Vol. 44 No. SIG 4(PRO 17) IPSJ Transactions on Programming Mar. 2003

Regular Paper

Essentially Algebraic Structure for Kleene Algebra with Tests and Its Application to Semantics of While Programs

Hitoshi Furusawa† and Yoshiki Kinoshita†

Kozen and Smith showed existence of Kleene algebra with tests freely generated by a pair (B, Σ) of finite sets. Their key idea is the construction of Kleene algebra $\mathcal{P}_{B,\Sigma}$ with tests. We show existence of free algebra without assuming the finiteness of B and Σ. Moreover, we give a construction of Kleene algebra $\mathcal{Q}_{B,\Sigma}$ with tests for any sets B and Σ, and show that whenever $\mathcal{P}_{B,\Sigma}$ is defined (that is, whenever B is finite), $\mathcal{Q}_{B,\Sigma}$ is isomorphic to $\mathcal{P}_{B,\Sigma}$. We use $\mathcal{Q}_{B,\Sigma}$ in an interpretation of **while** programs and we argue that it is really an interpretation by sets of runs.

1. Introduction

Kozen[12] introduced Kleene algebra with tests and applied it to algebraic semantics of **while** programs. Later, Kozen and Smith[10] showed existence of the free Kleene algebra with tests generated by a pair (B, Σ) of finite sets using universal algebraic technique. Given a pair (B, Σ) of a finite sets, they gave an explicit construction of a Kleene algebra with tests $\mathcal{P}_{B,\Sigma}$ and showed that an image under a canonical homomorphism into $\mathcal{P}_{B,\Sigma}$ is freely generated by (B, Σ).

Kozen and Smith's construction of free algebra is valid only for finite B's because $\mathcal{P}_{B,\Sigma}$ is defined only for such. In fact, they also assumed Σ is finite but that is not necessary.

We shall first show that the finiteness condition, however, is not necessary at all because the structure for Kleene algebra with tests can be described by a finite limit sketch (FL sketch) in the sense of Barr and Wells[1),2)]. An algebra freely generated by any pair (B, Σ) of sets exists; B and Σ do not have to be finite. We already reported this result[7),8)] but we shall present it more in detail here.

We shall also study $\mathcal{P}_{B,\Sigma}$, which plays the same role as Lang(A), the Kleene algebra consisting of the set of words over A, does in the theory of Kleene algebra and regular expressions. The definition of $\mathcal{P}_{B,\Sigma}$, however, is quite involved and it would be natural to ask why such a construction works. To give a (partial, at least) answer to this question, we provide another Kleene algebra with tests $\mathcal{Q}_{B,\Sigma}$ for any pair (B, Σ) of (not necessarily finite) sets and we shall show that $\mathcal{Q}_{B,\Sigma}$ is isomorphic to $\mathcal{P}_{B,\Sigma}$, whenever the latter is defined; note that $\mathcal{P}_{B,\Sigma}$ is not defined for infinite B. Moreover, $\mathcal{Q}_{B,\Sigma}$ is given by means of standard constructions such as coproducts and adjunctions from a pair (B, Σ) of sets.

We introduce the notion of **while** algebra[9)] as an algebraic structure for **while** programs and develop functorial semantics of **while** programs in arbitrary **while** algebras. Then we construct a faithful functor $\mathcal{I}$ from the category **Kat** of Kleene algebras with tests to the category **While** of **while** algebras so that **while** programs are interpreted in a Kleene algebra with tests. Specifically, an interpretation in $\mathcal{Q}_{B,\Sigma}$ is a semantics by sets of runs.

2. FL Sketch

We shall give an overview of FL sketch following Barr and Wells[1),2)], to the extent we need in the rest of this paper.

Definition 2.1 A **reflexive graph** G consists of a pair of sets G_0, G_1 together with three functions $\mathrm{src}, \mathrm{tgt}\colon \mathrm{G_1} \to \mathrm{G_0}$, $\mathrm{i}\colon \mathrm{G_0} \to \mathrm{G_1}$ satisfying $\mathrm{src} \circ \mathrm{i} = \mathrm{tgt} \circ \mathrm{i} = \mathrm{id}_{\mathrm{G_0}}$. Elements in G_0, G_1 are called **nodes** and **edges**, respectively. Functions src, tgt, and i are called **source** function, **target** function, and **loop** function. Reflexive graphs are two sorted algebra with three operations and two equational constraints. A **homomorphism** of reflexive graphs is defined to be a homomorphism of two sorted algebras. In the sequel, we mean reflexive graphs by writing "graphs".

