Formele specifikatie met PSF

dr. Sjouke Mauw

Sinds 1991 wordt bij de sektie Theoretische Informatica van de TU Eindhoven onderzoek verricht naar het gebruik van procesalgebra voor het beschrijven van gedistribueerde systemen. Bij praktische toepassingen wordt gebruik gemaakt van de taal PSF. Voor deze op procesalgebra gebaseerde specificatietaal zijn verschillende computertools ontworpen, welke te zamen de PSF-toolkit vormen. Dit jaar maakt PSF voor het eerst deel uit van het curriculum voor de tweejarige ontwerpersopleiding. Daarom volgt hieronder een overzicht van de taal en haar toepassingen.

Procesalgebra

Het lijkt wat overdadig om in een wereld die al overspoeld wordt door een grote verscheidenheid aan programmeertalen weer een nieuw specificatieformalisme in het leven te roepen. De belangrijkste reden om toch tot deze stap over te gaan is de wens om de toepasbaarheid van procesalgebra voor grotere applicaties te bestuderen. Procesalgebra is een wiskundige theorie voor het specificeren en verifiëren van parallelle systemen. Er bestaan verschillende benaderingen binnen de procesalgebra, waarvan CCS en CSP wel de bekendste zijn. Een meer algemene theorie is ACP, wat staat voor Algebra of Communicating Processes. Deze theorie is de laatste tien jaar ontwikkeld door Bergstra, Klop en Baeten bij het Centrum voor Wiskunde en Informatica en de Universiteit van Amsterdam.

Zoals geen enkele theorie zich direkt leent voor implementatie, kent ook ACP zijn bezwaren bij het ontwikkelen van computerondersteuning. De belangrijkste obstakels zijn de informele behandeling van datatypen, de informele non-ASCII syntax en – vooral een probleem voor grotere toepassingen – het gebrek aan struktureringsmogelijkheden. Dit is de motivatie geweest om een op ACP gebaseerd konkreet formalisme te ontwerpen. Deze taal heeft de naam PSF meegekregen, een afkorting van Process Specification Formalism. PSF staat zo dicht als mogelijk is bij ACP. Hierbij zijn keuzes gemaakt met betrekking tot de konkrete syntax, modulariseringskonstrukties en specificatie van datatypen (te weten algebraïsche specificaties). De relevantie van PSF ligt niet in het bestaan van een efficiënte implementatie, een elegante syntax of gebruik van het modewoord *object oriented*, maar in de wiskundige helderheid van de theorie ACP.

Processen

Een specificatie in PSF bestaat uit een aantal *modulen*. Een module bevat een aantal bij elkaar horende declaraties en definities en is bijvoorbeeld vergelijkbaar met het package begrip in Ada. Een zogenaamde procesmodule bevat de beschrijving van het gedrag van één of meer processen. Een proces is vergelijkbaar met het begrip task uit Ada. Een klein voorbeeldje van een procesmodule volgt hieronder. Deze bevat de beschrijving van een eenvoudige koffie- en thee-automaat.

```
process module koffie-machine
begin
  atoms
    dubbeltje, kwartje,
    thee, koffie
  processes
    automaat
  definitions
    automaat =
     (dubbeltje . thee +
      kwartje . koffie ) . automaat
end koffie-machine
```

In de module met de naam `koffie-machine` worden allereerst vier atomaire akties gedelareerd. Een dergelijke aktie is een primitieve ondeelbare eenheid van gedrag. De atomen `dubbeltje` en `kwartje` zijn te interpreteren als het inwerpen van een muntstuk, en de atomen `thee` en `koffie` als het uitschenken van een bekertje. Vervolgens wordt het proces `automaat` gedeklareerd en wordt zijn gedrag gespecificeerd. De + en de . zijn twee primitieve procesalgebra operatoren. Ze staan voor een alternatieve compositie (keuze tussen de operanden) en voor sequentiële compositie (opvolging van de operanden). De automaat kan dus een dubbeltje ontvangen, gevolgd door het serveren van thee of hij kan een kwartje ontvangen,

gevolgd door het schenken van een kopje koffie. Is het schenken afgelopen, dan zal in beide gevallen de automaat weer naar zijn uitgangssituatie terugkeren. Dit is weergegeven door de recursieve aanroep van het proces `automaat`.

