A Characterization of Weakest Preconditions*

MITCHELL WAND

Computer Science Department, Indiana University, Bloomington, Indiana 47401

Received June 11, 1976; revised November 24, 1976

If $S$ is a set of states, a function $f: 2^S \rightarrow 2^S$ is the "weakest precondition" map of some mechanism of bounded nondeterminacy if and only if it is strict, preserves binary intersections, and is continuous over directed sets. If $S$ is countable, the continuity condition may be weakened to continuity over $\omega$-chains.

1. Introduction

In [1], Dijkstra introduces the notions of "weakest precondition" and "mechanism of bounded nondeterminacy." In this note, we will give necessary and sufficient conditions for a function $2^S \rightarrow 2^S$ (a "predicate transformer") to be a weakest precondition map.

2. Definitions

The following definitions are taken, often inter alia, from [1]. Throughout, it is assumed that $S$ is an arbitrary set, called the state space.

Definition. A mechanism of bounded nondeterminacy (or just mechanism) on $S$ is a function $m: S \rightarrow 2^S$ such that for every $s \in S$, $m(s)$ is finite.

The intention is that an implementation of $m$, started at $s$, must halt at some $s' \in m(s)$. If it may fail to halt when started at $s$, then $m(s) = \emptyset$. (This is at the heart of the Goldbach's conjecture example [1, p. 208].)

Definition. If $m$ is a mechanism on $S$, the weakest precondition map generated by $m$ is the function $wp_m : 2^S \rightarrow 2^S$ defined as

$$wp_m(A) = \{ x \in S \mid m(x) \neq \emptyset \& m(x) \subseteq A \}. $$

Dijkstra uses the notation $wp(m, A)$. Note that for any mechanism, if $m(x) \neq \emptyset$, then $x \in wp_m(m(x))$.

Let $\omega$ denote the nonnegative integers $0, 1, 2, \ldots$.

* Research reported herein was supported in part by the National Science Foundation under grant number DCR75-06678.
**DEFINITION.** If $P$ is a complete lattice, then $D \subseteq P$ is *directed* iff $D$ is nonempty and every pair of elements of $D$ has an upper bound in $D$. An *ω-chain* in $P$ is a set $D \subseteq P$ equipped with an onto function $h: \omega \to D$ such that $i \leq j$ implies $h(i) \leq h(j)$. If $f: P \to P$, we say $f$ is *continuous* at $D$ iff $\bigcup\{f(A) \mid A \in D\} = f(\bigcup\{A \mid A \in D\})$.

Every ω-chain is clearly directed.

**DEFINITION.** Let $S$ be a set, and let $2^S$ denote the set of all subsets of $S$, partially ordered by inclusion. Let $f$ be a function $2^S \to 2^S$. Then

(i) $f$ is *strict* iff $f(\emptyset) = \emptyset$,

(ii) $f$ is *Δ-continuous* iff it is continuous at every directed set,

(iii) $f$ is *ω-continuous* iff it is continuous at every ω-chain,

(iv) $f$ is *monotone* iff $A \subseteq B$ implies $f(A) \subseteq f(B)$,

(v) $f$ preserves binary intersection iff $f(A \cap B) = f(A) \cap f(B)$.

Note that Δ-continuity implies ω-continuity implies monotonicity.

Dijkstra proposes that predicate transformers should be strict ("excluded miracle"), preserve binary intersections, and be ω-continuous. He credits J. Reynolds for the ω-continuity condition (which implies monotonicity). Our main result is that $f: 2^S \to 2^S$ is of the form $wp_m$ iff it is strict, preserves binary intersections, and is Δ-continuous.

The following lemma is due to Barry Rosen.

**LEMMA 1.** Let $S$ be countable and let $f: 2^S \to 2^S$ be ω-continuous. Then $f$ is Δ-continuous.

**Proof.** Let $D \subseteq 2^S$ be directed; we wish to show that $f(\bigcup\{x \mid x \in D\}) = \bigcup\{f(x) \mid x \in D\}$. It suffices to show that $f(\bigcup\{x \mid x \in D\}) \subseteq \bigcup\{f(x) \mid x \in D\}$, since the opposite inclusion follows from monotonicity.

