Proof Theory in the VDM-SL standard

Roger Bishop Jones

ICL Defence Systems

In order to support the process of reasoning about formal specifications in VDM-SL and to provide a firm basis for computer based support of this process it is though appropriate to supply proof theory for VDM-SL in the standard.

This standard proof theory will define what is a *formal* proof. We do not propose to offer any guidance on what level of detail should be presented in informal proofs, whatever their degree of rigour.

The particular proof rules will serve primarily to give a definition of what theorems should be provable. They will form an example of a proof system which is sound, and reasonably complete in respect of the standard VDM-SL semantics. Developers of tools intended to support proofs in VDM-SL need not adopt the axioms and inference rules provided in the standard, but insofar as they deviate they take upon themselves the obligation to demonstrate the soundness of their proof rules. This might be done by reference to (or relative to) the proof rules in the standard.

The aspects of proof theory which will be addressed are:

1 *Syntax of Proofs*
An abstract syntax will be supplied for formal proofs in VDM-SL. This will encompass formal specification of a decidable set of axioms, and a formal specification of what is a valid inference step. A soundness proof will be sought, but need not be published in the standard.

2 *Verification Conditions*
The documented "context conditions" for VDM indicate at various points that certain "verification conditions" need proof to establish the type correctness of the specification. If the type system of standard VDM-SL is not effectively decidable then these points at which proof is required will be fully documented in the standard.

3 *Proof Obligations*
The literature on VDM provides details of "proof obligations". Some of the information documented under this heading properly belongs under the heading "syntax of proofs" and as such will form part of the standard. Such material as genuinely constitutes advice about what should be proven rather than definitions of what constitutes a proof will be reproduced in the standard but will be clearly shown to be advisory.

The initial source of this material will be "Systematic Software Development using VDM". This will be enhanced in detail and precision as necessary to support fully formal proof, and will be modified as necessary to match the syntax and semantics of VDM-SL.