1-1-1979

# Order foundations for formal language theory.

Catherine L. Madden

# ORDER FOUNDATIONS FOR FORMAL LANGUAGE THEORY

by

Catherine L. Madden

A Thesis

Presented to the Graduate Committee

of Lehigh University

in Candidacy for the Degree of

Master of Science

in

Computer Science

Lehigh University

1979

## CERTIFICATE OF APPROVAL

Approved and recommended for acceptance as a thesis in partial fulfillment of the requirements for the degree of Master of Science.

Nov 30, 1979
(date)

Professor in Charge

Accepted Nov 30, 1979

Head of the Division

ACKNOWLEDGMENTS

This paper is the culmination of a sequence of seminars in Formal Language Theory offered by Professor Samuel L. Gulden. I wish to thank Professor Gulden for introducing me to this field which has such potential for future research, and for his gracious interest in my education throughout our association.

To my excellent typist and friend, Ms. Judy Arroyo, I am indebted and promise this to be my last thesis.

TABLE OF CONTENTS

ABSTRACT

The basis of this paper is the work of Blikle concerning the relationship of the productions of a formal grammar to their expression as equations. These equations are considered as the basis of the grammar. Their solutions are the elements of the associated formal language.

It is our intention to lay the mathematical foundation for considering a formal language as a subset of a Boolean semiring. To this end we introduce the concepts of $\sigma_i$-completeness of posets and of $\sigma_i$-continuity of functions between $\sigma_i$-complete posets.

It is our intention to use the power of this mathematical structure in future research to consider the relationship between normal forms of a context free grammars and matrix equations.

## ALGEBRAIC PRELIMINARIES

1. Definition. A monoid, $(M, \circ)$ is a system consisting of a set $M$ and a binary operation $\circ$ defined on $M$ such that $\circ$ is associative over $M$ and there exists an identity element $1 \in M$; that is $\circ(m,1) = m = \circ(1,m)$ for all $m \in M$.

Alternately we use the notations $(m,n)$ and $mn$ for $\circ(m,n)$. The identity element of a monoid is unique. If there were two identity elements $1$ and $1'$, we would have the immediate contradiction $1 = 11' = 1'$.

2. Definition. For $m \in M$ and $r \in Z^+ = \{p : p$ is a non-negative integer$\}$, we define $m^0 = 1$ and $m^{r+1} = mm^r$.

3. Lemma. $m^{p+q} = m^p m^q$ for $m \in M$ and $p, q \in Z^+$.

The proof of Lemma 3 is a standard application of the principle of mathematical induction.

4. Example. $Z^+$ under multiplication is a monoid with identity element 1.

5. Example. $Z^+$ under addition is a monoid with identity element 0.

6. Definition. For $r \in Z^+$ let $[r] = \{n \in Z^+ : 0 < n \leq r\}$. An r-sequence on a set X is a function $\alpha : [r] \to X$.

For $r > 0$ and $\alpha$ an r-sequence on X we may identify $\alpha$ with the r-tuple $\alpha_1, \ldots, \alpha_r$ where $\alpha_j = \alpha(j)$ for $0 < j \leq r$.

7. Definition. Let X be a set $X^r = \{\alpha : \alpha$ is an r-sequence on $X\}$. We identify $X^r$ with the r-tuple $X \times \ldots \times X$. Observe if $r = 0$ then $[r] = \emptyset$. Therefore $X^0 = \{\varepsilon\}$ where $\varepsilon$ is the empty set.

8. Definition. Let $\alpha \in X^r$ and $\beta \in X^s$. Define $\gamma \in X^{r+s}$ by

$$\gamma(j) = \begin{cases} \gamma(j) & 0 < j \leq r \\ \beta(j-r) & r < j \leq r+s \end{cases}$$

We write $\gamma = \gamma\beta$ .

9. Lemma. If $\alpha \in X^r$, $\beta \in X^s$ and $\gamma \in X^t$ then $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ and $\alpha\varepsilon = \alpha = \varepsilon\alpha$ .

[ i) $(\alpha\beta)\gamma(j) = \begin{cases} (\alpha\beta)(j) & 0 < j \leq r+s \\ \gamma(j) & r+s < j \leq r+s+t \end{cases}$

$$= \begin{cases} \alpha(j) & 0 < j \leq r \\ \beta(j-r) & r < j \leq r+s \\ \gamma(j-r-s) & r+s < j \leq r+s+t \end{cases}$$

$$= \begin{cases} \alpha(j) & 0 < j \leq r \\ \beta\gamma(j) & r < j \leq r+s+t \end{cases}$$

$$= \alpha(\beta\gamma)j.$$

ii) $\varepsilon\alpha(j) = \begin{cases} \varepsilon(j) & 0 < j \leq 0 \\ \alpha(j) & 0 < j \leq r \end{cases}$

$$= \alpha(j)$$

$$= \begin{cases} \alpha(j) & 0 < j \leq r \\ \varepsilon(j-0) & r < j \leq r+0 \end{cases}$$

$$= \alpha\varepsilon(j)$$ ]

10. Definition. $X^+ = \bigcup_{r>0} X^r$ and $X^* = \bigcup_{r\geq 0} X^r$.

We assume throughout that $X^+$ and $X^*$ have the binary operation of concatenation described in 8 defined on them. $X^*$ under concatenation is a monoid with identity element $\varepsilon$ [Lemma 9]. However $X^+$ under concatenation is not a monoid since $X^+$ does not have an identity element. Observe if $X = \emptyset$ then, $X^0 = \{\varepsilon\}$ but $X^r = \emptyset$ for $r > 0$. Identifying $X$ and $X^1$ we may write $\alpha \in X^+ = \bigcup_{r>0} X^r$ as $\alpha = (x_1, x_2, \ldots, x_j, \ldots)$ where $\alpha(j) = x_j \in X$.

11. Lemma. Let $M$ be a monoid. For $A, B \subset M$. Define $AB = \{ab : a \in A \text{ and } b \in B\}$. The power set of $M$, $\mathbb{P}(M)$, is a monoid under this product operation. Moreover, $\emptyset$ is the zero element of $\mathbb{P}(M)$; that is $\emptyset A = \emptyset = A\emptyset$

[ i) associativity: $(AB)C = \{xc : x \in AB \text{ and } c \in C\} = \{(ab)c : a \in A, b \in B \text{ and } c \in C\} = \{a(bc) : a \in A, b \in B, \text{ and } c \in C\} = \{ay : a \in A \text{ and } y \in BC\} = A(BC)$ since $M$ is a monoid.

ii) $\{1\}$ in the identity: $A\{1\} = \{a1 : a \in A\} = \{a : a \in A\} = A = \{1a : a \in A\} = \{1\} A$. If $M$ is a monoid, we assume throughout that $\mathbb{P}(M)$ carries the associated monoid structure defined in Lemma 11. ]

12. Definition. Let $M$ be a monoid and $A \subset M$ define $A^0 = \{1\}$, $A^{r+1} = A\,A^r$, $A^+ = \bigcup_{r>0} A^r$, and $A^* = \bigcup_{r\geq 0} A^r = A^0 + A^+$, $(r \in Z^+)$.

13. Lemma. Let $A,B,C \in \mathbf{P}(M)$ where $M$ is monoid.

Then 1) $(A \cup B) \cup C = AC \cup BC$

2) $C(A \cup B) = CA \cup CB$

3) $(A \cap B)\, C \subsetneq AC \cap BC$

Additionally if $A \subset B$ then

4) $AC \subset BC$

5) $CA \subset CB$ .

[The validity of 1, 2, 4, 5 and proper containment in 3 are standard set theoretic arguments. To show equality need not exist in 3, let $X = \{a\}$, $A = \{a, a^3\}$, $B = \{a^2, a^4\}$ and $C = \{a, a^2\}$. Recall $X^*$ is a monoid under concatenation [Lemma 9]. A, B and $C \subset X^*$. Direct computation yields $A \cap B = \emptyset$, $AC = \{a^2, a^3, a^4, a^5\}$, $BC = \{a^3, a^4, a^5, a^6\}$ and $AC \cap BC = \{a^3, a^4, a^5\} \not\subset \emptyset = (A \cap B)C$].

14. Definition. Let $X$ be a set and $\mathbf{P}(X)$ be the power set of $X$. Let $\mathbf{R}(X) = \mathbf{P}(X \times X)$. If $R,S \in \mathbf{R}(X)$ define $RS = \{(x,y) :$ there exists $z \in X$ with $(x,z) \in R$ and $(z,y) \in S\}$. This operation on $\mathbf{R}(X)$ is called the lexigraphic join as opposed to the usual functional join.

15. Lemma. $\mathbb{R}(X)$ is a monoid under lexigraphic join.

[If $R, S, T \in \mathbb{R}(X)$ then $(x,y) \in (RS)T$

if and only if $\exists\ p \in X$ such that $(x,p) \in RS$ and $(p,y) \in T$

if and only if $\exists\ q \in X$ such that $(x,q) \in R$, $(q,p) \in S$ and $(p,y) \in T$

if and only if $(x,q) \in R$ and $(q,y) \in ST$

if and only if $(x,y) \in R(ST)$.

That is lexigraphic join is associative over $\mathbb{R}(X)$. Now let $\Delta_X = \{(x,x) : x \in X\}$. Clearly $\Delta_X \in \mathbb{R}(X)$. $(x,y) \in R\Delta_X$ if and only if $\exists\ z \in X$ such that $(x,z) \in R$ and $(z,y) \in \Delta_X$

if and only if $(x,z) \in R$ and $z = y$

if and only if $(x,y) \in R$

if and only if $(x,y) \in R$ and $(x,x) \in \Delta_X$

if and only if $(x,y) \in \Delta_X R$.

That is $\Delta_X$ is the identity element of $\mathbb{R}(X)$ under lexigraphic join].

For $R \in \mathbb{R}(X)$ we shall also use the notations $xRy$ and $R(x,y)$ for $(x,y) \in R$. Recall $R \in \mathbb{R}(X)$ is symmetric if $R^{-1} = \{(x,y) : (y,x) \in R\} \subset R$, reflexive if $\Delta_X \subset R$ and transitive if $(x,y) \in R$

and $(y,z) \in R$, imply $(x,z) \in R$. Since $\mathbb{R}(X)$ is a monoid we have $R^+ = \bigcup_{n>0} \{R^n\}$ and $R^* = \bigcup_{n\geq 0} \{R^n\}$. Observe $R^* = R^0 \cup R^+ = \{\Delta_x\} \cup R^+$; that is $R^0 = \Delta_x$. Also $\emptyset^+ = \emptyset$ but $\emptyset^* = \{\Delta_x\}$.

