangle$  back_step by auto
thus  $\langle \exists q'. q \twoheadrightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' (\text{hml\_srbb\_inner.Obs } \alpha \varphi) \rangle$ 
  using  $\langle q \twoheadrightarrow q' \rangle$  by blast
qed
next
  case (Conj I  $\Psi$ )
  show ?case
  proof safe
    fix  $p q$ 
    assume case_assms:
       $\langle p \sim_\eta q \rangle$ 
       $\langle \text{Conj } I \Psi \in \mathcal{O}_{\text{inner}} (E \infty \infty \infty 0 0 \infty \infty \infty) \rangle$ 
       $\langle \text{hml\_srbb\_inner\_models } p (\text{Conj } I \Psi) \rangle$ 
    hence conj_price:  $\langle \forall i \in I. \Psi i \in \mathcal{O}_{\text{conjunct}} (E \infty \infty \infty 0 0 \infty \infty \infty) \rangle$ 
      unfolding  $\mathcal{O}_{\text{conjunct\_def}}$   $\mathcal{O}_{\text{inner\_def}}$ 
      by (simp, metis SUP_bot_conv(1) le_zero_eq sup_bot_left sup_ge1)
    from case_assms have  $\langle \forall i \in I. \text{hml\_srbb\_conjunct\_models } p (\Psi i) \rangle$  by auto
    hence  $\langle \forall i \in I. \text{hml\_srbb\_conjunct\_models } q (\Psi i) \rangle$ 
      using Conj  $\langle p \sim_\eta q \rangle$  conj_price by blast
    hence  $\langle \text{hml\_srbb\_inner\_models } q (\text{hml\_srbb\_inner.Conj } I \Psi) \rangle$  by simp
    thus  $\langle \exists q'. q \twoheadrightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' (\text{hml\_srbb\_inner.Conj } I \Psi) \rangle$ 
      using silent_reachable.refl by blast
  qed
next
  case (StableConj I  $\Psi$ )
  thus ?case unfolding  $\mathcal{O}_{\text{inner\_def}}$   $\mathcal{O}_{\text{def}}$  by auto
next
  case (BranchConj  $\alpha \varphi I \Psi$ )
  show ?case
  proof safe
    fix  $p q$ 
    assume case_assms:
       $\langle p \sim_\eta q \rangle$ 
       $\langle \text{BranchConj } \alpha \varphi I \Psi \in \mathcal{O}_{\text{inner}} (E \infty \infty \infty 0 0 \infty \infty \infty) \rangle$ 
       $\langle \text{hml\_srbb\_inner\_models } p (\text{BranchConj } \alpha \varphi I \Psi) \rangle$ 
    hence  $\langle \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty) \rangle$  unfolding  $\mathcal{O}_{\text{inner\_def}}$   $\mathcal{O}_{\text{def}}$ 
      by (simp, metis le_zero_eq sup_ge1)
    hence no_imm_conj:  $\langle \nexists I \Psi. \varphi = \text{ImmConj } I \Psi \wedge I \neq \{\} \rangle$  unfolding  $\mathcal{O}_{\text{def}}$  by force
    have back_step:  $\langle \forall p_0 p_1. p_1 \models_{\text{SRBB}} \varphi \longrightarrow p_0 \twoheadrightarrow p_1 \longrightarrow p_0 \models_{\text{SRBB}} \varphi \rangle$ 
  proof (cases  $\varphi$ )
    case TT
    then show ?thesis by auto
  next

```

```

    case (Internal _)
    then show ?thesis
      using silent_reachable_trans by auto
  next
    case (ImmConj _ _)
    then show ?thesis using no_imm_conj by auto
qed
from case_assms have conj_price:  $\langle \forall i \in I. \Psi \ i \in \mathcal{O}_{\text{conjunct}} (E \ \infty \ \infty \ \infty \ 0 \ 0 \ \infty \ \infty \ \infty) \rangle$ 
  unfolding  $\mathcal{O}_{\text{conjunct\_def}}$   $\mathcal{O}_{\text{inner\_def}}$ 
  by (simp, metis SUP_bot_conv(1) le_zero_eq sup_bot_left sup_ge1)
from case_assms have  $\langle \forall i \in I. \text{hml\_srbb\_conjunct\_models } p \ (\Psi \ i) \rangle$ 
   $\langle \text{hml\_srbb\_inner\_models } p \ (\text{Obs } \alpha \ \varphi) \rangle$ 
  using branching_conj_parts branching_conj_obs by blast+
then obtain p' where  $\langle p \mapsto_a \alpha \ p' \rangle \ \langle p' \models_{\text{SRBB}} \varphi \rangle$  by auto
then obtain q' q'' q''' where q'_q''_spec:
   $\langle q \Rightarrow q' \rangle \ \langle q' \mapsto_a \alpha \ q'' \rangle \ \langle q'' \Rightarrow q''' \rangle$ 
   $\langle p \sim_\eta q' \rangle \ \langle p' \sim_\eta q''' \rangle$ 
  using eta_bisim_sim  $\langle p \sim_\eta q \rangle$  silent_reachable.refl
  unfolding eta_simulation_def by blast
hence  $\langle q''' \models_{\text{SRBB}} \varphi \rangle$ 
  using BranchConj.hyps  $\langle p' \models_{\text{SRBB}} \varphi \rangle \ \langle \varphi \in \mathcal{O} (E \ \infty \ \infty \ \infty \ 0 \ 0 \ \infty \ \infty \ \infty) \rangle$  by auto
hence  $\langle q'' \models_{\text{SRBB}} \varphi \rangle$  using back_step q'_q''_spec by blast
hence  $\langle \text{hml\_srbb\_inner\_models } q' \ (\text{Obs } \alpha \ \varphi) \rangle$  using q'_q''_spec by auto
moreover have  $\langle \forall i \in I. \text{hml\_srbb\_conjunct\_models } q' \ (\Psi \ i) \rangle$ 
  using BranchConj.hyps  $\langle \forall i \in I. \text{hml\_srbb\_conjunct\_models } p \ (\Psi \ i) \rangle \ q'_q''_spec \ \text{conj\_price}$ 
  by blast
ultimately show  $\langle \exists q'. q \Rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \ (\text{BranchConj } \alpha \ \varphi \ I \ \Psi) \rangle$ 
  using  $\langle q \Rightarrow q' \rangle$  by auto
qed
next
case (Pos  $\chi$ )
show ?case
proof safe
  fix p q
  assume case_assms:
     $\langle p \sim_\eta q \rangle$ 
     $\langle \text{Pos } \chi \in \mathcal{O}_{\text{conjunct}} (E \ \infty \ \infty \ \infty \ 0 \ 0 \ \infty \ \infty \ \infty) \rangle$ 
     $\langle \text{hml\_srbb\_conjunct\_models } p \ (\text{Pos } \chi) \rangle$ 
  hence  $\langle \chi \in \mathcal{O}_{\text{inner}} (E \ \infty \ \infty \ \infty \ 0 \ 0 \ \infty \ \infty \ \infty) \rangle$ 
    unfolding  $\mathcal{O}_{\text{inner\_def}}$   $\mathcal{O}_{\text{conjunct\_def}}$  by simp
  from case_assms obtain p' where  $\langle p \Rightarrow p' \rangle \ \langle \text{hml\_srbb\_inner\_models } p' \ \chi \rangle$  by auto
  then obtain q' where  $\langle q \Rightarrow q' \rangle \ \langle \text{hml\_srbb\_inner\_models } q' \ \chi \rangle$ 
    using Pos  $\langle p \sim_\eta q \rangle \ \langle \chi \in \mathcal{O}_{\text{inner}} (E \ \infty \ \infty \ \infty \ 0 \ 0 \ \infty \ \infty \ \infty) \rangle$ 
    by (meson eta_bisimulated_silently_retained silent_reachable_trans)
  thus  $\langle \text{hml\_srbb\_conjunct\_models } q \ (\text{Pos } \chi) \rangle$  by auto
qed
next
case (Neg  $\chi$ )
show ?case
proof safe
  fix p q
  assume case_assms:
     $\langle p \sim_\eta q \rangle$ 
     $\langle \text{Neg } \chi \in \mathcal{O}_{\text{conjunct}} (E \ \infty \ \infty \ \infty \ 0 \ 0 \ \infty \ \infty \ \infty) \rangle$ 
     $\langle \text{hml\_srbb\_conjunct\_models } p \ (\text{Neg } \chi) \rangle$ 
  hence  $\langle \chi \in \mathcal{O}_{\text{inner}} (E \ \infty \ \infty \ \infty \ 0 \ 0 \ \infty \ \infty \ \infty) \rangle$ 
    unfolding  $\mathcal{O}_{\text{inner\_def}}$   $\mathcal{O}_{\text{conjunct\_def}}$  by simp
  from case_assms have  $\langle \forall p'. p \Rightarrow p' \longrightarrow \neg \text{hml\_srbb\_inner\_models } p' \ \chi \rangle$  by simp
  moreover have
     $\langle (\exists q'. q \Rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \ \chi) \longrightarrow (\exists p'. p \Rightarrow p' \wedge \text{hml\_srbb\_inner\_models } p' \ \chi) \rangle$ 

```

```

    using Neg eta_bisim_sym[OF <p ~η q>] eta_bisimulated_silently_retained
    silent_reachable_trans <χ ∈ O_inner (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)> by blast
    ultimately have <∀q'. q ⇒ q' → ¬hml_srbbs_inner_models q' χ> by blast
    thus <hml_srbbs_conjunct_models q (Neg χ)> by simp
  qed
qed
qed
thus ?thesis using assms by blast
qed

lemma modal_eta_sim_eq: <eta_simulation (equivalent (O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)))>
proof -
  have <#p α p' q. (equivalent (O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞))) p q ∧ p ↦ α p' ∧
    (α ≠ τ ∨ ¬(equivalent (O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞))) p' q) ∧
    (∀q' q'' q'''. q ⇒ q' → q' ↦ α q'' → q'' ⇒ q''')
    → ¬ equivalent (O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)) p q'
    ∨ ¬ equivalent (O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)) p' q''')>
  proof clarify
    fix p α p' q
    define Qα where
      <Qα ≡ {q'. q ⇒ q' ∧ (#φ. φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞))
        ∧ (distinguishes φ p q' ∨ distinguishes φ q' p)}>
    assume contradiction:
      <equivalent (O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)) p q> <p ↦ α p'>
      <∀q' q'' q'''. q ⇒ q' → q' ↦ α q'' → q'' ⇒ q''''>
      → ¬ equivalent (O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)) p q'
      ∨ ¬ equivalent (O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)) p' q''')
      <α ≠ τ ∨ ¬ equivalent (O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)) p' q>
    hence distinctions: <∀q'. q ⇒ q' →
      (∃φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞). distinguishes φ p q' ∨ distinguishes φ q' p) ∨
      (∀q'' q'''. q' ↦ α q'' → q'' ⇒ q''')
      → (∃φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞).
        distinguishes φ p' q'' ∨ distinguishes φ q'' p'))>
    unfolding equivalent_no_distinction
    by (metis silent_reachable.cases silent_reachable.refl)
    hence <∀q'' q'''. ∃q' ∈ Qα. q' ↦ α q'' → q'' ⇒ q''''>
      → (∃φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞).
        distinguishes φ p' q'' ∨ distinguishes φ q'' p'))
    unfolding Qα_def using silent_reachable.refl by fastforce
    hence <∀q'' q'''. q'' ⇒ q'''' → (∃q'. q ⇒ q' ∧ (#φ. φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞))
      ∧ (distinguishes φ p q' ∨ distinguishes φ q' p)) ∧ q' ↦ α q''>
      → (∃φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞).
        distinguishes φ p' q'' ∨ distinguishes φ q'' p'))
    unfolding Qα_def by blast
    hence <∀q'''. (∃q' q''. q ⇒ q' ∧ (#φ. φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞))
      ∧ (distinguishes φ p q' ∨ distinguishes φ q' p)) ∧ q' ↦ α q'' ∧ q'' ⇒ q''''>
      → (∃φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞).
        distinguishes φ p' q'' ∨ distinguishes φ q'' p'))
    by blast
    then obtain Φα where Φα_def:
      <∀q'''. (∃q' q''. q ⇒ q' ∧ (#φ. φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞))
        ∧ (distinguishes φ p q' ∨ distinguishes φ q' p)) ∧ q' ↦ α q'' ∧ q'' ⇒ q''''
        → (Φα q''') ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)
        ∧ (distinguishes (Φα q''') p' q'' ∨ distinguishes (Φα q''') q'' p'))> by metis
    hence distinctions_α: <∀q' ∈ Qα. ∀q'' q'''.
      q' ↦ α q'' → q'' ⇒ q''''
      → distinguishes (Φα q''') p' q'' ∨ distinguishes (Φα q''') q'' p'>
    unfolding Qα_def by blast
    from distinctions obtain Φη where
      <∀q'. q' ∈ {q'. q ⇒ q' ∧ (∃φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞).
        distinguishes φ p q' ∨ distinguishes φ q' p)}>

```

```

    → (distinguishes (Φη q') p q' ∨ distinguishes (Φη q') q' p)
      ∧ (Φη q') ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)
  unfolding mem_Collect_eq by moura
  hence
    <∀q'∈{q'. q → q' ∧ (∃φ∈O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)).
      distinguishes φ p q' ∨ distinguishes φ q' p}>.
      (distinguishes (Φη q') p q' ∨ distinguishes (Φη q') q' p)
    <∀q'∈{q'. q → q' ∧ (∃φ∈O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)).
      distinguishes φ p q' ∨ distinguishes φ q' p}>.
      (Φη q') ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)
  by blast+
  from distinction_conjunctification_two_way[OF this(1)]
    distinction_conjunctification_two_way_price[OF this]
  have <∀q'∈{q'. q → q' ∧ (∃φ∈O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)).
    distinguishes φ p q' ∨ distinguishes φ q' p}>.
    hml_srbb_conj.distinguishes (
      (if distinguishes (Φη q') p q'
        then conjunctify_distinctions
        else conjunctify_distinctions_dual) Φη p q') p q'
    ∧ (if distinguishes (Φη q') p q'
      then conjunctify_distinctions
      else conjunctify_distinctions_dual) Φη p q' ∈ O_conjunct (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)
  by fastforce
  then obtain Ψη where distinctions_η:
    <∀q'∈{q'. q → q' ∧ (∃φ∈O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)).
      distinguishes φ p q' ∨ distinguishes φ q' p}>.
    hml_srbb_conj.distinguishes (Ψη q') p q'
    ∧ Ψη q' ∈ O_conjunct (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)
  by auto
  have <p ↦ a α p'> using <p ↦ α p'> by simp
  from distinction_combination_eta_two_way[OF this, of q Φα] distinctions_α have obs_dist:
    <∀q'∈Qα.
      hml_srbb_inner.distinguishes (
        Obs α (Internal (Conj {q'''. ∃q'∈Qα. ∃q''. q' ↦ a α q'' ∧ q'' → q'''}
          (λq'''. (if distinguishes (Φα q''') p' q'''
            then conjunctify_distinctions else conjunctify_distinctions_dual) Φα p'
              q'''))))
        ) p q'>
  unfolding Qα_def by fastforce
  have <Qα ≠ {}>
  using Qα_def contradiction(1) silent_reachable.refl by fastforce
  hence conjunct_prices: <∀q'''∈{q'''. ∃q'∈Qα. ∃q''. q' ↦ a α q'' ∧ q'' → q'''}>.
    ((if distinguishes (Φα q''') p' q'''
      then conjunctify_distinctions
      else conjunctify_distinctions_dual) Φα p' q'''
    ) ∈ O_conjunct (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)
  using distinction_conjunctification_two_way_price[of
    <{q'''. ∃q'∈Qα. ∃q''. q' ↦ a α q'' ∧ q'' → q'''}>]
  using Qα_def Φα_def by auto
  have <(Conj {q'''. ∃q'∈Qα. ∃q''. q' ↦ a α q'' ∧ q'' → q'''}
    (λq'''. (if distinguishes (Φα q''') p' q'''
      then conjunctify_distinctions else conjunctify_distinctions_dual)
        Φα p' q''')) ∈ O_inner (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)>
  proof (cases <{q'''. ∃q'∈Qα. ∃q''. q' ↦ a α q'' ∧ q'' → q'''} = {}>)
  case True
  then show ?thesis
    unfolding O_inner_def O_conjunct_def
    by (auto simp add: True bot_enat_def)
  next
  case False
  then show ?thesis

```

```

using conjunct_prices
unfolding O_inner_def O_conjunct_def by force
qed
hence obs_price: <(Obs  $\alpha$  (Internal (Conj {q'''.  $\exists q' \in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \twoheadrightarrow q'''$ })
  ( $\lambda q'''$ . (if distinguishes ( $\Phi\alpha q'''$ ) p' q'''
    then conjunctify_distinctions else conjunctify_distinctions_dual
      )  $\Phi\alpha p' q'''$ ))))  $\in \mathcal{O}_{\text{inner}}$  ( $E \infty \infty \infty 0 0 \infty \infty \infty$ )>
using distinction_conjunctification_price distinctions_ $\alpha$ 
unfolding O_inner_def O_def by simp
from obs_dist distinctions_ $\eta$  have
  <hml_srbb_inner_models p (BranchConj  $\alpha$ 
    (Internal (Conj {q'''.  $\exists q' \in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \twoheadrightarrow q'''$ })
      ( $\lambda q'''$ . (if distinguishes ( $\Phi\alpha q'''$ ) p' q'''
        then conjunctify_distinctions else conjunctify_distinctions_dual
          )  $\Phi\alpha p' q'''$ ))))
    {q'.  $q \twoheadrightarrow q' \wedge (\exists \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty))$ .
      distinguishes  $\varphi p q' \vee$  distinguishes  $\varphi q' p$ }  $\Psi\eta$ >
using <Q $\alpha \neq \{\}$ > silent_reachable.refl
unfolding hml_srbb_conj.distinguishes_def hml_srbb_inner.distinguishes_def
by (smt (verit) Q $\alpha$ _def empty_Collect_eq hml_srbb_inner_models.simps(1,4) mem_Collect_eq)
moreover have < $\forall q'. q \twoheadrightarrow q' \longrightarrow \neg$  hml_srbb_inner_models q'
  (BranchConj  $\alpha$ 
    (Internal (Conj {q'''.  $\exists q' \in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \twoheadrightarrow q'''$ })
      ( $\lambda q'''$ . (if distinguishes ( $\Phi\alpha q'''$ ) p' q'''
        then conjunctify_distinctions
          else conjunctify_distinctions_dual)  $\Phi\alpha p' q'''$ ))))
    {q'.  $q \twoheadrightarrow q' \wedge (\exists \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty))$ .
      distinguishes  $\varphi p q' \vee$  distinguishes  $\varphi q' p$ }  $\Psi\eta$ >
proof safe
fix q'
assume contradiction: <q  $\twoheadrightarrow$  q'>
  <hml_srbb_inner_models q' (BranchConj  $\alpha$ 
    (Internal (Conj {q'''.  $\exists q' \in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \twoheadrightarrow q'''$ })
      ( $\lambda q'''$ . (if distinguishes ( $\Phi\alpha q'''$ ) p' q'''
        then conjunctify_distinctions
          else conjunctify_distinctions_dual)  $\Phi\alpha p' q'''$ ))))
    {q'.  $q \twoheadrightarrow q' \wedge (\exists \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty))$ .
      distinguishes  $\varphi p q' \vee$  distinguishes  $\varphi q' p$ }  $\Psi\eta$ >
  thus <False>
using obs_dist distinctions_ $\eta$  branching_conj_obs branching_conj_parts
unfolding distinguishes_def hml_srbb_conj.distinguishes_def
  hml_srbb_inner.distinguishes_def Q $\alpha$ _def
by blast
qed
moreover have branch_price:
  <(BranchConj  $\alpha$ 
    (Internal (Conj {q'''.  $\exists q' \in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \twoheadrightarrow q'''$ })
      ( $\lambda q'''$ . (if distinguishes ( $\Phi\alpha q'''$ ) p' q'''
        then conjunctify_distinctions
          else conjunctify_distinctions_dual)  $\Phi\alpha p' q'''$ ))))
    {q'.  $q \twoheadrightarrow q' \wedge (\exists \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty \infty \infty))$ .
      distinguishes  $\varphi p q' \vee$  distinguishes  $\varphi q' p$ }  $\Psi\eta$ )
   $\in \mathcal{O}_{\text{inner}}$  ( $E \infty \infty \infty 0 0 \infty \infty \infty$ )>
using distinctions_ $\eta$  obs_price
unfolding Q $\alpha$ _def O_inner_def O_def O_conjunct_def  $\Phi\alpha$ _def
by (simp, metis (mono_tags, lifting) SUP_bot_conv(2) bot_enat_def sup_bot_left)
ultimately have <distinguishes (Internal (BranchConj  $\alpha$ 
  (Internal (Conj {q'''.  $\exists q' \in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \twoheadrightarrow q'''$ })

```

```

      (λq'''. (if distinguishes (Φα q''') p' q'''
        then conjunctify_distinctions else conjunctify_distinctions_dual) Φα p'
        q'''))
    {q'. q → q' ∧ (∃φ∈O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞).
      distinguishes φ p q' ∨ distinguishes φ q' p)} Ψη)) p q>
  unfolding distinguishes_def Qα_def
  using silent_reachable.refl hml_srbbs_models.simps(2) by blast
  moreover have <(Internal (BranchConj α
    (Internal (Conj {q'''. ∃q'∈Qα. ∃q''. q' →a α q'' ∧ q'' → q'''}
      (λq'''. (if distinguishes (Φα q''') p' q'''
        then conjunctify_distinctions else conjunctify_distinctions_dual) Φα p'
        q'''))))
    {q'. q → q' ∧ (∃φ∈O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞).
      distinguishes φ p q' ∨ distinguishes φ q' p)} Ψη))
  ∈ O (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞)>
  using branch_price
  unfolding Qα_def O_def O_conjunct_def
  by (metis (no_types, lifting) O_inner_def expr_internal_eq mem_Collect_eq)
  ultimately show False using contradiction(1) equivalent_no_distinction by blast
qed
thus ?thesis
  unfolding eta_simulation_def by blast
qed

theorem eta_bisim_coordinate: <(p ~η q) = (p ~ (E ∞ ∞ ∞ 0 0 ∞ ∞ ∞) q)>
  using modal_eta_sim_eq logic_eta_bisim_invariant sympD equivalent_no_distinction
  unfolding eta_bisimulated_def expr_equiv_def distinguishes_def
  by (smt (verit, best) equivalent_equiv equivE)

```

5.3 η -Similarity

```

lemma logic_eta_sim_invariant:
  assumes
    <∃R. eta_simulation R ∧ R p0 q0>
    <φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
    <p0 ⊨SRBB φ>
  shows <q0 ⊨SRBB φ>
proof -
  have <∧φ χ ψ.
    (∀p q. (∃R. eta_simulation R ∧ R p q) → φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0)
      → p ⊨SRBB φ → q ⊨SRBB φ) ∧
    (∀p q. (∃R. eta_simulation R ∧ R p q) → χ ∈ O_inner (E ∞ ∞ ∞ 0 0 ∞ 0 0)
      → hml_srbbs_inner_models p χ → (∃q'. q → q' ∧ hml_srbbs_inner_models q' χ)) ∧
    (∀p q. (∃R. eta_simulation R ∧ R p q) → ψ ∈ O_conjunct (E ∞ ∞ ∞ 0 0 ∞ 0 0)
      → hml_srbbs_conjunct_models p ψ → hml_srbbs_conjunct_models q ψ)>
  proof -
    fix φ χ ψ
    show
      <(∀p q. (∃R. eta_simulation R ∧ R p q) → φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0)
        → p ⊨SRBB φ → q ⊨SRBB φ) ∧
        (∀p q. (∃R. eta_simulation R ∧ R p q) → χ ∈ O_inner (E ∞ ∞ ∞ 0 0 ∞ 0 0)
          → hml_srbbs_inner_models p χ → (∃q'. q → q' ∧ hml_srbbs_inner_models q' χ)) ∧
        (∀p q. (∃R. eta_simulation R ∧ R p q) → ψ ∈ O_conjunct (E ∞ ∞ ∞ 0 0 ∞ 0 0)
          → hml_srbbs_conjunct_models p ψ → hml_srbbs_conjunct_models q ψ)>
  proof (induct rule: hml_srbbs_hml_srbbs_inner_hml_srbbs_conjunct.induct)
    case TT
    then show ?case by simp
  next
    case (Internal χ)
    show ?case
  proof safe

```

```

fix p q R
assume case_assms:
  <eta_simulation R> <R p q> <p ⊨SRBB hml_srbب.Internal χ>
  <Internal χ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
then obtain p' where p'_spec: <p → p'> <hml_srbب_inner_models p' χ> by auto
have <χ ∈ O_inner (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
  using case_assms(4) unfolding O_inner_def O_def by auto
hence <∃q'. q → q' ∧ hml_srbب_inner_models q' χ>
  using Internal case_assms(1,2) p'_spec silence_retains_eta_sim
  by (metis silent_reachable_trans)
thus <q ⊨SRBB hml_srbب.Internal χ> by auto
qed
next
case (ImmConj I Ψ)
then show ?case unfolding O_inner_def O_def by auto
next
case (Obs α φ)
then show ?case
proof (safe)
fix p q R
assume case_assms:
  <eta_simulation R> <R p q>
  <Obs α φ ∈ O_inner (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
  <hml_srbب_inner_models p (hml_srbب_inner.Obs α φ)>
hence <φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0)> unfolding O_inner_def O_def by auto
hence no_imm_conj: <¬I Ψ. φ = ImmConj I Ψ ∧ I ≠ {}> unfolding O_def by force
have back_step: <∀p0 p1. p1 ⊨SRBB φ → p0 → p1 → p0 ⊨SRBB φ>
proof (cases φ)
  case TT
  then show ?thesis by auto
next
  case (Internal _)
  then show ?thesis
    using silent_reachable_trans by auto
next
  case (ImmConj _ _)
  then show ?thesis using no_imm_conj by auto
qed
from case_assms obtain p' where <p ↦a α p'> <p' ⊨SRBB φ> by auto
then obtain q' q'' q''' where <q → q'> <q' ↦a α q''> <q'' → q'''> <R p' q'''>
  using <eta_simulation R> <R p q> unfolding eta_simulation_def
  using silent_reachable.refl by blast
hence <q''' ⊨SRBB φ> using <p' ⊨SRBB φ> Obs <φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
  using case_assms(1) by blast
hence <hml_srbب_inner_models q' (hml_srbب_inner.Obs α φ)>
  using <q' ↦a α q''> <q'' → q'''> back_step by auto
thus <∃q'. q → q' ∧ hml_srbب_inner_models q' (hml_srbب_inner.Obs α φ)>
  using <q → q'> by blast
qed
next
case (Conj I Ψ)
show ?case
proof safe
fix p q R
assume case_assms:
  <eta_simulation R> <R p q>
  <Conj I Ψ ∈ O_inner (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
  <hml_srbب_inner_models p (Conj I Ψ)>
hence conj_price: <∀i∈I. Ψ i ∈ O_conjunct (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
  unfolding O_conjunct_def O_inner_def
  by (simp, metis SUP_bot_conv(1) le_zero_eq sup_bot_left sup_ge1)

```

```

from case_assms have < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } p (\Psi i)$ > by auto
hence < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } q (\Psi i)$ >
  using Conj <eta_simulation R> <R p q> conj_price by blast
hence <hml_srbb_inner_models q (hml_srbb_inner.Conj I  $\Psi$ )> by simp
thus < $\exists q'. q \rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' (\text{hml\_srbb\_inner.Conj } I \Psi)$ >
  using silent_reachable.refl by blast
qed
next
case (StableConj I  $\Psi$ )
thus ?case unfolding  $\mathcal{O}$ _inner_def  $\mathcal{O}$ _def by auto
next
case (BranchConj  $\alpha \varphi I \Psi$ )
show ?case
proof safe
  fix p q R
  assume case_assms:
    <eta_simulation R> <R p q>
    <BranchConj  $\alpha \varphi I \Psi \in \mathcal{O}$ _inner ( $E \infty \infty \infty 0 0 \infty 0 0$ )>
    <hml_srbb_inner_models p (BranchConj  $\alpha \varphi I \Psi$ )>
  hence < $\varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0)$ > unfolding  $\mathcal{O}$ _inner_def  $\mathcal{O}$ _def
    by (simp, metis le_zero_eq sup_ge1)
  hence no_imm_conj: < $\nexists I \Psi. \varphi = \text{ImmConj } I \Psi \wedge I \neq \{\}$ > unfolding  $\mathcal{O}$ _def by force
  have back_step: < $\forall p0 p1. p1 \models \text{SRBB } \varphi \rightarrow p0 \rightarrow p1 \rightarrow p0 \models \text{SRBB } \varphi$ >
  proof (cases  $\varphi$ )
    case TT
    then show ?thesis by auto
  next
    case (Internal _)
    then show ?thesis
      using silent_reachable_trans by auto
  next
    case (ImmConj _ _)
    then show ?thesis using no_imm_conj by auto
  qed
  from case_assms have conj_price: < $\forall i \in I. \Psi i \in \mathcal{O}$ _conjunct ( $E \infty \infty \infty 0 0 \infty 0 0$ )>
    unfolding  $\mathcal{O}$ _conjunct_def  $\mathcal{O}$ _inner_def
    by (simp, metis SUP_bot_conv(1) bot_enat_def bot_eq_sup_iff)
  from case_assms have < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } p (\Psi i)$ >
    <hml_srbb_inner_models p (Obs  $\alpha \varphi$ )>
    using branching_conj_parts branching_conj_obs by blast+
  then obtain p' where < $p \mapsto_a \alpha p'$ > < $p' \models \text{SRBB } \varphi$ > by auto
  then obtain q' q'' q''' where q'_q''_spec:
    < $q \rightarrow q'$ > < $q' \mapsto_a \alpha q''$ > < $q'' \rightarrow q'''$ >
    <R p q'> <R p' q'''>
    using <eta_simulation R> <R p q> silent_reachable.refl
    unfolding eta_simulation_def by blast
  hence < $q''' \models \text{SRBB } \varphi$ >
    using BranchConj < $p' \models \text{SRBB } \varphi$ > < $\varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0)$ > case_assms by auto
  hence < $q'' \models \text{SRBB } \varphi$ > using back_step q'_q''_spec by blast
  hence <hml_srbb_inner_models q' (Obs  $\alpha \varphi$ )> using q'_q''_spec by auto
  moreover have < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } q' (\Psi i)$ >
    using BranchConj q'_q''_spec conj_price case_assms
    < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } p (\Psi i)$ >
    by blast
  ultimately show < $\exists q'. q \rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' (\text{BranchConj } \alpha \varphi I \Psi)$ >
    using < $q \rightarrow q'$ > by auto
  qed
next
case (Pos  $\chi$ )
show ?case
proof safe

```

