XIV Summer Workshop in Mathematics MAT/UnB

Formalizing Theorems with PVS

Section 2: Case study - Group Theory

Thaynara Arielly de Lima (IME)

Mauricio Ayala-Rincón (CIC-MAT)

Funded by FAPDF DE grants 00193.0000.2144/2018-81, 00193-00000229/2021-21, and CNPq Research Grants 307672/2017-4 and 313290/2021-0

Jan 17 - 21 , 2022

Talk's Plan

1. Section 2
   - Specification of algebraic notions
   - Induction in PVS
   - Exercises - A case study on Group Theory

Closure in a group

```
G: VAR set[T]

closed?(G): bool = FORALL (x,y:(G)): member(x*y,G)

group?(G): bool = closed?(G) AND
                  associative?[(G)](*) AND
                  member(e,G) AND identity?[(G)](*)(e) AND
                  inv_exists?(G)
```

Conjecture power_closed in pred_algebra.pvs

For all group G, $y \in G$ and $n \in \mathbb{N}$ one can prove that $y^n = \underbrace{y * \ldots * y}_{n-times} \in G$.

A recursive function in PVS

$$\wedge(y, n) = \prod_{i=1}^{n} y, \text{ defined as } e \text{ for } n = 0$$

In PVS:

```
^(y : T, n : nat) : RECURSIVE T =
                    IF n = 0 THEN e
                    ELSE y * ^(y, n-1) ENDIF
                    MEASURE n
```

Type Correctness Conditions (TCCs)

The specification provides two conditions to be verified:

- **A TCC about the type of the argument in the recursive call**

```
% Subtype TCC generated (at line 52, column 22) for  n - 1
    % expected type  nat
caret_TCC1: OBLIGATION FORALL (n: nat): NOT n = 0 IMPLIES n - 1 >= 0;
```

- **A TCC that guarantes the termination of the recursive call**

```
% Termination TCC generated (at line 52, column 17) for  ^(y, n - 1)
caret_TCC2: OBLIGATION FORALL (n: nat): NOT n = 0 IMPLIES n - 1 < n;
```

Induction scheme: weak induction on naturals

power_closed:

```
|---
```

[1] FORALL(G : (group?), y : (G), n : nat) : member(∧(y, n), G)

Rule? (induct"n")

- Base case: power_closed.1

```
|---
```

[1] FORALL(G : (group?), y : (G)) : member(∧(y, 0), G)

- Inductive Step: power_closed.2

```
|---
```

[1] FORALLj :

(FORALL(G : (group?), y : (G)) : member((y ∧ j), G)) IMPLIES

(FORALL(G : (group?), y : (G)) : member((y ∧ (j + 1)), G))

Strong induction on naturals

Fibonacci Sequence

```
fibonacci(n:nat): RECURSIVE nat =
                    IF n <= 1 THEN n ELSE
                    fibonacci(n-1) + fibonacci(n-2)
                    ENDIF
                    MEASURE n
```

Conjecture fibonacci_exp_lim in fibonacci.pvs

$\texttt{fibonacci}(\texttt{n}) \leq 1.7^n$, for all $n \in \mathbb{N}$.

Exercises - A case study on Group Theory

See the file `pred_algebra.pvs` in Exercises directory