Definition 2.2 Let H and G be reflexive graphs. A **diagram** in G of **shape** H is a homomorphism $D\colon H \to G$ of reflexive graphs. D is called a **commutative diagram** if H has

† C.R.T. of Informatics, AIST

two distinguished nodes s and d, two paths from s to d, and all edges are part of either paths. If H is equipped with one distinguished node p and a family of edges $P = (\, P_x\colon p \to x \mid x \in H_0 \setminus \{\, p\,\}\,)$, and, for each edge f which is not in the image of P, neither the source nor target is p, the triple $(D\colon H \to G, p, P)$ is called a **cone** in G of **shape** H. The image $D(p)$ of the distinguished node p is called the **pivot** of the cone and $D(P_x)$ is called its **projection** to $D(x)$. If each edge of H is either a projection or loop, the cone is called **discrete**.

If H is finite, the diagram $D\colon H \to G$ is called a **finite diagram**. Similarly we use terms such as finite commutative diagrams, finite cones and so on.

Definition 2.3 An **FL sketch** (finite limit sketch) S is a triple (G, C, Γ) of a reflexive graph G, a set of commutative diagrams C, a set of finite cones Γ. Edges of G are called **operators** in S.

Definition 2.4 Let $f\colon a \to b$ be an operator in an FL sketch $S = (G, C, \Gamma)$. If Γ contains a discrete cone $(\gamma\colon H \to G, p, P)$ for which P takes p to a and all other nodes to b, f is called an n**-ary operator** on b in S, where n is the number of elements of $H_0 \setminus \{\, p\,\}$.

The arity is in general not uniquely determined since an operator can be 4-ary and 5-ary at the same time, for instance. We shall use the term "arity" for convenience, although it is not well-established notion.

If M is a model M of S, the following definition of models forces $M(a)$ to be an n-fold product of $M(b)$ and $M(f)$ to be a function $M(f)\colon M(b)^n \to M(b)$.

Definition 2.5 Let $S = (G, C, \Gamma)$ be an FL sketch. A reflexive graph homomorphism M from G to the underlying reflexive graph of the category **Set** is called a **model** of S if the following conditions hold: for each node a of G, M takes the loop i(a) to the identity map on $M(a)$; for each commutative diagram D in C, $M(D(f_n)) \circ \cdots \circ M(D(f_1)) \circ M(D(f_0)) = M(D(g_m)) \circ \cdots \circ M(D(g_1)) \circ M(D(g_0))$, where $f_0 f_1 \cdots f_n$ and $g_0 g_1 \cdots g_m$ are the two distinguished paths of D; and for each cone γ in Γ, $M \circ \gamma$ is a limit cone in **Set**. A **homomorphism** α from M to M' is a G_0-indexed family of maps $(\alpha_x \in \mathbf{Set}(M(x), M(x')) \mid x \in G_0)$ which satisfies $M'(f)\alpha_x = \alpha_y M(f)$ for each edge $f\colon x \to y$ of G. The models of an FL sketch S and homomorphisms between them give rise to a category which we shall denote by $\mathbf{Mod}(S)$.

By replacing **Set** above by any category Z with finite limits, we obtain a more general definition of models, but we shall use only models in **Set**, so the above definition suffices.

Example 2.6 Consider an FL sketch **2** whose graph has exactly two nodes 0 and 1 and all edges are loops, which has no commutative diagrams and no cones. It is obvious that $\mathbf{Mod}(\mathbf{2})$ is isomorphic to $\mathbf{Set} \times \mathbf{Set}$.

Definition 2.7 A category C is **FL sketchable** if there exists an FL sketch, category of whose models is equivalent to C.

Barr[3] has shown the following theorem which tells us the relationship between logical presentation and FL sketches.

Theorem 2.8 (Barr[3]) The category of models of a equational Horn theory is FL sketchable.

Definition 2.9 let $S = (G, C, \Gamma)$ and $S' = (G', C', \Gamma')$ be FL sketches. A **morphism** $h\colon S \to S'$ of FL sketches is a reflexive graph homomorphism which takes commutative diagrams and cones in G to commutative diagrams and cones in G', respectively, i.e., $h \circ D \in C'$ for each $D \in C$ and $h \circ \gamma \in \Gamma'$ for each $\gamma \in \Gamma$.

The following theorem appears in Barr and Wells[1]. See also Gray[4].

Theorem 2.10 If $h\colon S \to T$ is a morphism of FL sketches, then a functor $h^*\colon \mathbf{Mod}(T) \to \mathbf{Mod}(S)$ given by composing each model of T with h has a left adjoint $h_\sharp\colon \mathbf{Mod}(S) \to \mathbf{Mod}(T)$.

3. Kleene Algebra

The following definition is classical.

Definition 3.1 A **semiring** is a set S equipped with nullary operators 0, 1 and binary operators $+$, $\cdot$, subject to the following conditions.

(1) $(S, 0, +)$ is a commutative monoid.

(2) $(S, 1, \cdot)$ is a monoid.

(3) The operator $\cdot$ distributes over $+$ on both sides, i.e.,

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{and}$$
$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

(4) $x \cdot 0 = 0 = 0 \cdot x$.

A semiring is said to be **idempotent** if $+$ satisfies the law of idempotency $x + x = x$.

