Recursive Operator Definitions

Georges Gonthier, Leslie Lamport

Recursive Operator Definitions

Georges Gonthier, Leslie Lamport

RESEARCH REPORT
N° 9341
11 May 2020
Project-Teams Specfun

ISSN 0249-6399 ISRN INRIA/RR--9341--FR+ENG

Recursive Operator Definitions

Georges Gonthier, Leslie Lamport

Project-Teams Specfun

Research Report n° 9341 — 11 May 2020 — 17 pages

Abstract: TLA+ originally allowed recursive function definitions, but not recursive operator definitions, because it was not clear how to define their semantics. They were added to the language in 2006 after we discovered how to define a satisfactory semantics for them. We describe that semantics here.

Key-words: logic, formal methods, specification, TLA

Définitions récursives d'opérateurs

Résumé : Initialement, TLA+ autorisait les définitions récursives de fonctions, mais pas d'opérateurs, car la sémantique à donner à de telles définitions n'était pas claire. Elles furent finalement ajoutées au langage de spécification en 2006, lorsque nous avons découvert un moyen de leur donner une sémantique satisfaisante. Ce rapport décrit cette sémantique.

Mots-clés : logique, méthodes formelles, spécification, TLA

1 Introduction

Recursive function definitions were allowed in the first version of TLA$^+$ [2]. The definition

(1) $f[n \in Nat] \triangleq \text{IF } n = 0 \text{ THEN } 1 \text{ ELSE } n * f[n-1]$

is an abbreviation for:

(2) $$f \triangleq \text{CHOOSE } g : g = [n \in Nat \mapsto \text{IF } n = 0 \text{ THEN } 1 \text{ ELSE } n * g[n-1]]$$

However, recursive operator definitions were not allowed because it wasn't known how to assign a meaning to them.

Most of the time, recursive function definitions suffice—even to define a recursively defined operator. For example, consider the operator *Cardinality* recursively defined as follows so *Cardinality*(S) is the number of elements in a finite set S:

$$\begin{aligned} &Cardinality(S) \triangleq \\ &\quad \text{IF } S = \{\} \text{ THEN } 0 \text{ ELSE } 1 + Cardinality(S \setminus \{\text{CHOOSE } x : x \in S\}) \end{aligned}$$

It can be defined as follows using a recursively defined function:

$$\begin{aligned} &Cardinality(S) \triangleq \\ &\qquad \text{LET } f[T \in \text{SUBSET } S] \triangleq \\ &\qquad\qquad \text{IF } T = \{\} \text{ THEN } 0 \text{ ELSE } 1 + f[T \setminus \{\text{CHOOSE } x : x \in T\}] \\ &\qquad \text{IN } \quad f[S] \end{aligned}$$

While not mathematically necessary, recursive operator definitions may be necessary in practice. Defining a recursive function requires defining the function's domain, but that definition may be extremely complicated and the TLC model checker may not be able to evaluate it. This was the case with a specification of the PlusCal to TLA$^+$ translation—a specification that was tested by having the actual PlusCal translator call TLC to evaluate it to perform part of the translation. As of now, the TLAPS proof system handles only recursive function definitions, not recursive operator definitions.

Recursive operator definitions were added to TLA$^+$ when, in 2005, we figured out how to give them a correct semantics. This note belatedly explains that semantics and what "correct" means. The discussion here is informal but, we believe, rigorous. Our results are not quite expressed in TLA$^+$ because they require declarations of higher-level operator parameters, while TLA$^+$ only allows the definition of such operators. However, the meaning of those declarations should be clear.

Many of our results were independently discovered by Charguéraud [1]. While he was concerned with recursive definitions of functions rather than operators, some of his definitions and results closely match ours.

2 The Problem

To appreciate the problem posed by recursive operator definitions, consider this example:

(3) $\quad Op(x) \triangleq \text{CHOOSE } y : y \neq Op(x)$

It would appear to define Op so that $Op(42) \neq Op(42)$, which is impossible since every value equals itself.

Most logic texts that discuss definitions consider them to be axioms, so the meaning of (3) would be:

$$\text{AXIOM } \forall x : Op(x) = \text{CHOOSE } y : y \neq Op(x)$$

Since this axiom implies the false formula $Op(42) \neq Op(42)$, (3) could not be a legal definition. To be legal, a recursive definition would have to satisfy some rule, and showing that the rule is satisfied would essentially require proving a theorem.

In TLA$^+$, a definition simply asserts that one expression is a syntactic abbreviation for another expression. An ordinary, non-recursive definition

$$Op(x) \triangleq \ldots$$

asserts that, for any expression e, the expression $Op(e)$ is an abbreviation for the expression obtained by syntactically substituting the expression e for x in the expression to the right of the $\triangleq$. There is no need to prove a theorem to define a syntactic abbreviation.

There is nothing magic in declaring definitions to be abbreviations. To use the definition (1), we will have to prove this:

$$\text{THEOREM } \forall n \in Nat : f[n] = \text{IF } n = 0 \text{ THEN } 1 \text{ ELSE } n * f[n-1]$$

The proof of the theorem is, of course, the same proof needed to justify a recursive definition of factorial if the meaning of that definition is taken to be an axiom.

Mathematicians write proofs, so it makes little difference to them whether they have to write a proof to make a definition or to use it. However, most TLA$^+$ users are engineers who don't write proofs. If a proof were required to write a recursive operator definition in TLA$^+$, the recursive definitions one could write would have to be constrained so that the proof was obvious enough to be found by the parser. Such a constraint would have been unacceptably restrictive without drastically changing TLA$^+$. In particular, it would have required complicating the language by adding some form of typing.

