An Efficient Normalisation Procedure for Linear Temporal Logic: Isabelle/HOL Formalisation

Salomon Sickert

December 14, 2021

Abstract

In the mid 80s, Lichtenstein, Pnueli, and Zuck proved a classical theorem stating that every formula of Past LTL (the extension of LTL with past operators) is equivalent to a formula of the form $\bigwedge_{i=1}^{n} \mathbf{GF}\varphi_i \vee \mathbf{FG}\psi_i$, where φ_i and ψ_i contain only past operators [3, 6]. Some years later, Chang, Manna, and Pnueli built on this result to derive a similar normal form for LTL [2]. Both normalisation procedures have a non-elementary worst-case blow-up, and follow an involved path from formulas to counter-free automata to star-free regular expressions and back to formulas. We improve on both points. We present an executable formalisation of a direct and purely syntactic normalisation procedure for LTL yielding a normal form, comparable to the one by Chang, Manna, and Pnueli, that has only a single exponential blow-up.

Contents

1 Overview

This document contains the formalisation of the central results appearing in [4, Sections 4-6]. We refer the interested reader to [4] or to the extended version [5] for an introduction to the topic, related work, intuitive explanations of the proofs, and an application of the normalisation procedure, namely, a translation from LTL to deterministic automata.

The central result of this document is the following theorem:

Theorem 1. *Let φ be an LTL formula and let Δ_2, Σ_1, Σ_2, and Π_1 be the classes of LTL formulas from Definition 2. Then φ is equivalent to the following formula from the class Δ_2:*

$$\bigvee_{\substack{M \subseteq \mu(\varphi) \\ N \subseteq \nu(\varphi)}} \left(\varphi[M]_2^\Sigma \wedge \bigwedge_{\psi \in M} \mathbf{GF}(\psi[N]_1^\Sigma) \wedge \bigwedge_{\psi \in N} \mathbf{FG}(\psi[M]_1^\Pi) \right)$$

where $\psi[M]_2^\Sigma$, $\psi[N]_1^\Sigma$, and $\psi[M]_1^\Pi$ are functions mapping ψ to a formula from Σ_2, Σ_1, and Π_1, respectively.

Definition 2 (Adapted from [1]). *We define the following classes of LTL formulas:*

- *The class $\Sigma_0 = \Pi_0 = \Delta_0$ is the least set containing all atomic propositions and their negations, and is closed under the application of conjunction and disjunction.*
- *The class Σ_{i+1} is the least set containing Π_i and is closed under the application of conjunction, disjunction, and the* **X**, **U**, *and* **M** *operators.*
- *The class Π_{i+1} is the least set containing Σ_i and is closed under the application of conjunction, disjunction, and the* **X**, **R**, *and* **W** *operators.*
- *The class Δ_{i+1} is the least set containing Σ_{i+1} and Π_{i+1} and is closed under the application of conjunction and disjunction.*

2 A Normal Form for Linear Temporal Logic

theory *Normal-Form* **imports**
  LTL-Master-Theorem.Master-Theorem
begin

2.1 LTL Equivalences

Several valid laws of LTL relating strong and weak operators that are useful later.

lemma *ltln-strong-weak-2*:
$w \models_n \varphi\ U_n\ \psi \longleftrightarrow w \models_n (\varphi\ and_n\ F_n\ \psi)\ W_n\ \psi$ (**is** *?thesis1*)
$w \models_n \varphi\ M_n\ \psi \longleftrightarrow w \models_n \varphi\ R_n\ (\psi\ and_n\ F_n\ \varphi)$ (**is** *?thesis2*)
⟨*proof*⟩

lemma *ltln-weak-strong-2*:
$w \models_n \varphi\ W_n\ \psi \longleftrightarrow w \models_n \varphi\ U_n\ (\psi\ or_n\ G_n\ \varphi)$ (**is** *?thesis1*)
$w \models_n \varphi\ R_n\ \psi \longleftrightarrow w \models_n (\varphi\ or_n\ G_n\ \psi)\ M_n\ \psi$ (**is** *?thesis2*)
⟨*proof*⟩

2.2 $\psi[M]_1^\Pi$, $\psi[N]_1^\Sigma$, $\psi[M]_2^\Sigma$, and $\psi[N]_2^\Pi$

The following four functions use "promise sets", named M or N, to rewrite arbitrary formulas into formulas from the class Σ_1-, Σ_2-, Π_1-, and Π_2, respectively. In general the obtained formulas are not equivalent, but under some conditions (as outlined below) they are.

