

Converting The *MongoLoglessDynamicRaft* TLA+ Specification To Ivy

Ian Dardik

Northeastern University

1 Converting MLDR From TLA+ To Ivy

The *MongoLoglessDynamicRaft* (MLDR) protocol is introduced in [6] along with a TLA+ specification [5]. We converted the TLA+ specification to Ivy in order to compare *endive* with other invariant inference tools. This conversion was nontrivial; we describe the process in this appendix along with the challenges we faced. We targeted Ivy 1.8 in our conversion, the latest version of Ivy to date.

1.1 Ivy’s Decidable Logic Fragment

The Ivy tool suite is designed to work specifically for protocols and invariants that lie within the decidable logic fragment FAU [1]. The *ivy_check* command line tool—Ivy’s user interface for checking specifications—refuses to check a specification outside of FAU by default, and behaves unreliably if a user opts to bypass the logic fragment checks.

One of our primary goals is to validate the translated MLDR Ivy specification, and thus we aimed to fit the MLDR Ivy specification into FAU in order to leverage Ivy’s tool suite for our validation. A specification that lies within FAU, but uses no interpreted types, lies within the *Extended EPR* [4] logic fragment. We can easily avoid interpreted types in the MLDR Ivy specification, and hence we target the Extended EPR logic fragment. While we were able to translate the MLDR protocol itself into Extended EPR, the full specification, including our only known inductive invariant for MLDR, falls outside of Extended EPR. We discuss our MLDR protocol translation process into Extended EPR in section 1.2, followed by a discussion of our translation process for the inductive invariant that falls outside of Extended EPR in section 1.3.

1.2 Protocol Conversion

The conversion can be summarized as a mapping from each component of the MLDR TLA+ specification to a component in the MLDR Ivy specification. We show the mapping at a high level in Figure 1, and provide detail in the sections below.

Protocol	TLA+		Ivy 1.8
Sorts / Types	CONSTANT	→	type
State Variables	VARIABLE	→	individual / function
Initial Constraint	<i>Init</i> Operator	→	after init
Transition Relation	<i>Next</i> Operator	→	action
Helper Definitions	Operators	→	function / relation

Fig. 1. High level conversion mapping.

Sorts And Types TLA+ is untyped while Ivy is typed, and thus we need to introduce several types into the new Ivy specification. The first type is for the sort parameter for MLDR, *Server*. The sort is declared in TLA+ using the `CONSTANT` keyword, and maps to the `type` keyword in Ivy. Second, we include a `state_type` type in Ivy to denote primary versus secondary servers. Third, we introduce a `nat` type to represent natural numbers, which we equip with total order axioms and the `succ` operator. Finally, we include the types `quorum` and `conf` to represent quorums and configurations. While quorums and configurations are conceptually the same type—the power set of *Server*—we found that separating the two types yields a cleaner design in Ivy.

State Variables State variables are encoded in TLA+ using the `VARIABLE` keyword, and map to the `individual` and `function` keywords in Ivy, depending on whether each state variable has an individual or a function type. In the MLDR TLA+ specification, every state variable is a function whose universe of values is constrained by the *TypeOK* property. We use this property as a direct guide in our state variable conversion, which we show in Figure 2.

TLA+	Ivy1.8
$\overline{TypeOK} ==$	
$\wedge currentTerm \in [Server \rightarrow \mathbb{N}]$	function <i>current_term</i> (<i>S</i> : <i>server</i>) : <i>nat</i>
$\wedge state \in [Server \rightarrow \{Secondary, Primary\}]$	function <i>state</i> (<i>S</i> : <i>server</i>) : <i>state_type</i>
$\wedge config \in [Server \rightarrow \text{SUBSET } Server]$	function <i>config</i> (<i>S</i> : <i>server</i>) : <i>conf</i>
$\wedge configVersion \in [Server \rightarrow \mathbb{N}]$	function <i>config_version</i> (<i>S</i> : <i>server</i>) : <i>nat</i>
$\wedge configTerm \in [Server \rightarrow \mathbb{N}]$	function <i>config_term</i> (<i>S</i> : <i>server</i>) : <i>nat</i>

Fig. 2. State variable conversion mapping.