We therefore had to provide a semantics for recursive definitions in which any such definition is legal—including definition (3). A definition can then be incorrect only in the sense that it doesn't mean what its writer thought it meant. That kind of error can usually be found when the defined operator is used in a specification that is checked by a tool such as the TLC model checker.

3 Simple Recursive Definitions

We begin by considering a recursive definition of a single operator with a single argument. Such a definition has this form:[1]

(4) $F(x) \triangleq Def(x, F)$

(We consider multiple-argument operators and mutually recursive definitions below.) We fix *Def* by writing all subsequent definitions in this section in a module that begins with this declaration:

$\text{CONSTANT } Def(\_, \_(\_))$

(As mentioned in the introduction, TLA$^+$ doesn't allow such a higher-order operator declaration.)

3.1 The Semantics

In 2005, the second author had the idea of letting (4) assert that $F(x)$ equals $g[x]$ for some function g containing x in its domain such that $g[y]$ equals $Def(y, g)$ for all y in its domain. This isn't quite right, since the second argument of *Def* must be an operator that takes an argument. To correct it, let's define $def(y, g)$ to be $Def(y, G)$ when G is the operator "obtained from" g:

$def(y, g) \triangleq Def(y, \text{LAMBDA } z : g[z])$

The precise statement of the idea was to let $F(x)$ equal:[2]

(5)
$$\begin{array}{ll} \text{LET } f \triangleq \text{CHOOSE } g : & \land\ x \in \text{DOMAIN } g \\ & \land\ g = [y \in \text{DOMAIN } g \mapsto def(y, g)] \\ \text{IN } \ f[x] & \end{array}$$

It's not hard to see that this definition isn't right. For example, suppose *Def* were defined by:

(6) $Def(x, F(\_)) \triangleq \text{IF } x = 0 \text{ THEN } 1 \text{ ELSE } x * F(x - 1)$

We would expect this to define $F(n)$ to equal $n!$ (n factorial) for every natural number n. However, let g be the function with domain $\{3\}$ such that $g[3] = 0$. The semantics of TLA$^+$ doesn't specify what the value of $g[y]$ is if y is not in the domain of g. So, it's possible that $g[2] = 0$. In that case, $g[3] = 3 * g[2]$, so the body of the CHOOSE statement in (5) equals TRUE for this function g and $x = 3$. Thus, it's possible that the CHOOSE chooses this function g to equal f when x equals 3, thereby defining $F(3)$ to equal 0. This

[1] In TLA$^+$, this recursive operator definition must be preceded by a RECURSIVE $F(\_)$ declaration. We will not bother writing those declarations.

[2] A sophisticated TLA$^+$ user might think that the body of the CHOOSE should also assert that g is a function, but further thought shows that's not necessary.

means it's impossible to prove that $F(3)$ does not equal 0; and therefore it's impossible to prove that it does equal $3!$ as it should.

The first author came up with a way to fix this problem. For the factorial definition (6), we need to fix the choice of g in (5) so that, for a natural number x, the domain of g must include $0\,..\,x$. In general, we want to require that, if the recursion uniquely determines the value of $F(x)$, then the domain of g is large enough so it "fixes" (uniquely determines) the value of g on all its elements. We first define

$$\mathit{fdef}(S, g) \;\triangleq\; [x \in S \mapsto \mathit{def}(x, g)]$$

and then define the fixing condition to be $\mathit{fix}(g)$, where

$$\begin{aligned}\mathit{fix}(g) \;\triangleq\; & \forall\, h : (\forall\, x \in \text{DOMAIN}\, g : h[x] = g[x]) \Rightarrow \\ & \qquad\qquad (g = \mathit{fdef}(\text{DOMAIN}\, g, h))\end{aligned}$$

We give a semantics to the recursive definition (4) by letting it define F to be this operator Fr:

$$Fr(x) \;\triangleq\; (\,\text{CHOOSE}\; g : (x \in \text{DOMAIN}\, g) \land \mathit{fix}(g)\,)\,[x]$$

3.2 Inductive Definitions

Correctness of our semantics means that

(7) $\quad Fr(x) = \mathit{Def}(x, Fr)$

is true for those values of x for which we expect it to be true. For example, if Def is defined by (6), then we expect (7) to be true for all x in Nat. We expect it not to be true for any x when Def is defined by (3). (In this case, $\mathit{Op}(x)$ equals $(\text{CHOOSE}\; f : \text{FALSE})[x]$ for all x, but who cares?)

For Def defined by (6), we expect (7) to be true when $x \in \mathit{Nat}$ because Def is inductive on Nat. Intuitively, this means that it allows the value of $F(n)$ for any $n \in \mathit{Nat}$ to be computed by a finite number of applications of the definition (4). For example, we can compute $F(27)$ by applying the definition once to see that it equals $27 * F(26)$, applying it a second time to see that it equals $27 * 26 * F(25)$, and so on until we get to $F(0) = 1$. In general, Def is inductive on Nat iff for every $n \in \mathit{Nat}$, the value of $\mathit{Def}(n, F)$ depends only on the values of $\mathit{Def}(i, F)$ for $i \in 0\,..\,(n-1)$.

