Probability meets Non-Probability via Complete IL-Semirings

Norihiro TSUMAGARI

March 2012

Department of System Information Science
Graduate School of Science and Engineering
Kagoshima University

Abstract

This thesis aims to provide a path to abstraction between probabilistic systems and non-probabilistic systems in order to put the verification methods for probabilistic systems into practical use.

McIver et al have introduced a verification method for probabilistic systems using probabilistic Kleene algebras and their model of probabilistic systems. However it is difficult to put their method in practical use because their model of probabilistic systems still includes probabilistic components. Thus we have to find more abstract semantic domain excluded probabilistic components in order to enable their verification method to be put into practical use. This thesis offers multirelations — extended binary relations — as that abstract domain for probabilistic systems. And we generalize the model of probabilistic systems as probabilistic multirelations, then we consider probabilistic multirelations and non-probabilistic multirelations via an algebra called complete IL-semiring. Giving several Galois connections between them, we begin walking to abstraction for probabilistic systems.

Acknowledgements

Thanks to support, encouragement and suggestions from many people, this thesis has been finished here. I would like to list them as possible.

First of all, I would like to express my heartfelt appreciation to my supervisor Hitoshi Furusawa for his elaborated guidance, many constructive suggestions and constant encouragement during the whole of this study. I could never finished my PhD work without him. I thank Professor Shuichi Shinmori and Professor Shoji Yokura for their helpful comments and encouragement during my PhD study. I also thank Lecturer Kiwamu Aoyama for his encouragement from my undergraduate days.

I express my gratitude to Yasuo Kawahara, Professor Emeritus of the Kyushu University for his valuable advices and constant encouragement. Koki Nishizawa, Lecturer from Tottori University of Environmental and Information, gave me helpful suggestions and comments. I am very grateful to him for his cooperation. Without his support, this thesis would never have been finished. I am also very grateful to Professor Masahito Hasegawa from Kyoto University and Lecturer Ichiro Hasuo from Tokyo University, for their valuable suggestions and criticisms during my stay at Kyoto and Tokyo. Dr. Georg Struth and Tahiry Rabehaja gave me helpful suggestions and comments during my stay at Sheffield University. It was my first time to stay in University abroad. Thanks to their support, I could get good experience.

I thank my former colleagues Sarpono Dimulyo, Kazuhiko Nagayama, Fumiya Sanda and Akira Takenoshita for their friendship and encouragement. I also thank my old friends Tohru Ando, Takashi Kajiyama, Tomokazu Oita and Tsuyoshi Tanimura for their constant encouragement.

Finally, I am deeply grateful to my family. I wish to thank Jun for her encouragement and support. I would like to express my gratitude to my sisters, Eiko and Kyoko for their constant encouragement. My deepest appreciation goes to my parents, Koji and Nariko for their patience, support and understanding.

My PhD work was supported in part by Grant-in-Aid for JSPS Fellows 22-7560 from Japan Society for the Promotion of Science.

Contents

Chapter 1

Introduction

In this thesis we aim to provide a path to abstraction between probabilistic systems and non-probabilistic systems in order to put the verification methods for probabilistic systems into practical use. This chapter introduce the background and the outline of this thesis.

1.1 Formal Methods for Probabilistic Systems

In recent years, the importance of formal methods for systems on specification, development and verification is rising along. Actually in `IEC 61508` [IEC98], the formal methods are recommended to secure the higher reliability of systems, so the study on these methods are discussed from various perspectives. In addition, it is expected that new standards based on `IEC 61508` will be established for every various fields.

The formal methods are mathematical-based techniques for specification, development and verification of systems. These techniques based on strict descriptions are particularly important into systems required high reliability because the description written in natural language may allow errors caused by the ambiguity inherent in natural language. In fact there are many examples of the application of formal methods; for example, aircraft development, traffic control for trains, nuclear plant control, and so on.

The formal methods for probabilistic systems are studied by Carrol Morgan, Anabelle McIver, et al [Mor]. And their book [MM05] was published in 2005. On the other hand, a probabilistic model checker, `PRISM` [PMC] is now available, which is a tool for formal modeling and analysis of systems that exhibit random or probabilistic behavior.

Though computer programs and systems including techniques using uncertainty and randomization — *e.g. distributed computing, fault tolerant system, randomized algorithm* — are increasing, the formal methods for probabilistic systems are still the big challenge. The biggest problem we face is numerical computations. While we model probabilistic systems formally and calculate the property of the systems on computers, it entails enormous costs for complicated calculation caused by numerical computations than standard systems.

1.2 Kleene Algebras and Complete IL-semirings

A notion of Kleene algebras is introduced by Kozen [Koz94] as a complete axiomatization of regular expressions. It is known that the set of (usual) binary relations on a set forms a Kleene algebra. Having such a relational model, we can have interpretation of while-programs in a Kleene algebra without any difficulty. Moreover, relational models have suggested a direction of extension of Kleene algebras, for instance, to Kleene algebra with tests [Koz97] and Kleene algebra with domains [DMS06]. Then three weaker variants of Kleene algebras have been independently introduced for different purposes.

- Möller [Moe04] has introduced lazy Kleene algebras to handle both of finite and infinite streams. A lazy Kleene algebra subsumes Dijkstra's computation calculus (cf. [Dij00]), Cohen's omega algebra (cf. [Coh00]) and von Wright's demonic refinement algebra (cf. [Wri04]).

- A notion of monodic tree Kleene algebras has been introduced by Takai and Furusawa [TF06] to develop Kleene-like algebras for a class of tree languages, which is called monodic. Though, as reported by [TF08], the proof of their completeness result contains some mistakes, the set of monodic tree languages over a signature still forms a monodic tree Kleene algebra.

- A notion of probabilistic Kleene algebras is introduced by McIver and Weber [MW05] for probabilistic systems. More details will follow in the next section.

Though the notions of these three variants of Kleene algebras are very similar to each other, the relationship between them has not been studied before we study in the paper [NTF09]. By the way Kleene algebras deeply relate complete idempotent semirings (or quantales). In fact, it has already known that every complete idempotent semiring forms a Kleene algebra. Complete idempotent left semirings (IL-semirings) introduced by Möller [Moe04], are relaxations of complete idempotent semirings. In the paper [NTF09] we showed that every complete IL-semiring forms lazy Kleene algebra. Moreover we define a cube consisting of eight classes of lazy Kleene algebras, by introducing three axioms — the 0-axiom, the +-axiom, and the D-axiom — on a lazy Kleene algebra. A lazy Kleene algebra satisfies all of the three axioms if and only if it is a Kleene algebra. Also we define a cube consisting of eight classes of complete IL-semirings, by introducing three conditions (preservation of the right 0, the right +, and all right directed joins) on a complete IL-semiring. A complete IL-semiring satisfies all of the three conditions if and only if it is a complete idempotent semiring. And we obtain a mapping from the second cube to the first cube, by proving that a complete IL-semiring forms a lazy Kleene algebra and that preservation of the right 0, the right +, and all right directed joins on a complete IL-semiring imply the 0-axiom, the +-axiom, and the D-axiom on a lazy Kleene algebra, respectively. These results include the following facts:

- Every complete IL-semiring preserving all directed joins forms a monodic tree Kleene algebra.

- Every complete IL-semiring preserving all directed joins and the right 0 forms a probabilistic Kleene algebra.

1.3 Probabilistic Kleene Algebra

Using probabilistic Kleene algebras, Cohen's separation theorems [Coh00] are generalised for probabilistic distributed systems and the general separation results are applied to Rabin's solution [Rab82] to distributed mutual exclusion with bounded waiting in [MCC06]. This result shows that probabilistic Kleene algebras are useful to simplify a model of probabilistic distributed system without numerical calculations which are usually required and makes difficult to analyze systems while we consider probabilistic behaviors. However a model of probabilistic systems used in these results is too complicated because it includes probabilistic calculus. So it is difficult to put their verification method using probabilistic Kleene algebra in practical use. Then we have to find more abstract semantic domain for probabilistic systems, before their verification method can be put into practical use.

1.4 Multirelations

Up-closed multirelations are studied as a semantic domain of programs. They serve predicate transformer semantics with both of angelic and demonic nondeterminism in the same framework [MCR04, Rew03, RB06]. Also up-closed multirelations provide models of game logic introduced by Parikh [Par85]. The paper [PP03] is an excellent overview of this research area. Operations of the game logic have been studied from an algebraic point of view by [Gor03] and [Ven03]. They have given complete axiomatisation of iteration-free game logic. The iteration in games is corresponding to reflexive transitive closure on multirelations. We have already studied constructions of reflexive and transitive closure of up-closed multirelations in [TNF08b, TNF09].

In the paper [FTN08] authors show that the set of all finitary, total up-closed multirelations forms a probabilistic Kleene algebra. On the other hand, the semantics of probabilistic systems introduced by McIver et al[MCC06, MW05, Web08] can be generalized using probabilistic multirelations. The set of probabilistic multirelations also forms a probablistic Kleene algebra. These facts indicate that there may be a good relationship between probabilistic multirelations and ordinary multirelations. That is why we aim at abstraction between probabilistic multirelations and non-probabilistic multirelations in this thesis.

1.5 Galois Connection

A Galois connection is a particular correspondence between two partially ordered sets, and it appears in a theory of *Abstract Interpretation* formalised by Patrick Cousot et al [Cou00]. Abstract interpretation is a theory of sound approximation of the semantics of computer programs, and it can be viewed as a partial execution of a computer program which gains information about its semantics without performing all the calculations. This thesis will be finished with a comparison of several Galois connections between probabilistic multirelations and non-probablistic multirelations.

1.6 Thesis Outline

Chapter 2 studies basic properties of multirelations, and then shows that classes of multirelations provides models of three weaker variants of Kleene algebras. The material in chapter 2 is based on joint work [FNT09, FTN08, TNF08a] with Hitoshi Furusawa and Koki Nishizawa.

