数理解析研究所講究録
960巻 1996年 1-14

Complete Partial Orders and Fixpoints

Hans-Ulrich Bühler
Faculty of Applied Informatics and Mathematics
Fachhochschule Fulda
D-36039 Fulda, Germany

Abstract: The aim of this paper is to give an overview of a basic algebraic tool intensively used in describing the notational semantics of recursive programs. Specifically we'll present some elements on complete partial orders, continuous functions and fixpoints. Finally we'll give an example covering all necessary steps in proving the correctness of the computation by a recursive program. Our approch follows a classical line and the reader can find further details in [1], [2] and [3].

1 Preliminaries

In accordance with [3] a partial order set (poset) is a pair $M=(A;\leq)$ in which a binary relation $\leq$ on the set $A$ is reflexive, antisymmetric and transitive. There are countless examples of posets. Some of the simplest are:

EXAMPLE 1.1 Let $P(A)$ be the set of all subsets of a given set $A$ (including the empty set $\varnothing$ and $A$ itself) and $X \subseteq Y$ mean $X$ is a subset of $Y$. Then $(P(A);\subseteq)$ is a poset.

EXAMPLE 1.2 Let Z^+ be the set of positive integers and $n|m$ mean n divides m. Then $(Z^+;|)$ is a poset.

EXAMPLE 1.3 Let $A$ be a nonempty set and $\omega$ be an element that does not belong to $A$. Define a relation $\leq$ on $A_\omega = A \cup \{\omega\}$ by

$$a \leq b \text{ if and only if } a=\omega \; or \; a=b$$

then $(A_\omega;\leq)$ is a poset and is called the flat poset pertaining to $A$.

Let $S$ be a subset of $A$. An element $\perp_S \in S$ is the least element of $S$ if $\perp_S \leq a$ for all $a \in S$. The element $a' \in A$ is an upper bound of $S$, if $a \leq a'$ for all $a \in S$. The least upper bound of $S$, denoted by $lub\,S$ or $supS$, is the least element of all upper bounds of $S$.

The subset $S$ is called a chain in $A$ if $a \leq a'$ or $a' \leq a$ for any $a,a' \in S$.

A relation $f \subseteq A \times B$ with the property

$$\text{if } (a,b_1),(a,b_2) \in f \Rightarrow b_1 = b_2 \text{ for any } a \in A,\ b_1,b_2 \in B$$

is called a partial function from $A$ to $B$. If $dom(f) = A$ then $f$ is a (total) function.

By using the composition of functions the $n$th iterate f^n of $f: A \to A$ is defined by

$$f^{n+1} = f \circ f^n \text{ with } f^0 = \tau_A \text{ (identity function).}$$

Let $M = (A;\leq_A)$ and $M' = (B;\leq_B)$ be two posets. If the function $f: A \to B$ has the property $(\forall a_1,a_2 \in A)(a_1 \leq_A a_2 \Rightarrow f(a_1) \leq_B f(a_2))$ then $f$ is a monotonic function (homomorphism). The function $f$ preserves the order in M'.

If $f: A_1 \times \ldots \times A_n \to B$ be a function then any function $f_\omega: A_{1\omega} \times \ldots \times A_{n\omega} \to B_\omega$ with

$$f_{\omega|A_1 \times \ldots \times A_n} = f$$

is called ω – extension of $f$.

2 Complete Partial Orders

DEFINITION 2.1 A partial order $M = (A;\leq)$ is a complete partial order (cpo) if the two conditions hold:

(1) The set $M = (A;\leq)$ has a least element $\perp_M$.

(2) For every chain $K$ in $M$ the least upper bound $sup\,K$ exists.

EXAMPLE 2.1 Every poset with a least element and only finite chains is a cpo. So flat posets are cpo´s.

EXAMPLE 2.2 The set of the natural numbers with the common relation is a poset but not complete. The chain N has no supremum.