Data

Vaak zal het voorkomen dat twee onderscheiden akties grofweg gelijk zijn en slechts verschillen in de precieze gegevens die verwerkt worden. Zo zijn `dubbeltje` en `kwartje` twee bijzondere gevallen van een aktie muntinworp. We beschouwen `dubbeltje` en `kwartje` dan als elementen van een datatype dat gebruikt kan worden als index van een aktie `inworp`. Datatypen worden gespecificeerd in een datamodule.

```
data module geld-en-drank
begin
  exports
    begin
      sorts
        drank, munt
      functions
        thee : -> drank
        koffie : -> drank
        dubbeltje : -> munt
        kwartje : -> munt
        keuze : munt -> drank
    end
  equations
    [1] keuze(dubbeltje) = thee
    [2] keuze(kwartje) = koffie
end geld-en-drank
```

In deze module worden twee soorten (ofwel types) gedeklareerd: `drank` en `munt`. Er zijn twee constante functies van soort `drank` en twee constante functies van soort `munt`. Verder is er een éénplaatsige functie `keuze` die gegeven een munt bepaalt welke drank erbij hoort. Deze laatste functie is gedefinieerd in de sectie die begint met het woord `equations`. We hebben expliciet aangegeven dat de genoemde soorten en functies aan andere modulen ter beschikking worden gesteld door middel van het woord `exports`. Door nu de module `geld-en-drank` te importeren kan de volgende module gebruik maken van alle geëxporteerde objecten.

```
process module koffie-machine
begin
  imports
    geld-en-drank
  atoms
    inworp : munt
    schenk : drank
  processes
    automaat
  definitions
    automaat =
        sum(m in munt,
          inworp(m)
          schenk(keuze(m)))
          automaat
end koffie-machine
```

De nieuwe koffiemachine heeft nu twee geparametriseerde akties, `inworp` en `schenk`. Het gedrag van de koffiemachine is nu uniformer: Voor een willekeurige munt m is nu de aktie `inworp(m)` mogelijk. Vervolgens wordt bepaald welke drank bij de gegeven munt behoort en deze wordt geschonken.
Naast bovengenoemde operatoren bevat PSF ook operatoren voor bijvoorbeeld het parallel samenstellen van processen. Ook de mogelijkheden op het gebied van algebraïsch specificeren en modularisering zijn uitgebreider dan in het voorbeeldje aangegeven. Zo is het mogelijk om modules te parametriseren en dus geschikt te maken voor hergebruik.

Tools

In de afgelopen tijd zijn verschillende mensen bezig geweest bij het vervaardigen van computertools die PSF moeten ondersteunen. Dit werk is zowel door professionele programmeurs als door stagestudenten gedaan. De verzameling tools die zo is ontstaan wordt de PSF-toolkit genoemd. Het centrale onderdeel is de compiler die PSF naar een eenvoudig te verwerken interne representatie vertaalt. Behalve het controleren van syntax en statische semantiek biedt de compiler de mogelijkheid tot gescheiden compilatie per module. Hierdoor is het mogelijk grotere specificaties efficiënter te verwerken en bibliotheken van opnieuw te gebruiken modules te maken. Alle andere tools werken op de interne representatie en zijn onafhankelijk van elkaar. Dit zijn onder meer een simulator, waarmee gedrag van processen geobserveerd kan worden, en een termherschrijver, waarmee de definities van de datatypen getest kunnen worden. Daarnaast zijn er prototypes van tools die ondersteunen bij het verifiëren van de correctheid van een specificatie.