We can generalize from the set Nat to any set with a well-founded order relation on the set. An (irreflexive) partial order $\prec$ on a set S is well-founded iff there does not exist any infinite sequence $\ldots \prec s_3 \prec s_2 \prec s_1$ of elements of S. We fix the relation $\prec$ by making it a parameter of our module, declaring it with:

$$\text{CONSTANT}\; \_ \prec \_$$

It's convenient to define LT so $LT(x, S)$ is the set of elements of the set S that are $\prec x$:

$$LT(x, S) \;\triangleq\; \{y \in S : y \prec x\}$$

We define *WellFounded*(S) as follows to mean that $\prec$ is a well-founded partial order on S:

$$\begin{array}{l} \mathit{WellFounded}(S) \;\triangleq \\ \quad \land\; \forall\, x, y, z \in S \,:\, (x \prec y) \land (y \prec z) \Rightarrow (x \prec z) \\ \quad \land\; \forall\, T \in (\textsc{subset}\ S) \setminus \{\,\} \,:\, \exists\, x \in T \,:\, \mathit{LT}(x, S) = \{\,\} \end{array}$$

Proof by mathematical induction on the set of natural numbers is generalized to the following proof rule:

$$\begin{array}{ll} \multicolumn{2}{l}{\textsc{theorem}\ \mathit{GeneralInduction} \;\triangleq} \\ \quad \textsc{assume} & \textsc{new}\ S,\ \mathit{WellFounded}(S),\ \textsc{new}\ P(\_) \\ & \forall\, x \in S \,:\, (\forall\, y \in \mathit{LT}(x, S) \,:\, P(y)) \Rightarrow P(x) \\ \quad \textsc{prove} & \forall\, x \in S \,:\, P(x) \end{array}$$

The natural definition of what it means for *Def* to be inductive on a set S with well-founded order $\prec$ is that, for any operator G, the value of $\mathit{Def}(x, G)$ for any $x \in S$ depends only on the values of $G(y)$ for $y \in \mathit{LT}(x, S)$. More precisely, define *Def* inductive on S to mean that the following condition holds for any operators G and H:

(8) $\quad (\forall\, y \in \mathit{LT}(x, S) \,:\, G(y) = H(y)) \;\Rightarrow\; (\mathit{Def}(x, G) = \mathit{Def}(x, H))$

When *Def* is inductive on S, we expect (7) to be true for all $x \in S$.

We can't write this definition of inductive in TLA$^+$, since stating that (8) is true for all operators G and H mean quantifying over operators, which requires higher-order logic. However, we can write it as the following ASSUME/PROVE, which can appear as the hypothesis of a theorem:

(9) $\quad \begin{array}{ll} \textsc{assume} & \textsc{new}\ G(\_),\ \textsc{new}\ H(\_) \\ \textsc{prove} & \forall\, x \in S \,:\, (\forall\, y \in \mathit{LT}(x, S) \,:\, G(y) = H(y)) \\ & \qquad\qquad \Rightarrow\; (\mathit{Def}(x, G) = \mathit{Def}(x, H)) \end{array}$

We will prove that this hypothesis and *WellFounded*(S) imply that (7) holds for all $x \in S$. To do that, we define *Def* to be *contractive* on S iff (8) holds when G and H are obtained from functions. The precise definition is:

$$\begin{array}{l} \mathit{Contractive}(S) \;\triangleq \\ \quad \forall\, g, h \,:\, \forall\, x \in S \,:\, \\ \qquad (\forall\, y \in \mathit{LT}(x, S) \,:\, g[y] = h[y]) \;\Rightarrow\; (\mathit{def}(x, g) = \mathit{def}(x, h)) \end{array}$$

3.3 Correctness for Inductive Definitions

We will show that (7) holds if *Def* is contractive—more precisely, that *Def* contractive on S implies:

(10) $\quad \forall\, x \in S \,:\, \mathit{Fr}(x) = \mathit{Def}(x, \mathit{Fr})$

We begin our proof with the following lemma.

Lemma 1 $\forall\, S, f, g, x \;:\; \begin{array}{l} \land\ \mathit{WellFounded}(S) \\ \land\ \mathit{Contractive}(S) \\ \land\ \mathit{fix}(f) \land \mathit{fix}(g) \\ \land\ x \in (\textsc{domain}\, f) \cap (\textsc{domain}\, g) \cap S \\ \Rightarrow (f[x] = g[x]) \end{array}$

$\langle 1 \rangle$ DEFINE $h +\!\!+\, k \;\triangleq\; [y \in (\textsc{domain}\, h) \cup (\textsc{domain}\, k) \mapsto$
$\qquad\qquad$ IF $y \in \textsc{domain}\, h$ THEN $h[y]$ ELSE $k[y]\,]$

$\langle 1 \rangle 1.$ ASSUME NEW h, NEW k, $\mathit{fix}(h)$
PROVE $h = \mathit{fdef}(\textsc{domain}\, h,\, h +\!\!+\, k)$

PROOF: By the assumption $\mathit{fix}(h)$, since $h[z] = (h +\!\!+\, k)[z]$ for all z in DOMAIN h.

$\langle 1 \rangle 2.$ SUFFICES ASSUME NEW S, NEW f, NEW g,
$\mathit{Contractive}(S)$, $\mathit{fix}(f)$, $\mathit{fix}(g)$
PROVE $\forall\, x \in (\textsc{domain}\, f) \cap (\textsc{domain}\, g) \cap S \;:\; f[x] = g[x]$

PROOF: By simple logic.

