Chapter 1

Introduction

Modal and temporal logics have seen widespread usage in the industry as languages for expressing property about the evolution of complex systems. Various models based on graphs and automaton have model checkers developed upon. Most of them are based upon propositional variation of modal and temporal logics, however some reasearcher started working on first-order or second-order variants. These logics suffer mainly two issues: they are in general undecidable and the semantics evaluation model suffer various issue with trans-world identity. Counterpart relations solve most of these issues and recent works successfully use counterpart relations with monadic second-order modal logics to obtain a decidable calculus in finite domains and a companion model checker prototype. However they are based upon fixpoints and modal operators which are not really intuitive. The semantics evaluation function is complex and hard to follow by hand, and work is still needed regarding completeness and inference systems. The aim of this work is to develop a a counterpart semantics model for first-order/second-order linear temporal logic, and show that we can obtain a far simpler and understandable semantics but being still able to model plenty of properties and with an axiomatic model and an inference system.

We will first give an introduction to linear temporal logic and the issue of extending it to the first or second-order. Then we will present the mathematical tools used in our semantics, many-sorted algebras and counterpart models. We will defined the counterpart semantics for first-order/second-order linear temporal logic with many examples of properties and how to compute the semantics. Finally we will show some results on axioms and inference rules.

The main running example will be about multi-process communication over channels, modeled via graphs with processes as nodes and channels as edges. Some of the properties we will be able to express with our calculus are:

- Will all the channel be closed at the end of the execution?
- Which channels will be merged during execution?

- Are there isolated process at any point in time?
- Do the channels connection change at each step?
- Are new channels created during the execution?

Chapter 2

Linear Temporal Logic

2.1 Syntax

Definition 2.1.1 (Linear Temporal Logic)**.** *Let PROP be a set of atomic propositions. The set $\mathcal{F}$ of formulae for Linear Temporal Logic is the set generated by the following grammar:*

$$\phi ::= tt \mid p \mid \neg\phi \mid \phi \vee \phi \mid X\phi \mid \phi U \phi$$

where $p \in PROP$, X is a unary operator which states that ϕ must hold at the next step and U is a binary operator which states that the first formula must hold until the second formula holds at some point in the current or next steps.

Classical propositional logic connetives can be derived trivially:

$$\phi_1 \wedge \phi_2 \equiv \neg(\neg\phi_1 \vee \neg\phi_2) \quad \phi_1 \rightarrow \phi_2 \equiv \neg\phi_1 \vee \phi_2 \quad \phi_1 \leftrightarrow \phi_2 \equiv (\phi_1 \rightarrow \phi_2) \wedge (\phi_2 \rightarrow \phi_1)$$

Other temporal operators used in temporal logic literature are derivable as such:

$$F\phi \equiv tt\, U \phi \quad G\phi \equiv \neg F(\neg\phi) \quad \phi_1\, W \phi_2 \equiv (\phi_1\, U \phi_2) \vee G\phi_1$$

Intuitively $F\phi$ means that eventually at some next step in time the formula ϕ holds, $G\phi$ means that the formula ϕ holds at each possible next step.

LTL formulae can encode safety properties, commonly with the form $G\neg\phi$, and liveness properties of systems, commonly with the form $GF\phi$ or $G(\phi_1 \rightarrow F\phi_2)$. Let's assume that we have two concurrent processes and that we can encode with two atomic propositions, crit_1 and crit_2, when the two processes can access a critical section, then the property of mutual exclusivity can be model by the formula $G(\neg\text{crit}_1 \vee \neg\text{crit}_2)$. If we also have atomic propositions for wait conditions, wait_1, then we can model liveness conditions, for example $G(\text{wait}_1 \rightarrow F\text{crit}_1)$ which means that whenever a process reaches a wait condition, eventually will enter the critical section; we can also model fairness conditions, for example $GF\text{wait}_1 \rightarrow GF\text{crit}_1$ means that if the process infinitely often reaches a wait condition than infinitely often will reach the critical section.

2.2 Semantic

The de-facto standard semantics for Linear Temporal Logic and Temporal Logics in general are Kripke-style semantics, as for modal logics. In modal logic, the so-called Kripke-frames are pairs of worlds and an accessibility relation between worlds. For temporal logic, each world is a point in time and the accessibility relation models the flow of time, thus a temporal model is defined as:

Definition 2.2.1 (Temporal model)**.** *A* temporal model M *is a triple* $(T, \prec, L)$ *where* T *is a set of time-points,* $\prec$ *is an accessibility relations over* T *and* $L : T \to \mathcal{P}(PROP)$ *is a labelling function that for each point in time returns the subset of all atomic propositions which are valid at that point.*

Additionally, the pair $(T, \prec)$ is called a temporal frame. For linear temporal logic in particular each point in time t as a unique successor that we will denote with $s(t)$, and usually the chosen temporal frame is $(\mathbb{N}, <)$.

Definition 2.2.2 (LTL semantic)**.** *The truthness of a LTL formula* ϕ *at the time-point* t *over the temporal model* M*, denoted as* $M, t \vDash \phi$ *is defined inductively as follows:*

$$
\begin{array}{ll}
M, t \vDash tt & \\
M, t \vDash p & \textit{iff } p \in L(t) \\
M, t \vDash \neg\phi & \textit{iff } M, t \nvDash \phi \\
M, t \vDash \phi_1 \vee \phi_2 & \textit{iff } M, t \vDash \phi_1 \textit{ or } M, t \vDash \phi_2 \\
M, t \vDash X\phi & \textit{iff } M, s(t) \vDash \phi \\
M, t \vDash \phi_1 \, U \phi_2 & \textit{iff } \exists t' \geq t.\, M, t' \vDash \phi_2 \textit{ and } \forall t \leq t'' < t'.\, M, t'' \vDash \phi_1
\end{array}
$$

