SAP — TD7 — Interprétation abstraite (domaines numériques)

6 avril 2010

1 Élargissement

1.1 Cas facile

Dans un gros programme, on trouve :

```
while (true) {
  /* piloter l'avion */
  /* sans toucher la variable i */

  i++;
  if (i >= 20) {
    i=0;
  }
}
```

L'idée est qu'on quelque part dans la boucle des accès t[i] dans un tampon circulaire implémenté à l'aide d'un tableau t, et que les indices corrects sont 0..19. On doit donc afficher des avertissements si on ne peut prouver qu'ils sont bien dans cet intervalle.

Calculez les itérations successives des intervalles sur i. Pratiquez l'élargissement standard : que trouvez-vous ?

Faites tourner un tour de plus la boucle à partir de l'invariant inductif que vous avez obtenu : que trouvez-vous ? Cela vous convient-il ?

1.2 Cas plus dur

```
while (true) {
  /* piloter l'avion */
  /* sans toucher la variable i */

  i++;
  if (i == 20) {
    i=0;
  }
}
```

Calculez les itérations successives des intervalles sur i. Pratiquez l'élargissement standard : que trouvez-vous ?

Faites tourner un tour de plus la boucle à partir de l'invariant inductif que vous avez obtenu : que trouvez-vous ? Cela vous convient-il ?

Note : Une solution pas chère est de parcourir syntaxiquement le programme avant de lancer l'analyse, de repérer la comparaison $i = 20$ et de se dire qu'avant d'élargir à $+\infty$ il vaut mieux essayer d'élargir à 20 ± 1.

1.3 Autre cas qui ne fonctionne pas

```
while (true) {
  /* piloter l'avion */
  /* sans toucher la variable i */

  if (on_fait_un_truc()) {
    i++;
    if (i >= 20) {
      i=0;
    }
  }
}
```

Calculez les itérations successives des intervalles sur i. Pratiquez l'élargissement standard : que trouvez-vous ?

Faites tourner un tour de plus la boucle à partir de l'invariant inductif que vous avez obtenu : que trouvez-vous ? Cela vous convient-il ?

2 Manque de relations

```
/* x est dans -3, 6 */

y = x;

/* bla bla */

z = 1+x*y;
y = sqrt(z);
```

Calcul d'intervalle en avant, qu'obtenez-vous pour y, z ? Y aura-t-il un avertissement pour une possibilité de racine carrée de nombre négatif ?
Et concrètement, peut-il y avoir un problème ?

Note : le calcul ci-dessus correspond à un calcul d'hypoténuse, donc assez courant (termes de puissance etc.). L'outil Astrée détecte que $x = y$, voit qu'on calcule un carré, et sait qu'un carré est ≥ 0.

3 Analyse arrière

3.1 Un résultat décevant

Imaginez que dans un programme on trouve

```
if (toto) {
  /* code qui met x entre 500 et 1000 */
} else {
  /* code qui met x entre -800 et -100 */
}

/* code qui n'a rien a voir */

/* point A */
if (x >= 0) {
  y = x;
} else {
  y = -x;
}
double z = 1.0 / y;
```

Quel est l'intervalle de x au point A ? Une propagation d'intervalles en avant permet-elle d'éviter un avertissement pour division par zéro sur la dernière ligne ?

Note : Oui, je sais, on voit bien que $y = 0$ est inaccessible parce que $x \in [-800, -100] \cup [500, 1000]$ et que $y = |x|$. Imaginez que vous êtes un analyseur qui passe sur une code de lignes 500 000 de long avec 20 000 variables visibles et que vous ne propagez que des intervalles et pas des disjonctions d'intervalles, qui coûteraient trop cher.

3.2 Intervalles en arrière

On va maintenant regarder comment on peut arriver sur $y = 0$ en remontant *en arrière*.

Remontez par intervalles les valeurs de x qui éventuellement peuvent arriver sur $y = 0$. Que conclure ?

4 Matrices

```
for(int i=0; i<n; i++) {
  for(int j=i+1; j<n; j++) {
    t[i][j] = 5;
  }
}
```

Le tableau i est indexé par $0..n-1 \times 0..n-1$. Si on n'arrive pas à prouver que l'accès à t[i][j] est dans les bornes, alors on affiche un avertissement.

1. Pensez-vous que l'on pourra prouver que l'accès à t[i][j] est correct avec des intervalles ? Avec des inégalités de la forme $x_{\min} \leq\leq x_{\max}$ et $x - y \leq C_{xy}$?
2. On essaye avec des polyèdres. Faites tourner la boucle interne avec l'élargissement standard (dessinez), et avec un tour de boucle supplémentaire pour rétrécir.
3. Idem pour la boucle externe.

4. En conclure un domaine d'évolution des variables (i, j).

5 Polyèdres

On voudrait calculer sur des polyèdres convexes bornés. Pour cela on a besoin de faire :

- Intersection d'un polyèdre avec un test (on a un polyèdre avant un test $x \leq y$, après on a l'intersection du polyèdre avec le demi-espace $x \leq y$).
- Calculer l'image d'un polyèdre par une affectation $x := L$, où x est une variable et L une expression linéaire en les variables.
- Calculer des enveloppes convexes pour les fins de test.

On a le choix de représenter un polyèdre par un système d'inégalités (p.ex. ses faces), ou par un ensemble de points dont le polyèdre est l'enveloppe convexe (p.ex. ses sommets). Pour chacune des opérations ci-dessus, suggérez une des deux représentations pour laquelle l'opération est facile.

Est-il possible qu'un polyèdre ait un nombre de sommets exponentiel en le nombre de faces ?