A Cutoff Rule For A Special Class Of Parameterized Distributed Protocols

Ian Dardik

March 6, 2022

1 Introduction

In this note, we consider the verification problem of a transition system $T = (I, \Delta)$ where I is the initial constraint, Δ is the transition relation, and the system is parameterized by a single sort P of identical elements (We make the notion of "identical" precise in Assumption 1 below). We assume that we are given a candidate inductive invariant Φ which implies our key safety property. Φ is restricted to be in Prenex Normal Form (PNF) with only universal quantifiers, while Δ is restricted to be in PNF with only existential quantifiers. We adopt the convention of [2] where $T(P)$ is the template of T, and $T(|P|)$ is a finite instantiation.

In this note, we will build several lemmas that lead to an interesting result: let m be the number of variables that Φ quantifies over and n be the number of variables that Δ quantifies over, then if $\Phi(m+n)$ is an inductive invariant, $\Phi(k)$ is also an inductive invariant for all $k > m+n$. We will refer to this as the M-N Theorem in this note. This result is useful because it reduces the vefification problem on T to model checking a finite number of instances $T(1), T(2), ..., T(m+n)$. Essentially, $m+n$ is a cutoff instance size for proving that our inductive invariant holds.

Note: I think it is likely that if $\Phi(m+n)$ is an inductive invariant, then it is *also* the case for $\Phi(k)$ for all $k < m+n$, but I left this out of this note for the time being to focus on the $k > m+n$ case.

2 Preliminaries

In this section we cover several preliminary items that we use to prove the M-N Theorem.

2.1 Without Loss Of Generality

We will assume that the parameter $P = \{1, 2, ..., |P|\}$. This assumption comes without loss of generality because each member of P is assumed to be identical.

2.2 Assumptions

This section contains the list of assumptions for the transition system we work with. In other words, these assumptions are the requirements for the M-N Theorem to hold.

Assumption 1 (P Has Identical Elements)**.** Let f be a ground formula and let $\pi : P \to P$ be a bijective function, i.e. a permutation on P. Then we assume:

$$f \leftrightarrow \pi(f)$$

2.3 Definitions

Definition 1 (States)**.** Let $k \in \mathbb{N}$, then:

$$\text{States}(k) := \{\text{all states when } |P| = k\}$$

In this note we consider a state s to be a formula: a disjunction of cubes that describe one or more states in the transition system. Intuitively a single state ought to be a single cube, but we will implicitly refer to "a state" as potentially multiple states throughout this note.

Definition 2 (Ground Formulas)**.** Let F be a quantified formula and $k \in \mathbb{N}$.

$$\text{Gr}(F, k) := \{f | (f \text{ is a ground formula of } F(k)) \wedge (f \models F(k))\}$$

"$f \models F(k)$" is used here as syntactic sugar for "$f \rightarrow F(k)$". Essentially, $\text{Gr}(F, k)$ will contain all ground formulas of $F(k)$ that are necessarily *weaker*. Thus if $\text{Gr}(F, k)$ contains any elements (formulas) that are false, we can conclude that $F(k)$ is false. Likewise, if $F(k)$ is valid, then we can be sure that each element (formula) of $\text{Gr}(F, k)$ is valid as well.

Example 1. $\text{Gr}([\forall p, q, p = q], 2) := \{(1 = 1), (1 = 2), (2 = 1), (2 = 2)\}$
Note: we sometimes use square braces to wrap formulas when it looks better than parentheses.
Notice that $\text{Gr}([\forall p, q, p = q], 2)$ contains elements that are false. This indicates that $[\forall p, q, p = q](2)$ is a false statement.

Example 2. $\text{Gr}((\forall p, q, p \neq q \rightarrow \text{sv[p]} \neq \text{sv[q]}), 3) := \{(1 \neq 1 \rightarrow \text{sv}[1] \neq \text{sv}[1]), (1 \neq 2 \rightarrow \text{sv}[1] \neq \text{sv}[2]), ...\}$ Where sv is some state variable.

Remark 1. Notice that for any state $s \in \text{States}(k)$ and quantified formula F:

$$(s \models F(k)) \leftrightarrow (\forall f \in \text{Gr}(F, k), s \models f)$$

TODO: this remark needs to be proved.