```

fix p q R
assume case_assms:
  <eta_simulation R> <R p q>
  <Pos  $\chi \in \mathcal{O}_{\text{conjunct}} (E \infty \infty \infty 0 0 \infty 0 0)$ >
  <hml_srbb_conjunct_models p (Pos  $\chi$ )>
  hence < $\chi \in \mathcal{O}_{\text{inner}} (E \infty \infty \infty 0 0 \infty 0 0)$ >
    unfolding  $\mathcal{O}_{\text{inner\_def}}$   $\mathcal{O}_{\text{conjunct\_def}}$  by simp
  from case_assms obtain p' where <p  $\rightarrow$  p'> <hml_srbb_inner_models p'  $\chi$ > by auto
  then obtain q' where <q  $\rightarrow$  q'> <hml_srbb_inner_models q'  $\chi$ >
    using Pos case_assms < $\chi \in \mathcal{O}_{\text{inner}} (E \infty \infty \infty 0 0 \infty 0 0)$ > silence_retains_eta_sim
    by (smt (verit, ccfv_threshold) silent_reachable_trans)
  thus <hml_srbb_conjunct_models q (Pos  $\chi$ )> by auto
qed
next
case (Neg  $\chi$ )
show ?case
proof safe
  fix p q R
  assume case_assms:
    <eta_simulation R> <R p q>
    <Neg  $\chi \in \mathcal{O}_{\text{conjunct}} (E \infty \infty \infty 0 0 \infty 0 0)$ >
    <hml_srbb_conjunct_models p (Neg  $\chi$ )>
    hence False unfolding  $\mathcal{O}_{\text{conjunct\_def}}$  by auto
    thus <hml_srbb_conjunct_models q (Neg  $\chi$ )> by simp
  qed
qed
qed
thus ?thesis using assms by blast
qed

lemma modal_eta_sim: <eta_simulation (preordered ( $\mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0)$ ))>
proof -
  have < $\nexists p \alpha p'. (\text{preordered } (\mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0))) p q \wedge p \mapsto \alpha p' \wedge$   

    ( $\alpha \neq \tau \vee \neg(\text{preordered } (\mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0))) p' q) \wedge$   

    ( $\forall q'' q'''. q \rightarrow q' \rightarrow q' \mapsto \alpha q'' \rightarrow q'' \rightarrow q'''$   

 $\rightarrow \neg \text{preordered } (\mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0)) p q'$   

 $\vee \neg \text{preordered } (\mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0)) p' q'''$ >
  proof clarify
    have less_obs:
      <modal_depth ( $E \infty \infty \infty 0 0 \infty 0 0$ )  $\leq$  pos_conjuncts ( $E \infty \infty \infty 0 0 \infty 0 0$ )>
      by simp
    fix p  $\alpha$  p' q
    define Q $\alpha$  where
      <Q $\alpha \equiv \{q'. q \rightarrow q' \wedge (\nexists \varphi. \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0) \wedge \text{distinguishes } \varphi p q')\}$ >
    assume contradiction:
      <preordered ( $\mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0)$ ) p q> <p  $\mapsto \alpha p'$ >
      < $\forall q'' q'''. q \rightarrow q' \rightarrow q' \mapsto \alpha q'' \rightarrow q'' \rightarrow q'''$   

 $\rightarrow \neg \text{preordered } (\mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0)) p q'$   

 $\vee \neg \text{preordered } (\mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0)) p' q'''$ >
      < $\alpha \neq \tau \vee \neg \text{preordered } (\mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0)) p' q$ >
    hence distinctions: < $\forall q'. q \rightarrow q' \rightarrow$   

    ( $\exists \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0). \text{distinguishes } \varphi p q')$   $\vee$   

    ( $\forall q'' q'''. q' \mapsto \alpha q'' \rightarrow q'' \rightarrow q'''$   

 $\rightarrow (\exists \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0). \text{distinguishes } \varphi p' q''')$ >
    unfolding preordered_no_distinction
    by (metis silent_reachable.cases silent_reachable.refl)
  hence < $\forall q'' q'''. \forall q' \in Q\alpha.$   

    q'  $\mapsto \alpha q'' \rightarrow q'' \rightarrow q'''$   

 $\rightarrow (\exists \varphi \in \mathcal{O} (E \infty \infty \infty 0 0 \infty 0 0). \text{distinguishes } \varphi p' q''')$ >
    unfolding Q $\alpha$ _def using silent_reachable.refl by fastforce
  hence < $\forall q'' q'''. q'' \rightarrow q''' \rightarrow$ 

```

```

(∃ q'. q → q' ∧ (∄ φ. φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0) ∧ distinguishes φ p q')
  ∧ q' ↦ a α q'')
→ (∃ φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0). distinguishes φ p' q''')>
unfolding Qα_def by blast
hence <∀ q'''. (∃ q' q''. q → q' ∧
  (∄ φ. φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0) ∧ distinguishes φ p q') ∧ q' ↦ a α q''
  ∧ q'' → q''')
→ (∃ φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0). distinguishes φ p' q''')>
by blast
then obtain Φα where Φα_def:
  <∀ q'''. (∃ q' q''. q → q' ∧
    (∄ φ. φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0) ∧ distinguishes φ p q')
    ∧ q' ↦ a α q'' ∧ q'' → q''')
  → (Φα q''') ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0) ∧ distinguishes (Φα q''') p' q''')>
by metis
hence distinctions_α: <∀ q' ∈ Qα. ∀ q'' q'''.
  q' ↦ a α q'' → q'' → q''' → distinguishes (Φα q''') p' q''')>
unfolding Qα_def by blast
from distinctions obtain Φη where
  <∀ q'. q' ∈ {q'. q → q' ∧ (∃ φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0). distinguishes φ p q')}
  → distinguishes (Φη q') p q' ∧ (Φη q') ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
unfolding mem_Collect_eq by moura
then obtain Ψη where distinctions_η:
  <∀ q' ∈ {q'. q → q' ∧ (∃ φ ∈ O (E ∞ ∞ ∞ 0 0 ∞ 0 0). distinguishes φ p q')}.
  hml_srbconj.distinguishes (Ψη q') p q' ∧ (Ψη q')
  ∈ O_conjunct (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
using less_obs distinction_conjunctification distinction_conjunctification_price
by (smt (verit, del_insts))
have <p ↦ a α p'> using <p ↦ α p'> by auto
from distinction_combination_eta[OF this] distinctions_α have obs_dist:
  <∀ q' ∈ Qα. hml_srbconj_inner.distinguishes
    (Obs α (Internal (Conj {q'''. ∃ q' ∈ Qα. ∃ q''. q' ↦ a α q'' ∧ q'' → q'''}
      (conjunctify_distinctions Φα p')))) p q'>
unfolding Qα_def by blast
have <Qα ≠ {}>
using Qα_def contradiction(1) silent_reachable.refl by fastforce
hence conjunct_prices: <∀ q'''. ∃ q' ∈ Qα. ∃ q''. q' ↦ a α q'' ∧ q'' → q'''.
  (conjunctify_distinctions Φα p' q''') ∈ O_conjunct (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
using distinction_conjunctification_price[of
  <{q'''. ∃ q' ∈ Qα. ∃ q''. q' ↦ a α q'' ∧ q'' → q'''}>]
using Qα_def Φα_def by auto
have <(Conj {q'''. ∃ q' ∈ Qα. ∃ q''. q' ↦ a α q'' ∧ q'' → q'''}
  (conjunctify_distinctions Φα p')) ∈ O_inner (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
proof (cases <{q'''. ∃ q' ∈ Qα. ∃ q''. q' ↦ a α q'' ∧ q'' → q'''} = {}>)
case True
then show ?thesis
  unfolding O_inner_def O_conjunct_def
  by (auto simp add: True bot_enat_def)
next
case False
then show ?thesis
  using conjunct_prices
  unfolding O_inner_def O_conjunct_def by force
qed
hence obs_price: <(Obs α (Internal (Conj {q'''. ∃ q' ∈ Qα. ∃ q''. q' ↦ a α q'' ∧ q'' → q'''}
  (conjunctify_distinctions Φα p')))) ∈ O_inner (E ∞ ∞ ∞ 0 0 ∞ 0 0)>
using distinction_conjunctification_price distinctions_α
unfolding O_inner_def O_def by simp
from obs_dist distinctions_η have
  <hml_srbconj_inner_models p (BranchConj α
    (Internal (Conj {q'''. ∃ q' ∈ Qα. ∃ q''. q' ↦ a α q'' ∧ q'' → q'''}

```

```

      (conjunctify_distinctions  $\Phi\alpha$  p'))
    {q'. q  $\Rightarrow$  q'  $\wedge$  ( $\exists\varphi\in\mathcal{O}$  ( $E \infty \infty \infty 0 0 \infty 0 0$ ). distinguishes  $\varphi$  p q'))  $\Psi\eta$ >
  using contradiction(1) silent_reachable.refl
  unfolding Q $\alpha$ _def by force
  moreover have < $\forall q'. q \Rightarrow q' \longrightarrow \neg$  hml_srbb_inner_models q'
    (BranchConj  $\alpha$ 
      (Internal (Conj {q'''.  $\exists q'\in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \Rightarrow q'''$ }
        (conjunctify_distinctions  $\Phi\alpha$  p'))))
    {q'. q  $\Rightarrow$  q'  $\wedge$  ( $\exists\varphi\in\mathcal{O}$  ( $E \infty \infty \infty 0 0 \infty 0 0$ ). distinguishes  $\varphi$  p q'))  $\Psi\eta$ >
  proof safe
    fix q'
    assume contradiction: <q  $\Rightarrow$  q'>
    <hml_srbb_inner_models q' (BranchConj  $\alpha$ 
      (Internal (Conj {q'''.  $\exists q'\in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \Rightarrow q'''$ }
        (conjunctify_distinctions  $\Phi\alpha$  p'))))
      {q'. q  $\Rightarrow$  q'  $\wedge$  ( $\exists\varphi\in\mathcal{O}$  ( $E \infty \infty \infty 0 0 \infty 0 0$ ). distinguishes  $\varphi$  p q'))  $\Psi\eta$ >
    thus <False>
  using obs_dist distinctions_ $\eta$ 
  unfolding distinguishes_def hml_srbb_conj.distinguishes_def
    hml_srbb_inner.distinguishes_def Q $\alpha$ _def
  by (auto) blast+
qed
moreover have branch_price: <(BranchConj  $\alpha$ 
  (Internal (Conj {q'''.  $\exists q'\in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \Rightarrow q'''$ }
    (conjunctify_distinctions  $\Phi\alpha$  p'))))
  {q'. q  $\Rightarrow$  q'  $\wedge$  ( $\exists\varphi\in\mathcal{O}$  ( $E \infty \infty \infty 0 0 \infty 0 0$ ). distinguishes  $\varphi$  p q'))  $\Psi\eta$ 
 $\in \mathcal{O}_{\text{inner}}$  ( $E \infty \infty \infty 0 0 \infty 0 0$ )>
  using distinctions_ $\eta$  obs_price
  unfolding Q $\alpha$ _def  $\mathcal{O}_{\text{inner}}$ _def  $\mathcal{O}$ _def  $\mathcal{O}_{\text{conjunct}}$ _def  $\Phi\alpha$ _def
  by (simp, metis (mono_tags, lifting) SUP_bot_conv(2) bot_enat_def sup_bot_left)
ultimately have <distinguishes (Internal (BranchConj  $\alpha$ 
  (Internal (Conj {q'''.  $\exists q'\in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \Rightarrow q'''$ }
    (conjunctify_distinctions  $\Phi\alpha$  p'))))
  {q'. q  $\Rightarrow$  q'  $\wedge$  ( $\exists\varphi\in\mathcal{O}$  ( $E \infty \infty \infty 0 0 \infty 0 0$ ). distinguishes  $\varphi$  p q'))  $\Psi\eta$ )> p q>
  unfolding distinguishes_def Q $\alpha$ _def
  using silent_reachable.refl hml_srbb_models.simps(2) by blast
moreover have <(Internal (BranchConj  $\alpha$ 
  (Internal (Conj {q'''.  $\exists q'\in Q\alpha. \exists q''. q' \mapsto_a \alpha q'' \wedge q'' \Rightarrow q'''$ }
    (conjunctify_distinctions  $\Phi\alpha$  p'))))
  {q'. q  $\Rightarrow$  q'  $\wedge$  ( $\exists\varphi\in\mathcal{O}$  ( $E \infty \infty \infty 0 0 \infty 0 0$ ). distinguishes  $\varphi$  p q'))  $\Psi\eta$ )>
 $\in \mathcal{O}$  ( $E \infty \infty \infty 0 0 \infty 0 0$ )>
  using branch_price
  unfolding Q $\alpha$ _def  $\mathcal{O}$ _def  $\mathcal{O}_{\text{conjunct}}$ _def
  by (metis (no_types, lifting)  $\mathcal{O}_{\text{inner}}$ _def expr_internal_eq mem_Collect_eq)
ultimately show False using contradiction(1) preordered_no_distinction by blast
qed
thus ?thesis
  unfolding eta_simulation_def by blast
qed

theorem eta_sim_coordinate:
  <(p  $\preceq$  ( $E \infty \infty \infty 0 0 \infty 0 0$ ) q) = ( $\exists R. \text{eta\_simulation } R \wedge R$  p q)>
  using modal_eta_sim logic_eta_sim_invariant unfolding expr_preord_def
  by auto

end

end

```

6 Branching Bisimilarity

```
theory Branching_Bisimilarity
  imports Eta_Bisimilarity
begin
```

The whole of the modal logic of `hml_srb` precisely characterizes stability-respecting branching bisimilarity.

6.1 Definitions of (Stability-Respecting) Branching Bisimilarity

```
context lts_tau
begin

definition branching_simulation :: <'s  $\Rightarrow$  's  $\Rightarrow$  bool>  $\Rightarrow$  bool> where
  <branching_simulation R  $\equiv \forall p \alpha p' q. R p q \longrightarrow p \mapsto \alpha p' \longrightarrow$ 
     $((\alpha = \tau \wedge R p' q) \vee (\exists q' q''. q \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge R p q' \wedge R p' q''))$ >

lemma branching_simulation_intro:
  assumes
    < $\bigwedge p \alpha p' q. R p q \Longrightarrow p \mapsto \alpha p' \Longrightarrow$ 
       $((\alpha = \tau \wedge R p' q) \vee (\exists q' q''. q \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge R p q' \wedge R p' q''))$ >
  shows
    <branching_simulation R>
  using assms unfolding branching_simulation_def by simp

definition branching_simulated :: <'s  $\Rightarrow$  's  $\Rightarrow$  bool> where
  <branching_simulated p q  $\equiv \exists R. \text{branching\_simulation } R \wedge R p q$ >

definition branching_bisimulated :: <'s  $\Rightarrow$  's  $\Rightarrow$  bool> where
  <branching_bisimulated p q  $\equiv \exists R. \text{branching\_simulation } R \wedge \text{symp } R \wedge R p q$ >

definition sr_branching_bisimulated :: <'s  $\Rightarrow$  's  $\Rightarrow$  bool> (infix <~SRBB> 40) where
  <p ~SRBB q  $\equiv \exists R. \text{branching\_simulation } R \wedge \text{symp } R \wedge \text{stability\_respecting } R \wedge R p q$ >
```

6.2 Properties of Branching Bisimulation Equivalences

```
lemma branching_bisimilarity_branching_sim: <branching_simulation (~SRBB)>
  unfolding sr_branching_bisimulated_def branching_simulation_def by blast

lemma branching_sim_eta_sim:
  assumes <branching_simulation R>
  shows <eta_simulation R>
  using assms silent_reachable_refl
  unfolding branching_simulation_def eta_simulation_def by blast

lemma silence_retains_branching_sim:
  assumes
    <branching_simulation R>
    <R p q>
    <p  $\twoheadrightarrow$  p'>
  shows < $\exists q'. R p' q' \wedge q \twoheadrightarrow q'$ >
  using assms silence_retains_eta_sim branching_sim_eta_sim by blast

lemma branching_bisimilarity_stability: <stability_respecting (~SRBB)>
  unfolding sr_branching_bisimulated_def stability_respecting_def by blast

lemma sr_branching_bisimulation_silently_retained:
  assumes
    <p ~SRBB q>
    <p  $\twoheadrightarrow$  p'>
```

```

shows
  <math display="block">\exists q'. q \Rightarrow q' \wedge p' \sim \text{SRBB } q' > \text{ using } \text{assms}(2,1)
using branching_bisimilarity_branching_sim silence_retains_branching_sim by blast

lemma sr_branching_bisimulation_sim:
  assumes
    <math display="block">p \sim \text{SRBB } q >
    <math display="block">p \Rightarrow p' > \text{ } <math display="block">p' \mapsto_a \alpha p' >
  shows
    <math display="block">\exists q' q''. q \Rightarrow q' \wedge q' \mapsto_a \alpha q'' \wedge p' \sim \text{SRBB } q' \wedge p'' \sim \text{SRBB } q'' >
proof -
  obtain q' where <math display="block">q \Rightarrow q' > <sr\_branching\_bisimulated\ p'\ q' >
    using assms sr_branching_bisimulation_silently_retained by blast
  thus ?thesis
    using assms(3) branching_bisimilarity_branching_sim silent_reachable_trans
    unfolding branching_simulation_def
    by blast
qed

lemma sr_branching_bisimulated_sym:
  assumes
    <math display="block">p \sim \text{SRBB } q >
  shows
    <math display="block">q \sim \text{SRBB } p >
  using assms unfolding sr_branching_bisimulated_def by (meson sympD)

lemma sr_branching_bisimulated_symp:
  shows <math display="block">\text{symp } (\sim \text{SRBB}) >
  using sr_branching_bisimulated_sym
  using sympI by blast

lemma sr_branching_bisimulated_refl:
  shows <math display="block">\text{refl } (\sim \text{SRBB}) >
  unfolding sr_branching_bisimulated_def stability_respecting_def reflp_def
  using silence_retains_branching_sim silent_reachable.refl
  by (smt (verit) DEADID.rel_symp branching_simulation_intro)

lemma establish_sr_branching_bisim:
  assumes
    <math display="block">\forall \alpha p'. p \mapsto \alpha p' \Rightarrow
    ((\alpha = \tau \wedge p' \sim \text{SRBB } q) \vee (\exists q' q''. q \Rightarrow q' \wedge q' \mapsto \alpha q'' \wedge p \sim \text{SRBB } q' \wedge p' \sim \text{SRBB } q'')) >
    <math display="block">\forall \alpha q'. q \mapsto \alpha q' \Rightarrow
    ((\alpha = \tau \wedge p \sim \text{SRBB } q') \vee (\exists p' p''. p \Rightarrow p' \wedge p' \mapsto \alpha p'' \wedge p \sim \text{SRBB } q \wedge p'' \sim \text{SRBB } q')) >
    <math display="block">\text{stable\_state } p \Rightarrow (\exists q'. q \Rightarrow q' \wedge p \sim \text{SRBB } q' \wedge \text{stable\_state } q') >
    <math display="block">\text{stable\_state } q \Rightarrow (\exists p'. p \Rightarrow p' \wedge p' \sim \text{SRBB } q \wedge \text{stable\_state } p') >
  shows <math display="block">p \sim \text{SRBB } q >
proof -
  define R where <math display="block">R \equiv \lambda pp qq. pp \sim \text{SRBB } qq \vee (pp = p \wedge qq = q) \vee (pp = q \wedge qq = p) >
  hence
    R_cases: <math display="block">\bigwedge pp qq. R\ pp\ qq \Rightarrow pp \sim \text{SRBB } qq \vee (pp = p \wedge qq = q) \vee (pp = q \wedge qq = p) > \text{ and }
    bisim\_extension: <math display="block">\bigwedge pp qq. pp \sim \text{SRBB } qq \Rightarrow R\ pp\ qq > \text{ by } \text{blast+}
  have <math display="block">\text{symp } R >
    unfolding symp_def R_def sr_branching_bisimulated_def
    by blast
  moreover have <math display="block">\text{stability\_respecting } R >
    unfolding stability_respecting_def
  proof safe
    fix pp qq
    assume <math display="block">R\ pp\ qq > <\text{stable\_state } pp >
    then consider <math display="block">pp \sim \text{SRBB } qq > \mid <math display="block">pp = p \wedge qq = q > \mid <math display="block">pp = q \wedge qq = p >
      using R_cases by blast

```

```

thus < $\exists q'. qq \Rightarrow q' \wedge R \text{ pp } q' \wedge \text{stable\_state } q'$ >
proof cases
  case 1
  then show ?thesis
    using branching_bisimilarity_stability <stable\_state pp> bisim_extension
    unfolding stability_respecting_def
    by blast
  next
  case 2
  then show ?thesis
    using assms(3) <stable\_state pp> unfolding R_def by blast
  next
  case 3
  then show ?thesis
    using assms(4) <stable\_state pp> <symp R> unfolding R_def
    by (meson sr_branching_bisimulated_sym)
qed
moreover have <branching_simulation R> unfolding branching_simulation_def
proof clarify
  fix pp  $\alpha$  p' qq
  assume bc:
    <R pp qq> <pp  $\mapsto$   $\alpha$  p'>
    < $\nexists q' q''. qq \Rightarrow q' \wedge q' \mapsto \alpha q'' \wedge R \text{ pp } q' \wedge R \text{ p' } q''$ >
  then consider <pp ~SRBB qq> | <pp = p  $\wedge$  qq = q> | <pp = q  $\wedge$  qq = p>
  using R_cases by blast
  thus < $\alpha = \tau \wedge R \text{ p' } qq$ >
  proof cases
    case 1
    then show ?thesis
      by (smt (verit, del_insts) bc bisim_extension
        branching_bisimilarity_branching_sim branching_simulation_def)
    next
    case 2
    then show ?thesis
      using bc assms(1) bisim_extension by blast
    next
    case 3
    then show ?thesis
      using bc assms(2) bisim_extension sr_branching_bisimulated_sym by metis
  qed
  qed
  moreover have <R p q> unfolding R_def by blast
  ultimately show ?thesis
    unfolding sr_branching_bisimulated_def by blast
  qed

lemma sr_branching_bisimulation_stuttering:
  assumes
    <pp  $\neq$  []>
    < $\forall i < \text{length pp} - 1. \text{pp}!i \mapsto \tau \text{ pp}!(\text{Suc } i)$ >
    <hd pp ~SRBB last pp>
    <i < length pp>
  shows
    <hd pp ~SRBB pp!i>
proof -
  have chain_reachable: < $\forall j < \text{length pp}. \forall i \leq j. \text{pp}!i \Rightarrow \text{pp}!j$ >
    using tau_chain_reachability assms(2) .
  hence chain_hd_last:
    < $\forall i < \text{length pp}. \text{hd pp} \Rightarrow \text{pp}!i$ >
    < $\forall i < \text{length pp}. \text{pp}!i \Rightarrow \text{last pp}$ >

```

```

by (auto simp add: assms(1) hd_conv_nth last_conv_nth)
define R where
  <R  $\equiv$   $\lambda p q. (p = \text{hd } pp \wedge (\exists i < \text{length } pp. pp!i = q)) \vee ((q = \text{hd } pp \wedge (\exists i < \text{length } pp. pp!i = p))) \vee p \sim \text{SRBB } q$ >
have later_hd_sim: < $\bigwedge i p' \alpha. i < \text{length } pp \implies pp!i \mapsto \alpha p'$ 
 $\implies (\text{hd } pp) \twoheadrightarrow (pp!i) \wedge (pp!i) \mapsto \alpha p' \wedge R (pp!i) (pp!i) \wedge R p' p'$ >
  using chain_hd_last sr_branching_bisimulated_refl
  unfolding R_def
  by (simp add: reflp_def)
have hd_later_sim: < $\bigwedge i p' \alpha. i < \text{length } pp - 1 \implies (\text{hd } pp) \mapsto \alpha p'$ 
 $\implies (\exists q' q''. (pp!i) \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge R (\text{hd } pp) q' \wedge R p' q'')$ >
proof -
  fix i p'  $\alpha$ 
  assume case_assm: < $i < \text{length } pp - 1 \implies (\text{hd } pp) \mapsto \alpha p'$ >
  hence < $(\alpha = \tau \wedge p' \sim \text{SRBB } (\text{last } pp)) \vee (\exists q' q''. (\text{last } pp) \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge (\text{hd } pp) \sim \text{SRBB } q' \wedge p' \sim \text{SRBB } q'')$ >
    using assms branching_bisimilarity_branching_sim branching_simulation_def
    by auto
  thus < $(\exists q' q''. (pp!i) \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge R (\text{hd } pp) q' \wedge R p' q'')$ >
proof
  assume tau_null_step: < $\alpha = \tau \wedge p' \sim \text{SRBB } \text{last } pp$ >
  have < $pp ! i \twoheadrightarrow (pp!(\text{length } pp - 2))$ >
    using case_assm(1) chain_reachable by force
  moreover have < $pp!(\text{length } pp - 2) \mapsto \alpha (\text{last } pp)$ >
    using assms(1,2) case_assm(1) last_conv_nth tau_null_step
    by (metis Nat.lessE Suc_1 Suc_diff_Suc less_Suc_eq zero_less_Suc zero_less_diff)
  moreover have < $R (\text{hd } pp) (pp!(\text{length } pp - 2)) \wedge R p' (\text{last } pp)$ >
    unfolding R_def
    by (metis assms(1) diff_less length_greater_0_conv less_2_cases_iff tau_null_step)
  ultimately show < $\exists q' q''. pp ! i \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge R (\text{hd } pp) q' \wedge R p' q''$ >
    by blast
next
  assume < $\exists q' q''. \text{last } pp \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge \text{hd } pp \sim \text{SRBB } q' \wedge p' \sim \text{SRBB } q''$ >
  hence < $\exists q' q''. \text{last } pp \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge R (\text{hd } pp) q' \wedge R p' q''$ >
    unfolding R_def by blast
  moreover have < $i < \text{length } pp$ > using case_assm by auto
  ultimately show < $\exists q' q''. pp ! i \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge R (\text{hd } pp) q' \wedge R p' q''$ >
    using chain_hd_last silent_reachable_trans by blast
qed
qed
have <branching_simulation R>
proof (rule branching_simulation_intro)
  fix p  $\alpha p' q$ 
  assume challenge: < $R p q \implies p \mapsto \alpha p'$ >
  from this(1) consider
    < $(p = \text{hd } pp \wedge (\exists i < \text{length } pp. pp!i = q))$ > |
    < $(q = \text{hd } pp \wedge (\exists i < \text{length } pp. pp!i = p))$ > |
    < $p \sim \text{SRBB } q$ > unfolding R_def by blast
  thus < $\alpha = \tau \wedge R p' q \vee (\exists q' q''. q \twoheadrightarrow q' \wedge q' \mapsto \alpha q'' \wedge R p q' \wedge R p' q'')$ >
proof cases
  case 1
  then obtain i where i_spec: < $i < \text{length } pp \implies pp ! i = q$ > by blast
  from 1 have < $p = \text{hd } pp$ > ..
  show ?thesis
proof (cases < $i = \text{length } pp - 1$ >)
  case True
  then have < $q = \text{last } pp$ > using i_spec assms(1)
    by (simp add: last_conv_nth)
  then show ?thesis using challenge(2) assms(3) branching_bisimilarity_branching_sim
    unfolding R_def branching_simulation_def < $p = \text{hd } pp$ >
    by metis

```

```

    next
    case False
    hence <i < length pp - 1> using i_spec by auto
    then show ?thesis using <p = hd pp> i_spec hd_later_sim challenge(2) by blast
  qed
next
case 2
then show ?thesis
  using later_hd_sim challenge(2) by blast
next
case 3
then show ?thesis
  using challenge(2) branching_bisimilarity_branching_sim
  unfolding branching_simulation_def R_def by metis
qed
qed
moreover have <symp R>
  using sr_branching_bisimulated_sym
  unfolding R_def sr_branching_bisimulated_def
  by (smt (verit, best) sympI)
moreover have <stability_respecting R>
  using assms(3) stable_state_stable sr_branching_bisimulated_sym
  branching_bisimilarity_stability
  unfolding R_def stability_respecting_def
  by (metis chain_hd_last)
moreover have < $\bigwedge i. i < \text{length } pp \implies R \text{ (hd } pp) (pp[i])$ > unfolding R_def by auto
ultimately show ?thesis
  using assms(4) sr_branching_bisimulated_def by blast
qed

lemma sr_branching_bisimulation_stabilizes:
  assumes
    <sr_branching_bisimulated p q>
    <stable_state p>
  shows
    < $\exists q'. q \twoheadrightarrow q' \wedge \text{sr\_branching\_bisimulated } p \ q' \wedge \text{stable\_state } q'$ >
proof -
  from assms obtain R where
    R_spec: <branching_simulation R> <symp R> <stability_respecting R> <R p q>
  unfolding sr_branching_bisimulated_def by blast
  then obtain q' where <q  $\twoheadrightarrow$  q'> <stable_state q'>
  using assms(2) unfolding stability_respecting_def by blast
  moreover have <sr_branching_bisimulated p q'>
  using sr_branching_bisimulation_stuttering
  assms(1) calculation(1) sr_branching_bisimulated_def sympD
  by (metis assms(2) sr_branching_bisimulation_silently_retained stable_state_stable)
  ultimately show ?thesis by blast
qed

lemma sr_branching_bisim_stronger:
  assumes
    <sr_branching_bisimulated p q>
  shows
    <branching_bisimulated p q>
  using assms unfolding sr_branching_bisimulated_def branching_bisimulated_def by auto

```

6.3 hml_srbb as Modal Characterization of Stability-Respecting Branching Bisimilarity

