Essentially algebraic structure for Kleene algebra with tests and its application to semantics of while programs

Hitoshi Furusawa† Yoshiki Kinoshita†

Kozen and Smith showed the existence of Kleene algebra with tests freely generated by a pair (B, Σ) of finite sets. They give an explicit construction of Kleene algebra with tests $\mathcal{P}_{B,\Sigma}$, and prove that a certain subalgebra of $\mathcal{P}_{B,\Sigma}$ is the freely generated by (B, Σ). We show the existence of free algebra without assuming the finiteness condition. Moreover, we provide a construction of Kleene algebra with tests $\mathcal{Q}_{B,\Sigma}$ by means of standard constructions such as coproducts and adjunctions 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 also give an elementwise description of $\mathcal{Q}_{B,\Sigma}$: it consists of sets of strings over $B \uplus B$ and Σ. 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[10] introduced Kleene algebra with tests and applied it to algebraic semantics of **while** programs. Later, Kozen and Smith[9] 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)]. According to Barr[3)], 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[6),7)] but we shall present it more in detail here.

We shall also study on $\mathcal{P}_{B,\Sigma}$, which plays the same role as $\mathrm{Lang}(A)$, 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 contains ad hoc looking constructions. We provide another Kleene algebra with tests $\mathcal{Q}_{B,\Sigma}$ for any pair (B, Σ) of 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, which supports the claim that our construction is less ad hoc.

We introduce the notion of **while** algebra[8)] 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 of 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.

† C.R.T. of Informatics, AIST

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 $\mathrm{src}, \mathrm{tgt}\colon G_1 \to G_0$, $i\colon G_0 \to G_1$ satisfying $\mathrm{src} \circ i = \mathrm{tgt} \circ i = \mathrm{id}_{G_1}$. Elements in G_0, G_1 is 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 no equational constraints. A **homomorphism** of reflexive graphs is defined as 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 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 a and a family of edges $P = \{\, p_x\colon a \to x \mid x \in H_0 \setminus \{\, a \,\}\,\}$, and, for each edge f which is not in the image of P, neither the source nor target is a, 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 cone**. 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 $H_0 \setminus \{\, p \,\}$.

If M is a model M of S, the definition of models forces $M(a)$ to be an n-fold product of $M(b)$ and $M(f)$ to be a function $M(f)\colon M(b)^n \to M(b)$. So in this sense, the above definition of n-ary operator coincides the usual notion. We shall use the term "n-ary operator" in the usual sense as well.

Definition 2.5 Let $S = (G, C, \Gamma)$ be an FL sketch. A reflexive graph homomorphism M from G to the underlying graph of the category **Set** is called **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** between models of S is a "natural transformation," that is, 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 in Z, but we shall use only models in **Set**, so the above definition suffices.

Definition 2.6 A category C is **FL sketchable** if there exists an FL sketch, category of whose models is equivalent to C.

The following theorem tells us the relationship between symbolic logical presentation and FL sketches.

Theorem 2.7 (Barr[3)]) The category of models of a equational Horn theory is FL sketchable.

Example 2.8 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 2.9 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 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 is of some use when we need compare two sketches.

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

3. Kleene algebra

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) $\cdot$ distributes over $+$ from both side, i.e.,

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

(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

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

This partial order $\leq$ shall be used in this sense.

Definition 3.3 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 the first can be axiomatized by equational theory!), so, the categories of these algebras are all sketchable by FL sketches. For instance, the FL sketch KLEENE $= (G, C, \Gamma)$ for Kleene algebra 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 in[3)].

4. Kleene algebra with tests

Kozen[10)] 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 $j\colon B \to K$ is a map from B to K which preserves 0, 1, $+$, $\cdot$. Elements of K are called **commands**, elements of B are called **tests**.

Kleene algebra with tests in the sense of Kozen 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 as an equational Horn clause, so an FL Sketch KAT for **Kat** exists by Theorem 2.7.

We shall give an outline of KAT. 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 $(B, 0, 1, \neg, +_B, \cdot_B)$ a Boolean algebra. K has two nulary operators 0_K, 1_K, a unary operator * and two binary operators $+_K$, $\cdot_K$. There are commutative diagrams and cones which make $(K, 0, 1, ^*, +_K, \cdot_K)$ a Kleene algebra. Finally, there are commutative diagrams which express that j preserves 0, 1, +, $\cdot$.

