

# A Cutoff Rule For A Special Class Of Parameterized Distributed Protocols

Ian Dardik

March 7, 2022

## 1 Introduction

In this note, we consider the verification problem of a transition system  $T = (I, \Delta)$  where  $I$  is the initial constraint,  $\Delta$  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  $\Phi$  which implies our key safety property.  $\Phi$  is restricted to be in Prenex Normal Form (PNF) with only universal quantifiers, while  $\Delta$  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  $\Phi$  quantifies over and  $n$  be the number of variables that  $\Delta$  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 verification problem on  $T$  to model checking a finite number of instances  $T(1), T(2), \dots, T(m+n)$ . 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  $P = \{1, 2, \dots, |P|\}$ . This assumption comes without loss of generality because each member of  $P$  is assumed to be identical. This assumption also implies that for any two finite sort instances  $P$  and  $Q$ ,  $|P| \leq |Q| \leftrightarrow P \subseteq Q$ .

### 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  $\pi : P \rightarrow P$  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:

$$\text{States}(k) := \{s \mid s \text{ is a state of } T(k)\}$$

In this note we consider a state  $s \in \text{States}(k)$  to be a quantifier-free formula: a conjunction of constraints that describe a single state in  $T(k)$ .

**Definition 2** (Satisfaction). Let  $f$  and  $g$  be formulas in First Order Logic. Then we say  $f \models g$  iff  $f \rightarrow g$ . Alternatively,  $f$  satisfies  $g$  iff  $f$  is stronger than  $g$ .

**Example 1.** Consider the transition system  $T(P)$  with two state variables,  $x \in (P \rightarrow \mathbb{N})$  and  $y \in \mathbb{Z}$ . Let  $|P| = 2$ , then  $P = \{1, 2\}$ . Let  $s := (x[1] = 6 \wedge x[2] = 0 \wedge y = -22)$  be a state in the transition system. Let  $F := \forall p, q \in P, x[p] \neq x[q]$  and  $f := (x[1] \neq x[2])$ . Then  $f$  is a ground formula of  $F(2)$ ,  $F(2) \models f$ ,  $s \models F(2)$ , and  $s \models f$ .

**Definition 3** (Ground Formulas). Let  $F$  be a quantified formula and  $k \in \mathbb{N}$ .

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

**Example 2.**  $\text{Gr}([\forall p, q \in P, p = q], 2) = \{(1 = 1), (1 = 2), (2 = 1), (2 = 2)\}$

Note: we sometimes use square braces to wrap formulas when it looks better than parentheses.

Notice that  $\text{Gr}([\forall p, q \in P, p = q], 2)$  contains elements that are false. This indicates that the statement  $[\forall p, q \in P, p = q](2)$  is not valid.

**Example 3.** Let  $sv$  be a state variable, then:

$$\text{Gr}([\forall p, q \in P, p \neq q \rightarrow sv[p] \neq sv[q]], 3) = \{(1 \neq 1 \rightarrow sv[1] \neq sv[1]), (1 \neq 2 \rightarrow sv[1] \neq sv[2]), \dots\}$$

## 3 Helper Lemmas

**Lemma 1.** Let  $k \in \mathbb{N}$ ,  $s \in \text{States}(k)$ , and  $F$  be a universally quantified formula. Then:

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

*Proof.* Suppose that  $s \models F(k)$ . For an arbitrary formula  $f \in \text{Gr}(F, k)$ ,  $F(k) \models f$  and hence we see that  $s \rightarrow F(k) \wedge F(k) \rightarrow f$ . It follows that  $s \models f$ .