In chapter 3 we make progress on the result of chapter 2. We introduce a notion of type of multirelations. And then we give a sufficient condition on type T so that the set of up-closed multirelations of T belongs to the class, for each of eight classes of relaxation of Kleene algebra. The material in chapter 3 is also based on joint work [NTF09] with Hitoshi Furusawa and Koki Nishizawa.

Chapter 4 introduces another multirelational model of probabilistic Kleene algebra used by Weber et al [MW05, Web08] to obtain counterexamples in the model of probabilistic systems. That model consists of multirelations called bottomed. Bottomed multirelations may not be up-closed. We study the basic properties of bottomed multirelations and show that the set of bottomed multirelations forms a complete IL-semiring.

In chapter 5 we introduce a notion of probabilistic multirelations which is generalization of the semantics of probabilistic distributed systems given by McIver et al[MCC06], [MW05]. And then we show that the set of probabilistic multirelations forms a complete IL-semiring.

Chapter 6 studies relationship between probabilistic systems and non-probabilistic systems. Specifically we consider a number of Galois connections between probabilistic multirelations and ordinary multirelations, and compare them in terms of preservation of the properties.

Chapter 2

Multirelational Models of Lazy Kleene Algebras

This chapter studies basic properties of multirelations, and then shows that classes of multirelations provide models of three weaker variants of Kleene algebras, namely, lazy, monodic tree, and probabilistic Kleene algebras. Also it is shown that these classes of up-closed multirelations need not be models of Kozen's Kleene algebras unlike the case of ordinary binary relations.

2.1 Overview

In this chapter, we give multirelational models of three weaker variants of Kleene algebras. Since these are independently introduced, they have not been investigated from the unified point of view. Our giving models may reveal both of difference and commonality of these. Though it is known that the set of (usual) binary relations on a set forms a Kleene algebra, models here need not be. Essentially, this chapter is reorganizing and revising results (cf. [FTN08], [TNF08a]) presented at the International Conference on Relational Methods in Computer Science, Frauenwörth, Germany, 2008.

This chapter is organized as follows. We begin in Section 2.2 and 2.3 recalling definitions of three weaker variants of Kleene algebras and study basic notions and properties of up-closed multirelations. In Section 2.4, we show that the set of up-closed multirelations on a set forms a lazy Kleene algebra. Though [Moe04] has proved the fact via correspondence between up-closed multirelations and monotone predicate transformers, we prove it without using the correspondence. In the proof, right residue plays an important rôle. We also give an example which shows that the set of up-closed multirelations need not form a monodic tree Kleene algebra. We introduce the notion of finitary up-closed multirelations in the beginning of Section 2.5. Then we show that the set of finitary up-closed multirelations on a set forms a monodic tree Kleene algebra. Tarski's least fixed point theorem for continuous mappings is used to prove it. Assuming a notion called totality, which is introduced by [RB06], we obtain a multirelational model of probabilistic Kleene algebras.

2.2 Lazy, Monodic Tree, and Probabilistic Kleene Algebra

We recall the definition of lazy Kleene algebras introduced by Möller [Moe04].

Definition 2.1. *A tuple* $(K, +, 0, \cdot, 1)$ *satisfying the followings is called an* idempotent left semiring (IL-semiring) [Moe04]

- $(K, +, 0)$ *is an idempotent commutative monoid, that is*

$$0 + a = a \tag{2.1}$$
$$a + b = b + a \tag{2.2}$$
$$a + a = a \tag{2.3}$$
$$a + (b + c) = (a + b) + c \tag{2.4}$$

- $(K, \cdot, 1)$ *is a monoid, that is*

$$a(bc) = (ab)c \tag{2.5}$$
$$1a = a \tag{2.6}$$
$$a1 = a \tag{2.7}$$

- *The followings satisfy:*

$$ab + ac \leq a(b + c) \tag{2.8}$$

$$ac + bc = (a + b)c \tag{2.9}$$

$$0a = 0 \tag{2.10}$$

for all $a, b, c \in K$, where $\cdot$ is omitted and the order $\leq$ is defined by $a \leq b$ iff $a + b = b$.

Definition 2.2. *A* lazy Kleene algebra [Moe04] *is a tuple* $(K, +, \cdot, {}^*, 0, 1)$ *satisfying the followings:*

- $(K, +, 0, \cdot, 1)$ *is IL-semiring.*
- *The unary operator* * *satisfies*

$$1 + aa^* \leq a^* \tag{2.11}$$

$$ab \leq b \implies a^*b \leq b \tag{2.12}$$

for all $a, b, c \in K$.

The notion of monodic tree Kleene algebras introduced by Takai and Furusawa (2006) is as follows.

Definition 2.3. A lazy Kleene algebra $(K, +, \cdot, {}^*, 0, 1)$ satisfying

$$a(b + 1) \leq a \implies ab^* \leq a \tag{2.13}$$

for all $a, b \in K$ is called a *monodic tree Kleene algebra.*

The notion of probabilistic Kleene algebras introduced by [MW05] is as follows.

Definition 2.4. A monodic tree Kleene algebra $(K, +, \cdot, {}^*, 0, 1)$ satisfying

$$a0 = 0 \tag{2.14}$$

for all $a \in K$ is called a *probabilistic Kleene algebra.*

Kozen's Kleene algebras require stronger conditions

$$ab + ac = a(b + c) \tag{2.8'}$$

and

$$ab \leq a \implies ab^* \leq a \tag{2.13'}$$

instead of (2.8) and (2.13), respectively. Note that a probabilistic Kleene algebra satisfying (9') is a Kleene algebra in the sense of [Koz94].

2.3 Up-Closed Multirelation

In this section we recall definitions and basic properties of multirelations and their operations. More precise information on these can be obtained from [MCR04, Rew03, RB06].

A *multirelation* over a set A is a subset of the Cartesian product $A \times \wp(A)$ of A and the power set $\wp(A)$ of A. A multirelation R is called *up-closed* if $(x, X) \in R$ and $X \subseteq Y$ imply $(x, Y) \in R$ for each $x \in A$, $X, Y \subseteq A$. The null multirelation $\emptyset$ and the universal multirelation $A \times \wp(A)$ are up-closed, and will be denoted by 0 and ∇, respectively. The set of up-closed multirelations over A will be denoted by $\mathsf{UMR}(A)$.

For a family $\{R_i \mid i \in I\}$ of up-closed multirelations the union $\bigcup_{i\in I} R_i$ is up-closed since

$$\begin{array}{lll} & (x, X) \in \bigcup_{i\in I} R_i \text{ and } X \subseteq Y & \\ \iff & \exists i \in I.\, (x, X) \in R_i \text{ and } X \subseteq Y & \\ \implies & \exists i \in I.\, (x, Y) \in R_i & (R_i \text{ is up-closed}) \\ \iff & (x, Y) \in \bigcup_{i\in I} R_i \ . & \end{array}$$

So $\mathsf{UMR}(A)$ is closed under arbitrary union $\bigcup$. Then it is immediate that a tuple $(\mathsf{UMR}(A), \bigcup)$ is a sup-semilattice equipped with the least element 0 with respect to the inclusion ordering $\subseteq$.

Remark 2.1. $\mathsf{UMR}(A)$ *is also closed under arbitrary intersection* $\bigcap$. *So,* $\mathsf{UMR}(A)$ *forms a complete lattice together with the union and the intersection.* □

$R + S$ denotes $R \cup S$ for a pair of up-closed multirelations R and S. Then the following holds.

Proposition 2.1. *A tuple* $(\mathsf{UMR}(A), +, 0)$ *is an idempotent commutative monoid.*

For a pair of multirelations $R, S \subseteq A \times \wp(A)$ the composition $R; S$ is defined by

$$(x, X) \in R; S \ \text{ iff } \ \exists Y \subseteq A.((x, Y) \in R \text{ and } \forall y \in Y.(y, X) \in S) \ .$$

It is immediate from the definition that one of the zero laws

$$0 = 0; R$$

is satisfied. The other zero law

$$R; 0 = 0$$

need not hold.

Example 2.1. *Consider the universal multirelation* ∇ *on a singleton set* $\{x\}$*. Then, since* $(x, \emptyset) \in \nabla$*,* $\nabla; 0 = \nabla \neq 0$*.* □

Also the composition ; preserves the inclusion ordering $\subseteq$, that is,

$$P \subseteq P' \text{ and } R \subseteq R' \implies P; R \subseteq P'; R'$$

since

$$\begin{array}{rcl} (x, X) \in P; R & \iff & \exists Y \subseteq A.((x, Y) \in P \text{ and } \forall y \in Y.(y, X) \in R) \\ & \implies & \exists Y \subseteq A.((x, Y) \in P' \text{ and } \forall y \in Y.(y, X) \in R') \\ & \iff & (x, X) \in P'; R' \ . \end{array}$$

If R and S are up-closed, so is the composition $R; S$ since

$$\begin{array}{ll} & (x, X) \in R; S \text{ and } X \subseteq Z \\ \implies & \exists Y \subseteq A.((x, Y) \in R \text{ and } \forall y \in Y.(y, Z) \in S) \qquad (S \text{ is up-closed}) \\ \iff & (x, Z) \in R; S \ . \end{array}$$

In other words, the set $\mathsf{UMR}(A)$ is closed under the composition ;.