EXAMPLE 2.3 Let A and B are two sets and $(A \mapsto B)$ the set of all partial functions from A to B. With the relation

$$f \leq g \Leftrightarrow dom(f) \subseteq dom(g), f(x) = g(x), \forall x \in dom(f)$$

$((A \mapsto B); \leq)$ is a cpo.

This fact is easy to be shown: The empty set $\varnothing$ is the least element of $(A \mapsto B)$.

If $K = \{f_i | i \in I\}$ is a chain of partial functions then the function $f: A \mapsto B$ with $dom(f) = \bigcup_{i \in I} dom(f_i)$ and $f(x) = f_i(x)$ for all $x \in dom(f)$ where $x \in dom(f_i)$ is the supremum of K: $f = sup K$.

EXAMPLE 2.4 $(P(A); \subseteq)$ with the inclusion relation is a cpo.

More generally the following Theorem holds:

THEOREM 2.1 Let $M_i = (A_i; \leq_i)$, i=1,...,n, be cpo's. With the relation $\leq$ on $A_1 \times ... \times A_n$ defined by

$$(f_1, ..., f_n) \leq (g_1, ..., g_n) \Leftrightarrow f_i \leq_i g_i, \forall i = 1, ..., n$$

the cartesian product $M_1 \times ... \times M_n$ of this sets

$$(A_1 \times ... \times A_n; \leq)$$

is a cpo.

This theorem can also be extended to infinite cartesian products.

As a consequense the cartesian product of a flat cpo with itself is a cpo.

EXAMPLE 2.5 The set $(N_\omega \times ... \times N_\omega; \leq)$ is a cpo.

In order to show that the set of all functions equiped with a suitable relation built a cpo we need this technical lemma:

LEMMA 2.1 Let A be a set and $(B;\leq)$ a poset.
On the set $(A\to B)$ of all total functions from A to B we define a relation $\leq'$ by

$$f \leq' g \Leftrightarrow f(a)\leq g(a),\ \forall a\in A\ .$$

Then, the supremum *sup* S of a subset $S\subseteq(A\to B)$ exists if and only if the supremum of the sets $S(a)=\{f(a)|f\in S\}$ exists for every $a\in A$. If the function *sup* S exists, then

$$(sup\,S)(a)=sup\,S(a) \text{ for every } a\in A.$$

Proof Suppose the supremum $sup\,S$ exists and $a\in A$. We show that $(sup\,S)(a)$ is the least upper bound of $S(a)$. Indeed, $f\leq' sup\,S$ for any function $f\in S$, that is $f(x)\leq(sup\,S)(x),\forall x\in A$. Hence $f(a)\leq(sup\,S)(a)$ and so $(sup\,S)(a)$ is an upper bound of $S(a)$.

Let b be another upper bound of $S(a)$, that is $f(a)\leq b,\forall f\in S$, and let the function g defined by

$$g(x)=\begin{cases}(sup\,S)(x),\ x\neq a\\ \quad b,\ x=a\end{cases}.$$

Then $f\leq' g$ for every $f\in S$. Since $sup\,S$ is the least upper bound of S we have $sup\,S\leq' g$ and so $(sup\,S)(a)\leq g(a)=b$.

Analogous it can be shown that if $sup\,S(a)$ exists for arbitrary $a\in A$ then the function $sup\,S$ exists and $(sup\,S)(a)=sup\,S(a)$ for all $a\in A$. □

EXAMPLE 2.6 Let $K=\{f_i|i\geq 0\}$ be a set of functions $f_i{:}N_\omega\to N_\omega$, defined by

$$f_i(n)=\begin{cases}\omega,\text{ if n}=\omega\text{ or }n\in N,n\geq i\\ n!,\text{ if }n\in N,0\leq n\leq i-1\end{cases}.$$

By using the relation of Lemma 2.1 ($A = B = N_\omega$) we obtain the supremum of the chain K

$$(sup\,K)(n) = sup\,K(n) = \begin{cases} \omega, & \text{if } n = \omega \\ n!, & \text{if } n \in N \end{cases}.$$

Now we are able to show the completeness of the total functions with respect to the above relation.

