The M-N Theorem

Ian Dardik

February 23, 2022

1 Introduction

I begin with some preliminaries before introducing the M-N Theorem.

2 Preliminaries

Throughout this note we will consider a transition system $T = (I, \Delta)$ parameterized by a single sort P with identical elements (i.e. each element is interchangeable for another). Δ is the transition relation for T and we stipulate that it is in Prenex Normal Form (PNF). Φ is an inductive invariant candidate that is also in PNF, and our goal is to determine whether or not Φ is an inductive invariant for T.

Because Φ and Δ are in PNF, will also can refer directly to the matrices of these formulas as ϕ and δ respectively; i.e. ϕ and δ are propositional logic formulas parameterized by the variables that are quantified over in Φ and Δ respectively.

Because each element of P is interchangeable for another, we assume, without loss of generality, that $P = \{1, ..., |P|\}$. In other words, for two sorts P and Q, $|P| < |Q| \leftrightarrow P \subset Q$.

Another detail on the assumption that P's elements are identical: more precisely, let α be a FOL formula parameterized by the variables in sort P (possibly with primes), and let $g : P \to P$ be injective. Then:

$$\alpha \leftrightarrow \alpha[P \mapsto g(P)]$$

3 Finitely Instantiated Properties (FIPs)

In this section we introduce the FIP, a key tool for proving the M-N Theorem. We prove two basic lemmas about FIPs that will come in handy later.

Definition 1. *Let Φ and Δ be of two PNF formulas and let ϕ and δ be their respective matrices. Assume that Φ quantifies over $m \in \mathbb{N}$ variables while Δ quantifies over $n \in \mathbb{N}$ variables. Then a Finitely Instantiated Property (FIP) of $[\Phi \wedge \Delta](|P|)$ is a formula $(\phi \wedge \delta)[v_i \mapsto j]$, where each free variable v_i has been substituted for a concrete element $j \in P$.*

Remark 1:
We will often refer to $\phi \wedge \delta$ without the substitution syntax for brevity. In these cases, we will explicitly refer to $\phi \wedge \delta$ as a FIP, and not as a matrix.

Example 1:
Let $\Phi = \forall p, q \in P, \phi(p, q)$ and $\Delta = \exists p \in P, \delta(p)$. Then $\phi(1, 3) \wedge \delta(2)$ and $\phi(1, 1) \wedge \delta(1)$ are both FIPs of $[\Phi \wedge \Delta](3)$ (i.e. for the case when $|P| = 3$).

Definition 2. *Two FIPs $\phi_1 \wedge \delta_1$ and $\phi_2 \wedge \delta_2$ are equivalent iff $\phi_1 \wedge \delta_1$ is a permutation of $\phi_2 \wedge \delta_2$.*

Remark 2:
Let $\phi_1 \wedge \delta_1$ and $\phi_2 \wedge \delta_2$ both be FIPs for $\Phi \wedge \Delta$. If $\phi_1 \wedge \delta_1 \equiv \phi_2 \wedge \delta_2$ then $\phi_1 \equiv \phi_2$. This is because we syntactically separate the ϕ_i's and δ_i's to correspond to Φ and Δ respectively.

Remark 3:
If $\phi_1 \equiv \phi_2$, then it must be the case that $\phi_1' \equiv \phi_2'$ because priming is simply a syntactic transformation. TODO: we should probably include a proof for this.

Example 2:
Let $F_1 = \phi_1(1,2) \wedge \delta(1)$, $F_2 = \phi_2(2,3) \wedge \delta(2)$ and $F_3 = \phi(2,2) \wedge \delta(2)$ be FIPs of $[\Phi \wedge \Delta](3)$. Then $F_1 \equiv F_2$ because $F_1\ (1\ 2\ 3) = F_2$ (using cycle notation). However F_3 is a permutation of neither F_1 nor F_2 and hence is not equivalent to either.

The notion of equivalency is important because it partitions a formula $\Phi \wedge \Delta$ into distinct classes of FIPs. In the example above, F_1 and F_2 describe the same class of properties/actions because each element of P is interchangeable for one another. This leads us to the following lemma that is rather intuitive:

Lemma 1. *Let $\phi_1 \wedge \delta_1$ and $\phi_2 \wedge \delta_2$ both be FIPs for $\Phi \wedge \Delta$. Suppose that $\phi_1 \wedge \delta_1 \equiv \phi_2 \wedge \delta_2$. Then:*

$$(\phi_1 \wedge \delta_1) \leftrightarrow (\phi_2 \wedge \delta_2)$$

Proof. Because $\phi_1 \wedge \delta_1 \equiv \phi_2 \wedge \delta_2$, there exists a cycle C such that $(\phi_1 \wedge \delta_1)\ C = \phi_2 \wedge \delta_2$. However C is an injective map, and hence:

$$\phi_1 \wedge \delta_1 \leftrightarrow (\phi_1 \wedge \delta_1)[P \mapsto C(P)] = \phi_2 \wedge \delta_2$$

□

We next introduce the FIPS operator:

Definition 3. *Let Φ and Δ be PNF properties with respective matrices ϕ and δ. Suppose that Φ quantifies over $m \in \mathbb{N}$ variables while Δ quantifies over $n \in \mathbb{N}$ variables. Then:*

$$\mathit{FIPS}(\Phi \wedge \Delta, |P|) := \{\phi(v_1, ..., v_m) \wedge \delta(w_1, ..., w_n) | v_1, ..., v_m, w_1, ..., w_n \in P\}$$