no-notation *FG-advice* (-[-]$_\mu$ *[90,60] 89*)
no-notation *GF-advice* (-[-]$_\nu$ *[90,60] 89*)

notation *FG-advice* (-[-]$_{\Sigma 1}$ *[90,60] 89*)
notation *GF-advice* (-[-]$_{\Pi 1}$ *[90,60] 89*)

fun *flatten-sigma-2*:: *'a ltln* ⇒ *'a ltln set* ⇒ *'a ltln* (-[-]$_{\Sigma 2}$)
where
$(\varphi\ U_n\ \psi)[M]_{\Sigma 2} = (\varphi[M]_{\Sigma 2})\ U_n\ (\psi[M]_{\Sigma 2})$
$\mid (\varphi\ W_n\ \psi)[M]_{\Sigma 2} = (\varphi[M]_{\Sigma 2})\ U_n\ ((\psi[M]_{\Sigma 2})\ or_n\ (G_n\ \varphi[M]_{\Pi 1}))$
$\mid (\varphi\ M_n\ \psi)[M]_{\Sigma 2} = (\varphi[M]_{\Sigma 2})\ M_n\ (\psi[M]_{\Sigma 2})$
$\mid (\varphi\ R_n\ \psi)[M]_{\Sigma 2} = ((\varphi[M]_{\Sigma 2})\ or_n\ (G_n\ \psi[M]_{\Pi 1}))\ M_n\ (\psi[M]_{\Sigma 2})$
$\mid (\varphi\ and_n\ \psi)[M]_{\Sigma 2} = (\varphi[M]_{\Sigma 2})\ and_n\ (\psi[M]_{\Sigma 2})$
$\mid (\varphi\ or_n\ \psi)[M]_{\Sigma 2} = (\varphi[M]_{\Sigma 2})\ or_n\ (\psi[M]_{\Sigma 2})$
$\mid (X_n\ \varphi)[M]_{\Sigma 2} = X_n\ (\varphi[M]_{\Sigma 2})$
$\mid \varphi[M]_{\Sigma 2} = \varphi$

fun *flatten-pi-2* :: *'a ltln* ⇒ *'a ltln set* ⇒ *'a ltln* (-[-]$_{\Pi 2}$)
where
$(\varphi\ W_n\ \psi)[N]_{\Pi 2} = (\varphi[N]_{\Pi 2})\ W_n\ (\psi[N]_{\Pi 2})$
$\mid (\varphi\ U_n\ \psi)[N]_{\Pi 2} = (\varphi[N]_{\Pi 2}\ and_n\ (F_n\ \psi[N]_{\Sigma 1}))\ W_n\ (\psi[N]_{\Pi 2})$
$\mid (\varphi\ R_n\ \psi)[N]_{\Pi 2} = (\varphi[N]_{\Pi 2})\ R_n\ (\psi[N]_{\Pi 2})$
$\mid (\varphi\ M_n\ \psi)[N]_{\Pi 2} = (\varphi[N]_{\Pi 2})\ R_n\ ((\psi[N]_{\Pi 2})\ and_n\ (F_n\ \varphi[N]_{\Sigma 1}))$

| $(\varphi\ and_n\ \psi)[N]_{\Pi 2} = (\varphi[N]_{\Pi 2})\ and_n\ (\psi[N]_{\Pi 2})$
| $(\varphi\ or_n\ \psi)[N]_{\Pi 2} = (\varphi[N]_{\Pi 2})\ or_n\ (\psi[N]_{\Pi 2})$
| $(X_n\ \varphi)[N]_{\Pi 2} = X_n\ (\varphi[N]_{\Pi 2})$
| $\varphi[N]_{\Pi 2} = \varphi$

lemma *GF-advice-restriction*:
$\varphi[\mathcal{GF}\ (\varphi\ W_n\ \psi)\ w]_{\Pi 1} = \varphi[\mathcal{GF}\ \varphi\ w]_{\Pi 1}$
$\psi[\mathcal{GF}\ (\varphi\ R_n\ \psi)\ w]_{\Pi 1} = \psi[\mathcal{GF}\ \psi\ w]_{\Pi 1}$
⟨*proof*⟩

lemma *FG-advice-restriction*:
$\psi[\mathcal{FG}\ (\varphi\ U_n\ \psi)\ w]_{\Sigma 1} = \psi[\mathcal{FG}\ \psi\ w]_{\Sigma 1}$
$\varphi[\mathcal{FG}\ (\varphi\ M_n\ \psi)\ w]_{\Sigma 1} = \varphi[\mathcal{FG}\ \varphi\ w]_{\Sigma 1}$
⟨*proof*⟩

lemma *flatten-sigma-2-intersection*:
$M \cap subformulas_\mu\ \varphi \subseteq S \Longrightarrow \varphi[M \cap S]_{\Sigma 2} = \varphi[M]_{\Sigma 2}$
⟨*proof*⟩

lemma *flatten-sigma-2-intersection-eq*:
$M \cap subformulas_\mu\ \varphi = M' \Longrightarrow \varphi[M']_{\Sigma 2} = \varphi[M]_{\Sigma 2}$
⟨*proof*⟩

