# SPARK 2014 : Vérification de Programmes Ada

Claire Dross

AdaCore

28 avril 2014

# La Preuve Formelle de Programmes Ada

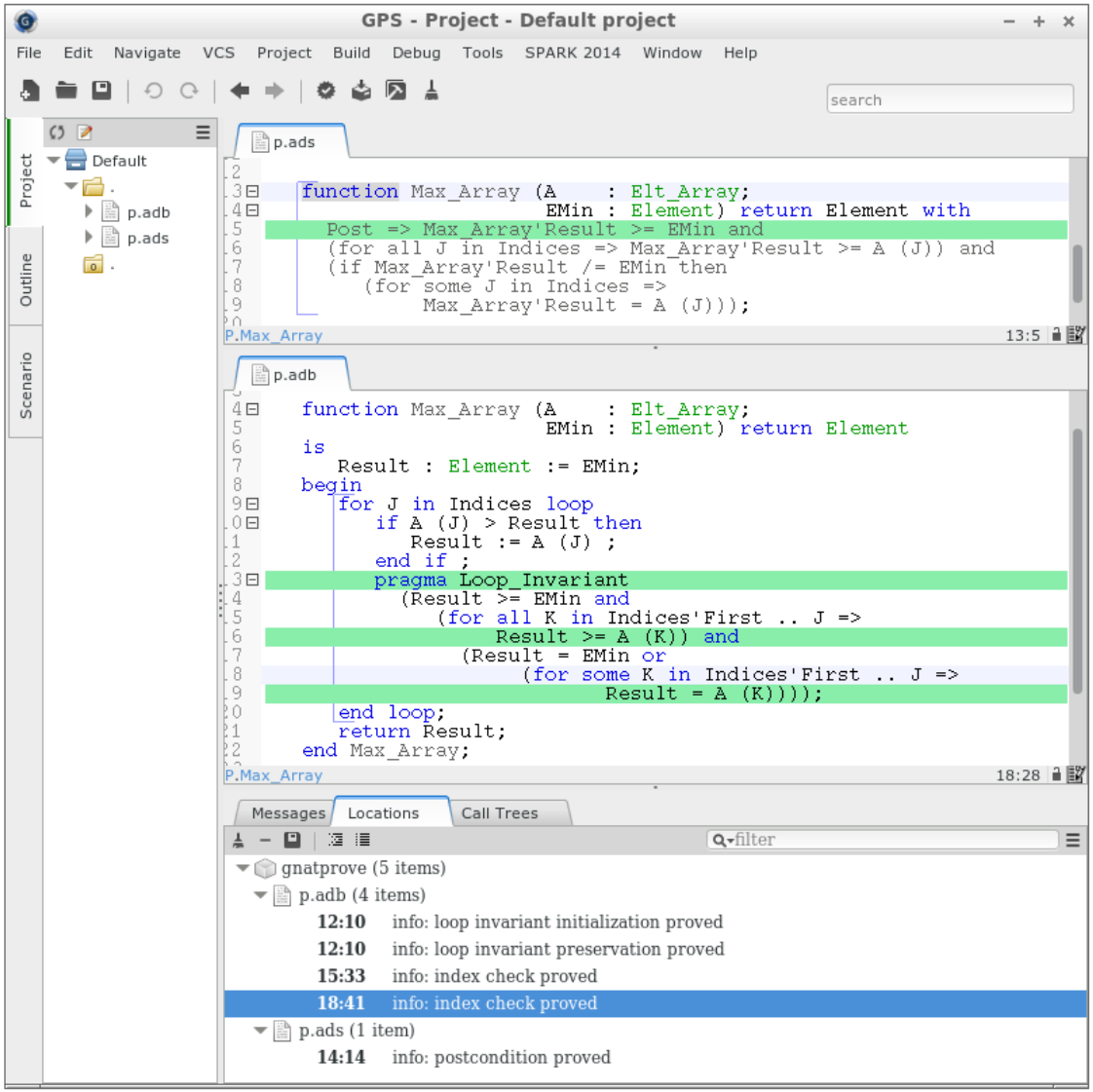
- Ada 2012 supporte la programmation par contrat
- Ces contrats peuvent être vérifiés à l'exécution
- SPARK 2014 est un sous-ensemble de Ada 2012 (pas de pointeurs, d'aliasing, d'effets de bord dans les expressions. . .)
  - L'outil SPARK 2014 est commercialisé par AdaCore et Altran (première version sortie en avril)
  - Il permet l'analyse de flux de données
  - Ainsi que la preuve formelle des contrats sur du code SPARK 2014

# La programmation par contrats en Ada 2012

```
procedure Double (Value : in out Natural) with
  Pre  => Value <= Natural'Last / 2,
  Post => Value = 2 * Value'Old;
```

```
function Max_Array (A : Elt_Array) return Element with
  Pre  => A'First < A'Last,
  Post =>
    (for all  J in A'Range =>
                    Max_Array'Result >= A (J)) and
    (for some J in A'Range =>
                    Max_Array'Result = A (J));
```

# La vérification formelle avec SPARK 2014



# L'outil de preuve formelle de SPARK 2014