2.3 First-Order Extension

Definition 2.3.1 (First-Order Linear Temporal Logic)**.** *Let* $\mathcal{P}$ *be a set of predicates each with a specific arity, and let* X *be a denumerable set of variables. The set* $\mathcal{F}_{FO}$ *of formulae for First-Order Linear Temporal Logic is the set generated by the following grammar:*

$$\phi ::= tt \mid P(x_1, \ldots, x_n) \mid \neg\phi \mid \phi \vee \phi \mid X\phi \mid \phi \, U \phi \mid \exists x.\, \phi$$

where $P \in \mathcal{P}$ *and* $x_1, \ldots, x_n \in X$ *are individual variables that match the arity required by* P*.*

Universal quantification can be modeled with the translation from the existential quantifier and negation:

$$\forall x.\, \phi \equiv \neg\exists x.\, \neg\phi$$

Example of properties can be modeled with the first-order extension are $\exists x.\, G(\text{channel}(x) \wedge \text{open}(x))$ with the intuitive meaning that there must always exists at least one open channel; or $\forall x.\, G(\text{channel}(x) \rightarrow (\text{open}(x)\, U(\neg\exists y.\, \text{message}(y) \wedge \text{pending}(x,$ which intuitively means that channels must always remain open until there are no more pending messages on that channel.

For quantified LTL we need to extend the temporal frames with the domain of values that makes sense to talk about at each points in time.

Definition 2.3.2 (Kripke frame)**.** *A* Kripke frame M *is a quadruple* $(T, \prec, D, d)$ *where* T *is a set of time-points,* $\prec$ *is an accessibility relations over* T*,* D *is a function assigning to each point in time* t *a non-empty set* $D(t)$ *s.t. if* $t \prec t'$ *then* $D(t) \subseteq D(t')$*,* d *is a function assigning to each point in time* t *a set* $d(t) \subseteq D(t)$*.*

Intuitively, the so-called outer domains $D(t)$ represent the collection of object that can be referenced at the point in time t, conversely the so-called inner domains $d(t)$ represent the collection of object actually existing the point in time t. An assignement function σ is a function from the set of variables X to the outer-domain $D(t)$ of a given point in time t. Finally, we need an interpretation function I such that $I(P, t)$ assign for each predicate constant $P \in \mathcal{P}$ and point in time t a subset of $D^n(t)$ where n is the arity of P, and $I(x, t) = \sigma(x)$ where $x \in X$ and σ is a suitable assignment that is said to be inducing I, noted as I^σ.

Definition 2.3.3 (FO-LTL semantic)**.** *The truthness of a FO-LTL formula* ϕ *at the point in time* t *over the Kripke model* M *and the induced interpretation* I^σ*, denoted as* $M, t, I^\sigma \vDash \phi$ *is defined inductively as follows:*

$M, t, I^\sigma \vDash tt$

$M, t, I^\sigma \vDash P(x_1, \ldots, x_n)$ *iff* $(\sigma(x_1), \ldots, \sigma(x_2)) \in I^\sigma(P, t)$

$M, t, I^\sigma \vDash \neg\phi$ *iff* $M, t, I^\sigma \nvDash \phi$

$M, t, I^\sigma \vDash \phi_1 \vee \phi_2$ *iff* $M, t, I^\sigma \vDash \phi_1$ *or* $M, t, I^\sigma \vDash \phi_2$

$M, t, I^\sigma \vDash X\phi$ *iff* $M, s(t), I^\sigma \vDash \phi$

$M, t, I^\sigma \vDash \phi_1\, U \phi_2$ *iff* $\exists t' \geq t.\, M, t', I^\sigma \vDash \phi_2$ *and* $\forall t \leq t'' < t'.\, M, t'', I^\sigma \vDash \phi_1$

$M, t, I^\sigma \vDash \exists x.\, \phi$ *iff* $\exists v \in d(t).\, M, t, I^{\sigma[v/x]} \vDash \phi$

2.4 Trans-World Identity

Kripke-frames requires that the so-called outer domains $D(t)$ are always increasing with time, i.e. if $t \prec t'$ then $D(t) \subseteq D(t')$. This condition is required to evaluate temporal operators, otherwise it would not be possible to denote a variable x in the future. However, by imposing such condition

we are identifying object *a priori* and universally, irrespective of time. This problem is called *trans-world identity* and extensive literature about it has been produced in the last half-century, be either philosophycal questions and possible solutions with Kripke-style semantics. Even with the additional constraints on object domains, there are still other issues with Kripke-style semantics and the system we are trying to model. Assume we are trying to model resource allocation in a complex system. Let i be a resource. Due to the outer domain condition, we can identify the exact point in time where the resource i is allocated, i.e. $i \in D(t)$ for some time point t. Note that the resource can be allocated, but still can be unused for a potentially infinite amount of time, since it may not belong to any inner domain, not even $d(t)$. However, at the same time, we cannot deallocate the resource i since it must always be referentiable at future point in times. This can be solved with infinite outer domains to ensure uniqueness or by restricting the class of admissible evolutions, but such solutions tend to hamper usability. Another desiderable behaviour is merging, for example while modeling memory allocations, we may want to merge two memory allocated segments into a single segment and treat it as a single resource. In the next chapter we will explore an alternative approach based on *counterpart relations*, which rejects the possibility of universally identifying objects among possible worlds.

