Travaux d'Etudes et de Recherches

Développement d'un mini analyseur statique de code intégré dans Éclipse

Encadrants : MOY Matthieu
MONNIAUX David

Plan :

- Sujet
- Analyse Statique
- Interprétation abstraite
- Travail
- Structure outil
- Exemple outil

Sujet :

Développement d'un analyseur statique pour un sous ensemble du langage Java intégré dans Eclipse.

- Mini Java :
  - Une classe
  - Une méthode *main*.
  - Variables de type *int*.

Exemple de Programme Java :


```
public class Valeur_Absolue {

        public static void main (String[] args){
                int x , y = 0;

                if (x <= 0){
                        x = -x;
                }
        }
}
```

```
public class boucle {

        public static void main (String[] args){
                int x = 0;

                while (x <= 100) {
                        x++;
                }
        }
}
```

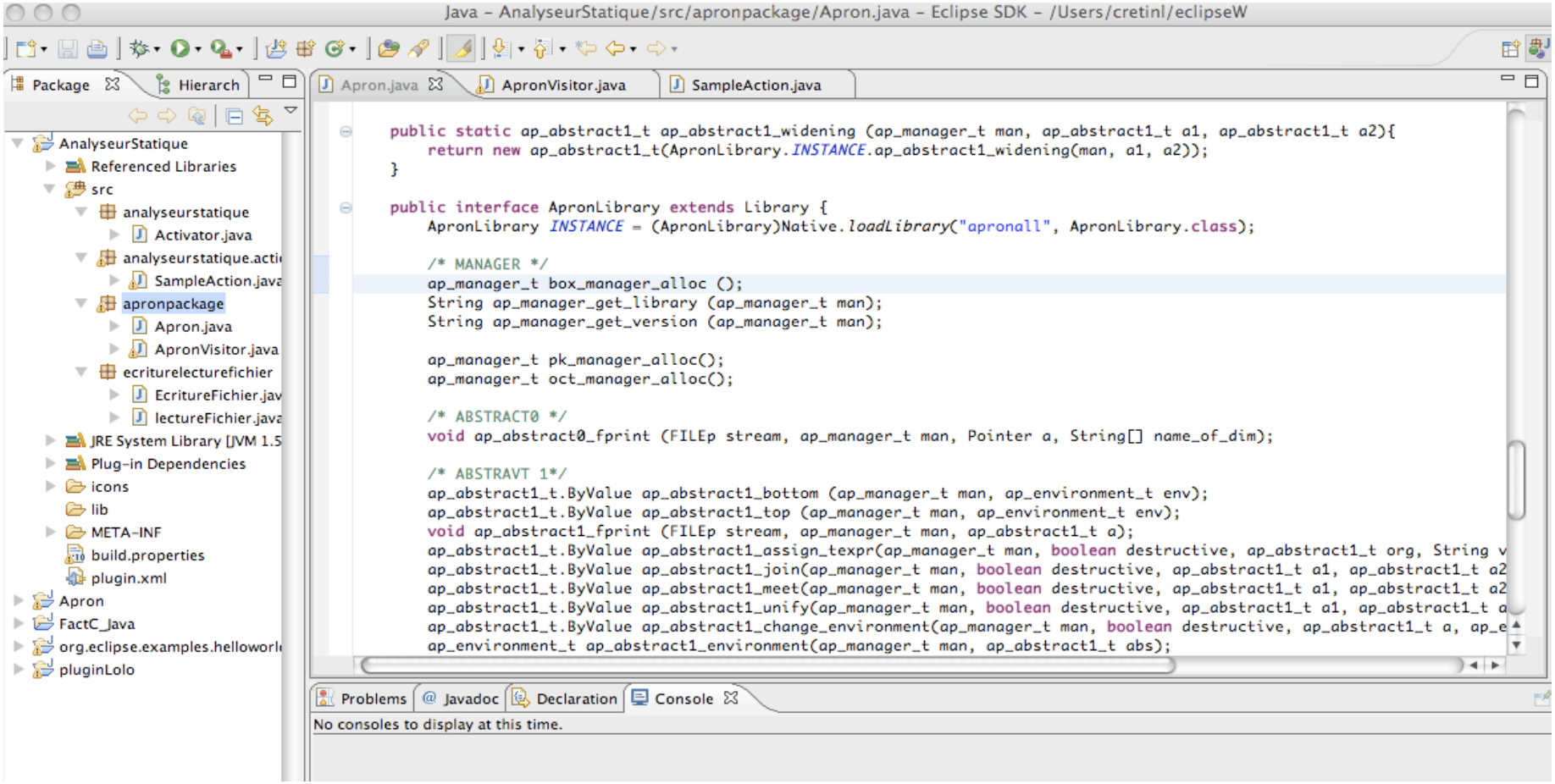
Sujet :

Développement d'un analyseur statique pour un sous ensemble du langage Java intégré dans Eclipse.