Lemma 2.1. *Up-closed multirelations are associative under the composition ;.*

Proof. Let P, Q, and R be up-closed multirelations over a set A. We prove $(P; Q); R \subseteq P; (Q; R)$.

$$\begin{array}{ll} & (x, X) \in (P; Q); R \\ \iff & \exists Y \subseteq A.((x, Y) \in P; Q \text{ and } \forall y \in Y.(y, X) \in R) \\ \iff & \exists Y \subseteq A.(\exists Z \subseteq A.((x, Z) \in P \text{ and } \forall z \in Z.(z, Y) \in Q) \text{ and} \\ & \qquad \forall y \in Y.(y, X) \in R) \\ \implies & \exists Z \subseteq A.((x, Z) \in P \text{ and} \\ & \qquad \forall z \in Z.\exists Y \subseteq A.((z, Y) \in Q \text{ and } \forall y \in Y.(y, X) \in R)) \\ \iff & \exists Z \subseteq A.((x, Z) \in P \text{ and } \forall z \in Z.(z, X) \in Q; R) \\ \iff & (x, X) \in P; (Q; R) \ . \end{array}$$

For $P; (Q; R) \subseteq (P; Q); R$ it is sufficient to show

$$\begin{array}{ll} & \exists Z \subseteq A.((x, Z) \in P \text{ and} \\ & \qquad \forall z \in Z.\exists Y \subseteq A.((z, Y) \in Q \text{ and } \forall y \in Y.(y, X) \in R)) \\ \implies & \exists Y \subseteq A.(\exists Z \subseteq A.((x, Z) \in P \text{ and } \forall z \in Z.(z, Y) \in Q) \text{ and} \\ & \qquad \forall y \in Y.(y, X) \in R) \ . \end{array}$$

Suppose that there exists a set Z such that

$$(x, Z) \in P \text{ and } \forall z \in Z.\exists Y \subseteq A.((z, Y) \in Q \text{ and } \forall y \in Y.(y, X) \in R) \ .$$

If Z is empty, it is obvious since we can take the empty set as Y. Otherwise, take a set Y_z satisfying

$$(z, Y_z) \in Q \text{ and } \forall y \in Y_z.(y, X) \in R$$

for each $z \in Z$. Then set $Y_0 = \bigcup_{z \in Z} Y_z$. Since Q is up-closed, $(z, Y_0) \in Q$ for each z. Also $(y, X) \in R$ for each $y \in Y_0$ by the definition of Y_0. Thus Y_0 satisfies

$$\exists Z \subseteq A.((x, Z) \in P \text{ and } \forall z \in Z.(z, Y_0) \in Q) \text{ and } \forall y \in Y_0.(y, X) \in R \ .$$

□

We used the fact that Q is up-closed to show $P; (Q; R) \subseteq (P; Q); R$. Multirelations need not be associative under composition.

Example 2.2. *Consider multirelations*

$$\begin{aligned} R &= \{(x, \{x, y, z\}), (y, \{x, y, z\}), (z, \{x, y, z\})\} \textit{ and} \\ Q &= \{(x, \{y, z\}), (y, \{x, z\}), (z, \{x, y\})\} \end{aligned}$$

on a set $\{x, y, z\}$. Here, R is up-closed but Q is not. Since $R; Q = 0$, $(R; Q); R = 0$. On the other hand, $R; (Q; R) = R$ since $Q; R = R$ and $R; R = R$. Therefore

$$(R; Q); R \subseteq R; (Q; R)$$

but

$$R; (Q; R) \not\subseteq (R; Q); R \ .$$

Replacing Q with an up-closed multirelation Q' defined by $Q' = Q + R$,

$$R; (Q'; R) = (R; Q'); R$$

holds since $Q'; R = R = R; Q'$. □

The *identity* $1 \in \mathsf{UMR}(A)$ is defined by

$$(x, X) \in 1 \text{ iff } x \in X \ .$$

Lemma 2.2. *The identity satisfies the unit laws, that is,*

$$1; R = R \textit{ and } R; 1 = R$$

for each $R \in \mathsf{UMR}(A)$.

Proof. First, we prove $1;R \subseteq R$.

$$\begin{array}{rcl} (x,X) \in 1;R & \iff & \exists Y \subseteq A.((x,Y) \in 1 \text{ and } \forall y \in Y.(y,X) \in R) \\ & \iff & \exists Y \subseteq A.(x \in Y \text{ and } \forall y \in Y.(y,X) \in R) \\ & \implies & (x,X) \in R \ . \end{array}$$

Conversely, if $(x,X) \in R$, then $(x,X) \in 1;R$ since $(x,\{x\}) \in 1$. Next, we prove $R;1 \subseteq R$.

$$\begin{array}{rcl} (x,X) \in R;1 & \iff & \exists Y \subseteq A.((x,Y) \in R \text{ and } \forall y \in Y.(y,X) \in 1) \\ & \iff & \exists Y \subseteq A.((x,Y) \in R \text{ and } \forall y \in Y.y \in X) \\ & \iff & \exists Y \subseteq A.((x,Y) \in R \text{ and } Y \subseteq X) \\ & \implies & (x,X) \in R \end{array}$$

since R is up-closed. Conversely, if $(x,X) \in R$, then $(x,X) \in R;1$ since, by the definition of 1, $(y,X) \in 1$ for each $y \in X$. □

Therefore the following property holds.

Proposition 2.2. *A tuple* $(\mathsf{UMR}(A), ;, 0, 1)$ *satisfies conditions* (2.5)*,* (2.10)*,* (2.6)*, and* (2.7) *in* Definition 2.4.

As Example 2.1 has shown, the condition (2.14) need not be satisfied. We discuss about this condition in Section 2.6

Since the composition ; preserves the inclusion ordering $\subseteq$, we have

$$\bigcup_{i \in I} R;S_i \subseteq R;(\bigcup_{i \in I} S_i)$$

for each up-closed multirelation R and a family $\{S_i \mid i \in I\}$. Also

$$\bigcup_{i \in I} R_i;S = (\bigcup_{i \in I} R_i);S$$

holds for each up-closed multirelation S and a family $\{R_i \mid i \in I\}$ since

$$\begin{array}{rcl} (x,X) \in \bigcup_{i \in I} R_i;S & \iff & \exists k.((x,X) \in R_k;S) \\ & \iff & \exists k.(\exists Y \subseteq A.((x,Y) \in R_k \text{ and } \forall y \in Y.(y,X) \in S)) \\ & \iff & \exists Y \subseteq A.(\exists k.((x,Y) \in R_k \text{ and } \forall y \in Y.(y,X) \in S)) \\ & \iff & \exists Y \subseteq A.((x,Y) \in \bigcup_{i \in I} R_i \text{ and } \forall y \in Y.(y,X) \in S)) \\ & \iff & (x,X) \in (\bigcup_{i \in I} R_i);S \ . \end{array}$$

Proposition 2.3. *A tuple* $(\mathsf{UMR}(A), +, ;)$ *satisfies conditions* (2.8) *and* (2.9) *in* Definition 2.4.

We give an example showing that the equation (9') need not hold in $\mathsf{UMR}(A)$.

Example 2.3. *Consider the up-closed multirelation*

$$R = \{(x, W) \mid z \in W\} \cup \{(y, W) \mid \{x, z\} \subseteq W\} \cup \{(z, W) \mid \{x, z\} \subseteq W\}$$

on a set $\{x, y, z\}$. *Clearly, this* R *is up-closed. Then,* $R; (1 + R) \not\subseteq R; 1 + R; R$ *since* $(y, \{z\}) \notin R; 1 + R; R$ *though* $(y, \{z\}) \in R; (1 + R)$. □

2.4 Multirelational Model of Lazy Kleene Algebra

For $R \in \mathsf{UMR}(A)$, a mapping $\varphi_R\colon \mathsf{UMR}(A) \to \mathsf{UMR}(A)$ is defined by

$$\varphi_R(\xi) = R; \xi + 1 \ .$$

Since $(\mathsf{UMR}(A), \cup, \cap)$ is a complete lattice and the mapping φ_R preserves the ordering $\subseteq$, φ_R has the least fixed point, given by $\bigcap\{\xi \mid \varphi_R(\xi) \subseteq \xi\}$.

For an up-closed multirelation R we define R^* as

$$R^* = \bigcap\{\xi \mid \varphi_R(\xi) \subseteq \xi\} \ .$$

Then the following (2.15) and (2.16) hold since R^* is the least fixed point of φ_R.

$$1 + R; R^* \subseteq R^* \tag{2.15}$$

$$1 + R; P \subseteq P \implies R^* \subseteq P \tag{2.16}$$

Thus, we have already shown the following proposition.

Proposition 2.4. *A tuple* $(\mathsf{UMR}(A), +, ;, {}^*, 0, 1)$ *satisfies the condition* (2.11) *in* Definition 2.2.

For $P, Q \in \mathsf{UMR}(A)$ we define P/Q as

$$P/Q = \bigcup\{\xi \mid \xi; Q \subseteq P\} \ .$$

Lemma 2.3. *For* $P, Q, R \in \mathsf{UMR}(A)$ *it holds that*

$$R \subseteq P/Q \iff R; Q \subseteq P \ .$$

Proof. Suppose that $R \subseteq P/Q$. By the left distributivity we have

$$\begin{array}{rcl} R;Q \subseteq (P/Q);Q &=& \bigcup\{\xi \mid \xi;Q \subseteq P\};Q \\ &=& \bigcup\{\xi;Q \mid \xi;Q \subseteq P\} \\ &\subseteq& P \ . \end{array}$$

Conversely, suppose that $R;Q \subseteq P$. Since $R \in \{\xi \mid \xi;Q \subseteq P\}$, $R \subseteq P/Q$ holds. □

Proposition 2.5. *For $P, R \in \mathsf{UMR}(A)$ it holds that*

$$R;P \subseteq P \implies R^*P \subseteq P \ .$$

Proof. Suppose that $R;P \subseteq P$. Then we have

$$\begin{array}{rcl} (1 + R;(P/P));P &=& P + R;(P/P);P \\ &\subseteq& P + R;P \\ &\subseteq& P \end{array}$$

since $(P/P);P \subseteq P$. So $1 + R;(P/P) \subseteq (P/P)$ holds. By (2.16) we have $R^* \subseteq P/P$. Therefore $R^*;P \subseteq P$ holds. □

Theorem 2.1. *A tuple $(\mathsf{UMR}(A), +, ;, ^*, 0, 1)$ is a lazy Kleene algebra.*

$(\mathsf{UMR}(A), +, ;, ^*, 0, 1)$ need not satisfy the condition (2.13).

