

# M-N Without Permutations

Ian Dardik

March 29, 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  $E = \{e_1, \dots\}$  of indistinguishable elements.

To begin, we will introduce notation for the template and finite instances of a transition system. We adopt the convention of [1] where  $T(E)$  is the template of  $T$  and  $T(|E|)$  is a finite instance. We can also refer to the template or a finite instance of a quantified formula  $F$  and the sort  $E$ . For example, suppose  $F$  is in Prenex Normal Form (PNF) and universally quantifies over  $j$  variables, i.e.  $F$  can be written as:

$$F := \forall x_1, \dots, x_j \in E, \phi(x_1, \dots, x_j)$$

where  $\phi$  is a non-quantified statement whose only free variables are  $x_1, \dots, x_j$ . Then  $F(k)$  is identical to the formula  $F$ , except  $E$  is replaced by  $E(k) \subseteq E$ , where  $E(k) = \{e_1, \dots, e_k\}$ , that is,  $k$  distinct arbitrary elements of  $E$ . Thus we see:

$$F(k) = \forall x_1, \dots, x_j \in E(k), \phi(x_1, \dots, x_j)$$

In this note, we are concerned with the specific scenario in which we are given a candidate inductive invariant  $\Phi$ , and the finite instances  $\Phi(1), \dots, \Phi(k)$  have been proved to be inductive invariants for  $T(1), \dots, T(k)$ ; we want to know whether  $\Phi$  is an inductive invariant for  $T$ . We are specifically concerned with the case in which both  $\Delta$  and  $\Phi$  are written in PNF and  $\Phi$  is restricted to universal quantification.

Throughout 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; if we suppose that  $\Phi(m+n)$  is an inductive invariant for  $T(m+n)$ , then  $\Phi(k)$  is also an inductive invariant for  $T(k)$  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  $T(1), \dots, T(m+n)$ . 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 Notation

**Definition 1** ( $E(k)$ ). We let  $E(k) := \{e_1, \dots, e_k\} \subseteq E$ , where each  $e_i$  is distinct and arbitrarily chosen from  $E$ . In particular, it is always the case that  $|E(k)| = k$ .

**Definition 2** ( $F(k)$ ). Let  $F$  be a quantified formula of the form  $Q_1 x_1, \dots, Q_m x_m \in E, f(x_1, \dots, x_m)$ , where each  $Q_i \in \{\forall, \exists\}$ . Then for any  $k > 0$ :

$$F(k) := Q_1 x_1, \dots, Q_m x_m \in E(k), f(x_1, \dots, x_m)$$

**Definition 3** (Finite Instances). Let  $F$  be a quantified formula of the form  $Q_1x_1, \dots, Q_mx_m \in E, f(x_1, \dots, x_m)$ , where each  $Q_i \in \{\forall, \exists\}$ . Then for any  $k > 0$ :

$$\text{FinInstances}(F, k) := \{Q_1x_1, \dots, Q_mx_m \in H, f(x_1, \dots, x_m) \mid H \subseteq E \wedge |H| = k\}$$

The sort  $E$  is assumed to be unbound, and hence  $\text{FinInstances}(F, k)$  is an infinite set.

### 3 Lemmas

**Lemma 1.** Let  $k \in \mathbb{N}$  such that  $s \in \text{States}(k)$  and  $F$  is 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  $F(k) := \forall x_1, \dots, x_m \in P, \phi(x_1, \dots, x_m)$  where  $m \geq 1$ . Then, because  $\neg F(k)$  holds, it must be the case that  $\exists x_1, \dots, x_m \in P, \neg \phi(x_1, \dots, x_m)$ . However,  $\phi(x_1, \dots, x_m) \in \text{Gr}(F, k)$  which, by our original assumption, implies  $\neg s$ . Hence we have both  $s$  and  $\neg s$  and we have reached a contradiction.  $\square$

**Lemma 2.** Let  $F$  be a quantified formula and  $k > 0$  be given, then:

$$F(k) \leftrightarrow \forall f \in \text{FinInstances}(F, k), f$$

*Proof.* Let  $F$  be a quantified formula of the form  $Q_1x_1, \dots, Q_mx_m \in E, f(x_1, \dots, x_m)$ .

