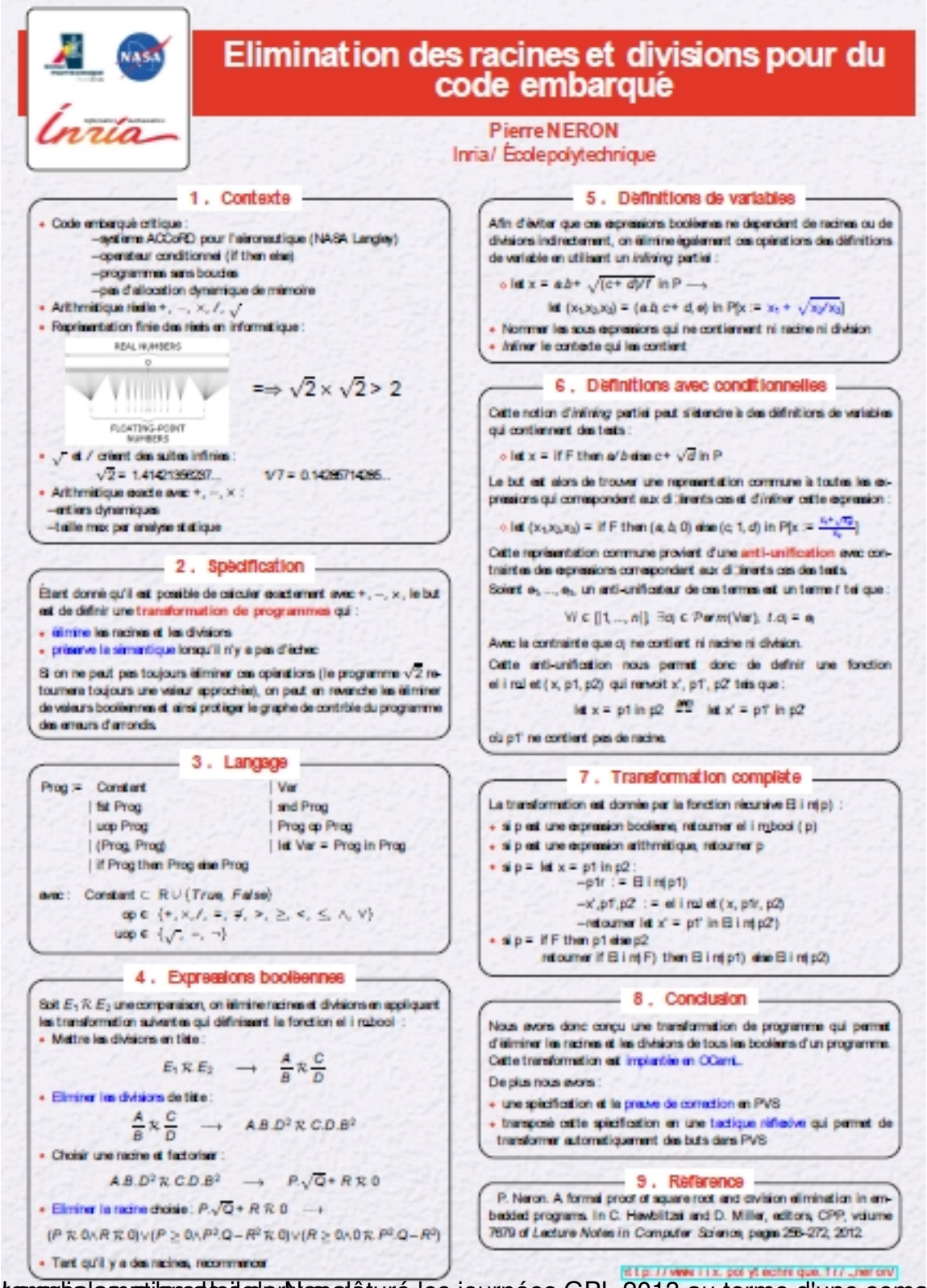
La session poster a réuni une quinzaine de posters et démos, installés le long de la "rue des posters" (merci à Jean-Pierre Jacquot pour cette photo).

Le prix du meilleur poster a été attribué à Pierre Neron pour son poster intitulé "Elimination des racines et divisions pour du code embarqué".



Elimination des racines et divisions pour du code embarqué

Pierre NERON
Inria/ Écolepolytechnique

1. Contexte

- Code embarqué critique :
  - système ACCoRD pour l'aéronautique (NASA Langley)
  - opérateur conditionnel (if then else)
  - programmes sans boucles
  - pas d'allocation dynamique de mémoire
- Arithmétique réelle $+, -, \times, /, \sqrt{}$
- Représentation finie des réels en informatique :

$\Rightarrow \sqrt{2} \times \sqrt{2} > 2$

- $\sqrt{}$ et / créent des suites infinies :
  $\sqrt{2} = 1.41421356237...$ $1/7 = 0.14285714286...$
- Arithmétique exacte avec $+, -, \times$:
  - entiers dynamiques
  - taille mix par analyse statique

2. Spécification

Étant donné qu'il est possible de calculer exactement avec $+, -, \times$, le but est de définir une transformation de programmes qui :

- élimine les racines et les divisions
- préserve la sémantique lorsqu'il n'y a pas d'échec

Si on ne peut pas toujours éliminer ces opérations (le programme $\sqrt{2}$ retournera toujours une valeur approchée), on peut en revanche les éliminer de valeurs booléennes et ainsi protéger le graphe de contrôle du programme des erreurs d'arrondis.