```

lemma modal_sym: <symp (preordered UNIV)>
proof -

```

```

have <# p q. preordered UNIV p q ∧ ¬preordered UNIV q p>
proof safe
  fix p q
  assume contradiction:
    <preordered UNIV p q>
    <¬preordered UNIV q p>
  then obtain  $\varphi$  where  $\varphi$ _distinguishes: <distinguishes  $\varphi$  q p> by auto
  thus False
proof (cases  $\varphi$ )
  case TT
  then show ?thesis using  $\varphi$ _distinguishes by auto
next
  case (Internal  $\chi$ )
  hence <distinguishes (ImmConj {undefined} ( $\lambda i$ . Neg  $\chi$ )) p q>
    using  $\varphi$ _distinguishes by simp
  then show ?thesis using contradiction preordered_no_distinction by blast
next
  case (ImmConj I  $\Psi$ )
  then obtain i where i_def: <i ∈ I> <hml_srbb_conj.distinguishes ( $\Psi$  i) q p>
    using  $\varphi$ _distinguishes srbb_dist_imm_conjunction_implies_dist_conjunct by auto
  then show ?thesis
proof (cases < $\Psi$  i>)
  case (Pos  $\chi$ )
  hence <distinguishes (ImmConj {undefined} ( $\lambda i$ . Neg  $\chi$ )) p q> using i_def by simp
  thus ?thesis using contradiction preordered_no_distinction by blast
next
  case (Neg  $\chi$ )
  hence <distinguishes (Internal  $\chi$ ) p q> using i_def by simp
  thus ?thesis using contradiction preordered_no_distinction by blast
qed
qed
qed
thus ?thesis unfolding symp_def by blast
qed

lemma modal_branching_sim: <branching_simulation (preordered UNIV)>
proof -
  have <# p  $\alpha$  p' q. (preordered UNIV) p q ∧ p  $\mapsto$   $\alpha$  p' ∧
    ( $\alpha \neq \tau \vee \neg(\text{preordered UNIV})$  p' q) ∧
    ( $\forall q' q''$ . q  $\Rightarrow$  q'  $\longrightarrow$  q'  $\mapsto$   $\alpha$  q'')
     $\longrightarrow$   $\neg$  preordered UNIV p q'  $\vee$   $\neg$  preordered UNIV p' q''>
  proof clarify
    fix p  $\alpha$  p' q
    define Q $\alpha$  where Q $\alpha$   $\equiv$  {q'. q  $\Rightarrow$  q' ∧ ( $\nexists \varphi$ . distinguishes  $\varphi$  p q')}>
    assume contradiction:
      <preordered UNIV p q> <p  $\mapsto$   $\alpha$  p'>
      < $\forall q' q''$ . q  $\Rightarrow$  q'  $\longrightarrow$  q'  $\mapsto$   $\alpha$  q''>
       $\longrightarrow$   $\neg$  preordered UNIV p q'  $\vee$   $\neg$  preordered UNIV p' q''>
      < $\alpha \neq \tau \vee \neg$  preordered UNIV p' q>
    hence distinctions: < $\forall q'$ . q  $\Rightarrow$  q'  $\longrightarrow$ 
      ( $\exists \varphi$ . distinguishes  $\varphi$  p q')  $\vee$ 
      ( $\forall q''$ . q'  $\mapsto$   $\alpha$  q''  $\longrightarrow$  ( $\exists \varphi$ . distinguishes  $\varphi$  p' q''))>
    using preordered_no_distinction
    by (metis equivpI equivp_def lts_semantics.preordered_preord modal_sym)
    hence < $\forall q''$ .  $\forall q' \in Q\alpha$ .
      q'  $\mapsto$   $\alpha$  q''  $\longrightarrow$  ( $\exists \varphi$ . distinguishes  $\varphi$  p' q'')>
    unfolding Q $\alpha$ _def by auto
    hence < $\forall q''$ . ( $\exists q'$ . q  $\Rightarrow$  q' ∧ ( $\nexists \varphi$ . distinguishes  $\varphi$  p q') ∧ q'  $\mapsto$   $\alpha$  q'')
       $\longrightarrow$  ( $\exists \varphi$ . distinguishes  $\varphi$  p' q'')>
    unfolding Q $\alpha$ _def by blast
    then obtain  $\Phi\alpha$  where

```

```

    <∀q''. (∃q'. q → q' ∧ (∄φ. distinguishes φ p q')) ∧ q' ↦a α q''>
      → distinguishes (Φα q'') p' q''> by metis
  hence distinctions_α: <∀q'∈Qα. ∀q''.
    q' ↦a α q'' → distinguishes (Φα q'') p' q''>
    unfolding Qα_def by blast
  from distinctions obtain Φη where
    <∀q'. q'∈{q'. q → q' ∧ (∃φ. distinguishes φ p q')}>
      → distinguishes (Φη q') p q'> unfolding mem_Collect_eq by moura
  with distinction_conjunctification obtain Ψη where distinctions_η:
    <∀q'∈{q'. q → q' ∧ (∃φ. distinguishes φ p q')}>.
      hml_srbb_conj.distinguishes (Ψη q') p q'>
    by blast
  have <p ↦a α p'> using <p ↦ α p'> by auto
  from distinction_combination[OF this] distinctions_α have obs_dist:
    <∀q'∈Qα.
      hml_srbb_inner.distinguishes (Obs α (ImmConj {q''. ∃q'''∈Qα. q''' ↦a α q''}
        (conjunctify_distinctions Φα p')))) p q'>

    unfolding Qα_def by blast
  with distinctions_η have
    <hml_srbb_inner_models p (BranchConj α
      (ImmConj {q''. ∃q'''∈Qα. q''' ↦a α q''}
        (conjunctify_distinctions Φα p'))
      {q'. q → q' ∧ (∃φ. distinguishes φ p q')}) Ψη)>
    using contradiction(1) silent_reachable.refl
    unfolding Qα_def distinguishes_def hml_srbb_conj.distinguishes_def
      hml_srbb_inner.distinguishes_def preordered_def
    by simp force
  moreover have <∀q'. q → q' → ¬ hml_srbb_inner_models q'
    (BranchConj α (ImmConj {q''. ∃q'''∈Qα. q''' ↦a α q''}
      (conjunctify_distinctions Φα p')) {q'. q → q' ∧ (∃φ. distinguishes φ p q')}) Ψη)>
  proof safe
    fix q'
    assume contradiction: <q → q'>
    <hml_srbb_inner_models q' (BranchConj α (ImmConj {q''. ∃q'''∈Qα. q''' ↦a α q''}
      (conjunctify_distinctions Φα p')) {q'. q → q' ∧ (∃φ. distinguishes φ p q')}) Ψη)>
    thus <False>
      using obs_dist distinctions_η
      unfolding distinguishes_def hml_srbb_conj.distinguishes_def
        hml_srbb_inner.distinguishes_def Qα_def
      by (auto) blast+
  qed
  ultimately have <distinguishes (Internal (BranchConj α
    (ImmConj {q''. ∃q'''∈Qα. q''' ↦a α q''} (conjunctify_distinctions Φα p'))
    {q'. q → q' ∧ (∃φ. distinguishes φ p q')}) Ψη)) p q>
    unfolding distinguishes_def Qα_def
    using silent_reachable.refl by (auto) blast+
  thus False using contradiction(1) preordered_no_distinction by blast
qed
thus ?thesis
  unfolding branching_simulation_def by blast
qed

lemma logic_sr_branching_bisim_invariant:
  assumes
    <sr_branching_bisimulated p0 q0>
    <p0 ⊨SRBB φ>
  shows <q0 ⊨SRBB φ>
proof -
  have <∧φ χ ψ.
    (∀p q. sr_branching_bisimulated p q → p ⊨SRBB φ → q ⊨SRBB φ) ∧
    (∀p q. sr_branching_bisimulated p q → hml_srbb_inner_models p χ

```

```

    → (∃ q'. q → q' ∧ hml_srbb_inner_models q' χ)) ∧
  (∀ p q. sr_branching_bisimulated p q → hml_srbb_conjunct_models p ψ
    → hml_srbb_conjunct_models q ψ) >
proof -
  fix φ χ ψ
  show
    <(∀ p q. sr_branching_bisimulated p q → p ⊨SRBB φ → q ⊨SRBB φ) ∧
    (∀ p q. sr_branching_bisimulated p q → hml_srbb_inner_models p χ
      → (∃ q'. q → q' ∧ hml_srbb_inner_models q' χ)) ∧
    (∀ p q. sr_branching_bisimulated p q → hml_srbb_conjunct_models p ψ
      → hml_srbb_conjunct_models q ψ)>
proof (induct rule: hml_srbb_hml_srbb_inner_hml_srbb_conjunct.induct)
  case TT
  then show ?case by simp
next
  case (Internal χ)
  show ?case
  proof safe
    fix p q
    assume <sr_branching_bisimulated p q> <p ⊨SRBB hml_srbb.Internal χ>
    then obtain p' where <p → p'> <hml_srbb_inner_models p' χ> by auto
    hence <∃ q'. q → q' ∧ hml_srbb_inner_models q' χ>
      using Internal <hml_srbb_inner_models p' χ>
      by (meson lts_tau.silent_reachable_trans <p ~SRBB q>
        sr_branching_bisimulation_silently_retained)
    thus <q ⊨SRBB hml_srbb.Internal χ> by auto
  qed
next
  case (ImmConj I Ψ)
  then show ?case by auto
next
  case (Obs α φ)
  then show ?case
  proof (safe)
    fix p q
    assume
      <sr_branching_bisimulated p q>
      <hml_srbb_inner_models p (hml_srbb_inner.Obs α φ)>
    then obtain p' where <p ↦a α p'> <p' ⊨SRBB φ> by auto
    then obtain q' q'' where <q → q'> <q' ↦a α q''> <sr_branching_bisimulated p' q''>
      using sr_branching_bisimulation_sim[OF <sr_branching_bisimulated p q>]
      silent_reachable.refl
    by blast
    hence <q' ⊨SRBB φ> using <p' ⊨SRBB φ> Obs by blast
    hence <hml_srbb_inner_models q' (hml_srbb_inner.Obs α φ)>
      using <q' ↦a α q''> by auto
    thus <∃ q'. q → q' ∧ hml_srbb_inner_models q' (hml_srbb_inner.Obs α φ)>
      using <q → q'> by blast
  qed
next
  case (Conj I Ψ)
  show ?case
  proof safe
    fix p q
    assume
      <sr_branching_bisimulated p q>
      <hml_srbb_inner_models p (hml_srbb_inner.Conj I Ψ)>
    hence <∀ i ∈ I. hml_srbb_conjunct_models p (Ψ i)> by auto
    hence <∀ i ∈ I. hml_srbb_conjunct_models q (Ψ i)>
      using Conj <sr_branching_bisimulated p q> by blast
    hence <hml_srbb_inner_models q (hml_srbb_inner.Conj I Ψ)> by simp
  qed

```

```

    thus < $\exists q'. q \rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \text{ (hml\_srbb\_inner.Conj I } \Psi)\text{>}$ 
      using silent_reachable.refl by blast
qed
next
case (StableConj I  $\Psi$ ) show ?case
proof safe
  fix p q
  assume
    <sr_branching_bisimulated p q>
    <hml_srbb_inner_models p (StableConj I  $\Psi$ )>
  hence < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } p \text{ (} \Psi \text{ } i\text{)>}$ 
    using stable_conj_parts by blast
  from <hml_srbb_inner_models p (StableConj I  $\Psi$ )> have <stable_state p> by auto
  then obtain q' where <math>q \rightarrow q'> <stable_state q'> <sr_branching_bisimulated p q'>
    using <sr_branching_bisimulated p q> sr_branching_bisimulation_stabilizes by blast
  hence < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } q' \text{ (} \Psi \text{ } i\text{)>}$ 
    using < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } p \text{ (} \Psi \text{ } i\text{)>}$  StableConj by blast
  hence <hml_srbb_inner_models q' (StableConj I  $\Psi$ )> using <stable_state q'> by simp
  thus < $\exists q'. q \rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \text{ (StableConj I } \Psi)\text{>}$ 
    using <math>q \rightarrow q'> by blast
qed
next
case (BranchConj  $\alpha \varphi$  I  $\Psi$ )
show ?case
proof safe
  fix p q
  assume
    <sr_branching_bisimulated p q>
    <hml_srbb_inner_models p (BranchConj  $\alpha \varphi$  I  $\Psi$ )>
  hence < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } p \text{ (} \Psi \text{ } i\text{)>}$ 
    <hml_srbb_inner_models p (Obs  $\alpha \varphi$ )>
    using branching_conj_parts branching_conj_obs by blast+
  then obtain p' where <math>p \mapsto_a \alpha p'> <math>p' \models_{\text{SRBB}} \varphi> by auto
  then obtain q' q'' where q'_q''_spec:
    <math>q \rightarrow q'> <math>q' \mapsto_a \alpha q''>
    <sr_branching_bisimulated p q'> <sr_branching_bisimulated p' q''>
    using sr_branching_bisimulation_sim[OF <sr_branching_bisimulated p q>]
      silent_reachable.refl[of p]
    by blast
  hence <math>q'' \models_{\text{SRBB}} \varphi> using BranchConj.hyps <math>p' \models_{\text{SRBB}} \varphi> by auto
  hence <hml_srbb_inner_models q' (Obs  $\alpha \varphi$ )> using q'_q''_spec by auto
  moreover have < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } q' \text{ (} \Psi \text{ } i\text{)>}$ 
    using BranchConj.hyps < $\forall i \in I. \text{hml\_srbb\_conjunct\_models } p \text{ (} \Psi \text{ } i\text{)>}$  q'_q''_spec by blast
  ultimately show < $\exists q'. q \rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \text{ (BranchConj } \alpha \varphi \text{ I } \Psi)\text{>}$ 
    using <math>q \rightarrow q'> by auto
qed
next
case (Pos  $\chi$ )
show ?case
proof safe
  fix p q
  assume
    <sr_branching_bisimulated p q>
    <hml_srbb_conjunct_models p (Pos  $\chi$ )>
  then obtain p' where <math>p \rightarrow p'> <hml_srbb_inner_models p'  $\chi$ > by auto
  then obtain q' where <math>q \rightarrow q'> <hml_srbb_inner_models q'  $\chi$ >
    using Pos <math>p \sim_{\text{SRBB}} q> sr_branching_bisimulation_silently_retained
    by (meson silent_reachable_trans)
  thus <hml_srbb_conjunct_models q (Pos  $\chi$ )> by auto
qed
next

```

```

case (Neg  $\chi$ )
show ?case
proof safe
  fix p q
  assume
    <sr_branching_bisimulated p q>
    <hml_srbb_conjunct_models p (Neg  $\chi$ )>
  hence < $\forall p'. p \rightarrow p' \rightarrow \neg \text{hml\_srbb\_inner\_models } p' \chi$ > by simp
  moreover have
    <( $\exists q'. q \rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \chi$ )
       $\rightarrow (\exists p'. p \rightarrow p' \wedge \text{hml\_srbb\_inner\_models } p' \chi)$ >
  using Neg sr_branching_bisimulated_sym[OF <sr_branching_bisimulated p q>]
    sr_branching_bisimulation_silently_retained
  by (meson silent_reachable_trans)
  ultimately have < $\forall q'. q \rightarrow q' \rightarrow \neg \text{hml\_srbb\_inner\_models } q' \chi$ > by blast
  thus <hml_srbb_conjunct_models q (Neg  $\chi$ )> by simp
qed
qed
qed
thus ?thesis using assms by blast
qed

lemma sr_branching_bisim_is_hmlsrbb: <sr_branching_bisimulated p q = preordered UNIV p q>
  using modal_stability_respecting_modal_sym modal_branching_sim
    logic_sr_branching_bisim_invariant  $\mathcal{O}_{\text{sup}}$  preordered_def
  unfolding sr_branching_bisimulated_def by metis

lemma sr_branching_bisimulated_transitive:
  assumes
    <p ~SRBB q>
    <q ~SRBB r>
  shows
    <p ~SRBB r>
  using assms unfolding sr_branching_bisim_is_hmlsrbb by simp

lemma sr_branching_bisimulated_equivalence: <equivp (~SRBB)>
proof (rule equivpI)
  show <symp (~SRBB)> using sr_branching_bisimulated_symp .
  show <reflp (~SRBB)> using sr_branching_bisimulated_refl .
  show <transp (~SRBB)>
    unfolding transp_def using sr_branching_bisimulated_transitive by blast
qed

lemma sr_branching_bisimulation_stuttering_all:
  assumes
    <pp  $\neq []$ >
    < $\forall i < \text{length pp} - 1. \text{pp}!i \mapsto \tau \text{pp}!(\text{Suc } i)$ >
    <hd pp ~SRBB last pp>
    <i  $\leq j$  < j < length pp>
  shows
    <pp!i ~SRBB pp!j>
  using assms equivp_def sr_branching_bisimulated_equivalence equivp_def order_le_less_trans
    sr_branching_bisimulation_stuttering
  by metis

theorem sr_branching_bisim_coordinate: <(p ~SRBB q) = (p  $\preceq$  (E  $\infty \infty \infty \infty \infty \infty \infty \infty$ ) q)>
  using sr_branching_bisim_is_hmlsrbb  $\mathcal{O}_{\text{sup}}$ 
  unfolding expr_preord_def by auto

end

```

end

7 Energy Games

```
theory Energy_Games
  imports Main
begin
```

Energy games are the foundation for the weak spectroscopy game. We introduce them through a recursive definition of attacker's winning budgets in energy reachability games.

7.1 Fundamentals

```
type_synonym 'energy update = <'energy  $\Rightarrow$  'energy option>
```

An energy game is played by two players on a directed graph labeled by energy updates. These updates represent the costs of choosing a certain move, in our case, for the attacker.

```
locale energy_game =
fixes
  weight_opt :: <'gstate  $\Rightarrow$  'gstate  $\Rightarrow$  'energy update option> and
  defender :: <'gstate  $\Rightarrow$  bool> and
  ord :: <'energy  $\Rightarrow$  'energy  $\Rightarrow$  bool>
assumes
  antisim: < $\bigwedge e e'.$  (ord e e')  $\implies$  (ord e' e)  $\implies$  e = e'> and
  monotonicity: < $\bigwedge g g' e e' eu eu'.$ 
    weight_opt g g'  $\neq$  None  $\implies$  the (weight_opt g g') e = Some eu
     $\implies$  the (weight_opt g g') e' = Some eu'  $\implies$  ord e e'  $\implies$  ord eu eu'> and
  defender_win_min: < $\bigwedge g g' e e'.$  ord e e'  $\implies$  weight_opt g g'  $\neq$  None
     $\implies$  the (weight_opt g g') e' = None  $\implies$  the (weight_opt g g') e = None>
begin

abbreviation attacker :: <'gstate  $\Rightarrow$  bool> where
  <attacker p  $\equiv \neg$  defender p>

abbreviation moves :: <'gstate  $\Rightarrow$  'gstate  $\Rightarrow$  bool> (infix < $\mapsto$ > 70) where
  <g1  $\mapsto$  g2  $\equiv$  weight_opt g1 g2  $\neq$  None>

abbreviation weighted_move
  :: <'gstate  $\Rightarrow$  'energy update  $\Rightarrow$  'gstate  $\Rightarrow$  bool> (<_  $\mapsto$  wgt _ _> [60,60,60] 70) where
  <weighted_move g1 u g2  $\equiv$  g1  $\mapsto$  g2  $\wedge$  (the (weight_opt g1 g2) = u)>

abbreviation <weight g1 g2  $\equiv$  the (weight_opt g1 g2)>

abbreviation <updated g g' e  $\equiv$  the (weight g g' e)>
```

7.2 Winning Budgets

The attacker wins a game if and only if they manage to force the defender to get stuck before running out of energy.

```
inductive attacker_wins :: <'energy  $\Rightarrow$  'gstate  $\Rightarrow$  bool> where
  Attack: <attacker_wins e g> if
    <attacker g> <g  $\mapsto$  g'> <weight g g' e = Some e'> <attacker_wins e' g'> |
  Defense: <attacker_wins e g> if
    <defender g> < $\forall g'.$  (g  $\mapsto$  g')  $\longrightarrow$  ( $\exists e'.$  weight g g' e = Some e'  $\wedge$  attacker_wins e' g')>

lemma attacker_wins_Ga_with_id_step:
  assumes <attacker_wins e g'> <g  $\mapsto$  wgt Some g'> <attacker g>
  shows <attacker_wins e g>
  using assms by (metis attacker_wins.simps)
```

If from a certain starting position g a game is won by the attacker with some energy e (i.e. e is in the winning budget of g), then the game is also won by the attacker with more energy.

```

lemma win_a_upwards_closure:
  assumes
    <attacker_wins e g>
    <ord e e'>
  shows
    <attacker_wins e' g>
using assms proof (induct arbitrary: e' rule: attacker_wins.induct)
  case (Attack g g' e eu e')
  with defender_win_min obtain eu' where <weight g g' e' = Some eu'> by fastforce
  then show ?case
    using Attack monotonicity attacker_wins.simps by blast
next
  case (Defense g e)
  with defender_win_min have < $\forall g'. g \succ g' \longrightarrow (\exists eu'. \text{weight } g g' e' = \text{Some } eu')$ > by fastforce
  then show ?case
    using Defense attacker_wins.Defense monotonicity by meson
qed

end — context energy_game

end

```

8 Weak Spectroscopy Game

```
theory Spectroscopy_Game
  imports Energy_Games Energy Labeled_Transition_Systems
begin
```

The weak spectroscopy game is an energy game played over an LTS. The attacker's moves in the weak spectroscopy game depend on the transitions of the processes and the available energy. Intuitively, each move type corresponds to a production in the construction of distinguishing formulas; and each attacker position to a non-terminal in the underlying grammar.

8.1 Game Rules

```
datatype ('s, 'a) spectroscopy_position =
  Attacker_Immediate (attacker_state: <'s>) (defender_states: <'s set>) |
  Attacker_Delayed (attacker_state: <'s>) (defender_states: <'s set>) |
  Attacker_Conjunct (attacker_state: <'s>) (defender_state: <'s>) |
  Attacker_Branch (attacker_state: <'s>) (defender_states: <'s set>) |

  Defender_Conj (attacker_state: <'s>) (defender_states: <'s set>) |
  Defender_Stable_Conj (attacker_state: <'s>) (defender_states: <'s set>) |
  Defender_Branch (attacker_state: <'s>) (attack_action: <'a>)
    (attacker_state_succ: <'s>) (defender_states: <'s set>)
    (defender_branch_states: <'s set>)

context lts_tau
begin
```

The names of moves of the weak spectroscopy game indicate the respective HML constructs they correspond to.

```
fun spectroscopy_moves :: <('s, 'a) spectroscopy_position  $\Rightarrow$  ('s, 'a) spectroscopy_position
 $\Rightarrow$  energy update option>
where
  delay:
    <spectroscopy_moves (Attacker_Immediate p Q) (Attacker_Delayed p' Q')
      = (if p' = p  $\wedge$  Q  $\rightarrow$ S Q' then id_up else None)> |

  procrastination:
    <spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Delayed p' Q')
      = (if (Q' = Q  $\wedge$  p  $\neq$  p'  $\wedge$  p  $\mapsto$   $\tau$  p') then id_up else None)> |

  observation:
    <spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Immediate p' Q')
      = (if ( $\exists$ a. p  $\mapsto$ a a p'  $\wedge$  Q  $\mapsto$ aS a Q') then (subtract 1 0 0 0 0 0 0 0)
        else None)> |

  f_or_early_conj:
    <spectroscopy_moves (Attacker_Immediate p Q) (Defender_Conj p' Q')
      = (if (Q  $\neq$  {}  $\wedge$  Q = Q'  $\wedge$  p = p') then (subtract 0 0 0 0 1 0 0 0)
        else None)> |

  late_inst_conj:
    <spectroscopy_moves (Attacker_Delayed p Q) (Defender_Conj p' Q')
      = (if p = p'  $\wedge$  Q = Q' then id_up else None)> |

  conj_answer:
    <spectroscopy_moves (Defender_Conj p Q) (Attacker_Conjunct p' q)
      = (if p = p'  $\wedge$  q  $\in$  Q then (subtract 0 0 1 0 0 0 0 0) else None)> |

  pos_neg_clause:
```

```

    <spectroscopy_moves (Attacker_Conjunct p q) (Attacker_Delayed p' Q')
      = (if (p = p') then
          (if {q} →S Q' then Some min1_6 else None)
        else (if {p} →S Q' ∧ q=p'
              then Some (λe. Option.bind (subtract_fn 0 0 0 0 0 0 1 e) min1_7)
              else None))> |

late_stbl_conj:
  <spectroscopy_moves (Attacker_Delayed p Q) (Defender_Stable_Conj p' Q')
    = (if (p = p' ∧ Q' = { q ∈ Q. (∄q'. q ↦τ q') } ∧ (∄p''. p ↦τ p''))
        then id_up else None)> |

conj_s_answer:
  <spectroscopy_moves (Defender_Stable_Conj p Q) (Attacker_Conjunct p' q)
    = (if p = p' ∧ q ∈ Q then (subtract 0 0 0 1 0 0 0 0)
        else None)> |

empty_stbl_conj_answer:
  <spectroscopy_moves (Defender_Stable_Conj p Q) (Defender_Conj p' Q')
    = (if Q = {} ∧ Q = Q' ∧ p = p' then (subtract 0 0 0 1 0 0 0 0)
        else None)> |

br_conj:
  <spectroscopy_moves (Attacker_Delayed p Q) (Defender_Branch p' α p'' Q' Qα)
    = (if (p = p' ∧ Q' = Q - Qα ∧ p ↦a α p'' ∧ Qα ⊆ Q) then id_up
        else None)> |

br_answer:
  <spectroscopy_moves (Defender_Branch p α p' Q Qα) (Attacker_Conjunct p'' q)
    = (if (p = p'' ∧ q ∈ Q) then (subtract 0 1 1 0 0 0 0 0) else None)> |

br_obsv:
  <spectroscopy_moves (Defender_Branch p α p' Q Qα) (Attacker_Branch p'' Q')
    = (if (p' = p'' ∧ Qα ↦aS α Q')
        then Some (λe. Option.bind ((subtract_fn 0 1 1 0 0 0 0 0) e) min1_6) else None)> |

br_acct:
  <spectroscopy_moves (Attacker_Branch p Q) (Attacker_Immediate p' Q')
    = (if p = p' ∧ Q = Q' then subtract 1 0 0 0 0 0 0 0 else None)> |

others: <spectroscopy_moves _ _ = None>

fun spectroscopy_defender where
  <spectroscopy_defender (Attacker_Immediate _ _) = False> |
  <spectroscopy_defender (Attacker_Branch _ _) = False> |
  <spectroscopy_defender (Attacker_Conjunct _ _) = False> |
  <spectroscopy_defender (Attacker_Delayed _ _) = False> |
  <spectroscopy_defender (Defender_Branch _ _ _ _) = True> |
  <spectroscopy_defender (Defender_Conj _ _) = True> |
  <spectroscopy_defender (Defender_Stable_Conj _ _) = True>

```

8.2 Energy Game Properties

Now, we are able to define the weak spectroscopy game on an arbitrary LTS.

