Rewriting rules for the encoding of TLA+ into first-order logic

This document lists the collection of rewriting rules applied during the preprocessing phase of the translation from (boolified) TLA$^+$ to unsorted and many-sorted first-order logic. This list is not comprehensive; trivial rules such as $x \land \textsc{true} \longrightarrow x$ are omitted. All the rewriting rules were encoded and mechanically verified in Isabelle/TLA$^+$.

Notation: the expression $[h_i \mapsto e_i]_{i:1\,..\,n}$ abbreviates $[h_1 \mapsto e_1, \ldots, h_n \mapsto e_n]$ and $[h_i : e_i]_{i:1\,..\,n}$ abbreviates $[h_1 : e_1, \ldots, h_n : e_n]$.

1 First-order logic and choose operator

$$\begin{aligned}
\forall x : x \in \{e_1, \ldots, e_n\} \Rightarrow p(x) &\longrightarrow p(e_1) \land \ldots \land p(e_n) && (x \notin FV_{1..n}) \\
\exists x : x \in \{e_1, \ldots, e_n\} \land p(x) &\longrightarrow p(e_1) \lor \ldots \lor p(e_n) && (x \notin FV_{1..n}) \\
\forall x \in \{y \in S : q(y)\} : p(x) &\longrightarrow \forall x \in S : q(x) \Rightarrow p(x) \\
\exists x \in \{y \in S : q(y)\} : p(x) &\longrightarrow \exists x \in S : q(x) \land p(x) \\
y = \textsc{choose}\ x : P(x) &\longrightarrow (\exists x : P(x)) \Leftrightarrow P(y)
\end{aligned}$$

where $FV_{1..n} = FV(e_1) \cup \ldots \cup FV(e_n))$.

2 Set theory

$$\begin{aligned}
x \in \{\} &\longrightarrow \textsc{false} & x \notin S &\longrightarrow \neg(x \in S) \\
x \in \{e_1, \ldots, e_n\} &\longrightarrow x = e_1 \lor \ldots \lor x = e_n & S \subseteq T &\longrightarrow \forall x : x \in S \Rightarrow x \in T \\
x \in \{y \in S : p(y)\} &\longrightarrow x \in S \land p(x) & x \in e_1 \cup e_2 &\longrightarrow x \in e_1 \lor x \in e_2 \\
S \in \textsc{subset}\ T &\longrightarrow \forall x : x \in S \Rightarrow x \in T & x \in e_1 \cap e_2 &\longrightarrow x \in e_1 \land x \in e_2 \\
x \in \textsc{union}\ S &\longrightarrow \exists T : T \in S \land x \in T & x \in e_1 \setminus e_2 &\longrightarrow x \in e_1 \land \neg(x \in e_2) \\
x \in e_1 \,..\, e_2 &\longrightarrow x \in Int \land e_1 \leq x \land x \leq e_2
\end{aligned}$$

Instances of set extensionality:

$$\begin{aligned}
S = \{\} &\longrightarrow \forall x : \neg(x \in S) \\
S = \{e_1, \ldots, e_n\} &\longrightarrow \forall x :\ x \in S \Leftrightarrow x = e_1 \vee \ldots \vee x = e_n \\
S = \textsc{subset}\ T &\longrightarrow \forall x :\ x \in S \Leftrightarrow (\forall y :\ y \in x \Rightarrow y \in T) \\
S = \textsc{union}\ T &\longrightarrow \forall x :\ x \in S \Leftrightarrow (\exists y :\ y \in T \wedge x \in y) \\
S = \{x \in T : p(x)\} &\longrightarrow \forall x :\ x \in S \Leftrightarrow x \in T \wedge p(x) \\
S = \{e(y) : y \in T\} &\longrightarrow \forall x :\ x \in S \Leftrightarrow (\exists y :\ y \in T \wedge x = e(y)) \\
S = T \cup U &\longrightarrow \forall x :\ x \in S \Leftrightarrow x \in T \vee x \in U \\
S = T \cap U &\longrightarrow \forall x :\ x \in S \Leftrightarrow x \in T \wedge x \in U \\
S = T \setminus U &\longrightarrow \forall x :\ x \in S \Leftrightarrow x \in T \wedge \neg(x \in U) \\
\forall x :\ x \in S \Leftrightarrow x \in T &\longrightarrow S = T
\end{aligned}$$