Let $D' = \{x' \mid x' \text{ is finite and } x' \subseteq x \text{ for some } x \in D\}$. $D'$ is directed, countable, and has the same sup as $D$. Then by [2, Theorem 1], there is a sequence $D_0, D_1, D_2, \ldots$ of finite directed subsets of $2^S$ such that

(i) $D_i \subseteq D_{i+1}$ for each $i \in \omega$,

(ii) $D' = \bigcup\{D_i \mid i \in \omega\}$,

(iii) $\bigcup\{x \mid x \in D'\} = \bigcup\{\bigcup\{x \mid x \in D_i\} \mid i \in \omega\}$.

By the ω-continuity of $f$, $f(\bigcup\{x \mid x \in D'\}) = \bigcup\{f(x) \mid x \in D_i\}$, and so $f(\bigcup\{x \mid x \in D'\}) = \bigcup\{f(x) \mid x \in D'\}$ since $f$ is continuous at each finite $D_i$. Hence by monotonicity $f(\bigcup\{x \mid x \in D'\}) = f(\bigcup\{x \mid x \in D'\}) = f(\bigcup\{f(x) \mid x \in D'\})$.

3. RESULTS

**PROPOSITION 1.** For every mechanism $m$, $wp_m$ is strict, preserves binary intersections, and is Δ-continuous.
Proof. The only nontrivial step is $\Delta$-continuity. Let $D \subseteq 2^S$ be a directed set. We must show

$$\left\{ x \mid m(x) \neq \emptyset \& m(x) \subseteq \bigcup_{A \in D} A \right\} = \bigcup_{A \in D} \{ x \mid m(x) \neq \emptyset \& m(x) \subseteq A \}.$$

If, for some $A \in D$, $m(x) \neq \emptyset$ and $m(x) \subseteq A$, then $m(x) \subseteq \bigcup_{A \in D} A$, so the right-hand side is trivially a subset of the left-hand side. To get the other inclusion, assume $m(x) \neq \emptyset$ and $m(x) \subseteq \bigcup_{A \in D} A$. Since $m(x)$ is finite, let $m(x) = \{s_1, \ldots, s_n\}$. Then there must be $A_1, \ldots, A_n \in D$ such that $s_i \in A_i$. But since $D$ is directed, there must be an $A \in D$ which is an upper bound for $A_1, \ldots, A_n$. So $m(x) \subseteq A$.

**Proposition 2.** If $f : 2^S \to 2^S$ and $f = wp_m$, then $x \in f(S)$ iff $m(x) \neq \emptyset$.

**Proof.** $f(S) = wp_m(S) = \{ x \mid m(x) \neq \emptyset \& m(x) \subseteq S \} = \{ x \mid m(x) \neq \emptyset \}.$

**Proposition 3.** If $f : 2^S \to 2^S$ and $f = wp_m$, then $m$ must be defined by

$$m(x) = \emptyset \quad \text{if} \quad x \not\in f(S),$$

$$m(x) = \bigcap \{ A \mid x \in f(A) \} \quad \text{if} \quad x \in f(S).$$

**Proof.** If $x \not\in f(S)$, then $m(x) = \emptyset$ by Proposition 2. So assume $x \in f(S)$, and hence $m(x) \neq \emptyset$. Let $X = \bigcap \{ A \mid x \in f(A) \}$. If $x \not\in f(A)$, then $m(x) \subseteq A$. Hence $x \in wp_m(m(x)) = f(m(x))$, so $X \subseteq m(x)$. Hence $m(x) = X$.

**Corollary.** If $wp_m = wp_n$, then $m = n$.

**Proposition 4.** Let $f : 2^S \to 2^S$ be $\Delta$-continuous and preserve binary intersection. Let $x \in f(S)$ and let $X = \bigcap \{ A \mid x \in f(A) \}$. Then $x \in f(X)$.