```

sublocale weak_spectroscopy_game:
  energy_game <spectroscopy_moves> <spectroscopy_defender> <(≤)>
proof
  fix e e' :: energy
  show <e ≤ e' ⇒ e' ≤ e ⇒ e = e'> unfolding less_eq_energy_def
    by (smt (z3) energy.case_eq_if energy.expand nle_le)

```

```

next
  fix g g' e e' eu eu'
  assume monotonicity_assms:
    <spectroscopy_moves g g' ≠ None>
    <the (spectroscopy_moves g g') e = Some eu>
    <the (spectroscopy_moves g g') e' = Some eu'>
    <e ≤ e'>
  show <eu ≤ eu'>
  proof (cases g)
    case (Attacker_Immediate p Q)
    with monotonicity_assms
    show ?thesis
      by (cases g', simp_all, (smt (z3) option.distinct(1) option.sel minus_component_leq)+)
  next
    case (Attacker_Branch p Q)
    with monotonicity_assms
    show ?thesis
      by (cases g', simp_all, (smt (z3) option.distinct(1) option.sel minus_component_leq)+)
  next
    case (Attacker_Conjunct p q)
  hence <∃p' Q'. g' = (Attacker_Delayed p' Q')>
    using monotonicity_assms(1,2)
    by (induct, auto)
  hence <spectroscopy_moves g g' = Some min1_6
    ∨ spectroscopy_moves g g'
      = Some (λe. Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7)>
    using monotonicity_assms(1,2) Attacker_Conjunct
    by (smt (verit, ccfv_threshold) spectroscopy_moves.simps(7))
  thus ?thesis
  proof safe
    assume <spectroscopy_moves g g' = Some min1_6>
    thus ?thesis
      using monotonicity_assms min.mono
      unfolding leq_components
      by (metis min_1_6_simps option.sel)
  next
    assume <spectroscopy_moves g g'
      = Some (λe. Option.bind (if ¬ E 0 0 0 0 0 0 0 1 ≤ e
        then None else Some (e - E 0 0 0 0 0 0 0 1)) min1_7)>
    thus ?thesis
      unfolding min_1_7_subtr_simp
      using monotonicity_assms
      by (smt (z3) enat_diff_mono energy.sel leq_components min.mono
        option.distinct(1) option.sel)
  qed
next
  case (Attacker_Delayed p Q)
  hence <(∃p' Q'. g' = Attacker_Delayed p' Q') ∨
    (∃p' Q'. g' = Attacker_Immediate p' Q') ∨
    (∃p' Q'. g' = Defender_Conj p' Q') ∨
    (∃p' Q'. g' = Defender_Stable_Conj p' Q') ∨
    (∃p' p'' Q' α Qα . g' = Defender_Branch p' α p'' Q' Qα)>
    using monotonicity_assms(1)
    by (induct, auto)
  thus ?thesis
  proof (safe)
    fix p' Q'
    assume <g' = Attacker_Delayed p' Q'>
    thus <eu ≤ eu'>
      using Attacker_Delayed monotonicity_assms local.procrastination
      by (metis option.sel)
  
```

```

next
  fix p' Q'
  assume <g' = Attacker_Immediate p' Q'>
  hence <spectroscopy_moves g g' = (subtract 1 0 0 0 0 0 0 0)>
    using Attacker_Delayed monotonicity_assms local.observation
    by (clarify, presburger)
  thus <eu ≤ eu'>
    by (smt (verit, best) mono_subtract monotonicity_assms option.distinct(1) option.sel)
next
  fix p' Q'
  assume <g' = Defender_Conj p' Q'>
  thus <eu ≤ eu'>
    using Attacker_Delayed monotonicity_assms local.late_inst_conj
    by (metis option.sel)
next
  fix p' Q'
  assume <g' = Defender_Stable_Conj p' Q'>
  thus <eu ≤ eu'>
    using Attacker_Delayed monotonicity_assms local.late_stbl_conj
    by (metis (no_types, lifting) option.sel)
next
  fix p' p'' Q' α Qα
  assume <g' = Defender_Branch p' α p'' Q' Qα>
  thus <eu ≤ eu'>
    using Attacker_Delayed monotonicity_assms local.br_conj
    by (metis (no_types, lifting) option.sel)
qed
next
  case (Defender_Branch p a p' Q' Qa)
  with monotonicity_assms show ?thesis
    by (cases g', auto simp del: leq_components, unfold min_1_6_subtr_simp)
      (smt (z3) enat_diff_mono mono_subtract option.discI energy.sel
        leq_components min.mono option.distinct(1) option.inject)+
next
  case (Defender_Conj p Q)
  with monotonicity_assms show ?thesis
    by (cases g', simp_all del: leq_components)
      (smt (verit, ccfv_SIG) mono_subtract option.discI option.sel)
next
  case (Defender_Stable_Conj x71 x72)
  with monotonicity_assms show ?thesis
    by (cases g', simp_all del: leq_components)
      (smt (verit, ccfv_SIG) mono_subtract option.discI option.sel)+
qed
next
  fix g g' e e'
  assume defender_win_min_assms:
    <e ≤ e'>
    <spectroscopy_moves g g' ≠ None>
    <the (spectroscopy_moves g g') e' = None>
  thus
    <the (spectroscopy_moves g g') e = None>
  proof (cases g)
    case (Attacker_Immediate p Q)
    with defender_win_min_assms show ?thesis
      by (cases g', auto simp del: leq_components)
        (smt (verit, best) option.distinct(1) option.inject order.trans)+
  next
    case (Attacker_Branch p Q)
    with defender_win_min_assms show ?thesis
      by (cases g', auto)

```

```

      (smt (verit, best) option.distinct(1) option.inject order.trans)+
next
  case (Attacker_Conjunct p q)
  hence < $\exists p' Q'. g' = (\text{Attacker\_Delayed } p' Q')$ >
    using defender_win_min_assms(2) by (induct, auto)
  hence <spectroscopy_moves g g' = Some min1_6
     $\vee$  spectroscopy_moves g g' = Some ( $\lambda e. \text{Option.bind } ((\text{subtract\_fn } 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1) \ e) \ \text{min1\_7}$ )>
    using defender_win_min_assms(2) Attacker_Conjunct
    by (smt (verit, ccfv_threshold) spectroscopy_moves.simps(7))
  thus ?thesis
proof safe
  assume <spectroscopy_moves g g' = Some min1_6>
  thus <the (spectroscopy_moves g g') e = None>
    using defender_win_min_assms min_1_6_some by fastforce
next
  assume <spectroscopy_moves g g'
    = Some ( $\lambda e. \text{Option.bind } (\text{if } \neg E \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \leq e$ 
      then None else Some ( $e - E \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1$ )) min1_7)>
  thus <the (spectroscopy_moves g g') e = None>
    using defender_win_min_assms(1,3) bind.bind_lunit dual_order.trans min_1_7_some
    by (smt (verit, best) option.sel)
qed
next
  case (Attacker_Delayed p Q)
  hence <( $\exists p' Q'. g' = (\text{Attacker\_Delayed } p' Q')$ )  $\vee$ 
    ( $\exists p' Q'. g' = (\text{Attacker\_Immediate } p' Q')$ )  $\vee$ 
    ( $\exists p' Q'. g' = (\text{Defender\_Conj } p' Q')$ )  $\vee$ 
    ( $\exists p' Q'. g' = (\text{Defender\_Stable\_Conj } p' Q')$ )  $\vee$ 
    ( $\exists p' p'' Q' \alpha Q\alpha. g' = (\text{Defender\_Branch } p' \alpha p'' Q' Q\alpha)$ )>
    using defender_win_min_assms(2) by (induct, auto)
  thus ?thesis
proof (safe)
  fix p' Q'
  assume <g' = Attacker_Delayed p' Q'>
  hence False
    using Attacker_Delayed defender_win_min_assms(2,3) local.procrastination
    by (metis option.distinct(1) option.sel)
  thus <the (spectroscopy_moves g (Attacker_Delayed p' Q')) e = None> ..
next
  fix p' Q'
  assume <g' = Attacker_Immediate p' Q'>
  moreover hence <spectroscopy_moves g g' = (subtract 1 0 0 0 0 0 0 0)>
    using Attacker_Delayed defender_win_min_assms(2,3) local.observation
    by (clarify, presburger)
  moreover hence < $\neg E \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \leq e'$ >
    using defender_win_min_assms by force
  ultimately show <the (spectroscopy_moves g (Attacker_Immediate p' Q')) e = None>
    using defender_win_min_assms(1) by force
next
  fix p' Q'
  assume <g' = Defender_Conj p' Q'>
  hence False
    using Attacker_Delayed defender_win_min_assms(2,3) local.late_inst_conj
    by (metis option.distinct(1) option.sel)
  thus <the (spectroscopy_moves g (Defender_Conj p' Q')) e = None> ..
next
  fix p' Q'
  assume <g' = Defender_Stable_Conj p' Q'>
  hence False
    using Attacker_Delayed defender_win_min_assms(2,3) local.late_stbl_conj
    by (metis (no_types, lifting) option.distinct(1) option.sel)

```

```

    thus <the (spectroscopy_moves g (Defender_Stable_Conj p' Q')) e = None> ..
next
  fix p' p'' Q'  $\alpha$  Q $\alpha$ 
  assume <g' = Defender_Branch p'  $\alpha$  p'' Q' Q $\alpha$ >
  hence False
    using Attacker_Delayed defender_win_min_assms(2,3) local.br_conj
    by (metis (no_types, lifting) option.distinct(1) option.sel)
  thus <the (spectroscopy_moves g (Defender_Branch p'  $\alpha$  p'' Q' Q $\alpha$ )) e = None> ..
qed
next
  case (Defender_Branch p a p' Q' Qa)
  hence <( $\exists q' \in Q'$ . g' = Attacker_Conjunct p q')
     $\vee$  ( $\exists Qa'$ . Qa  $\mapsto$  aS a Qa'  $\wedge$  g' = Attacker_Branch p' Qa')>
    using defender_win_min_assms by (cases g', auto) (metis not_None_eq)+
  hence <(spectroscopy_moves g g') = (subtract 0 1 1 0 0 0 0 0)  $\vee$ 
    (spectroscopy_moves g g') = Some ( $\lambda e$ . Option.bind (subtract_fn 0 1 1 0 0 0 0 0 e) min1_6)>
    using Defender_Branch option.collapse[OF defender_win_min_assms(2)]
    by (cases g', auto)
  thus ?thesis
    using defender_win_min_assms min_1_6_some
    by (smt (verit, best) bind.bind_lunit option.distinct(1) dual_order.trans option.sel)
next
  case (Defender_Conj p Q)
  with defender_win_min_assms show ?thesis
    by (cases g', auto)
    (smt (verit, best) option.distinct(1) option.inject order.trans)+
next
  case (Defender_Stable_Conj x71 x72)
  with defender_win_min_assms show ?thesis
    by (cases g', simp_all del: leq_components)
    (smt (verit) dual_order.trans option.discI option.sel)+
qed
qed

abbreviation <spectro_att_wins  $\equiv$  weak_spectroscopy_game.attacker_wins>

end — of lts_tau

end

```

9 Correctness

Energy levels where the defender wins in the spectroscopy game and equivalences coincide in the following sense: There exists a formula φ distinguishing a process p from a set of processes Q with expressiveness price of at most e if and only if e is in attacker's winning budget of `Attacker_Immediate` p Q .

The proof is split into two directions, closely following the structure of [3]. The forward direction is given by the lemma `distinction_implies_winning_budgets` combined with the upwards closure of winning budgets. To show the other direction, one can construct a (strategy) formula with an appropriate price using the constructive proof of `winning_budget_implies_strategy_formula`.

9.1 Distinction Implies Winning Budgets

```
theory Distinction_Implies_Winning_Budgets
  imports Spectroscopy_Game Expressiveness_Price
begin
```

```
context lts_tau
begin
```

We prove that if a formula distinguishes process p from a set of process Q , then the price of this formula is in attacker's winning budgets.

```
lemma distinction_implies_winning_budgets_empty_Q:
  assumes
    <distinguishes_from  $\varphi$  p {}>
  shows
    <spectro_att_wins (expressiveness_price  $\varphi$ ) (Attacker_Immediate p {})>
  using assms
proof -
  have <spectroscopy_moves (Defender_Conj p {}) p' = None> for p'
    by(rule spectroscopy_moves.elims, auto)
  moreover have <spectroscopy_defender (Defender_Conj p {})> by simp
  ultimately have conj_win: <spectro_att_wins (expressiveness_price  $\varphi$ ) (Defender_Conj p {})>
    by (simp add: weak_spectroscopy_game.attacker_wins.Defense)
  from late_inst_conj[of p <{}> p <{}>] have next_move0:
    <spectroscopy_moves (Attacker_Delayed p {}) (Defender_Conj p {}) = id_up> by force
  from delay[of p <{}> p <{}>] have next_move1:
    <spectroscopy_moves (Attacker_Immediate p {}) (Attacker_Delayed p {}) = id_up> by force
  moreover have <weak_spectroscopy_game.attacker (Attacker_Immediate p {})> by simp
  ultimately show ?thesis
    using weak_spectroscopy_game.attacker_wins.Attack next_move0 next_move1
    by (metis conj_win option.distinct(1) option.sel spectroscopy_defender.simps(4))
qed
```

```
lemma distinction_implies_winning_budgets:
  assumes
    <distinguishes_from  $\varphi$  p Q>
  shows
    <spectro_att_wins (expressiveness_price  $\varphi$ ) (Attacker_Immediate p Q)>
proof -
  have
    < ( $\forall p$  p. Q  $\neq$  {}  $\longrightarrow$  distinguishes_from  $\varphi$  p Q
       $\longrightarrow$  spectro_att_wins (expressiveness_price  $\varphi$ ) (Attacker_Immediate p Q))
     $\wedge$ 
    (( $\forall p$  Q. Q  $\neq$  {}  $\longrightarrow$  hml_srb_inner.distinguishes_from  $\chi$  p Q  $\longrightarrow$  Q  $\twoheadrightarrow$  S Q
       $\longrightarrow$  spectro_att_wins (expr_pr_inner  $\chi$ ) (Attacker_Delayed p Q))
     $\wedge$  ( $\forall \Psi_I \Psi$  p Q.  $\chi$  = Conj  $\Psi_I \Psi \longrightarrow$ 
      Q  $\neq$  {}  $\longrightarrow$  hml_srb_inner.distinguishes_from  $\chi$  p Q
       $\longrightarrow$  spectro_att_wins (expr_pr_inner  $\chi$ ) (Defender_Conj p Q))
```

```

 $\wedge (\forall \Psi\_I \Psi p Q. \chi = \text{StableConj } \Psi\_I \Psi \longrightarrow$ 
   $Q \neq \{\} \longrightarrow \text{hml\_srbb\_inner.distinguishes\_from } \chi p Q \longrightarrow (\forall q \in Q. \nexists q'. q \mapsto \tau q')$ 
   $\longrightarrow \text{spectro\_att\_wins } (\text{expr\_pr\_inner } \chi) (\text{Defender\_Stable\_Conj } p Q))$ 
 $\wedge (\forall \Psi\_I \Psi \alpha \varphi p Q p' Q\_a. \chi = \text{BranchConj } \alpha \varphi \Psi\_I \Psi \longrightarrow$ 
   $\text{hml\_srbb\_inner.distinguishes\_from } \chi p Q \longrightarrow p \mapsto a \alpha p' \longrightarrow p' \models \text{SRBB } \varphi \longrightarrow$ 
   $Q\_a = Q - \text{hml\_srbb\_inner.model\_set } (\text{Obs } \alpha \varphi)$ 
   $\longrightarrow \text{spectro\_att\_wins } (\text{expr\_pr\_inner } \chi) (\text{Defender\_Branch } p \alpha p' (Q - Q\_a) Q\_a)))$ 
 $\wedge$ 
   $(\forall p q. \text{hml\_srbb\_conj.distinguishes } \psi p q$ 
     $\longrightarrow \text{spectro\_att\_wins } (\text{expr\_pr\_conjunct } \psi) (\text{Attacker\_Conjunct } p q)) >$ 
  for  $\varphi \chi \psi$ 
proof -
  fix  $\varphi \chi \psi$ 
  show  $\langle (\forall Q p. Q \neq \{\} \longrightarrow \text{distinguishes\_from } \varphi p Q$ 
     $\longrightarrow \text{spectro\_att\_wins } (\text{expressiveness\_price } \varphi) (\text{Attacker\_Immediate } p Q)) >$ 
     $\wedge$ 
     $((\forall p Q. Q \neq \{\} \longrightarrow \text{hml\_srbb\_inner.distinguishes\_from } \chi p Q \longrightarrow Q \twoheadrightarrow S Q$ 
       $\longrightarrow \text{spectro\_att\_wins } (\text{expr\_pr\_inner } \chi) (\text{Attacker\_Delayed } p Q))$ 
     $\wedge (\forall \Psi\_I \Psi p Q. \chi = \text{Conj } \Psi\_I \Psi \longrightarrow$ 
       $Q \neq \{\} \longrightarrow \text{hml\_srbb\_inner.distinguishes\_from } \chi p Q$ 
       $\longrightarrow \text{spectro\_att\_wins } (\text{expr\_pr\_inner } \chi) (\text{Defender\_Conj } p Q))$ 
     $\wedge (\forall \Psi\_I \Psi p Q. \chi = \text{StableConj } \Psi\_I \Psi \longrightarrow$ 
       $Q \neq \{\} \longrightarrow \text{hml\_srbb\_inner.distinguishes\_from } \chi p Q \longrightarrow (\forall q \in Q. \nexists q'. q \mapsto \tau q')$ 
       $\longrightarrow \text{spectro\_att\_wins } (\text{expr\_pr\_inner } \chi) (\text{Defender\_Stable\_Conj } p Q))$ 
     $\wedge (\forall \Psi\_I \Psi \alpha \varphi p Q p' Q\_a. \chi = \text{BranchConj } \alpha \varphi \Psi\_I \Psi \longrightarrow$ 
       $\text{hml\_srbb\_inner.distinguishes\_from } \chi p Q \longrightarrow p \mapsto a \alpha p' \longrightarrow p' \models \text{SRBB } \varphi \longrightarrow$ 
       $Q\_a = Q - \text{hml\_srbb\_inner.model\_set } (\text{Obs } \alpha \varphi)$ 
       $\longrightarrow \text{spectro\_att\_wins } (\text{expr\_pr\_inner } \chi) (\text{Defender\_Branch } p \alpha p' (Q - Q\_a) Q\_a)))$ 
     $\wedge$ 
     $(\forall p q. \text{hml\_srbb\_conj.distinguishes } \psi p q$ 
       $\longrightarrow \text{spectro\_att\_wins } (\text{expr\_pr\_conjunct } \psi) (\text{Attacker\_Conjunct } p q)) >$ 
  proof (induct rule: hml_srbb_hml_srbb_inner_hml_srbb_conjunct.induct[of _ _ _  $\varphi \chi \psi$ ])
  case TT
  then show ?case
  proof (clarify)
    fix  $Q p$ 
    assume  $\langle Q \neq \{\} \rangle \langle \text{distinguishes\_from TT } p Q \rangle$ 
    hence  $\langle \exists q. q \in Q \rangle$ 
    by blast
    then obtain  $q$  where  $\langle q \in Q \rangle$  by auto
    hence  $\langle \text{distinguishes TT } p q \rangle$ 
    using  $\langle \text{distinguishes\_from TT } p Q \rangle$  distinguishes_from_def by auto
    with verum_never_distinguishes
    show  $\langle \text{spectro\_att\_wins } (\text{expressiveness\_price TT}) (\text{Attacker\_Immediate } p Q) \rangle$ 
    by blast
  qed
next
case (Internal  $\chi$ )
  show ?case
  proof (clarify)
    fix  $Q p$ 
    assume  $\langle Q \neq \{\} \rangle \langle \text{distinguishes\_from (Internal } \chi) p Q \rangle$ 
    then have
       $\langle \exists p'. p \twoheadrightarrow p' \wedge \text{hml\_srbb\_inner\_models } p' \chi \rangle$ 
       $\langle \forall q \in Q. (\nexists q'. q \twoheadrightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \chi) \rangle$ 
    by auto
    hence  $\langle \forall q \in Q. (\forall q'. q \twoheadrightarrow q' \longrightarrow \neg(\text{hml\_srbb\_inner\_models } q' \chi)) \rangle$  by auto
    then have  $\langle \forall q \in Q. (\forall q' \in Q'. q \twoheadrightarrow q' \longrightarrow \neg(\text{hml\_srbb\_inner\_models } q' \chi)) \rangle$ 
    for  $Q'$  by blast
    then have  $\langle Q \twoheadrightarrow S Q' \longrightarrow (\forall q' \in Q'. \neg(\text{hml\_srbb\_inner\_models } q' \chi)) \rangle$ 
    for  $Q'$  using  $\langle Q \neq \{\} \rangle$  by blast
  
```

```

define Q $\tau$  where <Q $\tau$   $\equiv$  silent_reachable_set Q>
with < $\bigwedge Q'. Q \rightarrow S Q' \rightarrow (\forall q' \in Q'. \neg(\text{hml\_srbb\_inner\_models } q' \ \chi))$ >
have < $\forall q' \in Q\tau. \neg(\text{hml\_srbb\_inner\_models } q' \ \chi)$ >
  using sreachable_set_is_sreachable by presburger
have <Q $\tau$   $\rightarrow S$  Q $\tau$ > unfolding Q $\tau$ _def
  by (metis silent_reachable_trans sreachable_set_is_sreachable
    silent_reachable.intros(1))
from < $\exists p'. p \rightarrow p' \wedge (\text{hml\_srbb\_inner\_models } p' \ \chi)$ >
obtain p' where <p  $\rightarrow$  p'> <hml_srbb_inner_models p'  $\chi$ > by auto
from this(1) have <p  $\rightarrow L$  p'> using silent_reachable_impl_loopless by blast
have <Q $\tau$   $\neq$  {}>
  using silent_reachable.intros(1) sreachable_set_is_sreachable Q $\tau$ _def <Q  $\neq$  {}>
  by fastforce
from <hml_srbb_inner_models p'  $\chi$ > < $\forall q' \in Q\tau. \neg(\text{hml\_srbb\_inner\_models } q' \ \chi)$ >
  have <hml_srbb_inner.distinguishes_from  $\chi$  p' Q $\tau$ > by simp
with <Q $\tau$   $\rightarrow S$  Q $\tau$ > <Q $\tau$   $\neq$  {}> Internal
have <spectro_att_wins (expr_pr_inner  $\chi$ ) (Attacker_Delayed p' Q $\tau$ )>
  by blast
moreover have <expr_pr_inner  $\chi$  = expressiveness_price (Internal  $\chi$ )> by simp
ultimately have <spectro_att_wins (expressiveness_price (Internal  $\chi$ ))
  (Attacker_Delayed p' Q $\tau$ )> by simp
hence <spectro_att_wins (expressiveness_price (Internal  $\chi$ )) (Attacker_Delayed p Q $\tau$ )>
proof(induct rule: silent_reachable_loopless.induct[of <p> <p'>, OF <p  $\rightarrow L$  p'>])
  case (1 p)
  thus ?case by simp
next
  case (2 p p' p'')
  hence <spectro_att_wins (expressiveness_price (Internal  $\chi$ ))
    (Attacker_Delayed p' Q $\tau$ )>
    by simp
  moreover have <spectroscopy_moves (Attacker_Delayed p Q $\tau$ ) (Attacker_Delayed p' Q $\tau$ )
    = id_up> using spectroscopy_moves.simps(2) <p  $\neq$  p'> <p  $\mapsto \tau$  p'> by auto
  moreover have <weak_spectroscopy_game.attacker (Attacker_Delayed p Q $\tau$ )> by simp
  ultimately show ?case
    using weak_spectroscopy_game.attacker_wins_Ga_with_id_step by auto
qed
have <Q  $\rightarrow S$  Q $\tau$ >
  using Q $\tau$ _def sreachable_set_is_sreachable by simp
hence <spectroscopy_moves (Attacker_Immediate p Q) (Attacker_Delayed p Q $\tau$ ) = id_up>
  using spectroscopy_moves.simps(1) by simp
with <spectro_att_wins (expressiveness_price (Internal  $\chi$ )) (Attacker_Delayed p Q $\tau$ )>
show <spectro_att_wins (expressiveness_price (Internal  $\chi$ )) (Attacker_Immediate p Q)>
  using weak_spectroscopy_game.attacker_wins_Ga_with_id_step
  by (metis option.discI option.sel spectroscopy_defender.simps(1))
qed
next
case (ImmConj I  $\psi$ s)
show ?case
proof (clarify)
  fix Q p
  assume <Q  $\neq$  {}> and <distinguishes_from (ImmConj I  $\psi$ s) p Q>
  from this(2) have < $\forall q \in Q. p \models \text{SRBB ImmConj I } \psi \text{ s} \wedge \neg q \models \text{SRBB ImmConj I } \psi \text{ s}$ >
    unfolding distinguishes_from_def distinguishes_def by blast
  hence < $\forall q \in Q. \exists i \in I. \text{hml\_srbb\_conjunct\_models } p (\psi \text{ s } i) \wedge \neg \text{hml\_srbb\_conjunct\_models } q (\psi \text{ s } i)$ >
    by simp
  hence < $\forall q \in Q. \exists i \in I. \text{hml\_srbb\_conj.distinguishes } (\psi \text{ s } i) p q$ >
    using hml_srbb_conj.distinguishes_def by simp
  hence < $\forall q \in Q. \exists i \in I. ((\psi \text{ s } i) \in \text{range } \psi \text{ s}) \wedge \text{hml\_srbb\_conj.distinguishes } (\psi \text{ s } i) p q$ > by blast
  hence < $\forall q \in Q. \exists i \in I.$ 

```

```

    spectro_att_wins (expr_pr_conjunct ( $\psi$  s i)) (Attacker_Conjunct p q) >
using ImmConj by blast
hence a_clause_wina:
  < $\forall q \in Q. \exists i \in I.$ 
    spectro_att_wins (expressiveness_price (ImmConj I  $\psi$ s) - E 0 0 1 0 1 0 0 0)
    (Attacker_Conjunct p q)>
using expressiveness_price_ImmConj_geq_parts
  weak_spectroscopy_game.win_a_upwards_closure by fast
from this <Q  $\neq \{\}$ > have <I  $\neq \{\}$ > by blast
hence subtracts:
  <subtract_fn 0 0 1 0 1 0 0 0 (expressiveness_price (ImmConj I  $\psi$ s))
    = Some (expressiveness_price (ImmConj I  $\psi$ s) - E 0 0 1 0 1 0 0 0)>
  <subtract_fn 0 0 1 0 0 0 0 0 (expressiveness_price (ImmConj I  $\psi$ s)
    - E 0 0 0 0 1 0 0 0)
    = Some (expressiveness_price (ImmConj I  $\psi$ s) - E 0 0 1 0 1 0 0 0)>
  by (simp add: <I  $\neq \{\}$ >)+
have def_conj: <spectroscopy_defender (Defender_Conj p Q)> by simp
have <spectroscopy_moves (Defender_Conj p Q) N  $\neq$  None
   $\implies$  N = Attacker_Conjunct (attacker_state N) (defender_state N)> for N
  by (metis spectroscopy_moves.simps(29,30,33,34,58,62)
    spectroscopy_position.exhaust_sel)
hence move_kind: <spectroscopy_moves (Defender_Conj p Q) N  $\neq$  None
   $\implies \exists q \in Q. N = \text{Attacker\_Conjunct } p \ q>$  for N
using conj_answer by metis
hence update: < $\bigwedge g'. \text{spectroscopy\_moves } (\text{Defender\_Conj } p \ Q) \ g' \neq \text{None} \implies$ 
  weak_spectroscopy_game.weight (Defender_Conj p Q) g' = subtract_fn 0 0 1 0 0 0 0 0>
  by fastforce
hence move_wina: < $\bigwedge g'. \text{spectroscopy\_moves } (\text{Defender\_Conj } p \ Q) \ g' \neq \text{None}$ 
   $\implies$  (subtract_fn 0 0 1 0 0 0 0 0) (expressiveness_price (ImmConj I  $\psi$ s)
    - E 0 0 0 0 1 0 0 0)
    = Some (expressiveness_price (ImmConj I  $\psi$ s) - E 0 0 1 0 1 0 0 0)
   $\wedge$  spectro_att_wins (expressiveness_price (ImmConj I  $\psi$ s) - E 0 0 1 0 1 0 0 0) g'>
using move_kind a_clause_wina subtracts by blast
from weak_spectroscopy_game.attacker_wins.Defense[OF def_conj] update move_wina have
  def_conj_wina:
    <spectro_att_wins (expressiveness_price (ImmConj I  $\psi$ s) - E 0 0 0 0 1 0 0 0)
      (Defender_Conj p Q)>
  by (metis (lifting))
have imm_to_conj:
  <spectroscopy_moves (Attacker_Immediate p Q) (Defender_Conj p Q)  $\neq$  None>
  by (simp add: <Q  $\neq \{\}$ >)
have imm_to_conj_wgt:
  <weak_spectroscopy_game.weight (Attacker_Immediate p Q) (Defender_Conj p Q)
    (expressiveness_price (ImmConj I  $\psi$ s))
    = Some (expressiveness_price (ImmConj I  $\psi$ s) - E 0 0 0 0 1 0 0 0)>
  using <Q  $\neq \{\}$ > leq_components subtracts(1) by force
from weak_spectroscopy_game.Attack[OF _ imm_to_conj imm_to_conj_wgt] def_conj_wina
show
  <spectro_att_wins (expressiveness_price (ImmConj I  $\psi$ s)) (Attacker_Immediate p Q)>
  by simp
qed
next
case (Obs  $\alpha \varphi$ )
have
  < $\forall p \ Q. Q \neq \{\} \longrightarrow \text{hml\_srbb\_inner.distinguishes\_from } (\text{hml\_srbb\_inner.Obs } \alpha \varphi) \ p \ Q$ 
   $\longrightarrow Q \twoheadrightarrow S \ Q \longrightarrow \text{spectro\_att\_wins } (\text{expr\_pr\_inner } (\text{hml\_srbb\_inner.Obs } \alpha \varphi))$ 
  (Attacker_Delayed p Q)>
proof(clarify)
  fix p Q
  assume
    <Q  $\neq \{\}$ >

```

```

    <hml_srb_inner.distinguishes_from (hml_srb_inner.Obs  $\alpha$   $\varphi$ ) p Q>
    < $\forall p \in Q. \forall q. p \Rightarrow q \longrightarrow q \in Q$ >
  have < $\exists p' Q'. p \mapsto a \alpha p' \wedge Q \mapsto aS \alpha Q'$ 
     $\wedge$  spectro_att_wins (expressiveness_price  $\varphi$ ) (Attacker_Immediate p' Q')>
  proof(cases < $\alpha = \tau$ >)
  case True
  with <hml_srb_inner.distinguishes_from (hml_srb_inner.Obs  $\alpha$   $\varphi$ ) p Q>
  have dist_unfold: <( $\exists p'. p \mapsto \tau p' \wedge p' \models SRBB \varphi$ )  $\vee$   $p \models SRBB \varphi$ > by simp
  then obtain p' where < $p' \models SRBB \varphi$ > < $p \mapsto a \alpha p'$ >
    unfolding True by blast
  from <hml_srb_inner.distinguishes_from (hml_srb_inner.Obs  $\alpha$   $\varphi$ ) p Q> have
    < $\forall q \in Q. (\neg q \models SRBB \varphi) \wedge (\nexists q'. q \mapsto \tau q' \wedge q' \models SRBB \varphi)$ >
    using True by auto
  hence < $\forall q \in Q. \neg q \models SRBB \varphi$ >
    using < $\forall p \in Q. \forall q. p \Rightarrow q \longrightarrow q \in Q$ > by fastforce
  hence <distinguishes_from  $\varphi$  p' Q>
    using < $p' \models SRBB \varphi$ > by auto
  with Obs have <spectro_att_wins (expressiveness_price  $\varphi$ ) (Attacker_Immediate p' Q)>
    using < $Q \neq \{\}$ > by blast
  moreover have < $Q \mapsto aS \alpha Q$ >
    unfolding True
    using < $\forall p \in Q. \forall q. p \Rightarrow q \longrightarrow q \in Q$ > silent_reachable_append_ $\tau$ 
    silent_reachable.intros(1) by blast
  ultimately show ?thesis using < $p \mapsto a \alpha p'$ > by blast
next
case False
with <hml_srb_inner.distinguishes_from (hml_srb_inner.Obs  $\alpha$   $\varphi$ ) p Q>
obtain p'' where < $(p \mapsto \alpha p'') \wedge (p'' \models SRBB \varphi)$ > by auto
let ?Q' = <step_set Q  $\alpha$ >
from <hml_srb_inner.distinguishes_from (hml_srb_inner.Obs  $\alpha$   $\varphi$ ) p Q>
have < $\forall q \in ?Q'. \neg q \models SRBB \varphi$ >
  using < $Q \neq \{\}$ > and step_set_is_step_set
  by force
from < $\forall q \in \text{step\_set } Q \alpha. \neg q \models SRBB \varphi$ > < $p \mapsto \alpha p'' \wedge p'' \models SRBB \varphi$ >
have <distinguishes_from  $\varphi$  p'' ?Q'> by simp
hence <spectro_att_wins (expressiveness_price  $\varphi$ ) (Attacker_Immediate p'' ?Q')>
  by (metis Obs distinction_implies_winning_budgets_empty_Q)
moreover have < $p \mapsto \alpha p''$ > using < $p \mapsto \alpha p'' \wedge p'' \models SRBB \varphi$ > by simp
moreover have < $Q \mapsto aS \alpha ?Q'$ > by (simp add: False lts.step_set_is_step_set)
ultimately show ?thesis by blast
qed
then obtain p' Q' where p'_Q': < $p \mapsto a \alpha p'$ > < $Q \mapsto aS \alpha Q'$ > and
  wina: <spectro_att_wins (expressiveness_price  $\varphi$ ) (Attacker_Immediate p' Q')> by blast
have attacker: <weak_spectroscopy_game.attacker (Attacker_Delayed p Q)> by simp
have
  <spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Immediate p' Q') =
    (if  $\exists a. p \mapsto a \alpha p' \wedge Q \mapsto aS \alpha Q'$  then subtract 1 0 0 0 0 0 0 0 else None)>
  for p Q p' Q' by simp
from this[of p Q p' Q'] have
  <spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Immediate p' Q') =
    subtract 1 0 0 0 0 0 0 0> using p'_Q' by auto
with expr_obs_phi[of  $\alpha$   $\varphi$ ] show
  <spectro_att_wins (expr_pr_inner (hml_srb_inner.Obs  $\alpha$   $\varphi$ )) (Attacker_Delayed p Q)>
  using weak_spectroscopy_game.Attack[OF attacker _ _ wina]
  by (smt (verit, best) option.sel option.simps(3))
qed
then show ?case by fastforce
next
case (Conj I  $\psi$ s)
have main_case:
  < $\forall \Psi_I \Psi p Q. \text{hml\_srb\_inner.Conj } I \psi s = \text{hml\_srb\_inner.Conj } \Psi_I \Psi \longrightarrow$ 

```