3 Functions

$$\begin{aligned}
[x \in S \mapsto e(x)][a] &\longrightarrow \textsc{if}\ a \in S\ \textsc{then}\ e(a)\ \textsc{else}\ \omega([x \in S \mapsto e(x)], a) \\
[f\ \textsc{except}\ ![x] = y][a] &\longrightarrow \textsc{if}\ a \in \textsc{domain}\ f \\
&\qquad\ \textsc{then}\ (\textsc{if}\ x = a\ \textsc{then}\ y\ \textsc{else}\ \alpha(f, a)) \\
&\qquad\ \textsc{else}\ \ \omega([f\ \textsc{except}\ ![x] = y], a) \\
\textsc{domain}\ [x \in S \mapsto e] &\longrightarrow S \\
\textsc{domain}\ [f\ \textsc{except}\ ![x] = y] &\longrightarrow \textsc{domain}\ f \\
f \in [S \to T] &\longrightarrow \wedge\ \mathit{isAFcn}(f) \\
&\qquad \wedge\ \textsc{domain}\ f = S \\
&\qquad \wedge\ \forall x \in S : \alpha(f, x) \in T \\
[g\ \textsc{except}\ [a] = b] \in [S \to T] &\longrightarrow \wedge\ \mathit{isAFcn}(g) \\
&\qquad \wedge\ \textsc{domain}\ g = S \\
&\qquad \wedge\ a \in S \\
&\qquad \wedge\ b \in T \\
&\qquad \wedge\ \forall x \in S \setminus \{a\} : \alpha(f, x) \in T \\
[x \in S' \mapsto e(x)] \in [S \to T] &\longrightarrow \wedge\ S' = S \\
&\qquad \wedge\ \forall x \in S : e(x) \in T \\
\mathit{isAFcn}([x \in S \mapsto e]) &\longrightarrow \textsc{true} \\
\mathit{isAFcn}([f\ \textsc{except}\ ![x] = y]) &\longrightarrow \textsc{true}
\end{aligned}$$

Instances of extensionality:

$$f = [x \in S \mapsto e(x)] \overset{e(x):\mathsf{Bool}}{\longrightarrow} \begin{array}{l} \land\ isAFcn(f) \\ \land\ \textsc{domain}\ f = S \\ \land\ \forall x \in S : \alpha(f, x)^b \Leftrightarrow e(x) \end{array}$$

$$f = [x \in S \mapsto e(x)] \longrightarrow \begin{array}{l} \land\ isAFcn(f) \\ \land\ \textsc{domain}\ f = S \\ \land\ \forall x \in S : \alpha(f, x) = e(x) \end{array}$$

$$g = [f\ \textsc{except}\ ![a] = b] \overset{b:\mathsf{Bool}}{\longrightarrow} \begin{array}{l} \land\ isAFcn(g) \\ \land\ \textsc{domain}\ f = \textsc{domain}\ g \\ \land\ a \in \textsc{domain}\ g \Rightarrow \alpha(g, a)^b \Leftrightarrow b \\ \land\ \forall x \in \textsc{domain}\ f \setminus \{a\} : \alpha(g, x) = \alpha(f, x) \end{array}$$

$$g = [f\ \textsc{except}\ ![a] = b] \longrightarrow \begin{array}{l} \land\ isAFcn(g) \\ \land\ \textsc{domain}\ f = \textsc{domain}\ g \\ \land\ a \in \textsc{domain}\ g \Rightarrow \alpha(g, a) = b \\ \land\ \forall x \in \textsc{domain}\ f \setminus \{a\} : \alpha(f, x) = \alpha(g, x) \end{array}$$

$$[x \in S \mapsto e(x)] = [x \in T \mapsto d(x)] \longrightarrow S = T \land \forall x \in S : e(x) = d(x)$$