The FIPS operator simply contains every possible FIP for a given formula $\Phi \wedge \Delta$. Next, we prove this intuitive result:

Lemma 2. *$\mathit{FIPS}(\Phi \wedge \Delta, |P|) \subseteq \mathit{FIPS}(\Phi \wedge \Delta, |Q|) \leftrightarrow |P| \leq |Q|$*

Proof. Recall that this note we assume $|P| \leq |Q| \leftrightarrow P \subseteq Q$. We begin by showing that $|P| \leq |Q| \rightarrow$ FIPS$(\Phi \wedge \Delta, |P|) \subseteq$ FIPS$(\Phi \wedge \Delta, |Q|)$:

$$\begin{aligned}
\text{FIPS}(\Phi \wedge \Delta, |P|) =& \{\phi(v_1, ..., v_m) \wedge \delta(w_1, ..., w_n) | v_1, ..., v_m, w_1, ..., w_n \in P\} \\
\subseteq& \{\phi(v_1, ..., v_m) \wedge \delta(w_1, ..., w_n) | v_1, ..., v_m, w_1, ..., w_n \in Q\} \\
=& \text{FIPS}(\Phi \wedge \Delta, |Q|)
\end{aligned}$$

Where the subset step follows from the fact that $P \subseteq Q$. Next we show that FIPS$(\Phi \wedge \Delta, |P|) \subseteq$ FIPS$(\Phi \wedge \Delta, |Q|) \rightarrow |P| \leq |Q|$. Suppose that FIPS$(\Phi \wedge \Delta, |P|) \subseteq$ FIPS$(\Phi \wedge \Delta, |Q|)$. Then we know that

$$\begin{aligned}
& \{\phi(v_1, ..., v_m) \wedge \delta(w_1, ..., w_n) | v_1, ..., v_m, w_1, ..., w_n \in P\} \\
\subseteq& \{\phi(v_1, ..., v_m) \wedge \delta(w_1, ..., w_n) | v_1, ..., v_m, w_1, ..., w_n \in Q\}
\end{aligned}$$

Which implies that $P \subseteq Q$, which in turn implies that $|P| \leq |Q|$.

□

4 Intuition

We will build intuition by proving the M-N Theorem for small examples. Coming soon.

5 M-N Theorem

Lemma 3. *Let Φ and Δ be formulas in PNF, where Φ quantifies over $m \in \mathbb{N}$ variables and Δ quantifies over $n \in \mathbb{N}$ variables. Then every FIP of $\Delta \wedge \Phi$ that appears when $|P| > m + n$ has an equivalent FIP that appears when $|P| = m + n$.*

Proof. Let $|P| = m + n + z$ where $z \in \mathbb{Z}_{>0}$. Then, because ϕ and δ are parameterized by exactly $m + n$ variables, there must be at least z unused variables. Let $P = \{v_i\}_{i=1}^{m+n+z}$ where each v_i is a variable, let $u \leq m + n$ be the *number* of variables that are used in $\phi \wedge \delta$, and finally let $\{v_{i_k}\}_{k=1}^{u}$ be the *set* of variables that are used. Consider the permuation using the following cycle notation: $C = (v_{i_1} v_1)...(v_{i_u} v_u)$. Notice that $(\phi \wedge \delta)\ C$ only uses variables $v_1...v_u$. Since $u \leq m+n$, it must be the case that $(\phi \wedge \delta)\ C$ is a FIP of $\Phi \wedge \Delta$ when $|P| = m + n$. $\square$

Theorem 1. *Let Φ and Δ be formulas in PNF, where Φ quantifies over $m \in \mathbb{N}$ variables and Δ quantifies over $n \in \mathbb{N}$ variables. Then Φ is an inductive invariant for $T(P)$ iff it is an inductive invariant for the finite instantiation $T(m + n)$.*

Proof. It is clear that if Φ is an inductive invariant, then it must be an inductive invariant for $T(m+n)$. We prove the opposite direction in the remainder of the proof.

In the case when the finite instantiation is less than $m + n$, the theorem follows by Lemma 2. We will focus on the case when the finite instantiation is larger than $m + n$ for the remainder of the proof.

Suppose that $\Phi(m + n) \wedge \Delta(m + n) \rightarrow \Phi(m + n)'$. Let $k > m + n$, then we must show that $\Phi(k) \wedge \Delta(k) \rightarrow \Phi(k)'$. Consider an arbitrary FIP $\phi \wedge \delta$ of $\Phi(k) \wedge \Delta(k)$. By Lemma 3, there exists a FIP $\phi_2 \wedge \delta_2$ of $\Phi(m + n) \wedge \Delta(m + n)$ such that $\phi_2 \wedge \delta_2 \equiv \phi \wedge \delta$. Now $\phi_2 \wedge \delta_2$ holds by Lemma 1, which implies ϕ_2'. By Remark 2, $\phi \equiv \phi_2$, and by Remark 3, $\phi' \equiv \phi_2'$. Finally, by Lemma 1, we can conclude that ϕ' holds. $\square$