Example 2.4. *Consider up-closed multirelations*

$$\begin{array}{l} P = \{(n, X) \mid X \textit{ is infinite}\} \textit{ and} \\ R = \{(0, \emptyset)\} \cup \{(n, X) \mid \exists m \in X . n \leq m + 1\} \end{array}$$

over the set $\mathbb{N}$ of natural numbers. It can be proved that $\varphi_R(\xi) = R;\xi + 1 \subseteq \xi$ implies $\forall m \in \mathbb{N}.(m, \{0\}) \in \xi$ by induction on m. So, $\forall m \in \mathbb{N}.(m, \{0\}) \in R^*$ holds since R^* is the least fixed point of φ_R. Moreover, $(n, \mathbb{N}) \in P$ holds for a natural number n. Therefore, $(n, \{0\}) \in P;R^*$ holds. Since $(n, \{0\}) \notin P$, we have $P;R^* \not\subseteq P$. However, $P;(R + 1) \subseteq P$ holds. □

Therefore $(\mathsf{UMR}(A), +, ;, ^*, 0, 1)$ need not be a monodic tree Kleene algebra.

2.5 Multirelational Model of Monodic Tree Kleene Algebra

For monodic tree Kleene algebras, we consider a subclass of up-closed multirelations.

Definition 2.5. An up-closed multirelation R is called *finitary* if $(x, Y) \in R$ implies that there exists a finite set Z such that $Z \subseteq Y$ and $(x, Z) \in R$.

Clearly all up-closed multirelations over a finite set are finitary. The set of finitary up-closed multirelations over a set A will be denoted by $\mathsf{UMR}_f(A)$.

Remark 2.2. *An up-closed multirelation R is called* disjunctive *(cf. Pauly and Parikh (2003)) or* angelic *(cf. [MCR04]) if, for each $x \in A$ and each $V \subseteq \wp(A)$,*

$$(x, \bigcup V) \in R \quad \textit{iff} \quad \exists Y \in V.(x, Y) \in R \ .$$

Let R be disjunctive and $(x, X) \in R$. And let V be the set of finite subsets of X. Then $\bigcup V = X$. By disjunctivity, there exists $Y \in V$ such that $(x, Y) \in R$. Also Y is finite by the definition of V. Therefore disjunctive up-closed multirelations are finitary. However, finitary up-closed multirelations need not be disjunctive. Consider a finitary up-closed multirelation $R = \{(x, \{x, y\})\}$ on a set $\{x, y\}$. Then $\bigcup\{\{x\}, \{y\}\} = \{x, y\}$ and $(x, \{x, y\}) \in R$ but $(x, \{x\}), (x, \{y\}) \notin R$. □

It is obvious that $0, 1 \in \mathsf{UMR}_f(A)$. Also the set $\mathsf{UMR}_f(A)$ is closed under arbitrary union $\bigcup$.

Proposition 2.6. *The set $\mathsf{UMR}_f(A)$ is closed under the composition* ;.

Proof. Let P and R be finitary up-closed multirelations. Suppose $(x, X) \in P; R$. Then, by the definition of the composition, there exists $Y \subseteq A$ such that

$$(x, Y) \in P \text{ and } \forall y \in Y.(y, X) \in R \ .$$

Since P is finitary, there exists a finite set $Y_0 \subseteq Y$ such that

$$(x, Y_0) \in P \text{ and } \forall y \in Y_0.(y, X) \in R \ .$$

Also, since R is finitary, there exists a finite set $X_y \subseteq X$ such that $(y, X_y) \in R$ for each $y \in Y_0$. Then the set $\bigcup_{y \in Y_0} X_y$ is a finite subset of X such that

$$(x, \bigcup_{y \in Y_0} X_y) \in P; R$$

since $(y, \bigcup_{y \in Y_0} X_y) \in R$ for each $y \in Y_0$. Therefore $P; R$ is finitary. □

Thus, if R and ξ are finitary, then so is $\varphi_R(\xi)$.

The set $\mathsf{UMR}_f(A)$ need not be closed under arbitrary intersection $\bigcap$.

Example 2.5. *For each natural number i, consider the finitary up-closed multirelation $R_i = \{(1, X) \mid i \in X\}$ over the set $\mathbb{N}$ of natural numbers. Then, $\bigcap\{R_i \mid i \in \mathbb{N}\}$ is not finitary since $\bigcap\{R_i \mid i \in \mathbb{N}\} = \{(1, \mathbb{N})\}$.* □

For a family $\{P_i \mid i \in I\}$ of $P_i \in \mathsf{UMR}_f(A)$ we define that

$$\bigwedge\{P_i \mid i \in I\} = \bigcup\{R \in \mathsf{UMR}_f(A) \mid \forall i \in I.R \subseteq P_i\} \ .$$

Then, in a poset $(\mathsf{UMR}_f(A), \subseteq)$, $\bigwedge\{P_i \mid i \in I\}$ is the greatest lower bound of a family $\{P_i \mid i \in I\}$.

For a finitary up-closed multirelation R we define R^* as

$$R^* = \bigwedge\{\xi \mid \varphi_R(\xi) \subseteq \xi\} \ .$$

Then, as the case of $\mathsf{UMR}(A)$ in the last section, it may be shown that a tuple $(\mathsf{UMR}_f(A), +, ;, ^*, 0, 1)$ is a Lazy Kleene algebra.

Moreover, for a finitary up-closed multirelation R, we obtain bottom-up construction of R^*. Proving the fact, we use the following lemma.

Lemma 2.4. *Let $\mathcal{D}$ be a directed subset of $\mathsf{UMR}_f(A)$ and let $R \in \mathsf{UMR}_f(A)$. Then it holds that*

$$R; (\bigcup \mathcal{D}) = \bigcup\{R; P \mid P \in \mathcal{D}\}.$$

Proof. $\bigcup\{R; P \mid P \in \mathcal{D}\} \subseteq R; (\bigcup \mathcal{D})$ holds by the monotonicity of composition. Suppose $(x, X) \in R; (\bigcup \mathcal{D})$. Then, by the definition of composition, there exists $Y \subseteq A$ such that

$$(x, Y) \in R \text{ and } \forall y \in Y.(y, X) \in \bigcup \mathcal{D} \ .$$

Since R is finitary, there exists a finite set $Y_0 \subseteq Y$ such that

$$(x, Y_0) \in R \text{ and } \forall y \in Y_0.(y, X) \in \bigcup \mathcal{D} \ .$$

Thus there exists $P_y \in \mathcal{D}$ such that $(y, X) \in P_y$ for each $y \in Y_0$. Since $\mathcal{D}$ is directed and Y_0 is finite, there exists $P_0 \in \mathcal{D}$ such that $P_y \subseteq P_0$ for each $y \in Y_0$. Therefore $(x, X) \in R; P_0$, and then $(x, X) \in \bigcup\{R; P \mid P \in \mathcal{D}\}$. □

Proposition 2.7. *Let R be a finitary up-closed multirelation. Then*

$$R^* = \bigcup_{n \geq 0} \varphi_R^n(0) \ ,$$

where φ_R^0 is the identity mapping and $\varphi_R^{n+1} = \varphi_R \circ \varphi_R^n$.

Proof. Since R^* is the least fixed point of φ_R, it is sufficient to show that φ_R is continuous, that is,

$$\bigcup\{\varphi_R(P) \mid P \in \mathcal{D}\} = \varphi_R(\bigcup \mathcal{D})$$

for each directed subset $\mathcal{D}$ of $\mathsf{UMR}_f(A)$. $\bigcup\{\varphi_R(P) \mid P \in \mathcal{D}\} \subseteq \varphi_R(\bigcup \mathcal{D})$ holds by the monotonicity of φ_R. On the other hand, it is obvious that

$$\begin{array}{l} 1 \subseteq \bigcup\{\varphi_R(P) \mid P \in \mathcal{D}\} \text{ and} \\ \bigcup\{R; P \mid P \in \mathcal{D}\} \subseteq \bigcup\{\varphi_R(P) \mid P \in \mathcal{D}\} \end{array}$$

by the definition of φ_R. Also, $R; (\bigcup \mathcal{D}) = \bigcup\{R; P \mid P \in \mathcal{D}\}$ holds by Lemma 2.4. Therefore it holds that $\varphi_R(\bigcup \mathcal{D}) \subseteq \bigcup\{\varphi_R(P) \mid P \in \mathcal{D}\}$. $\square$

Remark 2.3. *The bottom-up construction does not work in the case of* $\mathsf{UMR}(A)$*. Let* $\mathbb{N}$ *be the set of natural numbers and let* ω *satisfy*

$$\forall n \in \mathbb{N}. n < \omega \ .$$

Now consider an up-closed multirelation

$$R = \{(x, X) \mid y < x \implies y \in X\}$$

over $\mathbb{N} \cup \{\omega\}$*, which is not finitary. Then* $\bigcup_{n\geq 0} \varphi_R^n(0)$ *is not a fixed point of* φ_R *since* $(\omega, \emptyset) \notin \bigcup_{n\geq 0} \varphi_R^n(0)$ *and* $(\omega, \emptyset) \in \varphi_R(\bigcup_{n\geq 0} \varphi_R^n(0))$*.* $\square$

A condition related to the operator * is left to check.