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 $\eta_B \colon B \to B_0$ from B to the base set B_0 of $\mathbf{B}$, map $\eta_\Sigma \colon \Sigma \to K_0$ 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 $f \colon B \to B'$, $g \colon \Sigma \to K'$ there is a unique arrow $(\widehat{f}, \widehat{g}) \colon F(B, \Sigma) \to \mathbf{TK}'$ 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 the free Kleene algebra with tests generated by (B, Σ).

Proof Recall that an FL sketch **2** which appeared in example 2.8. 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 $i^* \colon \mathbf{Kat} \to \mathbf{Set} \times \mathbf{Set}$ 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 universality by the definition of adjoint functors.

Kozen and Smith[9)] gave a result equivalent to Theorem 4.3 assuming B is finite. They also assumed that Σ is finite, but that is not necessary. We make clear that B is not assumed to be finite in our proof of existence of the free Kleene algebra with tests by using notion of FL sketches.

5. Quantale

As the second author argued in[4),5)], it is very important, in the theory of Kleene algebras, that the set of languages on a set of alphabets gives a Kleene algebra. The Kleene algebra is the unital quantale freely generated by the set of alphabets. In this section we show that each unital quantale can be seen as a Kleene algebra with using a faithful functor from the category **UQuant** of unital quantales to the category **Kleene** of Kleene algebras. Also a construction of coproduct in **UQuant** is given.

5.1 Unital quantale and Kleene algebra

Definition 5.1 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 lattice, and $\bigvee$ is distributive with respect to $\cdot$, 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.

A **Quantale** may not have unit e with respect to multiplication $\cdot$.

Remark 5.2 Since a quantale is a complete upper semilattice, it always has the greatest element $\top \overset{\text{def}}{=} \bigvee Q$ and the least element $\bot \overset{\text{def}}{=} \bigvee \emptyset$. 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, $\mathrm{Lang}(X) \overset{\text{def}}{=} (P(M(X)), \{\epsilon\}, \circ, \bigcup)$ 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., $L \circ L' \overset{\text{def}}{=} \{\sigma \cdot \sigma' \mid \sigma \in L, \sigma' \in L'\}$, and $\bigcup$ is sum of sets.

The base set of $\mathrm{Lang}(X)$ is the set of all languages on set X of alphabets. Also $\mathrm{Lang}(X)$ is a Kleene algebra. All unital quantales as well as $\mathrm{Lang}(X)$ can be seen as Kleene algebras.

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 $E \colon \mathbf{UQuant} \to \mathbf{Kleene}$ from the category **UQuant** of unital quantales to the category **Kleene** of Kleene algebras is determined.

Also, unital quantales are related to idempotent semirings. The following proposition will be used later.

Proposition 5.5 A forgetful functor U_{UI} which takes a unital quantale $(Q, e, \cdot, \bigvee)$ to an idempotent semiring $(Q, \bot, e, \bigvee, \cdot)$ has a left adjoint F_{IU}.

5.2 Coproducts of unital quantale

A construction of coproducts which is called free products of two groups is well-known[11]. In similar way, we can construct coproducts of unital quantales.

Construction 5.6 Let $\mathbf{R_j} = (R_j, e_j, \cdot_j, \bigvee_j)$, $(j = 1, 2)$ be two unital quantales. We define X_0 to be the set of all finite alternate sequences (which includes empty word) of an element of R_1 and an element of R_2, so $X_0 \stackrel{\text{def}}{=} \{ x_0 x_1 x_2 \ldots x_n \mid 0 \leq n < \omega, (x_{2m} \in R_1 \wedge x_{2m+1} \in R_2) \vee (x_{2m} \in R_2 \wedge x_{2m+1} \in R_1) \}$. Defining a relation $\equiv$ on the power set $P(X_0)$ of X_0 by a unital quantale congruence which is generated by $\emptyset \equiv \{ \bot_j \} \quad (j = 1, 2)$ and $\bigvee_j Y_j \equiv \bigcup_j Y_j \quad (j = 1, 2,\ Y_j \subseteq R_j)$, X is defined by $X \stackrel{\text{def}}{=} P(X_0)/\equiv$. The equivalence class of $W \subseteq X_0$ with respect to $\equiv$ is denoted by $[W]$.