lemma *flatten-sigma-2-monotone*:
$w \models_n \varphi[M]_{\Sigma 2} \Longrightarrow M \subseteq M' \Longrightarrow w \models_n \varphi[M']_{\Sigma 2}$
⟨*proof*⟩

lemma *flatten-pi-2-intersection*:
$N \cap subformulas_\nu\ \varphi \subseteq S \Longrightarrow \varphi[N \cap S]_{\Pi 2} = \varphi[N]_{\Pi 2}$
⟨*proof*⟩

lemma *flatten-pi-2-intersection-eq*:
$N \cap subformulas_\nu\ \varphi = N' \Longrightarrow \varphi[N']_{\Pi 2} = \varphi[N]_{\Pi 2}$
⟨*proof*⟩

lemma *flatten-pi-2-monotone*:
$w \models_n \varphi[N]_{\Pi 2} \Longrightarrow N \subseteq N' \Longrightarrow w \models_n \varphi[N']_{\Pi 2}$
⟨*proof*⟩

lemma *ltln-weak-strong-stable-words-1*:
$w \models_n (\varphi\ W_n\ \psi) \longleftrightarrow w \models_n \varphi\ U_n\ (\psi\ or_n\ (G_n\ \varphi[\mathcal{GF}\ \varphi\ w]_{\Pi 1}))$ (**is** *?lhs* $\longleftrightarrow$ *?rhs*)
⟨*proof*⟩

lemma *ltln-weak-strong-stable-words-2*:
$w \models_n (\varphi\ R_n\ \psi) \longleftrightarrow w \models_n (\varphi\ or_n\ (G_n\ \psi[\mathcal{GF}\ \psi\ w]_{\Pi 1}))\ M_n\ \psi$ (**is** *?lhs* $\longleftrightarrow$ *?rhs*)
⟨*proof*⟩

lemma *ltln-weak-strong-stable-words*:
$w \models_n (\varphi\ W_n\ \psi) \longleftrightarrow w \models_n \varphi\ U_n\ (\psi\ or_n\ (G_n\ \varphi[\mathcal{GF}\ (\varphi\ W_n\ \psi)\ w]_{\Pi 1}))$
$w \models_n (\varphi\ R_n\ \psi) \longleftrightarrow w \models_n (\varphi\ or_n\ (G_n\ \psi[\mathcal{GF}\ (\varphi\ R_n\ \psi)\ w]_{\Pi 1}))\ M_n\ \psi$
⟨*proof*⟩

lemma *flatten-sigma-2-IH-lifting*:
assumes $\psi \in$ *subfrmlsn* φ
assumes *suffix i w* $\models_n \psi[\mathcal{GF}\ \psi\ (\textit{suffix } i\ w)]_{\Sigma 2} =$ *suffix i w* $\models_n \psi$
shows *suffix i w* $\models_n \psi[\mathcal{GF}\ \varphi\ w]_{\Sigma 2} =$ *suffix i w* $\models_n \psi$
⟨*proof*⟩

lemma *flatten-sigma-2-correct*:
$w \models_n \varphi[\mathcal{GF}\ \varphi\ w]_{\Sigma 2} \longleftrightarrow w \models_n \varphi$
⟨*proof*⟩

lemma *ltln-strong-weak-stable-words-1*:
$w \models_n \varphi\ U_n\ \psi \longleftrightarrow w \models_n (\varphi\ and_n\ (F_n\ \psi[\mathcal{FG}\ \psi\ w]_{\Sigma 1}))\ W_n\ \psi$ (**is** *?lhs* $\longleftrightarrow$ *?rhs*)
⟨*proof*⟩

lemma *ltln-strong-weak-stable-words-2*:
$w \models_n \varphi\ M_n\ \psi \longleftrightarrow w \models_n \varphi\ R_n\ (\psi\ and_n\ (F_n\ \varphi[\mathcal{FG}\ \varphi\ w]_{\Sigma 1}))$ (**is** *?lhs* $\longleftrightarrow$ *?rhs*)
⟨*proof*⟩

lemma *ltln-strong-weak-stable-words*:
$w \models_n \varphi\ U_n\ \psi \longleftrightarrow w \models_n (\varphi\ and_n\ (F_n\ \psi[\mathcal{FG}\ (\varphi\ U_n\ \psi)\ w]_{\Sigma 1}))\ W_n\ \psi$
$w \models_n \varphi\ M_n\ \psi \longleftrightarrow w \models_n \varphi\ R_n\ (\psi\ and_n\ (F_n\ \varphi[\mathcal{FG}\ (\varphi\ M_n\ \psi)\ w]_{\Sigma 1}))$
⟨*proof*⟩

lemma *flatten-pi-2-IH-lifting*:
assumes $\psi \in$ *subfrmlsn* φ
assumes *suffix i w* $\models_n \psi[\mathcal{FG}\ \psi\ (\textit{suffix } i\ w)]_{\Pi 2} =$ *suffix i w* $\models_n \psi$
shows *suffix i w* $\models_n \psi[\mathcal{FG}\ \varphi\ w]_{\Pi 2} =$ *suffix i w* $\models_n \psi$
⟨*proof*⟩

lemma *flatten-pi-2-correct*:
$w \models_n \varphi[\mathcal{FG}\ \varphi\ w]_{\Pi 2} \longleftrightarrow w \models_n \varphi$
⟨*proof*⟩