Remark 3.2 An idempotent commutative monoid is a semilattice. It is well-known that, in a semilattice, a partial oder $\leq$ is induced from the binary operator by

$$x \leq y \iff x + y = y.$$

In the sequel, the partial order $\leq$ shall be used in this sense.

Definition 3.3 (Kozen [11]) A **Kleene algebra** is a tuple $(K, 0, 1, +, \cdot, ^*)$, where $(K, 0, 1, +, \cdot)$ is an idempotent semiring, * is a unary operator on K which satisfies the following:

$$1 + (p \cdot p^*) = p^*$$
$$1 + (p^* \cdot p) = p^*$$
$$q + (p \cdot r) \leq r \Longrightarrow p^* \cdot q \leq r$$
$$q + (r \cdot p) \leq r \Longrightarrow q \cdot p^* \leq r$$

Kleene algebras, Boolean algebras, and idempotent semirings can be axiomatized by equational Horn theory (in fact, all except for the first can be axiomatized by equational theory!), so, the categories of these algebras are all FL sketchable by Theorem 2.8. For instance, the FL sketch KLEENE $= (G, C, \Gamma)$ for Kleene algebras may be defined in the following way. G has one distinguished node a. It has two nullary operators (in the sense of Definition 2.4) 0 and 1, one unary operator * and two binary operators $+$ and $\cdot$. The diagrams in C and Γ are determined by these arity conditions and Horn clause axioms, in the way described by Barr[3].

4. Kleene Algebra with Tests

Kozen [12] defined Kleene algebra with tests as a Kleene algebra whose base set includes Boolean algebra, sharing the addition and multiplication. The inclusion requirement, however, is rarely used in application, so we define Kleene algebra with tests as follows.

Definition 4.1 A **Kleene algebra with tests** is a triple $(\mathbf{B} \xrightarrow{j} \mathbf{K})$, where $\mathbf{B} = (B, 0_B, 1_B, +_B, \cdot_B, \neg)$ is a Boolean algebra, $\mathbf{K} = (K, 0_K, 1_K, +_K, \cdot_K, ^*)$ is a Kleene algebra, and j: $B \to K$ is a map from B to K which preserves 0, 1, + and $\cdot$. Elements of K are called **commands**, elements of B are called **tests**.
Kozen's Kleene algebra with tests is a special case where j is an inclusion.

We shall denote by **Kat** the category of Kleene algebras with tests and their homomorphisms. Kleene algebras with tests are axiomatized by an equational Horn clause, so an FL Sketch KAT for **Kat** exists by Theorem 2.8.

KAT may be described as follows. The reflexive graph of KAT has two distinct nodes B and K. B has two nullary operators 0_B, 1_B, a unary operator $\neg$ and two binary operators $+_B, \cdot_B$. There are commutative diagrams and cones which make $(B, 0, 1, \neg, +_B, \cdot_B)$ axiomatize a Boolean algebra. K has two nullary operators 0_K, 1_K, a unary operator * and two binary operators $+_K$, $\cdot_K$. There are commutative diagrams and cones which make $(K, 0, 1, ^*, +_K, \cdot_K)$ axiomatize a Kleene algebra. Finally, there are commutative diagrams which express that j preserves 0, 1, + and $\cdot$.

We define the notion of free Kleene algebra with tests by means of the forgetful functor $\mathbf{Kat} \to \mathbf{Set} \times \mathbf{Set}$.

Definition 4.2 A **free Kleene algebra with tests** generated by a pair (B, Σ) of sets B and Σ is defined to be a Kleene algebra with tests $F(B, \Sigma) = (\mathbf{B} \xrightarrow{j} \mathbf{K})$ and a map η_B: $B \to B_0$ from B to the base set B_0 of $\mathbf{B}$, map η_Σ: $\Sigma \to K_0$ from Σ to the base set K_0 of $\mathbf{K}$ which satisfy the following universality property:

for each Kleene algebra with tests $\mathbf{TK'} = (\mathbf{B'} \xrightarrow{j} \mathbf{K'})$ and maps f: $B \to B'$, g: $\Sigma \to K'$ there is a unique arrow $(\widehat{f}, \widehat{g})$: $F(B, \Sigma) \to \mathbf{TK'}$ in **Kat** such that $f = \widehat{f} \circ \eta_B$ and $g = \widehat{g} \circ \eta_\Sigma$.

Theorem 4.3 Let B and Σ be sets. Then there is a free Kleene algebra with tests generated by (B, Σ).