```

    Q ≠ {} → hml_srb_inner.distinguishes_from (hml_srb_inner.Conj I ψs) p Q
  → spectro_att_wins (expr_pr_inner (hml_srb_inner.Conj I ψs)) (Defender_Conj p Q)
proof clarify
  fix p Q
  assume case_assms:
    <Q ≠ {}>
    <hml_srb_inner.distinguishes_from (hml_srb_inner.Conj I ψs) p Q>
  hence distinctions: <∀q∈Q. ∃i∈I. hml_srb_inner.distinguishes (ψs i) p q>
    by auto
  hence inductive_wins: <∀q∈Q. ∃i∈I. hml_srb_inner.distinguishes (ψs i) p q
    ∧ spectro_att_wins (expr_pr_conjunct (ψs i)) (Attacker_Conjunct p q)>
    using Conj by blast
  define ψqs where
    <ψqs ≡ λq. (SOME ψ. ∃i∈I. ψ = ψs i ∧ hml_srb_inner.distinguishes ψ p q
    ∧ spectro_att_wins (expr_pr_conjunct ψ) (Attacker_Conjunct p q))>
  with inductive_wins someI have ψqs_spec:
    <∀q∈Q. ∃i∈I. ψqs q = ψs i ∧ hml_srb_inner.distinguishes (ψqs q) p q
    ∧ spectro_att_wins (expr_pr_conjunct (ψqs q)) (Attacker_Conjunct p q)>
    by (smt (verit))
  have conjuncts_present:
    <∀q∈Q. expr_pr_conjunct (ψqs q) ∈ expr_pr_conjunct ' (ψqs ' Q)>
    using <Q ≠ {}> by blast
  define e' where <e' = E
    (Sup (modal_depth ' (expr_pr_conjunct ' (ψqs ' Q))))
    (Sup (br_conj_depth ' (expr_pr_conjunct ' (ψqs ' Q))))
    (Sup (conj_depth ' (expr_pr_conjunct ' (ψqs ' Q))))
    (Sup (st_conj_depth ' (expr_pr_conjunct ' (ψqs ' Q))))
    (Sup (imm_conj_depth ' (expr_pr_conjunct ' (ψqs ' Q))))
    (Sup (pos_conjuncts ' (expr_pr_conjunct ' (ψqs ' Q))))
    (Sup (neg_conjuncts ' (expr_pr_conjunct ' (ψqs ' Q))))
    (Sup (neg_depth ' (expr_pr_conjunct ' (ψqs ' Q))))>
  from conjuncts_present have <∀q∈Q. (expr_pr_conjunct (ψqs q)) ≤ e'>
    unfolding e'_def
    by (metis SUP_upper energy.sel leq_components)
  with ψqs_spec weak_spectroscopy_game.win_a_upwards_closure
    have clause_win: <∀q∈Q. spectro_att_wins e' (Attacker_Conjunct p q)> by blast
  define eu' where <eu' = E
    (Sup (modal_depth ' (expr_pr_conjunct ' (ψs ' I))))
    (Sup (br_conj_depth ' (expr_pr_conjunct ' (ψs ' I))))
    (Sup (conj_depth ' (expr_pr_conjunct ' (ψs ' I))))
    (Sup (st_conj_depth ' (expr_pr_conjunct ' (ψs ' I))))
    (Sup (imm_conj_depth ' (expr_pr_conjunct ' (ψs ' I))))
    (Sup (pos_conjuncts ' (expr_pr_conjunct ' (ψs ' I))))
    (Sup (neg_conjuncts ' (expr_pr_conjunct ' (ψs ' I))))
    (Sup (neg_depth ' (expr_pr_conjunct ' (ψs ' I))))>
  have subset_form: <ψqs ' Q ⊆ ψs ' I>
    using ψqs_spec by fastforce
  hence <e' ≤ eu'> unfolding e'_def eu'_def leq_components
    by (simp add: Sup_subset_mono image_mono)
  define e where <e = E
    (modal_depth e')
    (br_conj_depth e')
    (1 + conj_depth e')
    (st_conj_depth e')
    (imm_conj_depth e')
    (pos_conjuncts e')
    (neg_conjuncts e')
    (neg_depth e')>
  have <e' = e - (E 0 0 1 0 0 0 0 0)> unfolding e_def e'_def by simp
  hence <Some e' = (subtract_fn 0 0 1 0 0 0 0 0) e>
    by (auto, smt (verit) add_increasing2 e_def energy.sel

```

```

    energy_leq_cases i0_lb le_numeral_extra(4))
have expr_lower: <(E 0 0 1 0 0 0 0 0) ≤ expr_pr_inner (Conj I ψs)>
  using case_assms(1) subset_form by auto
have eu'_comp: <eu' = (expr_pr_inner (Conj I ψs)) - (E 0 0 1 0 0 0 0 0)>
  unfolding eu'_def
  by (auto simp add: bot_enat_def image_image)
with expr_lower have eu'_characterization:
  <Some eu' = (subtract_fn 0 0 1 0 0 0 0 0) (expr_pr_inner (Conj I ψs))>
  by presburger
have <∀g'. spectroscopy_moves (Defender_Conj p Q) g' ≠ None
  → (∃q∈Q. (Attacker_Conjunct p q) = g')
  ∧ spectroscopy_moves (Defender_Conj p Q) g' = Some (subtract_fn 0 0 1 0 0 0 0 0)>
proof clarify
  fix g' upd
  assume upd_def: <spectroscopy_moves (Defender_Conj p Q) g' = Some upd>
  hence <∧px q. g' = Attacker_Conjunct px q
    ⇒ p = px ∧ q ∈ Q ∧ upd = (subtract_fn 0 0 1 0 0 0 0 0)>
    by (metis (mono_tags, lifting) local.conj_answer option.sel option.simps(3))
  with upd_def show
    <(∃q∈Q. Attacker_Conjunct p q = g')
      ∧ spectroscopy_moves (Defender_Conj p Q) g' = Some (subtract_fn 0 0 1 0 0 0 0 0)>
    by (cases g', auto)
qed
hence <∀g'. spectroscopy_moves (Defender_Conj p Q) g' ≠ None
  → (∃e'. (the (spectroscopy_moves (Defender_Conj p Q) g')) e = Some e'
    ∧ spectro_att_wins e' g'))>
  unfolding e_def
  using clause_win <Some e' = (subtract_fn 0 0 1 0 0 0 0 0) e> e_def by force
hence <spectro_att_wins e (Defender_Conj p Q)>
  unfolding e_def using weak_spectroscopy_game.attacker_wins.Defense
  by auto
moreover have <e ≤ expr_pr_inner (Conj I ψs)>
  using <e' ≤ eu'> eu'_characterization <Some e' = (subtract_fn 0 0 1 0 0 0 0 0) e>
  expr_lower case_assms(1) subset_form e_def
  by (smt (verit, ccfv_threshold) eu'_comp add_diff_cancel_enat
    add_mono_thms_linordered_semiring(1) enat.simps(3) enat_defs(2) energy.sel
    expr_pr_inner.simps idiff_0_right inst_conj_depth_inner.simps(2) le_numeral_extra(4)
    leq_components minus_energy_def not_one_le_zero)
ultimately show
  <spectro_att_wins (expr_pr_inner (hml_srbb_inner.Conj I ψs)) (Defender_Conj p Q)>
  using weak_spectroscopy_game.win_a_upwards_closure by blast
qed
moreover have
  <∀p Q. Q ≠ {} → hml_srbb_inner.distinguishes_from (hml_srbb_inner.Conj I ψs) p Q
    → Q →S Q → spectro_att_wins (expr_pr_inner (hml_srbb_inner.Conj I ψs))
      (Attacker_Delayed p Q)>
proof clarify
  fix p Q
  assume
    <Q ≠ {}>
    <hml_srbb_inner.distinguishes_from (hml_srbb_inner.Conj I ψs) p Q>
  hence
    <spectro_att_wins (expr_pr_inner (hml_srbb_inner.Conj I ψs)) (Defender_Conj p Q)>
    using main_case by blast
moreover have <spectroscopy_moves (Attacker_Delayed p Q) (Defender_Conj p Q) = id_up>
  by auto
ultimately show
  <spectro_att_wins (expr_pr_inner (hml_srbb_inner.Conj I ψs))
    (Attacker_Delayed p Q)>
  by (metis weak_spectroscopy_game.attacker_wins_Ga_with_id_step option.discI
    option.sel spectroscopy_defender.simps(4))

```

```

qed
ultimately show ?case by fastforce
next
case (StableConj I  $\psi$ s)
— The following proof is virtually the same as for Conj I  $\psi$ s
have main_case:  $\langle (\forall \Psi\_I \Psi p Q. \text{StableConj } I \psi = \text{StableConj } \Psi\_I \Psi \longrightarrow$ 
   $Q \neq \{\} \longrightarrow \text{hml\_srbb\_inner.distinguishes\_from } (\text{StableConj } I \psi) p Q \longrightarrow$ 
   $(\forall q \in Q. \nexists q'. q \mapsto \tau q') \longrightarrow \text{spectro\_att\_wins } (\text{expr\_pr\_inner } (\text{StableConj } I \psi)) (\text{Defender\_Stable\_Conj } p Q)) \rangle$ 
proof clarify
  fix p Q
  assume case_assms:
     $\langle Q \neq \{\} \rangle$ 
     $\langle \text{hml\_srbb\_inner.distinguishes\_from } (\text{StableConj } I \psi) p Q \rangle$ 
     $\langle \forall q \in Q. \nexists q'. q \mapsto \tau q' \rangle$ 
  hence distinctions:  $\langle \forall q \in Q. \exists i \in I. \text{hml\_srbb\_conj.distinguishes } (\psi i) p q \rangle$ 
  by (metis hml_srbb_conj.distinguishes_def hml_srbb_inner.distinguishes_from_def
    hml_srbb_inner_models.simps(3))
  hence inductive_wins:  $\langle \forall q \in Q. \exists i \in I. \text{hml\_srbb\_conj.distinguishes } (\psi i) p q$ 
     $\wedge \text{spectro\_att\_wins } (\text{expr\_pr\_conjunct } (\psi i)) (\text{Attacker\_Conjunct } p q) \rangle$ 
  using StableConj by blast
  define  $\psi$ qs where
     $\langle \psi$ qs  $\equiv \lambda q. (\text{SOME } \psi. \exists i \in I. \psi = \psi i \wedge \text{hml\_srbb\_conj.distinguishes } \psi p q$ 
       $\wedge \text{spectro\_att\_wins } (\text{expr\_pr\_conjunct } \psi) (\text{Attacker\_Conjunct } p q)) \rangle$ 
  with inductive_wins someI have  $\psi$ qs_spec:
     $\langle \forall q \in Q. \exists i \in I. \psi$ qs q =  $\psi$  i  $\wedge \text{hml\_srbb\_conj.distinguishes } (\psi$ qs q) p q
       $\wedge \text{spectro\_att\_wins } (\text{expr\_pr\_conjunct } (\psi$ qs q)) (\text{Attacker\_Conjunct } p q) \rangle
    by (smt (verit))
  have conjuncts_present:
     $\langle \forall q \in Q. \text{expr\_pr\_conjunct } (\psi$ qs q)  $\in \text{expr\_pr\_conjunct ' } (\psi$ qs ' Q) \rangle
  using  $\langle Q \neq \{\} \rangle$  by blast
  define e' where  $\langle e' = E$ 
    (Sup (modal_depth ' (expr_pr_conjunct ' ( $\psi$ qs ' Q))))
    (Sup (br_conj_depth ' (expr_pr_conjunct ' ( $\psi$ qs ' Q))))
    (Sup (conj_depth ' (expr_pr_conjunct ' ( $\psi$ qs ' Q))))
    (Sup (st_conj_depth ' (expr_pr_conjunct ' ( $\psi$ qs ' Q))))
    (Sup (imm_conj_depth ' (expr_pr_conjunct ' ( $\psi$ qs ' Q))))
    (Sup (pos_conjuncts ' (expr_pr_conjunct ' ( $\psi$ qs ' Q))))
    (Sup (neg_conjuncts ' (expr_pr_conjunct ' ( $\psi$ qs ' Q))))
    (Sup (neg_depth ' (expr_pr_conjunct ' ( $\psi$ qs ' Q))))
  from conjuncts_present have  $\langle \forall q \in Q. (\text{expr\_pr\_conjunct } (\psi$ qs q))  $\leq e' \rangle$  unfolding e'_def
  by (smt (verit, best) SUP_upper energy.sel energy.simps(3) energy_leq_cases image_iff)
  with  $\psi$ qs_spec weak_spectroscopy_game.win_a_upwards_closure
  have clause_win:  $\langle \forall q \in Q. \text{spectro\_att\_wins } e' (\text{Attacker\_Conjunct } p q) \rangle$  by blast
  define eu' where  $\langle eu' = E$ 
    (Sup (modal_depth ' (expr_pr_conjunct ' ( $\psi$ s ' I))))
    (Sup (br_conj_depth ' (expr_pr_conjunct ' ( $\psi$ s ' I))))
    (Sup (conj_depth ' (expr_pr_conjunct ' ( $\psi$ s ' I))))
    (Sup (st_conj_depth ' (expr_pr_conjunct ' ( $\psi$ s ' I))))
    (Sup (imm_conj_depth ' (expr_pr_conjunct ' ( $\psi$ s ' I))))
    (Sup (pos_conjuncts ' (expr_pr_conjunct ' ( $\psi$ s ' I))))
    (Sup (neg_conjuncts ' (expr_pr_conjunct ' ( $\psi$ s ' I))))
    (Sup (neg_depth ' (expr_pr_conjunct ' ( $\psi$ s ' I))))
  have subset_form:  $\langle \psi$ qs ' Q  $\subseteq \psi$ s ' I  $\rangle$ 
  using  $\psi$ qs_spec by fastforce
  hence  $\langle e' \leq eu' \rangle$  unfolding e'_def eu'_def
  by (simp add: Sup_subset_mono image_mono)
  define e where  $\langle e = E$ 
    (modal_depth e')
    (br_conj_depth e')
    (conj_depth e')

```

```

    (1 + st_conj_depth e')
    (imm_conj_depth e')
    (pos_conjuncts e')
    (neg_conjuncts e')
    (neg_depth e')>
have <e' = e - (E 0 0 0 1 0 0 0 0)> unfolding e_def e'_def by auto
hence <Some e' = (subtract_fn 0 0 0 1 0 0 0 0) e>
  by (metis e_def energy.sel energy_leq_cases i0_lb le_iff_add)
have expr_lower: <(E 0 0 0 1 0 0 0 0) ≤ expr_pr_inner (StableConj I ψs)>
  using case_assms(1) subset_form by force
have eu'_comp: <eu' = (expr_pr_inner (StableConj I ψs)) - (E 0 0 0 1 0 0 0 0)>
  unfolding eu'_def using energy.sel
  by (auto simp add: bot_enat_def, (metis (no_types, lifting) SUP_cong image_image)+)
with expr_lower have eu'_characterization:
  <Some eu' = (subtract_fn 0 0 0 1 0 0 0 0) (expr_pr_inner (StableConj I ψs))>
  by presburger
have <∀g'. spectroscopy_moves (Defender_Stable_Conj p Q) g' ≠ None
  → (∃q∈Q. (Attacker_Conjunct p q) = g')
  ∧ spectroscopy_moves (Defender_Stable_Conj p Q) g' = (subtract 0 0 0 1 0 0 0 0)>
proof clarify
  fix g' upd
  assume upd_def: <spectroscopy_moves (Defender_Stable_Conj p Q) g' = Some upd>
  hence <∧px q. g' = Attacker_Conjunct px q
    ⇒ p = px ∧ q ∈ Q ∧ upd = (subtract_fn 0 0 0 1 0 0 0 0)>
    by (metis (no_types, lifting) local.conj_s_answer option.discI option.inject)
  with upd_def case_assms(1) show
    <(∃q∈Q. Attacker_Conjunct p q = g')
      ∧ spectroscopy_moves (Defender_Stable_Conj p Q) g' = (subtract 0 0 0 1 0 0 0 0)>
    by (cases g', auto)
qed
hence <∀g'. spectroscopy_moves (Defender_Stable_Conj p Q) g' ≠ None
  → (∃e'. (the (spectroscopy_moves (Defender_Stable_Conj p Q) g')) e = Some e'
    ∧ spectro_att_wins e' g'))>
  unfolding e_def
  using clause_win <Some e' = (subtract_fn 0 0 0 1 0 0 0 0) e> e_def by force
hence <spectro_att_wins e (Defender_Stable_Conj p Q)>
  unfolding e_def
  by (auto simp add: weak_spectroscopy_game.attacker_wins.Defense)
moreover have <e ≤ expr_pr_inner (StableConj I ψs)>
  using <e' ≤ eu'> eu'_characterization expr_lower case_assms(1) subset_form
  unfolding e_def eu'_comp minus_energy_def leq_components
  by (metis add_diff_assoc_enat add_diff_cancel_enat add_left_mono enat.simps(3)
    enat_defs(2) energy.sel idiff_0_right)
ultimately show
  <spectro_att_wins (expr_pr_inner (StableConj I ψs)) (Defender_Stable_Conj p Q)>
  using weak_spectroscopy_game.win_a_upwards_closure by blast
qed
moreover have <(∀p Q. Q ≠ {}
  → hml_srbb_inner.distinguishes_from (StableConj I ψs) p Q → Q →S Q
  → spectro_att_wins (expr_pr_inner (StableConj I ψs)) (Attacker_Delayed p Q))>
proof clarify
  — This is where things are more complicated than in the Conj-case. (We have to differentiate
    situations where the stability requirement finishes the distinction.)
  fix p Q
  assume case_assms:
    <Q ≠ {}>
    <hml_srbb_inner.distinguishes_from (StableConj I ψs) p Q>
    <∀q'∈Q. ∃q∈Q. q → q'>
    <∀q∈Q. ∀q'. q → q' → q' ∈ Q>
  define Q' where <Q' = { q ∈ Q. (∄q'. q →τ q')}>
  with case_assms(2) have Q'_spec:

```

```

    <hml_srbb_inner.distinguishes_from (StableConj I  $\psi$ s) p Q' > < $\#p''$ . p  $\mapsto$   $\tau$  p'' >
  unfolding hml_srbb_inner.distinguishes_from_def by auto
hence move:
  <spectroscopy_moves (Attacker_Delayed p Q) (Defender_Stable_Conj p Q') = id_up>
  unfolding Q'_def by auto
show <spectro_att_wins (expr_pr_inner (StableConj I  $\psi$ s)) (Attacker_Delayed p Q)>
proof (cases <Q' = {}>)
  case True
  hence
    <spectroscopy_moves (Defender_Stable_Conj p Q') (Defender_Conj p {})>
    = (subtract 0 0 0 1 0 0 0 0) > by auto
  moreover have
    < $\forall g'$ . spectroscopy_moves (Defender_Stable_Conj p Q') g'  $\neq$  None
     $\longrightarrow$  g' = (Defender_Conj p {})>
  proof clarify
    fix g' u
    assume
      <spectroscopy_moves (Defender_Stable_Conj p Q') g' = Some u>
    with True show <g' = Defender_Conj p {}>
      by (induct g', auto, metis option.discI, metis empty_iff option.discI)
  qed
ultimately have win_transfer:
  < $\forall e$ . E 0 0 0 1 0 0 0 0  $\leq$  e
     $\wedge$  spectro_att_wins (e - E 0 0 0 1 0 0 0 0) (Defender_Conj p {})>
     $\longrightarrow$  spectro_att_wins e (Defender_Stable_Conj p Q') >
  using weak_spectroscopy_game.attacker_wins.Defense
  by (smt (verit, ccfv_SIG) option.sel spectroscopy_defender.simps(7))
have < $\forall g'$ . spectroscopy_moves (Defender_Conj p {}) g' = None>
proof
  fix g'
  show <spectroscopy_moves (Defender_Conj p {}) g' = None> by (induct g', auto)
qed
hence < $\forall e$ . spectro_att_wins e (Defender_Conj p {})>
  using weak_spectroscopy_game.attacker_wins.Defense by fastforce
moreover have
  < $\forall e$ . (subtract_fn 0 0 0 1 0 0 0 0) e  $\neq$  None  $\longrightarrow$  e  $\geq$  (E 0 0 0 1 0 0 0 0)>
  using minus_energy_def by presburger
ultimately have < $\forall e$ . e  $\geq$  (E 0 0 0 1 0 0 0 0)
   $\longrightarrow$  spectro_att_wins e (Defender_Stable_Conj p Q') >
  using win_transfer by presburger
moreover have <expr_pr_inner (StableConj I  $\psi$ s)  $\geq$  (E 0 0 0 1 0 0 0 0)>
  by auto
ultimately show ?thesis
  by (metis move weak_spectroscopy_game.attacker_wins_Ga_with_id_step option.discI
    option.sel spectroscopy_defender.simps(4))
next
  case False
  with move show ?thesis
    using main_case Q'_spec weak_spectroscopy_game.attacker_wins_Ga_with_id_step
    unfolding Q'_def
    by (metis (mono_tags, lifting) mem_Collect_eq option.distinct(1) option.sel
      spectroscopy_defender.simps(4))
  qed
qed
ultimately show ?case by blast
next
  case (BranchConj  $\alpha$   $\varphi$  I  $\psi$ s)
  have main_case:
    < $\forall p$  Q p' Q_ $\alpha$ .
      hml_srbb_inner.distinguishes_from (BranchConj  $\alpha$   $\varphi$  I  $\psi$ s) p Q  $\longrightarrow$  p  $\mapsto$  a  $\alpha$  p'
       $\longrightarrow$  p'  $\models$  SRBB  $\varphi \longrightarrow$  Q_ $\alpha$  = Q - hml_srbb_inner.model_set (Obs  $\alpha$   $\varphi$ )>

```

```

    → spectro_att_wins (expr_pr_inner (BranchConj  $\alpha$   $\varphi$  I  $\psi$ s))
      (Defender_Branch p  $\alpha$  p' (Q - Q $_{\alpha}$ ) Q $_{\alpha}$ )>
proof ((rule allI)+, (rule impI)+)
fix p Q p' Q $_{\alpha}$ 
assume case_assms:
  <hml_srbb_inner.distinguishes_from (BranchConj  $\alpha$   $\varphi$  I  $\psi$ s) p Q>
  <p  $\mapsto$  a  $\alpha$  p'>
  <p'  $\models$  SRBB  $\varphi$ >
  <Q $_{\alpha}$  = Q - hml_srbb_inner.model_set (Obs  $\alpha$   $\varphi$ )>
from case_assms(1) have distinctions:
  < $\forall q \in (Q \cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)$ ).
     $\exists i \in I. \text{hml\_srbb\_conj.distinguishes } (\psi \text{ s } i) \text{ p } q$ >
  using srbb_dist_branch_conjunction_implies_dist_conjunct_or_branch
    hml_srbb_inner.distinction_unlifting unfolding hml_srbb_inner.distinguishes_def
  by (metis Int_Collect)
hence inductive_wins: < $\forall q \in (Q \cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)$ ).
   $\exists i \in I. \text{hml\_srbb\_conj.distinguishes } (\psi \text{ s } i) \text{ p } q$ 
   $\wedge \text{spectro\_att\_wins (expr\_pr\_conjunct } (\psi \text{ s } i)) (\text{Attacker\_Conjunct p } q)$ >
  using BranchConj by blast
define  $\psi$ qs where
  < $\psi$ qs  $\equiv \lambda q. (\text{SOME } \psi. \exists i \in I. \psi = \psi \text{ s } i \wedge \text{hml\_srbb\_conj.distinguishes } \psi \text{ p } q$ 
     $\wedge \text{spectro\_att\_wins (expr\_pr\_conjunct } \psi) (\text{Attacker\_Conjunct p } q))$ >
with inductive_wins someI have  $\psi$ qs_spec:
  < $\forall q \in (Q \cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)$ ).
     $\exists i \in I. \psi$ qs q =  $\psi$  s i  $\wedge \text{hml\_srbb\_conj.distinguishes } (\psi$ qs q) p q
     $\wedge \text{spectro\_att\_wins (expr\_pr\_conjunct } (\psi$ qs q)) (\text{Attacker\_Conjunct p } q)>
  by (smt (verit))
have conjuncts_present:
  < $\forall q \in (Q \cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)$ ). expr\_pr\_conjunct ( $\psi$ qs q)
     $\in \text{expr\_pr\_conjunct ' } (\psi$ qs ' (Q  $\cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)))$ >
  by blast
define e'0 where <e'0 = E
  (Sup (modal_depth ' (expr\_pr\_conjunct '
    ( $\psi$ qs ' (Q  $\cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)))$ )))
  (Sup (br\_conj\_depth ' (expr\_pr\_conjunct '
    ( $\psi$ qs ' (Q  $\cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)))$ )))
  (Sup (conj\_depth ' (expr\_pr\_conjunct '
    ( $\psi$ qs ' (Q  $\cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)))$ )))
  (Sup (st\_conj\_depth ' (expr\_pr\_conjunct '
    ( $\psi$ qs ' (Q  $\cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)))$ )))
  (Sup (imm\_conj\_depth ' (expr\_pr\_conjunct '
    ( $\psi$ qs ' (Q  $\cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)))$ )))
  (Sup (pos\_conjuncts ' (expr\_pr\_conjunct '
    ( $\psi$ qs ' (Q  $\cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)))$ )))
  (Sup (neg\_conjuncts ' (expr\_pr\_conjunct '
    ( $\psi$ qs ' (Q  $\cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)))$ )))
  (Sup (neg\_depth ' (expr\_pr\_conjunct '
    ( $\psi$ qs ' (Q  $\cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)))$ )))>
from conjuncts_present have branch_answer_bound:
  < $\forall q \in Q \cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi). \text{expr\_pr\_conjunct } (\psi$ qs q)  $\leq$  e'0>
  using e'0_def SUP_upper energy.sel energy.simps(3) energy_leq_cases image_iff
  by (smt (z3))
with  $\psi$ qs_spec weak_spectroscopy_game.win_a_upwards_closure have
  conj_wins: < $\forall q \in (Q \cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)$ ).
    spectro\_att\_wins e'0 (Attacker\_Conjunct p q)> by blast
define eu'0 where <eu'0 = E
  (Sup (modal_depth ' (expr\_pr\_conjunct ' ( $\psi$ s ' I))))
  (Sup (br\_conj\_depth ' (expr\_pr\_conjunct ' ( $\psi$ s ' I))))
  (Sup (conj\_depth ' (expr\_pr\_conjunct ' ( $\psi$ s ' I))))
  (Sup (st\_conj\_depth ' (expr\_pr\_conjunct ' ( $\psi$ s ' I))))
  (Sup (imm\_conj\_depth ' (expr\_pr\_conjunct ' ( $\psi$ s ' I))))>

```

```

(Sup (pos_conjuncts ' (expr_pr_conjunct ' ( $\psi$ s ' I))))
(Sup (neg_conjuncts ' (expr_pr_conjunct ' ( $\psi$ s ' I))))
(Sup (neg_depth ' (expr_pr_conjunct ' ( $\psi$ s ' I))))>
have subset_form: < $\psi$ qs ' ( $Q \cap \text{hml\_srbb\_inner.model\_set (Obs } \alpha \varphi)$ )  $\subseteq \psi$ s ' I>
using  $\psi$ qs_spec by fastforce
hence < $e'0 \leq \text{eu}'0$ > unfolding  $e'0\_def \text{eu}'0\_def$ 
by (metis (mono_tags, lifting) Sup_subset_mono energy.sel energy_leq_cases image_mono)
have no_q_way: < $\forall q \in Q\_a. \nexists q'. q \mapsto \alpha q' \wedge \text{hml\_srbb\_models } q' \varphi$ >
using case_assms(4)
by fastforce
define Q' where <Q'  $\equiv (\text{soft\_step\_set } Q\_a \alpha)$ >
hence <distinguishes_from  $\varphi$  p' Q'>
using case_assms(2,3) no_q_way soft_step_set_is_soft_step_set mem_Collect_eq
unfolding case_assms(4)
by fastforce
with BranchConj have win_a_branch:
<spectro_att_wins (expressiveness_price  $\varphi$ ) (Attacker_Immediate p' Q')>
using distinction_implies_winning_budgets_empty_Q by (cases <Q' = {}>) auto
have <expr_pr_inner (Obs  $\alpha \varphi$ )  $\geq (E \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0)$ > by auto
hence <(subtract_fn 1 0 0 0 0 0 0 0) (expr_pr_inner (Obs  $\alpha \varphi$ ))
= Some (expressiveness_price  $\varphi$ )>
using expr_obs_phi by auto
with win_a_branch have win_a_step:
<spectro_att_wins (the ((subtract_fn 1 0 0 0 0 0 0 0) (expr_pr_inner (Obs  $\alpha \varphi$ ))))
(Attacker_Immediate p' Q')> by auto
define e' where <e' = E
(Sup (modal_depth ' ({expr_pr_inner (Obs  $\alpha \varphi$ )}  $\cup$  (expr_pr_conjunct ' ( $\psi$ s ' I))))
(Sup (br_conj_depth ' ({expr_pr_inner (Obs  $\alpha \varphi$ )}  $\cup$  (expr_pr_conjunct ' ( $\psi$ s ' I))))
(Sup (conj_depth ' ({expr_pr_inner (Obs  $\alpha \varphi$ )}  $\cup$  (expr_pr_conjunct ' ( $\psi$ s ' I))))
(Sup (st_conj_depth ' ({expr_pr_inner (Obs  $\alpha \varphi$ )}  $\cup$  (expr_pr_conjunct ' ( $\psi$ s ' I))))
(Sup (imm_conj_depth ' ({expr_pr_inner (Obs  $\alpha \varphi$ )}  $\cup$  (expr_pr_conjunct ' ( $\psi$ s ' I))))
(Sup ({1 + modal_depth_srbb  $\varphi$ }
 $\cup$  (pos_conjuncts ' ({expr_pr_inner (Obs  $\alpha \varphi$ )}  $\cup$  (expr_pr_conjunct ' ( $\psi$ s ' I))))))
(Sup (neg_conjuncts ' ({expr_pr_inner (Obs  $\alpha \varphi$ )}  $\cup$  (expr_pr_conjunct ' ( $\psi$ s ' I))))
(Sup (neg_depth ' ({expr_pr_inner (Obs  $\alpha \varphi$ )}  $\cup$  (expr_pr_conjunct ' ( $\psi$ s ' I))))>
have < $\text{eu}'0 \leq e'$ > unfolding  $e'_def \text{eu}'0\_def$ 
by (auto, meson sup.cobounded2 sup.coboundedI2)
have <spectroscopy_moves (Attacker_Branch p' Q') (Attacker_Immediate p' Q')
= Some (subtract_fn 1 0 0 0 0 0 0 0)> by simp
with win_a_step weak_spectroscopy_game.attacker_wins.Attack have obs_later_win:
<spectro_att_wins (expr_pr_inner (Obs  $\alpha \varphi$ )) (Attacker_Branch p' Q')>
by force
hence e'_win: <spectro_att_wins e' (Attacker_Branch p' Q')>
unfolding  $e'_def$  using weak_spectroscopy_game.win_a_upwards_closure
by auto
have depths: <1 + modal_depth_srbb  $\varphi$  = modal_depth (expr_pr_inner (Obs  $\alpha \varphi$ ))> by simp
have six_e': <pos_conjuncts e' = Sup ({1 + modal_depth_srbb  $\varphi$ }
 $\cup$  (pos_conjuncts ' ({expr_pr_inner (Obs  $\alpha \varphi$ )}  $\cup$  (expr_pr_conjunct ' ( $\psi$ s ' I))))>
using energy.sel(6) unfolding  $e'_def$  by blast
hence six_e'_simp: <pos_conjuncts e' = Sup ({1 + modal_depth_srbb  $\varphi$ }
 $\cup$  (pos_conjuncts ' (expr_pr_conjunct ' ( $\psi$ s ' I))))>
by (auto simp add: modal_depth_dominates_pos_conjuncts add_increasing
sup.absorb2 sup.coboundedI1)
hence <pos_conjuncts e'  $\leq$  modal_depth e'>
unfolding  $e'_def$ 
by (auto, smt (verit) SUP_mono energy.sel(1) energy.sel(6) image_iff
modal_depth_dominates_pos_conjuncts sup.coboundedI2)
hence <modal_depth (the (min1_6 e')) = (pos_conjuncts e')>
by simp
with six_e' have min_e'_def: <min1_6 e' = Some (E
(Sup ({1 + modal_depth_srbb  $\varphi$ }  $\cup$  pos_conjuncts ' (expr_pr_conjunct ' ( $\psi$ s ' I))))>

```