The Initial Constraint And Transition Relation The initial constraint is encoded in TLA+ as a conjunction of state variable constraints, and maps to

Ivy as a sequence of function constraints, wrapped in an `after init` block. The initial constraint mapping for MLDR from TLA+ to Ivy is shown in Figure 3.

The transition relation is encoded in TLA+ as a disjunction of actions, each of which maps to an exported Ivy `action` block. Within each action, guards are specified in TLA+ as a constraint on unprimed state variables, and map to the `assume` keyword in Ivy. The actions are described symbolically in TLA+ as a relation between unprimed and primed state variables, and map to assignment operators on individuals, functions, and relations in Ivy.

TLA+		Ivy 1.8
$Init ==$		<code>after init {</code>
$\wedge currentTerm = [i \in Server \mapsto 0]$		<code>current_term(S) := zero;</code>
$\wedge state = [i \in Server \mapsto Secondary]$		<code>state(S) := secondary;</code>
$\wedge config = [i \in Server \mapsto 1]$	\rightarrow	<code>config_version(S) := zero;</code>
$\wedge configVersion = [i \in Server \mapsto 0]$		<code>config_term(S) := zero;</code>
$\wedge \exists c \in SUBSET Server :$		<code>assume config(S) = config(T);</code>
$\wedge c \neq \emptyset$		<code>}</code>
$\wedge config = [i \in Server \mapsto c]$		

Fig. 3. Initial constraint conversion mapping.

Helper Definitions In TLA+ it is standard to wrap the initial constraint, transition relation, and each individual action in an operator. However, operators are also often used as “helpers” as a means to make a specification modular and readable. These helper operators directly map to functions and relations in Ivy. We provide an example mapping for the *IsNewerConfig* operator in Figure 4.

TLA+		Ivy 1.8
$IsNewerConfig(s,t) ==$		<code>relation newer_config</code>
$\vee configTerm[s] > configTerm[t]$		<code>(S:server, T:server) =</code>
$\vee \wedge configTerm[s] = configTerm[t]$	\rightarrow	<code>1t(config_term(T), config_term(S))</code>
$\wedge configVersion[s] > configVersion[t]$		<code> config_term(T) = config_term(S)</code>
		<code>& 1t(config_version(T),</code>
		<code>config_version(S))</code>

Fig. 4. The conversion mapping for *IsNewerConfig*, a helper operator. `1t` is another helper operator in the MLDR TLA+ specification that has been translated into an Ivy relation, and represents the *less than* operator on the `nat` type.

The Protocol Lies Within Extended EPR The MLDR Ivy specification has the quantifier alternation graph: $\text{conf} \rightarrow \text{quorum} \rightarrow \text{server}$. This graph is stratified, and hence fits into Extended EPR.

1.3 Inductive Invariant Conversion

Endive successfully synthesized an inductive invariant for MLDR which we converted from TLA+ to Ivy [3]. Unfortunately, this inductive invariant introduces a cycle in the quantifier alternation graph of the MLDR Ivy specification, and hence falls outside of Extended EPR [4]. The cycle is introduced in the *ActiveConfigSafeAtTerms* conjunct as a $\forall\exists$ edge from **server** to itself, and is shown in Figure 5.

Although techniques exist that may fit a protocol into Extended EPR—such as splitting code with mutually dependent types into modules [2,4]—these techniques may require significant effort and, in general, are not guaranteed to be complete [4]. Instead of manually using Ivy to find an inductive invariant in Extended EPR, we left this task for the invariant inference tools.

```
invariant [ActiveConfigSafeAtTerms]
  forall S, T : server. active_config(T) →
    forall Q:quorum. quorumof(Q,config(T)) →
      exists N:server. qmember(N,Q)
        & (config_term(S) = current_term(N) | lt(config_term(S), current_term(N)))
```

Fig. 5. The inductive invariant conjunct *ActiveConfigsSafeAtTerms* introduces a $\forall\exists$ edge from **server** to itself because `exists N:server` appears within the scope of `forall S, T : server`.