Proof Recall that an FL sketch **2** which appeared in Example 2.6. Let i be a homomorphism of FL sketches from **2** to KAT which takes 0 and 1 to B and K, respectively. Since $\mathbf{Mod}(\mathbf{2}) \cong \mathbf{Set} \times \mathbf{Set}$ and $\mathbf{Mod}(\mathrm{KAT}) \cong \mathbf{Kat}$, a functor i^*: $\mathbf{Kat} \to \mathbf{Set} \times \mathbf{Set}$ induced from i has a left adjoint $i_\#$ by Theorem 2.10. Therefore, if two sets B and Σ are given, then a Kleene algebra with tests $i_\#(B, \Sigma)$ and a morphism $\eta_{(B,\Sigma)} = (\eta_B, \eta_\Sigma)$ from (B, Σ) to $i^*(i_\#(B, \Sigma))$ in $\mathbf{Set} \times \mathbf{Set}$ are determined. It is trivial that these data have the universal property.

Kozen and Smith[10] gave a result equivalent to Theorem 4.3 assuming B is finite. They also assumed that Σ is finite, but that is not necessary even for their construction. Theorem 4.3 claims that B is not necessarily finite.

5. Quantale

Kozen and Smith[10] introduced Kleene algebra $\mathcal{P}_{B,\Sigma}$ with tests to show the existence of free Kleene algebra with tests. This section and the next are devoted to show that the construction of $\mathcal{P}_{B,\Sigma}$ is not ad hoc but composition of standard constructions such as coproduct and adjoint functors. This section briefly reviews quantales. As the second author argued[5),6)], it is very important in the theory of Kleene algebras that the set of languages on a set of alphabets gives a Kleene algebra. This Kleene algebra happens to be the unital quantale freely generated by the set of alphabets. In this section we show that there is a faithful functor from the category **UQuant** of unital quantales to the category **Kleene** of Kleene algebras. Also existence of coproduct in **UQuant** is given.

5.1 Unital Quantale and Kleene Algebra

Definition 5.1 (Mulvey[14)]) A **unital quantale** is a tuple $(Q, e, \cdot, \bigvee)$ which satisfies the following conditions: $(Q, e, \cdot)$ is a monoid, $(Q, \bigvee)$ is a complete upper semilattice, and $\bigvee$ distributes over $\cdot$, i.e., $\bigvee\{a \cdot b_i \mid i \in I\} = a \cdot \bigvee\{b_i \mid i \in I\}$ and $\bigvee\{b_i \cdot a \mid i \in I\} = \bigvee\{b_i \mid i \in I\} \cdot a$ hold for each element $a \in Q$ and family $(b_i \mid i \in I)$ of elements of Q.

Remark 5.2 Since a quantale is a complete upper semilattice, it always has the greatest element $\top \stackrel{\text{def}}{=} \bigvee Q$ and the least element $\bot \stackrel{\text{def}}{=} \bigvee \emptyset$. Moreover, $x \cdot \bot = \bot = \bot \cdot x$ holds by distributive law.

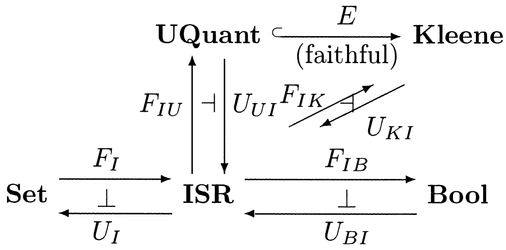
Example 5.3 If $(M(X), \epsilon, \cdot)$ denotes the free monoid generated by a set X, Lang(X) $\stackrel{\text{def}}{=}$ $(\mathrm{P}(\mathrm{M}(\mathrm{X})), \{\epsilon\}, \circ, \bigcup)$ is a unital quantale. Where $P(M(X))$ is the power set of $M(X)$, $\circ$ is defined by pointwise extension of $\cdot$, i.e., $L \circ L' \stackrel{\text{def}}{=} \{\sigma \cdot \sigma' \mid \sigma \in L, \sigma' \in L'\}$, and $\bigcup$ is sum of sets.
The base set of Lang(X) is the set of all languages on set X of alphabets.

Proposition 5.4 By taking unital quantale $(Q, e, \cdot, \bigvee)$ to $(Q, \bot, e, \bigvee, \cdot, [x \mapsto \bigvee\{x^n \mid n \in \omega\}])$, a faithful functor E: **UQuant** $\to$ **Kleene** from **UQuant** to **Kleene** is determined.
Also, unital quantales are related to idempotent semirings. The following proposition will be used later.

Proposition 5.5 The forgetful functor U_{UI} which takes a unital quantale $(Q, e, \cdot, \bigvee)$ to an idempotent semiring $(Q, \bot, e, \vee, \cdot)$, $\vee$ being defined by $a \vee b \stackrel{\text{def}}{=} \bigvee\{a, b\}$, has a left adjoint F_{IU}.

It is well-known that the forgetful functor U_B: **Bool** $\to$ **Set** has a left adjoint and so does U_I: **ISR** $\to$ **Set**. The situation of those functors which appeared in Proposition 5.4, 5.5 are depicted in **Fig. 1**.