4 If-then-else

$$\textsc{if}\ c\ \textsc{then}\ t\ \textsc{else}\ u \overset{t,u:\mathsf{Bool}}{\longrightarrow} c \Rightarrow t \land \neg c \Rightarrow u \qquad \text{(when } c \text{ is a variable)}$$

$$\textsc{if}\ c\ \textsc{then}\ t\ \textsc{else}\ u \overset{t,u:\mathsf{Bool}}{\longrightarrow} \exists z : (z \Leftrightarrow c) \land c \Rightarrow t \land \neg c \Rightarrow u$$

$$x \otimes \textsc{if}\ c\ \textsc{then}\ t\ \textsc{else}\ f \longrightarrow \textsc{if}\ c\ \textsc{then}\ x \otimes t\ \textsc{else}\ x \otimes f$$

$$f[\textsc{if}\ c\ \textsc{then}\ t\ \textsc{else}\ u] \longrightarrow \textsc{if}\ c\ \textsc{then}\ f[t]\ \textsc{else}\ f[u]$$

$$O_1(\textsc{if}\ c\ \textsc{then}\ t\ \textsc{else}\ u) \longrightarrow \textsc{if}\ c\ \textsc{then}\ O_1(t)\ \textsc{else}\ O_1(u)$$

where x is a term, $\otimes$ is an infix binary TLA$^+$ operator such as $=$, $\in$, $\Rightarrow$, $\land$, $\Leftrightarrow$, $+$, or $<$, and O_1 is a prefix unary TLA$^+$ operator such as $\neg$, DOMAIN, SUBSET or UNION.

5 Tuples and records

$$\langle e_1, \ldots, e_n \rangle[i] \longrightarrow e_i \qquad \text{(when } i \in 1 \mathrel{..} n\text{)}$$

$$t \in S_1 \times \ldots \times S_n \longrightarrow \begin{array}{l} \land\ isAFcn(t) \\ \land\ \textsc{domain}\ t = 1 \mathrel{..} n \\ \land\ \alpha(t, 1) \in S_1\ \land\ \ldots\ \land\ \alpha(t, n) \in S_n \end{array}$$

$$
\begin{aligned}
[h_i \mapsto e_i]_{i:1..n}.h_j &\longrightarrow e_j \qquad \text{when } j \in 1 \,..\, n\\
[r \text{ EXCEPT } !.h_1 = e].h_2 &\longrightarrow \text{IF } \text{“}\mathsf{h_1}\text{”} = \text{“}\mathsf{h_2}\text{”} \text{ THEN } e \text{ ELSE } r.h_2\\
r.h &\longrightarrow r[\text{“}\mathsf{h}\text{”}]\\
r \in [h_i : S_i]_{i:1..n} &\longrightarrow \wedge\ isAFcn(r)\\
&\qquad \wedge\ \text{DOMAIN } r = \{\text{“}\mathsf{h_1}\text{”}, \ldots, \text{“}\mathsf{h_n}\text{”}\}\\
&\qquad \wedge\ \alpha(r, \text{“}\mathsf{h_1}\text{”}) \in S_1 \wedge \ldots \wedge \alpha(r, \text{“}\mathsf{h_n}\text{”}) \in S_n\\
[h_i \mapsto e_i]_{i:1..n} \in [f_j : S_j]_{j:1..m} &\longrightarrow \wedge\ \{\text{“}\mathsf{h_1}\text{”}, \ldots, \text{“}\mathsf{h_n}\text{”}\} = \{\text{“}\mathsf{f_1}\text{”}, \ldots, \text{“}\mathsf{f_m}\text{”}\}\\
&\qquad \wedge\ \bigwedge e_i \in S_j \qquad \text{when } h_i = f_j, i \in 1 \,..\, n, j \in 1 \,..\, m
\end{aligned}
$$