Chapter 3

Counterpart Semantic

3.1 Algebra

Definition 3.1.1 (Many-sorted Signature)**.** *A* many-sorted signature Σ *is a pair* (S_Σ, F_Σ) *where* $S_\Sigma = \{ \tau_1, \ldots, \tau_n \}$ *is a set of sorts, and* $F_\Sigma = \{ f_\Sigma : \tau_1 \times \cdots \times \tau_n \to \tau \mid \tau_i, \tau \in \Sigma_\tau, i = 1, \ldots, n \}$ *is a set of function symbols.*

Definition 3.1.2 (Many-sorted Algebra)**.** *A* many-sorted algebra $\mathbf{A}$ *with signature* Σ*, or* Σ*-algebra, is a pair* $(A, F_\Sigma^{\mathbf{A}})$ *such that:*

- A *is a family of carrier sets indexed by the sorts of* Σ*;*
- $F_\Sigma^{\mathbf{A}}$ *is a family of functions indexed by the function symbols of* Σ*,* $\{ f_\Sigma^{\mathbf{A}} : A_{\tau_1} \times \cdots \times A_{\tau_n} \to A_\tau \mid f_\Sigma : \tau_1 \times \cdots \times \tau_n \to \tau \in F_\Sigma \}$*.*

Definition 3.1.3 (Homomorphism)**.** *Given two* Σ*-algebras* $\mathbf{A}$ *and* $\mathbf{B}$*, a* (partial) homomorphism *is a family of (partial) functions indexed by the sorts of* Σ*,* $\{ \rho_\tau : A_\tau \rightharpoonup B_\tau \mid \tau \in S_\Sigma \}$*, such that for each function symbol* $f_\Sigma : \tau_1 \times \cdots \times \tau_n \in F_\Sigma$ *and list of elements* $a_1 \in A_{\tau_1}, \ldots, a_n \in A_{\tau_n}$*, if each function* ρ_{τ_i} *is defined for the element* a_i *then* ρ_τ *is defined for the element* $f_\Sigma^{\mathbf{A}}(a_1, \ldots, a_n)$ *and* $\rho_\tau(f_\Sigma^{\mathbf{A}}(a_1, \ldots, a_n)) = f_\Sigma^{\mathbf{B}}(\rho_{\tau_1}(a_1), \ldots, \rho_{\tau_n}(a_n))$*.*

Example 3.1.1 (Graph algebra)**.** *Simple directed graphs can be modeled by the signature* $\Sigma = (\{ \tau_v, \tau_e \}, \{ s : \tau_e \to \tau_v, t : \tau_e \to \tau_v \})$*, where* τ_v *is the sort of vertices,* τ_e *is the sort of edges and* s*,* t *determine respectively the source and target vertex for a given edge. Each* Σ*-algebra for this signature is a particular graph, i.e. the graphs in figure 1 are visual representations of the following algebras:* $\mathbf{G}_0 = (\{ \{ n_0, n_1, n_2 \}, \{ e_0, e_1, e_2 \} \}, \{ s^{\mathbf{G}_0}, t^{\mathbf{G}_0} \})$*, where* $s^{\mathbf{G}_0} = \{ e_0 \mapsto n_0, e_1 \mapsto n_1, e_2 \mapsto n_2 \}$ *and* $t^{\mathbf{G}_0} = \{ e_0 \mapsto n_1, e_1 \mapsto n_2, e_2 \mapsto n_0 \}$*.*

To model existential properties, we can extend a signature Σ with a denumerable set X of variables typed over S_Σ, obtaining the signature Σ_X. The τ-typed subset of X is denoted with X_τ, and typed variables are denoted with x_τ or $x : \tau$. τ-sorted terms are denoted with ϵ_τ or $\epsilon : \tau$.

Definition 3.1.4 (Term)**.** *Let Σ be a signature, let X be a denumerable set of individual variables typed over S_Σ, and let Σ_X be the signature obtained by extending Σ with X. The (many-sorted) set $T(\Sigma_X)$ of* terms *is the smallest set such that:*

$$\frac{}{X \subseteq T(\Sigma_X)} \qquad \frac{f : \tau_1 \times \cdots \tau_n \to \tau \in F_\Sigma \quad \forall i \in [1,n].\, \epsilon_i : \tau_i \in T(\Sigma_X)}{f(\epsilon_1, \ldots, \epsilon_n) : \tau \in T(\Sigma_X)}$$

Example 3.1.2 (Terms)**.** *Let be $\Sigma = (\{\tau\}, \{1 : \tau, \otimes : \tau \to \tau\})$ a monoidal signature with a single sort. Let be X a denumerable set of variables with $x, y, z \in X$, then some example of terms in $T(\Sigma_X)$ are $1 \otimes 1 : \tau$, $x \otimes y \otimes 1$ and $(x \otimes 1) \otimes (1 \otimes y)$. Examples from the previously defined graph algebra Σ are $s(x_{\tau_e})$ and $t(y_{\tau_e})$ which represent respectively the source vertex for an edge x_{τ_e} and the target vertex for an edge y_{τ_e}.*

3.2 Counterpart model

Definition 3.2.1. *Let Σ be a signature, and $\mathcal{A}$ the set of algebras over the signature Σ. A* counterpart model *M is a triple $(W, \rightsquigarrow, d)$ such that:*

- *W is a set of worlds;*
- *$d : W \to \mathcal{A}$ is a function assigning to each world $w \in W$ a Σ-algebra;*
- *$\rightsquigarrow \subseteq W \times (\mathcal{A} \rightharpoonup \mathcal{A}) \times W$ is the* accessibility relation *over W, enriched with (partial) homomorphisms (*counterpart relations*) between the algebras of the connected worlds, i.e. for every $(w_1, cr, w_2) \in \rightsquigarrow$ it must hold that $cr : d(w_1) \rightharpoonup d(w_2)$ is a (partial) homomorphism.*

As a shorthand notation, counterpart relations between two worlds in the accessibility relation, $(w_1, cr, w_2) \in \rightsquigarrow$, will be also denoted as $w_1 \overset{cr}{\rightsquigarrow} w_2$.