2.3 Main Theorem

Using the four previously defined functions we obtain our normal form.

theorem *normal-form-with-flatten-sigma-2*:
$w \models_n \varphi \longleftrightarrow$
$(\exists\, M \subseteq subformulas_\mu\ \varphi.\ \exists\, N \subseteq subformulas_\nu\ \varphi.$
$w \models_n \varphi[M]_{\Sigma 2} \wedge (\forall\, \psi \in M.\ w \models_n G_n\ (F_n\ \psi[N]_{\Sigma 1})) \wedge (\forall\, \psi \in N.\ w \models_n$
$F_n\ (G_n\ \psi[M]_{\Pi 1})))$ (**is** *?lhs* $\longleftrightarrow$ *?rhs*)
⟨*proof*⟩

theorem *normal-form-with-flatten-pi-2*:
$w \models_n \varphi \longleftrightarrow$
$(\exists\, M \subseteq subformulas_\mu\ \varphi.\ \exists\, N \subseteq subformulas_\nu\ \varphi.$
$w \models_n \varphi[N]_{\Pi 2} \wedge (\forall\, \psi \in M.\ w \models_n G_n\ (F_n\ \psi[N]_{\Sigma 1})) \wedge (\forall\, \psi \in N.\ w \models_n$
$F_n\ (G_n\ \psi[M]_{\Pi 1})))$ (**is** *?lhs* $\longleftrightarrow$ *?rhs*)
⟨*proof*⟩

end

3 Size Bounds

We prove an exponential upper bound for the normalisation procedure. Moreover, we show that the number of proper subformulas, which correspond to states very-weak alternating automata (A1W), is only linear for each disjunct.

theory *Normal-Form-Complexity* **imports**
Normal-Form
begin

3.1 Inequalities and Identities

lemma *inequality-1*:
$y > 0 \Longrightarrow y + 3 \leq (2 :: nat)\ \hat{}\ (y + 1)$
⟨*proof*⟩

lemma *inequality-2*:
$x > 0 \Longrightarrow y > 0 \Longrightarrow ((2 :: nat)\ \hat{}\ (x + 1)) + (2\ \hat{}\ (y + 1)) \leq (2\ \hat{}\ (x$
$+ y + 1))$
⟨*proof*⟩

lemma *size-gr-0*:
$size\ (\varphi :: 'a\ ltln) > 0$
⟨*proof*⟩

lemma *sum-associative*:
finite $X \Longrightarrow (\sum x \in X.\ f\, x + c) = (\sum x \in X.\ f\, x) + \mathit{card}\ X * c$
$\langle \mathit{proof} \rangle$

3.2 Length

We prove that the length (size) of the resulting formula in normal form is at most exponential.

lemma *flatten-sigma-1-length*:
$\mathit{size}\ (\varphi[N]_{\Sigma 1}) \leq \mathit{size}\ \varphi$
$\langle \mathit{proof} \rangle$

lemma *flatten-pi-1-length*:
$\mathit{size}\ (\varphi[M]_{\Pi 1}) \leq \mathit{size}\ \varphi$
$\langle \mathit{proof} \rangle$

lemma *flatten-sigma-2-length*:
$\mathit{size}\ (\varphi[M]_{\Sigma 2}) \leq 2\ \hat{}\ (\mathit{size}\ \varphi + 1)$
$\langle \mathit{proof} \rangle$

lemma *flatten-pi-2-length*:
$\mathit{size}\ (\varphi[N]_{\Pi 2}) \leq 2\ \hat{}\ (\mathit{size}\ \varphi + 1)$
$\langle \mathit{proof} \rangle$

definition *normal-form-length-upper-bound*
where *normal-form-length-upper-bound* φ
$\equiv (2 :: \mathit{nat})\ \hat{}\ (\mathit{size}\ \varphi) * (2\ \hat{}\ (\mathit{size}\ \varphi + 1) + 2 * (\mathit{size}\ \varphi + 2)\ \hat{}\ 2)$

