# Basic Theorems about Predicate Transformers

M is the set of all possible machine states, assumed countable. Small letters from the begining of the alphabet will be used to represent subsets of M ( $a,b\in 2^M$ ) and small letters from the middle of the alphabet to represent individual machine states ( $m,n\in M$ ).

Definition

For some family of sets F we define

$$\Pi F = \phi \quad \text{if } F = \phi$$
$$= \cap \{f \mid f\in F\} \quad \text{otherwise}$$

Definition

A function $S : 2^M \to 2^M$ is a predicate transformer. S is multiplicative if and only if

$$S(\Pi\{b_i \mid i\in\Gamma\}) = \Pi\{S(b_i) \mid i\in\Gamma\}$$

where $b_i \in 2^M$ $\forall i\in\Gamma$, an arbitrary index set.

In all that follows, S is a multiplicative predicate transformer.

Theorem 1 (Strictness)

$$S(\phi) = \phi$$

Proof

$S(\phi) = S(\Pi\{b_i \mid i\in\phi\})$    def of $\Pi$

$= \Pi\{S(b_i) \mid i\in\phi\}$    multiplicative

$= \phi$    def of $\Pi$

Theorem 2 (Monotonicity)

$$a \subseteq b \Leftrightarrow S(a) \subseteq S(b)$$

Proof

$$\begin{aligned} a \subseteq b &\Leftrightarrow a = a \cap b \\ &\Leftrightarrow S(a) = S(a \cap b) \\ &\Leftrightarrow S(a) = S(a) \cap S(b) && \text{multiplicative} \\ &\Leftrightarrow S(a) \subseteq S(b) \end{aligned}$$

Definition

$S': M \to 2^M$ is given by

$$S'(m) = \Pi \{ b \mid m \in S(b) \}$$

Lemma 1

$$(\exists b.\ m \in S(b)) \Rightarrow m \in S(S'(m))$$

Proof

$$\begin{aligned} S(S'(m)) &= S(\Pi \{ b \mid m \in S(b) \}) && \text{def of } S' \\ &= \Pi \{ S(b) \mid m \in S(b) \} && \text{multiplicative} \\ &= \cap \{ S(b) \mid m \in S(b) \} && \text{anticedent and def of } \Pi \\ &\supseteq \cap \{ a \mid m \in a \} && \text{substitution} \end{aligned}$$

Clearly $m \in \cap\{ a \mid m \in a \}$, so $m \in S(S'(m))$.

Theorem 3

$$m \in S(b) \Leftrightarrow S'(m) \subseteq b \wedge S'(m) \neq \phi$$

Proof $\Rightarrow$

$$\begin{aligned} (1) \quad m \in S(b) &\Rightarrow m \in S(S'(m)) && \text{Lemma 1} \\ &\Rightarrow S(S'(m)) \neq \phi \\ &\Rightarrow S'(m) \neq \phi && \text{Strictness} \end{aligned}$$

(2) let $n \in S'(m)$

| | |
|---|---|
| $\Leftrightarrow n \in \Pi\{ a \mid m \in S(a) \}$ | def of S' |
| $\Leftrightarrow n \in \cap\{ a \mid m \in S(a) \}$ | $\{ a \mid m \in S(a) \} \neq \phi$ |
| $\Leftrightarrow \forall a \, ( m \in S(a) \Rightarrow n \in a )$ | props of ∩ |
| $\Rightarrow ( m \in S(b) \Rightarrow n \in b )$ | props of ∀ |
| $\Rightarrow n \in b$ | $m \in S(b)$ |
| $\therefore \forall n \, (n \in S'(m) \Rightarrow n \in b )$ | |
| $\therefore S'(m) \subseteq b$ | def of ⊆ |

<u>Proof ⇐</u>

| | |
|---|---|
| $S'(m) \neq \phi \Rightarrow \Pi\{ b \mid m \in S(b) \} \neq \phi$ | def of S' |
| $\Rightarrow \{ b \mid m \in S(b) \} \neq \phi$ | def of Π |
| $\Rightarrow \exists b.\ m \in S(b)$ | |
| $\Rightarrow m \in S(S'(m))$ | Lemma 1 |
| $S'(m) \subseteq b \Rightarrow S(S'(m)) \subseteq S(b)$ | monotonicity |
| $\therefore \ m \in S(b)$ | |

<u>Corollary</u>

$$m \in S(S'(m)) \Leftrightarrow S'(m) \neq \phi$$

<u>Proof</u>

Put $b = S'(m)$ in Theorem.

