

Oversigt over ISO/VDM-SL Standarden

Peter Gorm Larsen
 IFAD
 Instituttet For Anvendt Datateknik
 Forskerparken 10, DK-5230 Odense
 peter@ifad.dk

Abstract

VDM-SL er notationen, som bliver benyttet i den formelle metode VDM. Dette specifikationsprog bliver i øjeblikket standardiseret under både ISO og BSI. Det er et af de eneste specifikationsprog hvor den precise syntaks og semantik er blevet formelt defineret. I denne artikel vil jeg give et overblik over standarden og rapportere omkring den øjeblikkelige status for standardiseringen. Endelig vil jeg illustrere, hvorfor jeg mener, at det er vigtigt, at Danmark er med i dette arbejde.

1 Introduktion

Værdien af formelle metoder til udvikling af programmel bliver mere og mere accepteret. Formelle metoder giver en matematisk baseret tilgang til specifikation og efterfølgende udvikling af programmel. På denne måde opnår man en mere ingeniørmæssig tilgangsvinkel til programmeludvikling. På samme måde, som bygningsingeniøren bygger forskellige modeller og kan udføre forskellige beregninger på disse modeller, sætter dette programmeludvikleren i stand til at ræsonnere om sine modeller af programmet, som skal udvikles.

En af de mest modne formelle metoder, som primært er velegnet til specifikation og udvikling af de funktionelle aspekter ved programmel systemer, er VDM (Vienna Development Method) [1, 4]. Udviklingen af VDM startede i halvfjerdserne i IBM's afdeling i Wien. To af deltagerne i dette arbejde var Dines Bjørner og Cliff Jones. Senere blev Dines Bjørner ansat som professor på Danmarks Tekniske Højskole (DtH), hvor arbejdet med VDM fortsatte. Det centrale element i VDM er specifikationsproget VDM-SL, som kan benyttes både til meget abstrakte specifikationer men også til meget konkrete specifikationer.

I parallel med det videre arbejde med VDM på DtH blev Cliff Jones professor på Manchester Universitet, hvor hans gruppe koncentrerede sig om at benytte VDM til andre ting. Begge disse 'skoler' afledte en række

dialekter af specifikationsproget VDM-SL. Det øgede brug af VDM og det stigende antal af dialekter førte til en anerkendelse af nødvendigheden for en standard for VDM-SL. Det foregår under ISO/IEC JTC1. I Danmark følges arbejdet af en specialgruppe hos DS.

Det forventes, at en international standard for VDM-SL vil føre til:

- Øget brug af VDM. Standarden virker som et reference dokument for VDM-SL, således at den præcise betydning og udseende af VDM-SL specifikationer er fastlagt.
- Øget værktøjsstøtte for VDM. Tilgængeligheden af en standard øger mulighederne for at flytte specifikationer imellem forskellige værktøjer, og dette gør det meget mere attraktivt at udvikle sådanne værktøjer.
- En dybere indsigt i problemerne, som opstår ved en komplet formel definition af et specifikationsprog. Alle aspekter af VDM-SL er blevet formelt defineret, og naturligt sprog er kun benyttet til yderligere forklaring af definitionen.

I denne artikel vil jeg præsentere en kort oversigt over standarden for VDM-SL. En mere uddybende oversigt findes i [5] mens [3] kan benyttes som reference manual til sproget.

2 Oversigt over standarden

Allerede ved starten af standardiseringsprocessen var man enige om, at standarden primært skulle være baseret på eksisterende arbejde. En anden beslutning, som blev taget helt fra begyndelsen var, at standarden selv skulle være formelt defineret for at gøre den så præcis som muligt.