16. Definition. $R^+$ is called the transitive closure of $R$ and $R^*$ is called reflexive transitive closure of $R$.

17. Lemma. If $R$ is a transitive relation then $R^2 \subset R$. Inductively $R^m \subset R$. [$(x,z) \in R^2 \Rightarrow \exists\ y \in X$ such that $(x,y) \in R$ and $(y,z) \in R$. Since $R$ is transitive $(x,z) \in R$.] Thus if $R$ is transitive we have $R \supset \bigcup_{n>0} R^n = R^+$, therefore, $R^+ = R$.

18. Lemma. If $R$ is a symmetric relation then $R^{-1} = R$. [Since $R$ is symmetric, it sufficies to show $R \subset R^{-1}$. $(x,y) \in R \Rightarrow (y,x) \in R^{-1} \Rightarrow (x,y) \in R^{-1}$]

19. Lemma. i) $(R^{-1})^{-1} = R$

ii) $(RS)^{-1} = S^{-1}R^{-1}$

[i) $(x,y) \in (R^{-1})^{-1}$ if and only if $(y,x) \in R^{-1}$ if and only if $(x,y) \in R$.

ii) $(x,y) \in (RS)^{-1}$ if and only if $(y,x) \in RS$ if and only if there exists $z \in X$ such that $(y,z) \in R$ and $(z,x) \in S$ if and only if there exists $z \in X$ such that $(z,y) \in R^{-1}$ and $(x,z) \in S^{-1}$ if and only if $(x,y) \in S^{-1}R^{-1}$].

20. Definition. A simering, $(S;\circ,+)$ is a system consisting of a set $S$ and two binary operations defined on $S$ such that $(S;+)$ is a monoid with identity $0$, $(S;\circ)$ is a monoid with identity 1, and such that for $a,b,c \in S$ we have

i) $a(b+c) = ab + ac$

ii) $(a+b)c = ac + bc$

iii) $a \circ 0 = 0 = 0 \circ a$

iv) $a + b = b + a$

21. Example. $(Z^+;+,\circ)$ is a semiring.

22. Example. $(\mathbf{P}(M);+,\circ)$ is a semiring where $M$ is a monoid, $+$ is set union, and $\circ$ is the concatenation operation described in Lemma 11. $\{1\}$ is the identity for concatenation and $\emptyset$ is identity for set union.

23. Definition. A partial order on a set $X$ is a relation $\leq \in \mathbf{R}(X)$ which is reflexive, transitive, and antisymmetric; that is $(x,y) \in \leq$ and $(y,x) \in \leq$ imply $x = y$.

24. Definition. A poset is a pair $(X;\leq)$ such that $X$ is a set and $\leq$ is a partial order defined on $X$.

25. Definition. Let $X$ be a poset and $A \subset X$. $x \in X$ is an upper bound for $A$ if $a \leq x$ for all $a \in A$.

26. Definition. Let $X$ be a poset and $A \subset X$. $x \in X$ is the supremum for $A$ if $x$ is an upper bound for $A$ and $x \leq y$ for all upper bounds $y$ of $A$.

27. Definition. A poset $X$ is a semilattice if for any $x, y \in X$ $\sup\{x,y\}$ exists. Inductively if $X$ is a semilattice and $A$ is a finite subset of $X$ then $\sup A$ exists.

28. Lemma. Let $X$ be a poset and $A \subset X$, if $a = \sup A$ then $a$ is unique. [Let $a_1$ and $a_2$ equal sup A. Since $a_1$ and $a_2$ are upper bounds for A, $a_1 \leq a_2$ and $a_2 \leq a_1$. However $\leq$ is antisymmetric, thus $a_1 = a_2$].

29. Definition. Let $X$ be a set and $f : X \to Y$. $x_0$ is a fixed point of $f$ if $f(x_0) = x_0$.

30. Definition. Let $X$ and $Y$ be posets. A function $f : X \to Y$ is an order morphism if for $u,v \in X$ with $u \leq v$ then $f(u) \leq f(v)$.

31. Definition. Let $X$ be a poset. A floor for $X$ is an element $\perp \in X$ such that $\perp \leq x$ for all $x \in X$. We assume throughout that all the posets which we discuss have a floor.

32. Definition. Let $S$ be a semiring. $S$ is called Boolean if for each $s \in S$, $s + s = s$.

33. Definition. Let $S$ be a Boolean semiring. For $s_1, s_2 \in S$ define $s_1 \leq s_2$ if $s_1 + s_2 = s_2$.

34. Lemma. $\leq$ is a partial order on a Boolean semiring $S$.

[ i) If $x+x = x$ then $x \leq x$; that is $\leq$ is reflexive over $S$.

ii) If $x \leq y$ and $y \leq z$ then $x + z = x + (y+z) = (x+y) + z = y + z = z$; that is, $\leq$ is transitive over $S$.

iii) If $x \leq y$ and $y \leq x$ then $y = x + y = y + x = x$; that is $\leq$ is antisymmetric over $S$. ]

35. Lemma. Let $S$ be a Boolean semiring and $a,b \in S$. If $a \leq b$ then $ac \leq bc$ and $ca \leq cb$ for all $c \in S$.

[ i) $bc = (a+b)c = ac + bc$; that is $ac \leq bc$

ii) $cb = c(a+b) = ca + cb$; that is $ca \leq cb$ ].

36. Corollary. Let $S$ be a Boolean semiring, $A \subset S$ and $s \in S$. If $a = \sup A$ then $(as)$ is an upper bound for $A\{s\} = As$. [$b \leq a$ for all $b \in A$. By Lemma 35 $bs \leq as$; that is $(as)$ is an upper bound for $As$.]

37. Definition. Let $A_1,\ldots,A_n$ be posets. We define a partial order on $\prod_{i=1}^{n} A_i$ by $(a_1,a_2,\ldots,a_n) \leq (b_1,b_2,\ldots,b_n)$ if and only if $a_i \leq b_i$ for $1 \leq i \leq n$.

38. Lemma. Let $A_1,\ldots,A_n$ be posets. If $C_i \subset A_i$ and $c_i = \sup C_i$ $(1 \leq i \leq n)$ then $(c_1,c_2,\ldots,c_n) = \sup \prod_{i=1}^{n} C_i$. [Since $c_i = \sup C_i$, $c = (c_1,\ldots,c_n)$ is an upper bound for $C = \prod_{i=1}^{n} C_i$. Let $w = (w_1,\ldots,w_n)$ be an upper bound for $C$. $c_i \leq w_i$ since $c_i = \sup C_i$. Hence $c \leq w$.]

39. Lemma. Let $S$ be a Boolean semiring. If $a,b \in S$ then $a + b = \sup\{a,b\}$. Inductively $\sum_{i=1}^{n} a_i = \sup\{(a_i)_{i=1}^{n}\}$. [ Since $a + (a+b) = a + b$,

$a \leq a+b$. Similarly $b \leq a+b$ since $+$ is commatative over a semiring. Thus $a + b$ is an upper bound of $\{a,b\}$. Let $c$ be an upper bound of $\{a,b\}$. Thus $a + c = c$ and $b + c = c$. Hence $a + b + c = a + c = c$. That is $a + b \leq c$; therefore, $a + b = \sup \{a,b\}$ ▯].

40. Lemma. Let $A$ be a poset and $(A_\alpha : \alpha \in \Gamma)$ be an indexed family of subsets $A_\alpha \subset A$. Let $a_\alpha = \sup A_\alpha$ and $a = \sup B$ where $B = \cup\{A_\alpha : \alpha \in \Gamma\}$. Then $a = \sup\{a_\alpha : \alpha \in \Gamma\}$. [$b \leq a$ for each $b \in B$. Thus $a_\alpha \leq a$ for each $\alpha \in \Gamma$. Suppose $y$ is an upper bound for $\{a_\alpha : \alpha \in \Gamma\}$ then $y$ is an upper bound for $B$. Thus $a = \sup B \leq y$. Therefore $a = \sup\{a_\alpha : \alpha \in \Gamma\}$ ▯].

41. Lemma. Let $S$ be a Boolean semiring with $x \leq y$ and $u \leq v$ then $x + b \leq y + b$, $x + u \leq y + v$ and $ax \leq ay$.

[ i) $x + y = y \Rightarrow x + y + b + b = y + b$. Since $+$ is commutative over a semiring $x + b + y + b = y + b$; that is $x + b \leq y + b$.

ii) Sinc $x + y = y$ and $u + v = v$, $x + y + u + v = y + v$. By commutativity $x + u + y + v = y + v$; that is, $x + u \leq y + v$.

iii) Since $x + y = y$, $a(x+y) = ay = ax + ay$; that is $ax \leq ay$.]

42. Corollary. Let $S$ be a Boolean semiring and $A \subset S$. If $y \in S$ and $a = \sup A$ then $\sup[A+y] = a + y$ where $A + y = \{x+y : x \in A\}$. [For all $x \in A$, $x \leq a$; therefore $x + y \leq a + y$, that is, $a + y$ is an upper bound for $A + y$. Let $w$ be an upper bound of $A + y$. If $u \in A$ then $u \leq u + y \leq w$. Hence $a \leq w$. Similarly $y \leq w$. Hence $a + y \leq w + w = w$; that is, $a + y = \sup[A+y]$.]

43. Lemma. Let $S$ be a Boolean semiring and $A, B \subset S$. If $a = \sup A$, $b = \sup B$ then $a + b = \sup[A+B]$. [For $x \in A$ and $y \in B$, $x \leq a$ and $y \leq b$. Hence $x + y \leq a + b$ for $(x,y) \in A \times B$. Let $w$ be an upper bound of $A + B$. For $u \in A$ and $v \in B$, $u \leq u + y \leq w$ and $v \leq v + x \leq w$. Hence $a \leq w$ and $b \leq w$. Therefore $a + b \leq w + w = w$; that is $a + b = \sup[A+B]$.]

44. Lemma. Let $S_1, S_2, \ldots, S_k$ be Boolean semiring and $S = \prod_{i=1}^{k} S_i$. If $S$ carries the inherited coordinatewise addition and multiplication operations then, $S$ is a Boolean semiring.

