Mondex in VDM++

Latest Status

The abstract and concrete models have been proposed in executable VDM++, plus pre/post specifications and are presented here. The abstract model consists of an Abstract Purse and an Abstract World. The concrete model is made up of a Concrete Purse, Concrete World, Ether and Perfect Ether. To prove properties of the models, flattened VDM-SL versions have been produced, consisting of a Concrete World and an Abstract World

Following some tutorials on proof (given by John), we've started hand-proofs of refinement. Again, we have been concentrating on spreading proof skills in the group and involving as many folk as possible. The totality and adequecy proofs are completed, and we are in the process of typesetting these. We are now concentrating on the domain and result proofs.

We intend to set up the VDM->HOL environment developed by SanderVermolen. This has already been used to discharge the consistency proof obligations of a VDM-SL version of the abstract Mondex model. We'll look to apply it to the concrete model and to the refinement proof obligation (or at least the major lemmas of that).

We are in the process of experimenting with the combinatorial testing capabilities of Overture for the abstract model. We have completed traces which test the preconditions of the AbWorld transfer operations, and are looking into ways to test the (strong) post-conditions and class invariant.

Participants

ZoeAndrews, Steve Riddle, JohnFitzgerald, JeremyBryans, KenPierce, JohnHughes, RichardPayne, SarahClarke.

An overview of Mondex by Ken

- Newcastle_Mondex_12th_February_2007_(K.G.Pierce).ppt: Ken's slides 12th Feb 2007

Actions

- We wish to be able to use SanderVermolen's VDM->HOL environment to discharge the proof obligations of the concrete model produced. This requires the setting up of the proof generator, and subsequently learning to work with HOL.
- We wish to produce a student crib-sheet style document for 2nd year students studying VDM++. This documents brings together the fundamental concepts in a short guide
- Hand proofs for domain and result
- Produce outline for possible paper on VDM Mondex approach
- Develop a graphical user interface for interaction with the Mondex model, MondexGui

- Experiment with the combinatorial testing capabilities of Overture for both the abstract and concrete models.

Proof Effort

The following is a list of proof obligations that make up the proof effort for the VDM-SL specification.

Rule	Resp.	Done	Typeset	Check1	Check2
inv-ConWorld-form	Completed	Yes	Yes	Yes	Yes
ConWorld-1-form	Completed	Yes	Yes	Yes	Yes
retr-form	Completed	Yes	Yes	Yes	Yes
diff-\not-=	Completed	Yes	Yes	Yes	Yes
comp-set-ind	Completed	Yes	Yes	Yes	Yes
TransferLost-dom	Completed	Yes	Yes	Yes	Yes
dom-purses-=	Completed	Yes	Yes	Yes	Yes
bal-purses-equal	Completed	Yes	Yes	Yes	Yes
\delta-pre-AbTransferLost	Completed	Yes	Yes	Yes	Yes
retr-adequate	Completed	Yes	Yes	Yes	Yes
TransferLost-res	Completed	Yes	Yes	Yes	Yes
auth-=	Completed	Yes	Yes	Yes	Yes
+-=	Completed	Yes	Yes	Yes	Yes
con-assign	Completed	Yes	Yes	Yes	Yes
ConWorld-AbWorld-form	Completed	Yes	Yes	Yes	Yes
\delta->=	Completed	Yes	Yes	Yes	Yes
post-forall-=	Completed	Yes	Yes	Yes	Yes
post-dom-=	Completed	Yes	Yes	Yes	Yes
post-bal-geq	Completed	Yes	Yes	Yes	Yes
post-abauth-=	Completed	Yes	Yes	Yes	Yes
post-total-=	Completed	Yes	Yes	Yes	Yes
total-C-form	Completed	Yes	Yes	Yes	Yes
in-eq-set	Completed	Yes	Yes	Yes	Yes
total-purses-=	Completed	Yes	Yes	Yes	Yes
at-mk-abpurse-defn	Completed	Yes	Yes	Yes	Yes
{a,b}-form	Completed	Yes	Yes	Yes	Yes

forall-elem-I	Completed	Yes	Yes	Yes	Yes
neq-add	Completed	Yes	Yes	Yes	Yes
subset-add	Completed	Yes	Yes	Yes	Yes
sumval-defn1	Completed	Yes	Yes	Yes	Yes
=-mk-AbPurse	Completed	Yes	Yes	Yes	Yes
card=O-E	Completed	Yes	Yes	Yes	Yes
sumval-form	JohnFitzgerald	Yes	Yes	No	No

External resources

A link to Richard Banach's slides on retrenchments: http://www.jiscmail.ac.uk/files/VSR-CONTRIBUTORS/SecondMondexWorkshop/banach.pdf

Slide 93 onwards contains the discussion Ken was talking about. It's in relation to the 'missing' balance enquiry operation (it's not included in the Z) The diagrams should help.

Slides from the other meetings are at http://isegserv.itd.rl.ac.uk/gc6wiki/ThirdMondexWorkshopAgenda (from October, with latest results) andhttp://isegserv.itd.rl.ac.uk/gc6wiki/SecondMondexWorkshopAgenda (from May, intermediate results).

Below are the final FACS papers on six approaches

- Alloy.pdf: Alloy approach
- KIV.pdf: KIV approach
- event-b.pdf: Event-B approach
- UML-OCL-USE.pdf: UML-OCL-USE approach
- RAISE.pdf: RAISE approach
- Z.pdf: Z approach

-- RichardPayne - 06 Nov 2007