Suppose that  $F(k)$  is true. Consider arbitrary  $f \in \text{FinInstances}(F, k)$ .  $f$  has the form  $Q_1x_1, \dots, Q_mx_m \in H, f(x_1, \dots, x_m)$  where  $H = \{h_1, \dots, h_k\}$  is a particular subset of  $E$ . Notice that  $F(k) \rightarrow f$ , and hence  $f$  must be true.

Now suppose that  $\forall f \in \text{FinInstances}(F, k), f$ , then the result follows trivially.  $\square$

### 4 The M-N Theorem

In this section, we will establish initiation and consecution in two separate lemmas using similar techniques. The M-N Theorem follows immediately from these two lemmas.

**Lemma 3** (M-N Initiation). Suppose that  $\Phi(m)$  is an inductive invariant for  $T(m)$ , then  $I(k) \rightarrow \Phi(k)$  for all  $k > m$ .

**Lemma 4** (M-N Consecution). Suppose that  $\Phi$  and  $\Delta$  are both in PNF, while  $\Phi$  is restricted to universal quantification. Let  $m$  be the number of variables that  $\Phi$  quantifies over and  $n$  be the number of variables that  $\Delta$  quantifies over. If  $\Phi(\ell)$  is an inductive invariant for all  $1 \leq \ell \leq m + n$ , then  $\Phi(k)$  is inductive for any  $k > m + n$ .

*Proof.* Assume that  $[\Phi \wedge \Delta \rightarrow \Phi'](\ell)$  is valid for all  $1 \leq \ell \leq m + n$ . Let  $k > m + n$  be given, we want to show that  $[\Phi \wedge \Delta \rightarrow \Phi'](k)$  is also valid. Let  $s \in \text{States}(k)$  such that  $s \models \Phi(k)$  and let  $\delta \in \text{Gr}(\Delta, k)$  such that  $\delta \models \Delta(k)$ . Then  $(s \wedge \delta)$  is a formula that describes the states reachable from  $s$  in one “ $\delta$  step”, and it suffices to show that  $(s \wedge \delta) \models \Phi'(k)$ . Furthermore, let  $\phi' \in \text{Gr}(\Phi', k)$  be arbitrary, then, by Lemma 1 and the fact that  $\Phi'$  is in PNF and universally quantified, it suffices to show that  $(s \wedge \delta) \models \phi'$ .

Let  $f_1, \dots, f_i$  be the unique elements of  $E$  in  $\phi$  and let  $d_1, \dots, d_j$  be the unique elements of  $E$  in  $\delta$ . We know that  $1 \leq i \leq m$  because  $\phi \in \text{Gr}(\Phi, k)$  and  $\Phi$  quantifies over  $m$  variables; likewise, we know that  $1 \leq j \leq n$  because  $\delta \in \text{Gr}(\Delta, k)$  and  $\Delta$  quantifies over  $n$  variables. Then:

$$(s \wedge \delta) \models [\Phi \wedge \Delta](E = \{f_1, \dots, f_i, d_1, \dots, d_j\}) \in \text{FinInstances}(F, i + j)$$

By our initial assumption,  $[\Phi \wedge \Delta \rightarrow \Phi'](i + j)$  is valid because  $1 \leq i + j \leq m + n$ . Thus, by Lemma 2,  $[\Phi \wedge \Delta \rightarrow \Phi'](E = \{f_1, \dots, f_i, d_1, \dots, d_j\})$  is also valid. Hence:

$$(s \wedge \delta) \models \Phi'(E = \{f_1, \dots, f_m, d_1, \dots, d_n\}) \models \phi'$$

□

Next we present 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.* This follows immediately from the previous two lemmas. □

## References

- [1] 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.