Toepassingen

Bij het ontwerp van de taal en de toolkit is niet in eerste instantie gestreefd naar een commercieel bruikbaar produkt. De syntax van PSF is niet altijd ideaal en uit case studies blijkt dat er regelmatig behoefte is aan extra operatoren zoals bijvoorbeeld

voor interrupt-afhandeling. Daaarnaast is de toolkit slechts een verzameling prototypes waarmee onderzocht kan worden aan welke computerondersteuning behoefte is en hoe speciaal ontworpen algoritmen zich in de praktijk gedragen. Toch wordt PSF bij diverse commerciële instellingen toegepast voor pilot-studies. Bij Philips worden met PSF communicatieprotocollen voor diverse toepassingen ontworpen en getest. Bij DEC is al het derde vervolgproject gaande voor het beschrijven van CIM architecturen met PSF en sinds kort wordt in samenwerking met nederland-haarlem getracht verkeersregelsystemen te beschrijven. Samenwerkingsprojekten met bijvoorbeeld de PTT en academische partners leveren ook regelmatig case studies op. Samenvattend kan ik stellen dat PSF niet alleen aan zijn doelstelling als academisch onderzoeksobject voldoet, maar dat in veel praktische situaties blijkt dat men uitstekend met PSF uit de voeten kan.

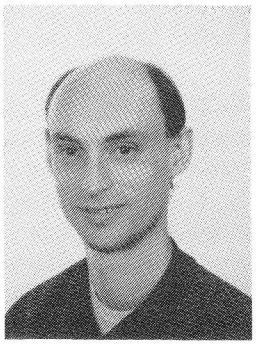
Literatuur

Wie meer wil weten over ACP, PSF en toepassingen kan kontakt opnemen met de auteur. De volgende werken vormen de basisreferenties voor ACP en PSF.

- J.C.M. Baeten en W.P. Weijland, "Process algebra", *Cambridge Tracts in Theoretical Computer Science* Vol. 18, Cambridge University Press, 1990.

- S. Mauw en G.J. Veltink, "A process specification formalism", *Fundamenta Informaticae* XIII (1990), pp. 85-139, IOS Press, 1990.

□



Dr. Sjouke Mauw is universitair docent bij de sektie Theoretische Informatica van de Technische Universiteit Eindhoven. In 1991 is hij gepromoveerd op het ontwerp en de toepassing van PSF.

Certificering OOTI

Vervolg van pagina 17

kommissie gevormd met mensen van BSO, Hollandse Signaal, Philips en Shell. In vergelijking met voorgaande kommissies die andere opleidingen onder de loupe namen, is deze kommissie erg grondig te werk gegaan. Waar anderen zich beperkten tot gesprekken met de opleidingsgroep en het inzien van afstudeerverslagen, heeft deze kommissie zich ook de moeite getroost interviews te houden met kursisten en afgestudeerden en hun bazen. Wellicht is dat de reden dat het adviesrapport wat op zich heeft laten wachten. Er werd verwacht dat het rapport in de CCTO vergadering van 23 maart jl. besproken had kunnen worden, maar omdat het rapport daar nog niet gearriveerd was, zal het nu pas mei worden voordat er een beslissing over certificatie genomen kan worden. Overigens, naar verluid is het rapport positief over de OOTI opleiding en zal certificering dus geen struikelblok vormen.

Openbaarheid

Het lijkt wel of feit dat er financiële belangen gemoeid zijn met het oordeel van de CCTO ertoe heeft geleid dat de CCTO besloten heeft de inhoud van het adviesrapport van de beoordelingskommissie als vertrouwelijk te beschouwen. Of er al dan niet een certificaat is verstrekt en welke procedure bij de beoordeling is gevolgd is publiceerbaar, maar het wordt aan het CvB van de betreffende universiteit overgelaten of de gedetailleerde bevindingen en aanbevelingen worden vrijgegeven. De redaktie van het "XOOTIC MAGAZINE" is het niet eens met deze stellingname. In het geval van OOTI hebben kursisten en afgestudeerden meegewerkt aan de beoordeling en zouden zij alleen al uit dien hoofde recht moeten hebben op terugmelding van de resultaten. Verder vindt de redaktie dat potentiële kursisten recht hebben op een open en eerlijke voorlichting over de opleiding, waarvoor zij hun karriëre nog twee jaar willen uitstellen. Of de opleiding van hun keuze over voldoende kwaliteit beschikt, kunnen zij niet te weten komen uit wervende folders, maar wel uit een rapport van een externe beoordelingskommissie. Naar de mening van de redaktie zou het "XOOTIC MAGAZINE" dé plaats zijn om de resultaten van zo'n rapport te bespreken. Tenslotte heeft "XOOTIC" een in haar statuten verankerde kritische, maar opbouwende houding ten opzichte van OOTI. □