$\langle 1 \rangle$ DEFINE $\mathit{Sfg} \;\triangleq\; (\textsc{domain}\, f) \cap (\textsc{domain}\, g) \cap S$

$\langle 1 \rangle 3.$ SUFFICES ASSUME NEW $x \in \mathit{Sfg}$,
$\forall\, y \in \mathit{LT}(x, \mathit{Sfg}) \;:\; f[y] = g[y]$
PROVE $f[x] = g[x]$

PROOF: $\mathit{Sfg} \subseteq S$ implies $\mathit{WellFounded}(\mathit{Sfg})$, so to prove $f[x] = g[x]$, by *GeneralInduction*, it suffices to prove it under the assumption that $f[y] = g[y]$ for all $y \in \mathit{LT}(x, \mathit{Sfg})$.

$\langle 1 \rangle 4.$ $\forall\, y \in \mathit{LT}(x, S) \;:\; (f +\!\!+\, g)[y] = (g +\!\!+\, f)[y]$

PROOF: Since $\mathit{LT}(x, S) \subseteq S$, if y is in $(\textsc{domain}\, f) \cap (\textsc{domain}\, g)$ then it is also in Sfg, so $\langle 1 \rangle 3$ implies $(f +\!\!+\, g)[y] = (g +\!\!+\, f)[y]$. If y is not in $(\textsc{domain}\, f) \cap (\textsc{domain}\, g)$, then the definition of $+\!\!+$ implies $(f +\!\!+\, g)[y] = (g +\!\!+\, f)[y]$.

$\langle 1 \rangle 5.$ $\mathit{def}(x, f +\!\!+\, g) = \mathit{def}(x, g +\!\!+\, f)$

PROOF: By $\langle 1 \rangle 4$ and $\mathit{Contractive}(S)$ (from $\langle 1 \rangle 2$).

$\langle 1 \rangle 6.$ Q.E.D.

PROOF: $\begin{array}{ll} f[x] = \mathit{def}(x, f +\!\!+\, g) & [\text{by } \langle 1 \rangle 1,\ \mathit{fix}(f) \text{ (from } \langle 1 \rangle 2\text{), and} \\ & \ x \in \textsc{domain}\, f \text{ (from } \langle 1 \rangle 3)] \\ \quad = \mathit{def}(x, g +\!\!+\, f) & [\text{by } \langle 1 \rangle 5] \\ \quad = g[x] & [\text{by } \langle 1 \rangle 1,\ \mathit{fix}(g) \text{ (from } \langle 1 \rangle 2\text{), and} \\ & \ x \in \textsc{domain}\, g \text{ (from } \langle 1 \rangle 3)] \end{array}$

We now define $\mathit{fr}(S)$ to be the function with domain S that agrees with Fr on that set:

$$\mathit{fr}(S) \;\triangleq\; [x \in S \mapsto \mathit{Fr}(x)]$$

The next theorem shows that if Def is contractive on S, then $fr(S)$ equals $fdef(S, fr(S))$, and this equality uniquely determines the function $fr(S)$.

Theorem 1 $\forall S : WellFounded(S) \land Contractive(S) \Rightarrow$
$(\forall f : (f = fdef(S, f)) \equiv (f = fr(S)))$

$\langle 1\rangle 1.$ ASSUME NEW S, $WellFounded(S)$, $Contractive(S)$,
NEW f, $f = fdef(S, f)$
PROVE $fix(f) \land (\text{DOMAIN}\, f = S)$

$\langle 2\rangle 1.$ DOMAIN $f = S$

PROOF: By the $\langle 1\rangle 1$ assumption and the definition of $fdef$.

$\langle 2\rangle 2.$ SUFFICES ASSUME NEW g, $\forall x \in S : g[x] = f[x]$
PROVE $fdef(S, g) = f$

PROOF: By $\langle 2\rangle 1$ it suffices to prove $fix(f)$, which by $\langle 2\rangle 1$ and the definition of fix means proving that the $\langle 2\rangle 2$ ASSUME implies $f = fdef(S, g)$.

$\langle 2\rangle 3.$ $\forall x \in S : \forall y \in LT(x, S) : g[x] = f[x]$

PROOF: By the $\langle 2\rangle 2$ assumption, since $LT(x, S) \subseteq S$ by definition of LT.

$\langle 2\rangle 4.$ Q.E.D.

PROOF: $\langle 2\rangle 3$ and the assumption $Contractive(S)$ (from $\langle 1\rangle 1$) imply $\forall x \in S : def(x, g) = def(x, f)$, which by definition of $fdef$ implies $fdef(S, g) = fdef(S, f)$. By the $\langle 1\rangle 1$ assumption, this is equivalent to the current goal.

$\langle 1\rangle 2.$ SUFFICES ASSUME NEW S, $WellFounded(S)$, $Contractive(S)$
PROVE $fr(S) = fdef(S, fr(S))$

$\langle 2\rangle 1.$ ASSUME NEW S, $WellFounded(S)$, $Contractive(S)$,
$fr(S) = fdef(S, fr(S))$,
NEW f, $f = fdef(S, f)$
PROVE $f = fr(S)$

PROOF: $\langle 1\rangle 1$ and the assumptions imply $fix(f)$, $fix(fr(S))$, and both DOMAIN f and DOMAIN $fr(S)$ equal S. By Lemma 1, this implies $f = fr(S)$.