A operator $\bigvee$ on X is defined by $\bigvee\{ [W_k] \mid k \in I \} \stackrel{\text{def}}{=} [\bigcup\{ W_k \mid k \in I \}]$. To define a binary operator $\cdot$, we define $x_0 x_1 \ldots x_m \cdot_0 y_0 y_1 \ldots y_n$ for two elements $x_0 x_1 \ldots x_m$ and $y_0 y_1 \ldots y_n$ of X_0 as follows: if $x_m = e_j$, $(x_0 \ldots x_{m-1}) \cdot_0 (y_0 \ldots y_n)$; if $y_0 = e_j$, $(x_0 \ldots x_m) \cdot_0 (y_1 \ldots y_n)$; $x_m, y_0 \in R_j$; if $x_m, y_0 \in R_j$ and $x_m, y_0 \neq e_j$, $x_0 \ldots x_{m-1}(x_m \cdot_j y_0) y_1 \ldots y_n$; otherwise $x_0 \ldots x_m y_0 \ldots y_n$. Then for $A, B \in X$ take $A_0 \in A$ and $B_0 \in B$ and define $A \cdot B \stackrel{\text{def}}{=} [\{a \cdot_0 b \mid a \in A_0,\ b \in B_0\}]$. The two operators $\bigvee$ and $\cdot$ are well-defined, and $(X, \{ \epsilon \}, \cdot, \bigvee)$ is a unital quantale which we denote by $R_1 + R_2$.

The injection ι_j from R_j $(j = 1, 2)$ to $R_1 + R_2$ is defined by $R_j \ni x \longmapsto [\{ x \}]$.

These data satisfies the following proposition.

Proposition 5.7 $R_1 \xrightarrow{\iota_1} R_1 + R_2 \xleftarrow{\iota_2} R_2$ is a coproduct diagram in the category **UQuant** of unital quantales.

It is well-known that the forgetful functor U_B: **Bool** $\to$ **Set** has a left adjoint and so does U_{ISR}: **ISR** $\to$ **Set**. These functors and adjoint functors and faithful functors which appeared in proposition 5.4, 5.5 are depicted in Figure 1.

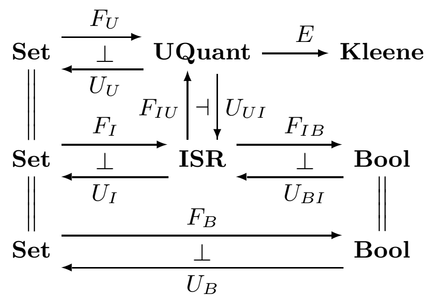

図 1 Adjunctions around **Kleene**

6. Kozen-Smith construction

The construction of $\mathcal{P}_{B,\Sigma}$ given by Kozen and Smith[9] looks rather ad hoc. We introduce a Kleene algebra with tests $\mathcal{Q}_{B,\Sigma}$ by using standard constructions such as adjunctions appeared in figure 1 and coproducts. Our $\mathcal{Q}_{B,\Sigma}$ is an extension of $\mathcal{P}_{B,\Sigma}$ in the sense that it is isomorphic to $\mathcal{P}_{B,\Sigma}$, whenever the latter is defined.

Construction 6.1 ($\mathcal{Q}_{B,\Sigma}$) Given two sets B and Σ, consider a unital quantale $UQ_{B,\Sigma} = F_{IU}(U_{BI}(F_B(B))) + F_U(\Sigma))$ and injection ι: $F_{IU}(U_{BI}(F_B(B))) \to UQ_{B,\Sigma}$. ι preserves 0, 1, addition and multiplication, so $F_B(B) \xrightarrow{\iota} K_{B,\Sigma})$ is a Kleene algebra with tests, where $K_{B,\Sigma} = E(UQ_{B,\Sigma})$. We denote it by $\mathcal{Q}_{B,\Sigma}$.

Here, assuming B is finite set, we give a point-wise construction of $\mathcal{Q}_{B,\Sigma}$.

