Lero THE IRISH SOFTWARE RESEARCH CENTRE

Science Foundation Ireland sfi For what's next

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

fPAISEAN

Dr. Anila Mjeda, Supervised by: Dr. Andrew Butterfield

1 Research Focus

» To explore the scope of formal methods as a way to increase the degree of rigorous analysis that can be applied to descriptions of large, complex processes.
  › Need for process flexibility
  › Account for context-aware process equivalence

» Formalising the Process Modelling Language (PML)

» Exploring its use in modelling Clinical Health Pathways (CHPs)
  › CHPs: dynamic, context sensitive, event driven, knowledge sensitive.
  › CHP example:

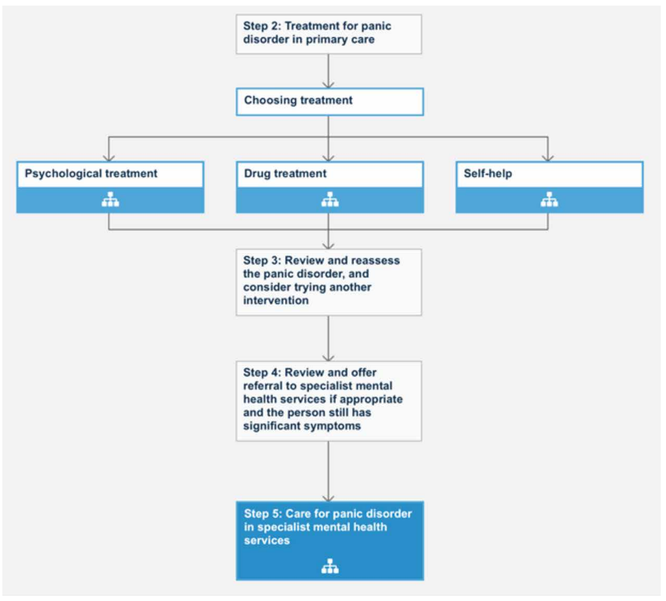

Fig 1: Treatment for panic disorder in primary care (NICE CHP)

2 Our Approach

» Using UTP to formalise PML
  › UTP models systems as 1st/2nd order predicates that describe relationships between starting, intermediate and terminating values of observable aspects of program behaviour such as: program variable values; program start and stop; traces of externally observable events.
  › UTP supports multiple semantic models and their linkages.
  › UTP semantics for PML could be linked to domain-specific semantic model associated with application areas.

» PML Semantics
  › Resources- we model resource expressions as predicates, on the state of a (global) resource pool:

$$
\begin{array}{rcll}
i & \widehat{=} & i \in \mathrm{dom}\,\rho & \text{«def:res:i»} \\
(i_1)(i_2)\cdots(i_n)i & \widehat{=} & i \in \mathrm{dom}\,\rho \wedge \pi_1(\rho i) = \langle i_1, i_2, \ldots, i_n \rangle & \text{«def:res:q:i»} \\
i_1.i_2 & \widehat{=} & i_1 \in \mathrm{dom}\,\rho \wedge i_2 \in \mathrm{dom}\,\pi_2(\rho i_1) & \text{«def:res:i.i»} \\
(i_1)(i_2)\cdots(i_n)i.i_a & \widehat{=} & (i_1)(i_2)\cdots(i_n)i \wedge i.i_a & \text{«def:res:q:i.i»} \\
v.i \bowtie s & \widehat{=} & v.i \wedge (\pi_2(\rho v))(i) \bowtie s & \text{«def:res:v.i:rel:s»} \\
s \bowtie v.i & \widehat{=} & v.i \wedge s \bowtie (\pi_2(\rho v))(i) & \text{«def:res:s:rel:v.i»} \\
v.i \bowtie n & \widehat{=} & v.i \wedge (\pi_2(\rho v))(i) \bowtie n & \text{«def:res:v.i:rel:n»} \\
n \bowtie v.i & \widehat{=} & v.i \wedge n \bowtie (\pi_2(\rho v))(i) & \text{«def:res:n:rel:v.i»} \\
v_1.i_1 \bowtie v_2.i_2 & \widehat{=} & v_1.i_1 \wedge v_2.i_2 \wedge (\pi_2(\rho v_1))(i_1) \bowtie (\pi_2(\rho v_2))(i_2) & \text{«def:res:v.i:rel:v.i»} \\
v_1 = v_2 & \widehat{=} & v_1 \wedge (v_1 = v_2) & \text{«def:res:v:eq:v»}
\end{array}
$$

» Basic Actions- have a pre-condition – the resources required for them to run. When run, their outcome is that new/updated resources are provided.