$\langle 2\rangle 2.$ ASSUME NEW S, $WellFounded(S)$, $Contractive(S)$,
$fr(S) = fdef(S, fr(S))$,
NEW f, $f = fr(S)$
PROVE $f = fdef(S, f)$

PROOF: The conclusion follows immediately from the hypotheses $fr(S) = fdef(S, fr(S))$ and $f = fr(S)$.

$\langle 2\rangle 3.$ Q.E.D.

PROOF: By simple logic, $\langle 2\rangle 1$ and $\langle 2\rangle 2$ show that the ASSUME/PROVE of $\langle 1\rangle 2$ implies the theorem.

$\langle 1\rangle 3.$ SUFFICES ASSUME NEW $x \in S$,
$\quad \forall\, y \in LT(x, S) : Fr(y) = def(y, fr(S))$
PROVE $Fr(x) = def(x, fr(S))$

$\langle 2\rangle 1.$ ASSUME $\forall\, x \in S :$
$\quad (\forall\, y \in LT(x, S) : Fr(y) = def(y, fr(S))$
$\quad\quad \Rightarrow (Fr(x) = def(x, fr(S)))$
PROVE $fr(S) = fdef(S, fr(S))$

$\langle 3\rangle 1.$ $\forall\, x \in S : Fr(x) = def(x, fr(S))$

PROOF: By $WellFounded(S)$ (by $\langle 1\rangle 2$), the $\langle 2\rangle 1$ assumption and *GeneralInduction*.

$\langle 3\rangle 2.$ Q.E.D.

PROOF: For all $x \in S$:

$$\begin{aligned} fr(S) &= [x \in S \mapsto Fr(x)] && \text{[by definition of } fr(S)] \\ &= [x \in S \mapsto def(x, fr(S))] && \text{[by } \langle 3\rangle 1] \\ &= fdef(S, fr(S)) && \text{[by definition of } fdef] \end{aligned}$$

$\langle 2\rangle 2.$ Q.E.D.

PROOF: By $\langle 2\rangle 1$, since its ASSUME formula is equivalent to the ASSUME/PROVE of $\langle 1\rangle 3$, and its PROVE formula is the goal introduced by $\langle 1\rangle 2$.

$\langle 1\rangle$ DEFINE $LE(x, T) \triangleq \{y \in T : (y \prec x) \lor (y = x)\}$
$\quad fx \triangleq fdef(LE(x, S), fr(S))$

$\langle 1\rangle 4.$ $fx = fdef(LE(x, S), fx)$

$\langle 2\rangle 1.$ SUFFICES ASSUME NEW $y \in LE(x, S)$
PROVE $def(y, fr(S)) = def(y, fx)$

PROOF: By the definitions of fx and $fdef$.

$\langle 2\rangle 2.$ SUFFICES ASSUME NEW $z \in LT(y, S)$
PROVE $fr(S)[z] = fx[z]$

PROOF: $Contractive(S)$ (assumed in $\langle 1\rangle 2$) implies that $\langle 2\rangle 2$ implies the current goal (introduced by $\langle 2\rangle 1$).

$\langle 2\rangle 3.$ $z \in S \land z \in LT(x, S) \land z \in LE(x, S)$

PROOF: By $\langle 2\rangle 1$, $\langle 2\rangle 2$, the definitions of LE and LT, and the transitivity of $\prec$ (implied by $WellFounded(S)$).

$\langle 2\rangle 4.$ Q.E.D.

PROOF:
$$\begin{aligned} fr(S)[z] &= Fr(z) && \text{[definition of } fr \text{ and } \langle 2\rangle 3] \\ &= def(z, fr(S)) && [\langle 1\rangle 3 \text{ and } \langle 2\rangle 3] \\ &= fx[z] && \text{[definitions of } fx \text{ and } fdef\text{, and } \langle 2\rangle 3] \end{aligned}$$

$\langle 1\rangle 5.$ $WellFounded(LE(x, S)) \land Contractive(LE(x, S))$

PROOF: $\langle 1\rangle 2$ implies $WellFounded(S)$ and $Contractive(S)$. The definition of LE implies $LE(x, S) \subseteq S$. That and $WellFounded(S)$ imply $WellFounded(LE(x, S))$. From $x \in S$ and the transitivity of $\prec$ on S (by $WellFounded(S)$), we have $LT(y, LE(x, S)) = LT(y, S)$ for all $y \in LE(x, S)$. This and $Contractive(S)$ imply $Contractive(LE(x, S))$.

$\langle 1 \rangle 6.$ $fix(fx) \wedge (x \in \text{DOMAIN } fx)$

PROOF: By $\langle 1 \rangle 5$, $\langle 1 \rangle 1$ (with $LE(x, S)$ substituted for S), and $\langle 1 \rangle 4$.

$\langle 1 \rangle$ DEFINE $gx \triangleq \text{CHOOSE } g : (x \in \text{DOMAIN } g) \wedge fix(g)$

$\langle 1 \rangle 7.$ $(x \in \text{DOMAIN } gx) \wedge fix(gx)$

PROOF: By $\langle 1 \rangle 6$ the defining property of gx is satisfied by fx.

$\langle 1 \rangle 8.$ Q.E.D.