Construction 6.2 Let B consist of n elements. $\mathcal{Q}_{B,\Sigma} = (\mathbf{B} \xrightarrow{j} \mathbf{K})$ is constructed as follows. $\mathbf{B}$ is the free Boolean algebra $F_B(B)$ generated by B, as it is well-known, $\mathbf{B}$ is a Boolean algebra consists of the second power set $P(P(B))$. A Kleene algebra $\mathbf{K} = (K, 0_K, 1_K, +_K, \cdot_K, {}^*)$ which consists of commands of $\mathcal{Q}_{B,\Sigma}$ is defined as follows. To define a set K consider the set X_0 of finite sequences on a set $B \uplus B \uplus \Sigma$ which includes the empty word ϵ, i.e.,

$$X_0 \stackrel{\text{def}}{=} \{ x_1 \ldots x_m \mid x_k \in B \uplus B \uplus \Sigma,\ 0 \leq m \}$$

Then K is a quotient set $P(X_0)/\equiv$ where $P(X_0)$ is the power set of X_0 and $\equiv$ is a Kleene algebra congruence which is generated by a binary relation $\{ a, \neg a \} \equiv \{\epsilon\}$, $\{ a \cdot \neg a \} \equiv \emptyset$, $\{ a \cdot b \} \equiv \{ b \cdot a \}$,

$\{ a \cdot b, a \} \equiv \{ a \}$, $\{ a \cdot a \} \equiv \{ a \}$ for each $a, b \in B$. The equivalence class of $U \in P(X_0)$ with respect to $\equiv$ is denoted by $[U]$, operators of $\mathbf{K}$ are defined by $0_K = [\emptyset]$, $1_K = [\{\epsilon\}]$, $[U] +_K [V] = [U \cup V]$, $[U] \cdot_K [V] = [\{ uv \mid u \in U,\ v \in V \}]$, $[U]^* = [\{ u^m \mid u \in U,\ 0 \le m \}]$. j is defined by $P(P(B)) \ni \mathcal{A} \mapsto [\{ x_1 \dots x_n \mid \{x_1, \cdots, x_n\} = A \uplus (B \setminus A),\ A \in \mathcal{A}\}]$.

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

Construction 6.3 ($\mathcal{P}_{B,\Sigma}$[9]) Let B be a finite set and Σ be a (possibly infinite) set. Define $\mathcal{A}(F_B(B))$ to be the set of all atoms in the Boolean algebra $F_B(B)$, that is, $\mathcal{A}(F_B(B)) \stackrel{\text{def}}{=} \{ x \in F_B(B) \mid 0 \le y \le x \Longrightarrow y = 0 \vee y = x \}$. Then $C_{B,\Sigma} = (\mathcal{P}(X), \emptyset, \mathcal{A}(F_B(B)), \diamond, \bigcup)$ is a unital quantale, where $X = \{\alpha_1 p_1 \cdots \alpha_n p_n \alpha_{n+1} \mid \alpha_i \in \mathcal{A}(F_B(B)) \wedge p_i \in \Sigma\}$, $\mathcal{P}(X)$ is its power set, and $\diamond\colon \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$ is defined by $C \diamond D \stackrel{\text{def}}{=} \{x\alpha y \mid x\alpha \in C \wedge \alpha y \in D \wedge \alpha \in \mathcal{A}(F_B(B))\}$.

Define a map j from $F_B(B)$ to $E(C_{B,\Sigma})$ by $j(b) \stackrel{\text{def}}{=} \{ x \in \mathcal{A}(F_B(B)) \mid x \le b \}$. Then $(E(C_{B,\Sigma}), F_B(B), j)$ is a Kleene algebra with tests, which we shall denonte by $\mathcal{P}_{B,\Sigma}$. This is essentially the same definition as[9].

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 Define a homomorphism i_1 from $F_B(B)$ to $\mathcal{P}(X)$ by $b \mapsto \{\alpha \mid \alpha \in \mathcal{A}(F_B(B)) \wedge \alpha \le b\}$. Also define a homomorphism i_2 from $F_U(\Sigma)$ to $\mathcal{P}(X)$ as a unique extension of a map $p \mapsto \{\alpha p \beta \mid \alpha, \beta \in \mathcal{A}(F_B(B))\}$ from Σ to $\mathcal{P}(X)$. i_1 and i_2 are standard injection of coproducts. In fact, given a unital quantale $\mathbf{Q}$ and homomorphism $g_1\colon, F_B(B) \to \mathbf{Q}$, $g_2\colon, F_U(\Sigma) \to \mathbf{Q}$, and if h is defined by $h(C) \stackrel{\text{def}}{=} e_{\mathcal{Q}}$ if $C = \mathcal{A}(F_B(B))$, $h(C) \stackrel{\text{def}}{=} \bigvee\{ g_1(\alpha_1) g_2(p_1) \cdots g_1(\alpha_{m+1}) \mid \alpha_1 p_1 \cdots \alpha_{m+1} \in C\}$ otherwise, h is a unique unital quantale homomorphism which satisfies $g_j = h \circ i_j \quad (j = 1, 2)$.