Definition 3.2.2. *Let $X, \mathcal{X}$ be denumerable sets of respectively first-order and second-order variables, and $M = (W, \rightsquigarrow, d)$ be a counterpart model over a signature Σ. A* variable assignment *$\sigma = (\sigma^1, \sigma^2)$ for a world $w \in W$ is a pair of (partial) functions such that $\sigma^1 : X \to d(w)$ and $\sigma^2 : \mathcal{X} \to 2^{d(w)}$.*

Given a term $\epsilon \in T(\Sigma_X)$ and an assignment $\sigma = (\sigma^1, \sigma^2)$, we will denote as $\sigma(\epsilon)$ or $\sigma^1(\epsilon)$ the lifting of σ^1 to the set $T(\Sigma_X)$. If any of the variables in ϵ are not in the domain of σ^1 than $\sigma(\epsilon)$ is also undefined. We will write $cr \circ \sigma$ as a shorthand for $(cr \circ \sigma^1, 2^{cr} \circ \sigma^2)$ where cr is a (partial) homomorphism between algebras and 2^{cr} is the lifting of cr to sets of values. Also, when clear from context, we will overload the notation for domain restriction, $\sigma|_A$ depending on the type of variables in the set A. If A is a set of first-order variables then $\sigma|_A = (\sigma^1|_A, \sigma^2)$, conversely if A is a set of second-order variables then $\sigma|_A = (\sigma^1, \sigma^2|_A)$.

The set of of pairs (σ, w) for σ a variable assignment over the world w in the counterpart model M is denoted as $\Omega(M)$. When clear from context, we will omit the counterpart model. The set of pairs where the domain of σ^1 is a subset of the first-order context Γ and the domain of σ^2 is exactly the second-order context Δ will be denoted as $\Omega_\Gamma\Delta$.

3.3 Syntax

Definition 3.3.1 (First-Order Linear Temporal Logic)**.** *Let Σ be a (multi-sorted) signature and X a denumerable set of variables typed over S_Σ. The set $\mathcal{F}_\Sigma$ of formulae for First-Order Linear Temporal Logic is the set generated by the following grammar:*

$$\phi ::= tt \mid x_\tau = \epsilon_\tau \mid \neg\phi \mid \phi \vee \phi \mid \exists x_\tau.\, \phi \mid X\phi \mid \phi\, U \phi$$

where ϵ is a term in $T(\Sigma_X)$, $\exists x_\tau$ ranges over variables of sort $\tau \in S_\Sigma$, O is a unary operator which states that ϕ must hold at the next step and U is a binary operator which states that the first formula must hold until the second formula holds at some point in the current or next steps.

Classical propositional logic and other temporal operators can be derived as for LTL, with the addition of the trivially derivable universal quantifier, $\forall x_\tau.\, \phi \equiv \neg\exists x_\tau.\, \neg\phi$.

3.4 Semantics

Definition 3.4.1 (First-order semantic function)**.** *Let ϕ be a formula-in-context, and Γ a first-order context. The evaluation of ϕ in the counterpart model M with context Γ is given by the function $[\![\cdot]\!]_\Gamma : \mathcal{F}_\Gamma \to \Omega_\Gamma$ defined as:*

$$\begin{aligned}
[\![tt]\!]_\Gamma &= \Omega_\Gamma \\
[\![x_\tau = \epsilon_\tau]\!]_\Gamma &= \{\, (\sigma, w) \in \Omega_\Gamma \mid \sigma(\epsilon) \textit{ is defined and } \sigma(x) = \sigma(\epsilon) \,\} \\
[\![\neg\phi]\!]_\Gamma &= \Omega_\Gamma \setminus [\![\phi]\!]_\Gamma \\
[\![\phi_1 \vee \phi_2]\!]_\Gamma &= [\![\phi_1]\!]_\Gamma \cup [\![\phi_2]\!]_\Gamma \\
[\![\exists x_\tau.\, \phi]\!]_\Gamma &= \{\, (\sigma|_\Gamma, w) \mid (\sigma, w) \in [\![\phi]\!]_{\Gamma,x} \,\} \\
[\![X\phi]\!]_\Gamma &= \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w') \in [\![\phi]\!]_\Gamma \,\} \\
[\![\phi_1\, U \phi_2]\!]_\Gamma &= [\![\phi_2]\!]_\Gamma \cup \{\, (\sigma, w) \in [\![\phi_1]\!]_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w') \in [\![\phi_1\, U \phi_2]\!]_\Gamma \,\}
\end{aligned}$$

The formula tt holds for any possible pair assignement-world. The predicate $=$ models the standard notion of equality for typed terms, thus $x_\tau = \epsilon_\tau$ is valid only if both terms share the same type τ and the evaluation for the term ϵ is defined and equal to the evaluation for the variable x. The negation of a formula is satisfied by all the pairs that do not satisfy the

formula without the negation. The semantic of a disjunction of formulae is the union of the semantics, within the same context. Existentially quantied formulae are evaluated in two steps, first we introduce a new variable x in the context Γ and we evaluate the formula in this new context Γ, x, then the set of pairs that satisfy the formula is the set of pairs in the new context Γ, x restricted to the original context Γ. Next we look at temporal operators. For formulae containing the next operator, e.g. $X\phi$, for each world w we search all the worlds w' related via the counterpart relation and we check wether an assignment σ in w satisfies the argument of the operator after being updated by the (partial) homomorphism. Formulae with the until operator, instead, are satisfied by all the pairs that satisfies the post-condition and by all the pairs that satisfy the pre-condition and evolve via the counterpart relation into a pair that also satisfy the complete formula with the until operator.