Proposition 2.8. *Let* $P, R \in \mathsf{UMR}_f(A)$*. Then the following implication holds.*

$$P; (R + 1) \subseteq P \implies P; R^* \subseteq P$$

Proof. It will be follow from $P; \varphi_R^n(0) \subseteq P$ since

$$P; R^* \subseteq P; (\bigcup_{n\geq 0} \varphi_R^n(0)) = \bigcup_{n\geq 0} P; \varphi_R^n(0) \subseteq P$$

by Lemma 2.4. Supposing that $P; (R + 1) \subseteq P$, we show that $P; \varphi_R^n(0) \subseteq P$ by induction on n. For $n = 0$ it holds since φ_R^0 is the identity. For $n = 1$

$$P; \varphi_R(0) = P; (R; 0 + 1) \subseteq P; (R + 1) \subseteq P \ .$$

Assume that $P; \varphi_R^n(0) \subseteq P$ for $n \geq 1$. Then we have

$$\begin{array}{rcl} P; \varphi_R^{n+1}(0) & = & P; (R; \varphi_R^n(0) + 1) \\ & \subseteq & P; (R; \varphi_R^n(0) + \varphi_R^n(0)) \\ & = & P; (R + 1); \varphi_R^n(0) \\ & \subseteq & P; \varphi_R^n(0) \\ & \subseteq & P \end{array}$$

since $1 \subseteq R; \varphi_R^{n-1}(0) + 1 = \varphi_R^n(0)$ for $n \geq 1$. $\square$

Remark 2.4. *Kozen's Kleene algebras requires the condition (2.13')*

$$ab \le a \implies ab^* \le a$$

instead of (2.13). The following example shows that the condition (2.13') need not hold for finitary up-closed multirelations. Consider the up-closed multirelation R appeared in Example 2.3. Then $R; R \subseteq R$ since

$$R; R = \{(w, W) \mid w \in \{x, y, z\}, \{x, z\} \subseteq W\} \subseteq R \ .$$

Also, we have already seen that $(y, \{z\}) \in R; (R + 1)$ in Example 2.3. Since

$$R; (R+1) \subseteq R; \varphi_R^2(0) \subseteq R; (\bigcup_{n \ge 0} \varphi_R^n(0)) = R; R^* \ ,$$

$(y, \{z\}) \in R; R^*$. But $(y, \{z\}) \notin R$. So, $R; R^* \not\subseteq R$ in spite of $R; R \subseteq R$. □

We have already shown the following.

Theorem 2.2. *A tuple $(\mathsf{UMR}_f(A), +, ;, ^*, 0, 1)$ is a monodic tree Kleene algebras.*

Example 2.1 shows that $(\mathsf{UMR}_f(A), +, ;, ^*, 0, 1)$ need not be a probabilistic Kleene algebra.

2.6 Multirelational Model of Probabilistic Kleene Algebra

It has been shown by [RB06] that the following notion ensures the right zero law.

Definition 2.6. A multirelation R on a set A is called *total* if $(x, \emptyset) \notin R$ for each $x \in A$.

Clearly, the null multirelation 0 and the identity 1 are total.

The set of total finitary up-closed multirelations will be denoted by $\mathsf{UMR}_f^+(A)$. Then $\mathsf{UMR}_f^+(A)$ is closed under $\bigcup$, $\bigwedge$, ;, and *.

Theorem 2.3. *A tuple $(\mathsf{UMR}_f^+(A), +, ;, ^*, 0, 1)$ is a probabilistic Kleene algebra.*

$(\mathsf{UMR}_f^+(A), +, ;, ^*, 0, 1)$ need not be a Kozen's Kleene algebra. It is induced from either Example 2.3 or the last remark in which we consider only finitary total up-closed multirelations.

Table 2.1: Summary

	$\mathsf{UMR}(A)$	$\mathsf{UMR}_f(A)$	$\mathsf{UMR}_f^+(A)$
lazy KA?	◯	◯	◯
monodic tree KA?	×	◯	◯
probabilistic KA?	×	×	◯
KA?	×	×	×

◯ : Yes
× : Not always

2.7 Summary

This chapter has studied up-closed multirelations carefully. Then we have shown that classes of up-closed multirelations provides models of three weaker variants of Kleene algebras:

- the set $\mathsf{UMR}(A)$ of up-closed multirelations forms a lazy Kleene algebra,
- the set $\mathsf{UMR}_f(A)$ of finitary up-closed multirelations forms a monodic tree Kleene algebra,
- and the set $\mathsf{UMR}_f^+(A)$ of total finitary up-closed multirelations forms a probabilistic Kleene algebra.

Also we have shown that

- (2.13) need not hold in $\mathsf{UMR}(A)$ and
- (2.14) need not hold in $\mathsf{UMR}(A)$ nor $\mathsf{UMR}_f(A)$.

Table 2.1 summarizes the results of this chapter.

Chapter 3

Cube of Lazy Kleene Algebras and Triangular Prism of Multirelations

In this chapter, we refine and extend the known results that the set of ordinary binary relations forms a Kleene algebra, the set of up-closed multirelations forms a lazy Kleene algebra, the set of up-closed finite multirelations forms a monodic tree Kleene algebra, and the set of total up-closed finite multirelations forms a probabilistic Kleene algebra. For the refinement, we introduce a notion of type of multirelations. For each of eight classes of relaxation of Kleene algebra, we give a sufficient condition on type T so that the set of up-closed multirelations of T belongs to the class. Some of the conditions are not only sufficient, but also necessary.

3.1 Overview

We study the relationship between the two different research topics. It is known that the set of ordinary binary relations on a set forms a Kleene algebra. However, it does not seem that there are enough results about what class of multirelations forms what relaxation of Kleene algebras. In chapter 2 we show that the set of up-closed multirelations forms a lazy Kleene algebra, that the set of finitary up-closed multirelations forms a monodic tree Kleene algebra, and that the set of total finitary up-closed multirelations forms a probabilistic Kleene algebra. This chapter extends these results as follows.

First, we define a cube consisting of eight classes of lazy Kleene algebras, by introducing three axioms (the 0-axiom, the +-axiom, and the D-axiom) on a lazy Kleene algebra. And also we define a cube consisting of eight classes of complete IL-semirings, by introducing three conditions (preservation of the right 0, the right +, and all right directed joins) on a complete IL-semiring. And we obtain a mapping from the second cube to the first cube, by proving that a complete IL-semiring forms a lazy Kleene algebra and that preservation of the right 0, the right +, and all right directed joins on a complete IL-semiring imply the 0-axiom, the +-axiom, and the D-axiom on a lazy Kleene algebra, respectively. This is a new explanation of the fact that a complete I-semiring forms a Kleene algebra.

Second, we focus on a notion of multirelations. While a multirelation over a set A is defined to be a subset of $A \times \wp(A)$, this chapter extends this notion. We call a subfunctor T of the covariant powerset functor $\wp\colon \mathbf{Set} \to \mathbf{Set}$ a *type* where **Set** is the category of sets and call a subset of $A \times T(A)$ a *multirelation of type T over A*. And we give a sufficient condition on T such that the set of up-closed multirelations of T forms a complete IL-semiring. We call a type satisfying this condition a *closed type*. We also define a cube consisting of eight classes of closed types, by introducing three conditions (total, affine and finite) on a closed type. The cube is actually a triangular prism, since affineness implies finiteness. We show that a closed type T is total, affine, and finite *if and only if* the set of up-closed multirelations of type T over an arbitrary set A forms a complete IL-semiring preserving the right 0, the right +, and all right directed joins, respectively.

Combining the above results, we show which type of up-closed multirelations forms a lazy Kleene algebra satisfying which axiom. The result includes the results for ordinary binary relations, up-closed multirelations, finitary up-closed multirelations, and total finitary up-closed multirelations.

This chapter is organized as follows. Section 3.2 shows that the set of up-closed multirelations forms a complete IL-semiring. In Section 3.3, we show that every complete IL-semiring forms a lazy Kleene algebra. Section 3.4 defines the cube consisting of eight classes of lazy Kleene algebras. In Section 3.5, we define the cube consisting of eight classes of complete IL-semirings and define a mapping from it to the cube of lazy Kleene algebras. Section 3.6 defines a notion of types, a triangular prism consisting of six classes of types, and a mapping from it to the cube of complete IL-semirings. Section 3.7 summarizes this work and future work.

3.2 Multirelational Model of Complete IL-semiring

In this section, we show that the set of up-closed multirelations forms a complete IL-semiring.

Complete IL-semirings are relaxations of complete I-semirings (or quantales).

Definition 3.1. *A* complete IL-semiring *is a tuple* $(K, +, 0, \cdot, 1, \bigvee)$ *with the following properties:*

1. $(K, +, 0, \cdot, 1)$ *is an IL-semiring.*
2. $(K, \leq)$ *has the join* $\bigvee S$ *for each subset* S *of* K*.*
3. $(\bigvee S) \cdot a = \bigvee\{x \cdot a | x \in S\}$.

A complete IL-semiring also has the meet (greatest lower bound) for each subset. We write $\bigwedge S$ for the meet of subset S.

Example 3.1. *For a set* A*, a tuple* $(K, +, 0, \cdot, 1, \bigvee)$ *forms a complete IL-semiring where*

- K *is the set of all ordinary binary relations over* A*,*
- $R + Q$ *is the binary union of* R *and* Q*,*
- 0 *is the empty relation,*
- $R \cdot Q$ *is the composition of* R *and* Q*,*
- 1 *is the identity (diagonal) relation on* A*, and*
- $\bigvee$ *is the union operator.*

We obtain the following proposition by the proposition 2.1, 2.2, 2.3.

Proposition 3.1. *For a set* A*, a tuple* $\mathsf{UMR}(A) = (K, +, 0, \cdot, 1, \bigvee)$ *forms a complete IL-semiring where*

- *K is the set of all up-closed multirelations over A,*

- *$R + Q$ is the binary union of R and Q,*

- *0 is the empty set,*

- *$(a, X) \in R \cdot Q \iff \exists Y.(a, Y) \in R$ and $\forall y \in Y.(y, X) \in Q$,*

- *$1 = \{(a, X) | a \in X, X \subseteq A\}$, and*

- *$\bigvee$ is the union operator.*

Up-closed multirelations can not be composed in the same way as ordinary binary relations. The above operation $R \cdot Q$ is called the *composition* of up-closed multirelations R, Q.

3.3 Complete IL-semirings and Lazy Kleene Algebras

In this section, we show the theorem that a complete IL-semiring forms a lazy Kleene algebra.

Every complete IL-semiring $(K, +, 0, \cdot, 1, \bigvee)$ satisfies $a \cdot b \leq c \iff a \leq c/b$ where $c/b = \bigvee\{x \in K \mid x \cdot b \leq c\}$ (left residual). Note that $(c/b) \cdot b \leq c$ holds, since $(c/b) \cdot b \leq c \iff c/b \leq c/b$.