definition *normal-form-disjunct-with-flatten-pi-2-length*
where *normal-form-disjunct-with-flatten-pi-2-length* $\varphi\ M\ N$
$\equiv \mathit{size}\ (\varphi[N]_{\Pi 2}) + (\sum \psi \in M.\ \mathit{size}\ (\psi[N]_{\Sigma 1}) + 2) + (\sum \psi \in N.\ \mathit{size}\ (\psi[M]_{\Pi 1}) + 2)$

definition *normal-form-with-flatten-pi-2-length*
where *normal-form-with-flatten-pi-2-length* φ
$\equiv \sum (M, N) \in \{(M, N) \mid M\ N.\ M \subseteq \mathit{subformulas}_\mu\ \varphi \wedge N \subseteq \mathit{subformulas}_\nu\ \varphi\}.$ *normal-form-disjunct-with-flatten-pi-2-length* $\varphi\ M\ N$

definition *normal-form-disjunct-with-flatten-sigma-2-length*
where *normal-form-disjunct-with-flatten-sigma-2-length* $\varphi\ M\ N$
$\equiv \mathit{size}\ (\varphi[M]_{\Sigma 2}) + (\sum \psi \in M.\ \mathit{size}\ (\psi[N]_{\Sigma 1}) + 2) + (\sum \psi \in N.\ \mathit{size}\ (\psi[M]_{\Pi 1}) + 2)$

definition *normal-form-with-flatten-sigma-2-length*
where *normal-form-with-flatten-sigma-2-length* φ
$\equiv \sum (M, N) \in \{(M, N) \mid M\, N.\ M \subseteq subformulas_\mu\ \varphi \wedge N \subseteq subformulas_\nu\ \varphi\}.$ *normal-form-disjunct-with-flatten-sigma-2-length* $\varphi\ M\ N$

lemma *normal-form-disjunct-length-upper-bound*:
assumes
$M \subseteq subformulas_\mu\ \varphi$
$N \subseteq subformulas_\nu\ \varphi$
shows
normal-form-disjunct-with-flatten-sigma-2-length $\varphi\ M\ N \leq 2\ \hat{}\ (size\ \varphi + 1) + 2 * (size\ \varphi + 2)\ \hat{}\ 2$ (**is** *?thesis1*)
normal-form-disjunct-with-flatten-pi-2-length $\varphi\ M\ N \leq 2\ \hat{}\ (size\ \varphi + 1) + 2 * (size\ \varphi + 2)\ \hat{}\ 2$ (**is** *?thesis2*)
⟨*proof*⟩

theorem *normal-form-length-upper-bound*:
normal-form-with-flatten-sigma-2-length $\varphi \leq$ *normal-form-length-upper-bound* φ (**is** *?thesis1*)
normal-form-with-flatten-pi-2-length $\varphi \leq$ *normal-form-length-upper-bound* φ (**is** *?thesis2*)
⟨*proof*⟩

3.3 Proper Subformulas

We prove that the number of (proper) subformulas (sf) in a disjunct is linear and not exponential.

fun *sf* :: *'a ltln* ⇒ *'a ltln set*
where
$sf\ (\varphi\ and_n\ \psi) = sf\ \varphi \cup sf\ \psi$
$\mid sf\ (\varphi\ or_n\ \psi) = sf\ \varphi \cup sf\ \psi$
$\mid sf\ (X_n\ \varphi) = \{X_n\ \varphi\} \cup sf\ \varphi$
$\mid sf\ (\varphi\ U_n\ \psi) = \{\varphi\ U_n\ \psi\} \cup sf\ \varphi \cup sf\ \psi$
$\mid sf\ (\varphi\ R_n\ \psi) = \{\varphi\ R_n\ \psi\} \cup sf\ \varphi \cup sf\ \psi$
$\mid sf\ (\varphi\ W_n\ \psi) = \{\varphi\ W_n\ \psi\} \cup sf\ \varphi \cup sf\ \psi$
$\mid sf\ (\varphi\ M_n\ \psi) = \{\varphi\ M_n\ \psi\} \cup sf\ \varphi \cup sf\ \psi$
$\mid sf\ \varphi = \{\}$

lemma *sf-finite*:
finite $(sf\ \varphi)$
⟨*proof*⟩

lemma *sf-subset-subfrmlsn*:
$sf\ \varphi \subseteq subfrmlsn\ \varphi$
⟨*proof*⟩

lemma *sf-size*:
$\psi \in sf\ \varphi \Longrightarrow size\ \psi \leq size\ \varphi$
⟨*proof*⟩

lemma *sf-sf-subset*:
$\psi \in sf\ \varphi \Longrightarrow sf\ \psi \subseteq sf\ \varphi$
⟨*proof*⟩

lemma *subfrmlsn-sf-subset*:
$\psi \in subfrmlsn\ \varphi \Longrightarrow sf\ \psi \subseteq sf\ \varphi$
⟨*proof*⟩