The validity of Lemma 44 is a consequence of associativity and the existence of additive and multiplicative identities over $S_i$. Similarly the distributive laws remain valid and all elements of $S$ are idempotent with respect to addition. $0 = \{0, 0, \ldots, 0\}$

is the zero element of $S$ and $1 = \{1,1,\ldots,1\}$ is the identity for multiplication. The partial order on $S$ is the standard product partial order.

45. Let $U$ be a countable subset of $S = \prod_{i=1}^{k} S_i$ where $S_i$ is a Boolean semiring. Let $U_i$ be the ith projection of $U$. If $u_i = \sup U_i$ then $u = (u_1,\ldots,u_k) = \sup U$. [The product partial order assures that $u$ is an upper bound for $U$. If $w = (w_1,\ldots,w_n)$ is an upper bound for $U$ then $w_i \geq \sup U_i$, $(1 \leq i \leq k)$. Therefore $w_i \geq u_i$ and hence $u \leq w$; that is $u = \sup U$.]

46. Definition. Let $X$ be a poset. $A \subset X$ is directed if for each pair $x,y \in A$ there exists $z \in A$ such that $x \leq z$ and $y \leq z$.

## II. $\sigma_i$-COMPLETENESS AND $\sigma$-CONTINUITY

1. Definition. Let $X$ be a poset and $A \in X$.

i) If $\sup A$ exists whenever $A$ is countable then $X$ is $\sigma_0$-complete.

ii) If $\sup A$ exists whenever $A$ is countable and directed then $X$ is $\sigma_1$-complete.

iii) If $\sup[\left\{a_n\right\}_{n=1}^{\infty}]$ exists for every montone increasing sequence then $X$ is $\sigma_2$-complete.

iv) If $\sup A$ exists whenever $A$ is directed then $X$ is $\sigma_3$-complete.

Clearly, $\sigma_0$ implies $\sigma_1$-complete, $\sigma_1$ implies $\sigma_2$-complete, and $\sigma_3$ implies $\sigma_1$-complete.

2. Lemma. $\sigma_2$-complete implies $\sigma_1$-complete. [Let $X$ be a $\sigma_2$-complete poset and $S \subset X$ be countable and directed, $S = \left\{b_n : n \in Z^+\right\}$. Let $c_1 = b_1$. There exists $c_2 \in S$ such that $c_1 \leq c_2$ and $b_2 \leq c_2$, since $S$ is directed. Iteratively choose $c_{k+1} \in S$ such that $b_{k+1} \leq c_{k+1}$ and $c_k \leq c_{k+1}$. $C = \left\{c_n : n \in Z^+\right\}$ is a monotone increasing sequence with $b_k = c_k$ for all $k$. Since $X$ is $\sigma_2$-complete, there exists $c \in X$ such that $c = \sup C$. Clearly $c$ is an upper bound of $S$. Let $y$ be an upper bound for $S$. $y \geq c_k$ for all $k$ since $C \subset S$. Thus $c \leq y$; that is, $c = \sup S$.]

3. Lemma. If $X$ is a $\sigma_0$-complete poset then, $X$ is a semilattice. [Let $A$ be a two element subset of $X$. Since $X$ is $\sigma_0$-complete, $\sup[A]$ exists.]

4. Lemma. Every Boolean semiring $S$ is a semilattice. [Let $A = \{x, y\} \subset S$. $x + y = x + x + y$ and $y + x = y + y + x$. Therefore $x \leq x + y$ and $y \leq y + x = x + y$; that is $x + y$ is an upper bound of $A$. Let $z$ be an upper bound for $A$. Now $x \leq z$ and $y \leq z$ imply $x + y \leq z + z = z$. [Lemma 1.4]. That is $x + y = \sup\{x, y\}$.]

5. Lemma. If $X$ is a semilattice then $\sigma_0$, $\sigma_1$ and $\sigma_2$-completeness are equivalent. [It suffices to show $\sigma_1$-complete implies $\sigma_0$-complete. Let $A = \{a_n : n \geq 0\}$. For $m \geq 0$ let $b_m = \sup\{a_n : 0 \leq n \leq m\}$. Notice $b_m$ exists since $X$ is a semilattice. Moreover $B = \{b_0, b_1, \ldots, b_j \ldots\}$ is countable and directed for $b_0 \leq b_1 \leq \ldots b_j \ldots$ . Let $b = \sup B$. Clearly $b \geq a_j$ for all $j$; that is, $b$ is an upper bound for $A$. Let $z$ be an upper bound for $A$, $b_j \leq z$ for $j \geq 0$. Hence $b \leq z$; that is $b = \sup A$.]

6. Definition. Let S be a Boolean semiring. S is $\sigma_i$-complete $(0 \leq i \leq 3)$ if

i) as a poset $(S;\leq)$ is $\sigma_i$-complete

ii) $f : S \times S \to S$ defined by $f(x,y) = xy$ satisfies $f[\sup[A \times B]] = \sup[f[A \times B]]$ for all countable $A, B \subset S$.

7. Corollary: If S is a Boolean semiring then $\sigma_0$, $\sigma_1$ and $\sigma_2$-completeness are equivalent.

8. Definition. Let S be a Boolean semiring. If $a \in S$ and $\sup_n \left\{ a^n : n \geq 0 \right\}$ exists then $a^* = \sup_n \left\{ a^n : n \geq 0 \right\}$.

9. Corollary. If S is a $\sigma_i$-complete Boolean semiring then $a^*$ exists for all $a \in S$, $(i=0,\ldots,2)$. [$\sigma_i$-complete are equivalent in a Boolean semiring].

10. Corollary. If S is a $\sigma_i$-complete Boolean semiring and $a \in S$ then

i) $0^* = 1$

ii) if $a \geq 1$ then $a^* \geq 1$

iii) if $a \leq 1$ then $a^* = 1$

iv) $1 \leq a^*$

[i) $0^* = \sup_n \{0^n : n \geq 0\} = \sup[1, \sup_n \{0^n : n \geq 1\}]$
$= \sup\{0, 1\} = 1$

ii) $1 \leq a \Rightarrow 1 \leq a \leq a^2 \Rightarrow 1 \leq a \leq a^2 \leq \ldots < a^n$ hence $a^* \geq 1 = a^0$

iii) $a \leq 1 \Rightarrow a^2 \leq a \leq 1 \Rightarrow a^n \leq a^{n-1} \leq \ldots \leq a \leq 1$ hence $a^* = 1 = a^0$.

iv) follows from ii and iii.]

11. Definition. A Boolean semiring is regular if $a^*$ exists for all $a \in S$.

12. Corollary. A $\sigma_i$-complete Boolean semiring is regular, $(i = 0, \ldots, 2)$ [Corollary 9].

13. Definition. Let X, Y be $\sigma_0$-complete posets and $f : X \to Y$ be an order morphism. f is $\sigma$-preserving if given a countable subset, $A \subset X$ with $a = \sup A$ then $f(a) = \sup[f(A)]$.

14. Theorem. (Tarsky). If X is a floored $\sigma_0$-complete poset and $f : X \to X$ is $\sigma$-preserving then f has a least fixed point $x_0$; that is, $x_0 = f(x_0)$ and if $y = f(y)$ then $x_0 \leq y$.

Proof. Let $\perp$ be the floor of X. Let $x_0 = \sup[\{\perp\} \cup \{f^n(\perp) : n > 0\}]$. Since f is σ-preserving,

$$f(x_0) = \sup[\{f(\perp)\} \cup \{f^n(\perp) : n > 1\}]$$

$$= \sup[\{f^n(\perp) : n > 0\}]$$

$$= x_0 \quad [\perp \text{ is the floor of } X].$$

Thus $x_0$ is a fixed point of f. If y is a fixed point of f then, $f(\perp) \leq f(y) = y$ since f is an order morphism. Inductively $f^n(\perp) \leq y$. Therefore $x_0 \leq y$. //

15. Lemma. Let S be a $\sigma_1$-complete Boolean semiring. Define $\ell_x : S \to S$ and $r_x : S \to S$ by $\ell_x(y) = xy$ and $r_x(y) = yx$. Let $V_1, V_2 \subset S$ be countable with $u_1 = \sup V_1$ and $u_2 = \sup V_2$. If $\ell_x$ and $r_x$ are σ-preserving then $\sup\{\ell_x(y) : y \in V_2\} = r_{u_2}(x)$ and $\sup\{r_x(y) : y \in V_2\} = \ell_{u_2}(x)$ for $x \in S$.

[$\sup\{\ell_x(y) : y \in V_2\} = \ell_x(u_2) = x\,u_2 = r_{u_2}x$ and $\sup\{r_x(y) : y \in V_2\} = r_x(u_2) = u_2x = \ell_{u_2}(x)$]

16. Lemma. Let $S$ be a $\sigma_1$-complete Boolean semiring. The following statements are equivalent.

i) $f : S \times S \to S$ defined by $f(x,y) = xy$ is $\sigma$-preserving where $S \times S$ carries the standard product structure.

ii) For each $x \in S$ the functions $\ell_x$ and $r_x$ are $\sigma$-preserving.

[ i $\Rightarrow$ ii Let $B \subset S$ be countable with $b = \sup B$ $\ell_x(\sup B) = \ell_x(b) = x\,b = f[\sup(x \times B)]$ $\sup[f(x \times B)] = \sup[xB] = \sup[\ell_x(B)]$.

ii $\Rightarrow$ i Let $V \subset S \times S$ be countable with $u = (u_1, u_2) = \sup V$. If $V_1$ and $V_2$ are the coordinate projections of $V$ then $u_1 = \sup V_1$ and $u_2 = \sup V_2$. For $a \in V_1$ define $B_a = \left\{b \in V_2 : (a,b) \in V\right\}$. $\sup\left\{f(V)\right\} = \sup\left\{\sup f(a, B_a)\right\} = \sup\left\{\sup \ell_a(B_a)\right\} = \sup \ell_a(u_2) = \sup[au_2] = \sup[r_{u_2}(a)] = r_{u_2}(u_1) = u_1u_2 = f(u_1,u_2)] = f[\sup V]$. ]

17. Definition. Let $S$ be a $\sigma_1$-complete Boolean semiring. For $a \in S$ let $a^* = \sup\left\{a^n : n \geq 0\right\}$.

18. Lemma. Let $S$ be a $\sigma_1$-complete Boolean semiring. Define $f : S \to S$ by $f(x) = xa + b$ where $a,b \in S$. $f$ is $\sigma$-preserving and the least fixed point of $f$ is $ba^*$.