3. Langage

Prog :=	Constant	| Var
	| fst Prog	| snd Prog
	| uop Prog	| Prog op Prog
	| (Prog, Prog)	| let Var = Prog in Prog
	| if Prog then Prog else Prog	

avec : Constant $\subset \mathbb{R} \cup \{True, False\}$
$op \in \{+, \times, /, =, \neq, >, \geq, <, \leq, \wedge, \vee\}$
$uop \in \{\sqrt{}, -, \neg\}$

4. Expressions booléennes

Soit $E_1 \mathbin{\mathcal{R}} E_2$ une comparaison, on élimine racines et divisions en appliquant les transformation suivantes qui définissent la fonction el i m_bool :

- Mettre les divisions en tête :

$$E_1 \mathbin{\mathcal{R}} E_2 \longrightarrow \frac{A}{B} \mathbin{\mathcal{R}} \frac{C}{D}$$

- Eliminer les divisions de tête :

$$\frac{A}{B} \mathbin{\mathcal{R}} \frac{C}{D} \longrightarrow A.B.D^2 \mathbin{\mathcal{R}} C.D.B^2$$

- Choisir une racine et factoriser :

$$A.B.D^2 \mathbin{\mathcal{R}} C.D.B^2 \longrightarrow P.\sqrt{Q} + R \mathbin{\mathcal{R}} 0$$

- Eliminer la racine choisie : $P.\sqrt{Q} + R \mathbin{\mathcal{R}} 0 \longrightarrow$

$$(P \mathbin{\mathcal{R}} 0 \wedge R \mathbin{\mathcal{R}} 0) \vee (P \geq 0 \wedge P^2.Q - R^2 \mathbin{\mathcal{R}} 0) \vee (R \geq 0 \wedge 0 \mathbin{\mathcal{R}} P^2.Q - R^2)$$

- Tant qu'il y a des racines, recommencer

5. Définitions de variables

Afin d'éviter que ces expressions booléennes ne dépendent de racines ou de divisions indirectement, on élimine également ces opérations des définitions de variable en utilisant un *inlining* partiel :

- let $x = a.b + \sqrt{(c + d)/f}$ in P $\longrightarrow$

  let $(x_1,x_2,x_3) = (a,b,c+d,e)$ in P[$x := x_1 + \sqrt{x_2/x_3}$]

- Nommer les sous expressions qui ne contiennent ni racine ni division
- Inliner le contexte qui les contient

6. Définitions avec conditionnelles

Cette notion d'*inlining* partiel peut s'étendre à des définitions de variables qui contiennent des tests :

- let x = if F then a/b else $c + \sqrt{d}$ in P

Le but est alors de trouver une représentation commune à toutes les expressions qui correspondent aux différents cas et d'inliner cette expression :

- let (x_1,x_2,x_3) = if F then $(a,b,0)$ else $(c,1,d)$ in P[$x := \frac{x_1 + \sqrt{x_2}}{x_3}$]

Cette représentation commune provient d'une anti-unification avec contraintes des expressions correspondent aux différents cas des tests.
Soient $e_1, ..., e_n$ un anti-unificateur de ces termes et un terme t tel que :

$$\forall\, c \in [|1, ..., n|],\ \exists \sigma_c \in Perm(Var),\ t.\sigma_c = e_c$$

Avec la contrainte que σ_c ne contient ni racine ni division.
Cette anti-unification nous permet donc de définir une fonction el i nal et (x, p1, p2) qui renvoit x', pT, pZ tels que :

let x = p1 in p2 $\overset{pT}{\longrightarrow}$ let x' = pT in p2

où pT ne contient pas de racine.

7. Transformation complète

La transformation est donnée par la fonction récursive El i m(p) :

- si p est une expression booléenne, retourner el i m_bool (p)
- si p est une expression arithmétique, retourner p
- si p = let x = p1 in p2 :
  - p1r : = El i m(p1)
  - x',pT,pZ' : = el i nal et (x, p1r, p2)
  - retourner let x' = pT in El i m(pZ)
- si p = if F then p1 else p2
  retourner if El i m(F) then El i m(p1) else El i m(p2)

8. Conclusion

Nous avons donc conçu une transformation de programme qui permet d'éliminer les racines et les divisions de tous les booléens d'un programme. Cette transformation est implantée en OCaml.

De plus nous avons :

- une spécification et la preuve de correction en PVS
- transposé cette spécification en une tactique réflexive qui permet de transformer automatiquement des buts dans PVS

9. Référence

P. Neron. A formal proof of square root and division elimination in embedded programs. In C. Havelitzai and D. Miller, editors, CPP, volume 7679 of *Lecture Notes in Computer Science*, pages 256-272, 2012.

http://www.lix.polytechnique.fr/~neron/

Le poster a valu le 3e prix au concours de posters. Nancy a clôturé les journées GPL 2013 au terme d'une semaine bien


PierreNeron