THEOREM 2.2 Let A be a set and $(B;\leq)$ a cpo.

Then the set $((A \to B),\leq')$ is a cpo (with the relation $\leq'$ of Lemma 2.1).

Proof The function $\perp_{(A\to B)}: A \to B$ defined by $\perp_{(A\to B)}(a) = \perp_B$ for all $a \in A$ is the least element of $(A \to B)$: $\perp_{(A\to B)}(a) = \perp_B \leq f(a)$ for all $a \in A$ and every function $f: A \to B$. Consider a chain $S \subseteq (A \to B)$.

To show that the least upper bound of S exists, it is sufficient by Lemma 2.1 to prove that for every $a \in A$ the set $S(a)$ is a chain ($(B;\leq)$ is a cpo).

Let $b_1, b_2 \in S(a)$ then there are functions $f, g \in S$ with $b_1 = f(a)$ and $b_2 = g(a)$. It is $f \leq' g$ or $g \leq' f$ and hence $b_1 \leq b_2$ or $b_2 \leq b_1$ and $S(a)$ is a chain. □

EXAMPLE 2.7 The set $((N_\omega \to N_\omega),\leq')$ is a cpo (see Example 2.1 with $A = N$).

We have seen that the property ′completeness′ can carry over from $(B;\leq)$ to the set $((A \to B);\leq')$. This is not necessarily the case for a subset of a cpo: the subset does not necessarily have a least element and the supremum of every chain don′t must lie in the subset. So the following definition is justified.

DEFINITION 2.2 Let $M=(A;\leq)$ be a cpo and $B\subseteq A$. Then $M'=(B;\leq_{|B})$ is called a sub-cpo of *M*, if

(1) the poset M' is a cpo and

(2) $sup_{M'}K=sup_{M}K$ for all chains *K* in M'.

We mention that the second condition does not necessarily follow from the first. To demonstrate this we consider the cpo $M=(P(N);\subseteq)$ and the set $X=\{C|C\subseteq N,C\text{ finite}\}\cup\{\varnothing,N\}\subseteq P(N)$. It is easy to see that the subset $M'=(X;\subseteq_{X})$ is a cpo, but the chain

$$K=\{\{0\},\{0,2\},\{0,2,4\},\ldots\}$$

has in *M* the supremum $sup_{M}K=\{0,2,4,\ldots\}$ and in M' the supremum $sup_{M'}K=N$.
The second condition is not meet and M' isn't a sub-cpo of M.

THEOREM 2.3 Let $M=(A;\leq)$ be a cpo and *B* a subset of *A*. Then $M'=(B;\leq_{|B})$ is a sub-cpo of *M*, if and only if the two conditions hold:

(1) M' has a least element,

(2) $sup_{M}K$ lies in M' for every chain *K* in M'.

Proof Suppose M' is a sub-cpo of *M*. Then M' is a cpo and has a least element.
If K is a chain in M' then $sup_{M}K=sup_{M'}K$. This shows us that $sup_{M}K$ lies in *B* and $sup_{M'}K$ too.
Conversely, the conditions (1) and (2) leeds us to the fact that M' is a cpo. Moreover from (2) we have $sup_{M}K=sup_{M'}K$, since otherwise the supremum in M' woudn't be unique. □

EXAMPLE 2.8 Let $(A;\leq_{A})$ be a poset, $(B;\leq_{B})$ a cpo and $(A\xrightarrow[m]{}B)$ the set of all monotonic functions from A to B. Then $M'=((A\xrightarrow[m]{}B);\leq')$ with the above relation is a sub-cpo of the cpo $M=((A\rightarrow B);\leq')$.

3 Continuous Functions

To establish the existence of fixpoints we need continuous functions.
Similar to the case in analysis a function is continuous if it is compatible with the construction of least upper bounds.

DEFINITION 3.1 Let $M=(A;\leq_A)$ and $M'=(B;\leq_B)$ be cpo's. A function $f:A\rightarrow B$ is said to be continuous if for every chain K in M the supremum $sup_{M'}\,f(K)$ of the set $f(K)$ exists and $f(sup_M\,K)=sup_{M'}\,f(K)$.