Proof: $f$ is an order morphism [Lemma 1.35, 41]. Let $Y$ be a countable subset of $S$ and $y = \sup Y$. For $x \in Y$, $x \leq y$ implies $f(x) \leq f(y)$; that is, $f(y)$ is an upper bound of $f[Y]$. If $w$ is an upper bound of $f[Y]$ then $xa \leq xa + b \leq w$. Now $ya = \sup [Ya]$ since $g(x,y) = xy$ is $\sigma$-preserving because $S$ is $\sigma_i$-complete semiring. Thus $ya \leq w$. Moreover $b \leq ya + b \leq w$. Hence $ya + b \leq w + w = w$. That is, $f(y) = ya + b = \sup[f(y)]$. Therefore $f$ is $\sigma$-preserving. Recall $\perp$ is the zero element of the semiring. $f(\perp) = x\perp + b = b$. Iteratively $f^2(\perp) = f(b) = ba + b$, $f^3(\perp) = ba^2 + ba + b, \ldots, f^n(\perp) = ba^{n-1} + ba^{n-2} + \ldots + ba + b$. That is $f^n(\perp) = \sup\left\{ba^k : 0 \leq k \leq n-1\right\} = b \sup\left\{a^k : 0 \leq k \leq n-1\right\}$. If $x_0$ is the least fixed point of $f$ then $x_0 = \sup\left\{f^n(\perp) : n \geq 0\right\}$ [Theorem 14]. Therefore $x_0 = \sup\left\{ba^k : k \geq 0\right\}$. Since multiplication is $\sigma$-preserving $x_0 = b \sup\left\{a^k : k \geq 0\right\} = ba^*$. //

A similar argument yields the least fixed point of $g(x) = ax + b$ is $a^*b$.

19. Lemma. Let $\left\{S_i\right\}_{i=1}^{n}$ be a sequence of $\sigma_i$-complete Boolean semirings. If $S = \prod_{i=1}^{n} S_i$ then $S$ is a $\sigma_i$-copplete Boolean semiring. [S is a Boolean semiring [Lemma 1.44]. To demonstrate that $S$ is $\sigma_i$-complete, let $\left\{\delta^j\right\}_{j=1}^{\infty}$ be a countable family in $S$. Let $P_n(\delta^j) = \delta_n^j$. Since $\left\{\delta_n^j\right\}$ is countable subset of $S_n$ $\sup_j\left\{\delta_n^j\right\}$ exists. Let $\sup_j\left\{\delta_n^j\right\} = \delta_n$ and $\delta = \left\{\delta_n\right\}$. $\delta$ is an upper bound of $S$ by construction. Let $w$ be any upper bound of $S$. Then $w_n$ is an upper bound of $\{\delta_n^j\}$, hence $\delta_n \leq w_n$ and $\delta \leq w$. ]

20. Definition. Let $S$ be a $\sigma_i$-complete Boolean semiring and $F : S^{(k+n)} \to S^k$ be $\sigma$-preserving $n \geq 1$. For each $a \in S^{(n)}$, $\frac{\delta F(x,a)}{\delta x}$ is the least fixed of $g_a : S^k \to S^k$ such that $g_a(x) = F(x,a)$ $(x \in S^k$, $i = 0,\ldots,2)$.

21. Example. Let $F(x,y) = xy + b$. $\frac{\delta F(x,y)}{\delta x} = \|g_y\| = by^*$ where $g_y(x) = xy + b$ [Theorem 14].

22. Definition. Let X and Y be $\sigma_i$-complete posets ($i = 0,\ldots,3$) and $S \subset X$ be countable and directed. If $\sup[f(S)]$ exists and $\sup[f(S)] = f[\sup(S)]$ then f is $\sigma_i$-continuous.

As with $\sigma_i$-completeness we have $\sigma_0$-continuous implies $\sigma_1$-continuous, $\sigma_1$-continuous is equivalent to $\sigma_2$-continuous, and $\sigma_3$-continuous implies $\sigma_1$-continuous.

23. Lemma. Let $f : X \to Y$ be $\sigma_i$-continuous. If $x \leq y$ then $f(x) \leq f(y)$.

[ $\{x,y\}$ is countable and directed. Since f is $\sigma_i$-continuous, $f(x) \leq \sup\{f(x),f(y)\} = f[\sup\{x,y\}] = f(y)$. Thus f being $\sigma_i$-continuous implies f is an order morphism.]

24. Corollary. If $f : X \to X$ is $\sigma_2$-continuous then f has a least fixed point.

[ $\{\perp, f(\perp), f^2(\perp)\ldots f^n(\perp)\ldots\}$ is a monotone increasing sequence in X. Let $x_0 = \sup[\{\perp\} \cup \{f^n(\perp) : n > 0\}]$. As in Tarsky's Theorem $x_0$ is a fixed point of f. If y is a fixed point of f, $f^n(\perp) \leq y$ for all n. Therefore $x_0 \leq y$].

25. Lemma. The $\sigma_i$-continuous image of a directed set is directed.

Let $f : X \to Y$ be $\sigma_i$-continuous where $X$ and $Y$ are $\sigma_i$-complete. Let $S \subset X$ be directed. If $\{y_1, y_2\} \subset f(S)$ there exists $\{x_1, x_2\} \subset S$ such that $f(x_1) = y_1$, $f(x_2) = y_2$. Since $S$ is directed there exists $x_3 \in S$ with $x_1 \leq x_3$ and $x_2 \leq x_3$. Therefore $y_1 = f(x_1) \leq f(x_3)$ and $y_2 = f(x_2) \leq f(x_3)$ [Lemma 23]; that is $f[S]$ is directed.

26. Lemma. Let $X, Y_1, \ldots, Y_k$ by $\sigma_i$-complete posets $(i = 0, \ldots, 3)$. Define $f : X \to Y_1 \times \ldots \times Y_k$ by $f(x) = (f_1(x), \ldots, f_k(x))$. $f$ is $\sigma_i$-continuous if and only if each $f_j$ is $\sigma_i$-continuous $(j = 1, \ldots, k)$. $\Rightarrow$ Let $f$ be $\sigma_i$-continuous and $S \subset X$ be countable and directed with $s = \sup S$. By definition of $\sigma_i$-continuity we also have $y = (y_1, \ldots, y_k) = \sup[f(S)]$ exists. Therefore $y = \sup[f(S)] = f[\sup(S)] = f(s)$. Moreover $f_j(S)$ is countable and directed since the projection mappings are $\sigma_i$-continuous. Thus $z_j = \sup f_j[S]$ exists. Therefore $f_j(x) \leq z_j$ for all $x \in S$. That is $f(x) = (f_1(x), \ldots, f_k(x)) \leq (z_1, \ldots, z_k)$ for all $x \in S$. Since $y = \sup[f(S)]$, $y_j \leq z_j$ $(j = 1, \ldots, k)$. Clearly $y_j \geq f_j(x)$ for all $x \in S$.

Therefore $y_j \geq z_j$ $(j = 1,\ldots,k)$; that is $y_j = z_j$. Thus $\sup[f_j(S)] = z_j = y_j = f_j(s) = f_j[\sup S]$; that is $f_j$ is $\sigma_i$-continuous.

<= Conversely suppose $f_j$ is $\sigma_i$-continuous $(j = 1,\ldots,k)$. Let $S \subset X$ be countable and directed with $s = \sup S$ and $y_j = f_j(s)$. Since $f_j$ is $\sigma_i$-continuous, $y_j = f_j(s) = \sup[f_j(S)]$; that is $y = (y_1,\ldots,y_k)$ is an upper bound for $f[S]$. Now $f$ is order preserving since each $f_j$ is order preserving. Hence $f[S]$ is directed. Let $u = (u_1,\ldots,u_k) = \sup[f(S)]$. Thus $u_j$ is an upper bound for $f_j(S)$. Therefore $y_j \leq u_j$ $(j = 1,\ldots,k)$. Thus $y = u$. That is $f[\sup(S)] = f(s) = y = u = \sup[f[S]]$ ∎

27. Lemma. Let X, Y, Z be $\sigma_i$-complete posets $(i = 0,\ldots,3)$. If $f : X \to Y$ and $g : Y \to Z$ are $\sigma_i$-continuous then $f \circ g : X \to Z$ is $\sigma_i$-continuous, [Let $S \subset X$ be countable and directed. $f[S]$ and $g[f[S]]$ are countable and directed [Lemma 25]. Since $f$ and $g$ are $\sigma_i$-continuous $\sup[fg(S)] = \sup[g(fS)] = g[\sup f(S)] = g[f(\sup S)] = fg(\sup S)$] .

28. Definition. A poset X is complete if each subset of X has a sup.

29. Lemma. Let X be a complete poset. If $A \subset X$ then $\inf[A]$ exists.

[Observe $z = \inf A$ if $z \leq a$ for all $a \in A$ and if $y$ is a lower bound for $A$ then $z \geq y_1$. Let $B = \{x : x \text{ is a lower bound for } A\}$. B is not empty since all posets are assumed to have a floor. Let $b = \sup B$. $x \leq a$ for all $a \in A$, $x \in B$, therefore $b \leq a$ for all $a \in A$. That is $b$ is a lower bound for A. By definition $x \leq b$ for all $x \in B$, hence $b = \inf A$].

30. Lemma. Let X be a complete poset and $f : X \to X$ be an order morphism. If $Q = \{x : f(x) \leq x\}$ and $y = \inf Q$ then $f(y) = y$ and $y$ is the least fixed point of f.

[$y \leq x$ for each $x \in Q$. Hence $f(y) \leq f(x) \leq x$. Thus $f(y)$ is a lower bound for Q, hence $f(y) \leq y$, and $y \in Q$. For $x \in Q$, $f(x) \leq x$. Since f is an order morphism $f[f(x)] \leq f(x)$; therefore $f(x) \in Q$ whenever $x \in Q$. In particular $f(y) \in Q$. Since $y = \inf Q$ $y \leq f(y)$; therefore $y = f(y)$ and $y$ is a fixed point of f. Since all fixed points of f are in Q, y is the least fixed point of f.]

31. Corollary. Let $X$ be a complete poset and $f : X \to X$ be an order morphism. If $R = \{x : x \leq f(x)\}$ and $z = \sup R$ then $f(z) = z$ and $z$ is the greatest fixed point of $f$.

32. Lemma. Let $X$ be a complete poset, and $x, y \in X$ with $x \leq y$. If $[x,y] = \{z \in X : x \leq z \leq y\}$ then $[x,y]$ is a complete poset.

