

# 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

The screenshot displays the SPARK 2014 IDE interface. The main editor shows two files: `p.ads` and `p.adb`.

**p.ads:**

```
function Max_Array (A : Elt_Array;
                   EMin : Element) return Element with
  Post => Max_Array'Result >= EMin and
  (for all J in Indices => Max_Array'Result >= A (J)) and
  (if Max_Array'Result /= EMin then
   (for some J in Indices =>
    Max_Array'Result = A (J)));
```

**p.adb:**

```
function Max_Array (A : Elt_Array;
                   EMin : Element) return Element
is
  Result : Element := EMin;
begin
  for J in Indices loop
    if A (J) > Result then
      Result := A (J);
    end if;
  pragma Loop_Invariant
  (Result >= EMin and
   (for all K in Indices'First .. J =>
    Result >= A (K)) and
   (Result = EMin or
    (for some K in Indices'First .. J =>
     Result = A (K))));
  end loop;
  return Result;
end Max_Array;
```

**Messages:**

- gnatprove (5 items)
  - p.adb (4 items)
    - 12:10 info: loop invariant initialization proved
    - 12:10 info: loop invariant preservation proved
    - 15:33 info: index check proved
    - 18:41 info: index check proved
  - p.ads (1 item)
    - 14:14 info: postcondition proved

# L'outil de preuve formelle de SPARK 2014