Definition 3.4.2. *A formula $\phi \in \mathcal{F}_\Sigma$ is called* valid for the counterpart model *M, denoted by $\vDash_M \phi$, if $(\sigma, w) \in [\![\phi]\!]_\Gamma$ for every world-assignement pair $(\sigma, w) \in \Omega_\Gamma(M)$ and context Γ such that the ϕ is well-scoped.*

Definition 3.4.3. *A formula $\phi \in \mathcal{F}_\Sigma$ is called a* consequence *of a set $F \subseteq \mathcal{F}_\Sigma$, denoted $F \vDash \phi$, if $\vDash_M \phi$ holds for every model M with $\vDash_M \psi$ for all $\psi \in F$.*

Definition 3.4.4.

A formula $\phi \in \mathcal{F}_\Sigma$ is called valid*, denoted by $\vDash \phi$, if $\emptyset \vDash \phi$ holds.*

3.5 Other operators

Let's explore the semantics of the other common operators defined in the previous chapters.

$$
\begin{aligned}
[\![\phi_1 \wedge \phi_2]\!]_\Gamma &= [\![\neg(\neg\phi_1 \vee \neg\phi_2)]\!]_\Gamma \\
&= \Omega_\Gamma \setminus [\![(\neg\phi_1 \vee \neg\phi_2)]\!]_\Gamma = \Omega_\Gamma \setminus ((\Omega_\Gamma \setminus [\![\phi_1]\!]_\Gamma) \cup (\Omega_\Gamma \setminus [\![\phi_2]\!]_\Gamma)) \\
&= [\![\phi_1]\!]_\Gamma \cap [\![\phi_2]\!]_\Gamma && (3.1)
\end{aligned}
$$

$$
[\![\phi_1 \to \phi_2]\!]_\Gamma = [\![\neg\phi_1 \vee \phi_2]\!]_\Gamma = (\Omega_\Gamma \setminus [\![\phi_1]\!]_\Gamma) \cup [\![\phi_2]\!]_\Gamma \qquad (3.2)
$$

$$
\begin{aligned}
[\![\phi_1 \leftrightarrow \phi_2]\!]_\Gamma &= [\![(\phi_1 \to \phi_2) \wedge (\phi_2 \to \phi_1)]\!]_\Gamma \\
&= ((\Omega_\Gamma \setminus [\![\phi_1]\!]_\Gamma) \cup [\![\phi_2]\!]_\Gamma) \cap ((\Omega_\Gamma \setminus [\![\phi_2]\!]_\Gamma) \cup [\![\phi_1]\!]_\Gamma) \\
&= ((\Omega_\Gamma \setminus [\![\phi_1]\!]_\Gamma) \cap (\Omega_\Gamma \setminus [\![\phi_2]\!]_\Gamma)) \cup ([\![\phi_1]\!]_\Gamma \cap [\![\phi_2]\!]_\Gamma) \\
&= ([\![\neg\phi_1 \wedge \neg\phi_2]\!]_\Gamma) \cup ([\![\phi_1 \wedge \phi_2]\!]_\Gamma) && (3.3)
\end{aligned}
$$

$$
[\![\forall x.\, \phi]\!]_\Gamma = [\![\neg\exists x.\, \neg\phi]\!]_\Gamma = \Omega_\Gamma \setminus \{\, (\sigma|_\Gamma, w) \mid (\sigma, w) \in \Omega_{\Gamma,x} \setminus [\![\phi]\!]_{\Gamma,x} \,\} \qquad (3.4)
$$

$$
\begin{aligned}
[\![F\phi]\!]_\Gamma &= [\![tt\, U \phi]\!]_\Gamma \\
&= [\![\phi]\!]_\Gamma \cup \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w') \in [\![F\phi]\!]_\Gamma \,\} \\
&= [\![\phi]\!]_\Gamma \cup [\![XF\phi]\!]_\Gamma = [\![\phi \vee XF\phi]\!]_\Gamma && (3.5)
\end{aligned}
$$

$$
\begin{aligned}
[\![G\phi]\!]_\Gamma &= [\![\neg F\neg\phi]\!]_\Gamma = [\![\neg(tt\, U \neg\phi)]\!]_\Gamma \\
&= \Omega_\Gamma \setminus ([\![\neg\phi]\!]_\Gamma \cup \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w') \in [\![F\neg\phi]\!]_\Gamma \,\}) \\
&= [\![\phi]\!]_\Gamma \cap (\Omega_\Gamma \setminus \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w') \in [\![F\neg\phi]\!]_\Gamma \,\}) \\
&= [\![\phi]\!]_\Gamma \cap \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w') \in [\![G\phi]\!]_\Gamma \,\} \\
&= [\![\phi]\!]_\Gamma \cap [\![XG\phi]\!]_\Gamma = [\![\phi \wedge XG\phi]\!]_\Gamma && (3.6)
\end{aligned}
$$

Chapter 4

Proof System

4.1 Axioms

Definition 4.1.1 (Axiomatic system)**.** *The axiomatic system for FO-LTL contains the following axioms:*

1. $\phi_1 \to (\phi_2 \to \phi_1)$;
2. $(\phi_1 \to (\phi_2 \to \phi_3)) \to ((\phi_1 \to \phi_2) \to (\phi_1 \to \phi_3))$;
3. $(\neg\phi_1 \to \neg\phi_2) \to (\phi_2 \to \phi_1)$;
4. $\neg X\phi \leftrightarrow X\neg\phi$;
5. $X(\phi_1 \to \phi_2) \to (X\phi_1 \to X\phi_2)$;
6. $\phi \to X\phi$ *if* ϕ *is rigid;*
7. $\phi_1 U \phi_2 \leftrightarrow \phi_2 \vee (\phi_1 \wedge X(\phi_1 U \phi_2))$;
8. $\phi_1 U \phi_2 \to F\phi_2$;
9. $\phi[t/x] \to \exists x.\, \phi$, *with* x *free in* ϕ;
10. $x = x$;
11. $x = y \to (\phi \to \phi[y/x])$.