[Let $A \subset [x,y]$. Let $a = \sup_X[A]$. $a \in [x,y]$ since $y$ is an upper bound of $A$. Thus $a = \sup_A[x,y]$]

33. Lemma. Let $X$ be a complete poset and $f : X \to X$ be an order morphism. If $P$ is the set of fixed points of $f$ then $P$ is a complete poset.

Proof: Let $x_* = \inf_X P$, $x_*$ exists by Tarsky Theorem. Let $x^* = \sup_X P$, $x^*$ exists for $X$ is a complete poset. Let $\bot = \inf X$ and $\top = \sup X$. Choose $A \subset P$ such that $A \neq \emptyset$. Let $a = \sup_X A$. $[a,\top]$ is a complete poset. If $x \in A$ then $x \leq a$. Hence $x = f(x) \leq f(a)$. Since $a = \sup_X[A]$, $a \leq f(a)$. Thus $a \leq f(a) \leq \top$. Let $g = f_{1[a,\top]}$. In particular $g : [a,\top] \to [a,\top]$ and $g$ is an order morphism since $f$ is. Since $[a,\top]$ is a complete poset $g$ has a least fixed point $w \in [a,\top]$ [Lemma 30]. Therefore $w \in P$. Let $v$ be an upper bound of $A$ and $v \in P$. Therefore $a \leq v$, and $v \in [a, \top]$. Thus $g(v) = v$. Since $w$ is least fixed point of $g$, $w \leq v$. Hence $w = \sup_P[A]$ and therefore $P$ is complete. //

34. Corollary. If $X$ is a complete poset and $f : X \to X$ is an order morphism then $P$, the set of fixed points of $f$, is a lattice.

35. Lemma. Let $X$ be a $\sigma_i$-complete poset and $\{x_n : n \geq 0\}$ be a sequence of elements in $X$ such that $x_j \leq x_{j+1}$ for all $j$. Let $\{i_n : n \geq 1\}$ be a sequence of integers such that $0 < i_k < i_{k+1}$ for all $k$. If $u = \sup\{x_n\}$ then $u = \sup\{x_{i_k} : k \geq 1\}$.

Proof: Since $i_k < i_{k+1}$ we have $x_{i_k} \leq x_{i_{k+1}}$. Let $v = \sup\{x_{i_k} : k \geq 1\}$. Observe $i_\ell \geq \ell$ for all $\ell$. Hence $x_\ell \leq x_{i_\ell} \leq v$ and $u \leq v$. However $u = \sup\{x_n\}$ implies $v \leq u$. Therefore $u = v$. //

Observe if $S$ is a $\sigma_i$-complete Boolean semiring $(i = 0,\ldots,3)$ and $f : S\times S \to S$ is defined by $f(x,y) = xy$ then $f$ is $\sigma_i$-continuous by Definition 1.6. Also we have shown $g : S\times S \to S$ defined by $g(x,y) = x+y$ is $\sigma_i$-continuous in Lemma 1.43.

36. Lemma. Let S be a $\sigma_i$-complete Boolean semiring and $A = \{a_j : j \geq 0\}$ then $\sup(bA) = b \sup A$.

[multiplication is $\sigma_i$-continuous].

37. Lemma. Let S be a $\sigma_i$-complete Beeolean semiring. $(a^*)^n = a^*$ for $n \geq 1$.

[$(a^*)^{n+1} = a^*(a^*)^n$. Hence it is sufficient to establish $(a^*)^n = a^*$ for $n = 2$ and apply mathematical induction. Since $a^o = 1$, $1 \leq a^*$ hence $a^* \leq a^*a^* = (a^*)^2$. Moreover $aa^* = a \sup\{a^j : j \geq 0\}$ $= \sup\{aa^j : j \geq 0\}$, hence $aa^* = \sup\{a^j : j \geq 1\} \leq$ $\sup\{a^j : j \geq 0\} = a^*$. That is $aa^* \leq a^*$. Therefore $a^2a^* = a(aa^*) \leq aa^* \leq a^*$. Inductively, $a^na^* \leq a^*$ for $n \geq 0$. Thus $a^*a^* = \sup\{a^j : j \geq 0\}a^* = \sup\{a^ja^* : j \geq 0\}$ $\leq a^*$. Therefore $(a^*)^2 = a^*$ and inductively $(a^*)^n = a^*$ for $n \geq 1$.]

38. Corollary. Let S be a $\sigma_i$-complete Boolean semiring and $a \in S$. $(a^*)^* = a^*$

[$(a^*)^* = \sup_n\{(a^*)^n : n \geq 0\} = \sup\{1, a^*\} = a^*$.]

39. Corollary. Let S be a $\sigma_i$-complete Boolean semiring and $a \in S$, $b \in S$. $(a+b)^* = a^*b^*$

$$[ (a+b)^* = \sup_n \{(a+b)^n\} = \sup_n \sum_{j=0}^{n} a^j b^{n-j} = \sum_{\substack{p=0\\q=0}}^{\infty} a^p b^q$$

$$= (\sum_{p=0}^{\infty} a^p)(\sum_{q=0}^{\infty} b^q) = (\sup_p \{a^p\})(\sup_q \{b^q\}) = a^*b^* ]$$

40. Corollary. Let S be a $\sigma_i$-complete Boolean semiring and $a \in S$. $(a+1)^* = a^*$.

$$[(a+1)^* = a^*1^* = a^*1 = a^*]$$

41. Corollary. Let S be a $\sigma_i$-complete Boolean semiring and $a \in S$. $a^* = (1+aa^*)$.

$$[a^* = \sum_{n=0}^{\infty} a^n = 1 + \sum_{n=1}^{\infty} a^n = 1 + a \sum_{n=0}^{\infty} a^n = 1 + aa^*]$$

## III. FIXED POINT THEORY

1. Definition. Let $X$ and $Y$ be $\sigma_i$-complete posets $(i = 0,\ldots,3)$. $\mathbb{F}_i(X,Y)$ is the set of $\sigma_i$-continuous functions $f : X \to Y$.

2. Definition. Let $f,g \in \mathbb{F}_i(X,Y)$. $f \leq g$ if $f(x) \leq g(x)$ for all $x \in X$.

Under this definition $\mathbb{F}_i(X,Y)$ is a poset whose floor is the constant function $\perp_Y$.

3. Definition. Let $X = Y$ and define $\| \ \| : \mathbb{F}_i(X,X) \to X$ by $\|f\| = \sup\{f^n(\perp) : n \geq 0\}$.

Recall $f$ being $\sigma_i$-continuous implies $f$ is monotonic [Lemma 2.23]. Therefore $\perp \leq f(\perp) \leq \ldots \leq f^n(\perp)$ and $\|f\|$ is the least fixed point of $f$ [Theorem 2.24]

4. Lemma. Let $X$ and $Y$ be $\sigma_i$-complete posets $(i = 0,\ldots,3)$. If $F : X \times Y \to X$ is $\sigma_i$-continuous then $F_y : X \to X$ is $\sigma_i$-continuous where $F_y(x) = F(x,y)$. [Let $S$ be a countable directed subset of $X$. $F_y(S) = F[S \times \{y\}]$. Since $F$ is $\sigma_i$-continuous $\sup[F(S \times \{y\})] = \sup[F_y(S)] = F[\sup(S \times \{y\})] = F_y[\sup(S)]$]

As the $\sigma_i$-continuous image of directed set is directed, of a countable set is countable, of a monotone sequence is a monotone sequence, we shall limit our proofs to a single case. Other cases may be derived in a similar fashion.

5. Lemma. Let X and Y be $\sigma_2$-complete posets and let $\{f_n : n \geq 1\}$ be a monotonic increasing sequence of functions in $\mathbf{F}_2(X,Y)$. If $g(x) = \sup\{f_n(x) : n \geq 1\}$ then $g$ is $\sigma_2$-continuous.

Proof: Let $\{x_n : n \geq 1\}$ be a monotonic increasing sequence in X with $x^* = \sup\{x_n\}$. Consider the following relationships:

$$f_1(x_1) \leq f_2(x_1) \leq \cdots \leq f_n(x_1) \leq \cdots \leq g(x_1)$$

$$f_1(x_2) \leq f_2(x_2) \leq \cdots \leq f_n(x_2) \leq \cdots \leq g(x_2)$$

$$\vdots$$

$$f_1(x^*) \leq f_2(x^*) \leq \cdots \leq f_n(x^*) \leq \cdots \leq g(x^*) ,$$

$g$ is monotonic. [Let $x \leq y$. For each $n$ $f_n(y) \leq g(y)$. Since $\{f_n\}$ is monotonic $f_n(x) \leq f_n(y) \leq g(y)$. However $g(x) = \sup\{f_n(x) : n \geq 1\}$; therefore, $g(x) \leq g(y)$]. Since $g$ is monotonic increasing $g(x^*) = \sup\{g(x_n) : n \geq 1\}$; that is, $g$ is $\sigma_2$-continuous.//

6. Definition. $\frac{\delta F(x,y)}{\delta x} = \|F_y\|$ is the least fixed point of $F_y : X \to X$ such that $F_y(x) = F(x,y)$.

7. Example. Let $F : X \to X$ be defined by $F(x) = x$ $\frac{\delta F(x)}{\delta x} = \perp$.

8. Example. Let $F : X \to X$ where $F(x) = a$. As $a$ is the unique fixed point of $F$, $\frac{\delta F(x)}{\delta x} = a$.

9. Example. Let $F : X \to X$ where $F(x) = x^2 + a$. Let $y$ be any fixed point of $F$. Since $\perp \leq y$ and $F$ is $\sigma_i$-continuous $F^k(\perp) \leq F^k(y)$ for all $k$. Now $F(\perp) = a$, $F^2(\perp) = a^2 + a$, $F^3(\perp) = a^4 + a^3 + a^2 + a, \ldots, F^n(\perp)$ $= \sum_{j=1}^{2^{n-1}} a^j$. Thus $a^+ = \sup_n \left\{a^n : n > 0\right\} = \frac{\delta F(x)}{\delta x}$.

We shall primarily be interested in the case where $S_1$ and $S_2$ are $\sigma_i$-complete Boolean semirings of the form $S_1 = S^n$ and $S_2 = S^m$ and $F : S_1 \times S_2 \to S_1$ is $\sigma_i$-continuous. Notice if $u = \|F_y\|$ then $u = F_y(u)$; that is, $u$ is a solution of $x = F(x,y)$.