PROOF:
$$\begin{array}{rcll} Fr(x) & = & gx[x] & \text{[definitions of } Fr \text{ and } gx] \\ & = & fx[x] & \text{[Lemma 1, } \langle 1 \rangle 6, \langle 1 \rangle 7, \text{ and } \langle 1 \rangle 3] \\ & = & def(x, fr(S)) & \text{[definition of } fx \text{ and } \langle 1 \rangle 7] \end{array}$$

Theorem 1 has the following corollary:

Corollary 1 $\forall S : WellFounded(S) \wedge Contractive(S) \Rightarrow$
$\qquad \forall x \in S : Fr(x) = def(x, fr(S))$

PROOF: Theorem 1 implies $fr(S) = fdef(S, fr(S))$, and the result then follows from the definitions of fr and $fdef$.

The conclusion of Corollary 1 is very close to our goal, which is proving (10); but it doesn't imply that goal. In fact, the following example shows that $Contractive(S)$ is too weak a condition to imply (10). Define

$$fromFcn(G(\_)) \triangleq \exists g : \forall x : G(x) = g[x]$$

and suppose Def is defined by

$$Def(x, G) \triangleq \text{IF } fromFcn(G) \text{ THEN } 1 \text{ ELSE } 0$$

For any function f and any $x \in \text{DOMAIN } f$, the definition of def implies $def(x, f) = 1$ for this operator Def. This implies Def is contractive on any partially ordered set S. For any x, let f_x be the function $[y \in \{x\} \mapsto 1]$. It's easy to see that $fix(f_x)$ is true, and that this implies $Fr(x) = 1$ for all x. However, for a function f, the semantics of TLA$^+$ says nothing about the value of $f[y]$ for $y \notin \text{DOMAIN } f$. Therefore, there may be no function g such that $\forall x : g[x] = 1$ is true. In that case, $fromFcn(Fr)$ equals FALSE, so $Def(x, Fr)$ equals 0 for all x, and therefore $Fr(x) \neq Def(x, Fr)$ for all x.

The reason we can't derive (10) from the hypothesis that Def is contractive on S is that this hypothesis still allows the value of $Def(x, Fr)$ to depend on values of $Fr(y)$ for $y \notin S$ even though $x \in S$. This possibility is effectively ruled out by the condition that Fr is *representable* on S, where representable is defined by:

$$\begin{array}{l} Representable(G(\_), S) \triangleq \\ \qquad \forall x \in S : Def(x, G) = def(x, [y \in S \mapsto G(y)]) \end{array}$$

The following theorem shows that *Def* contractive on S and *Fr* representable on S implies (10), and that any operator satisfying the recurrence condition equals *Fr* on S.

Theorem 2

$$\begin{array}{ll}\textsc{assume} & \textsc{new}\ S,\ \mathit{WellFounded}(S),\ \mathit{Contractive}(S),\\ & \textsc{new}\ G(\_),\ \mathit{Representable}(G,S)\\ \textsc{prove} & (\forall\, x \in S : G(x) = \mathit{Def}(x,G)) \ \equiv\ (\forall\, x \in S : G(x) = \mathit{Fr}(x))\end{array}$$

Proof: Let $f \triangleq [x \in S \mapsto G(x)]$. Then:

$$\begin{array}{ll}(\forall\, x \in S : G(x) = \mathit{Def}(x,G))) & \\ \quad \equiv (f = \mathit{fdef}(S,f)) & [\text{definitions of } f \text{ and } \mathit{fdef}, \text{ and}\\ & \ \text{the } \mathit{Representable}(G,S) \text{ assumption}]\\ \quad \equiv (f = \mathit{fr}(S)) & [\text{Theorem 1}]\\ \quad \equiv (\forall\, x \in S : G(x) = \mathit{Fr}(x)) & [\text{definitions of } f \text{ and } \mathit{fr}(S)]\end{array}$$

The following corollary to Theorem 2 asserts that *Def* contractive and representable on S implies (10).

Corollary 2

$$\begin{array}{l}\forall\, S : \mathit{WellFounded}(S) \wedge \mathit{Contractive}(S) \wedge \mathit{Representable}(\mathit{Fr})\\ \qquad\qquad \Rightarrow\ (\forall\, x \in S : \mathit{Fr}(x) = \mathit{Def}(x,\mathit{Fr}))\end{array}$$

Proof: By Theorem 2 applied to *Fr*.

Our goal is to prove that $\mathit{WellFounded}(S)$ and *Def* inductive on S imply (10). We have proved that $\mathit{WellFounded}(S)$ and *Def* implies (10). To complete the proof of our goal, we have to show that $\mathit{WellFounded}(S)$ and *Def* inductive on S imply *Def* is contractive and representable on S. Since *Def* inductive on S is expressed by (9), this is done by the following theorem.

Theorem 3

$$\begin{array}{ll}\textsc{assume} & \textsc{new}\ S,\ \mathit{WellFounded}(S),\ \textsc{new}\ G(\_),\\ & \begin{array}{ll}\textsc{assume} & \textsc{new}\ H(\_),\ \textsc{new}\ J(\_)\\ \textsc{prove} & \forall\, x \in S : (\forall\, y \in \mathit{LT}(x,S) : H(y) = J(y))\\ & \qquad\qquad \Rightarrow\ (\mathit{Def}(x,H) = \mathit{Def}(x,J))\end{array}\\ \textsc{prove} & \mathit{Contractive}(S) \wedge \mathit{Representable}(G,S)\end{array}$$

$\langle 1\rangle 1.$ $\textsc{assume}$ $\textsc{new}\ g,\ \textsc{new}\ h,\ \textsc{new}\ x \in S,\ (\forall\, y \in \mathit{LT}(x,S) : g[y] = h[y])$
$\textsc{prove}$ $\mathit{def}(x,g) = \mathit{def}(x,h)$

Proof: Apply the theorem's assumption with $H(y) \triangleq g[y]$ and $J(y) \triangleq h[y]$.