3 Helper Lemmas

Lemma 1. *Let $k \in \mathbb{N}$, and $s \in \text{States}(k)$ such that $s \models \Phi(k)$. Then for $j \leq k$, it is also the case that $s \models \Phi(j)$.*

Proof. Let $j \leq k$ be given. We will begin by observing that $\text{Gr}(\Phi, j) \subseteq \text{Gr}(\Phi, k)$ due to the fact that Φ is a universally quantified PNF formula. The result then follows immediately from Remark 1. □

Lemma 2. *Let s be a state, f be a ground formula, and π be a permutation. Then:*

$$(s \models f) \leftrightarrow (\pi(s) \models \pi(f))$$

Proof. Suppose that $s \models f$, which is syntactic sugar for $s \rightarrow f$ because s and f are both formulas. By Assumption 1, $s \leftrightarrow \pi(s)$ and $f \leftrightarrow \pi(f)$, and the result follows immediately.

Now suppose that $\pi(s) \models \pi(f)$. π is a bijection–and hence invertible–thus π^{-1} is a permutation as well. By Assumption 1, $\pi(s) \leftrightarrow \pi^{-1}(\pi(s)) = s$ and $\pi(f) \leftrightarrow \pi^{-1}(\pi(f)) = f$. The result follows immediately. □

Lemma 3. *Let $k \in \mathbb{N}$ and s be a state such that $s \models \Phi(k)$. If π is a permutation then it is also the case that $\pi(s) \models \Phi(k)$.*

Proof. Suppose that $s \models \Phi(k)$. Then by Remark 1, $\forall f \in \text{Gr}(\Phi, k), s \models f$. But Assumption 1 shows that $s \leftrightarrow \pi(s)$ and hence $\forall f \in \text{Gr}(\Phi, k), \pi(s) \models f$ which gives us our result by Remark 1. □

4 The M-N Theorem

Theorem 1 (M-N)**.** Suppose that Φ is in PNF with only universal quantifiers, while Δ is in PNF with only existential quantifiers. Let m be the number of variables that Φ quantifies over and n be the number of variables that Δ quantifies over. If $\Phi(m+n)$ is an inductive invariant, then $\Phi(k)$ is also an inductive invariant for any $k > m+n$.

Proof. Let $k > m+n$ be given and assume that $[\Phi \wedge \Delta \to \Phi'](m+n)$ is valid. Let $s \in \text{States}(k)$ such that $s \models \Phi(k)$, and let δ be an arbitrary transition such that $\delta \models \Delta(k)$. Finally, let $f' \in \text{Gr}(\Phi', k)$ be arbitrary, then, by Remark 1, it suffices to show that $(s \wedge \delta) \models f'$.

Let π be a permutation such that $\pi(\delta) \models \Delta(m+n)$ and $\pi(f') \in \text{Gr}(\Phi', m+n)$, i.e. $\pi(f') \models \Phi'(m+n)$. We know that we can find such a π because δ will contain at most n distinct elements of P and f' will contain at most m distinct elements of P. Now by Lemma 1 we see that $s \models \Phi(m+n)$, and furthermore $\pi(s) \models \Phi(m+n)$ by Lemma 3. Thus $\pi(s \wedge \delta) \models [\Phi \wedge \Delta](m+n)$ which implies $\pi(s \wedge \delta) \models \Phi'(m+n)$ by our initial assumption. In particular, $\pi(s \wedge \delta) \models \pi(f')$ by Remark 1, and therefore $s \wedge \delta \models f'$ by Lemma 2. $\square$

5 Case Studies

In this section we visit several (more coming soon) distributed protocols that are parameterized by a single sort and satisfy Assumption 1.

5.1 Peterson's Mutex Protocol

Peterson's Mutex Protocol can be encoded with a transition function Δ in PNF that quantifies over two variables. A sample inductive invariant candidate is given in [1] that quantifies of two variables and works for $|P| = 2$:

```
Phi == \A p,q \in ProcSet :
   /\ pc[p] \in {"a3","a4","cs"} => flag[p]
   /\ (p#q /\ pc[p] = "cs" /\ pc[q] = "a4") => turn = p
   /\ (p # q) => ~(pc[p] = "cs" /\ pc[q] = "cs")
```

However, by the M-N Theorem, we must show that Φ is an inductive invariant for the cases when $|P| = 1, ..., 4$. In fact, we easily see that Φ fails to be inductive in the case:

```
/\ turn = 1              /\ turn = 2
/\ pc[1] = "cs"          /\ pc[1] = "cs"
/\ pc[2] = "a4"    ->    /\ pc[2] = "a4"
/\ pc[3] = "a3"          /\ pc[3] = "a4"
/\ a3(3,2)
```

References

[1] Parametric Peterson's Mutex Protocol. `https://github.com/iandardik/iinf/blob/master/ii_cutoff/mn_thm/PetersonParametric.tla`, 2022.

[2] Aman Goel and Karem Sakallah. On Symmetry and Quantification: A New Approach to Verify Distributed Protocols. In *NASA Formal Methods Symposium*, pages 131–150. Springer, 2021.