Now suppose that  $\forall f \in \text{Gr}(F, k), s \models f$ . Suppose, for the sake of contradiction, that  $s \not\models F(k)$ . Then it must be the case that  $s \wedge \neg F(k)$ . We know that  $F$  is universally quantified, so let  $F(k) := \forall \hat{x}, \phi(\hat{x})$  where  $\hat{x}$  is the vector of variables that we quantify over. Then it must be the case that  $\exists \hat{x}, \neg \phi(\hat{x})$ , but  $\phi(\hat{x}) \in \text{Gr}(F, k)$ . However this contradicts our original assumption, and hence the result is proved.  $\square$

**Lemma 2.** 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  $k$  and  $j \leq k$  be given and suppose that  $s \models \Phi(k)$ . By Lemma 1,  $\forall f \in \text{Gr}(F, k), s \models \Phi(k)$ . Now observe that  $\text{Gr}(\Phi, j) \subseteq \text{Gr}(\Phi, k)$  due to the fact that  $\Phi$  is a universally quantified PNF formula. Thus it is also the case that  $\forall f \in \text{Gr}(F, j), s \models \Phi(j)$ , and then the result follows from Lemma 1.  $\square$

**Lemma 3.** Let  $s$  be a state,  $f$  be a ground formula, and  $\pi$  be a permutation. Then:

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

*Proof.* Suppose that  $s \models f$ , and hence  $s \rightarrow f$ . By Assumption 1,  $s \leftrightarrow \pi(s)$  and  $f \leftrightarrow \pi(f)$ , and the result follows immediately.

Now suppose that  $\pi(s) \models \pi(f)$ .  $\pi$  is a bijection—and hence invertible—thus  $\pi^{-1}$  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.  $\square$

**Lemma 4.** Let  $k \in \mathbb{N}$  and  $s$  be a state such that  $s \models \Phi(k)$ . If  $\pi$  is a permutation then it is also the case that  $\pi(s) \models \Phi(k)$ .

*Proof.* Suppose that  $s \models \Phi(k)$ . Then by Lemma 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 Lemma 1.  $\square$

## 4 The M-N Theorem

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

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

Next, we will construct a permutation  $\pi$  as follows: let  $x_1, \dots, x_j$  be the distinct elements of  $P$  used in  $\delta$  and  $f'$ . We know that  $j \leq m+n$  because  $\Delta$  quantifies over  $n$  variables while  $\Phi$  quantifies over  $m$  variables. Let:

$$\pi := \begin{pmatrix} x_1 & x_2 & \dots & x_j \\ 1 & 2 & \dots & j \end{pmatrix}$$

Notice that the formulas  $\pi(\delta)$  and  $\pi(s)$  now only contain the elements  $1, \dots, j$  and, in particular,  $\pi(\delta) \models \Delta(m+n)$  and  $\pi(f') \in \text{Gr}(\Phi', m+n)$ , i.e.  $\pi(f') \models \Phi'(m+n)$ . By Lemma 2 we see that  $s \models \Phi(m+n)$ , and furthermore  $\pi(s) \models \Phi(m+n)$  by Lemma 4. 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 Lemma 1, and therefore  $s \wedge \delta \models f'$  by Lemma 3.  $\square$

## 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 relation  $\Delta$  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  $\Phi$  is an inductive invariant for the cases when  $|P| = 1, \dots, 4$ . In fact, we easily see that  $\Phi(3)$  fails to be inductive in the following counter example:

$\wedge \text{ turn} = 1$		$\wedge \text{ turn} = 2$
$\wedge \text{ pc}[1] = \text{"cs"}$		$\wedge \text{ pc}[1] = \text{"cs"}$
$\wedge \text{ pc}[2] = \text{"a4"}$	$\rightarrow$	$\wedge \text{ pc}[2] = \text{"a4"}$
$\wedge \text{ pc}[3] = \text{"a3"}$		$\wedge \text{ pc}[3] = \text{"a4"}$
$\wedge \text{ a3}(3,2)$		

## References

- [1] Parametric Peterson's Mutex Protocol. [https://github.com/iandardik/iinf/blob/master/ii\\_cutoff/mn\\_thm/PetersonParametric.tla](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.