Theorem 3.1. *Every complete IL-semiring forms a lazy Kleene algebra. Moreover, every homomorphism between complete IL-semirings is also a homomorphism between the induced lazy Kleene algebras.*

Proof. Consider a complete IL-semiring $(K, +, 0, \cdot, 1, \bigvee)$. For each $a \in K$, the function $f(x) = 1 + a \cdot x$ is monotone, since $+$ and $\cdot$ are monotone. By Tarski's fixed point theorem, we have

- $1 + a \cdot a^* \leq a^*$ and

- $1 + a \cdot b \leq b$ implies $a^* \leq b$

where $a^* = \bigwedge\{x|1 + a \cdot x \leq x\}$. Therefore, the second property of Definition 2.2 is satisfied. The third property is satisfied, since

$$\begin{array}{rcl} a^* \cdot b \leq c & \Longleftrightarrow & a^* \leq c/b \\ & \Longleftarrow & 1 + a \cdot (c/b) \leq c/b \\ & \Longleftrightarrow & (1 + a \cdot (c/b)) \cdot b \leq c \\ & \Longleftrightarrow & 1 \cdot b + a \cdot (c/b) \cdot b \leq c \\ & \Longleftarrow & b + a \cdot c \leq c. \end{array}$$

Therefore, it is proved that $(K, +, 0, \cdot, 1, {}^*)$ forms a lazy Kleene algebra.

Next, we prove the property about homomorphisms. Let $(K, +, 0, \cdot, 1, \bigvee)$ and $(L, +, 0, \cdot, 1, \bigvee)$ be complete IL-semirings. Let $(K, +, 0, \cdot, 1, {}^*)$ and $(L, +, 0, \cdot, 1, {}^*)$ be the induced lazy Kleene algebras. Let f be a function $f\colon K \to L$ preserving $+$, 0, $\cdot$, 1, and $\bigvee$. The following $g\colon L \to K$ is called the right adjoint to f and it satisfies $f(x) \leq y \iff x \leq g(y)$.

$$g(y) = \bigvee\{x \in K \mid f(x) \leq y\}$$

Now, f preserves * as follows.

$$\begin{array}{rcl} (f(a))^* \leq f(a^*) & \Longleftarrow & 1 + f(a) \cdot f(a^*) \leq f(a^*) \\ & \Longleftrightarrow & f(1 + a \cdot a^*) \leq f(a^*) \\ & \Longleftarrow & 1 + a \cdot a^* \leq a^* \end{array}$$

$$\begin{array}{rcl} f(a^*) \leq (f(a))^* & \Longleftrightarrow & a^* \leq g((f(a))^*) \\ & \Longleftarrow & 1 + a \cdot g((f(a))^*) \leq g((f(a))^*) \\ & \Longleftrightarrow & f(1 + a \cdot g((f(a))^*)) \leq (f(a))^* \\ & \Longleftrightarrow & 1 + f(a) \cdot f(g((f(a))^*)) \leq (f(a))^* \\ & \Longleftarrow & 1 + f(a) \cdot (f(a))^* \leq (f(a))^* \end{array}$$

□

3.4 Cube of Kleene Algebras

In this section, we define a cube consisting of eight classes of lazy Kleene algebras, by defining three independent axioms. A lazy Kleene algebra satisfying all of the three axioms is a Kleene algebra. Therefore, the cube consists of eight classes between lazy Kleene algebras and Kleene algebras.

Definition 3.2 (Cube of lazy Kleene algebra)**.** *A tuple* $(K, +, 0, \cdot, 1, {}^*)$ *is called a lazy Kleene algebra satisfying*

- *the* 0-axiom *if* $a \cdot 0 = 0$ *for each* $a \in K$*,*
- *the* $+$-axiom *if* $a \cdot (b + c) = a \cdot b + a \cdot c$ *for each* $a, b, c \in K$*, and*
- *the* D-axiom *if* $a \cdot (b + 1) \leq a$ *implies* $a \cdot b^* \leq a$ *for each* $a, b \in K$*,*

respectively.

The reason why we call the third axiom the D-axiom is that this axiom has a relationship with directed sets (explained in the next section).

We write **LKA** for the category whose objects are lazy Kleene algebras and whose arrows are homomorphisms between them. We write $\mathbf{LKA}_0$ for the full subcategory of **LKA** whose objects are lazy Kleene algebras satisfying the 0-axiom. Similarly, we define $\mathbf{LKA}_{0,+,D}$, $\mathbf{LKA}_{0,+}$, and so on. The eight categories and forgetful functors between them form the cube of Fig. 3.1.

$$
\begin{tikzcd}
\mathsf{LKA}_{0,+,D} \arrow[rr] \arrow[dr] \arrow[dd] & & \mathsf{LKA}_{0,+} \arrow[dr] \arrow[dd] & \\
& \mathsf{LKA}_{0,D} \arrow[rr] \arrow[dd] & & \mathsf{LKA}_0 \arrow[dd] \\
\mathsf{LKA}_{+,D} \arrow[rr] \arrow[dr] & & \mathsf{LKA}_{+} \arrow[dr] & \\
& \mathsf{LKA}_D \arrow[rr] & & \mathsf{LKA}
\end{tikzcd}
$$

Figure 3.1: The cube of lazy Kleene algebras

Objects of $\mathbf{LKA}_D$, $\mathbf{LKA}_{0,D}$, and $\mathbf{LKA}_{0,+,D}$ are known as monodic tree Kleene algebras, probabilistic Kleene algebras, and Kleene algebras, respectively. We obtain the followings immediately.

Proposition 3.2. *A lazy Kleene algebra satisfies the D-axiom if and only if it is a monodic tree Kleene algebra [TF06]. A lazy Kleene algebra satisfies the* 0*-axiom and the D-axiom if and only if it is a probabilistic Kleene algebra [MW05]. A lazy Kleene algebra satisfies the* 0*-axiom, the* $+$*-axiom, and the D-axiom if and only if it is a Kleene algebra [Koz94].*

3.5 Cube of Complete IL-Semirings

In this section, we define a cube consisting of eight classes of complete IL-semirings, by introducing three independent axioms on a complete IL-semiring. We also obtain a mapping from it to the cube of the previous section, by using Theorem 3.1 and proving that the three conditions on a complete IL-semiring imply the three axioms on a lazy Kleene algebra, respectively.

Definition 3.3 (Directed set)**.** *A subset S of a lattice is called* directed *if each finite subset of S has an upper bound in S.*

A directed set always has an element, since a directed set must have an upper bound of the empty subset.

Definition 3.4 (Cube of complete IL-semiring)**.** *A tuple $(K, +, 0, \cdot, 1, \bigvee)$ is called a complete IL-semiring preserving*

- *the* right 0 *if $a \cdot 0 = 0$ for each $a \in K$,*
- *the* right + *if $a \cdot (b + c) = a \cdot b + a \cdot c$ for each $a, b, c \in K$, and*
- *all* right directed joins *if $a \cdot \bigvee S = \bigvee\{a \cdot x | x \in S\}$ for each $a \in K$ and each directed $S \subseteq K$,*

respectively.

We write **CILS** for the category whose objects are complete IL-semirings and whose arrows are homomorphisms between them. We write $\mathbf{CILS}_D$ for the full subcategory of **CILS** whose objects are complete IL-semirings preserving all right directed joins. Similarly, we define $\mathbf{CILS}_{0,+,D}$, $\mathbf{CILS}_{0,+}$, and so on. The eight categories and forgetful functors between them form the cube of Fig. 3.2.

Proposition 3.3. *A tuple $(K, +, 0, \cdot, 1, \bigvee)$ is a complete I-semiring [Moe04] (or, quantale) if and only if it is a complete IL-semiring preserving the right* 0*, the right* +*, and all right directed joins.*

Proof. A complete I-semiring is defined to be a complete IL-semiring satisfying $a \cdot (\bigvee S) = \bigvee\{a \cdot x | x \in S\}$. Trivially, a complete I-semiring is a complete IL-semiring preserving the right 0, the right +, and all right directed joins. Conversely, let K be a complete IL-semiring preserving the right 0, the right +, and all right directed

$$
\begin{tikzcd}
\mathbf{CILS}_{0,+,D} \arrow[rr] \arrow[dr] \arrow[dd] & & \mathbf{CILS}_{0,+} \arrow[dr] \arrow[dd] & \\
& \mathbf{CILS}_{0,+} \arrow[rr] \arrow[dd] & & \mathbf{CILS}_{0} \arrow[dd] \\
\mathbf{CILS}_{+,D} \arrow[rr] \arrow[dr] & & \mathbf{CILS}_{+} \arrow[dr] & \\
& \mathbf{CILS}_{D} \arrow[rr] & & \mathbf{CILS}
\end{tikzcd}
$$

Figure 3.2: The cube of complete IL-semirings

joins. For an arbitrary subset S of K, $\bigvee S = \bigvee\{\bigvee X \mid X \subseteq S, X \text{ is finite}\}$ and the set $\{\bigvee X \mid X \subseteq S, X \text{ is finite}\}$ is directed. Therefore,

$$
\begin{array}{rcl}
a \cdot (\bigvee S) & = & a \cdot (\bigvee\{\bigvee X \mid X \subseteq S, X \text{ is finite}\}) \\
& = & \bigvee\{a \cdot (\bigvee X) \mid X \subseteq S, X \text{ is finite}\} \\
& = & \bigvee\{\bigvee\{a \cdot x \mid x \in X\} \mid X \subseteq S, X \text{ is finite}\} \\
& = & \bigvee\{a \cdot x \mid x \in S\}.
\end{array}
$$

□

Theorem 3.2. *Every complete IL-semiring C forms a lazy Kleene algebra L. Moreover, the following hold.*

1. *L satisfies the 0-axiom if and only if C preserves the right 0.*

2. *L satisfies the $+$-axiom if and only if C preserves the right $+$.*

3. *L satisfies the D-axiom if C preserves all right directed joins.*

Proof. Similarly to the proof of Theorem 3.1, we construct L from C. By the construction, the case 1 and the case 2 trivially hold. We show the case 3. Assume that C preserves all right directed joins. Each function $f_b(x) = 1 + b \cdot x$ preserves the join of an arbitrary directed subset. Therefore, by the fixed point theorem, the least fixed point b^* of f_b is equal to $\bigvee\{f_b^n(0) | n \in \mathbb{N}\}$. Assume $a \cdot (b + 1) \leq a$. We show that $a \cdot f_b^n(0) \leq a$ holds for each $n \in \mathbb{N}$ by induction on n.