10. Theorem. Let $X$ and $Y$ be $\sigma_i$-complete posets $(i = 0,\ldots,3)$ and $F : X \times Y \to X$ be $\sigma_i$-continuous. If $g : Y \to X$ is defined by $g(y) = \frac{\delta F(x,y)}{\delta x}$ then $g$ is $\sigma_i$-continuous.

Proof: $g(y) = \frac{\delta F(x,y)}{\delta x} = \|F_y\| = \sup\left\{F_y^n(\perp) : n \geq 0\right\}$ [Theorem 2.14]. As usual we need only consider the case $i = 2$. Notice $F_y^2(\perp) = F_y[F_y(\perp)] = F_y[F(\perp, y)]$ $= F(F(\perp, y), y]$. This process is iterative. Let $\left\{y_n : n \geq 1\right\}$ be a monotonic increasing sequence and let $y^* = \sup\left\{y_n : n \geq 1\right\}$. We show first that $F_y^n(0)$ is $\sigma_2$-continuous. We know this is true for $n = 0$ on $n = 1$. Suppose $F_y^n$ is $\sigma_2$-continuous for $n = k$. $F_y^{k+1}(\perp) = F_y[F_y^k(\perp)] = F[F_y^k(\perp), y]$. Since $y^* = \sup\left\{y_n\right\}$ and $F$ is $\sigma_2$-continuous, $\sup\left\{F(\perp, y_n) : n \geq 1\right\}$ $= F(\perp, y^*)$. Let $v_n = F(\perp, y_n)$ then $\sup[F[F(\perp, y_n), y_n]$ $= \sup[F(v_n, y_n)] = F[F(\perp, y^*), y^*] = \sup\left\{F_{y_n}^2(\perp) : n \geq 0\right\}$ $= F_{y^*}^2(\perp)$ since $F(v_n, y_n)$ is a monotonic increasing sequence. Let $w_n = F_{y_n}^k(\perp)$. By the induction hypotheses $\left\{w_n : n \geq 1\right\}$ is monotonic increasing. Thus $\sup\left\{w_n : n \geq 1\right\} = \sup\left\{F_{y_n}^k(\perp) : n \geq 1\right\} = F_{y^*}^k(\perp) = w^*$. Now $\left\{(w_n, y_n) : n \geq 1\right\}$ is monotonic increasing sequence in $X \times Y$ and $\sup\left\{(w_n, y_n) : n \geq 1\right\} = (w^*, y^*)$. Therefore $\sup[F_{y_n}^{k+1}(\perp)] = \sup[F[F_{y_n}^k(\perp), y_n]] = \sup[F(w_n, y_n)]$ $= F(w^*, y^*) = F[F_{y^*}^k(\perp), y^*] = F_{y^*}^{k+1}(\perp)$. Therefore $F_y^n(\perp)$ is $\sigma_2$-continuous and $\left\{F_y^n(\perp)\right\}$ is monotonic increasing hence $g(y^*) = \sup[g(y_n)]$; that is $g$ is $\sigma_2$-continuous [Lemma 5].

11. Theorem (Lezczylowski). Let $X$ and $Y$ be $\sigma_i$-complete posets $(i = 0,\ldots,3)$ and $F : X\times Y \to X\times Y$ be $\sigma_i$-continuous. Let $(x^o,y^o) = \|F\|$, the least fixed point of $F$. Let $g(y) = \frac{\delta F_1}{\delta x}(x,y)$ $(y \in Y)$. Define $G : X\times Y \to X\times Y$ by $G(x,y) = (g(y),F_2(g(y),y))$ where $F(x,y) = (F_1(x,y),F_2(x,y))$. Then i) $\|G\| = \|F\|$, ii) and if $h(y) = F_2(g(y),y)$ then $\|h\| = y^o$ and iii) $g(y^o) = x_o$.

Proof: i) Let $(x^1,y^1) = \|G\|$, in particular we have $G(x^1,y^1) = (x^1,y^1) = (g(y^1), F_2(g(y^1),y^1))$. Therefore $x^1 = g(y^1)$ and $y^1 = F_2(g(y^1),y^1) = F_2(x^1,y^1)$. Since $g(y)$ is least fixed point of $F_1$ for all $y$, $F_1(g(y),y) = g(y)$. Therefore $x^1 = g(y^1) = F_1(g(y^1),y^1) = F_1(x^1,y^1)$. Consequently $F(x^1,y^1) = (F_1(x^1,y^1), F_2(x^1,y^1)) = (x^1,y^1)$. Since $(x^o,y^o) = \|F\|$, $(x^o,y^o) \le (x^1,y^1)$; that is $\|F\| \le \|G\|$. Conversely, $F(x^o,y^o) = (x^o,y^o)$. Hence $F_1(x^o,y^o) = x^o$ and $F_2(x^o,y^o) = y^o$. Now $x^o$ is a fixed point of $F_{y^o}$ thus $g(y^o) \le x^o$. Therefore $G(x^o,y^o) = (g(y^o), F_2(g(y^o),y^o)) = (g(y^o), F_2(x^o,y^o)) \le (x^o,y^o)$. Since $(\perp_X,\perp_Y) \le (x^o,y^o)$, $G(\perp_X,\perp_Y) \le G(x^o,y^o)$. Inductively $G^n(\perp_X,\perp_Y) \le (x^o,y^o$; that is

$\|G\| \leq (x^o, y^o) = \|F\|$. Thus $\|G\| = \|F\|$. ii) Define $h : Y \to Y$ by $h(y) = F_2(g(y), y)$. Observe $F_2(g(y^1), y^1) = y^1$. Hence $\|h\| \leq y^1$. Let $y^2 = \|h\|$ and $x^2 = g(y^2)$. $G(x^2, y^2) = (g(y^2), F_2(g(y^2), y^2) = (x^2, y^2)$ since $y^2$ is the least fixed point of h. Therefore $(x^1, y^1) \leq (x^2, y^2)$ and $y^1 \leq y^2 = \|h\|$ hence $y^o \leq y^2$ which implies $y^o = y^1 = \|h\|$. iii) Finally $g(y^o) = g(y^1) = x^1 = x^o$. //

12. Theorem. Let X be a $\sigma_i$-complete poset and $f, g : X \to X$ be $\sigma_i$-continuous. Define $h : X \times X \to X \times X$ by $h(x,y) = (g(y), f(x))$, then $\|h\| = (\|fg\|, \|gf\|)$ and h is $\sigma_i$-continuous.

Proof: Let $\{(x_n, y_n) : n \geq 0\}$ be a monotone non-decreasing sequence in $X \times X$. If $(u,v) = \sup\{(x_n, y_n)\}$ then $u = \sup\{x_n\}$ and $v = \sup\{y_n\}$. Now

$$\sup\{h(x_n, y_n) = \sup\{g(y_n), f(x_n)\}$$

$$= \sup\{g(y_n, f(x_n)\}$$

$$= (\sup\{g(y_n)\}, \sup\{f(x_n)\})$$

$$= (g(\sup\{y_n\}), f(\sup\{x_n\}))$$

$$= (g(v), f(u)) = h(u,v) = h[\sup\{(x_n, y_n)\}];$$

that is $h$ is $\sigma_i$-continuous. Recall $fg(x) = g[f(x)]$ and $\|h\| = \sup\{h^n(\bot,\bot) : n \geq 0\}$ and $h^0(\bot,\bot) = (\bot,\bot)$. Straightforward calculations yield $h^{2n}(\bot,\bot) = ((fg)^n(\bot), (gf)^n(\bot))$ and $h^{2n+1}(\bot,\bot) = ((gf)^n g(\bot), (fg)^n f(\bot))$. Since composition of $\sigma_i$-continuous functions is continuous $\bot \leq (fg)(\bot) \leq \ldots \leq (fg)^n(\bot)$ and $\bot \leq (gf)(\bot) \leq \ldots \leq (gf)^n(\bot) \ldots$ [Lemma 2.27]. Considering only the even powers of $h$ with the first and second coordinates, Lemma 24 yields $\|h\| = (\|fg\|, \|gf\|)$. //

13. Lemma. Let $S$ be a $\sigma_o$-complete Boolean semiring with $a,b \in S$. The least $u$ satisfying $au + b \leq u$ is $a^*b$.

[Let $g(x) = (a+1)x + b$. We know $\|g\| = (a+1)^*b$ [Lemma 2.18]. Let $c = (a+1)^*$. Then $(a+1)c + b = ac + c + b = c$. Hence $ac + b \leq c$. Choose $u$ such that $au + b \leq u$. Equivalently $au + u + b = u$. Applying the distributive law we have $(a+1)u + b = u$. Hence $u$ is a fixed point of $g$. Therefore $c \leq u$. Thus $cb = (a+1)^*b$ is least point satisfying $au + b \leq u$. However $(a+1)^* = a^*$ [Lemma 2.39]].

## IV. FORMAL LANGUAGES

1. Definition. Let X be a set. A formal language on X is any subset of $X^* = \bigcup_{r \geq 0} \{X^r\}$.

Recall $X^*$ under concatenation is the free monoid, $M_F(X)$, [Definition 1.10]. Moreover if $X = \emptyset$ then $X^0 = \{\varepsilon\}$ but $X^r = \emptyset$ for $r > 0$. X is the alphabet of the formal language $\mathcal{L}(X) \subset X^*$. In an attempt to abstract the essence of natural language in order to make their study applicable to computer technology, N. Chomsky developed a theory of phrase structured or generative grammars (1963-1968). ALGOL was the first computer language developed using this theory of formal language.

2. Definition. A phrase structured grammar, P.S.G., consists of

i) a nonempty set V, the vocabulary, such that $V = V_N \cup V_T$, $V_N \cap V_T = \emptyset$, $V_N \neq \emptyset$, $V_T \neq \emptyset$. $V_N$ is called the nonterminal set and $V_T$ the terminal set.

ii) a finite sequence of ordered pairs $(\mu, \nu)$ in $V^* \times V^*$ called productions such that $\mu \in V^+ \sim V_T^*$; that is at least one element of $V_N$ is embedded in $\mu$.

iii) There exists $S \in V_N$ designated as the initial or start symbol.