We remark that the 'completeness' of M and M' don't ensures the existence of the supremum of the set *f(K)* because we don't know if *f(K)* is a chain. The formulation ' the supremum $sup_{M'}\,f(K)$ of the set $f(K)$ exists' is necessarily.

The set of all continuous functions from $M=(A;\leq_A)$ to $M'=(B;\leq_B)$ will be denoted by $[M\rightarrow M']$ or $[A\rightarrow B]$ if the partial orders are clear.

The following theorem establishes a helpfull connection between continuity and monotonicity.

THEOREM 3.1 Let $M=(A;\leq_A)$ and $M'=(B;\leq_B)$ be cpo's and $f:A\rightarrow B$ be a function. The function f is continuous if and only if f is monotonic and for every chain K in M is

$$f(sup_M\,K)\leq_B sup_{M'}\,f(K)\ .$$

Proof Let f be continuous. It remains to show the monotonicity of f, since $f(sup K)\leq_B sup\,f(K)$ follows directly from the continuity of f.

Let $a,a'\in A$ be such that $a\leq_A a'$. Then $K=\{a,a'\}$ is a chain in M and $sup\,K$ exists (M is complete) with $sup\,K=a'$. Consider the set $f(K)=\{f(a),f(a')\}$. The Continiuty of f establishes the existence of $sup\,f(K)$ and $sup\,f(K)=f(sup\,K)=f(a')$, that is $f(a) \leq_B f(a')$. Hence f is monotonic.

Conversely, suppose that f is monotonic and for every chain K in M is $f(sup K) \leq_B sup f(K)$.

We have to show that for every chain K in M the supremum $sup f(K)$ exists and $sup f(K) \leq_B f(sup K)$. Is K a chain so $f(K)$ too because of the monotonicity of f (with $a,a' \in K$ we have either $f(a) \leq_B f(a')$ or $f(a') \leq_B f(a)$). This together with the completeness of M' delivers the existence of $sup f(K)$.

Since $a \leq_A sup K$ for every $a \in K$, by the monotonicity of f, $f(a) \leq_B f(sup K)$, $\forall a \in K$. Therefore $f(sup K)$ is an upper bound of the chain $f(K)$. Since $sup f(K)$ is the least upper bound we have $sup f(K) \leq_B f(sup K)$. This together with the hypothesis gives the continuity of f. □

Two important consequenses of this theorem are the following corollaries.

COROLLARY 3.1 Let $M = (A; \leq_A)$ and $M' = (B; \leq_B)$ be cpo's and $f: A \rightarrow B$ a function. If M contains only finite chains then f is continuous if and only if f is monotonic.

Proof By Theorem 3.1 it remains to show that for every finite chain K in M and every monotonic function f from A to B : $f(sup K) \leq_B sup f(K)$. Let $K = \{a_1, \ldots, a_n\}$, $n \geq 1$, be any finite chain in M, then $sup K = a_n$. Then $f(a_1) \leq_B f(a_2) \leq_B \ldots \leq_B f(a_n) = f(sup K)$ for the elements of the chain $f(K)$ because f is monotonic. So $f(sup K) = f(a_n) \in f(K)$ and hence $f(sup K) \leq_B sup f(K)$. Furthermore, we have $sup f(K) = f(a_n) = f(sup K)$. □

COROLLARY 2.2 Let $M_i = (A_i; \leq_i)$, $\mathrm{i} = 1, \ldots, \mathrm{n}$, be flat posets and $M' = (B, \leq_B)$ a cpo. A monotonic function from $M = M_1 \times \ldots \times M_n$ in M' is continuous.

Proof Any flat poset is complete and the Cartesian product of this cpo's is a cpo with only finite chains $\{\perp, a\}$. By the previous corollary we get the assertion. □

The continuity of functions must be proved from case to case. Here is one important result.

