

The M-N Theorem

Ian Dardik

February 24, 2022

TODOS

1. Check cycle / cycle notation to make sure I'm saying it correctly.
2. Make sure the proof for the M-N theorem on the last few lines is clearer.
3. The proofs / language for the first 3 lemmas needs to be cleaned up.
4. Pin down Assumption 1.
5. Clean up preliminaries.
6. Write the intuition section.

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 $P = \{1, \dots, |P|\}$. In other words, for two sorts P and Q , $|P| < |Q| \leftrightarrow P \subset Q$.

Assumption 1. Another detail on the assumption that P 's elements are identical: more precisely, let ϕ be the matrix of a PNF property we care about (possibly with primes), let δ be the matrix of the transition relation, and let $g : P \rightarrow P$ be injective. Then:

$$\phi \wedge \delta \leftrightarrow (\phi \wedge \delta)[P \mapsto g(P)]$$

TODO: this needs to be introduced after the FIPs section because $\phi \wedge \delta$ should be a FIP (not matrices).

Assumption 2. Let P be a sort, then $|P| \leq |Q| \leftrightarrow P \subseteq Q$.

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.

3.1 FIP Basics

Definition 1 (FIP). 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 $(\phi \wedge \delta)[v_i \mapsto e_i]$, where each free variable v_i has been substituted for a concrete element $e_i \in P$.

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 $|P| = 3$).

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.

Definition 2 (Equivalent). Let $\phi_1 \wedge \delta_1$ and $\phi_2 \wedge \delta_2$ be FIPs, then $\phi_1 \wedge \delta_1 \equiv \phi_2 \wedge \delta_2$ iff $\phi_1 \wedge \delta_1$ is a permutation of $\phi_2 \wedge \delta_2$. In this case, $\phi_1 \wedge \delta_1$ and $\phi_2 \wedge \delta_2$ are said to be *equivalent*.

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.

Remark 2. FIP equivalency is commutative because permutations are commutative.

Remark 3. We specifically write a FIP of $[\Phi \wedge \Delta](|P|)$ as “ $\phi \wedge \delta$ ” to show the syntactic correspondence of ϕ to Φ and δ to Δ . In other words, it is always the case that $\phi = \text{RemoveMatrix}(\Phi)[v_i \mapsto e_i]$ and $\delta = \text{RemoveMatrix}(\Delta)[v_i \mapsto e_i]$.

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. We now present several basic lemmas about FIPs.

Lemma 1. Let $\phi_1 \wedge \delta_1$ and $\phi_2 \wedge \delta_2$ both be FIPs of $[\Phi \wedge \Delta](|P|)$. Then:

$$((\phi_1 \wedge \delta_1) \equiv (\phi_2 \wedge \delta_2)) \rightarrow ((\phi_1 \equiv \phi_2) \wedge (\delta_1 \equiv \delta_2))$$

Proof. Suppose $(\phi_1 \wedge \delta_1) \equiv (\phi_2 \wedge \delta_2)$. Then there exists a cycle C such that $(\phi_1 \wedge \delta_1) C = (\phi_2 \wedge \delta_2)$, and equivalently $(\phi_1 C) \wedge (\delta_1 C) = (\phi_2 \wedge \delta_2)$. From Remark 3, we see that ϕ_1 and ϕ_2 are identical up to a finite instantiation, and hence $\phi_1 C = \phi_2$; a similar argument shows that $\delta_1 C = \delta_2$. \square

Lemma 2. Let ϕ_1 and ϕ_2 be quantifier-free properties parameterized by the sort P . Then:

$$(\phi_1 \equiv \phi_2) \leftrightarrow (\phi'_1 \equiv \phi'_2)$$

Proof. Suppose that $\phi_1 \equiv \phi_2$. Then there exists a cycle C such that $\phi_1 C = \phi_2$. Notice that the prime operator only affects state variables, and not parameters or their elements. Thus it is the case that $(\phi_1 C)' = (\phi'_1) C$. We now see:

$$\phi'_2 = (\phi_1 C)' = (\phi'_1) C$$

Showing that $\phi'_1 \equiv \phi'_2$ by definition. We omit the proof in the other direction since it is nearly identical. \square

Lemma 3. 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 by Assumption 1:

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

\square

3.2 The FIPS Operator

In this section we 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:

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

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

Lemma 4. $\text{FIPS}(\Phi \wedge \Delta, |P|) \subseteq \text{FIPS}(\Phi \wedge \Delta, |Q|) \leftrightarrow |P| \leq |Q|$

Proof. We begin by showing that $|P| \leq |Q| \rightarrow \text{FIPS}(\Phi \wedge \Delta, |P|) \subseteq \text{FIPS}(\Phi \wedge \Delta, |Q|)$. Suppose $|P| \leq |Q|$, and then it follows that $P \subseteq Q$ by Assumption 2. Then:

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

Next we show that $\text{FIPS}(\Phi \wedge \Delta, |P|) \subseteq \text{FIPS}(\Phi \wedge \Delta, |Q|) \rightarrow |P| \leq |Q|$. Suppose that $\text{FIPS}(\Phi \wedge \Delta, |P|) \subseteq \text{FIPS}(\Phi \wedge \Delta, |Q|)$. Then we know that

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

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 5 (FIP Saturation). 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 $[\Delta \wedge \Phi](k)$, for $k > m + n$, has an equivalent FIP in $[\Delta \wedge \Phi](m + n)$.

Proof. Let $k = |P| = m + n + z$ where $z \in \mathbb{Z}_{>0}$ (recall that $P = \{1, \dots, k\}$). Let $\phi \wedge \delta$ be an arbitrary FIP of $[\Phi \wedge \Delta](k)$. Then, because $[\Phi \wedge \Delta](k)$ quantifies over exactly $m + n$ variables, there must be at least z elements in P that do not appear in $\phi \wedge \delta$. Let $u \leq m + n$ be the number of elements of P that are used in $\phi \wedge \delta$, and let $\{e_i\}_{i=1}^u$ be the subset of elements that are used. Consider the permutation using the following cycle notation: $C = (e_1 \ 1) \dots (e_u \ u)$. Notice that $(\phi \wedge \delta) \circ C$ only uses elements $1 \dots u$. Since $u \leq m + n$, it must be the case that $(\phi \wedge \delta) \circ C$ is a FIP of $[\Phi \wedge \Delta](m + n)$. □

Theorem 1 (M-N). 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 4. 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 $[\Phi \wedge \Delta](k)$. By Lemma 5, there exists a FIP $\phi_2 \wedge \delta_2$ of $[\Phi \wedge \Delta](m+n)$ such that $\phi_2 \wedge \delta_2 \equiv \phi \wedge \delta$. Now $\phi_2 \wedge \delta_2$ holds by Lemma 3, which implies ϕ'_2 . By Lemma 1, $\phi \equiv \phi_2$, and by Lemma 2, $\phi' \equiv \phi'_2$. Finally, by Lemma 3, we can conclude that ϕ' holds. \square

6 Case Studies