- Mini Java :
  - Une classe
  - Une méthode *main*.
  - Variables de type *int*.

- Eclipse :
  - Environnement de développement lancé par IBM.
  - Architecture développée autour de la notion de *plug-in*.
  - Obtention facile de l'arbre abstrait du programme java.

Environnement de développement : Eclipse



Analyse Statique

- Utilisé dans le monde industriel pour le développement de logiciel critique.
- Obtenir des résultats sur l'exécution du programme sans l'exécuter.
- Permet de :
    - Repérer des erreurs de programmation
    - Prouver formellement des propriétés

- Analyse Statique => Interprétation abstraite.

Interprétation abstraite

L'interprétation Abstraite est une théorie de la résolution approchée d'équations de point fixe appliquée à l'analyse de programmes.

- Permet de prouver des propriétés de manières automatiques.
- Découverte d'invariants.
- Principe : Définir un domaine abstrait où l'on exécutera le programme. Par exemple chaque ensemble de valeurs en tout point du programme.

Travail

- Interprétation abstraite de domaines numériques :

  Calculer, en chaque point du programme, les intervalles dans lesquels se trouvent les variables.

  - Un “vrai” langage mais peu de temps.
  - Choix techniques :
    - Analyse Arrière / Analyse avant
    - Graphe de flot de contrôle / Arbre Abstrait
    - Elargissement

Travail

- Interprétation abstraite de domaines numériques :

  Calculer, en chaque point du programme, les intervalles dans lesquels se trouvent les variables.

  - Librairie APRON pour les domaines abstraits (v0.9.8).
    - Expressions
    - Séparation domaine abstrait et analyseur
    - Générique
      - Intervalles : BOX
      - Octogones : OCT
      - Polyhèdres convexes : NEWPOLKA

Travail

- Interprétation abstraite de domaines numériques :

  Calculer, en chaque point du programme, les intervalles dans lesquels se trouvent les variables.

- Java Native Access pour l'appel de fonctions C en java.
  - Accès facile à des bibliothèques partagées.
  - Accès dynamique au moment de l'exécution.
  - Interface Java pour décrire les fonctions et les structures C.

Travail

- postCondition **Analyser_IF**(predCondition, Arbre) {

  resIF = **Analyser_Arbre** (Condition *Inter* predCondition, Branche_THEN);
  resELSE = **Analyser_Arbre**(!Condition *Inter* predCondition, Branche_ELSE);

