V³F : Validation & Vérification en présence de calculs à Virgule Flottante

Partenaires : *laboratoires et équipes*

- LIFC - CNRS - INRIA - *Cassis* (Coordinateur)
- I3S - CNRS - CERMICS - INRIA - *Coprin*
- IRISA - CNRS - INRIA – *Vertecs / Lande*
- CEA – *Lsl / List*

http://lifc.univ-fcomte.fr/%7Ev3f/

Logiciels Critiques

⌘ Dans des systèmes à fortes contraintes de sécurité

⌘ Domaines concernés :

Transport férroviaire et automobile (Meteor, ABS, Airbag, …)
Energie (contrôle/commande des centrales nucléaires,…)
Avionique civile et militaire (calculateurs, systèmes d'armes,…)
Espace (logiciels embarqués dans les satellites, robots,…)

⌘ Nécessitent un effort accru de V&V

en particulier, en présence de calculs à virgule flottante

Les nombres à virgule flottante (IEEE 754)

⌘ Normalisés ($0 < e < e_{max}$)

mantisse (23, 52 bits ou étendus)

$$(-1)^s \; 1.f \; 2^{(e - biais)}$$

Signe (1 bit)

exposant (8, 11 bits ou étendus)

⌘ Dénormalisés ($e = 0$) $(-1)^s \; 0.f \; 2^{(-biais + 1)}$

+0.0, -0.0, +INF, -INF, NaNs ($e = e_{max}$)

⌘ 4 modes d'arrondi (near,up,down,chop), 5 types d'exceptions

⌘ Pour +, -, x, /, √, remainder et conversions :
le résultat flottant d'une opération élémentaire entre flottants est l'arrondi du résultat exact

Problème posé par les flottants en V&V

⌘ Approximation très pauvre des nombres réels (ens. fini, non uniform. réparti, + et x non associatifs,…)

⌘ Absorption ($X_r + \varepsilon == X_r$), Cancellation ($X_r - Y_r == K.(X-Y)$)

⌘ Exemple de problème-type en V&V :

if(X + 16.0 == 16.0 && X > 0.0 **)**

…

Ici, aucune solution sur les réels, beaucoup de solutions sur les flottants (arrondi = near)

Résolution de contraintes par propagation d'intervalles

- **Arithmétique des Intervalles**

  [a, b] + [c, d] = [a+c, b+d]

  [a, b] - [c, d] = [a-d, b-c]

  exp([a,b]) = [exp(a), exp(b)] car exp est strict. croissante

  …

- **Relations sur Intervalles** (fonctions de projections)

  $X \in [a,b], Y \in [c,d], \quad X = Y$

  $X \leftarrow Y$ donne $X,Y \in [\max\{a,c\}, \min\{b,d\}]$

  $Y \leftarrow X$

- **Propagation de contraintes et convergence**

  jusqu'à atteindre un point fixe

Exemple : $X + \log(X) = 0$

4 fonctions de projections

$X \leftarrow \exp(Y)$ ①

$Y \leftarrow \log(X)$ ②

$X \leftarrow -Y$ ③

$Y \leftarrow -X$ ④

	①	①	①	①
$X \in$	$[-\infty,+\infty]$	$[0,+\infty]$	$[0, 1]$	$[0.56, 1]$	$[0.56, 0.57]$
$Y \in$	$[-\infty,+\infty]$	$[-\infty, 0]$	$[-1, 0]$	$[-1, -0.56]$	$[-0.57,-0.56]$
	④	④	④	④	

Si il existe une solution X, alors $X \in [0.56, 0.57]$

Ici, X est vu comme un réel et non pas un flottant !

Applications potentielles d'un solveur sur les flottants en V&V

- Génération automatique de cas de tests structurels et fonctionnels
- Génération automatique de l'oracle depuis une spécification formelle
- Animation de modèle
- Analyse statique du code source pour la détection automatique de fautes
- Preuve de programmes (vérification déductive)

…

Projet V³F

⌘ 36 mois - 4 partenaires académiques

- **LIFC - CNRS - INRIA - *Cassis* (Coordinateur)**
  - Animation de modèle B par contraintes ensemblistes
  - Génération automatique de cas de test fonctionnel
- **I3S - CNRS - CERMICS - INRIA - *Coprin***
  - Contraintes sur les domaines continus et flottants
- **IRISA - CNRS - INRIA – *Vertecs / Lande***
  - Génération automatique de cas de test de conformité
  - Génération automatique de cas de test structurel
- **CEA – *Lsl / List***
  - Génération de test fonctionnel à partir de Lustre
  - Validation de la précision numérique

Travaux à mener

- Solveur sur les flottants (I3S-Coprin)
- Etude de l'intégration des flottants dans plusieurs notations formelles (LUSTRE, B, OCL, IF, …) et de la formalisation du test en présence de flottants
- Mise en œuvre dans les outils des partenaires
  LIFC-Cassis : BZ-Testing-Tools
  IRISA-Vertecs/Lande : TGV-STG, UML-Casting
  Lsl/List-CEA : GATEL, Fluctuat
- Exploitation du solveur et évaluation expérimentale

Participants

⌘ Fabrice Ambert, Fabrice Bouquet, Sébastien Chemin, Bruno Legeard, Fabien Nicolet, Nicolas Vacelet

⌘ Hélène Collavizza, David Daney, Claude Michel, Yahia Lebbah, Michel Rueher

⌘ Arnaud Gotlieb, Bertrand Jeannet, Thierry Jéron

⌘ Eric Goubault, Bruno Marre, Matthieu Martel, Sylvie Putot, Franck Védrine