And the following induction rules:

mp $\phi_1, \phi_1 \to \phi_2 \vdash \phi_2$;

nex $\phi \vdash X\phi$;

ind $\phi_1 \to \phi_3 \vee (\phi_2 \wedge X\phi_1) \vdash \phi_1 \to \phi_2 U \phi_3$;

par $\phi_1 \to \phi_2 \vdash \exists x.\, \phi_1 \to \phi_2$ *with* x *not free in* ϕ_2.

Theorem 4.1.1. *Let $\phi_1, \phi_2 \in \mathcal{F}_\Sigma$, $\vDash \phi_1 \to \phi_2$ if and only if $[\![\phi_1]\!] \subseteq [\![\phi_2]\!]$.*

Proof. Let M be a counterpart model and Γ a context such that ϕ_1 and ϕ_2 are well-scoped. By Equation (3.2), $[\![\phi_1 \to \phi_2]\!]_\Gamma = (\Omega \setminus [\![\phi_1]\!]_\Gamma) \cup [\![\phi_2]\!]_\Gamma$. Let $(\sigma, w) \in [\![\phi_1 \to \phi_2]\!]_\Gamma$. If $(\sigma, w) \in [\![\phi_1]\!]_\Gamma$ then it must follow that $(\sigma, w) \in [\![\phi_2]\!]_\Gamma$. □

Corollary 4.1.2. *Let $\phi_1, \phi_2 \in \mathcal{F}_\Sigma$, $\vDash \phi_1 \leftrightarrow \phi_2$ holds if and only if $[\![\phi_1]\!] = [\![\phi_2]\!]$.*

Lemma 4.1.3. *Let $\phi_1, \phi_2, \phi_3 \in \mathcal{F}_\Sigma$.*

1. *$\vDash \phi_1 \to (\phi_2 \to \phi_1)$;*
2. *$\vDash (\phi_1 \to (\phi_2 \to \phi_3)) \to ((\phi_1 \to \phi_2) \to (\phi_1 \to \phi_3))$;*
3. *$\vDash (\neg\phi_1 \to \neg\phi_2) \to (\phi_2 \to \phi_1)$.*

Proof. Let M be a counterpart model and Γ a context such that ϕ_1 and ϕ_2 are well-scoped.

1. From trivial applications of the semantic rules it follows that $[\![\phi_1 \to (\phi_2 \to \phi_1)]\!]_\Gamma = [\![\neg\phi_1]\!]_\Gamma \cup [\![\neg\phi_2]\!]_\Gamma \cup [\![\phi_1]\!]_\Gamma = \Omega_\Gamma$.
2. By Corollary 4.1.2 we show that $\vDash (\phi_1 \to (\phi_2 \to \phi_3)) \to ((\phi_1 \to \phi_2) \leftrightarrow (\phi_1 \to \phi_3))$. From the semantic rules:

$$[\![\phi_1 \to (\phi_2 \to \phi_3)]\!]_\Gamma = [\![\neg\phi_1]\!]_\Gamma \cup [\![\neg\phi_2]\!]_\Gamma \cup [\![\phi_3]\!]_\Gamma$$

$$\begin{aligned}[\![(\phi_1 \to \phi_2) \to (\phi_1 \to \phi_3)]\!]_\Gamma &= ([\![\phi_1]\!]_\Gamma \cap [\![\neg\phi_2]\!]_\Gamma) \cup [\![\neg\phi_1]\!]_\Gamma \cup [\![\phi_3]\!]_\Gamma \\ &= [\![\neg\phi_1]\!]_\Gamma \cup [\![\neg\phi_2]\!]_\Gamma \cup [\![\phi_3]\!]_\Gamma\end{aligned}$$

3. By Corollary 4.1.2 we show that $\vDash (\neg\phi_1 \to \neg\phi_2) \leftrightarrow (\phi_2 \to \phi_1)$. From the semantic rules:

$$[\![\neg\phi_1 \to \neg\phi_2]\!]_\Gamma = [\![\phi_1]\!]_\Gamma \cup [\![\neg\phi_2]\!]_\Gamma = [\![\neg\phi_2]\!]_\Gamma \cup [\![\phi_1]\!]_\Gamma = [\![\phi_2 \to \phi_1]\!]_\Gamma$$

□

Lemma 4.1.4. *Let $\phi \in \mathcal{F}_\Sigma$, $\vDash \neg X\phi \leftrightarrow X\neg\phi$.*

Proof. Let M be a counterpart model and Γ a context such that ϕ is well-scoped. By the definitions of the operators next and implication:

$$[\![\neg X\phi]\!]_\Gamma = \Omega_\Gamma \setminus \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w) \in [\![\phi]\!]_\Gamma \,\}.$$

By assumptions, for every world w there is always at least one world w' which is accessible from w, i.e. $w \overset{cr}{\rightsquigarrow} w'$, thus:

$$[\![\neg X\phi]\!]_\Gamma = \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w) \in \Omega_\Gamma \setminus [\![\phi]\!]_\Gamma \,\} = [\![X\neg\phi]\!]_\Gamma.$$

□

Lemma 4.1.5. *Let $\phi_1, \phi_2 \in \mathcal{F}_\Sigma$, $\vDash X(\phi_1 \to \phi_2) \to (X\phi_1 \to X\phi_2)$.*

Proof. Let M be a counterpart model and Γ a context such that ϕ_1 and ϕ_2 are well-scoped. By definition of the operators next and implication:

$$\begin{aligned}
[\![X(\phi_1 \to \phi_2)]\!]_\Gamma &= \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w) \in [\![\neg\phi_1]\!]_\Gamma \cup [\![\phi_2]\!]_\Gamma \,\} \\
&= \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w) \in [\![\neg\phi_1]\!]_\Gamma \,\} \\
&\qquad \cup \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w) \in [\![\phi_2]\!]_\Gamma \,\} \\
&= [\![X\neg\phi_1]\!]_\Gamma \cup [\![X\phi_2]\!]_\Gamma \\
&= [\![\neg X\phi_1]\!]_\Gamma \cup [\![X\phi_2]\!]_\Gamma \\
&= [\![X\phi_1 \to X\phi_2]\!]_\Gamma
\end{aligned}$$