The sequence of production $\left\{(\mu,\nu)_n\right\}_{n=1}^{k}$ is often designated by $\mathbb{P} = \left\{P_1,\ldots,P_k\right\}$. $\mu$ is said to produce $\nu$ if there exists $P \in \mathbb{P}$ with $P \equiv (\mu,\nu)$. This is also written in a functional notation as $P : \mu \rightarrow \nu$. The phrase structured grammar, G, may then be identified as the ordered quadtriple $\left\{V_N, V_T, \mathbb{P}, S\right\}$.

3. Example. $V_N = \left\{a,b\right\}$, $V_T = \left\{A,B\right\}$, $S = b$ and $P_1 : a \rightarrow A$, $P_2 : S \rightarrow B$, $P_3 : S \rightarrow aS$ and $P_4 : S \rightarrow B$. G then generates $\left\{A^nB : n \geq 0\right\}$.

For G a phrase structured grammar, the language generated by G is defined to be $L(G) = \left\{\beta : \beta \in V_T^*, S \rightarrow^* \beta\right\}$.

4. Definition. Let X be a set and $(\mu,\nu) \in X^* \times X^*$ such that $\mu \neq \varepsilon$. Define $P_{(\mu,\nu)} \in \mathbb{R}_{\mathbb{P}}(X^*)$ by $(\alpha,\beta) \in P_{(\mu,\nu)}$ of there exist $(\alpha_1,\alpha_2) \in X^* \times X^*$ such that $\alpha = \alpha_1 \mu \alpha_2$ and $\beta = \alpha_1 \nu \alpha_2$. $P_{(\mu,\nu)}$ is the production determined by $(\mu,\nu)$.

Alternately we use the notation $\alpha P_{(\mu,\nu)} \beta$ for $(\alpha,\beta) \in P_{(\mu,\nu)}$ and $\mu \rightarrow \nu$ for the pair $(\mu,\nu)$. Recall

$\varepsilon$ is the null or empty sequence. With respect to $\mathbf{R}_{\mathbb{P}}^{*}$ we have $(\mu, \nu) \in \mathbf{R}_{\mathbb{P}}^{*}$ if $\mu \to^{*} \nu$.

5. Definition. Let $\mathbb{P} = \left\{P_{(\mu,\nu)_1}, \ldots, P_{(\mu,\nu)_k}\right\}$ be a finite set of productions on X. $(X, \mathbb{P})$ is a generalized grammar on X determined by $\mathbb{P}$.

6. Definition. Let $(x,y) \in X^{*} \times X^{*}$. x derives y if there exists $P \in \mathbb{P}^{*}$ such that $xPy$; that is there exists $\left\{P_{(\mu,\nu)_{i_j}} \in \mathbb{P} : j = 1, \ldots, r\right\}$ and $\left\{x_1, \ldots, x_{r-1}\right\}$ $\in X^{*}$ such that

$$
\begin{gathered}
x \; P_{(\mu,\nu)_{i_1}} x_1 \\
x_1 \; P(\mu,\nu)_{i_2} x_2 \\
\vdots \\
x_{r-1} P(\mu,\nu)_{i_r} y \; .
\end{gathered}
$$

7. Definition. Let $R \subset A \times B$ be a relation. For $A' \subset A$ define $R[A'] = \left\{b : \text{there exists } a \in A' \text{ with } (a,b) \in R\right\}$.

8. Definition. The language generated by a formal grammar G is defined to be $\mathcal{L}(G) = \mathbf{R}_{\mathbb{P}}[\{S\}] \cap T^{*} \subseteq T^{*}$.

9. Definition. Let G and G' be formal grammars with the same set of terminal elements $X_1 = N_1 \cup T$ $G = (N_1, T, \mathbb{P}_1, S_1)$ and $X_2 = N_2 \cup T$, $G' = (N_2, T, \mathbb{P}_2, S_2)$ G and G' are equivalent grammars if $\mathcal{L}(G) = \mathcal{L}(G')$.

10. Definition. Let $\alpha \in X^*$ define the cardinality of $\alpha$ as

$$|\alpha| = \left\{ \begin{array}{ll} n & \text{if } \alpha = x_1, \ldots, x_n (x_i \in X) \\ 0 & \text{if } \alpha = \varepsilon \end{array} \right. . \}$$

11. Definition. G is a contextfree grammar, CFG, if and only if for each production $(\alpha, \beta) \in \mathbb{P} = \mathbb{R}_{\mathbb{P}}(X^*)$ $\text{card}(\alpha) = 1$. This assures that $\alpha$ is a single element of $V_N$.

12. A language $L \subset T^*$ is called contextfree if there exists a contextfree grammar G such that $L = \mathcal{L}(G)$.

13. Theorem. Given a contextfree grammar $G = (N, T, \mathbb{P}, S)$, there exists an equivalent context $G' = (N', T, \mathbb{P}', S)$ such that for each $(\alpha, \beta) \in \mathbb{P}'$ either $\beta \in N'^*$ or $|\beta| = 1$ and $\beta \in T$.

Proof: Let $N_T = \{N\} \times T$. Clearly $N_T \cap N = \emptyset = N_T \cap T$. For each $a \in T$ let $x_a = (N, a)$. Let $N' = N \cup N_T$. On a free monoid a homomorphism defined only on the generators may be generalized to the entire monoid through concatenation. Define a homomorphism $h : (N \cup T)^* \to N'^*$ by $h(x) = \{x : \text{if } x \in N\}$ and $h(a) = x_a = (N, a)$ for $a \in T$. Define $\mathbb{P}'$ by $\mathbb{P}' = \{\alpha \to h(B) : \alpha \to \beta \in \mathbb{P}\} \cup \{x_a \to a : a \in T\}$. The equivalence of G and G' may be accomplished by replacing every terminal a by $x_a$. Thus every production in G will also be a production in G', since the last step will be a string of terminals. Moreover if $(\alpha,\beta) \in \mathbb{P}'$ is in $\mathbb{P}$ then $\beta \in (N \cup N_T)^* = N'^*$; otherwise $(\alpha,\beta) = (x_a, a)$ and $|B| = 1$ and $\beta = a \in T$. //

14. Theorem (Shelion-Grenbach). Given G a context free grammar $G = (N,T,\mathbb{P},S)$ there exists an equivalent context free grammar $G' = (N',T,P',S)$ such that for each $(\alpha,\beta) \in \mathbb{P}'$ either $\beta = a\beta'$ where $a \in T$ and $\beta' \in N'^*$ or $\beta \in T$ or $\beta = \varepsilon$.

Theorems of this type are used in parsing a language.

15. Example. Let $T = \{1\}$, $N = \{S\}$, $\mathbb{P} = \{S \to S11, S \to 11\}$ $L(G) = \{\gamma : \gamma \in T^* \text{ and } S \xrightarrow{*} \gamma\}$ consists of strings containing pairs of ones.

16. Definition. Let S be a Boolean semiring. A binary relation $\theta$ on S is admissible if $\theta$ is an equivalence relation on S and for $x, y, u, v \in S$ if $x\theta u$ and $y\theta v$ then $x + y\theta u + v$ and $xy\theta\, uv$.

17. Definition. $[x]_\theta = \{y : x\theta y\}$ and $S/\theta = \{[x]_\theta : x \in S\}$.

As usual we define $[x]_\theta + [y]_\theta = [x+y]_\theta$ and $[x]_\theta \bullet [y]_\theta = [xy]_\theta$. With respect to formal languages we identify the multiplicative identity 1 with $\{\varepsilon\}$ and the additive identity 0 with $\emptyset$.

18. Theorem. $S/\theta$ is a Boolean semiring [Observe $[x]_\theta + [0]_\theta = [x+0]_\theta = [x+0]_\theta = [x]_\theta = [0+x]_\theta = [0]_\theta + [x]_\theta$; that is $[0]_\theta$ is the additive identity. Similar calculations yield that $[1]_\theta$ is the multiplicative identity. That + and $\cdot$ are associative over $S/\theta$ is a direct consequence of the associativity of + and $\cdot$ over S. Since S is a Boolean semiring $[a]_\theta + [a]_\theta = [a+a]_\theta = [a]_\theta$. The remaining requirement [Definition 1-20] for $S/\theta$ to be a semiring are straightforward using the fact that S is a Boolean semiring.]

19. Definition. Let $S$ be $\sigma_2$-complete Boolean semiring and $\theta$ an admissible relation on $S$. $\theta$ is $\sigma_2$-compatible if given monotonic sequences $\{x_n\}$ and $\{u_n\}$ $(n \geq 1)$ in $S$ with $x_n \; \theta \; u_n$ for all $n$ then $x \; \theta \; u$ where $x = \sup\{x_n\}$ and $\mu = \sup\{u_n\}$.

20. Lemma. Let $S$ be a Boolean semiring and $\theta$ an admissible relation on $S$. If $x \leq y$ then $[x]_\theta \leq [y]_\theta$ [ $x \leq y$ if and only if $x + y = y$]. Since $\theta$ is admissible $[x+y]_\theta = [y]_\theta = [x]_\theta + [y]_\theta$. Therefore $[x]_\theta \leq [y]_\theta$. ▯

21. Definition. Let $S$ be a Boolean semiring. $G^n(S)$ is the set of $n \times n$ matrices with entries in $S$. $G^n(S)$ has the standard matrix operations of addition and multiplication.

The usual computations, based on $S$ being a Boolean semiring, show that $G^n(S)$ is also a semiring. Since $a + a = a$ for all $a \in S$, $A + A = A$ for all $A \in G^n(S)$. Thus we have

22. Lemma. If $S$ is a Boolean semiring then $G^n(S)$ is a Boolean semiring.

23. Definition. For $A, B \in G^n(S)$, $A \leq B$ if $a_{i,j} \leq b_{i,j}$ $(1 \leq i,\ j \leq n)$.

24. Theorem. If $S$ is a $\sigma_i$-complete Boolean semiring then $G^n(S)$ is $\sigma_i$-complete $(i = 0,\ldots,3)$.

[Let $A^k$ be a countable subset of $G^n(S)$. $A^k = (a^k_{ij})$. For each pair $p,q$ $\{a^k_{p,q}\}$ is a countable subset of $S$. Let $a_{p,q} = \sup_k\{a^k_{p,q}\}$. Then $A = (a_{p,q})$ is an upper bound for $\{A^k\}$. Let $B$ be an upper bound of $A^k$ then $b_{p,q}$ is an upper bound for $\{A^k\}$. Let $B$ be an upper bound for $A^k$ then $b_{p,q}$ is an upper bound for $\{a^k_{p,q}\}$. Since $a_{p,q} = \sup_k\{a^k_{p,q}\}$, $a_{p,q} \leq b_{p,q}$. Thus $A \leq B$ and $A = \sup_k\{A^k\}$.]