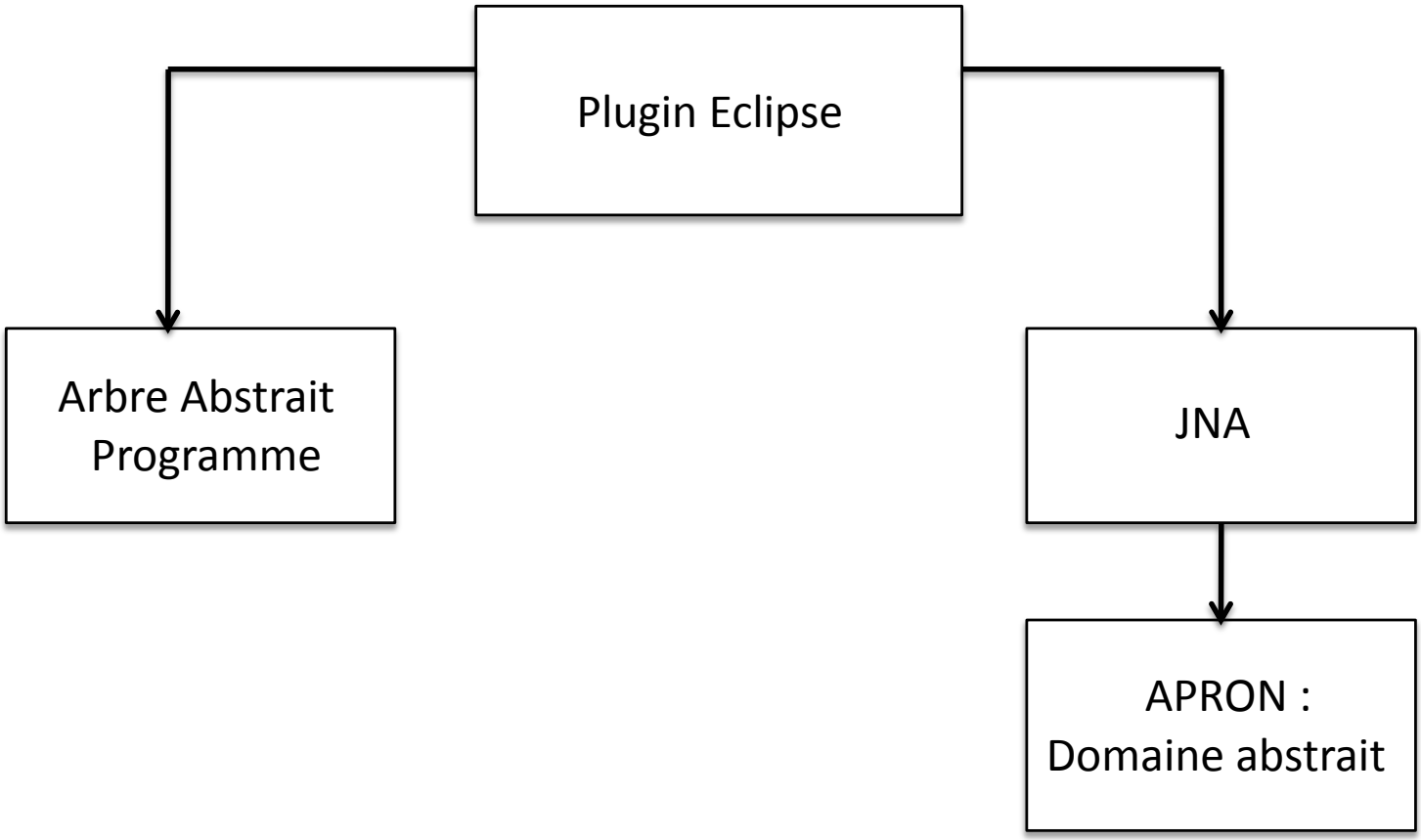
  return resIF Union resELSE;
  }

Travail

- postCondition **Analyser_WHILE**(predCondition, Arbre) {

```
x= predCondition;
do {
      tmp = Analyser_Arbre (Condition Inter x, Branche_BODY);
      y = predCondition Union tmp;
      x = Widening(predCondition, y);
} while (!Inclu(y,x));
// rétrécissement
x = Analyser_Arbre (Condition Inter x, Branche_BODY);
y = predCondition Union tmp;
// sortie de la boucle : filtrage
return y Inter !Condition;
}
```

Structure outil



Exemple : If (c) then … else …

Valeur_Absolue.java

```
public class Valeur_Absolue {

    public static void main (String[] args){
        int x ;
        int y ;

        if (x <= 0){
            x = -x;
            y = 0;
        }else {
            y = 10;
        }
    }
}
```

Resultat Analyse Statique

```
public class Valeur_Absolue{
    public static void main (String[] args){
      int  x;
      int  y;
      if ( x <= 0 ) {
        // x in [-oo,0], y in [-oo,+oo],
        x = - x ;
        y = 0 ;
      }else{
        // x in [1,+oo], y in [-oo,+oo],
        y = 10 ;
      }
    }
    // x in [0,+oo], y in [0,10],
}
```

OK

Exemple : while (c) …

boucle.java

```
public class boucle {
    public static void main (String[] args){
        int x = 0;

        while (x <= 100) {
            x++;
        }
    }
}
```

Resultat Analyse Statique

```
public class boucle{
    public static void main (String[] args){
      int  x =0 ;
      while (x <= 100 ) {
        // x in [0,100],
        x ++ ;
      }
    }
    // x in [101,101],
}
```

OK

Merci de votre attention