The M-N Theorem

Ian Dardik

February 22, 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.

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 $\Phi \wedge \Delta$ is a formula $(\phi \wedge \delta)[v_i \mapsto j]$, where each free variable v_i has been substituted for a concrete element $j \in P$.*

Example:
Let $\Phi = \forall p, q \in P, \phi(p, q)$ and $\Delta = \exists p \in P, \delta(p)$. Then if $P = \{1, 2, 3\}$ is a finite instantiation of T, the formulas $\phi(1, 3) \wedge \delta(2)$ and $\phi(1, 1) \wedge \delta(1)$ are both FIPs of $\Phi \wedge \Delta$.

Definition 2. *Two FIPs $F_1 = \phi_1 \wedge \delta_1$ and $F_2 = \phi_2 \wedge \delta_2$ are equivalent iff F_1 is a permutation of F_2.*

Example:
Let $P = \{1, 2, 3\}$, $F_1 = \phi_1(1, 2) \wedge \delta(1)$, $F_2 = \phi_2(2, 3) \wedge \delta(2)$ and $F_3 = \phi(2, 2) \wedge \delta(2)$. 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 both.

The notion of equivalency is important because it partitions a FIP into distinct classes of action types. In the example above, F_1 and F_2 describe the same class of property and action 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 $\phi_2 \wedge \delta_2$ be FIPs for $\Phi_1 \wedge \Delta_1$ and $\Phi_2 \wedge \Delta_2$ respectively. Suppose that $\phi_1 \wedge \delta_1 \equiv \phi_2 \wedge \delta_2$, i.e. there exists a cycle C such that $(\phi_1 \wedge \delta_1)\ C = \phi_2 \wedge \delta_2$. Then*

$$((\phi_1 \wedge \delta_1)\ C \rightarrow \phi_1') \leftrightarrow (\phi_2 \wedge \delta_2 \rightarrow \phi_2')$$

Proof. This result follows immediately from the fact that each element of P is interchangeable for one another. □

3 Intuition

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

4 M-N Theorem

Lemma 2. *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 any FIP of $\Delta \wedge \Phi$ that appears when $|P| > m + n$ also 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 (very similar to the Pigeonhole Principle). 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: $C = (v_{i_1} v_1)...(v_{i_u} v_u)$. It is clear that $(\phi \wedge \delta)\ C \equiv (\phi \wedge \delta)$, but 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 $|P| = m + n$. □

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.

We will skip the case when the finite instantiation is less than $m+n$ and focus when it is larger for now.

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 the FIP when $|P| = k$: $\phi(1...m) \wedge \delta(1...n)$. By Lemma 2, we know that this FIP exists in $T(m + n)$, and hence we have a cycle R and a permutation $(\phi(1...m) \wedge \delta(1...n)\ R)$ that only contains the variables $v_1...v_{m+n}$. By Lemma 1, $(\phi(1...m) \wedge \delta(1...n)\ R) \rightarrow (\phi(1...m)'\ R)$, which is equivalent to $\phi(1...m)'$ by definition. □