$(n = 0)$ $a \cdot f_b^0(0) = a \cdot 0 \leq a \cdot 1 = a$.

$(n = 1)$ $a \cdot f_b^1(0) = a \cdot (1 + b \cdot 0) \leq a \cdot (1 + b \cdot 1) \leq a$.

$(n \geq 2)$ Note that $1 \leq 1 + b \cdot f_b^{n-2}(0) = f_b^{n-1}(0)$. Assume $a \cdot f_b^{n-1}(0) \leq a$. Then, we have

$$\begin{aligned} a \cdot f_b^n(0) &= a \cdot (1 + b \cdot f_b^{n-1}(0)) \\ &\leq a \cdot (f_b^{n-1}(0) + b \cdot f_b^{n-1}(0)) \\ &\leq a \cdot (1 + b) \cdot f_b^{n-1}(0) \\ &\leq a \cdot f_b^{n-1}(0) \\ &\leq a. \end{aligned}$$

Therefore, we have $\bigvee\{a \cdot f_b^n(0) | n \in \mathbb{N}\} \leq a$. Since the set $\{f_b^n(0) | n \in \mathbb{N}\}$ is directed and C preserves all right directed joins, we have

$$a \cdot b^* = a \cdot \bigvee\{f_b^n(0) | n \in \mathbb{N}\} = \bigvee\{a \cdot f_b^n(0) | n \in \mathbb{N}\} \leq a.$$

□

In the above theorem, 1 and 2 give necessary and sufficient conditions respectively, but 3 does not. In fact, all authors do not know whether if L satisfies the D-axiom then C preserves all right directed joins.

This theorem can be represented by Fig. 3.3. The functor F from **CILS** to **LKA** is given by Theorem 3.1. The other seven functors from the cube of complete IL-semirings to the cube of lazy Kleene algebras are given by Theorem 3.2. By 1 of Theorem 3.2, the square consisting of **CILS**, $\mathbf{CILS}_0$, **LKA**, and $\mathbf{LKA}_0$ is not only a commutative square, but also a pullback square in **Cat**, that is, an object C of **CILS** belongs to $\mathbf{CILS}_0$ *if and only if* $F(C)$ belongs to $\mathbf{LKA}_0$. Similarly, every square in Fig. 3.3 is a pullback square, except for squares consisting of three solid arrows and one dotted arrow.

3.6 Triangular Prism of Multirelations

In chapter 2, we show that the set of up-closed multirelations forms a lazy Kleene algebra, that the set of finitary up-closed multirelations forms a monodic tree Kleene algebra, and that the set of total finitary up-closed multirelations forms a probabilistic Kleene algebra. To extend these results, in this section, we define a triangular prism consisting of six classes of multirelations and obtain a mapping from it to the cube of lazy Kleene algebras.

First, we extend the notion of multirelations.

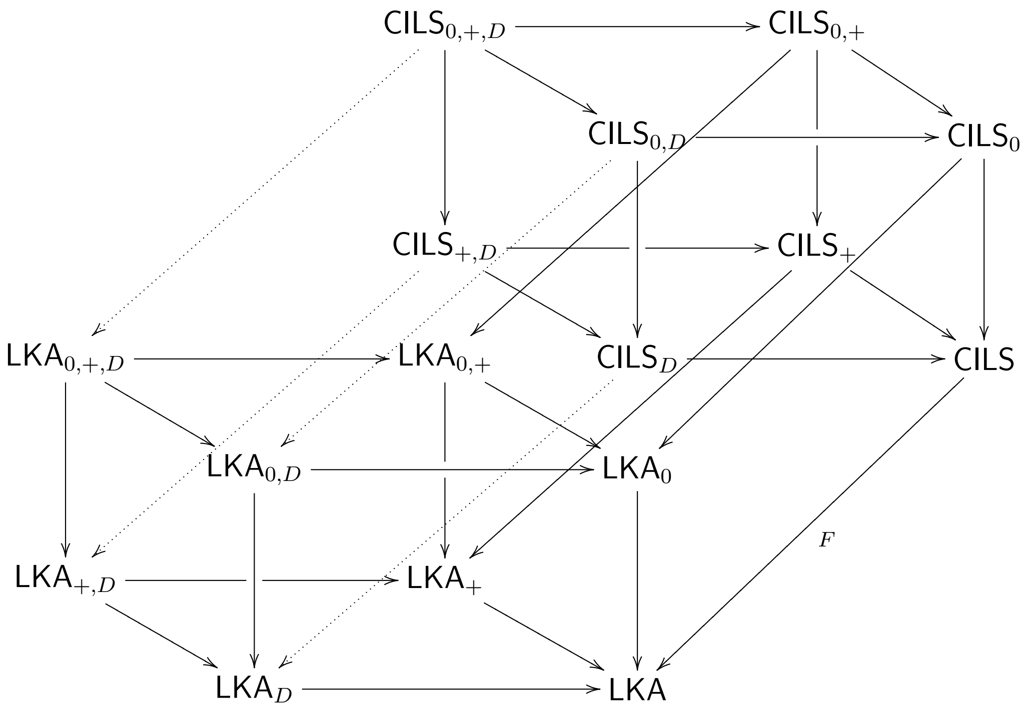

Figure 3.3: The maps from the cube of **CILS** to the cube of **LKA**

Definition 3.5 (Typed multirelation)**.** *A* type T *of multirelation is a subfunctor of the powerset functor* $\wp$: **Set** $\to$ **Set** *(i.e.,* $T(A) \subseteq \wp(A)$ *for each set* A*). A* multirelation of type T over A *is a subset of* $A \times T(A)$*. A multirelation* R *of type* T *over* A *is called* up-closed *if* $(a, X) \in R$ *and* $X \subseteq Y$ *imply* $(a, Y) \in R$ *for each* $a \in A$*,* $X, Y \in T(A)$*.*

We give a sufficient condition on a type T such that the set of up-closed multirelations of type T over an arbitrary set A forms a complete IL-semiring. We call a type satisfying this condition *closed.*

Definition 3.6 (Closed type)**.** *A type* T *is called* closed *if for each set* A*,*

1. $\forall a \in A.\{a\} \in T(A)$*, and*

2. *if a family* $\{X_i\}_{i\in I}$ *of subsets of* A *satisfies* $I \in T(A)$ *and* $\forall i \in I.X_i \in T(A)$*, then* $\bigcup_{i\in I} X_i \in T(A)$*.*

Example 3.2. *Every submonad of the powerset monad forms a closed type. In fact, all closed types mentioned in this section are submonads of the powerset monad.*

Proposition 3.4. *For an arbitrary set A, a tuple T-$\mathsf{UMR}(A) = (K, +, 0, \cdot, 1, \bigvee)$ forms a complete IL-semiring where*

- *K is the set of all up-closed multirelations of type T over A,*
- *$R + Q$ is the binary union of R and Q,*
- *0 is the empty set,*
- *$(a, X) \in R \cdot Q \iff \exists Y \in T(A).(a, Y) \in R$ and $\forall y \in Y.(y, X) \in Q$,*
- *$1 = \{(a, X) | a \in X, X \in T(A)\}$, and*
- *$\bigvee$ is the union operator,*

if and only if T is a closed type or the constant functor to the empty set.

Proof. ($\Longleftarrow$) If T is the constant functor to the empty set, then T-$\mathsf{UMR}(A)$ is the trivial complete IL-semiring.

On the other hand, let T be a closed type. We show $R \subseteq 1 \cdot R$. If $T(A) = \emptyset$, then $R = 0 \subseteq 1 \cdot R$. Assume $T(A) \neq \emptyset$ and $(a, X) \in R$. By the first condition of Definition 3.6, we have $\{a\} \in T(A)$. Therefore, $(a, X) \in 1 \cdot R$. Therefore, $R \subseteq 1 \cdot R$.

Next, we show $R \cdot (Q \cdot P) \subseteq (R \cdot Q) \cdot P$. Assume $(a, X) \in R \cdot (Q \cdot P)$. Then, there exists $Y \in T(A)$ such that $(a, Y) \in R$ and $\forall y \in Y.\exists Z_y \in T(A).(y, Z_y) \in Q$ and $\forall z \in Z_y.(z, X) \in P$. By the second condition of Definition 3.6, we have $\bigcup_{y \in Y} Z_y \in T(A)$. It satisfies $(a, \bigcup_{y \in Y} Z_y) \in R \cdot Q$, since $(a, Y) \in R$ and $\forall y \in Y.(y, \bigcup_{y \in Y} Z_y) \in Q$. Since $\forall z \in \bigcup_{y \in Y} Z_y.(z, X) \in P$, we have $(a, X) \in (R \cdot Q) \cdot P$. Therefore, $R \cdot (Q \cdot P) \subseteq (R \cdot Q) \cdot P$.

The other conditions for complete IL-semirings are easy to prove.

($\Longrightarrow$) Assume that T is neither a closed type nor the constant functor to the empty set. There exists a set A which does not satisfy 1 of Definition 3.6 or which does not satisfy 2 of Definition 3.6. We show that T-$\mathsf{UMR}(A)$ does not form a complete IL-semiring.