THEOREM 3.2 Let $M=(A;\leq_A)$ and $M'=(B;\leq_B)$ be two cpo's. Then the set $[M\rightarrow M']$ of all continuous functions is a sub-cpo of the set $(M\rightarrow M')$ of all functions from $A$ to $B$ (with the partial order from Lemma 2.1).

4 Fixpoints

There are many practical problems where the fixpoint of a function is the solution of this problem.

DEFINITION 4.1 Let $A$ be a set and $f$ a function from $A$ into itself. An element $x\in A$ is called a fixpoint of $f$, if $f(x)=x$.

There are functions with one, several or no fixpoints. For example the function $f:R\rightarrow R$, defined by $f(x)=ax+b$, has the unique fixpoint $x_0=\frac{b}{1-a}$, where $a\neq 1$. For $a=1$ and $b\neq 0$ the function has no fixpoints.

So the question arise: How we can 'see' if a function has a fixpoint ? To realise some properties we consider the following lemma.

LEMMA 4.1 Let A be a set and $(P(A);\subseteq)$ be the poset of all subsets of $A$. Then any monotonic function $f:P(A)\rightarrow P(A)$ has a fixpoint in $P(A)$.

Proof Let $C=\{B\in P(A)|B\subseteq f(B)\}$. $C$ is nonempty since $\varnothing\in C$. Let $X=\bigcup C$. We will show that $X$ is a fixpoint of $f$. For any $B\in C$ is $f(B)\subseteq f(X)$ by monotonicity of $f$ ($B\subseteq\bigcup C=X$). With the definition of the set $C$ we have $B\subseteq f(B)\subseteq f(X), \forall B$ and therefore $\bigcup\{B|B\in C\}\subseteq f(X)$, that is $\bigcup C=X\subseteq f(X)$. Hence $X\subseteq f(X)$.
By monotonicity of $f$, $f(X)\subseteq f(f(X))$, that is $f(X)\in C$ and then $f(X)\subseteq\bigcup C=X$. Finally $f(X)=X$. □

We have seen, from Example 2.4, the set $(P(A);\subseteq)$ is a cpo.

Furthermore the function f is continuous: Let $K=\{A_i|i\in I\}$ be a chain in $(P(A);\subseteq)$. By monotonicity of f, $f(K)$ is a chain too. $\bigcup_{i\in I} A_i$ and $\bigcup_{i\in I} f(A_i)$ are the least upper bounds of K and $f(K)$, respectively. With the rules of De Morgan, $f(\bigcup_{i\in I} A_i)=\bigcup_{i\in I} f(A_i)$, hence f is continuous.

It can be shown that a continuous function from a cpo into itself has fixpoints and the least fixpoint is unique.

This lemma has a technical character.

LEMMA 4.2 Let $M=(A;\leq)$ be a poset and $f:M\to M$ a monotonic function. If M has a least element $\perp$ then

$$\perp, f(\perp),\ldots,f^n(\perp),\ldots$$

is a chain.

Proof By induction it will be shown that for all $n\geq 0$, $f^n(\perp)\leq f^{n+1}(\perp)$.
In the case $n=0$ it is $\perp\leq f(\perp)$, since $\perp$ is the least element of the poset M.
Suppose $f^n(\perp)\leq f^{n+1}(\perp)$, then by the monotonicity of f, we have $f^{n+1}(\perp)\leq f^{n+2}(\perp)$ and the induction step is done. □

Now we obtain the Fixpoint Theorem:

THEOREM 4.1 A continuous function f from a cpo M into itself has a unique least fixpoint. Furthermore, if $\perp$ is the least element of M then the least fixpoint of f is the supremum of the chain $\perp, f(\perp),\ldots,f^n(\perp),\ldots$.

Proof Let a be the supremum of the chain $K=\{f^i(\perp)|i\in N\}$ (this element exists since M is a cpo). It will be shown that a is the least fixpoint of f. By the continuity of f we have $f(a)=f(sup\,K)=sup\,f(K)=sup\,K=a$. Thus, a is a fixpoint of f . Let b be another fixpoint of f . Then $\perp\leq b$ and by induction one obtains $f^n(\perp)\leq b, \forall n\geq 0$. Hence b is a supremum of the chain K and $sup\,K\leq b$, that is $a\leq b$. □

THEOREM 4.2 Let $M=(A;\leq)$ be a cpo. The function $\mu:[M\to M]\to M$, defined by $\mu(f)$ is the least fixpoint of the continuous function $f:M\to M$, is continuous.