Den komplette definition af standarden for VDM-SL (som den er præsenteret i [2]) kan deles op i en række komponenter: en syntaks, symbolrepræsentationer, en statisk semantik, en dynamisk semantik og en syntaks

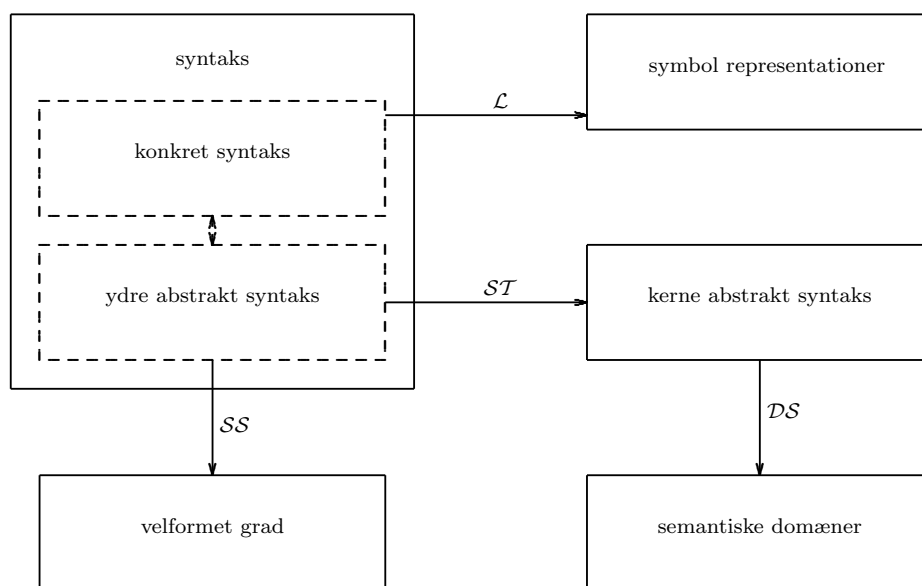


Figure 1: Strukturen af VDM-SL standarden

transformation. Relationen mellem disse komponenter er indikeret i figur 1 og hver komponent er yderligere beskrevet nedenfor.

2.1 Syntaksen

Syntaksen for VDM-SL eksistere i to former:

1. *EBNF omskrivningsregler*. EBNF formalismen er i dag den mest accepterede form til at definere den konkrete syntaks for et formelt sprog.
2. *VDM-SL type definitioner*. Denne form kaldes den Ydre Abstrakte Syntaks (YAS). Dette er indført til brug for de dele af standarden, som er defineret vha. VDM-SL funktioner. Til dette formål kan EBNF formen ikke bruges, fordi det er en helt anderledes formalisme. YAS bliver brugt både af den statiske semantik (\mathcal{SS}) og af syntaks transformationen (\mathcal{ST}).

2.2 Symbol repræsentationer

En VDM-SL specifikation har en repræsentation på papir, computer skærme osv. Standarden indeholder to sådanne forskellige repræsentationer:

1. En matematisk repræsentation. Den matematiske repræsentation indeholder matematiske sym-

boler, som ligger så tæt som muligt op ad generelt accepteret matematisk notation.

2. En ASCII repræsentation som primært er defineret for at gøre det muligt at behandle VDM-SL specifikationer automatisk vha. værktøjer.

2.3 Kerne Abstrakt Syntaksen

Ud over den ydre abstrakte syntaks indeholder standarden også en anden abstrakt syntaks, som er mindre kompliceret: kerne abstrakt syntaksen. Denne bliver brugt som basis for definitionen af den formelle semantik af sproget (også kaldet den dynamiske semantik). Kerne abstrakt syntaksen blev indført for at simplificere den formelle semantik af sproget.

2.4 Syntaks transformationen

Standarden indeholder en formel definition af en syntaks transformation (\mathcal{ST}) fra specifikationer formuleret i den ydre abstrakte syntaks til specifikationer formuleret i kerne abstrakt syntaksen.

2.5 Den dynamiske semantik

Alle VDM specifikationer, som kan repræsenteres i kerne abstrakt syntaksen, får tildelt en betydning af

den dynamiske semantik (\mathcal{DS}). Betydningen af en VDM specifikation kan betragtes som *en mængde af modeller*, fordi specifikationer kan være *løse*. Løs specifikation er en teknik, som kan benyttes i VDM-SL ved på en abstrakt måde at specificere at forskellig funktionalitet er acceptabel.