```

(Sup (br_conj_depth ' ({expr_pr_inner (Obs α φ)} ∪ (expr_pr_conjunct ' (ψs ' I))))
(Sup (conj_depth ' ({expr_pr_inner (Obs α φ)} ∪ (expr_pr_conjunct ' (ψs ' I))))
(Sup (st_conj_depth ' ({expr_pr_inner (Obs α φ)} ∪ (expr_pr_conjunct ' (ψs ' I))))
(Sup (imm_conj_depth ' ({expr_pr_inner (Obs α φ)} ∪ (expr_pr_conjunct ' (ψs ' I))))
(Sup ({1 + modal_depth_srbb φ}
      ∪ (pos_conjuncts ' ({expr_pr_inner (Obs α φ)} ∪ (expr_pr_conjunct ' (ψs ' I))))))
(Sup (neg_conjuncts ' ({expr_pr_inner (Obs α φ)} ∪ (expr_pr_conjunct ' (ψs ' I))))
(Sup (neg_depth ' ({expr_pr_inner (Obs α φ)} ∪ (expr_pr_conjunct ' (ψs ' I))))>
using e'_def min1_6_def six_e'_simp
by (smt (z3) energy.case_eq_if energy.sel min_1_6_simps(1))
hence <expr_pr_inner (Obs α φ) ≤ the (min1_6 e')>
by force
hence obs_win: <spectro_att_wins (the (min1_6 e')) (Attacker_Branch p' Q')>
using obs_later_win weak_spectroscopy_game.win_a_upwards_closure by blast
define e where <e = E
(modal_depth e')
(1 + br_conj_depth e')
(1 + conj_depth e')
(st_conj_depth e')
(imm_conj_depth e')
(pos_conjuncts e')
(neg_conjuncts e')
(neg_depth e')>
have <e' = e - (E 0 1 1 0 0 0 0 0)> unfolding e_def e'_def by auto
hence e'_comp: <Some e' = (subtract_fn 0 1 1 0 0 0 0 0) e>
by (metis e_def energy.sel energy_leq_cases i0_lb le_iff_add)
have expr_lower: <(E 0 1 1 0 0 0 0 0) ≤ expr_pr_inner (BranchConj α φ I ψs)>
using case_assms subset_form by auto
have e'_minus: <e' = expr_pr_inner (BranchConj α φ I ψs) - E 0 1 1 0 0 0 0 0>
unfolding e'_def using energy.sel
by (auto simp add: bot_enat_def sup.left_commute,
    (metis (no_types, lifting) SUP_cong image_image)+)
with expr_lower have e'_characterization:
<Some e' = (subtract_fn 0 1 1 0 0 0 0 0) (expr_pr_inner (BranchConj α φ I ψs))>
by presburger
have moves: <∀g'. spectroscopy_moves (Defender_Branch p α p' (Q - Q_α) Q_α) g' ≠ None
→ (((Attacker_Branch p' Q' = g')
  ∧ (spectroscopy_moves (Defender_Branch p α p' (Q - Q_α) Q_α) g'
    = Some (λe. Option.bind ((subtract_fn 0 1 1 0 0 0 0 0) e) min1_6)))
  ∨ ((∃q∈(Q - Q_α). Attacker_Conjunct p q = g'
    ∧ spectroscopy_moves (Defender_Branch p α p' (Q - Q_α) Q_α) g'
    = (subtract 0 1 1 0 0 0 0 0))))>
proof clarify
fix g' u
assume no_subtr_move:
<spectroscopy_moves (Defender_Branch p α p' (Q - Q_α) Q_α) g' = Some u>
<¬ (∃q∈Q - Q_α. Attacker_Conjunct p q = g'
  ∧ spectroscopy_moves (Defender_Branch p α p' (Q - Q_α) Q_α) g'
    = subtract 0 1 1 0 0 0 0 0)>
hence <g' = Attacker_Branch p' Q'>
unfolding Q'_def using soft_step_set_is_soft_step_set no_subtr_move local.br_answer
by (cases g', auto, (metis (no_types, lifting) option.discI)+)
moreover have <Attacker_Branch p' Q' = g'
→ spectroscopy_moves (Defender_Branch p α p' (Q - Q_α) Q_α) g'
  = Some (λe. Option.bind ((subtract_fn 0 1 1 0 0 0 0 0) e) min1_6)>
unfolding Q'_def using soft_step_set_is_soft_step_set by auto
ultimately show <Attacker_Branch p' Q' = g'
  ∧ spectroscopy_moves (Defender_Branch p α p' (Q - Q_α) Q_α) g'
    = Some (λe. Option.bind ((subtract_fn 0 1 1 0 0 0 0 0) e) min1_6)>
by blast
qed

```

```

have obs_e:
  <∃e'. (λe. Option.bind ((subtract_fn 0 1 1 0 0 0 0 0) e) min1_6) e = Some e'
    ∧ spectro_att_wins e' (Attacker_Branch p' Q')>
  using obs_win e'_comp min_e'_def
  by (smt (verit, best) bind.bind_lunit min_1_6_some option.collapse)
have <∀q∈(Q - Q_α).
  spectroscopy_moves (Defender_Branch p α p' (Q - Q_α) Q_α) (Attacker_Conjunct p q)
  = (subtract 0 1 1 0 0 0 0 0)
  → spectro_att_wins e'0 (Attacker_Conjunct p q)>
  using conj_wins <eu'0 ≤ e'> case_assms(4) by blast
with obs_e moves have move_wins:
  <∀g'. spectroscopy_moves (Defender_Branch p α p' (Q - Q_α) Q_α) g' ≠ None
  → (∃e'. (the (spectroscopy_moves (Defender_Branch p α p' (Q - Q_α) Q_α) g')) e
    = Some e' ∧ spectro_att_wins e' g')>
  using <eu'0 ≤ e'> e'_comp <e'0 ≤ eu'0> weak_spectroscopy_game.win_a_upwards_closure
  by (smt (verit, ccfv_SIG) option.sel)
moreover have <expr_pr_inner (BranchConj α φ I ψs) = e>
  using e'_characterization e'_minus unfolding e_def by force
ultimately show <spectro_att_wins (expr_pr_inner (BranchConj α φ I ψs))
  (Defender_Branch p α p' (Q - Q_α) Q_α)>
  using weak_spectroscopy_game.attacker_wins.Defense spectroscopy_defender.simps(5)
  by metis
qed
moreover have
  <∀p Q. Q ≠ {} → hml_srbb_inner.distinguishes_from (BranchConj α φ I ψs) p Q
  → spectro_att_wins (expr_pr_inner (BranchConj α φ I ψs)) (Attacker_Delayed p Q)>
proof clarify
  fix p Q
  assume case_assms:
    <hml_srbb_inner.distinguishes_from (BranchConj α φ I ψs) p Q>
  from case_assms(1) obtain p' where p'_spec: <p ↦ α p'> <p' ⊨ SRBB φ>
  unfolding hml_srbb_inner.distinguishes_from_def
  and distinguishes_def by auto
  define Q_α where <Q_α = Q - hml_srbb_inner.model_set (Obs α φ)>
  have <spectro_att_wins (expr_pr_inner (BranchConj α φ I ψs))
    (Defender_Branch p α p' (Q - Q_α) Q_α)>
    using main_case case_assms(1) p'_spec Q_α_def by blast
  moreover have <spectroscopy_moves (Attacker_Delayed p Q)
    (Defender_Branch p α p' (Q - Q_α) Q_α) = id_up>
    using p'_spec Q_α_def by auto
  ultimately show
    <spectro_att_wins (expr_pr_inner (BranchConj α φ I ψs)) (Attacker_Delayed p Q)>
    using weak_spectroscopy_game.attacker_wins_Ga_with_id_step by auto
qed
ultimately show ?case by blast
next
case (Pos χ)
show ?case
proof clarify
  fix p q
  assume case_assms: <hml_srbb_conj.distinguishes (Pos χ) p q>
  then obtain p' where p'_spec: <p ⇒ p'> <p' ∈ hml_srbb_inner.model_set χ>
  unfolding hml_srbb_conj.distinguishes_def by auto
  moreover have q_reach: <silent_reachable_set {q} ∩ hml_srbb_inner.model_set χ = {}>
  using case_assms sreachable_set_is_sreachable
  unfolding hml_srbb_conj.distinguishes_def by force
  ultimately have distinction:
    <hml_srbb_inner.distinguishes_from χ p' (silent_reachable_set {q})>
  unfolding hml_srbb_inner.distinguishes_from_def by auto
  have q_reach_nonempty:
    <silent_reachable_set {q} ≠ {}>

```

```

    <silent_reachable_set {q}  $\rightarrow$ S silent_reachable_set {q} >
  unfolding silent_reachable_set_def
  using silent_reachable.intros(1) silent_reachable_trans by auto
  hence <spectro_att_wins (expr_pr_inner  $\chi$ )
    (Attacker_Delayed p' (silent_reachable_set {q}))>
    using distinction Pos by blast
  from p'_spec(1) this have
    <spectro_att_wins (expr_pr_inner  $\chi$ ) (Attacker_Delayed p (silent_reachable_set {q}))>
    by (induct, auto,
      metis weak_spectroscopy_game.attacker_wins_Ga_with_id_step procrastination
        option.distinct(1) option.sel spectroscopy_defender.simps(4))
  moreover have <spectroscopy_moves (Attacker_Conjunct p q)
    (Attacker_Delayed p (silent_reachable_set {q})) = Some min1_6>
    using q_reach_nonempty sreachable_set_is_sreachable by fastforce
  moreover have <the (min1_6 (expr_pr_conjunct (Pos  $\chi$ )))  $\geq$  expr_pr_inner  $\chi$ >
    unfolding min1_6_def
    by (auto simp add: energy_leq_cases modal_depth_dominates_pos_conjuncts)
  ultimately show <spectro_att_wins (expr_pr_conjunct (Pos  $\chi$ )) (Attacker_Conjunct p q)>
    using weak_spectroscopy_game.attacker_wins.simps
      weak_spectroscopy_game.win_a_upwards_closure spectroscopy_defender.simps(3)
    by (metis (no_types, lifting) min_1_6_some option.discI option.exhaust_sel option.sel)
qed
next
case (Neg  $\chi$ )
show ?case
proof clarify
  fix p q
  assume case_assms: <hml_srbj_conj.distinguishes (Neg  $\chi$ ) p q>
  then obtain q' where q'_spec: <q  $\rightarrow$  q'> <q'  $\in$  hml_srbj_inner.model_set  $\chi$ >
    unfolding hml_srbj_conj.distinguishes_def by auto
  moreover have p_reach: <silent_reachable_set {p}  $\cap$  hml_srbj_inner.model_set  $\chi$  = {}>
    using case_assms sreachable_set_is_sreachable
    unfolding hml_srbj_conj.distinguishes_def by force
  ultimately have distinction:
    <hml_srbj_inner.distinguishes_from  $\chi$  q' (silent_reachable_set {p})>
    unfolding hml_srbj_inner.distinguishes_from_def by auto
  have <p  $\neq$  q> using case_assms unfolding hml_srbj_conj.distinguishes_def by auto
  have p_reach_nonempty:
    <silent_reachable_set {p}  $\neq$  {}>
    <silent_reachable_set {p}  $\rightarrow$ S silent_reachable_set {p}>
    unfolding silent_reachable_set_def
    using silent_reachable.intros(1) silent_reachable_trans by auto
  hence <spectro_att_wins (expr_pr_inner  $\chi$ )
    (Attacker_Delayed q' (silent_reachable_set {p}))>
    using distinction Neg by blast
  from q'_spec(1) this have
    <spectro_att_wins (expr_pr_inner  $\chi$ ) (Attacker_Delayed q (silent_reachable_set {p}))>
    by (induct, auto,
      metis weak_spectroscopy_game.attacker_wins_Ga_with_id_step procrastination
        option.distinct(1) option.sel spectroscopy_defender.simps(4))
  moreover have <spectroscopy_moves (Attacker_Conjunct p q)
    (Attacker_Delayed q (silent_reachable_set {p}))
    = Some ( $\lambda e$ . Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7)>
    using p_reach_nonempty sreachable_set_is_sreachable <p  $\neq$  q> by fastforce
  moreover have <the (min1_7 (expr_pr_conjunct (Neg  $\chi$ ) - E 0 0 0 0 0 0 1))
     $\geq$  (expr_pr_inner  $\chi$ )>
    using min1_7_def energy_leq_cases
    by (simp add: modal_depth_dominates_neg_conjuncts)
  moreover from this have
    < $\exists e'$ . Some e' = ( $\lambda e$ . Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7)
      (expr_pr_conjunct (Neg  $\chi$ ))  $\wedge$  e'  $\geq$  (expr_pr_inner  $\chi$ )>

```

```

    unfolding min_1_7_subtr_simp by auto
    ultimately show <spectro_att_wins (expr_pr_conjunct (Neg  $\chi$ )) (Attacker_Conjunct p q)>
    using weak_spectroscopy_game.attacker_wins.Attack
    weak_spectroscopy_game.win_a_upwards_closure spectroscopy_defender.simps(3)
    by (metis (no_types, lifting) option.discI option.sel)
  qed
qed
qed
thus ?thesis
  by (metis assms distinction_implies_winning_budgets_empty_Q)
qed

end

end

```

9.2 Strategy Formulas

```

theory Strategy_Formulas
  imports Spectroscopy_Game Expressiveness_Price
begin

```

Strategy formulas express attacker strategies in HML. They bridge between HML formulas, the spectroscopy game and winning budgets. We show that, if some energy e suffices for the attacker to win, there exists a strategy formula with expressiveness price $\leq e$. We also prove that this formula actually distinguishes the processes of the attacker position.

```

context lts_tau
begin

inductive
  strategy_formula
  :: <('s, 'a) spectroscopy_position  $\Rightarrow$  energy  $\Rightarrow$  ('a, 's) hml_srbbs  $\Rightarrow$  bool>
and
  strategy_formula_inner
  :: <('s, 'a) spectroscopy_position  $\Rightarrow$  energy  $\Rightarrow$  ('a, 's) hml_srbbs_inner  $\Rightarrow$  bool>
and
  strategy_formula_conjunct
  :: <('s, 'a) spectroscopy_position  $\Rightarrow$  energy  $\Rightarrow$  ('a, 's) hml_srbbs_conjunct  $\Rightarrow$  bool>
where
  delay: <strategy_formula (Attacker_Immediate p Q) e (Internal  $\chi$ )>
    if < $\exists Q'$ .
      spectroscopy_moves (Attacker_Immediate p Q) (Attacker_Delayed p Q') = id_up
       $\wedge$  spectro_att_wins e (Attacker_Delayed p Q')
       $\wedge$  strategy_formula_inner (Attacker_Delayed p Q') e  $\chi$ >
  |
  procrastination: <strategy_formula_inner (Attacker_Delayed p Q) e  $\chi$ >
    if < $\exists p'$ .
      spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Delayed p' Q) = id_up
       $\wedge$  spectro_att_wins e (Attacker_Delayed p' Q)
       $\wedge$  strategy_formula_inner (Attacker_Delayed p' Q) e  $\chi$ >
  |
  observation: <strategy_formula_inner (Attacker_Delayed p Q) e (Obs  $\alpha$   $\varphi$ )>
    if < $\exists p' Q'$ . spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Immediate p' Q')
      = (subtract 1 0 0 0 0 0 0 0)
       $\wedge$  spectro_att_wins (e - E 1 0 0 0 0 0 0) (Attacker_Immediate p' Q')
       $\wedge$  strategy_formula (Attacker_Immediate p' Q') (e - E 1 0 0 0 0 0 0)  $\varphi$ 
       $\wedge$  p  $\mapsto$  a  $\alpha$  p'  $\wedge$  Q  $\mapsto$  a S  $\alpha$  Q'>
  |
  early_conj: <strategy_formula (Attacker_Immediate p Q) e  $\varphi$ >
    if < $\exists p'$ . spectroscopy_moves (Attacker_Immediate p Q) (Defender_Conj p' Q')

```

```

      = (subtract 0 0 0 0 1 0 0 0)
      ∧ spectro_att_wins (e - E 0 0 0 0 1 0 0 0) (Defender_Conj p' Q')
      ∧ strategy_formula (Defender_Conj p' Q') (e - E 0 0 0 0 1 0 0 0) φ>
|
late_conj: <strategy_formula_inner (Attacker_Delayed p Q) e χ>
  if <(spectroscopy_moves (Attacker_Delayed p Q) (Defender_Conj p Q)
    = id_up ∧ (spectro_att_wins e (Defender_Conj p Q))
    ∧ strategy_formula_inner (Defender_Conj p Q) e χ)>
|
conj: <strategy_formula_inner (Defender_Conj p Q) e (Conj Q Φ)>
  if <∀q ∈ Q. spectroscopy_moves (Defender_Conj p Q) (Attacker_Conjunct p q)
    = (subtract 0 0 1 0 0 0 0 0)
    ∧ (spectro_att_wins (e - (E 0 0 1 0 0 0 0 0)) (Attacker_Conjunct p q))
    ∧ strategy_formula_conjunct (Attacker_Conjunct p q) (e - E 0 0 1 0 0 0 0 0) (Φ q)>
|
imm_conj: <strategy_formula (Defender_Conj p Q) e (ImmConj Q Φ)>
  if <∀q ∈ Q. spectroscopy_moves (Defender_Conj p Q) (Attacker_Conjunct p q)
    = (subtract 0 0 1 0 0 0 0 0)
    ∧ (spectro_att_wins (e - (E 0 0 1 0 0 0 0 0)) (Attacker_Conjunct p q))
    ∧ strategy_formula_conjunct (Attacker_Conjunct p q) (e - E 0 0 1 0 0 0 0 0) (Φ q)>
|
pos: <strategy_formula_conjunct (Attacker_Conjunct p q) e (Pos χ)>
  if <(∃Q'. spectroscopy_moves (Attacker_Conjunct p q) (Attacker_Delayed p Q')
    = Some min1_6 ∧ spectro_att_wins (the (min1_6 e)) (Attacker_Delayed p Q')
    ∧ strategy_formula_inner (Attacker_Delayed p Q') (the (min1_6 e)) χ)>
|
neg: <strategy_formula_conjunct (Attacker_Conjunct p q) e (Neg χ)>
  if <∃P'. (spectroscopy_moves (Attacker_Conjunct p q) (Attacker_Delayed q P')
    = Some (λe. Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7)
    ∧ spectro_att_wins (the (min1_7 (e - E 0 0 0 0 0 0 0 1))) (Attacker_Delayed q P'))
    ∧ strategy_formula_inner (Attacker_Delayed q P')
      (the (min1_7 (e - E 0 0 0 0 0 0 0 1))) χ>
|
stable: <strategy_formula_inner (Attacker_Delayed p Q) e χ>
  if <(∃Q'. spectroscopy_moves (Attacker_Delayed p Q) (Defender_Stable_Conj p Q')
    = id_up ∧ spectro_att_wins e (Defender_Stable_Conj p Q')
    ∧ strategy_formula_inner (Defender_Stable_Conj p Q') e χ)>
|
stable_conj: <strategy_formula_inner (Defender_Stable_Conj p Q) e (StableConj Q Φ)>
  if <∀q ∈ Q. spectroscopy_moves (Defender_Stable_Conj p Q) (Attacker_Conjunct p q)
    = (subtract 0 0 0 1 0 0 0 0)
    ∧ spectro_att_wins (e - (E 0 0 0 1 0 0 0 0)) (Attacker_Conjunct p q)
    ∧ strategy_formula_conjunct (Attacker_Conjunct p q) (e - E 0 0 0 1 0 0 0 0) (Φ q)>
|
branch: <strategy_formula_inner (Attacker_Delayed p Q) e χ>
  if <∃p' Q' α Qα. spectroscopy_moves (Attacker_Delayed p Q)
    (Defender_Branch p α p' Q' Qα) = id_up
    ∧ spectro_att_wins e (Defender_Branch p α p' Q' Qα)
    ∧ strategy_formula_inner (Defender_Branch p α p' Q' Qα) e χ>
|
branch_conj:
  <strategy_formula_inner (Defender_Branch p α p' Q Qα) e (BranchConj α φ Q Φ)>
  if <∃Q'. spectroscopy_moves (Defender_Branch p α p' Q Qα) (Attacker_Branch p' Q')
    = Some (λe. Option.bind ((subtract_fn 0 1 1 0 0 0 0 0) e) min1_6)
    ∧ spectroscopy_moves (Attacker_Branch p' Q') (Attacker_Immediate p' Q')
    = subtract 1 0 0 0 0 0 0 0
    ∧ (spectro_att_wins (the (min1_6 (e - E 0 1 1 0 0 0 0 0)) - E 1 0 0 0 0 0 0 0)
      (Attacker_Immediate p' Q'))
    ∧ strategy_formula (Attacker_Immediate p' Q')
      (the (min1_6 (e - E 0 1 1 0 0 0 0 0)) - E 1 0 0 0 0 0 0 0) φ>
  <∀q ∈ Q. spectroscopy_moves (Defender_Branch p α p' Q Qα) (Attacker_Conjunct p q)

```

```

    = (subtract 0 1 1 0 0 0 0 0)
    ∧ spectro_att_wins (e - (E 0 1 1 0 0 0 0 0)) (Attacker_Conjunct p q)
    ∧ strategy_formula_conjunct (Attacker_Conjunct p q) (e - E 0 1 1 0 0 0 0 0) (Φ q)⟩

lemma winning_budget_implies_strategy_formula:
  assumes
    <spectro_att_wins e g>
  shows
    <case g of
      Attacker_Immediate p Q ⇒ ∃φ. strategy_formula g e φ ∧ expressiveness_price φ ≤ e
    | Attacker_Delayed p Q ⇒ ∃χ. strategy_formula_inner g e χ ∧ expr_pr_inner χ ≤ e
    | Attacker_Conjunct p q ⇒
      ∃ψ. strategy_formula_conjunct g e ψ ∧ expr_pr_conjunct ψ ≤ e
    | Defender_Conj p Q ⇒ ∃χ. strategy_formula_inner g e χ ∧ expr_pr_inner χ ≤ e
    | Defender_Stable_Conj p Q ⇒ ∃χ. strategy_formula_inner g e χ ∧ expr_pr_inner χ ≤ e
    | Defender_Branch p α p' Q Qa ⇒
      ∃χ. strategy_formula_inner g e χ ∧ expr_pr_inner χ ≤ e
    | Attacker_Branch p Q ⇒
      ∃φ. strategy_formula (Attacker_Immediate p Q) (e - E 1 0 0 0 0 0 0 0) φ
      ∧ expressiveness_price φ ≤ e - E 1 0 0 0 0 0 0 0>
  using assms
proof(induction rule: weak_spectroscopy_game.attacker_wins.induct)
  case (Attack g g' e e')
  then show ?case
  proof (induct g)
    case (Attacker_Immediate p Q)
    hence move: <
      (∃p Q. g' = Defender_Conj p Q) ⟶
      (∃φ. strategy_formula_inner g' (the (weak_spectroscopy_game.weight g g' e)) φ
        ∧ expr_pr_inner φ ≤ weak_spectroscopy_game.updated g g' e) ∧
      (∃p Q. g' = Attacker_Delayed p Q) ⟶
      (∃φ. strategy_formula_inner g' (the (weak_spectroscopy_game.weight g g' e)) φ
        ∧ expr_pr_inner φ ≤ weak_spectroscopy_game.updated g g' e)>
    using weak_spectroscopy_game.attacker_wins.cases
    by simp
  from move Attacker_Immediate have move_cases:
    <(∃p' Q'. g' = (Attacker_Delayed p' Q')) ∨ (∃ p' Q'. g' = (Defender_Conj p' Q'))>
  using spectroscopy_moves.simps
  by (smt (verit, del_insts) spectroscopy_defender.elims(2,3))
  show ?case using move_cases
  proof(rule disjE)
    assume <∃p' Q'. g' = Attacker_Delayed p' Q'>
    then obtain p' Q' where g'_att_del: <g' = Attacker_Delayed p' Q'> by blast
    have e_comp:
      <the (spectroscopy_moves (Attacker_Immediate p Q) (Attacker_Delayed p' Q')) e
        = Some e>
    by (smt (verit, ccfv_threshold) Spectroscopy_Game.lts_tau.delay g'_att_del
      Attacker_Immediate move option.exhaust_sel option.inject)
    have <p' = p>
      by (metis g'_att_del Attacker_Immediate(2) spectroscopy_moves.simps(1))
    moreover have <(spectro_att_wins e (Attacker_Delayed p Q'))>
      using <g' = Attacker_Delayed p' Q'> <p' = p> Attacker_Immediate
      weak_spectroscopy_game.win_a_upwards_closure e_comp
      by simp
    ultimately have <(∃χ.
      strategy_formula_inner g'
      (the (weak_spectroscopy_game.weight (Attacker_Immediate p Q) g' e)) χ ∧
      expr_pr_inner χ ≤ weak_spectroscopy_game.updated (Attacker_Immediate p Q) g' e)>
      using g'_att_del Attacker_Immediate by fastforce
    then obtain χ where
      <(strategy_formula_inner (Attacker_Delayed p Q') e χ ∧ expr_pr_inner χ ≤ e)>

```

```

    using <p' = p> e_comp g'_att_del by auto
  hence < $\exists Q'$ . spectroscopy_moves (Attacker_Immediate p Q) (Attacker_Delayed p Q') = id_up
     $\wedge$  (spectro_att_wins e (Attacker_Delayed p Q'))
     $\wedge$  strategy_formula_inner (Attacker_Delayed p Q') e  $\chi$ >
    using g'_att_del
    by (smt (verit) Spectroscopy_Game.lts_tau.delay
      <spectro_att_wins e (Attacker_Delayed p Q')> Attacker_Immediate)
  hence <strategy_formula (Attacker_Immediate p Q) e (Internal  $\chi$ )>
    using strategy_formula_strategy_formula_inner_strategy_formula_conjunct.delay by blast
  moreover have <expressiveness_price (Internal  $\chi$ )  $\leq$  e>
    using <(strategy_formula_inner (Attacker_Delayed p Q') e  $\chi$   $\wedge$  expr_pr_inner  $\chi \leq$  e)>
    by auto
  ultimately show ?case by auto
next
  assume < $\exists p' Q'$ . g' = Defender_Conj p' Q'>
  then obtain p' Q' where g'_def_conj: <g' = Defender_Conj p' Q'> by blast
  hence M: <spectroscopy_moves (Attacker_Immediate p Q) (Defender_Conj p' Q')
    = (subtract 0 0 0 0 1 0 0 0)>
    using local.f_or_early_conj Attacker_Immediate by presburger
  hence Qp': <Q  $\neq$  {}> <Q = Q'> <p = p'>
    using Attack.hyps(2) Attacker_Immediate g'_def_conj local.f_or_early_conj by metis+
  from M have M':
    <weak_spectroscopy_game.updated (Attacker_Immediate p Q) (Defender_Conj p' Q') e
      = e - (E 0 0 0 0 1 0 0 0)>
    using Attack.hyps(3) g'_def_conj Attacker_Immediate
    by (smt (verit) option.distinct(1) option.sel)
  hence M'': <(spectro_att_wins (e - (E 0 0 0 0 1 0 0 0)) (Defender_Conj p Q'))>
    using g'_def_conj Qp' Attacker_Immediate weak_spectroscopy_game.win_a_upwards_closure
    by force
  with g'_def_conj have IH_case: < $\exists \chi$ .
    strategy_formula_inner g'
      (weak_spectroscopy_game.updated (Attacker_Immediate p Q) g' e)  $\chi$ 
     $\wedge$  expr_pr_inner  $\chi \leq$  weak_spectroscopy_game.updated (Attacker_Immediate p Q) g' e>
    using Attacker_Immediate by auto
  hence < $\exists \chi$ . strategy_formula_inner (Defender_Conj p Q) (e - E 0 0 0 0 1 0 0 0)  $\chi$ 
     $\wedge$  expr_pr_inner  $\chi \leq$  (e - E 0 0 0 0 1 0 0 0)>
    using <spectro_att_wins (e - (E 0 0 0 0 1 0 0 0)) (Defender_Conj p Q')> IH_case
    Qp' M' g'_def_conj by auto
  then obtain  $\chi$  where S:
    <strategy_formula_inner (Defender_Conj p Q) (e - E 0 0 0 0 1 0 0 0)  $\chi$ 
     $\wedge$  expr_pr_inner  $\chi \leq$  e - E 0 0 0 0 1 0 0 0>
    by blast
  hence < $\exists \psi$ .  $\chi$  = Conj Q  $\psi$ >
    using strategy_formula_strategy_formula_inner_strategy_formula_conjunct.conj
    g'_def_conj Attacker_Immediate
    unfolding Qp'
    by (smt (verit) spectroscopy_moves.simps(64,70) spectroscopy_position.distinct(17)
      spectroscopy_position.inject(5) strategy_formula_inner.cases)
  then obtain  $\psi$  where < $\chi$  = Conj Q  $\psi$ > by auto
  hence <strategy_formula (Defender_Conj p Q) (e - (E 0 0 0 0 1 0 0 0)) (ImmConj Q  $\psi$ )>
    using S strategy_formula_strategy_formula_inner_strategy_formula_conjunct.conj
    strategy_formula_strategy_formula_inner_strategy_formula_conjunct.imm_conj
    Qp' Attacker_Immediate unfolding g'_def_conj
    by (smt (verit) lts_tau.spectroscopy_moves.simps(70) hml_srbb_inner.inject(2)
      spectroscopy_position.distinct(17,37) strategy_formula_inner.cases)
  hence SI: <strategy_formula (Attacker_Immediate p Q) e (ImmConj Q  $\psi$ )>
    using delay early_conj Qp'
    by (metis (no_types, lifting) M'' local.f_or_early_conj)
  have <expr_pr_inner (Conj Q  $\psi$ )  $\leq$  (e - (E 0 0 0 0 1 0 0 0))>
    using S < $\chi$  = Conj Q  $\psi$ > by simp
  hence <expressiveness_price (ImmConj Q  $\psi$ )  $\leq$  e> using expr_imm_conj Qp'

```

