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, Δ is the transition relation, and the system is parameterized by a single sort $E = \{e_1, ...\}$ of indistinguishable elements (We make the notion of "indistinguishable" precise in Assumption **??** below).

To begin, we will introduce notation for the template and finite instances of a transition system. We adopt the convention of [**?**] 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 univerally quantifies over j variables, i.e. F can be written as:

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

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

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

In this note, we are concerned with the specific scenario in which we are given a candidate inductive invariant Φ, and the finite instances $\Phi(1), ..., \Phi(k)$ have been proved to be inductive invariants for $T(1), ..., T(k)$; we want to know whether Φ is an inductive invariant for T. We are specifically concerned with the case in which both Δ and Φ are written in PNF and Φ 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 Φ quantifies over and n be the number of variables that Δ 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 $T(1), ..., T(m + n)$. 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 (Finite Instances)**.** Let F be a quantified formula of the form:

$$Q_1 x_1, ..., Q_m x_m \in E, f(x_1, ..., x_m)$$

Where each $Q_i \in \{\forall, \exists\}$. Then for any $k > 0$:

$$\text{FinInstances}(F, k) = \{Q_1\ x_1, ..., Q_m\ x_m \in H, f(x_1, ..., x_m) \mid H \subseteq E \wedge |H| = k\}$$

Lemma 1. 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:

$$Q_1 x_1, ..., Q_m x_m \in E, f(x_1, ..., x_m)$$

Now suppose that $F(k)$ is true. Then it is the case that:

$$Q_1 x_1, ..., Q_m x_m \in \{e_1, ..., e_k\}, f(x_1, ..., x_m)$$

for arbitrary elements $e_i \in E$. Hence $\forall f \in \text{FinInstances}(F, k), f$.

TODO finish converse. □

3 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 2 (M-N Initiation)**.** Suppose that $\Phi(m)$ is an inductive invariant for $T(m)$, then $I(k) \to \Phi(k)$ for all $k > m$.

Lemma 3 (M-N Consecution)**.** Suppose that Φ is in PNF with only universal quantifiers, while Δ is in PNF. 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 inductive for any $k > m+n$.

Proof. Assume that $[\Phi \wedge \Delta \to \Phi'](m+n)$ is valid. Let $k > m+n$ be given and $s \in \text{States}(k)$ such that $s \models \Phi(k)$. Let $\delta \in \text{Gr}(\Delta, k)$, i.e. δ is a ground "transition". Let $t \in \text{States}(k)$ such that $t' \models (s \wedge \delta)$, that is, t' is an arbitrary "next" state of s. Finally, let $\phi' \in \text{Gr}(\Phi', k)$ be arbitrary, then, by Lemma **??** and the fact that Φ' is in PNF and universally quantified, it suffices to show that $t' \models \phi'$.

$\phi' \in \text{Gr}(\Phi, m+n)$ because Φ is in PNF and universally quantified. Let $f_1, ..., f_m$ be the elements of E in ϕ and let $d_1, ..., d_n$ be the elements of E in δ. Then:

$$(s \wedge \delta) \models [\Phi \wedge \Delta](E = \{f_1, ..., f_m, d_1, ..., d_n\}) \models [\Phi \wedge \Delta](m+n)$$

And hence $(s \wedge \delta) \models \Phi'(E = \{f_1, ..., f_m, d_1, ..., d_n\})$ because $[\Phi \wedge \Delta \to \Phi'](m+n)$ is valid. Finally, we see:

$$t' \models (s \wedge \delta) \models \Phi'(E = \{f_1, ..., f_m, d_1, ..., d_n\}) \models \phi'$$

□

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