

Google Groups

Re: Safe, regular or atomic registers

Leslie Lamport

Dec 1, 2018 2:26 AM

Posted in group: **tlaplus**

My original definitions of safe, regular, and atomic (for a single writer) were given in a formalism whose semantics is not the trace semantics of TLA, a direct translation of those concepts into TLA+ is not nice. But it's not difficult. Here's one way. Just let the writer have a variable that contains the current value of the register, and let each reader have a data structure including a sequence of writer operations to which, when the reader is currently writing, the writer appends something when it begins and finishes each write operation.

I believe the following simpler TLA+ implementations can be proven to be equivalent. For an atomic register, just make the reads and writes atomic. For safe and regular, here are implementations of a register r to which a single writer can write a value in a set T of possible values and any number of readers can read the value.

Safe Register - Method 1

```
-----
Define notValue == CHOOSE t : t \notin T
Write(v)  a: r := notValue ;
          b: r := v ;
Read      c: with (v \in IF r = notValue THEN T ELSE {r})
          { result := v }
```

Safe Register - Method 2

```
-----
Write(v) a: with (v \in T) {r := v}
          either goto a
              or await r = v ;
Read      result := r
```

Regular Register

```
-----
Write(v)  r := v ;
Read      Seen := {}
          a: either { Seen := Seen \cup {r};
                    goto a }
              or with (v \in Seen)
                 { return v }
```

Leslie

On Friday, November 30, 2018 at 7:17:24 AM UTC-8, fl wrote:

In the first lesson of his course on distributed computing, Dr. Guerraoui gives a definition of a safe, regular or atomic register at 6:15.

<http://www.college-de-france.fr/site/rachid-guerraoui/course-2018-10-26-10h00.htm>

This definition is given informally and as such is ambiguous. And above all it is given for boolean variables.

In his article on p.19, Dr. Lamport gives slightly different definitions and in particular for multivalued variables.

<https://lamport.azurewebsites.net/pubs/interprocess.pdf>

Could someone give formal definitions of these notions (with TLAPLUS macros) and/or/xor show the compatibility of Dr. Gerraoui's and Dr. Lamport's définitions.

I think one must use temporal logic concepts to do so and it is not especially simple at first sight.

--

FL