$\langle 1\rangle 2.$ $\mathit{Representable}(G,S)$

Proof: Define
$$\begin{array}{rcl} h & \triangleq & [y \in S \mapsto G(y)]\ .\\ H(x) & \triangleq & h[x]\end{array}$$

By definition of *Representable*, it suffices to assume $x \in S$ and prove $\mathit{Def}(x,G) = \mathit{def}(x,h)$, which is done as follows:

$$\begin{aligned} Def(x, G) &= Def(x, H) && \text{[By the ASSUME/PROVE assumption]} \\ &= def(x, h) && \text{[By definition of } def\text{]} \end{aligned}$$

$\langle 1 \rangle 3.$ Q.E.D.

By $\langle 1 \rangle 1$, which is the definition of *Contractive*(S), and $\langle 1 \rangle 2$.

Our goal is now a simple corollary of Corollary 2 and Theorem 3.

Corollary 3

```
ASSUME  NEW $S$, $WellFounded(S)$,
        ASSUME  NEW $G(\_)$, NEW $H(\_)$
        PROVE   $\forall x \in S : (\forall y \in LT(x, S) : G(y) = H(y))$
                                  $\Rightarrow (Def(x, G) = Def(x, H))$
PROVE   $\forall x \in S : Fr(x) = Def(x, Fr)$
```

PROOF: By Theorem 3, substituting *Fr* for G, and Corollary 2.

In practice, for any v, the value of $Def(v, F)$ is defined in terms of v and $F(v_1)$, ..., $F(v_k)$ for some finite set $\{v_1, \ldots, v_k\}$. There is then an obvious recursive algorithm for computing $F(v)$. Our results imply that if this algorithm terminates, then it computes $F(v)$ equal to $Fr(v)$. To prove this, let S equal the set of all values x for which the algorithm computes $F(x)$, and define the relation $\prec$ on S so $x \prec y$ is true iff the algorithm computes $F(x)$ when computing $F(y)$. Termination of the algorithm implies that $\prec$ is an irreflexive partial order on S and that S is finite, so $\prec$ is well-founded on S. Let $G(x)$ be the value computed by the algorithm for all $x \in S$. Theorem 3 implies *Representable*(G, S) and Theorem 2 then implies $G(v) = Fr(v)$.

Our theorems and corollaries cannot be expressed in TLA$^+$ because *Def* needs to be declared as CONSTANT, and TLA$^+$ does not support declarations of operators with an operator argument. To state these results in a more easy to use way, we would write them as ASSUME /PROOF statements with *Def* declared in a NEW clause, which TLA$^+$ also does not permit. Our results should be provable now with TLAPS by writing an arbitrary definition of *Def* and proving them without using that definition.

4 Multiple Arguments

TLA$^+$ permits recursive definitions of operators that take multiple arguments. We must therefore assign a meaning to this definition, for all $n \in Nat$:

(11) $F(x_1, \ldots, x_n) \triangleq Def(x_1, \ldots, x_n, F)$

where F is declared by

$$\text{CONSTANT } F(\_, \ldots, \_, \_(\_, \ldots, \_))$$

For $n = 0$, in which (11) is $F \triangleq Def(F)$, its obvious meaning is:

$$F \triangleq \text{CHOOSE } G : G = Def(G)$$

We've already defined (11) for $n = 1$. For $n > 1$, we define $F(x_1, \ldots, x_n)$ to equal $G(\langle x_1, \ldots, x_n \rangle)$ for an operator G that has a single argument. To simplify things, we introduce some notation. Let $\mathbf{x}$ stand for $x_1, \ldots, x_n$, so we can therefore write (11) as

$$F(\mathbf{x}) \triangleq \mathit{Def}(\mathbf{x}, F)$$

We will define the operator G such that $F(\mathbf{x})$ equals $G(\langle \mathbf{x} \rangle)$. For any expression z and any operator H of a single argument, we define

$$\begin{aligned} {}_n z &\triangleq z[1], \ldots z[n] \\ {}^n H(\mathbf{x}) &\triangleq H(\langle \mathbf{x} \rangle) \end{aligned}$$

We define G by the recursive definition

(12) $G(z) \triangleq \mathit{Def}_G(z, G)$

where Def_G is defined by

(13) $\mathit{Def}_G(z, H) \triangleq \mathit{Def}({}_n z, {}^n H)$

Let fix_G and Fr_G be the operators fix and Fr defined in Section 3, when Def_G is substituted for Def. In that section we defined G to be this operator:

$$\mathit{Fr}_G(x) \triangleq (\text{CHOOSE } g : (x \in \text{DOMAIN } g) \land \mathit{fix}_G(g))[x]$$

Expanding definitions, we obtain:

$$\begin{aligned} &\mathit{fix}_G(g) \equiv \\ &\quad \forall h : (\forall x \in \text{DOMAIN } g : h[x] = g[x]) \Rightarrow \\ &\qquad\qquad (g = [x \in \text{DOMAIN } g \mapsto \mathit{Def}({}_n x, {}^n(\text{LAMBDA } y : g[y]))]) \end{aligned}$$

We then define F to equal ${}^n\mathit{Fr}_G$. Applying Corollary 3 to Def_G and Fr_G and expanding definitions, we get this result:

$$\begin{array}{lll} (14) & \text{ASSUME} & \text{NEW } S,\ \mathit{WellFounded}(S), \\ & & \text{ASSUME NEW } G(\_, \ldots, \_),\ \text{NEW } H(\_, \ldots, \_) \\ & & \text{PROVE } \ \forall x \in S : (\forall y \in \mathit{LT}(x, S) : G(y) = H(y)) \\ & & \qquad\qquad\qquad \Rightarrow (\mathit{Def}({}_n x, G) = \mathit{Def}({}_n x, H)) \\ & \text{PROVE} & \forall \langle \mathbf{x} \rangle \in S : F(\mathbf{x}) = \mathit{Def}(\mathbf{x}, F) \end{array}$$

Like Corollary 3 of Section 3, the theorem (14) is the correctness condition for the meaning we assign to the definition (11).

