AUTOMATICKÉ OVĚŘOVÁNÍ TEMPORÁLNÍCH VLASTNOSTÍ PROGRAMŮ ZA BĚHU

14

Petra Sečkařová
xsecka02@stud.fit.vutbr.cz

O CO JDE?

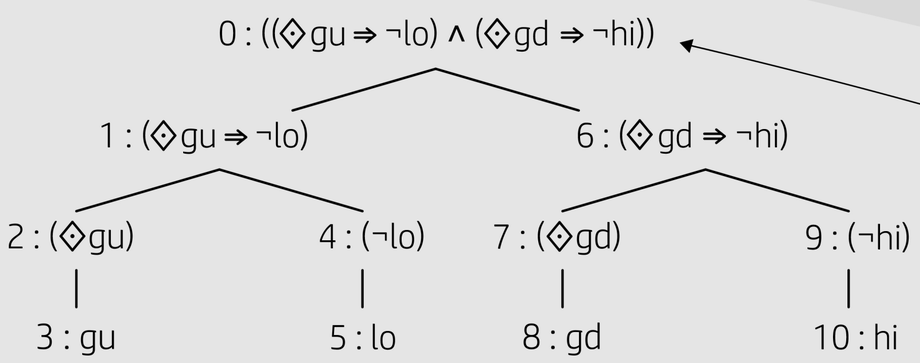
Cílem práce je vytvoření nástroje pro dynamické **ověřování temporálních vlastností** programů v jazycích C/C++, specifikovaných pomocí logiky **Past-Time LTL**. Tento nástroj vzniká v rámci platformy Testos a na základě uživatelem specifikovaných vlastností vytvoří statickou knihovnu obsahující monitor pro dané vlastnosti, která se slinkuje s testovaným programem a za běhu detekuje porušení specifikace.

PAST-TIME LTL

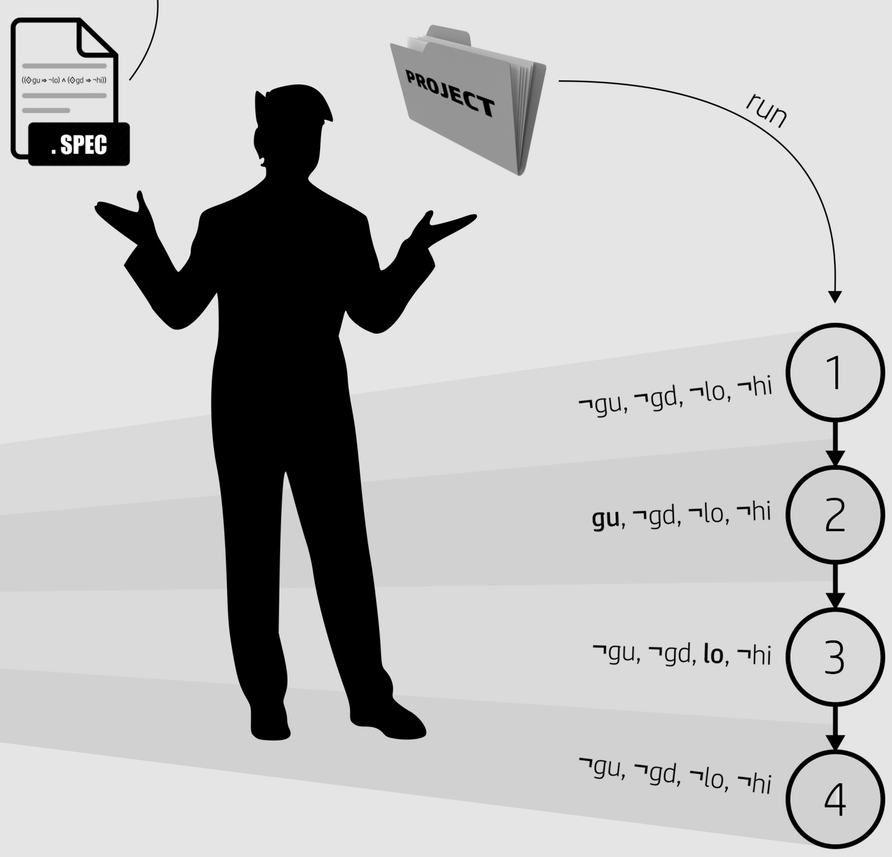
Past-Time LTL je logika používající výrokové logické operátory doplněné navíc o speciální **temporální operátory** pro popis vztahů, které musí platit mezi **stavy dosavadní historie** běhu systému. Ty jsou definovány nad konkrétní sekvencí stavů systému $\sigma = s_1, s_2, s_3, \ldots$ takto:

$$
\begin{aligned}
&\textit{Previously}: && s_j \models \diamondsuit\ p && \iff && \exists n,\ 1 \leq n \leq j\ s_n \models p \\
&\textit{Globally}: && s_j \models \boxdot\ p && \iff && \forall n,\ 1 \leq n \leq j\ s_n \models p \\
&\textit{Since}: && s_j \models p\ \mathcal{S}\ q && \iff && \exists n,\ 1 \leq n \leq j\ s_n \models q \wedge \forall i,\ n < i \leq j\ s_i \models p \\
&\textit{Last}: && s_j \models \odot\ p && \iff && \text{pro } j > 1\ s_{j-1} \models p,\ s_1 \models p
\end{aligned}
$$

Specifikace programu pro nástroj T-Props Checker může obsahovat mnoho těchto formulí a tak je možné ověřovat **celou sadu** temporálních **vlastností jedním monitorem**.



T-PROPS CHECKER



MONITOR

STAVOVÉ PROMĚNNÉ
gd: going down
gu: going up
hi: higher
lo: lower

GENEROVÁNÍ MONITORU

Formule specifikace jsou nejprve rozloženy do stromu podformulí. Následně je těmto formulím na míru generován kód monitoru, jehož ověřovací algoritmus vychází z rekurzivního vyjádření temporálních operátorů. Aktuální platnost formule je za běhu vyhodnocována pouze **na základě její platnosti v předchozím stavu programu a aktuálních hodnot** stavových proměnných, na začátku jsou hodnoty předchozího stavu inicializovány podle aktuálních hodnot stavových proměnných.

Vygenerovaný kód monitoru je uložen jako **statická knihovna**, umožňující velmi snadné zapojení výstupu tohoto nástroje do stávajícího projektu. Je spouštěn souběžně s ověřovaným programem a v případě neočekávaného chování vytiskne **na chybový výstup zprávu** o okolnostech vedoucích k aktuálnímu neplatnému stavu. Díky tomu, že monitor vychází pouze ze specifikace a je integrován do ověřovaného programu, může kontrolovat **libovolné běhy programu bez nutnosti nového zpracování** monitoru.

$$
\begin{aligned}
s_j \models p\ \mathcal{S}\ q &\iff s_j \models q \vee (j > 1 \wedge s_j \models p \wedge s_{j-1} \models p\ \mathcal{S}\ q) \\
s_j \models \boxdot\ p &\iff s_j \models p \wedge s_{j-1} \models \boxdot\ p \\
s_j \models \diamondsuit\ p &\iff s_j \models p \vee s_{j-1} \models \diamondsuit\ p \\
s_j \models \odot\ p &\iff s_{j-1} \models p
\end{aligned}
$$