TP PEP – Frama-C / Analyse de Valeurs

Nikolaï Kosmatov

CEA LIST
Laboratoire de Sûreté des Logiciels
nikolai.kosmatov@cea.fr

Analyse de valeurs de Frama-C

- une analyse par interprétation abstraite
- calcule une sur-approximation des domaines des variables en chaque point de programme
- détecte les erreurs à l'exécution
- vérifie la validité de certaines propriétés ACSL
- utilisée par autres greffons de Frama-C

Options pour l'analyseur de valeurs

- Options générales de Frama-C, utiles à l'analyse de valeurs :
  - -main <s> : le point d'entrée du programme est la fonction s
  - -lib-entry : considère que le point d'entrée est une fonction bibliothèque

Options pour l'analyseur de valeurs

- Options de Frama-C spécifiques à l'analyse de valeurs :
  - -val : exécute l'analyse de valeurs par interprétation abstraite et affiche les résultats
  - -ulevel <n> : déroule syntaxiquement n fois chaque boucle
  - -slevel <n> : déroule sémantiquement n fois chaque boucle

Options pour l'analyseur de valeurs

- Bibliothèque standard de Frama-C :
  - les fichiers .[hc] du répertoire 'frama-c -print-path'
  - primitives C comprises par Frama-C, par exemple Frama_C_interval du fichier builtin.c
  - fonctions de la libc dans le fichier libc.c

Exemple

Code

```
void main(){
    A = Frama-C_interval(0, 100);
    B = Frama-C_interval(200, 300);
    C = max(A,B);
}
```

Analyse

A in [0..100]

B in [200..300]

C in ???

frama-c-gui -val max_VA.c share/builtin.c

Visualiser le domaine de C après l'appel de max.