We cannot write (11) in TLA$^+$ because we cannot express "...", as in $G(\_, \ldots, \_)$. (Neither can we write the definition (14).) We can view (14) as a collection of theorems, one for each number n. A TLAPS library file could contain perhaps the first dozen of those theorems. Alternatively, instead of defining F by (11), we can first define G by (12) and (13) and then define $F(x_1, \ldots, x_n)$ to equal $G(\langle x_1, \ldots, x_n \rangle)$. We can then deduce the desired property of F by applying Corollary 3 to G.

5 Mutual Recursion

In TLA$^+$, an operator not declared in a RECURSIVE statement cannot be used before (or in) its definition. In defining the meaning of a module, all occurrences of such an operator can be eliminated by expanding the operator's definition. What remains is a sequence of sets of definitions of recursive operator definitions, each set having this form for some k:

$$(15)\quad \begin{aligned} F_1(x_1,\ldots,x_{n_1}) &\triangleq Def_1(x_1,\ldots,x_{n_1},F_1,\ldots,F_k)\\ &\;\vdots\\ F_k(x_1,\ldots,x_{n_k}) &\triangleq Def_k(x_1,\ldots,x_{n_k},F_1,\ldots,F_k)\end{aligned}$$

(Each Def_i need not actually depend on all the F_i.) For $k > 1$, this is called a set of mutually recursive definitions. We define the meaning of (15) in terms of a recursive definition of a single operator G taking a single argument by:

$$(16)\quad F_i(x_1,\ldots,x_{n_i}) \triangleq G(\langle i, \langle x_1,\ldots,x_{n_i}\rangle\rangle)$$

We define G by this recursive definition of the form (4):

$$(17)\quad G(z) \triangleq Def_G(z, G)$$

with Def_G defined by

$$(18)\quad \begin{aligned} &Def_G(z,H) \triangleq\\ &\quad \text{CASE } z[1]=1 \to Def_1(\langle z[2][1],\ldots,z[2][n_1],\widehat{H}_1,\ldots,\widehat{H}_k)\\ &\qquad\qquad \vdots\\ &\qquad \Box\ z[1]=k \to Def_k(z[2][1],\ldots,z[2][n_k],\widehat{H}_1,\ldots,\widehat{H}_k)\\ &\quad \text{where } \widehat{H}_i(x_1,\ldots,x_{n_i}) \triangleq H(i,\langle x_1,\ldots,x_{n_i}\rangle)\end{aligned}$$

Just as we obtained (14) for the case $k = 1$, we can apply Corollary 3 to G and expand definitions to get this result:

$$(19)\quad \begin{aligned} &\text{ASSUME}\ \ \text{NEW } S,\ WellFounded(S),\\ &\qquad\qquad \text{ASSUME}\ \ \text{NEW } H(\_),\ \text{NEW } J(\_)\\ &\qquad\qquad \text{PROVE}\ \ \forall x \in S : (\forall y \in LT(x,S) : H(y) = J(y))\\ &\qquad\qquad\qquad\qquad\qquad \Rightarrow (Def_G(x,H) = Def_G(x,J))\\ &\text{PROVE}\ \ \forall \langle i, \langle x_1,\ldots,x_{n_i}\rangle\rangle \in S :\\ &\qquad\quad (i \in 1\,..\,k) \Rightarrow\\ &\qquad\qquad F_i(x_1,\ldots,x_{n_i}) = Def_i(x_1,\ldots,x_{n_i},F_1,\ldots,F_k)\end{aligned}$$

where (18) defines Def_G in terms of the F_i.

As with (14), formula (19) is not expressible in TLA$^+$. It is a collection of formulas, one for each choice of the numbers k, n_1, …, n_k. Unlike the $k = 1$ case, writing these as separate theorems in a TLAPS library file does not seem feasible. We can use the alternative approach of not writing (15), but instead first defining G by (17) and (18), and then defining the F_i by (16).

References

[1] Arthur Charguéraud. The optimal fixed point combinator. In Matt Kaufmann and Lawrence C. Paulson, editors, *Interactive Theorem Proving, First International Conference, ITP 2010, Edinburgh, UK, July 11-14, 2010. Proceedings*, volume 6172 of *Lecture Notes in Computer Science*, pages 195–210. Springer, 2010.

[2] Leslie Lamport. *Specifying Systems.* Addison-Wesley, Boston, 2003. Also available on the Web via a link at `http://lamport.org`.

Contents

RESEARCH CENTRE
SACLAY – ÎLE-DE-FRANCE

1 rue Honoré d'Estienne d'Orves
Bâtiment Alan Turing
Campus de l'École Polytechnique
91120 Palaiseau

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-0803