lemma *sf-subset-insert*:
assumes $sf\ \varphi \subseteq insert\ \varphi\ X$
assumes $\psi \in subfrmlsn\ \varphi$
assumes $\varphi \neq \psi$
shows $sf\ \psi \subseteq X$
⟨*proof*⟩

lemma *flatten-pi-1-sf-subset*:
$sf\ (\varphi[M]_{\Pi 1}) \subseteq (\bigcup \varphi{\in}sf\ \varphi.\ sf\ (\varphi[M]_{\Pi 1}))$
⟨*proof*⟩

lemma *flatten-sigma-1-sf-subset*:
$sf\ (\varphi[M]_{\Sigma 1}) \subseteq (\bigcup \varphi{\in}sf\ \varphi.\ sf\ (\varphi[M]_{\Sigma 1}))$
⟨*proof*⟩

lemma *flatten-sigma-2-sf-subset*:
$sf\ (\varphi[M]_{\Sigma 2}) \subseteq (\bigcup \psi{\in}sf\ \varphi.\ sf\ (\psi[M]_{\Sigma 2}))$
⟨*proof*⟩

lemma *sf-set1*:
$sf\ (\varphi[M]_{\Sigma 2}) \cup sf\ (\varphi[M]_{\Pi 1}) \subseteq (\bigcup \psi \in (sf\ \varphi).\ (sf\ (\psi[M]_{\Sigma 2}) \cup sf\ (\psi[M]_{\Pi 1})))$
⟨*proof*⟩

lemma *ltln-not-idempotent* [*simp*]:
$\varphi\ and_n\ \psi \neq \varphi\ \psi\ and_n\ \varphi \neq \varphi\ \varphi \neq \varphi\ and_n\ \psi\ \varphi \neq \psi\ and_n\ \varphi$
$\varphi\ or_n\ \psi \neq \varphi\ \psi\ or_n\ \varphi \neq \varphi\ \varphi \neq \varphi\ or_n\ \psi\ \varphi \neq \psi\ or_n\ \varphi$
$X_n\ \varphi \neq \varphi\ \varphi \neq X_n\ \varphi$

$\varphi\ U_n\ \psi \neq \varphi\ \varphi \neq \varphi\ U_n\ \psi\ \psi\ U_n\ \varphi \neq \varphi\ \varphi \neq \psi\ U_n\ \varphi$
$\varphi\ R_n\ \psi \neq \varphi\ \varphi \neq \varphi\ R_n\ \psi\ \psi\ R_n\ \varphi \neq \varphi\ \varphi \neq \psi\ R_n\ \varphi$
$\varphi\ W_n\ \psi \neq \varphi\ \varphi \neq \varphi\ W_n\ \psi\ \psi\ W_n\ \varphi \neq \varphi\ \varphi \neq \psi\ W_n\ \varphi$
$\varphi\ M_n\ \psi \neq \varphi\ \varphi \neq \varphi\ M_n\ \psi\ \psi\ M_n\ \varphi \neq \varphi\ \varphi \neq \psi\ M_n\ \varphi$
⟨*proof*⟩

lemma *flatten-card-sf-induct*:
assumes *finite X*
assumes $\bigwedge x.\ x \in X \Longrightarrow sf\ x \subseteq X$
shows $card\ (\bigcup\varphi{\in}X.\ sf\ (\varphi[N]_{\Sigma 1})) \leq card\ X$
$\wedge\ card\ (\bigcup\varphi{\in}X.\ sf\ (\varphi[M]_{\Pi 1})) \leq card\ X$
$\wedge\ card\ (\bigcup\varphi{\in}X.\ sf\ (\varphi[M]_{\Sigma 2}) \cup sf\ (\varphi[M]_{\Pi 1})) \leq 3 * card\ X$
⟨*proof*⟩

theorem *flatten-card-sf*:
$card\ (\bigcup\psi \in sf\ \varphi.\ sf\ (\psi[M]_{\Sigma 1})) \leq card\ (sf\ \varphi)$ (**is** *?t1*)
$card\ (\bigcup\psi \in sf\ \varphi.\ sf\ (\psi[M]_{\Pi 1})) \leq card\ (sf\ \varphi)$ (**is** *?t2*)
$card\ (sf\ (\varphi[M]_{\Sigma 2}) \cup sf\ (\varphi[M]_{\Pi 1})) \leq 3 * card\ (sf\ \varphi)$ (**is** *?t3*)
⟨*proof*⟩

corollary *flatten-sigma-2-card-sf*:
$card\ (sf\ (\varphi[M]_{\Sigma 2})) \leq 3 * (card\ (sf\ \varphi))$
⟨*proof*⟩

end

4 Code Export

theory *Normal-Form-Code-Export* **imports**
LTL.Code-Equations
LTL.Rewriting
LTL.Disjunctive-Normal-Form
HOL.String
Normal-Form
begin