COROLLARY 4.1 Let $M=(A;\leq)$ be a cpo and $f:M \to M$ be a continuous function. If $\exists x \in A, f(x) \leq x$ then $\mu(f) \leq x$.

Proof By induction over $i \in N$ it will be shown that $f^i(\perp) \leq x$ with $f(x) \leq x$. The induction basis $\perp \leq x, \forall x \in A$ is clear. Assume $f^i(\perp) \leq x$, $i \geq 0$ then by monotonicity of f, $f^{i+1}(\perp) \leq f(x)$. Thus, $f^{i+1}(\perp) \leq x$. So x is an upper bound of the chain $\perp, f(\perp), \ldots, f^n(\perp), \ldots$ and hence $\mu(f) \leq x$ by Theorem 2.6. □

This Corollary is said to be the Park's Theorem.

The construction of the least fixpoint $\mu(f)$ as the least upper bound of a chain suggest to the so-called Induction Principle of Scott. In fact, that fixpoint induction principle is nothing more than usual induction on n to show a property for the chain $K = \{f^n(\perp) | n \geq 0\}$ and its supremum $\mu(f)$. On reaching this a special class of predicates will be introduced.

DEFINITION 4.2 Let $M=(A;\leq)$ be a cpo and $P:A \to \{0,1\}$ be a predicate. P is called admissible if for every chain K in M the condition holds: $P(a), \forall a \in K \;\Rightarrow\; P(\sup K)$.

Now the Induction Principle of Scott can be formulated.

THEOREM 4.3 Let $M=(A;\leq)$ be a cpo, $f:M \to M$ be a continuous function and $P:M \to \{0,1\}$ an admissible predicate. If $P(\perp)$ and $P(x)$ implies $P(f(x))$ for every $x \in M$, then $P(\mu(f))$.

Proof By the Theorem 4.1, $K: \perp, f(\perp), \ldots, f^n(\perp), \ldots$ is a chain and $\mu(f) = \sup K$. By classical induction on n one can show that $P(f^n(\perp)), \forall n$. Since P is an admmissible predicate the Theorem is proved. □

5 Application

One important application of the Fixpoint Theorem consists in the proof of the correctness of the computation by recursive programs.

Consider the recursive program for computing factorials:

$$F(x) \Leftarrow if\ x = 0 \text{ then } 1 \text{ else } x * F(x-1)\ .$$

The computation starts by a call to the function procedure of the function variable F and the program is recalled by itself. Normally the computation sequence will be finished after finite steps and will provide the output value of the program for the given input value x (meaning or semantics of the program).

In fact, this recursive program defines a function $fac: N \to N$ with

$$fac(n) = n * (n-1) * \ldots * 2 * 1,\ n \in N\ .$$

By interpreting $' \Leftarrow '$ as an equality sign the meaning of this program is defined as a function $f: N_\omega \to N_\omega$ such that

$$f(x) = \ if - then - else(x = 0, 1, x * f(x-1)) \text{ for all } x \in N_\omega .$$

This functions are the fixpoints of the functional $\Phi:(N_\omega \to N_\omega) \to (N_\omega \to N_\omega)$ defined by

$$\Phi(f)(x) = \ if - then - else(x = 0, 1, x * f(x-1))\ .$$

By applying the functional Φ to the function $f: N_\omega \to N_\omega$ we obtain

$$\Phi(f)(n) = \begin{cases} \omega, \text{ if } n = \omega \\ 1, \text{ if } n = 0 \\ \omega, \text{ if } n \neq 0 \text{ and } f(n-1) = \omega \\ n * f(n-1), \text{ othewise} \end{cases} .$$

It can be shown ([1]) that a functional Φ is associated to every recursive program that is the least fixpoint of Φ exists and has the semantics of the program.

