STELLINGEN

ABSTRACT INTERPRETATION AND PARTITION REFINEMENT FOR MODEL CHECKING

DENNIS RENÉ DAMS

T U E
F W I

I

Abstracte interpretatie is primair gericht op *data-flow analyse* van programma's; voor toepassing in programma*verificatie* dient deze techniek te worden uitgebreid met methodes ter verfijning van abstracties.

Zie: dit proefschrift.

II

Lemma 3.3.1.1 in dit proefschrift is een *folk theorem* in de zin van [Har80].

[Har80] David Harel. On folk theorems. *Communications of the ACM*, 23(7):379–389, 1980.

III

Hoewel in elk model met eindige vertakkingsgraad de implicatie $\equiv^i_{\text{bis}} = \equiv^{i+1}_{\text{bis}} \;\Rightarrow\; \equiv^i_{\text{bis}} = \equiv_{\text{bis}}$ geldt, volgt uit $\mathit{simeq}^i = \mathit{simeq}^{i+1}$ niet altijd dat $\mathit{simeq}^i = \mathit{simeq}$ in dergelijke modellen.

Zie: Sectie 5.5.1 van dit proefschrift. De *approximanden* simeq^i en $\equiv^i_{\text{bis}}$ van simulatie equivalentie (*simeq*) en bisimulatie ($\equiv_{\text{bis}}$) resp. worden gedefinieerd in Definitie 2.4.2.6 en 6.4.0.5.

IV

Hoewel het onderscheidende vermogen van de logica's CTL$^*(\mathsf{U})$ en flatCTL$^*(\mathsf{U})$ hetzelfde is, is het expressieve vermogen verschillend: de formule $\exists\mathsf{U}(r \vee \mathsf{U}(p, q \wedge \mathsf{U}(q, r)), s \wedge \mathsf{U}(s, t \wedge \mathsf{U}(t, u)))$ in CTL$^*(\mathsf{U})$ heeft geen equivalent in flatCTL$^*(\mathsf{U})$.

Zie: o.a. Sectie 6.5 van dit proefschrift. CTL$^*(\mathsf{U})$ (= CTL* zonder *next*) wordt gedefinieerd in Definitie 2.3.1.1, flatCTL$^*(\mathsf{U})$ (= CTL$^*(\mathsf{U})$ waarin het linker argument van de *until* geen temporele modaliteiten mag bevatten) in Definitie 6.5.0.1.

V

De *metric operators* van [Koy89] en de *freeze quantifiers* van [AH89] suggereren twee verschillende manieren om CTL* en CTL uit te breiden met kwantitatieve temporele operatoren (zie [ACD93], pagina's 30–31). In het eerste geval zal dit resulteren in *real-time* versies van deze logica's met een verschillend onderscheidend vermogen, terwijl in het tweede geval het onderscheidende vermogen hetzelfde blijft.

[Koy89] Ron Koymans. *Specifying Message Passing and Time-Critical Systems with Temporal Logic*. Proefschrift, Technische Universiteit Eindhoven, mei 1989.

[AH89] Rajeev Alur en Thomas A. Henzinger. A really temporal logic. In *30th IEEE Symposium on Foundations of Computer Science*, pagina's 164–169. IEEE Computer Society Press, Los Alamitos, CA, 1989.

[ACD93] Rajeev Alur, Costas Courcoubetis, en David Dill. Model-checking in dense real-time. *Information and Computation*, 104:2–34, 1993.

VI

Onderdeel 5b van Lemma 2.2 in [CDY91], dat incorrect gesteld is (zie [Kin94]), kan zonder gevolgen voor de ernaar refererende bewijzen van Lemmata 5.2 en 5.3 hersteld worden door de laatste regel, "x and y are not both in p", te vervangen door "x and y are on opposite sides of e, or x and y are both in $vars(q)$".

[CDY91] Michael Codish, Dennis Dams, en Eyal Yardeni. Derivation and safety of an abstract unification algorithm for groundness and aliasing analysis. In Koichi Furukawa, editor, *Logic Programming. Proceedings of the Eighth International Conference*, pagina's 79–93. The MIT Press, Cambridge, Mass., 1991.

[Kin94] Andy King. A synergistic analysis for sharing and groundness which traces linearity. In Donald Sanella, editor, *Programming Languages and Systems — ESOP '94*, nummer 788 in LNCS, pagina's 363–378. Springer-Verlag, Berlijn, 1994.

VII

Publicatiedruk leidt tot fragmentering van het wetenschappelijke cultuurgoed.

VIII

Indien de Derde Joodse Tempel naar model van de vorige twee er ooit komt, zal dit dagelijks tot slachtoffers op het tempelplein leiden.

Zie: Leviticus 1–9.

Misjna Zebachim. (Uitgave: H. Danby, editor. Oxford University Press, 1933.)

E. P. Sanders. Judaism : practice and belief. SCM Press, Londen, 1992.

IX

Het gebruik van de term *fair-play sport* met betrekking tot specifieke sporten als ultimate frisbie impliceert dat andere sporten op gemeen spel gebaseerd zijn.

X

Hoewel het messiaanse thema een andere oorsprong heeft dan het graalthema, zijn beide gebaseerd op de universeel-menselijke behoefte om te hopen op een *point sublime*, waarop alle tegenstellingen worden opgeheven (vgl. het voorwoord van [Gra48]). Een belangrijk verschil is dat in het geval van de graal de queeste een belangrijk element vormt, terwijl de komst van de messias afgewacht wordt.

[Gra48] Julien Gracq. Le roi pêcheur (toneel). Librairie José Corti, Parijs, 1948.

z.o.z.

XI

Het is niet duidelijk welke versie van de in de afgelopen jaren opgestelde concept-promotiereglementen van de TUE van kracht is op de onderhavige promotie.

XII

De grens tussen noord- en zuid-Nederland ligt in het oosten noordelijker dan in het westen.

XIII

Hoewel er niet altijd een scherpe scheidslijn tussen stellingen en meningen getrokken kan worden, meen ik te mogen stellen dat de “schertsstelling” veelal een mening verwoordt.