fun *flatten-pi-1-list* :: *String.literal ltln* ⇒ *String.literal ltln list* ⇒ *String.literal ltln*
where
flatten-pi-1-list $(\psi_1\ U_n\ \psi_2)$ M = (*if* $(\psi_1\ U_n\ \psi_2) \in$ *set M then* (*flatten-pi-1-list* ψ_1 M) W_n (*flatten-pi-1-list* ψ_2 M) *else* $false_n$)
| *flatten-pi-1-list* $(\psi_1\ W_n\ \psi_2)$ M = (*flatten-pi-1-list* ψ_1 M) W_n (*flatten-pi-1-list* ψ_2 M)

| *flatten-pi-1-list* (ψ_1 M_n ψ_2) M = (*if* (ψ_1 M_n ψ_2) $\in$ *set* M *then* (*flatten-pi-1-list* ψ_1 M) R_n (*flatten-pi-1-list* ψ_2 M) *else false*$_n$)
| *flatten-pi-1-list* (ψ_1 R_n ψ_2) M = (*flatten-pi-1-list* ψ_1 M) R_n (*flatten-pi-1-list* ψ_2 M)
| *flatten-pi-1-list* (ψ_1 *and*$_n$ ψ_2) M = (*flatten-pi-1-list* ψ_1 M) *and*$_n$ (*flatten-pi-1-list* ψ_2 M)
| *flatten-pi-1-list* (ψ_1 *or*$_n$ ψ_2) M = (*flatten-pi-1-list* ψ_1 M) *or*$_n$ (*flatten-pi-1-list* ψ_2 M)
| *flatten-pi-1-list* (X_n ψ) M = X_n (*flatten-pi-1-list* ψ M)
| *flatten-pi-1-list* φ - = φ

fun *flatten-sigma-1-list* :: *String.literal ltln* $\Rightarrow$ *String.literal ltln list* $\Rightarrow$ *String.literal ltln*
where
flatten-sigma-1-list (ψ_1 U_n ψ_2) N = (*flatten-sigma-1-list* ψ_1 N) U_n (*flatten-sigma-1-list* ψ_2 N)
| *flatten-sigma-1-list* (ψ_1 W_n ψ_2) N = (*if* (ψ_1 W_n ψ_2) $\in$ *set* N *then true*$_n$ *else* (*flatten-sigma-1-list* ψ_1 N) U_n (*flatten-sigma-1-list* ψ_2 N))
| *flatten-sigma-1-list* (ψ_1 M_n ψ_2) N = (*flatten-sigma-1-list* ψ_1 N) M_n (*flatten-sigma-1-list* ψ_2 N)
| *flatten-sigma-1-list* (ψ_1 R_n ψ_2) N = (*if* (ψ_1 R_n ψ_2) $\in$ *set* N *then true*$_n$ *else* (*flatten-sigma-1-list* ψ_1 N) M_n (*flatten-sigma-1-list* ψ_2 N))
| *flatten-sigma-1-list* (ψ_1 *and*$_n$ ψ_2) N = (*flatten-sigma-1-list* ψ_1 N) *and*$_n$ (*flatten-sigma-1-list* ψ_2 N)
| *flatten-sigma-1-list* (ψ_1 *or*$_n$ ψ_2) N = (*flatten-sigma-1-list* ψ_1 N) *or*$_n$ (*flatten-sigma-1-list* ψ_2 N)
| *flatten-sigma-1-list* (X_n ψ) N = X_n (*flatten-sigma-1-list* ψ N)
| *flatten-sigma-1-list* φ - = φ

fun *flatten-sigma-2-list* :: *String.literal ltln* $\Rightarrow$ *String.literal ltln list* $\Rightarrow$ *String.literal ltln*
where
flatten-sigma-2-list (φ U_n ψ) M = (*flatten-sigma-2-list* φ M) U_n (*flatten-sigma-2-list* ψ M)
| *flatten-sigma-2-list* (φ W_n ψ) M = (*flatten-sigma-2-list* φ M) U_n ((*flatten-sigma-2-list* ψ M) *or*$_n$ (G_n (*flatten-pi-1-list* φ M)))
| *flatten-sigma-2-list* (φ M_n ψ) M = (*flatten-sigma-2-list* φ M) M_n (*flatten-sigma-2-list* ψ M)
| *flatten-sigma-2-list* (φ R_n ψ) M = ((*flatten-sigma-2-list* φ M) *or*$_n$ (G_n (*flatten-pi-1-list* ψ M))) M_n (*flatten-sigma-2-list* ψ M)
| *flatten-sigma-2-list* (φ *and*$_n$ ψ) M = (*flatten-sigma-2-list* φ M) *and*$_n$ (*flatten-sigma-2-list* ψ M)
| *flatten-sigma-2-list* (φ *or*$_n$ ψ) M = (*flatten-sigma-2-list* φ M) *or*$_n$ (*flatten-sigma-2-list* ψ M)