We show that this functional Φ is continuous: It is enough to show, by Theorem 3.1, that
(i) Φ is monotonic and
(ii) $\Phi(sup K) \leq' sup\, \Phi(K)$ for every chain K in $M = ((N_\omega \to N_\omega);\leq')$.

For (i) consider $f,g\colon N_\omega \to N_\omega$ with $f \leq' g$ (with the relation in Lemma 2.1). According to the definition of Φ we have to distinguish the three cases:

(1) $n = \omega$: $\Phi(f)(n) = \omega \leq \Phi(g)(n)$
(2) $n = 0$: $\Phi(f)(n) = 1 = \Phi(g)(n)$
(3) $n \neq \omega, 0$: *if* $f(n-1) = \omega$ then $\Phi(f)(n) = \omega \leq \Phi(g)(n)$
if $f(n-1) \neq \omega$ then $\Phi(f)(n) = n * f(n-1) = n * g(n-1) = \Phi(g)(n)$,
since $f(n-1) = g(n-1)$.

It follows $\Phi(f) \leq' \Phi(g)$ and Φ is monotonic.

To show (ii) let $K = \{f_i | i \in N\}$ be a chain in M. Because of Lemma 2.1 we have to prove that

$$\Phi(sup\, K)(n) \leq (sup\, \Phi(K))(n) = sup(\Phi(K)(n)) \equiv sup\{\Phi(f_i)(n) | f_i \in K\},\ \forall n \in N_\omega .$$

We have to distinguish the three cases:

(1) $n = \omega$: $\Phi(sup\, K)(n) = \omega \leq sup(\Phi(K)(n))$
(2) $n = 0$: $\Phi(sup\, K)(n) = 1 = sup(\Phi(K)(n))$
(3) $n \neq \omega, 0$: *if* $f(n-1) = \omega$ for all $f_i \in$ K then $sup\, K(n-1) = \omega$,
hence $\Phi(sup\, K)(n) = \omega \leq sup(\Phi(K)(n))$
if $f(n-1) = m \neq \omega$ for at least one $f_i \in$ K then
$sup\, K(n-1) = sup\{f_i(n-1) | f_i \in K\} = m$ and so it is
$\Phi(sup\, K)(n) = n * (sup\, K)(n-1) = n * m = sup(\Phi(K)(n))$.

Hence $\Phi(sup\, K)(n) \leq sup(\Phi(K)(n)),\ \forall n \in N_\omega$ or $\Phi(sup\, K) \leq' sup\, \Phi(K)$ for all K.

By the Fixpoint Theorem the functional Φ has a least fixpoint $\mu(\Phi)$ and it is

$$\mu(\Phi) = sup\{\Phi^i(\bot_{(N_\omega \to N_\omega)}) | i \in N\} .$$

By induction on i we can show that

$$\Phi^i(\bot_{(N_\omega \to N_\omega)})(n) = f_i(n) = \begin{cases} \omega, \text{ if } n = \omega \text{ or } n \in N, n \geq i \\ n!, \text{ if } n \in N, 0 \leq n \leq i-1 \end{cases} \quad \text{for all } i \in N .$$

Since by Example 2.6

$$sup\{f_i(n)|i \in N\} = \begin{cases} \omega, \text{ if } n = \omega \\ n!, \text{ if } n \in N \end{cases}$$

the fixpoint $\mu(\Phi)$ is the ω-extension of the factorial function *fac*.

Finally the correctness of the computing by the given recursive program is proved.

REFERENCES

[1] Loeckx, J. and Sieber, K.: *The Foundations of Program Verifikation*, Wiley-Teubner Series in Computer Science, Stuttgart, 1987

[2] Roitman, J.: *Introduction to Modern Set Theory*, Wiley-Interscience Publication, New York, 1990

[3] Wechler, W.: *Universal Algebra for Computer Scientists*, Springer-Verlag, Heidelberg, 1992