2.6 Den statiske semantik

VDM specifikationer, som er syntaktiske korrekte i forhold til EBNF reglerne, følger ikke nødvendigvis type- og virkefelts-reglerne for sproget. Standarden indeholder derfor også en formel definition af hvorvidt en specifikation er velformet: den statiske semantik (\mathcal{SS}) af sproget. Den statiske semantik er selv formuleret i VDM-SL.

De VDM specifikationer som har mindst en model i den dynamiske semantik kan betragtes som dem der er velformede. Generelt er det ikke afgørende hvorvidt en VDM specifikation er velformet eller ej. Definitionen af den statiske semantik afviger fra, hvad der er blevet defineret for andre sprog, ved kun at acceptere de specifikationer, som helt sikkert er velformet, og kun afvise specifikationer som helt sikkert ikke er velformet. Derfor levere den statiske semantik en velformet grad til enhver VDM specifikation.

3 Status

Arbejdet, som har ført frem til det udkast til standarden for VDM-SL, startede i BSI regi med et panel af internationale eksperter. I udkastet har panelet været sammen om at stå for syntaksen og symbolrepræsentationerne, mens Delft Universitet fra Holland har været ansvarlig for syntaks transformationen. DtH har været ansvarlig for den statiske semantik, og IFAD har været ansvarlig for kerne abstrakt syntaksen og den tilhørende dynamiske semantik. Der er derfor allerede meget af standarden, som er lavet fra dansk side, og derfor mener jeg, at det er vigtigt, at det videre arbejde med denne standard får dansk indflydelse. Det er dog endnu mere væsentligt, at VDM-SL faktisk bliver industrielt anvendt herhjemme. Både Teleteknisk Forskningslabo-

ratorium (TFL), Dansk Datamatik Center – International (DDC-I) og IFAD selv anvender VDM-SL i udviklingen af specifikationer og design.

I April 1993 vil der blive afholdt en konference, som hedder “Formal Methods Europe ’93” i Odense, som IFAD er ansvarlig for at arrangere. Denne konference handler generelt om formelle metoder, hvor VDM blot er en af dem. I ugen efter vil det næste SC/WG19 møde (tre dage) blive afholdt hos IFAD, hvor det forventes at det forløbige udkast til VDM standarden ophøjes til “draft for comments”.

Med hensyn til værktøjer så ser det også ud til at arbejdet med standarden har øget interessen for konstruktion af værktøjsstøtte. I [6] kan det ses at mange værktøjsproducenter er skiftet fra deres egen tidligere dialekt af VDM-SL til at følge den kommende standard. Dette var også synligt ved VDM’91 konferencen (forløber for FME’93) hvor en stor række værktøjer, som understøttede standarden, blev demonstreret. IFAD har også selv produceret en VDM-SL toolbox som bliver solgt kommercielt.

Yderligere information

Yderligere information om standardiseringen af VDM-SL kan fås fra den danske arbejdsgruppe. Kontakt sekretariatet, Dansk Standard.

References

- [1] Dines Bjørner and Cliff B. Jones. *Formal Specification & Software Development*. Series in Computer Science. Prentice-Hall International, 1982.
- [2] VDM Specification Language – Proto-Standard. British Standards Institution, August 1992. BSI IST/5/19 N-231.
- [3] John Dawes. *The VDM-SL Reference Guide*. Pitman, 1991.
- [4] Cliff B. Jones. *Systematic Software Development Using VDM (second edition)*. Prentice-Hall International, Englewood Cliffs, New Jersey, 1990.
- [5] Nico Plat and Peter Gorm Larsen. An Overview of the ISO/VDM-SL Standard. *Sigplan Notices*, 27:76–82, August 1992.
- [6] Nico Plat and Hans Toetenel. Tool support for VDM. Technical Report 89-81, Delft University of Technology, 1989.