| *flatten-sigma-2-list* $(X_n\ \varphi)\ M = X_n$ (*flatten-sigma-2-list* φ M)
| *flatten-sigma-2-list* φ - = φ

lemma *flatten-code-equations*[*simp*]:
$\varphi[set\ M]_{\Pi 1}$ = *flatten-pi-1-list* φ M
$\varphi[set\ M]_{\Sigma 1}$ = *flatten-sigma-1-list* φ M
$\varphi[set\ M]_{\Sigma 2}$ = *flatten-sigma-2-list* φ M
⟨*proof*⟩

abbreviation *and-list* ≡ *foldl And-ltln* $true_n$

abbreviation *or-list* ≡ *foldl Or-ltln* $false_n$

definition *normal-form-disjunct* (φ :: *String.literal ltln*) M N
≡ (*flatten-sigma-2-list* φ M)
and_n (*and-list* (*map* ($\lambda\psi$. G_n (F_n (*flatten-sigma-1-list* ψ N))) M)
and_n (*and-list* (*map* ($\lambda\psi$. F_n (G_n (*flatten-pi-1-list* ψ M))) N)))

definition *normal-form* (φ :: *String.literal ltln*)
≡ *or-list* (*map* ($\lambda(M, N)$. *normal-form-disjunct* φ M N) (*advice-sets* φ))

lemma *and-list-semantic*: $w \models_n$ *and-list xs* ⟷ ($\forall x \in$ *set xs*. $w \models_n x$)
⟨*proof*⟩

lemma *or-list-semantic*: $w \models_n$ *or-list xs* ⟷ ($\exists x \in$ *set xs*. $w \models_n x$)
⟨*proof*⟩

theorem *normal-form-correct*:
$w \models_n \varphi$ ⟷ $w \models_n$ *normal-form* φ
⟨*proof*⟩

definition *normal-form-with-simplifier* (φ :: *String.literal ltln*)
≡ *min-dnf* (*simplify Slow* (*normal-form* (*simplify Slow* φ)))

lemma *ltl-semantics-min-dnf*:
$w \models_n \varphi$ ⟷ ($\exists C \in$ *min-dnf* φ. $\forall \psi$. ψ |∈| C ⟶ $w \models_n \psi$) (**is** *?lhs* ⟷ *?rhs*)
⟨*proof*⟩

theorem
$w \models_n \varphi$ ⟷ ($\exists C \in$ (*normal-form-with-simplifier* φ). $\forall \psi$. ψ |∈| C ⟶ $w \models_n \psi$) (**is** *?lhs* ⟷ *?rhs*)
⟨*proof*⟩

In order to export the code run `isabelle build -D [PATH] -e`.

export-code *normal-form* **in** *SML*
export-code *normal-form-with-simplifier* **in** *SML*

end

References

[1] Ivana Černá and Radek Pelánek. Relating hierarchy of temporal properties to model checking. In Branislav Rovan and Peter Vojtás, editors, *Mathematical Foundations of Computer Science 2003, 28th International Symposium, MFCS 2003, Bratislava, Slovakia, August 25-29, 2003, Proceedings*, volume 2747 of *Lecture Notes in Computer Science*, pages 318–327. Springer, 2003. doi:10.1007/978-3-540-45138-9_26.

[2] Edward Y. Chang, Zohar Manna, and Amir Pnueli. Characterization of temporal property classes. In Werner Kuich, editor, *Automata, Languages and Programming, 19th International Colloquium, ICALP92, Vienna, Austria, July 13-17, 1992, Proceedings*, volume 623 of *Lecture Notes in Computer Science*, pages 474–486. Springer, 1992. doi:10.1007/3-540-55719-9_97.

[3] Orna Lichtenstein, Amir Pnueli, and Lenore D. Zuck. The glory of the past. In Rohit Parikh, editor, *Logics of Programs, Conference, Brooklyn College, New York, NY, USA, June 17-19, 1985, Proceedings*, volume 193 of *Lecture Notes in Computer Science*, pages 196–218. Springer, 1985. doi:10.1007/3-540-15648-8_16.

[4] Salomon Sickert and Javier Esparza. An efficient normalisation procedure for linear temporal logic and very weak alternating automata. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2020, Saarbrücken, Germany, July 8-11, 2020*. ACM, 2020. doi:10.1145/3373718.3394743.

[5] Salomon Sickert and Javier Esparza. An efficient normalisation procedure for linear temporal logic and very weak alternating automata. *CoRR*, abs/2005.00472, 2020. arXiv:2005.00472.

[6] Lenore D. Zuck. *Past Temporal Logic*. PhD thesis, The Weizmann Institute of Science, Israel, August 1986.