$$
\begin{aligned}
\text{DOMAIN } \langle\rangle &\longrightarrow \{\}\\
\text{DOMAIN } [h_i \mapsto e_i]_{i:1..n} &\longrightarrow \{\text{“}\mathsf{h_1}\text{”}, \ldots, \text{“}\mathsf{h_n}\text{”}\}\\
\text{DOMAIN } \langle e_1, \ldots, e_n\rangle &\longrightarrow 1 \,..\, n\\
\text{DOMAIN } [r \text{ EXCEPT } !.h = e] &\longrightarrow \text{DOMAIN } r
\end{aligned}
$$

Instances of extensionality:

$$
\begin{aligned}
t = \langle e_1, \ldots, e_n\rangle &\longrightarrow \wedge\ isAFcn(t)\\
&\qquad \wedge\ \text{DOMAIN } t = 1..n\\
&\qquad \wedge\ \textstyle\bigwedge_{e_i:\mathsf{Bool}} \alpha(t, i)^b \Leftrightarrow e_i\\
&\qquad \wedge\ \textstyle\bigwedge_{e_i:\mathsf{U}} \alpha(t, i) = e_i\\
T = S_1 \times \ldots \times S_n &\longrightarrow \forall x :\ x \in T \Leftrightarrow \wedge\ isAFcn(x)\\
&\qquad\qquad \wedge\ \text{DOMAIN } x = 1..n\\
&\qquad\qquad \wedge\ \alpha(x, 1) \in S_1\ \wedge\ \ldots\ \wedge\ \alpha(x, n) \in S_n\\
r = [h_i \mapsto e_i]_{i:1..n} &\longrightarrow \wedge\ isAFcn(r)\\
&\qquad \wedge\ \text{DOMAIN } r = \{\text{“}\mathsf{h_1}\text{”}, \ldots, \text{“}\mathsf{h_n}\text{”}\}\\
&\qquad \wedge\ \text{“}\mathsf{h_1}\text{”} \in \text{DOMAIN } r \wedge \ldots \wedge \text{“}\mathsf{h_n}\text{”} \in \text{DOMAIN } r\\
&\qquad \wedge\ \textstyle\bigwedge_{e_i:\mathsf{Bool}} \alpha(r, \text{“}\mathsf{h_i}\text{”})^b \Leftrightarrow e_i\\
&\qquad \wedge\ \textstyle\bigwedge_{e_i:\mathsf{U}} \alpha(r, \text{“}\mathsf{h_i}\text{”}) = e_i\\
x = [y \text{ EXCEPT } !.h = e] &\longrightarrow \wedge\ isAFcn(x)\\
&\qquad \wedge\ \text{DOMAIN } x = \text{DOMAIN } y\\
&\qquad \wedge\ \text{“}\mathsf{h}\text{”} \in \text{DOMAIN } y \Rightarrow \alpha(x, \text{“}\mathsf{h}\text{”}) = e\\
&\qquad \wedge\ \forall k \in \text{DOMAIN } y \setminus \{\text{“}\mathsf{h}\text{”}\} :\ \alpha(x, k) = \alpha(y, k)\\
R = [h_i : S_i]_{i:1..n} &\longrightarrow \forall r :\ r \in R \Leftrightarrow\\
&\qquad\quad \wedge\ isAFcn(r)\\
&\qquad\quad \wedge\ \text{DOMAIN } r = \{\text{“}\mathsf{h_1}\text{”}, \ldots, \text{“}\mathsf{h_n}\text{”}\}\\
&\qquad\quad \wedge\ \text{“}\mathsf{h_1}\text{”} \in \text{DOMAIN } r \wedge \ldots \wedge \text{“}\mathsf{h_n}\text{”} \in \text{DOMAIN } r\\
&\qquad\quad \wedge\ \alpha(r, \text{“}\mathsf{h_1}\text{”}) \in S_1 \wedge \cdots \wedge \alpha(r, \text{“}\mathsf{h_n}\text{”}) \in S_n
\end{aligned}
$$