Remark 5.6 **Kat** may be defined as the comma category $(U_{BI} \downarrow U_{KI})$, so a Kleene algebra with tests is a idempotent semiring homomorphism (arrow of ISR) of the shape $U_{BI}(\mathbf{B}) \to U_{KI}(\mathbf{K})$ for some Boolean algebra $\mathbf{B}$ and Kleene algebra $\mathbf{K}$.



$$F_B \stackrel{\text{def}}{=} F_{IB} \circ F_I \qquad F_U \stackrel{\text{def}}{=} F_{IU} \circ F_I$$
$$U_B \stackrel{\text{def}}{=} U_I \circ U_{BI} \qquad U_U \stackrel{\text{def}}{=} U_I \circ U_{UI}$$
$$U_K \stackrel{\text{def}}{=} U_I \circ U_{KI} \qquad U_{UI} = U_{KI} \circ E$$

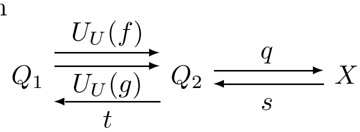
Fig. 1 Adjunctions around **Kleene**.

5.2 Coproduct of Unital Quantales

We show that coproduct of unital quantales exist. Since the category $\mathbf{Set}^{\mathsf{T}}$ of T-algebras is cocomplete for each monad T[1)], it is sufficient to show that the functor U_U is monadic (tripleable).

Proposition 5.7 The functor U_U: **UQuant** $\to$ **Set** creates coequalizer for those pair of parallel arrows f, g in **UQuant** for which $U_U(f), U_U(g)$ has a split coequalizer in **Set**.

Proof Consider unital quantales $\mathbf{Q}_i = (Q_i, e_i, \cdot^i, \bigvee^i)$ $(i = 1, 2)$ and homomorphisms f, g: $\mathbf{Q}_1 \to \mathbf{Q}_2$ between them and assume the diagram



is a split fork. Maps $\cdot^X$: $X \times X \to X$ and $\bigvee^X$: $P(X) \to X$ are defined by $a \cdot^X b \stackrel{\text{def}}{=} q(s(a) \cdot^2 s(b))$ for $a, b \in X$ and $\bigvee^X A \stackrel{\text{def}}{=} q(\bigvee^2 s(A))$ for $A \subseteq X$. It is a routine to show that $(X, q(e_2), \cdot^X, \bigvee^X)$ is the unique unital quantale such that q becomes a unital quantale homomorphism and q is the unique coequalizer of f and g.

By Beck's (precise tripleability) theorem[1),13)] and Proposition 5.7, the functor U_U is monadic. It is known that C is complete and cocomplete if a functor U: $C \to$ **Set** is monadic. (See Barr and Wells[1)].) Therefore, we obtain the following Proposition.

Proposition 5.8 **UQuant** is complete and cocomplete.

In particular, any pair of unital quantales has a coproduct.

6. Kozen-Smith construction

We introduce a Kleene algebra with tests $\mathcal{Q}_{B,\Sigma}$ by using standard constructions of adjunctions appeared in Fig. 1 and coproducts, in order to show that the construction of $\mathcal{P}_{B,\Sigma}$ given by Kozen and Smith [10] is not ad hoc. Moreover, we show $\mathcal{Q}_{B,\Sigma}$ is isomorphic to $\mathcal{P}_{B,\Sigma}$, whenever the latter is defined.

Construction 6.1 ($\mathcal{Q}_{B,\Sigma}$) Let B and Σ be sets. We construct the Kleene algebra with tests $\mathcal{Q}_{B,\Sigma}$ as follows. Let η be the unit of adjunction $F_{UI} \dashv U_{UI}$ and ι: $F_{IU}U_{BI}F_B(B) \to F_{IU}U_{BI}F_B(B) + F_U(\Sigma)$ be the canonical injection. Consider the idempotent semiring homomorphism $U_{KI}E(\iota) \circ \eta_{U_{BI}F_B(B)}$:

$$\mathcal{Q}_{B,\Sigma} \stackrel{\mathrm{def}}{=} \left(\begin{array}{c} U_{BI}F_B(B) \\ \downarrow \eta_{U_{BI}F_B(B)} \\ U_{UI}F_{IU}U_{BI}F_B(B) \\ \parallel \\ U_{KI}EF_{IU}U_{BI}F_B(B) \\ \downarrow U_{KI}E(\iota) \\ U_{KI}E(F_{IU}U_{BI}F_B(B) + F_U(\Sigma)) \end{array} \right)$$

We define $\mathcal{Q}_{B,\Sigma}$ to be this Kleene algebra with tests. (See Remark 5.6.)

Remark 6.2 The adjunction $F_{UI} \dashv U_{UI}$ provides bijective correspondence between $\mathcal{Q}_{B,\Sigma}$ and ι since $U_{UI} = U_{KI} \circ E$.

Kozen and Smith introduced $\mathcal{P}_{B,\Sigma}$ in their proof of existence theorem of free Kleene algebra with tests, but our proof of Theorem 4.3 uses neither $\mathcal{P}_{B,\Sigma}$ nor $\mathcal{Q}_{B,\Sigma}$.