□

Lemma 4.1.6. *Let $\phi \in \mathcal{F}_\Sigma$ be a rigid formula, $\vDash \phi \to X\phi$.*

Proof. Let M be a counterpart model and Γ a context such that ϕ is well-scoped. Let $(\sigma, w) \in [\![\phi]\!]_\Gamma$ and w' such that $w \overset{cr}{\rightsquigarrow} w'$. By definition, $(\sigma, w) \in [\![X\phi]\!]_\Gamma$ iff $(cr \circ \sigma, w') \in [\![\phi]\!]_\Gamma$. Since ϕ is a rigid formula, $cr \circ \sigma = \sigma$, therefore $(\sigma, w') \in [\![\phi]\!]_\Gamma$. □

Lemma 4.1.7. *Let $\phi_1, \phi_2 \in \mathcal{F}_\Sigma$, $\vDash \phi_1\, U \phi_2 \leftrightarrow \phi_2 \vee (\phi_1 \wedge X(\phi_1\, U \phi_2))$.*

Proof. Let M be a counterpart model and Γ a context such that ϕ_1 and ϕ_2 is well-scoped.

$$\begin{aligned}
[\![\phi_1\, U \phi_2]\!]_\Gamma &= [\![\phi_2]\!]_\Gamma \cup \{\, (\sigma, w) \in [\![\phi_1]\!]_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w') \in [\![\phi_1\, U \phi_2]\!]_\Gamma \,\} \\
&= [\![\phi_2]\!]_\Gamma \cup ([\![\phi_1]\!]_\Gamma \cap \{\, (\sigma, w) \in \Omega_\Gamma \mid \forall w \overset{cr}{\rightsquigarrow} w'.\, (cr \circ \sigma, w') \in [\![\phi_1\, U \phi_2]\!]_\Gamma \,\}) \\
&= [\![\phi_2]\!]_\Gamma \cup ([\![\phi_1]\!]_\Gamma \cap [\![X(\phi_1\, U \phi_2)]\!]_\Gamma) \\
&= [\![\phi_2 \wedge (\phi_1 \vee X(\phi_1\, U \phi_2))]\!]_\Gamma
\end{aligned}$$

□

Lemma 4.1.8. *Let $\phi_1, \phi_2 \in \mathcal{F}_\Sigma$, $\vDash \phi_1\, U \phi_2 \to F\phi_1$.*

Proof. Let M be a counterpart model and Γ a context such that ϕ_1 and ϕ_2 is well-scoped. By the definitions of the operators:

$$\begin{aligned}
[\![\phi_1\, U \phi_2]\!]_\Gamma &= [\![\phi_2]\!]_\Gamma \cup ([\![\phi_1]\!]_\Gamma \cap [\![X(\phi_1\, U \phi_2)]\!]_\Gamma) \\
[\![F\phi_2]\!]_\Gamma &= [\![\phi_2]\!]_\Gamma \cup [\![XF\phi_2]\!]_\Gamma
\end{aligned}$$

However it's trivialy to see that $[\![\phi_1]\!]_\Gamma \cap [\![X(\phi_1\, U \phi_2)]\!]_\Gamma$ is a subset of $[\![XF\phi_2]\!]_\Gamma$, hence the conclusion follows from Theorem 4.1.1.

□

Lemma 4.1.9. *Let $\phi \in \mathcal{F}_\Sigma$ with $x \in X$ free in ϕ, $\vDash \phi[t/x] \to \exists x.\, \phi$.*

Proof. Let M be a counterpart model and Γ a context such that $\phi[t/x]$ is well-scoped. Let $(\sigma, w) \in [\![\phi[t/x]]\!]_\Gamma$, then $(\sigma[t/x], w) \in [\![\phi]\!]_{\Gamma,x}$. However $\sigma[t/x]|_\Gamma = \sigma$ thus $(\sigma, w) \in [\![\exists x.\, \phi]\!]_\Gamma$. □

Lemma 4.1.10. *Let $\phi \in \mathcal{F}_\Sigma$ and $x, y \in X$,*

1. *$x = x$ if x is defined;*
2. *$x = y \to (\phi \to \phi[y/x])$ if x and y are defined.*

Proof. Let M be a counterpart model and Γ a context such that ϕ is well-scoped.

1. foo
2. bar

□

Lemma 4.1.11. *If $F \vDash \phi_1$ and $F \vDash \phi_1 \to \phi_2$, then $F \vDash \phi_2$.*

Proof. Let M be a model that satisfies $\vDash_M \psi$ for every $\psi \in F$ and Γ a context such that ϕ_1 and ϕ_2 are well-scoped. By definition $[\![\phi_1 \to \phi_2]\!]_\Gamma = [\![\neg\phi_1]\!]_\Gamma \cup [\![\phi_2]\!]_\Gamma = \Omega_\Gamma$, and by hypothesis $[\![\neg\phi_1]\!]_\Gamma = \emptyset$, hence it must follow that $[\![\phi_2]\!]_\Gamma = \Omega_\Gamma$. □

Lemma 4.1.12. *If $F \vDash \phi$, then $F \vDash X\phi$ and $F \vDash G\phi$.*

Proof. Let M be a model that satisfies $\vDash_M \psi$ for every $\psi \in F$ and Γ a context such that ϕ is well-scoped. Then $[\![\phi]\!]_\Gamma = \Omega_\Gamma$. In particular, let $(\sigma, w) \in \Omega_\Gamma$, for every w' such that $w \overset{cr}{\rightsquigarrow} w'$ it's true that $(cr \circ \sigma, w') \in \Omega_\Gamma$ hence $F \vDash X\phi$. $F \vDash G\phi$ follows trivially by Equation (3.6). □

