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 implictly assume that $T = (I, \Delta)$ represents a transition system with one parameter P. The parameter P is a sort with identical elements (i.e. completely interchangable). We will often use Φ and Δ to refer to formulas in Prenex Normal Form (PNF), where Φ is generally a property and Δ is the transition relation. We will also refer 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 the matries of two PNF formulas, where ϕ is parameterized over $m \in \mathbb{N}$ variables and δ is parameterized over $n \in \mathbb{N}$ variables. A Finitely Instantiated Property (FIP) of $\phi \wedge \delta$ is a formula $(\phi \wedge \delta)[v_i \mapsto j]$, i.e. 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, then $\phi(1, 3) \wedge \delta(2)$ is a FIP as well as $\phi(1, 1) \wedge \delta(1)$.

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

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

3 M-N Theorem

Lemma 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 any FIP of $T(P)$ 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 $P = \{v_i\}_{i=1}^{i=m+n+z}$, let $u \leq m + n$ be the *number* of variables that are used, and finally let $\{v_{i_k}\}_{k=1}^{k=u}$ 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 $(\phi \wedge \delta)\ C = (\phi \wedge \delta)$, but notice that $(\phi \wedge \delta)\ C$ only uses variables $1...u$. Since $u \leq m + n$, it must be the case that $(\phi \wedge \delta)\ C$ is a FIP of T 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. 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 1, 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 $1...(m+n)$. Thus $(\phi(1...m) \wedge \delta(1...n)\ R) \rightarrow (\phi(1...m)'\ R)$, which is equal to $\phi(1...m)'$ by definition. $\square$