Construction 6.3 ($\mathcal{P}_{B,\Sigma}$[10]) Let B be a finite set and Σ be a (possibly infinite) set. Let $\mathcal{A}(F_B(B))$ be the set of all atoms in the Boolean algebra $F_B(B)$:

$$\mathcal{A}(F_B(B)) \stackrel{\mathrm{def}}{=} \{ x \in F_B(B) \mid 0 \le y \le x \Longrightarrow y = 0 \vee y = x \}.$$

Then

$$C_{B,\Sigma} \stackrel{\mathrm{def}}{=} (P(X),\ \mathcal{A}(F_B(B)), \diamond, \bigcup)$$

is a unital quantale, where

$$X = \{\alpha_1 p_1 \cdots \alpha_{n-1} p_{n-1} \alpha_n \mid \alpha_i \in \mathcal{A}(F_B(B)) \wedge p_i \in \Sigma\},$$

$P(X)$ being the power set of X, and $\diamond$: $P(X) \times P(X) \to P(X)$ being defined by $C \diamond D \stackrel{\mathrm{def}}{=} \{x\alpha y \mid x\alpha \in C \wedge \alpha y \in D \wedge \alpha \in \mathcal{A}(F_B(B))\}$.

Define a map j from $U_B F_B(B)$ to $U_K E(C_{B,\Sigma})$ by $j(b) \stackrel{\mathrm{def}}{=} \{ x \in \mathcal{A}(F_B(B)) \mid x \le b \}$. Then $(F_B(B) \xrightarrow{j} E(C_{B,\Sigma}))$ is a Kleene algebra with tests. We shall denote by $\mathcal{P}_{B,\Sigma}$. By Remark 5.6 $\mathcal{P}_{B,\Sigma}$ may be described as follows:

$$\mathcal{P}_{B,\Sigma} = U_{BI}F_B(B) \xrightarrow{j} U_{KI}E(C_{B,\Sigma}).$$

Lemma 6.4 The unital quantale $C_{B,\Sigma}$ which consists of commands of $\mathcal{P}_{B,\Sigma}$ is a coproduct of $F_{IU}U_{BI}F_B(B)$ and $F_U(\Sigma)$.

Proof Let the unital quantale homomorphism i_1 from $F_{IU}U_{BI}F_B(B)$ to $C_{B,\Sigma}$ be the unique extension of an idempotent semiring homomorphism j in Construction 6.3 and let the unital quantale homomorphism i_2 from $F_U(\Sigma)$ to $C_{B,\Sigma}$ be the unique extension of a map $p \mapsto \{\alpha p \beta \mid \alpha, \beta \in \mathcal{A}(F_B(B))\}$ from Σ to $U_U(C_{B,\Sigma})$.

$$F_{IU}U_{BI}F_B(B) \xrightarrow{i_1} C_{B,\Sigma} \xleftarrow{i_2} F_U(\Sigma)$$

is a coproduct diagram. In fact, given a unital quantale $\mathbf{Q}$ and unital quantale homomorphisms g_1: $F_{IU}U_{BI}F_B(B) \to \mathbf{Q}$ and g_2: $F_U(\Sigma) \to \mathbf{Q}$, h defined as follows is the unique unital quantale homomorphism subject to $g_j = h \circ i_j \quad (j = 1, 2)$:

- $h(C) \stackrel{\mathrm{def}}{=} e_{\mathcal{Q}}$, if $C = \mathcal{A}(F_B(B))$.
- $h(C) \stackrel{\mathrm{def}}{=} \bigvee\{ g_1(\alpha_1) g_2(p_1) \cdots g_1(\alpha_m) \mid \alpha_1 p_1 \cdots \alpha_m \in C\}$, otherwise.

Theorem 6.5 $\mathcal{P}_{B,\Sigma}$ is isomorphic to $\mathcal{Q}_{B,\Sigma}$ whenever $\mathcal{P}_{B,\Sigma}$ is defined.

Proof The Boolean algebras of $\mathcal{P}_{B,\Sigma}$ and $\mathcal{Q}_{B,\Sigma}$ are exactly the same. Their Kleene algebras are isomorphic by Lemma 6.4. Let the canonical isomorphism be k; it is the mediating arrow of the coproduct $F_{IU}U_{BI}F_B(B) + F_U(\Sigma)$ with respect to i_1, i_2. Moreover the following diagram commutes since $i_1 = k \circ \iota$.

$$\begin{array}{ccc} U_{BI}F_B(B) & = & U_{BI}F_B(B) \\ \mathcal{Q}_{B,\Sigma} \downarrow (= U_{KI}E(\iota) \circ \eta_{U_{BI}F_B(B)}) & & \mathcal{P}_{B,\Sigma} \downarrow (= j) \\ U_{KI}E(F_{IU}U_{BI}F_B(B) + F_U(\Sigma)) & \xrightarrow[U_{KI}E(k)]{\cong} & U_{KI}E(C_{B,\Sigma}) \end{array}$$

7. Semantics of While Programs by Sets of Runs

In this section we introduce **while** algebras as an algebraic structure of **while** programs and give a functorial semantics of it. Also note that there is a faithful functor $\mathcal{I}$ from the category of Kleene algebras with tests to the category of **while** algebras and by using $\mathcal{I}$ **while** programs are interpreted in each Kleene algebra with tests. In particular, considering interpretation in $\mathcal{Q}_{B,\Sigma}$, it is semantics by sets of runs.