Now $m \in S(S'(m)) \Leftrightarrow S'(m) \subseteq S'(m) \wedge S'(m) \neq \phi$

$\therefore$ $m \in S(S'(m)) \Leftrightarrow S'(m) \neq \phi$

<u>Definitions</u>

Define a relation $p \subset M \times M$ corresponding to S

$$p = \{ (m,n) \mid n \in S'(m) \}$$

Define the binary operators <u>a</u>, <u>e</u>: $[2^{M \times M} \times 2^M] \rightarrow 2^M$

$$p \ \underline{a} \ b = \{ m \in M \mid \exists n.\ (m,n) \in p \wedge n \in b \}$$
$$= \{ m \in M \mid \exists n.\ n \in S'(m) \wedge n \in b \}$$
$$= \{ m \in M \mid S'(m) \cap b \neq \phi \}$$

and

$$p \;\underline{e}\; b = \sim(p \;\underline{a}\; \sim b)$$
$$= \{\, m \in M \mid S'(m) \cap \sim b = \phi \,\}$$
$$= \{\, m \in M \mid S'(m) \subseteq b \,\}$$

<u>Theorem 4</u>

$$S(b) = (p \;\underline{a}\; b) \cap (p \;\underline{e}\; b)$$

<u>Proof</u>

$$(p \;\underline{a}\; b) \cap (p \;\underline{e}\; b) = \{\, m \in M \mid S'(m) \cap b \neq \phi \wedge S'(m) \subseteq b \,\}$$
$$= \{\, m \in M \mid m \in S(b) \,\} \qquad \text{Theorem 3}$$
$$= S(b)$$

<u>Definition</u>

S is <u>continuous</u> if, given an ascending chain of $b_i \in 2^M$ (i.e., $\forall i \in N,\ b_i \subseteq b_{i+1}$)

$$S(\bigcup_{i \in N} b_i) \subseteq \bigcup_{i \in N} S(b_i)$$

<u>Theorem 5</u>

If S is continuous, $S'(m)$ is a finite set $\forall m \in M$.

<u>Proof</u>

Either (i) $\nexists b.\ m \in S(b)$

or (ii) $\exists b.\ m \in S(b)$

If (i), $S'(m) = \phi$ by definition

$\therefore$ $S'(m)$ is finite

If (ii), let $b_i$ be an ascending chain of finite sets such that

$$\bigcup_{i \in N} b_i = b$$

(This can be done because M countable $\Rightarrow$ b countable.)

Then $m \in S(b) \Leftrightarrow m \in S(\bigcup_{i \in N} b_i)$

$\Leftrightarrow m \in \bigcup_{i \in N} S(b_i)$ — continuity of S

$\Leftrightarrow \exists i \in N.\ m \in S(b_i)$ — def of $\cup$

$\Rightarrow \exists i \in N.\ S'(m) \subseteq b_i$ — Theorem 3

but $b_i$ is finite, so S'(m) is also finite.

Theorem 6

If S'(m) is finite $\forall m \in M$, then S is continuous.

Proof

$m \in S(\bigcup_{i \in N} b_i) \Rightarrow S'(m) \subseteq \bigcup_{i \in N} b_i \wedge S'(m) \neq \phi$ — Theorem 3

$\Rightarrow \exists i \in N.\ (S'(m) \subseteq b_i) \wedge S'(m) \neq \phi$ — S'(m) finite and $b_i$ is an ascending chain

$\Rightarrow S(S'(m)) \subseteq S(b_i) \wedge S'(m) \neq \phi$ — monotonicity

$\Rightarrow S(S'(m)) \subseteq S(b_i) \wedge m \in S(S'(m))$ — Corollary to Theorem 3

$\Rightarrow m \in S(b_i)$

$\Rightarrow m \in \bigcup_{i \in N} S(b_i)$ — props of $\cup$

Since this holds $\forall m \in M$,

$$S(\bigcup_{i \in N} b_i) \subseteq \bigcup_{i \in N} S(b_i)$$

So S is continuous.