25. Lemma. Let $F : G^n(S) \to G^n(S)$ be defined by $F(X) = A(X) + C$ then $\|F\| = A^*C$.

[This is a special case of Lemma 2.18] Recall if $S$ is $\sigma_i$-complete Boolean semiring then $+$ and $\cdot$ are $\sigma_i$-continuous over $S$. Hence matrix multiplication and matrix addition are $\sigma_i$-continuous over $G^n(S)$]

26. Definition. Let $\mathfrak{L}^{p,q}(S)$ be the set of matrices with entries in $S$. In particular $G^n(S) = \mathfrak{L}^{nn}(S)$.

In general $\mathcal{L}^{p,q}(S)$ is not a semiring for matrix multiplication need not be defined unless $p = q$. However $\mathcal{L}^{p,q}(S)$ can be embedded in a minimal semiring $G^n(S)$ where $n = \max(p,q)$.

27. Definition. Let $A \in \mathcal{L}^{p,q}(S)$ and $n = \max(p,q)$. Let

$$\hat{A} = (\hat{a}_{jk}) = \begin{cases} a_{jk} & \text{if } j,k \leq n \\ 0 & \text{otherwise} \end{cases} .$$

$\hat{A}$ is the extension of $A$ to $G^n(S)$ and we may identify $A$ and $\hat{A}$.

28. Definition. Let $X$ and $Y$ be posets and $f : X \to Y$. $f$ is $\sigma_i$-continuous if

i) there exists $\sigma_i$-complete Boolean semiring $S_1$ and $S_2$ such that $X$ is embedded in $S_1$ and $Y$ is embedded in $S_2$.

ii) there exists a $\sigma_i$-continuous function $F : S_1 \to S_2$ such that $F|_X = f$.

29. Lemma: Let $S$ be a $\sigma_i$-complete Boolean semiring. Let $f : \mathcal{L}^{p,q}(S) \times \mathcal{L}^{q,r}(S) \to \mathcal{L}^{pr}(S)$ be defined by $f(A,B) = AB$ then $f$ is $\sigma_i$-continuous. [Let $n = \max(p,q,r)$ and $S_1 = G^n(S) \times G^n(S)$ and $S_2 = G^n(S)$.

$F : S_1 \to S_2$ is $\sigma_i$-continuous as matrix multiplication and addition are $\sigma_i$-continuous over $G^n(S)$. $F(\hat{A},\hat{B}) = f(A,B)$]

30. Lemma: Let $A \in G^n(S)$ and $X, C \in \mathcal{X}^{n,1}(S)$ and $f : \mathcal{X}^{n,1} \to \mathcal{X}^{n,1}$ be defined by $f(X) = AX + C$ then $f$ is $\sigma_i$-continuous.

[Let $S_1 = S_2 = G^n(S)$ and $F(\hat{X}) = A\hat{X} + \hat{C}$ for $X$ and $C \in \mathcal{X}^{n,1}$.

$F$ is $\sigma_i$-continuous as the composition of $\sigma_i$-continuous function and $F|_{\mathcal{X}^{n-1}(S)} = f$ since $\hat{X} \equiv X$].

31. Corollary. Let $f : \mathcal{X}^{n,1}(S) \to {}^{n,1}(S)$ be defined by $f(X) = AX + C$ for $X, C \in \mathcal{X}^{n,1}(S)$ and $A \in G^n(S)$, then $\|f\| = A^*C$.

[Extend $f$ to $F : G^n(S) \to G^n(S)$ in the usual manner $f(X) = AX + C = A\hat{X} + \hat{C} = F(\hat{X})$. $\|F\| = A^*C$ [Lemma 25]. Thus $\|f\| = A^*C$ as $\hat{C}$ is identifiable with C.]

32. Example. Let S be a $\sigma_i$-complete Boolean semiring $(i = 0,\ldots,2)$ and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G^2(S)$ then

$$A^* = B = \begin{pmatrix} (a+bd^*c)^* & a^*b(ca^*b+d)^* \\ d^*c(a+bd^*c)^* & (ca^*b+d)^* \end{pmatrix}$$

$A^* = I + AA^*$. Let $\begin{pmatrix} e & f \\ g & h \end{pmatrix} = A^*$

$$\begin{pmatrix} e & g \\ g & h \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

Thus

$$e = 1 + ac + bg \qquad f = af + bh$$

$$g = ce + dg \qquad h = 1 + cf + dh\ .$$

Recall the least fixed point of $x \to ax + b = a^*b$ and the least fixed point of $x \to xa + b = ba^*$. Also $+$ is commutative. Therefore

i) $a^*bh \leq f$

ii) $d^*ce \leq g$ .

Using i we obtain

$$e = 1 + ae + bg \geq 1 + ae + b(d^*ce)$$

Thus

$$e \geq 1 + (a+bd^*c)e$$

by distributivity and

$$e \geq (a+bd^*c)^*.$$

Using ii we obtain

$$g \geq d^*ce \geq d^*c(a+bd^*c)^*$$

equivalently

$$d^*c(a+bd^*c)^* \leq g \ .$$

Similarly since $h = 1 + cf + dh$ and substituting for $f$ we obtain $h \geq 1 + ca^*bh + dh = 1 + (ca^*b+d)h$. By fixed point theory $h \geq (ca^*b+d)^*$ and therefore $a^*b(ca^*b+d)^* \leq a^*bh \leq f$. Hence $A^* \geq B$. Consider equation $I + AB$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} (a+bd^*c)^* & a^*b(ca^*b+d)^* \\ d^*c(a+bd^*c)^* & (ca^*b+d)^* \end{pmatrix}$$

$$= \begin{pmatrix} 1+a(a+bd^*c)^*+bd^*c(a+bd^*a)^* & aa^*b(ca^*b+d)^*+b(ca^*b+a)^* \\ c(a+bd^*c)^*+dd^*c(a+bd^*c)^* & 1^*ca^*b(ca^*b+d)^*+d(ca^*b+d)^* \end{pmatrix}$$

$$= \begin{pmatrix} 1+(a+bd^*c)(a+bd^*c)^* & (aa^*+1)b(ca^*b+d)^* \\ (1+dd^*)c(a+bd^*c)^* & 1+(ca^*b+d)(ca^*b+d)^* \end{pmatrix}$$

Since $u^* = 1 + uu^*$ this reduces to

$$\begin{pmatrix} (a+bd^*c)^* & a^*b(ca^*b+d)^* \\ d^*c(a+bd^*c)^* & (ca^*b+d)^* \end{pmatrix}$$

$$= B \ .$$

Thus B is in fixed point hence we must have $B \geq A^*$. Hence $A^* = B$.

33. Definition. Let S be a Boolean semiring. For $n \geq 1$, $F^n(S) = \left\{g : g : S^n \to S\right\}$.

34. Definition. $R_o^n = \left\{g : g \in F^n(S)\right.$ such that g is constant. For $m \geq 0$ $R_{m+1}^n = \left\{f : f = g_1+g_2,\ f = g_1g_2,\right.$ $\left. f = g_1^* \text{ where } g_1, g_2 \in R_m^n\right\}$ $g_1^*(x_1,\ldots,x_n) = g_1(x_1,\ldots,x_n)^*$ Observe $R_m^n < R_{m+1}^n$ $(m \geq 0)$.

35. Definition. $R^n(S) = \cup \left\{R_m^n(S) : m > 0\right\}$.

36. Definition. Let S be a $\sigma_i$-complete Boolean semiring $(i = 0,\ldots,3)$, $A \subset S$ and $a \in S$. a is regular over A of these exists an $n \geq 1$ and an $f \in R^n$, $b_1,\ldots,b_n \in A$ such that $a = f\,(b_1,\ldots,b_n)$.

37. Definition. $A^R = \left\{a : a \text{ is regular over } A\right\}$. Notice $A^R \subseteq S$.

38. Definition. A is a regular base for S if $A^R = S$.

39. Lemma. If S is a $\sigma_i$-complete Boolean semiring then $A^R$ is a $\sigma_i$-complete subsemiring of S.

[Notice if $f \in R^n$ then $F : S^{n+k} \to S$ defined by $F(b_1,\ldots,b_n,b_{n+1},\ldots,b_{n+k}) = f(b_1,\ldots,b_n) \in R^{n+k}$. For $a_1$ and $a_2 \in A^R$ there exist $f \in R^n$ and $g \in R^k$ such that

$$
\begin{aligned}
a_1 + a_2 &= f(b_1,\ldots,b_n) + g(c_1,\ldots,c_k) \\
&= F(b_1,\ldots,b_n,b_{n+1},\ldots,b_{n+k}) \\
&\qquad + G(c_1,\ldots,c_k,c_{k+1},\ldots,c_{k+n}) \\
&= H(d_1,\ldots,d_{n+k})
\end{aligned}
$$

since $R^{n+k}$ is closed under +. Thus $A^R$ is closed under addition. A semilar argument shows $A^R$ to be closed under multiplication. The remaining properties of $A^R$ be a semiring follow from S being a semiring. To show completeness let k be a countable subset of $A^R$. Since S is $\sigma_i$-complete there exists a $k \in S$ such that $k = \sup_S K$. Hence $g_1^*(K) = g_1(K^*) = g_1(k)$ hence $k \in A^R$.]

BIBLIOGRAPHY


1. A. Blikle, Equations in a space language. CCPAS Reports 43, Computation Center, Polish Academy of Sciences, Warsaw, 1971.

2. A. Blikle, Equational languages. Computation Center, Polish Academy of Sciences, Warsaw, 1972.

3. D. Rosenkrantz, Matrix equations and normal forms for context-free grammars. Journal of Association for Computing Machinery, vol 14.3, 1967.

4. A. Salomad, Formal languages. Academic Press, 1973.

## VITA

Catherine L. Madden, daughter of Mrs. Catherine Madden, was born in Philadelphia, Pennsylvania on July 25, 1944. She received a Bachelor of Arts degree in mathematics from D'Youville College, Buffalo, New York, 1966.

A Master of Arts in mathematics from Villanova University, Villanova, Pennsylvania was conferred in 1970 and a Doctor of Philosophy in mathematics from Lehigh University was conferred in 1978.

Currently she is a member of the Technical Staff of Bell Telephone Laboratory, Piscataway, New Jersey.