7.1 While Algebra

Definition 7.1 A **while algebra** is defined as follows as a many sorted algebra. For short we use description of algebraic specification languages such as CASL, OBJ and so on.

sort **Test**, **Com**.
op **abort**, **skip**: $\to$ **Com**.
op **;**, []: **Com** $\times$ **Com** $\to$ **Com**.
op **if**: **Test** $\times$ **Com** $\times$ **Com** $\to$ **Com**.
op **while**: **Test** $\times$ **Com** $\to$ **Com**.
op **tt**, **ff**: $\to$ **Test**.
op $\neg$: **Test** $\to$ **Test**.
op $\wedge, \vee$: **Test** $\times$ **Test** $\to$ **Test**.
infix **;**, $[], \wedge, \vee$.
eq equations which show
(**Com**, **skip**, **;**) is a monoid.
eq equations which show
(**Com**, **abort**, []) is a semilattice.
eq $c;y \, [] \, c;z = c;(y \, [] \, z)$.
eq $\mathbf{abort};c = \mathbf{abort} = c;\mathbf{abort}$.
eq $\mathbf{if}(\mathbf{tt}, c, c') = c$. **eq** $\mathbf{if}(\mathbf{ff}, c, c') = c'$.
eq $\mathbf{while}(b, c) = \mathbf{if}(b, c; \mathbf{while}(b, c), \mathbf{skip})$.
eq equations which show
(**Test**, **ff**, **tt**, $\vee, \wedge, \neg$) is a Boolean algebra.

In other words **while** algebra **W** is an algebraic equipped with two base sets $W_{\mathbf{Test}}$, $W_{\mathbf{Com}}$, structure of Boolean algebra whose base set is $W_{\mathbf{Test}}$, structure of idempotent semiring whose base set is $W_{\mathbf{Com}}$, and connections **if**, **while** between the structures. Homomorphisms of **while** algebras are defined as homomorphism of many sorted algebras, i.e., a **while** algebra homomorphism f from **W** to **V** is a pair of a Boolean algebra homomorphism $f_{\mathbf{Test}}$ from $W_{\mathbf{Test}}$ to $V_{\mathbf{Test}}$ and an idempotent semiring homomorphism $f_{\mathbf{Com}}$ from $W_{\mathbf{Com}}$ to $V_{\mathbf{Com}}$ which preserves **if** and **while**.

Since axioms of **while** algebras are given by only equations, for any two sets B and Σ there exists the free **while** algebra $F(B, \Sigma)$ generated by (B, Σ). That is, for each **while** algebra **W**, maps $f_1 : B \to W_{\mathbf{Test}}$ and $f_2 : \Sigma \to W_{\mathbf{Com}}$ are always extended to a **while** algebra homomorphism $(\widehat{f_1}, \widehat{f_2})$: $F(B, \Sigma) \to \mathbf{W}$.

An element of $F(B, \Sigma)$ is a equivalence class with respect to a congruence which express "equivalence of programs" of **while** programs whose atomic tests are elements of B and whose atomic commands are elements of Σ. Thus we call elements of $F(B, \Sigma)$ **while programs**.

The category **While** is defined to be the category of **while** algebras and homomorphism between them. The free construction we mentioned above can be translated as follows.

Theorem 7.2 An forgetful functor U: **While** $\to$ **Set** $\times$ **Set** which takes a **while** algebra to a pair of base sets of it has a left adjoint.

Definition 7.3 A **while** algebra homomorphism from $F(B, \Sigma)$ to **while** algebra **W** is called an interpretation in **W** of **while** programs whose atomic tests belong to B and whose atomic commands belong to Σ

By Theorem 7.2, an interpretation in **W** of **while** program is determined uniquely by a pair of maps from B to $W_{\mathbf{Test}}$ and from Σ to $W_{\mathbf{Com}}$.