Lemma 4.1.13. *If $F \vDash \phi_1 \to \phi_2$ and $F \vDash \phi_1 \to X\phi_1$, then $F \vDash \phi_1 \to G\phi_2$.*

Proof. Let M be a model that satisfies $\vDash_M \psi$ for every $\psi \in F$ and Γ a context such that ϕ_1 and ϕ_2 are well-scoped. $F \vDash \phi_1 \to G\phi_2$ holds trivially if $[\![\phi_1]\!]_\Gamma = \emptyset$, so assume that $[\![\phi_1]\!]_\Gamma = \Omega_\Gamma$. Let $(\sigma, w) \in \Omega_\Gamma$, by the assumption $F \vDash \phi_1 \to X\phi_1$ it follows that $(\sigma, w) \in [\![X\phi_1]\!]_\Gamma$, and for every w' such that $w \overset{cr}{\rightsquigarrow} w'$ it's true that $(cr \circ \sigma, w') \in \Omega_\Gamma$ hence for the same reasoning $(cr \circ \sigma, w') \in [\![\phi_1]\!]_\Gamma$ and $(cr \circ \sigma, w') \in [\![X\phi_1]\!]_\Gamma$, thus inductively for any infinite sequence of accessible worlds starting with w it always holds both $(\sigma_n, w_n) \in [\![\phi_1]\!]_\Gamma$ and $(\sigma_n, w_n) \in [\![X\phi_1]\!]_\Gamma$, where w_n is the n-th world in the sequence and σ_n is constructed by composing the counterpart relations with the starting assignement σ. The assumption $F \vDash \phi_1 \to \phi_2$ implies that for any infinite sequence of accessible worlds starting with w it always holds $(\sigma_n, w_n) \in [\![\phi_2]\!]_\Gamma$, thus by definition of the G temporal operator $(\sigma, w) \in [\![\phi_1 \to G\phi_2]\!]_\Gamma$. □

Lemma 4.1.14. *If $F \vDash \phi_1 \to \phi_2$ and x not free in ϕ_2, then $F \vDash \exists x.\, \phi_1 \to \phi_2$.*

Proof. Let M be a model that satisfies $\vDash_M \psi$ for every $\psi \in F$ and Γ a context such that ϕ_1 and ϕ_2 are well-scoped, then $\vDash_M \phi_1 \to \phi_2$. Assume $(\sigma, w) \notin [\![\exists x.\, \phi_1 \to \phi_2]\!]_\Gamma$ for some $(\sigma, w) \in \Omega_\Gamma$, hence $(\sigma, w) \in [\![\exists x.\, \phi_1]\!]_\Gamma$ and $(\sigma, w) \notin [\![\phi_2]\!]_\Gamma$. Then there is a σ' for the context Γ, x such that $\sigma'|_\Gamma = \sigma$ and $(\sigma', w) \in [\![\phi_1]\!]_{\Gamma,x}$. Since ϕ_2 does not contain x as a free variable, $(\sigma', w) \notin [\![\phi_2]\!]_{\Gamma,x}$, therefore $(\sigma', w) \notin [\![\phi_1 \to \phi_2]\!]_{\Gamma,x}$ which is a contradiction to $\vDash_M \phi_1 \to \phi_2$. □

Theorem 4.1.15 (Soundness)**.** *Let $\phi \in \mathcal{F}_\Sigma$ and $F \subseteq \mathcal{F}_\Sigma$, if $F \vdash \phi$ then $F \vDash \phi$.*

Proof. By induction on the derivation of ϕ from F:

1. if ϕ is an axiom: lorem ipsum dolor sit amet;
2. if $\phi \in F$ then $F \vDash \phi$ holds trivially;
3. if ϕ is the conclusion of a (mp) rule with premises $F \vdash \psi$ and $F \vdash \psi \to \phi$: by induction hypothesis we have $F \vDash \psi$ and $F \vDash \psi \to \phi$, hence $F \vDash \phi$ follows by Lemma 4.1.11;
4. if ϕ is the conclusion of a (nex) rule with premises $F \vdash \psi$, thus $\phi \equiv X\psi$: by induction hypothesis we have $F \vDash \psi$, hence $F \vDash X\psi$ follows by Lemma 4.1.12;
5. if ϕ is the conclusion of a (ind) rule with premises $F \vdash \psi_1 \to \psi_2$ and $F \vdash \psi_1 \to X\psi_1$, thus $\phi \equiv \psi_1 \to G\psi_2$: by induction hypothesis we have $F \vDash \psi_1 \to \psi_2$ and $F \vDash \psi_1 \to X\psi_2$, hence $F \vDash \psi_1 \to G\psi_2$ follows by Lemma 4.1.13;
6. if ϕ is the conclusion of a (par) rule with premises $F \vdash \psi_1 \to \psi_2$, thus $\phi \equiv \exists x.\, \psi_1 \to \psi_2$ with x not free in ψ_2: by induction hypothesis we have $F \vDash \psi_1 \to \psi_2$, hence $F \vDash \exists x \psi_1 \to \psi_2$ follows by Lemma 4.1.14.

□

Theorem 4.1.16. *Let $\phi_1, \phi_2 \in \mathcal{F}_\Sigma$ and $F \subseteq \mathcal{F}_\Sigma$. If $F \cup \{\, \phi_1 \,\} \vdash \phi_2$ and this deriviation of ϕ_2 does not contains application of the rule (par) for a variable occurring free in ϕ_1, then $F \vdash G\phi_1 \to \phi_2$.*