**Proof.** Let $X = \{(S - A) \cup X \mid x \in f(A) \}$. If $x \in f(A_1)$ and $x \in f(A_2)$, then $(S - (A_1 \cap A_2)) \cup X$ is an upper bound in $D$ for $(S - A_1) \cup X$ and $(S - A_2) \cup X$, so $D$ is directed. We claim that $\bigcup \{ B \mid B \in D \} = S$. If $s \in X$, then trivially $s \in \bigcup \{ B \mid B \in D \} \subseteq \bigcup \{ B \mid B \in D \}$. If $s \in S - X$, then there must be some $A$ such that $x \not\in f(A)$ but $s \not\in A$. Then $s \in (S - A) \cup X$. So indeed, $\bigcup \{ B \mid B \in D \} = S$. Since $D$ is a directed set whose lub is $S$, and $x \not\in f(S)$, then the $\Delta$-continuity of $f$, there must be some $B \in D$ such that $x \not\in f(B)$. Then $B = (S - A) \cup X$ for some $A$ such that $x \not\in f(A)$. Hence, $x \in f((S - A) \cap X) \cap f(A) = f((S - A) \cap X) \cap f(A) = f(X \cap A) = f(X)$.

**Proposition 5.** Let $f : 2^S \to 2^S$ be $\Delta$-continuous, strict, and preserve binary intersections. Then $f = wp_m$ for some mechanism $m$.

**Proof.** Let $m$ be as in Proposition 3. We must first show that $m(x)$ is finite. Assume for some $x$, $m(x)$ is infinite. Let $m(x) = \{x_1, x_2, \ldots\}$. Let $A_k = S - \{x_i \mid i \geq k\}$. Then for every $n$, $m(x) \subseteq A_n$. Now, $\bigcup_{k} A_k = S$ and $x \not\in f(S)$ by the construction of $m$, so $x \not\in f(A_n)$ for some $n$. Hence $m(x) \subseteq A_n$, a contradiction. So $m(x)$ is finite for each $x$. Hence $m$ is a mechanism.
Now we must show that $f = \wp_m$. We will show that for every $x$, $x \in f(A)$ iff $x \in \wp_m(A)$. If $x \notin f(S)$, then $m(x) = \emptyset$, so $x \notin \wp_m(A)$ for every $A$. If $x \in f(A)$ for any $A$, then $x \in f(S)$. So $x \notin f(A)$ for any $A$. Now we assume $x \in f(S)$. Let $X$ denote $\bigcap \{B \mid x \in f(B)\} = m(x)$. By Proposition 4, $x \in f(X)$. If $X = \emptyset$, then $f(X) = \emptyset$ by the strictness of $f$. So $X \neq \emptyset$. Now

$$x \in \wp_m(A) \quad \text{iff} \quad (m(x) \neq \emptyset) \& (m(x) \subseteq A),$$

$$\text{iff} \quad (X \neq \emptyset) \& (X \subseteq A),$$

$$\text{iff} \quad (X \subseteq A).$$

Thus, if $x \in \wp_m(A)$, then $X \subseteq A$; since $x \in f(X)$, by monotonicity it follows that $x \in f(A)$. Conversely, if $x \in f(A)$, then $X \subseteq A$ by the construction of $X$; hence $x \in \wp_m(A)$. ♦

From Propositions 1 and 5 we have

**Theorem 1.** Let $f : 2^S \to 2^S$. Then $f = \wp_m$ for some mechanism $m$ iff $f$ is strict, preserves binary intersections, and is $A$-continuous. ♦

By Lemma 1 we have

**Theorem 2.** Let $S$ be countable and $f : 2^S \to 2^S$. Then $f = \wp_m$ for some mechanism $m$ iff $f$ is strict, preserves binary intersections, and is $\omega$-continuous. ♦

It remains open whether the $A$-continuity condition can be weakened for uncountable $S$. However, since all reasonable (e.g., recursive) state sets are countable, Theorem 2 should suffice.

**Acknowledgment**

Barry Rosen pointed out Lemma 1, which replaced an earlier independent proof of Theorem 2.

**References**