7.2 Models in Kleene Algebra with Tests

Let $(\mathbf{B} \xrightarrow{j} \mathbf{K})$ be a Kleene algebra with tests. By define values in Kleene algebra with tests of sort **Test** by **B**, operators **tt**, **ff**, $\neg$, $\wedge$, $\vee$ by 1_B, 0_B, $\neg$, $\cdot_B$, $+_B$, respectively, values of sort **Com** by **K**, operators **abort**, **skip**, **;**, [], **if**, **while** by 0_K, 1_K, $\cdot_K$, and $+_K$ $[(b, c, c') \mapsto j(b) \cdot_K c +_K j(\neg b) \cdot_K c']$, $[(b, c) \mapsto (j(b) \cdot_K c)^* \cdot_K j(\neg b)]$, we obtain a **while** algebra. A faithful functor $\mathcal{I}$: **Kat** $\to$ **While** is determined by taking $(\mathbf{B} \xrightarrow{j} \mathbf{K})$ to the **while** algebra. We define an interpretations in Kleene algebra with tests by using Definition 7.3 and $\mathcal{I}$.

Definition 7.4 Let **T** be a Kleene algebra with tests. We call an interpretation in a **while** algebra $\mathcal{I}(\mathbf{T})$ of **while** program an interpretation in **T**.

This interpretation coincides with interpretation of **while** programs given by Kozen [12]. By Theorem 7.2 an interpretation in **T** is determined by a pair of maps from B to **B** and from Σ to **K**.

Since states of **while** programs are completely determined by value of prepared tests, we may consider propositions over B as states of a system. On the other hand, words over Σ may be considered as state transitions of a system. Therefore if we consider interpretations in a Kleene algebra with tests $\mathcal{Q}_{B,\Sigma}$, we obtain interpretation of **while** programs by sets of runs.

References

1) Barr, M. and Wells, C.: *Toposes, Triples and Theories*, Springer (1985).
2) Barr, M. and Wells, C.: *Category theory for computing science*, 2nd ed., Prentice-Hall (1995).
3) Barr, M.: Models of horn theory, *Proc. Summer Research Conference, Categories in Computer Science and Logic*, Gray, J. and Scedrov,

A. (eds.), No.92, pp.1–7, AMS, Contemporary Mathematics (1989).
4) Gray, J.W.: Categorical aspects of data type constructors, *Journal of Theoretical Computer Science*, Vol.50, pp.103–135 (1987).
5) Kinoshita, Y.: Algebraic structures for fixpoints, in Japanese. Submitted, preliminary version is in *Proc.* Ref.6).
6) Kinoshita, Y.: Algebraic structures for fixpoints, in Japanese, *Proc. 18th JSSST annual meeting*, JSSST (2001). CD-ROM.
7) Kinoshita, Y. and Furusawa, H.: Essentially algebraic structure for Kleene algebra with tests, in Japanese. Submitted, preliminary version is in *Proc.* Ref.8).
8) Kinoshita, Y. and Furusawa, H.: Essentially algebraic structure for Kleene algebra with tests, *Proc. 19th JSSST annual meeting*, *JSSST* in Japanese, (2002). CD-ROM.
9) Kinoshita, Y. and Furusawa, H.: Semantics of while programs by sets of runs, *Proc. Forum on Information Technology* (*FIT2002*), *IEICE* and *IPSJ* in Japanese, (2002). CD-ROM.
10) Kozen, D. and Smith, F.: Kleene algebra with tests: Completeness and decidability, *Proc. 10th Int. Workshop Computer Science Logic* (*CSL'96*), van Dalen, D. and Bezem, M.(eds.), Springer Lecture Notes in Computer Science, No.1258, pp.244–259 (1996).
11) Kozen, D.: On Kleene algebras and closed semirings, *Proc. Mathematical Foundations of Computer Science*, Rovan (ed.), Springer Lecture Notes in Computer Science, Vol.452, pp.26–47 (1990).
12) Kozen, D.: Kleene Algebra with Tests, *ACM Trans. Programming Languages and Systems*, Vol.19, No.3, pp.427–443 (1997).
13) Mac Lane, S.: *Categories for the Working Mathematician*, 2nd ed., Springer (1998).
14) Mulvey, C. and Pelletier, J.: A quantisation of calculus of relations, *Proc. Categories Theory 1991*, *CMS Conference Proceedings*, No.13, pp.345–360, AMS (1992).

(Received September 30, 2002)
(Accepted November 12, 2002)

Hitoshi Furusawa was born in 1969. He received his D.Sc. degree from Kyushu University in 1998. He was a research assistant at University of the Federal Armed Forces Munich and engaged in research on relation algebras for foundations of relational specification. Since 1999 he had been in ETL as a research associate and has been a researcher at AIST since 2002. His current research interests are algebraic methods in programming semantics and verification.

Yoshiki Kinoshita is the Leader of Informatics Group at National Institute of Advanced Industrial Science and Technology (AIST). After receiving D.Sc. (doctor of science) degree in 1989 from the University of Tokyo, he had worked for Electrotechnical Laboratory (ETL) until it was reformulated as AIST in 2001. He has given introductory lectures on category theory and semantics in Chiba, Tsukuba and Tokyo. He visited the Laboratory for Foundations of Comp. Sci. (LFCS) in Edinburgh in the year 1992/93. He is interested in programming semantics and verification.