```

    by (smt (verit) M g'_def_conj Attacker_Immediate option.sel option.simps(3))
  thus ?thesis using SI by auto
qed
next
case (Attacker_Branch p Q)
hence g'_def: <g' = Attacker_Immediate p Q> using br_acct
  by (induct g', auto) (metis option.discI)+
hence move:
  <spectroscopy_moves (Attacker_Branch p Q) g' = subtract 1 0 0 0 0 0 0 0> by simp
then obtain  $\varphi$  where
  <strategy_formula g' (weak_spectroscopy_game.updated (Attacker_Branch p Q) g' e)  $\varphi$   $\wedge$ 
    expressiveness_price  $\varphi \leq$  weak_spectroscopy_game.updated (Attacker_Branch p Q) g' e>
  using Attacker_Branch g'_def by auto
hence <(strategy_formula (Attacker_Immediate p Q) (e - E 1 0 0 0 0 0 0 0)  $\varphi$ )
   $\wedge$  expressiveness_price  $\varphi \leq$  e - E 1 0 0 0 0 0 0 0>
  using move Attacker_Branch unfolding g'_def
  by (smt (verit, del_insts) option.distinct(1) option.sel)
then show ?case by auto
next
case (Attacker_Conjunct p q)
hence <( $\exists p' Q'. g' =$  (Attacker_Delayed p' Q'))>
  using Attack.hyps spectroscopy_moves.simps
  by (smt (verit, del_insts) spectroscopy_defender.elims(1))
then obtain p' Q' where
  g'_att_del: <g' = Attacker_Delayed p' Q'> by blast
show ?case
proof(cases <p = p'>)
  case True
  hence <{q}  $\rightarrow$ S Q'>
    using g'_att_del local.pos_neg_clause Attacker_Conjunct by presburger
  hence post_win:
    <(the (spectroscopy_moves (Attacker_Conjunct p q) g') e) = min1_6 e>
    <(spectro_att_wins (the (min1_6 e)) (Attacker_Delayed p Q'))>
    using <{q}  $\rightarrow$ S Q'> Attacker_Conjunct weak_spectroscopy_game.win_a_upwards_closure
    unfolding True g'_att_del
    by auto
  then obtain  $\chi$  where  $\chi_{\text{spec}}$ :
    <strategy_formula_inner (Attacker_Delayed p Q') (the (min1_6 e))  $\chi$ >
    <expr_pr_inner  $\chi \leq$  the (min1_6 e)>
    using Attacker_Conjunct Attack True post_win unfolding g'_att_del
    by (smt (verit) option.sel spectroscopy_position.simps(51))
  hence
    <spectroscopy_moves (Attacker_Conjunct p q) (Attacker_Delayed p Q') = Some min1_6>
    <spectro_att_wins (the (min1_6 e)) (Attacker_Delayed p Q'))>
    <strategy_formula_inner (Attacker_Delayed p Q') (the (min1_6 e))  $\chi$ >
    using <{q}  $\rightarrow$ S Q'> local.pos_neg_clause post_win by auto
  hence <strategy_formula_conjunct (Attacker_Conjunct p q) e (Pos  $\chi$ )>
    using strategy_formula_strategy_formula_inner_strategy_formula_conjunct.delay pos
    by blast
  thus ?thesis
    using  $\chi_{\text{spec}}$  expr_pos by fastforce
next
case False
hence Qp': <{p}  $\rightarrow$ S Q'> <p' = q>
  using local.pos_neg_clause Attacker_Conjunct unfolding g'_att_del
  by presburger+
hence move: <spectroscopy_moves (Attacker_Conjunct p q) (Attacker_Delayed p' Q')
  = Some ( $\lambda e$ . Option.bind ((subtract_fn 0 0 0 0 0 0 0 1) e) min1_7)>
  using False by auto
hence win:
  <spectro_att_wins (the (min1_7 (e - E 0 0 0 0 0 0 1))) (Attacker_Delayed p' Q'))>

```

```

    using Attacker_Conjunct unfolding g'_att_del
  by (smt (verit) bind.bind_lunit bind.bind_lzero option.distinct(1) option.sel)
hence < $\exists \varphi$ . strategy_formula_inner (Attacker_Delayed p' Q')
      (the (min1_7 (e - E 0 0 0 0 0 0 1)))  $\varphi$ 
  & expr_pr_inner  $\varphi \leq$  the (min1_7 (e - E 0 0 0 0 0 0 1))>
  using Attack Attacker_Conjunct move unfolding g'_att_del
  by (smt (verit, del_insts) bind.bind_lunit bind.eq_None_conv option.discI
      option.sel spectroscopy_position.simps(51))
then obtain  $\chi$  where  $\chi_{\text{spec}}$ :
  <strategy_formula_inner (Attacker_Delayed p' Q')
    (the (min1_7 (e - E 0 0 0 0 0 0 1)))  $\chi$ >
  <expr_pr_inner  $\chi \leq$  the (min1_7 (e - E 0 0 0 0 0 0 1))>
  by blast
hence <strategy_formula_conjunct (Attacker_Conjunct p q) e (Neg  $\chi$ )>
  using strategy_formula_strategy_formula_inner_strategy_formula_conjunct.delay
  neg Qp' win move by blast
thus ?thesis
  using  $\chi_{\text{spec}}$  Attacker_Conjunct expr_neg move
  unfolding g'_att_del
  by (smt (verit, best) bind.bind_lunit bind.eq_None_conv option.distinct(1)
      option.sel spectroscopy_position.simps(52))
qed
next
case (Attacker_Delayed p Q)
then consider
  (Att_Del) < $\exists p$  Q.  $g' = \text{Attacker\_Delayed } p \ Q$ > |
  (Att_Imm) < $\exists p' \ Q'.$   $g' = \text{Attacker\_Immediate } p' \ Q'$ > |
  (Def_Conj) < $\exists p \ Q.$   $g' = \text{Defender\_Conj } p \ Q$ > |
  (Def_St_Conj) < $\exists p \ Q.$   $g' = \text{Defender\_Stable\_Conj } p \ Q$ > |
  (Def_Branch) < $\exists p' \ \alpha \ p'' \ Q' \ Q\alpha.$   $g' = \text{Defender\_Branch } p' \ \alpha \ p'' \ Q' \ Q\alpha$ >
  by (cases g', auto)
then show ?case
proof (cases)
case Att_Del
  then obtain p' Q' where
    g'_att_del: < $g' = \text{Attacker\_Delayed } p' \ Q'$ > by blast
  have Qp': < $Q' = Q$ > < $p \neq p'$ > < $p \mapsto \tau \ p'$ >
    using Attacker_Delayed g'_att_del Spectroscopy_Game.lts_tau.procrastination
    by metis+
  hence e_comp: <(the (spectroscopy_moves (Attacker_Delayed p Q)  $g'$ ) e) = Some e>
    using g'_att_del
    by simp
  hence att_win: <(spectro_att_wins e (Attacker_Delayed p' Q'))>
    using g'_att_del Qp' Attacker_Delayed weak_spectroscopy_game.attacker_wins.Defense e_comp
    by (metis option.sel)
  have <(weak_spectroscopy_game.updated (Attacker_Delayed p Q)  $g'$  e) = e>
    using g'_att_del Attacker_Delayed e_comp by fastforce
  then obtain  $\chi$  where  $\chi_{\text{spec}}$ :
    <strategy_formula_inner (Attacker_Delayed p' Q') e  $\chi \wedge \text{expr\_pr\_inner } \chi \leq e$ >
    using Attacker_Delayed g'_att_del by auto
  hence < $\exists p'.$  spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Delayed p' Q) = id_up
    & spectro_att_wins e (Attacker_Delayed p' Q)
    & strategy_formula_inner (Attacker_Delayed p' Q) e  $\chi$ >
    using e_comp g'_att_del Qp' local.procrastination Attack.hyps att_win
    Spectroscopy_Game.lts_tau.procrastination
    by metis
  hence <strategy_formula_inner (Attacker_Delayed p Q) e  $\chi$ >
    using procrastination by blast
  moreover have <expr_pr_inner  $\chi \leq e$ >
    using  $\chi_{\text{spec}}$  by blast
  ultimately show ?thesis by auto

```

```

next
  case Att_Imm
  then obtain p' Q' where
    g'_att_imm: <g' = Attacker_Immediate p' Q'> by blast
  hence move: <spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Immediate p' Q') ≠ None>
    using Attacker_Delayed by blast
  hence <∃ a. p → a a p' ∧ Q → aS a Q'> unfolding spectroscopy_moves.simps(3) by presburger
  then obtain α where α_prop: <p → a α p'> <Q → aS α Q'> by blast
  moreover then have weight:
    <spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Immediate p' Q')
      = subtract 1 0 0 0 0 0 0 0>
    by (simp, metis)
  moreover then have update:
    <weak_spectroscopy_game.updated (Attacker_Delayed p Q) g' e
      = e - (E 1 0 0 0 0 0 0 0)>
    using g'_att_imm Attacker_Delayed
    by (smt (verit, del_insts) option.distinct(1) option.sel)
  moreover then obtain χ where χ_prop:
    <strategy_formula (Attacker_Immediate p' Q') (e - E 1 0 0 0 0 0 0 0) χ>
    <expressiveness_price χ ≤ e - E 1 0 0 0 0 0 0 0>
    using Attacker_Delayed g'_att_imm
    by auto
  moreover have <spectro_att_wins (e - (E 1 0 0 0 0 0 0 0)) (Attacker_Immediate p' Q')>
    using weak_spectroscopy_game.attacker_wins.Attack Attack.hyps(4)
    Attacker_Delayed.premis(3) calculation(4) g'_att_imm
    by force
  ultimately have <strategy_formula_inner (Attacker_Delayed p Q) e (Obs α χ)>
    using local.observation[of p Q e χ α] by blast
  moreover have <expr_pr_inner (Obs α χ) ≤ e>
    using expr_obs χ_prop Attacker_Delayed g'_att_imm weight update
    by (smt (verit) option.sel)
  ultimately show ?thesis by auto
next
  case Def_Conj
  then obtain p' Q' where
    g'_def_conj: <g' = Defender_Conj p' Q'> by blast
  hence <p = p'> <Q = Q'>
    using local.late_inst_conj Attacker_Delayed by presburger+
  hence
    <the (spectroscopy_moves (Attacker_Delayed p Q) (Defender_Conj p' Q')) e = Some e>
    by fastforce
  hence
    <spectro_att_wins e (Defender_Conj p' Q')>
    <weak_spectroscopy_game.updated g g' e = e>
    using Attacker_Delayed Attack unfolding g'_def_conj by simp+
  then obtain χ where
    χ_prop: <strategy_formula_inner (Defender_Conj p' Q') e χ ∧ expr_pr_inner χ ≤ e>
    using Attack g'_def_conj by auto
  hence
    <spectroscopy_moves (Attacker_Delayed p Q) (Defender_Conj p' Q') = id_up
      ∧ spectro_att_wins e (Defender_Conj p' Q')
      ∧ strategy_formula_inner (Defender_Conj p' Q') e χ>
    by (simp add: <Q = Q'> <spectro_att_wins e (Defender_Conj p' Q')> <p = p'>)
  then show ?thesis
    using χ_prop <Q = Q'> <spectro_att_wins e (Defender_Conj p' Q')> <p = p'> late_conj
    by fastforce
next
  case Def_St_Conj
  then obtain p' Q' where g'_def: <g' = Defender_Stable_Conj p' Q'> by blast
  hence pQ': <p = p'> <Q' = { q ∈ Q. (∄ q'. q → τ q')}> <∄ p''. p → τ p''>
    using local.late_stbl_conj Attacker_Delayed

```

```

    by meson+
  hence <the (spectroscopy_moves (Attacker_Delayed p Q) (Defender_Stable_Conj p' Q')) e
    = Some e>
    by auto
  hence <spectro_att_wins e (Defender_Stable_Conj p' Q')>
    <weak_spectroscopy_game.updated g g' e = e>
    using Attacker_Delayed Attack unfolding g'_def by force+
  then obtain  $\chi$  where  $\chi_{\text{prop}}$ :
    <strategy_formula_inner (Defender_Stable_Conj p' Q') e  $\chi$ > <expr_pr_inner  $\chi \leq e$ >
    using Attack g'_def by auto
  have <spectroscopy_moves (Attacker_Delayed p Q) (Defender_Stable_Conj p' Q') = id_up
     $\wedge$  spectro_att_wins e (Defender_Stable_Conj p' Q')
     $\wedge$  strategy_formula_inner (Defender_Stable_Conj p' Q') e  $\chi$ >
    using Attack  $\chi_{\text{prop}}$  <spectro_att_wins e (Defender_Stable_Conj p' Q')> late_stbl_conj
    pQ' g'_def
    by force
  thus ?thesis using local.stable[of p Q e  $\chi$ ] pQ'  $\chi_{\text{prop}}$  by fastforce
next
case Def_Branch
then obtain p'  $\alpha$  p'' Q' Q $\alpha$  where
  g'_def_br: <g' = Defender_Branch p'  $\alpha$  p'' Q' Q $\alpha$ > by blast
hence pQ': <p = p'> <Q' = Q - Q $\alpha$ > <p  $\mapsto$  a  $\alpha$  p''> <Q $\alpha \subseteq Q$ >
  using br_conj Attacker_Delayed by metis+
hence
  <the (spectroscopy_moves (Attacker_Delayed p Q) (Defender_Branch p'  $\alpha$  p'' Q' Q $\alpha$ )) e
    = Some e>
    by auto
  hence post:
    <spectro_att_wins e (Defender_Branch p'  $\alpha$  p'' Q' Q $\alpha$ )>
    <weak_spectroscopy_game.updated g g' e = e>
    using Attack option.inject Attacker_Delayed unfolding g'_def_br by auto
  then obtain  $\chi$  where  $\chi_{\text{prop}}$ :
    <strategy_formula_inner (Defender_Branch p'  $\alpha$  p'' Q' Q $\alpha$ ) e  $\chi$ >
    <expr_pr_inner  $\chi \leq e$ >
    using g'_def_br Attack Attacker_Delayed
    by auto
  hence <spectroscopy_moves (Attacker_Delayed p Q) (Defender_Branch p'  $\alpha$  p'' Q' Q $\alpha$ ) = id_up
     $\wedge$  spectro_att_wins e (Defender_Branch p'  $\alpha$  p'' Q' Q $\alpha$ )
     $\wedge$  strategy_formula_inner (Defender_Branch p'  $\alpha$  p'' Q' Q $\alpha$ ) e  $\chi$ >
    using g'_def_br local.branch Attack post pQ' by simp
  hence <strategy_formula_inner (Attacker_Delayed p Q) e  $\chi$ >
    using Attack Attacker_Delayed local.br_conj branch
    unfolding g'_def_br by fastforce
  thus ?thesis using  $\chi_{\text{prop}}$ 
    by fastforce
qed
qed force+
next
case (Defense g e)
thus ?case
proof (induct g)
  case (Defender_Branch p  $\alpha$  p' Q Q $\alpha$ )
  hence conjs:
    < $\forall q \in Q$ . spectroscopy_moves (Defender_Branch p  $\alpha$  p' Q Q $\alpha$ ) (Attacker_Conjunct p q)
      = subtract 0 1 1 0 0 0 0 0>
    by simp
  obtain e' where e'_spec:
    < $\forall q \in Q$ . weak_spectroscopy_game.weight (Defender_Branch p  $\alpha$  p' Q Q $\alpha$ )
      (Attacker_Conjunct p q) e = Some e'
       $\wedge$  spectro_att_wins e' (Attacker_Conjunct p q)
       $\wedge$  ( $\exists \psi$ . strategy_formula_conjunct (Attacker_Conjunct p q) e'  $\psi$ )

```

```

     $\wedge \text{expr\_pr\_conjunct } \psi \leq e' \rangle$ 
  using conjs Defender_Branch option.distinct(1) option.sel
  by (smt (z3) spectroscopy_position.simps(52))
hence e'_def:  $\langle Q \neq \{\} \implies e' = e - E \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \rangle$  using conjs
  by (smt (verit) all_not_in_conv option.distinct(1) option.sel)
then obtain  $\Phi$  where  $\Phi_{\text{spec}}$ :
   $\langle \forall q \in Q. \text{strategy\_formula\_conjunct } (\text{Attacker\_Conjunct } p \ q) \ e' \ (\Phi \ q) \wedge \text{expr\_pr\_conjunct } (\Phi \ q) \leq e' \rangle$ 
  using e'_spec by metis
have obs:  $\langle \text{spectroscopy\_moves } (\text{Defender\_Branch } p \ \alpha \ p' \ Q \ Qa) \ (\text{Attacker\_Branch } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ = \ \text{Some } (\lambda e. \text{Option.bind } ((\text{subtract\_fn } 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0) \ e) \ \text{min1\_6}) \rangle$ 
  by (simp add: soft_step_set_is_soft_step_set)
have  $\langle \forall p \ Q. \text{Attacker\_Branch } p' \ (\text{soft\_step\_set } Qa \ \alpha) = \text{Attacker\_Branch } p \ Q \implies p = p' \wedge Q = \text{soft\_step\_set } Qa \ \alpha \rangle$  by blast
with option.discI[OF obs] obtain e'' where
   $\langle \exists \varphi. \text{strategy\_formula } (\text{Attacker\_Immediate } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ (e'' - E \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0) \ \varphi \wedge \text{expressiveness\_price } \varphi \leq e'' - E \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \rangle$ 
  using Defense.IH option.distinct(1) option.sel
  by (smt (verit, best) Defender_Branch.prem(2) spectroscopy_position.simps(53))
then obtain  $\varphi$  where
   $\langle \text{strategy\_formula } (\text{Attacker\_Immediate } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ (\text{weak\_spectroscopy\_game.updated } (\text{Defender\_Branch } p \ \alpha \ p' \ Q \ Qa) \ (\text{Attacker\_Branch } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ e - E \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0) \ \varphi \rangle$ 
   $\langle \text{expressiveness\_price } \varphi \leq \text{weak\_spectroscopy\_game.updated } (\text{Defender\_Branch } p \ \alpha \ p' \ Q \ Qa) \ (\text{Attacker\_Branch } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ e - E \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \rangle$ 
  using Defender_Branch.prem(2) option.discI[OF obs]
  by (smt (verit, best) option.sel spectroscopy_position.simps(53))
hence obs_strat:
   $\langle \text{strategy\_formula } (\text{Attacker\_Immediate } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ (\text{the } (\text{min1\_6 } (e - E \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0)) - E \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0) \ \varphi \rangle$ 
   $\langle \text{expressiveness\_price } \varphi \leq (\text{the } (\text{min1\_6 } (e - E \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0)) - E \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0) \rangle$ 
  by (smt (verit, best) Defender_Branch.prem(2) bind.bind_lunit bind.bind_lzero obs option.distinct(1) option.sel)+
have  $\langle \text{spectroscopy\_moves } (\text{Attacker\_Branch } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ (\text{Attacker\_Immediate } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ = \ (\text{subtract } 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0) \rangle$  by simp
obtain e'' where win_branch:
   $\langle \text{Some } e'' = \text{min1\_6 } (e - E \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0) \rangle$ 
   $\langle \text{spectro\_att\_wins } e'' \ (\text{Attacker\_Branch } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \rangle$ 
  using Defender_Branch
  by (smt (verit, ccfv_threshold) bind.bind_lunit bind.eq_None_conv obs option.discI option.sel)
then obtain g'' where g''_spec:
   $\langle \text{spectroscopy\_moves } (\text{Attacker\_Branch } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ g'' \neq \text{None} \rangle$ 
   $\langle \text{spectro\_att\_wins } (\text{weak\_spectroscopy\_game.updated } (\text{Attacker\_Branch } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ g'' \ (\text{the } (\text{min1\_6 } (e - E \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0)))) \ g'' \rangle$ 
  using weak_spectroscopy_game.attacker_wins.cases
  by (metis spectroscopy_defender.simps(2) option.sel)
hence move_immediate:
   $\langle g'' = (\text{Attacker\_Immediate } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \wedge \text{spectroscopy\_moves } (\text{Attacker\_Branch } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \ (\text{Attacker\_Immediate } p' \ (\text{soft\_step\_set } Qa \ \alpha)) = \text{subtract } 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \rangle$ 
  using br_acct
  by (cases g'', auto) (metis option.discI)+
then obtain e''' where win_immediate:
   $\langle \text{Some } e''' = \text{subtract\_fn } 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ e''' \rangle$ 
   $\langle \text{spectro\_att\_wins } e''' \ (\text{Attacker\_Immediate } p' \ (\text{soft\_step\_set } Qa \ \alpha)) \rangle$ 

```

```

using g''_spec win_branch option.distinct(1) option.sel spectroscopy_defender.elims(1)
spectroscopy_defender.simps(2)
weak_spectroscopy_game.attacker_wins.cases[0F win_branch(2)]
by (smt (verit, del_insts) local.br_acct spectroscopy_moves.simps(23,53,57,61,66,72))
hence strat:
  <strategy_formula_inner (Defender_Branch p  $\alpha$  p' Q Qa) e (BranchConj  $\alpha$   $\varphi$  Q  $\Phi$ )>
using branch_conj obs move_immediate obs_strat  $\Phi$ _spec conjs e'_def e'_spec
by (smt (verit, best) option.distinct(1) option.sel win_branch(1))
have <E 1 0 0 0 0 0 0 0  $\leq$  e''> using win_branch g''_spec
by (metis option.distinct(1) win_immediate(1))
hence above_one: <0 < min (modal_depth e) (pos_conjuncts e)>
using win_immediate win_branch
by (metis energy.sel(1) energy.sel(6) gr_zeroI idiff_0_right leq_components
min_1_6_simps(1) minus_energy_def not_one_le_zero option.sel)
have < $\forall q \in Q. \text{expr\_pr\_conjunct } (\Phi q) \leq (e - (E 0 1 1 0 0 0 0 0))$ >
using  $\Phi$ _spec e'_def by blast
moreover have <expressiveness_price  $\varphi$ 
 $\leq$  the (min1_6 (e - E 0 1 1 0 0 0 0 0)) - E 1 0 0 0 0 0 0 0>
using obs_strat(2) by blast
moreover hence <modal_depth_srb  $\varphi \leq$  min (modal_depth e) (pos_conjuncts e) - 1>
by simp
hence <1 + modal_depth_srb  $\varphi \leq$  min (modal_depth e) (pos_conjuncts e)>
by (metis above_one add.right_neutral add_diff_cancel_enat
add_mono_thms_linordered_semiring(1) enat.simps(3) enat_defs(2) ileI1
le_iff_add plus_1_eSuc(1))
moreover hence <1 + modal_depth_srb  $\varphi \leq$  pos_conjuncts e> by simp
ultimately have <expr_pr_inner (BranchConj  $\alpha$   $\varphi$  Q  $\Phi$ )  $\leq$  e>
using expr_br_conj e'_def obs Defender_Branch(2) win_branch(1) win_immediate(1)
by (smt (verit, best) bind_eq_None_conv option.distinct(1) option.sel option.simps(3))
then show ?case using strat by force
next
case (Defender_Conj p Q)
hence moves:
  < $\forall g'. \text{spectroscopy\_moves } (\text{Defender\_Conj } p \ Q) \ g' \neq \text{None}$ 
 $\rightarrow (\exists e'. \text{weak\_spectroscopy\_game.weight } (\text{Defender\_Conj } p \ Q) \ g' \ e = \text{Some } e'$ 
 $\wedge \text{spectro\_att\_wins } e' \ g')$ 
 $\wedge (\exists q. g' = (\text{Attacker\_Conjunct } p \ q))$ >
using local.conj_answer
lts_tau.spectroscopy_defender.elims spectroscopy_moves.simps(30,33,34,47,58,62)
by (smt (verit, best))
show ?case
proof (cases <Q = {}>)
case True
then obtain  $\Phi$  where < $\forall q \in Q. \text{spectroscopy\_moves } (\text{Defender\_Conj } p \ Q) \ (\text{Attacker\_Conjunct } p \ q)$ 
 $= \text{subtract } 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0$ 
 $\wedge \text{spectro\_att\_wins } (e - (E 0 0 1 0 0 0 0 0)) \ (\text{Attacker\_Conjunct } p \ q)$ 
 $\wedge \text{strategy\_formula\_conjunct } (\text{Attacker\_Conjunct } p \ q) \ (e - E 0 0 1 0 0 0 0 0) \ (\Phi \ q)$ >
by (auto simp add: emptyE)
hence Strat: <strategy_formula_inner (Defender_Conj p Q) e (Conj {}  $\Phi$ )>
using <Q = {}> conj by blast
hence
  <modal_depth_srb_inner (Conj Q  $\Phi$ ) = Sup ((modal_depth_srb_inner conjunct  $\circ$   $\Phi$ ) ' Q)>
  <branch_conj_depth_inner (Conj Q  $\Phi$ ) = Sup ((branch_conj_depth_inner conjunct  $\circ$   $\Phi$ ) ' Q)>
  <inst_conj_depth_inner (Conj Q  $\Phi$ ) = 0>
  <st_conj_depth_inner (Conj Q  $\Phi$ ) = Sup ((st_conj_depth_inner conjunct  $\circ$   $\Phi$ ) ' Q)>
  <imm_conj_depth_inner (Conj Q  $\Phi$ ) = Sup ((imm_conj_depth_inner conjunct  $\circ$   $\Phi$ ) ' Q)>
  <max_pos_conj_depth_inner (Conj Q  $\Phi$ ) = Sup ((max_pos_conj_depth_inner conjunct  $\circ$   $\Phi$ ) ' Q)>
  <max_neg_conj_depth_inner (Conj Q  $\Phi$ ) = Sup ((max_neg_conj_depth_inner conjunct  $\circ$   $\Phi$ ) ' Q)>
  <neg_depth_inner (Conj Q  $\Phi$ ) = Sup ((neg_depth_inner conjunct  $\circ$   $\Phi$ ) ' Q)>
using <Q = {}> by auto

```

```

hence
  <modal_depth_srbb_inner (Conj Q  $\Phi$ ) = 0>
  <branch_conj_depth_inner (Conj Q  $\Phi$ ) = 0>
  <inst_conj_depth_inner (Conj Q  $\Phi$ ) = 0>
  <st_conj_depth_inner (Conj Q  $\Phi$ ) = 0>
  <imm_conj_depth_inner (Conj Q  $\Phi$ ) = 0>
  <max_pos_conj_depth_inner (Conj Q  $\Phi$ ) = 0>
  <max_neg_conj_depth_inner (Conj Q  $\Phi$ ) = 0>
  <neg_depth_inner (Conj Q  $\Phi$ ) = 0>
  using <Q = {}> by (simp add: bot_enat_def)+
hence <expr_pr_inner (Conj Q  $\Phi$ ) = (E 0 0 0 0 0 0 0 0)>
  using <Q = {}> by force
hence price: <expr_pr_inner (Conj Q  $\Phi$ )  $\leq$  e>
  by auto
with Strat price True show ?thesis by auto
next
case False
hence fa_q: < $\forall q \in Q. \exists e'.$ 
  Some  $e' = \text{subtract\_fn } 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ e$ 
   $\wedge \text{spectroscopy\_moves (Defender\_Conj } p \ Q) (\text{Attacker\_Conjunct } p \ q)$ 
     $= \text{subtract } 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0$ 
   $\wedge \text{spectro\_att\_wins } e' (\text{Attacker\_Conjunct } p \ q)$ >
  using moves local.conj_answer option.distinct(1)
  by (smt (z3) option.sel)
have q_ex_e': < $\forall q \in Q. \exists e'.$ 
  spectroscopy_moves (Defender_Conj p Q) (Attacker_Conjunct p q)
     $= \text{subtract } 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0$ 
   $\wedge \text{Some } e' = \text{subtract\_fn } 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ e$ 
   $\wedge \text{spectro\_att\_wins } e' (\text{Attacker\_Conjunct } p \ q)$ 
   $\wedge (\exists \varphi. \text{strategy\_formula\_conjunct (Attacker\_Conjunct } p \ q) \ e' \ \varphi$ 
     $\wedge \text{expr\_pr\_conjunct } \varphi \leq e')$ >
proof safe
fix q
assume <q  $\in$  Q>
then obtain e' where e'_spec:
  <Some  $e' = \text{subtract\_fn } 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ e$ 
  <spectroscopy_moves (Defender_Conj p Q) (Attacker_Conjunct p q)
     $= \text{subtract } 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0$ 
  <spectro_att_wins  $e' (\text{Attacker\_Conjunct } p \ q)$ >
  using fa_q by blast
hence <weak_spectroscopy_game.weight (Defender_Conj p Q) (Attacker_Conjunct p q) e
  = Some  $e'$ >
  by simp
then have < $\exists \psi. \text{strategy\_formula\_conjunct (Attacker\_Conjunct } p \ q) \ e' \ \psi$ 
   $\wedge \text{expr\_pr\_conjunct } \psi \leq e'$ >
  using Defender_Conj e'_spec
  by (smt (verit, best) option.distinct(1) option.sel spectroscopy_position.simps(52))
thus < $\exists e'. \text{spectroscopy\_moves (Defender\_Conj } p \ Q) (\text{Attacker\_Conjunct } p \ q)$ 
   $= \text{subtract } 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0$ 
   $\wedge \text{Some } e' = \text{subtract\_fn } 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ e$ 
   $\wedge \text{spectro\_att\_wins } e' (\text{Attacker\_Conjunct } p \ q)$ 
   $\wedge (\exists \varphi. \text{strategy\_formula\_conjunct (Attacker\_Conjunct } p \ q) \ e' \ \varphi$ 
     $\wedge \text{expr\_pr\_conjunct } \varphi \leq e')$ >
  using e'_spec by blast
qed
hence < $\exists \Phi. \forall q \in Q. \text{spectro\_att\_wins (e - E 0 0 1 0 0 0 0 0) (Attacker\_Conjunct } p \ q)$ 
   $\wedge (\text{strategy\_formula\_conjunct (Attacker\_Conjunct } p \ q) (e - E 0 0 1 0 0 0 0 0) (\Phi \ q)$ 
   $\wedge \text{expr\_pr\_conjunct } (\Phi \ q) \leq (e - E 0 0 1 0 0 0 0 0))$ >
  by (metis (no_types, opaque_lifting) option.distinct(1) option.inject)
then obtain  $\Phi$  where IH:

```