$$
\begin{array}{rcll}
?rr\ !pr & \widehat{=} & resof(pr) : [rr, pr] & \text{«def:task:frame-spec»} \\
resof & : & Expr \to \mathcal{P} ResName & \text{«sig:resof»} \\
resof(\neg e) & \widehat{=} & resof(e) & \text{«def:resof:not»} \\
resof(e_1 \wedge e_2) & \widehat{=} & resof(e_1) \cup resof(e_2) & \text{«def:resof:and»} \\
resof(e_1 \vee e_2) & \widehat{=} & resof(e_1) \cup resof(e_2) & \text{«def:resof:or»} \\
resof((i)^* i) & \widehat{=} & \{i\} & \text{«def:resof:rname»} \\
resof((i)^* i.i_a) & \widehat{=} & \{i\} & \text{«def:resof:attr»} \\
resof(u_1 \bowtie u_2) & \widehat{=} & resof(u_1) \cup resof(u_2) & \text{«def:resof:rel»} \\
resof(v_1 = v_2) & \widehat{=} & \{v\} & \text{«def:resof:eq»} \\
resof(e) & \widehat{=} & \{\} & \text{«def:resof:default»}
\end{array}
$$

3 Results to date

» **Weak PML semantics**
  › An interpretation that ignores all flow-of-control constructs
  › All basic actions are viewed as running in parallel
  › At any point in time one basic action, whose required resources are available, is non-deterministically chosen to execute.
  › The overall "flow-of-control" is determined by the induced dependencies between required and provided resources of all the tasks

$$
\begin{array}{rcll}
isBlk, isRdy, isDone & : & Res \to TBody \to \mathbb{B} & \\
isBlk_r(?rr\ !pr) & \widehat{=} & \neg rr[r/\rho] & \\
isRdy_r(?rr\ !pr) & \widehat{=} & rr[r/\rho] \wedge \neg pr[r/\rho] & \\
isDone_r(?rr\ !pr) & \widehat{=} & rr[r/\rho] \wedge pr[r/\rho] &
\end{array}
$$

$$
\begin{array}{rcll}
(N\ tbody) & \widehat{=} & & \text{«def:task»} \\
 & & (isBlk_r(tbody) \implies II) & \text{«def:task:blk»} \\
 & \wedge & (isRdy_r(tbody) \implies \Delta(N\ tbody)) & \text{«def:task:rdy»} \\
 & \wedge & (isDone_r(tbody) \implies (II \sqcap \Delta(N\ tbody))) & \\
\Delta(N\ ?rr\ !pr) & \widehat{=} & \mathbf{P3}(\ \mathbf{true} \vdash (?rr\ !pr)[r, r'/\rho, \rho'] \wedge h' = h \frown \langle N \rangle\ ) & \text{«def:do:task»} \\
\omega & \widehat{=} & someReady(\omega, r)* & \text{«weak:semantics»} \\
 & & (\exists T \bullet T \in \mathrm{dom}\,\omega \wedge \neg isBlk_r(\omega T) \wedge (N\ \omega T)) & \\
\omega\ |_{R,H} & \widehat{=} & \mathbf{var}\ r, h := R, H\ ;\ \omega & \text{«weak:init»} \\
 & someReady(\omega, r) & & \\
 & \widehat{=} & \exists T \bullet T \in \mathrm{dom}\,\omega \bullet isRdy_r(\omega T) & \text{«def:someReady»}
\end{array}
$$

Fig 2: Highlights from Weak PML semantics

» **The Strict (and Flexible) PML semantics**
  › For concurrent/parallel programs with flow of control and global shared state (or variables)
  › Building on "UTPP" by Hughes and Woodcock
  › Developing fully compositional semantics
    - Context information is propagated in a top-down manner

4

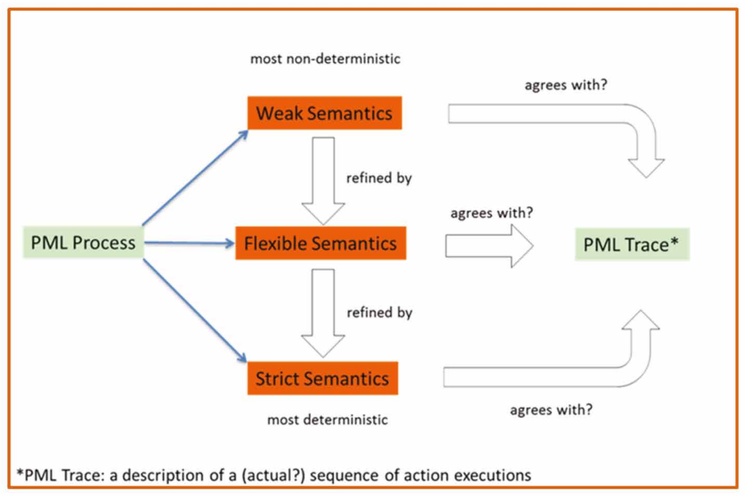

Fig 3: PML semantics – relating semantics

» **Prototype tool support for PML semantics**
  › Written in Haskell
  › Parses full PML concrete syntax
  › Supports formal analysis
    - Including calculating the semantics

Future work

» Clinical Health Pathways Case studies and theoretical publications

» Prototype tool will support more formal analysis

» Exploring novel uses of formality in safety-critical model-based development.

* This poster reports work by Dr. Andrew Butterfield and Dr. Anila Mjeda.

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union

European Union
European Regional Development Fund

SOUTHERN Regional Assembly
Promoting our Region