1.4 Validating The Translation

Once we completed the conversion process, we sought to verify that the Ivy specification was correct. The ideal test would have been to translate the inductive invariant that *endive* synthesized to prove correctness, yet unfortunately, the inductive invariant places the specification outside of Extended EPR as we noted in section 1.3. Instead, we leveraged IC3PO for our sanity checks. IC3PO may accept a protocol outside of Ivy’s decidable fragment, and hence we were able to pass the MLDR Ivy specification along with *endive*’s synthesized inductive invariant. We performed sanity checks by running IC3PO for several finite instances and confirming that it terminated successfully without adding additional invariants. This sanity check gave us confidence that our conversion process for MLDR was successful.

1.5 Discussion

TLA+ is a rather expressive language where we can explicitly create a protocol and model check safety properties to gain confidence. Ivy, on the other hand, is a more restricted language, and forces protocol designers to write complex code within an individual module in a more implicit fashion. This implicit fashion entails defining bear bones constructs and providing key axioms—this workflow is aimed at keeping each construct powerful enough to prove key properties, but light enough to remain in the decidable fragment FAU. For example, consider quorums in the MLDR protocol, whose type is the power set of *Server*. In TLA+, we can explicitly use a power set operator, making quorums simple to define. In Ivy, however, there is no support for power sets; instead, a protocol designer can define a binary *member* \subseteq *server* \times *quorum* relation as a means for providing key axioms that will be necessary for any proofs about quorums.

Ivy’s implicit construction workflow begs an important question: how does a protocol designer know when she has provided sufficient axioms in order to prove key theorems on implicitly-defined types? Presumably, the designer who uses Ivy’s interactive workflow will eventually deduce when the set of axioms are insufficient, along with which additional axioms are needed. Invariant inference tools, however, provide little to no insight into whether a failure is due to insufficient axioms versus other potential reasons.

Furthermore, it is not clear that a protocol that lies within FAU is guaranteed to have an inductive invariant that is also in FAU. For any invariant inference tool that operates exclusively in FAU—or even *works better* in FAU—the tool may experience issues if it is tough, or even impossible, for an inductive invariant to exist in FAU. In this case, presumably, a designer using Ivy’s interactive workflow would eventually discover the need to split the protocol and invariants into modules that avoid quantifier alternation graph cycles, along with exactly how this may be done. Unfortunately, invariant inference tools offer little to no insight into whether a protocol must be split into modules, and how it may be done.

We do not know the answer to the questions posed above, however, we consider these aspects to be potential limitations of any invariant inference tool that operates within FAU or relies on SMT queries in an unbounded domain. Thus we believe that, to the best of our abilities, we provide a fair comparison for the MLDR protocol between *endive* and any tool that accepts the Ivy version as input.

References

1. Yeting Ge and Leonardo Moura. Complete instantiation for quantified formulas in satisfiability modulo theories. In *Proceedings of the 21st International Conference on Computer Aided Verification, CAV ’09*, page 306–320, Berlin, Heidelberg, 2009. Springer-Verlag.
2. Kenneth L. McMillan and Oded Padon. Deductive verification in decidable fragments with ivy. In Andreas Podelski, editor, *Static Analysis - 25th International*

- Symposium, SAS 2018, Freiburg, Germany, August 29-31, 2018, Proceedings*, volume 11002 of *Lecture Notes in Computer Science*, pages 43–55. Springer, 2018.
3. MLDR Ivy Specification. https://github.com/will62794/invariant-inference-et-al/blob/master/examples/tools/ic3po/mldr_epr.ivy, 2022.
 4. Oded Padon, Giuliano Losa, Mooly Sagiv, and Sharon Shoham. Paxos Made EPR: Decidable Reasoning about Distributed Protocols. *Proc. ACM Program. Lang.*, 1(OOPSLA), oct 2017.
 5. William Schultz. Mongoraftreconfig tla+ specifications. <https://doi.org/10.5281/zenodo.5715511>, November 2021.
 6. William Schultz, Siyuan Zhou, Ian Dardik, and Stavros Tripakis. Design and Analysis of a Logless Dynamic Reconfiguration Protocol. In Quentin Bramas, Vincent Gramoli, and Alessia Milani, editors, *25th International Conference on Principles of Distributed Systems (OPODIS 2021)*, volume 217 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 26:1–26:16, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.