```

    <∀q ∈ Q. spectro_att_wins (e - E 0 0 1 0 0 0 0 0) (Attacker_Conjunct p q)
      ∧ (strategy_formula_conjunct (Attacker_Conjunct p q) (e - E 0 0 1 0 0 0 0 0) (Φ q)
        ∧ expr_pr_conjunct (Φ q) ≤ (e - E 0 0 1 0 0 0 0 0))> by auto
  hence <strategy_formula_inner (Defender_Conj p Q) e (Conj Q Φ)>
    by (simp add: conj)
  moreover have <expr_pr_inner (Conj Q Φ) ≤ e>
    using IH expr_conj <Q ≠ {}> q_ex_e'
    by (metis (no_types, lifting) equalsOI option.distinct(1))
  ultimately show ?thesis by auto
qed
next
case (Defender_Stable_Conj p Q)
hence cases:
  <∀g'. spectroscopy_moves (Defender_Stable_Conj p Q) g' ≠ None →
    (∃e'. weak_spectroscopy_game.weight (Defender_Stable_Conj p Q) g' e = Some e'
      ∧ spectro_att_wins e' g')
    ∧ ((∃p' q. g' = Attacker_Conjunct p' q) ∨ (∃p' Q'. g' = Defender_Conj p' Q'))>
  by (metis (no_types, opaque_lifting)
      spectroscopy_defender.elims(2,3) spectroscopy_moves.simps(35,36,37,38,74))
show ?case
proof(cases <Q = {}>)
  case True
  then obtain e' where e'_spec:
    <weak_spectroscopy_game.weight (Defender_Stable_Conj p Q) (Defender_Conj p Q) e
      = Some e'>
    <e' = e - (E 0 0 0 1 0 0 0 0)>
    <spectro_att_wins e' (Defender_Conj p Q)>
    using cases local.empty_stbl_conj_answer
    by (smt (verit, best) option.discI option.sel)
  then obtain Φ where Φ_prop: <strategy_formula_inner (Defender_Conj p Q) e' (Conj Q Φ)>
    using conj True by blast
  hence strategy: <strategy_formula_inner (Defender_Stable_Conj p Q) e (StableConj Q Φ)>
    by (simp add: True stable_conj)
  have <E 0 0 0 1 0 0 0 0 ≤ e> using e'_spec
    using option.sel True by fastforce
  moreover have <expr_pr_inner (StableConj Q Φ) = E 0 0 0 1 0 0 0 0>
    using True by (simp add: bot_enat_def)
  ultimately have <expr_pr_inner (StableConj Q Φ) ≤ e> by simp
  with strategy show ?thesis by auto
next
case False
  then obtain e' where e'_spec:
    <e' = e - (E 0 0 0 1 0 0 0 0)>
    <∀q ∈ Q. weak_spectroscopy_game.weight (Defender_Stable_Conj p Q)
      (Attacker_Conjunct p q) e = Some e'
      ∧ spectro_att_wins e' (Attacker_Conjunct p q)>
    using cases local.conj_s_answer
    by (smt (verit, del_insts) option.distinct(1) option.sel)
  hence IH: <∀q ∈ Q. ∃ψ.
    strategy_formula_conjunct (Attacker_Conjunct p q) e' ψ ∧
    expr_pr_conjunct ψ ≤ e'>
    using Defender_Stable_Conj local.conj_s_answer
    by (smt (verit, best) option.distinct(1) option.inject spectroscopy_position.simps(52))
  hence <∃Φ. ∀q ∈ Q.
    strategy_formula_conjunct (Attacker_Conjunct p q) e' (Φ q) ∧
    expr_pr_conjunct (Φ q) ≤ e'>
    by meson
  then obtain Φ where Φ_prop: <∀q ∈ Q.
    strategy_formula_conjunct (Attacker_Conjunct p q) e' (Φ q)
    ∧ expr_pr_conjunct (Φ q) ≤ e'>
    by blast

```

```

have <E 0 0 0 1 0 0 0 0 ≤ e>
  using e'_spec False by fastforce
hence <expr_pr_inner (StableConj Q Φ) ≤ e>
  using expr_st_conj e'_spec Φ_prop False by metis
moreover have <strategy_formula_inner (Defender_Stable_Conj p Q) e (StableConj Q Φ)>
  using Φ_prop e'_spec stable_conj
  unfolding e'_spec by fastforce
ultimately show ?thesis by auto
qed
qed force+
qed

lemma strategy_formulas_distinguish:
  shows
    <(strategy_formula g e φ →
      (case g of
        Attacker_Immediate p Q ⇒ distinguishes_from φ p Q
      | Defender_Conj p Q ⇒ distinguishes_from φ p Q
      | _ ⇒ True))
    ∧
    (strategy_formula_inner g e χ →
      (case g of
        Attacker_Delayed p Q ⇒ (Q →S Q) → distinguishes_from (Internal χ) p Q
      | Defender_Conj p Q ⇒ hml_srbb_inner.distinguishes_from χ p Q
      | Defender_Stable_Conj p Q ⇒ (∀q. ¬ p ↦ τ q)
        → hml_srbb_inner.distinguishes_from χ p Q
      | Defender_Branch p α p' Q Qa ⇒ (p ↦α p' ∧ Qa ≠ {})
        → hml_srbb_inner.distinguishes_from χ p (Q ∪ Qa)
      | _ ⇒ True))
    ∧
    (strategy_formula_conjunct g e ψ →
      (case g of
        Attacker_Conjunct p q ⇒ hml_srbb_conj.distinguishes ψ p q
      | _ ⇒ True))>
proof(induction rule: strategy_formula_strategy_formula_inner_strategy_formula_conjunct.induct)
  case (delay p Q e χ)
  then show ?case
    by (smt (verit) distinguishes_from_def option.discI silent_reachable.intros(1)
      silent_reachable_trans spectroscopy_moves.simps(1) spectroscopy_position.simps)
next
  case (procrastination p Q e χ)
  from this obtain p' where IH:
    <spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Delayed p' Q) = id_up ∧
    spectro_att_wins e (Attacker_Delayed p' Q) ∧
    strategy_formula_inner (Attacker_Delayed p' Q) e χ ∧
    (case Attacker_Delayed p' Q of Attacker_Delayed p Q ⇒
      Q →S Q → distinguishes_from (hml_srbb.Internal χ) p Q |
      Defender_Branch p α p' Q Qa ⇒ p ↦α p' ∧ Qa ≠ {}
        → hml_srbb_inner.distinguishes_from χ p (Q ∪ Qa) |
      Defender_Conj p Q ⇒ hml_srbb_inner.distinguishes_from χ p Q |
      Defender_Stable_Conj p Q ⇒ (∀q. ¬ p ↦ τ q)
        → hml_srbb_inner.distinguishes_from χ p Q |
      _ ⇒ True)> by fastforce
  hence D: <Q →S Q → distinguishes_from (hml_srbb.Internal χ) p' Q>
    using spectroscopy_position.simps(53) by fastforce
  from IH have <p →p'>
    by (metis option.discI silent_reachable.intros(1)
      silent_reachable_append_τ spectroscopy_moves.simps(2))
  hence <Q →S Q → distinguishes_from (hml_srbb.Internal χ) p Q> using D
    by (smt (verit) silent_reachable_trans distinguishes_from_def hml_srbb_models.simps(2))
  then show ?case by simp

```

```

next
case (observation p Q e  $\varphi$   $\alpha$ )
then obtain p' Q' where IH:
  <spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Immediate p' Q')
    = subtract 1 0 0 0 0 0 0 0  $\wedge$ 
    spectro_att_wins (e - E 1 0 0 0 0 0 0 0) (Attacker_Immediate p' Q')  $\wedge$ 
    (strategy_formula (Attacker_Immediate p' Q') (e - E 1 0 0 0 0 0 0 0)  $\varphi$   $\wedge$ 
      (case Attacker_Immediate p' Q' of Attacker_Immediate p Q  $\Rightarrow$  distinguishes_from  $\varphi$  p Q
        | Defender_Conj p Q  $\Rightarrow$  distinguishes_from  $\varphi$  p Q | _  $\Rightarrow$  True))  $\wedge$ 
    p  $\mapsto$  a  $\alpha$  p'  $\wedge$  Q  $\mapsto$  aS  $\alpha$  Q' > by auto
hence D: <distinguishes_from  $\varphi$  p' Q' > by auto
hence <p'  $\models$  SRBB  $\varphi$  > by auto
have observation: <spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Immediate p' Q')
  = (if ( $\exists$  a. p  $\mapsto$  a a p'  $\wedge$  Q  $\mapsto$  aS a Q') then (subtract 1 0 0 0 0 0 0 0) else None) >
  for p p' Q Q' by simp
from IH have <spectroscopy_moves (Attacker_Delayed p Q) (Attacker_Immediate p' Q')
  = subtract 1 0 0 0 0 0 0 0 > by simp
also have <...  $\neq$  None > by blast
finally have <( $\exists$  a. p  $\mapsto$  a a p'  $\wedge$  Q  $\mapsto$  aS a Q') > unfolding observation by metis
from IH have <p  $\mapsto$  a  $\alpha$  p' > and <Q  $\mapsto$  aS  $\alpha$  Q' > by auto
hence P: <p  $\models$  SRBB (Internal (Obs  $\alpha$   $\varphi$ )) > using <p'  $\models$  SRBB  $\varphi$  >
  using silent_reachable.intros(1) by auto
have <Q  $\twoheadrightarrow$  S Q  $\longrightarrow$  ( $\forall$  q  $\in$  Q.  $\neg$ (q  $\models$  SRBB (Internal (Obs  $\alpha$   $\varphi$ )))) >
  by (simp, meson D <Q  $\mapsto$  aS  $\alpha$  Q' > distinguishes_from_def)
hence <Q  $\twoheadrightarrow$  S Q  $\longrightarrow$  distinguishes_from (hml_srbbs.Internal (hml_srbbs_inner.Obs  $\alpha$   $\varphi$ )) p Q >
  using P by fastforce
then show ?case by simp
next
case (early_conj Q p Q' e  $\varphi$ )
then show ?case
  by (simp, metis not_None_eq)
next
case (late_conj p Q e  $\chi$ )
then show ?case
  using silent_reachable.intros(1)
  by auto
next
case (conj Q p e  $\Phi$ )
then show ?case by auto
next
case (imm_conj Q p e  $\Phi$ )
then show ?case by auto
next
case (pos p q e  $\chi$ )
then show ?case using silent_reachable.refl
  by (simp) (metis option.discI silent_reachable_trans)
next
case (neg p q e  $\chi$ )
then obtain P' where IH:
  <spectroscopy_moves (Attacker_Conjunct p q) (Attacker_Delayed q P')
    = Some ( $\lambda$ e. Option.bind (subtract_fn 0 0 0 0 0 0 0 1 e) min1_7) >
  <spectro_att_wins (the (min1_7 (e - E 0 0 0 0 0 0 0 1))) (Attacker_Delayed q P')  $\wedge$ 
    strategy_formula_inner (Attacker_Delayed q P')
      (the (min1_7 (e - E 0 0 0 0 0 0 0 1)))  $\chi$   $\wedge$ 
    (case Attacker_Delayed q P' of
      Attacker_Delayed p Q  $\Rightarrow$  Q  $\twoheadrightarrow$  S Q  $\longrightarrow$  distinguishes_from (hml_srbbs.Internal  $\chi$ ) p Q
    | Defender_Branch p  $\alpha$  p' Q Qa
       $\Rightarrow$  p  $\mapsto$   $\alpha$  p'  $\wedge$  Qa  $\neq$  {}  $\longrightarrow$  hml_srbbs_inner.distinguishes_from  $\chi$  p (Q  $\cup$  Qa)
    | Defender_Conj p Q  $\Rightarrow$  hml_srbbs_inner.distinguishes_from  $\chi$  p Q
    | Defender_Stable_Conj p Q
       $\Rightarrow$  ( $\forall$  q.  $\neg$  p  $\mapsto$   $\tau$  q)  $\longrightarrow$  hml_srbbs_inner.distinguishes_from  $\chi$  p Q
  >

```

```

| _  $\Rightarrow$  True> by fastforce
hence D:  $\langle P' \Rightarrow S P' \Rightarrow \text{distinguishes\_from (hml\_srbb.Internal } \chi) q P' \rangle$  by simp
have  $\langle \{p\} \Rightarrow S P' \rangle$  using IH(1) spectroscopy_moves.simps
  by (metis (no_types, lifting) not_Some_eq)
have  $\langle P' \Rightarrow S P' \Rightarrow p \in P' \rangle$  using  $\langle \{p\} \Rightarrow S P' \rangle$  by (simp add: silent_reachable.intros(1))
hence  $\langle \text{hml\_srbb\_conj.distinguishes (hml\_srbb\_conjunct.Neg } \chi) p q \rangle$  using D  $\langle \{p\} \Rightarrow S P' \rangle$ 
  unfolding hml_srbb_conj.distinguishes_def distinguishes_from_def
  by (smt (verit) lts_tau.silent_reachable_trans hml_srbb_conjunct_models.simps(2)
      hml_srbb_models.simps(2) silent_reachable.refl)
then show ?case by simp
next
case (stable p Q e  $\chi$ )
then obtain Q' where IH:
  <spectroscopy_moves (Attacker_Delayed p Q) (Defender_Stable_Conj p Q') = id_up>
  <spectro_att_wins e (Defender_Stable_Conj p Q') &
  strategy_formula_inner (Defender_Stable_Conj p Q') e  $\chi$  &
  (case Defender_Stable_Conj p Q' of
    Attacker_Delayed p Q  $\Rightarrow$  Q  $\Rightarrow$  S Q  $\Rightarrow$  distinguishes_from (hml_srbb.Internal  $\chi$ ) p Q
  | Defender_Branch p  $\alpha$  p' Q Qa
     $\Rightarrow$  p  $\mapsto \alpha$  p'  $\wedge$  Qa  $\neq \{\}$   $\Rightarrow$  hml_srbb_inner.distinguishes_from  $\chi$  p (Q  $\cup$  Qa)
  | Defender_Conj p Q
     $\Rightarrow$  hml_srbb_inner.distinguishes_from  $\chi$  p Q
  | Defender_Stable_Conj p Q
     $\Rightarrow$  ( $\forall q. \neg p \mapsto \tau q$ )  $\Rightarrow$  hml_srbb_inner.distinguishes_from  $\chi$  p Q
  | _  $\Rightarrow$  True)> by auto
hence  $\langle \#p''. p \mapsto \tau p'' \rangle$ 
  by (metis local.late_stbl_conj option.distinct(1))
from IH have  $\langle (\forall q. \neg p \mapsto \tau q) \Rightarrow \text{hml\_srbb\_inner.distinguishes\_from } \chi p Q' \rangle$  by simp
hence  $\langle \text{hml\_srbb\_inner.distinguishes\_from } \chi p Q' \rangle$  using  $\langle \#p''. p \mapsto \tau p'' \rangle$  by auto
hence  $\langle \text{hml\_srbb\_inner\_models p } \chi \rangle$  by simp
hence  $\langle p \models \text{SRBB (hml\_srbb.Internal } \chi) \rangle$ 
  using lts_tau.refl by force
have  $\langle Q \Rightarrow S Q \Rightarrow \text{distinguishes\_from (hml\_srbb.Internal } \chi) p Q \rangle$ 
proof
  assume  $\langle Q \Rightarrow S Q \rangle$ 
  have  $\langle (\forall q \in Q. \neg (q \models \text{SRBB (hml\_srbb.Internal } \chi))) \rangle$ 
  proof (clarify)
    fix q
    assume  $\langle q \in Q \rangle \langle (q \models \text{SRBB (hml\_srbb.Internal } \chi)) \rangle$ 
    hence  $\langle \exists q'. q \Rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \chi \rangle$  by simp
    then obtain q' where X:  $\langle q \Rightarrow q' \wedge \text{hml\_srbb\_inner\_models } q' \chi \rangle$  by auto
    hence  $\langle q' \in Q \rangle$  using  $\langle Q \Rightarrow S Q \rangle \langle q \in Q \rangle$  by blast
    then show <False>
  proof (cases  $\langle q' \in Q' \rangle$ )
    case True — stable cases
    thus <False> using X  $\langle \text{hml\_srbb\_inner.distinguishes\_from } \chi p Q' \rangle$ 
      by simp
  next
  case False — unstable cases
  from IH have  $\langle \text{strategy\_formula\_inner (Defender\_Stable\_Conj p Q') e } \chi \rangle$  by simp
  hence  $\langle \exists \Phi. \chi = \text{StableConj } Q' \Phi \rangle$  using strategy_formula_inner.simps
    by (smt (verit) spectroscopy_defender.simps(4,7)
        spectroscopy_position.distinct(37,41) spectroscopy_position.inject(6))
  then obtain  $\Phi$  where P:  $\langle \chi = (\text{StableConj } Q' \Phi) \rangle$  by auto
  from IH(1) have  $\langle Q' = \{q \in Q. (\#q''. q \mapsto \tau q'')\} \rangle$ 
    by (metis (full_types) local.late_stbl_conj option.distinct(1))
  hence  $\langle \exists q''. q' \mapsto \tau q'' \rangle$  using False  $\langle q' \in Q \rangle$  by simp
  from X have  $\langle \text{hml\_srbb\_inner\_models } q' (\text{StableConj } Q' \Phi) \rangle$  using P by auto
  then show ?thesis using  $\langle \exists q''. q' \mapsto \tau q'' \rangle$  by simp
qed
qed

```

```

    thus <distinguishes_from (hml_srbb.Internal  $\chi$ ) p Q>
      using <p  $\models$  SRBB (hml_srbb.Internal  $\chi$ )> by simp
qed
then show ?case by simp
next
case (stable_conj Q p e  $\Phi$ )
hence IH: < $\forall q \in Q$ . hml_srbb_conj.distinguishes ( $\Phi$  q) p q> by simp
hence Q: < $\forall q \in Q$ . hml_srbb_conjunct_models p ( $\Phi$  q)> by simp
hence <( $\forall q$ .  $\neg$  p  $\mapsto$   $\tau$  q)  $\longrightarrow$  hml_srbb_inner.distinguishes_from (StableConj Q  $\Phi$ ) p Q>
  using IH by auto
then show ?case by simp
next
case (branch p Q e  $\chi$ )
then obtain p' Q'  $\alpha$  Q $\alpha$  where IH:
  <spectroscopy_moves (Attacker_Delayed p Q) (Defender_Branch p  $\alpha$  p' Q' Q $\alpha$ ) = id_up>
  <spectro_att_wins e (Defender_Branch p  $\alpha$  p' Q' Q $\alpha$ )  $\wedge$ 
  strategy_formula_inner (Defender_Branch p  $\alpha$  p' Q' Q $\alpha$ ) e  $\chi$   $\wedge$ 
  (case Defender_Branch p  $\alpha$  p' Q' Q $\alpha$  of
    Attacker_Delayed p Q  $\Rightarrow$  Q  $\Rightarrow$  S Q  $\longrightarrow$  distinguishes_from (Internal  $\chi$ ) p Q
  | Defender_Branch p  $\alpha$  p' Q Q $\alpha$ 
     $\Rightarrow$  p  $\mapsto$  a  $\alpha$  p'  $\longrightarrow$  hml_srbb_inner.distinguishes_from  $\chi$  p (Q  $\cup$  Q $\alpha$ )
  | Defender_Conj p Q  $\Rightarrow$  hml_srbb_inner.distinguishes_from  $\chi$  p Q
  | Defender_Stable_Conj p Q
     $\Rightarrow$  ( $\forall q$ .  $\neg$  p  $\mapsto$   $\tau$  q)  $\longrightarrow$  hml_srbb_inner.distinguishes_from  $\chi$  p Q
  | _  $\Rightarrow$  True)> by blast
from IH(1) have <p  $\mapsto$  a  $\alpha$  p'>
  by (metis local.br_conj option.distinct(1))
from IH have <p  $\mapsto$  a  $\alpha$  p'  $\longrightarrow$  hml_srbb_inner.distinguishes_from  $\chi$  p (Q'  $\cup$  Q $\alpha$ )> by simp
hence D: <hml_srbb_inner.distinguishes_from  $\chi$  p (Q'  $\cup$  Q $\alpha$ )> using <p  $\mapsto$  a  $\alpha$  p'> by auto
from IH have <Q' = Q - Q $\alpha$   $\wedge$  p  $\mapsto$  a  $\alpha$  p'  $\wedge$  Q $\alpha$   $\subseteq$  Q>
  by (metis (no_types, lifting) br_conj option.discI)
hence <Q=(Q'  $\cup$  Q $\alpha$ )> by auto
then show ?case
  using D silent_reachable.refl by auto
next
case (branch_conj p  $\alpha$  p' Q1 Q $\alpha$  e  $\psi$   $\Phi$ )
hence A1: < $\forall q \in Q1$ . hml_srbb_conjunct_models p ( $\Phi$  q)> by simp
from branch_conj obtain Q' where IH:
  <spectroscopy_moves (Defender_Branch p  $\alpha$  p' Q1 Q $\alpha$ ) (Attacker_Branch p' Q')
    = Some ( $\lambda$ e. Option.bind (subtract_fn 0 1 1 0 0 0 0 0 e) min1_6)>
  <spectroscopy_moves (Attacker_Branch p' Q') (Attacker_Immediate p' Q')
    = subtract 1 0 0 0 0 0 0 0  $\wedge$ 
    spectro_att_wins (the (min1_6 (e - E 0 1 1 0 0 0 0 0))) - E 1 0 0 0 0 0 0 0)
    (Attacker_Immediate p' Q')  $\wedge$ 
    strategy_formula (Attacker_Immediate p' Q')
    (the (min1_6 (e - E 0 1 1 0 0 0 0 0))) - E 1 0 0 0 0 0 0 0)  $\psi$   $\wedge$ 
    (case Attacker_Immediate p' Q' of
      Attacker_Immediate p Q  $\Rightarrow$  distinguishes_from  $\psi$  p Q
    | Defender_Conj p Q  $\Rightarrow$  distinguishes_from  $\psi$  p Q | _  $\Rightarrow$  True)> by auto
hence <distinguishes_from  $\psi$  p' Q'> by simp
hence X: <p'  $\models$  SRBB  $\psi$ > by simp
have Y: < $\forall q \in Q'$ .  $\neg$ (q  $\models$  SRBB  $\psi$ )> using <distinguishes_from  $\psi$  p' Q'> by simp
have <p  $\mapsto$  a  $\alpha$  p'  $\longrightarrow$  hml_srbb_inner.distinguishes_from (BranchConj  $\alpha$   $\psi$  Q1  $\Phi$ ) p (Q1  $\cup$  Q $\alpha$ )>
  proof
    assume <p  $\mapsto$  a  $\alpha$  p'>
    hence <p  $\mapsto$  a  $\alpha$  p'> by simp
    with IH(1) have <Q $\alpha$   $\mapsto$  aS  $\alpha$  Q'>
      by (simp, metis option.discI)
    hence A2: <hml_srbb_inner_models p (Obs  $\alpha$   $\psi$ )> using X <p  $\mapsto$  a  $\alpha$  p'> by auto
    have A3: < $\forall q \in (Q1 \cup Q\alpha)$ . hml_srbb_inner.distinguishes (BranchConj  $\alpha$   $\psi$  Q1  $\Phi$ ) p q>
      proof (safe)

```

```

fix q
assume <q ∈ Q1>
hence <hml_srbb_conj.distinguishes (Φ q) p q> using branch_conj(2) by simp
thus <hml_srbb_inner.distinguishes (BranchConj α ψ Q1 Φ) p q>
  using A1 A2 srbb_dist_conjunct_or_branch_implies_dist_branch_conjunction <q ∈ Q1>
  by blast
next
fix q
assume <q ∈ Qα>
hence <¬(hml_srbb_inner_models q (Obs α ψ))>
  using Y <Qα ↦ aS α Q'> by auto
hence <hml_srbb_inner.distinguishes (Obs α ψ) p q>
  using A2 by auto
thus <hml_srbb_inner.distinguishes (BranchConj α ψ Q1 Φ) p q>
  using A1 A2 srbb_dist_conjunct_or_branch_implies_dist_branch_conjunction by blast
qed
have <hml_srbb_inner_models p (BranchConj α ψ Q1 Φ)>
  using A3 A2 by fastforce
with A3 show <hml_srbb_inner.distinguishes_from (BranchConj α ψ Q1 Φ) p (Q1 ∪ Qα)>
  by simp
qed
then show ?case by simp
qed

end

end

```

9.3 Correctness Theorem

```

theory Silent_Step_Spectroscopy
imports
  Distinction_Implies_Winning_Budgets
  Strategy_Formulas
begin

```

We now only combine the results of `Distinction_Implies_Winning_Budgets` and `Strategy_Formulas` to obtain the main characterization theorem of the weak spectroscopy game characterizing a whole spectrum of weak equivalences.

```

context lts_tau
begin

```

```

theorem spectroscopy_game_correctness:
  fixes e p Q
  shows <(∃ φ. distinguishes_from φ p Q ∧ expressiveness_price φ ≤ e)
    ↔ spectro_att_wins e (Attacker_Immediate p Q)>
proof
  assume <∃ φ. distinguishes_from φ p Q ∧ expressiveness_price φ ≤ e>
  then obtain φ where φ_spec:
    <distinguishes_from φ p Q> <expressiveness_price φ ≤ e>
  by blast
  from distinction_implies_winning_budgets φ_spec(1) have
    <spectro_att_wins (expressiveness_price φ) (Attacker_Immediate p Q)> .
  thus <spectro_att_wins e (Attacker_Immediate p Q)>
  using weak_spectroscopy_game.win_a_upwards_closure φ_spec(2) by simp
next
  assume <spectro_att_wins e (Attacker_Immediate p Q)>
  with winning_budget_implies_strategy_formula have
    <∃ φ. strategy_formula (Attacker_Immediate p Q) e φ ∧ expressiveness_price φ ≤ e>
  by force
  hence <∃ φ. strategy_formula (Attacker_Immediate p Q) e φ ∧ expressiveness_price φ ≤ e>

```

```

    by blast
  thus < $\exists \varphi$ . distinguishes_from  $\varphi$  p Q  $\wedge$  expressiveness_price  $\varphi \leq e$ >
    using strategy_formulas_distinguish by fastforce
qed

```

An implicit result of the correctness theorem is that attacker wins on bigger Q imply wins on smaller ones.

```

proposition attacker_subet_wins:
  assumes
    <spectro_att_wins e (Attacker_Immediate p Q)>
    <Q'  $\subseteq$  Q>
  shows
    <spectro_att_wins e (Attacker_Immediate p Q')>
  using assms spectroscopy_game_correctness
  unfolding distinguishes_from_def subset_iff
  by meson

end

end

```

References

- [1] Benjamin Bisping. Process equivalence problems as energy games. In Constantin Enea and Akash Lal, editors, *Computer Aided Verification*, pages 85–106, Cham, 2023. Springer Nature Switzerland. doi:10.1007/978-3-031-37706-8_5.
- [2] Benjamin Bisping. *Generalized Equivalence Checking of Concurrent Programs*. PhD thesis, Technische Universität Berlin, 2025. URL: <https://generalized-equivalence-checking.equiv.io/>.
- [3] Benjamin Bisping and David N. Jansen. Linear-time–branching-time spectroscopy accounting for silent steps, 2023. arXiv:2305.17671, doi:10.48550/arXiv.2305.17671.
- [4] Benjamin Bisping and David N. Jansen. One energy game for the spectrum between branching bisimilarity and weak trace semantics. In Georgiana Caltais and Cinzia Di Giusto, editors, Proceedings Combined 31st International Workshop on *Expressiveness in Concurrency* and 21st Workshop on *Structural Operational Semantics*, Calgary, Canada, 9th September 2024, volume 412, pages 71–88. Open Publishing Association, 2024. doi:10.4204/EPTCS.412.6.
- [5] Matthew Hennessy and Robin Milner. On observing nondeterminism and concurrency. In J. W. de Bakker and J. van Leeuwen, editors, *Automata, Languages and Programming*, volume 85, pages 299–309. Springer, Berlin, 1980. doi:10.1007/3-540-10003-2_79.
- [6] Rob J. van Glabbeek. The linear time–branching time spectrum: extended abstract. In J. C. M. Baeten and J. W. Klop, editors, *CONCUR’90*, volume 458, pages 278–297. Springer, Berlin, 1990. doi:10.1007/BFb0039066.
- [7] Rob J. van Glabbeek. The linear time–branching time spectrum II: The semantics of sequential systems with silent moves; extended abstract. In Eike Best, editor, *CONCUR’93*, volume 715, pages 66–81. Springer, Berlin, 1993. doi:10.1007/3-540-57208-2_6.