Lemma 6.4 shows that $E(C_{B,\Sigma})$ and $K_{B,\Sigma}$ are both coproducts of $F_{IU} U_{BI} F_B(B)$ and $F_U(\Sigma)$, so these two are isomorphic. Also both Boolean algebras consists of tests of them are $F_B(B)$.

An isomorphism from $E(C_{B,\Sigma})$ to $K_{B,\Sigma}$ is an intermediating arrow h in the case that g_j is replaced by standard injection with respect to $K_{B,\Sigma}$. Moreover, $j \circ h = \iota$, so we have proved the following theorem.

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

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

In other words **while** algebra $\mathbf{W}$ 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 $\mathbf{W}$ to $\mathbf{V}$ 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 $\mathbf{W}$, 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**.

We denote the category of **while** algebras and homomorphism between them **While**. 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 $\mathbf{W}$ is called an interpretation in $\mathbf{W}$ of **while** programs whose atomic tests belong to B and whose atomic commands belong to Σ

By theorem 7.2, an interpretation in $\mathbf{W}$ 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 $\mathbf{B}$, operators **tt**, **ff**, $\neg$, $\wedge$, $\vee$ by 1_B, 0_B, $\neg$, $\cdot_B$, $+_B$, respectively, values of sort **Com** by $\mathbf{K}$, 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 $\mathbf{T}$ be a Kleene algebra with tests. We call an interpretation in a **while** algebra $\mathcal{I}(\mathbf{T})$ of **while** program an interpretation in $\mathbf{T}$.

This interpretation coincides with interpretation of **while** programs given by Kozen[10]. By theorem 7.2 an interpretation in $\mathbf{T}$ is determined by a pair of maps from B to $\mathbf{B}$ and from Σ to $\mathbf{K}$.

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.

参 考 文 献

1) Barr, M. and Wells, C.: *Toposes, Triples and Theories*, Springer (1985).
2) Barr, M. and Wells, C.: *Category theory for computing science, second edition*, Prentice-Hall (1995).
3) Barr, M.: Models of horn theory, *Proc. of a Summer Research Conference, Categories in Computer Science and Logic* (Gray, J. and Scedrov, A.(eds.)), Contemporary Mathematics, No. 92, AMS, pp. 1–7 (1989).
4) Kinoshita, Y.: Algebraic structures for fixpoints. submitted, preliminary version is in proceedings[5], in Japanese.
5) Kinoshita, Y.: Algebraic structures for fixpoints, *Proceedings of 18th JSSST annual meeting*, JSSST (2001). CD-ROM, in Japanese.
6) Kinoshita, Y. and Furusawa, H.: Essentially algebraic structure for Kleene algebra with tests. submitted, preliminary version is in proceedings[7], in Japanese.
7) Kinoshita, Y. and Furusawa, H.: Essentially

algebraic structure for Kleene algebra with tests, *Proceedings of 19th JSSST annual meeting*, JSSST (2002). CD-ROM, in Japanese.

8) Kinoshita, Y. and Furusawa, H.: Semantics of while programs by sets of runs, *Proceedings of Forum on Information Technology (FIT2002)*, IEICE and IPSJ (2002). CD-ROM, in Japanese.

9) Kozen, D. and Smith, F.: Kleene algebra with tests: Completeness and decidability, *Proc 10th Int. Workshop Computer Science Logic (CSL'96)* (van Delen, D. and Bezem, M.(eds.)), Springer Lecture Notes in Computer Science, No. 1258, pp. 244–259 (1996).

10) Kozen, D.: Kleene Algebra with Tests, *ACM Transactions on Programming Languages and Systems*, Vol. 19, No. 3, pp. 427–443 (1997).

11) Steinberger, M.: *Algebra*, PWS Publishing Company (1994).