- Assume that 1 of Definition 3.6 does not hold. We can take $a \in A$ satisfying $\{a\} \notin T(A)$. Since T is a functor on **Set**, if $T(A)$ is empty, then $T(X)$ is empty for each set X, that is, T is the constant functor to the empty set. Therefore, $T(A)$ is not empty. We can take $X \in T(A)$. Let $R = \{(a, Y) | Y \in T(A)\}$. We have $(a, X) \in R$ but $(a, X) \notin 1 \cdot R$. Therefore, $R \not\subseteq 1 \cdot R$.
- Assume that 2 of Definition 3.6 does not hold. We can take $\{X_i\}_{i \in I}$ satisfying $I \in T(A)$, $\forall i \in I.X_i \in T(A)$, and $\bigcup_{i \in I} X_i \notin T(A)$. If $A = \emptyset$ then every

$T(A) \subseteq \wp(A)$ (i.e., $T(A) = \emptyset$ or $T(A) = \{\emptyset\}$) satisfies the second condition of Definition 3.6. Therefore, A is not empty. We can take $a \in A$. Let $R = \{(a, X) | X \in T(A), I \subseteq X\}$, $Q = \{(i, X) | i \in I, X \in T(A), X_i \subseteq X\}$, and $P = \{(x, X) | x \in \bigcup_{i \in I} X_i, X \in T(A)\}$. Then, we have $(a, I) \in R \cdot (Q \cdot P)$, since $(a, I) \in R$, $\forall i \in I.(i, X_i) \in Q$, and $\forall i \in I.\forall x \in X_i.(x, I) \in P$. But we have $(a, I) \notin (R \cdot Q) \cdot P$, since $(a, I) \in (R \cdot Q) \cdot P$ implies $\bigcup_{i \in I} X_i \in T(A)$. Therefore, $R \cdot (Q \cdot P) \not\subseteq (R \cdot Q) \cdot P$.

□

By the above proposition, T is not always closed, even if T-$\mathsf{UMR}(A)$ forms a complete IL-semiring for an arbitrary set A. However, this is not a problem, since the trivial complete IL-semiring is not such an important counterexample.

We write $|X|$ for the number of elements of X.

Definition 3.7 (Cube of type of multirelation)**.** *A closed type T of multirelations is called*

- total *if for an arbitrary set A, $A \neq \emptyset$ implies $\emptyset \notin T(A)$,*
- affine *if for an arbitrary set A, $\forall X \in T(A).|X| \leq 1$, and*
- finite *if for an arbitrary set A, $\forall X \in T(A).X$ is finite,*

respectively.

We write UMR for the category whose objects are complete IL-semirings T-$\mathsf{UMR}(A)$ for some closed type T and some set A and whose arrows are homomorphisms between them. We write UMR_t for the full subcategory of UMR whose object is a complete IL-semiring T-$\mathsf{UMR}(A)$ for some total closed type T and some set A. Similarly, we write UMR_a for the case of affine closed types and UMR_f for the case of finite closed types. The eight categories and forgetful functors between them form the cube of Fig. 3.4. Note that $\mathsf{UMR}_{a,f} = \mathsf{UMR}_a$ and $\mathsf{UMR}_{t,a,f} = \mathsf{UMR}_{t,a}$ since affineness implies finiteness. Therefore, this cube is actually a triangular prism.

Example 3.3. *$T(A) = \wp(A)$ is a closed type. In this case, T-$\mathsf{UMR}(A)$ is equal to the complete IL-semiring $\mathsf{UMR}(A)$ consisting of all up-closed multirelations on A (defined in Proposition 3.1).*

$$
\begin{tikzcd}
\mathsf{UMR}_{t,a,f} \arrow[rr, equal] \arrow[dr] \arrow[dd] & & \mathsf{UMR}_{t,a} \arrow[dr] \arrow[dd] & \\
& \mathsf{UMR}_{t,f} \arrow[rr] \arrow[dd] & & \mathsf{UMR}_{t} \arrow[dd] \\
\mathsf{UMR}_{a,f} \arrow[rr, equal] \arrow[dr] & & \mathsf{UMR}_{a} \arrow[dr] & \\
& \mathsf{UMR}_{f} \arrow[rr] & & \mathsf{UMR}
\end{tikzcd}
$$

Figure 3.4: The cube of complete IL-semirings of multirelations

Example 3.4. $T(A) = \{\{a\} | a \in A\}$ *is a closed, total, and affine (and finite) type. In this case,* T-$\mathsf{UMR}(A)$ *is isomorphic to the complete IL-semiring consisting of all ordinary binary relations on* A *(defined in Example 3.1).*

We obtain the correspondence between the cube of Fig. 3.4 and the cube of complete IL-semirings.

Theorem 3.3. *Let* T *be a closed type.* T-$\mathsf{UMR}(A)$ *forms a complete IL-semiring for each* A*. Moreover, the following hold.*

1. T-$\mathsf{UMR}(A)$ *preserves the right* 0 *for each* A *if and only if* T *is total,*

2. T-$\mathsf{UMR}(A)$ *preserves the right* $+$ *for each* A *if and only if* T *is affine, and*

3. T-$\mathsf{UMR}(A)$ *preserves all right directed joins for each* A *if and only if* T *is finite.*

Proof. 1. ($\Longleftarrow$) Assume that T is total. If $A = \emptyset$, then $R \cdot 0 = 0 \cdot 0 = 0$. If $A \neq \emptyset$, then $R \cdot 0 = \{(a, X) \,|\, X \in T(A), (a, \emptyset) \in R\} = 0$.

($\Longrightarrow$) Conversely, assume that T is not total. Let R be $A \times T(A)$. There exists a set A satisfying $A \neq \emptyset$ and $\emptyset \in T(A)$. There exists $a \in A$ such that $(a, \emptyset) \in R$. Therefore, $R \cdot 0 = \{(a, X) \,|\, X \in T(A), (a, \emptyset) \in R\} \neq 0$.

2. ($\Longleftarrow$) Assume that T is affine. $R \cdot Q + R \cdot P \subseteq R \cdot (Q + P)$ holds trivially. We show $R \cdot (Q+P) \subseteq R \cdot Q + R \cdot P$. Let (a, X) be an element of $R \cdot (Q+P)$. We can take $Y \in T(A)$ such that $(a, Y) \in R$ and $\forall y \in Y.(y, X) \in Q+P$. If $|Y| = 0$, then $(a, \emptyset) \in R$. Therefore, $(a, X) \in R \cdot Q \subseteq R \cdot Q + R \cdot P$. If $|Y| = 1$, then $Y = \{y\}$

and $(y, X) \in Q+P$. Moreover, if $(y, X) \in Q$, then $(a, X) \in R \cdot Q \subseteq R \cdot Q + R \cdot P$. If $(y, X) \in P$, then $(a, X) \in R \cdot P \subseteq R \cdot Q + R \cdot P$.

($\Longrightarrow$) Conversely, assume that T is not affine. Take a set A and $X \in T(A)$ satisfying $2 \leq |X|$, and take $a \in X$. Let $R = \{(a, Y) | X \subseteq Y, Y \in T(A)\}$, $Q = \{(a, Y) | a \in Y, Y \in T(A)\}$, and $P = \bigcup_{y \in X \setminus \{a\}} \{(y, Y) | y \in Y, Y \in T(A)\}$. Then, $(a, X) \in R \cdot (Q+P)$ but $(a, X) \notin R \cdot Q + R \cdot P$. Therefore, $R \cdot (Q+P) \not\subseteq R \cdot Q + R \cdot P$.

3. ($\Longleftarrow$) Assume that T is finite. Let D be a directed subset of T-$\mathsf{UMR}(A)$. For each $R \in T$-$\mathsf{UMR}(A)$, $\bigvee\{R \cdot Q \,|\, Q \in D\} \subseteq R \cdot \bigvee D$ holds trivially. We show $R \cdot \bigvee D \subseteq \bigvee\{R \cdot Q \,|\, Q \in D\}$. Let (a, X) be an element of $R \cdot \bigvee D$. We can take $Y \in T(A)$ such that $(a, Y) \in R$ and $\forall y \in Y. \exists Q_y \in D. (y, X) \in Q_y$. Since Y is finite and D is directed, there exists $P \in D$ such that $\forall y \in Y. Q_y \subseteq P$. Therefore, $(a, X) \in R \cdot P \subseteq \bigvee\{R \cdot Q \,|\, Q \in D\}$.

   ($\Longrightarrow$) Conversely, assume that T is not finite. There exist a set A and an infinite set X satisfying $X \in T(A)$. Let $R_x = \{(x, Y) | X \subseteq Y, Y \in T(A)\}$ for each $x \in X$. Let $D = \{\bigcup_{x \in I} R_x \,|\, I \subseteq X, I \text{ is finite}\}$. Then, D is directed. Take $a \in X$. We have $(a, X) \in R_a \cdot \bigvee D$ but $(a, X) \notin \bigvee\{R_a \cdot Q | Q \in D\}$. Therefore, $R_a \cdot \bigvee D \not\subseteq \bigvee\{R_a \cdot Q | Q \in D\}$.

□

This theorem can be represented by Fig. 3.5. The functor G from UMR to **CILS** is given by Proposition 3.4. The other seven functors are given by Theorem 3.3. Every square in Fig. 3.5 is a pullback square.

As a corollary of Theorem 3.2 and Theorem 3.3, we get the mapping from the cube of complete IL-semirings consisting of up-closed typed multirelations to the cube of lazy Kleene algebras. The case 1 and the case 2 of this corollary give necessary and sufficient conditions, since the case 1 and the case 2 of Theorem 3.2 do so.

Corollary 3.1. *Let T be a closed type. T-$\mathsf{UMR}(A)$ forms a lazy Kleene algebra for each A. Moreover, the following hold.*

1. *T-$\mathsf{UMR}(A)$ satisfies the 0-axiom for each A if and only if T is total,*

2. *T-$\mathsf{UMR}(A)$ satisfies the $+$-axiom for each A if and only if T is affine, and*

3. *T-$\mathsf{UMR}(A)$ satisfies the D-axiom for each A if T is finite.*

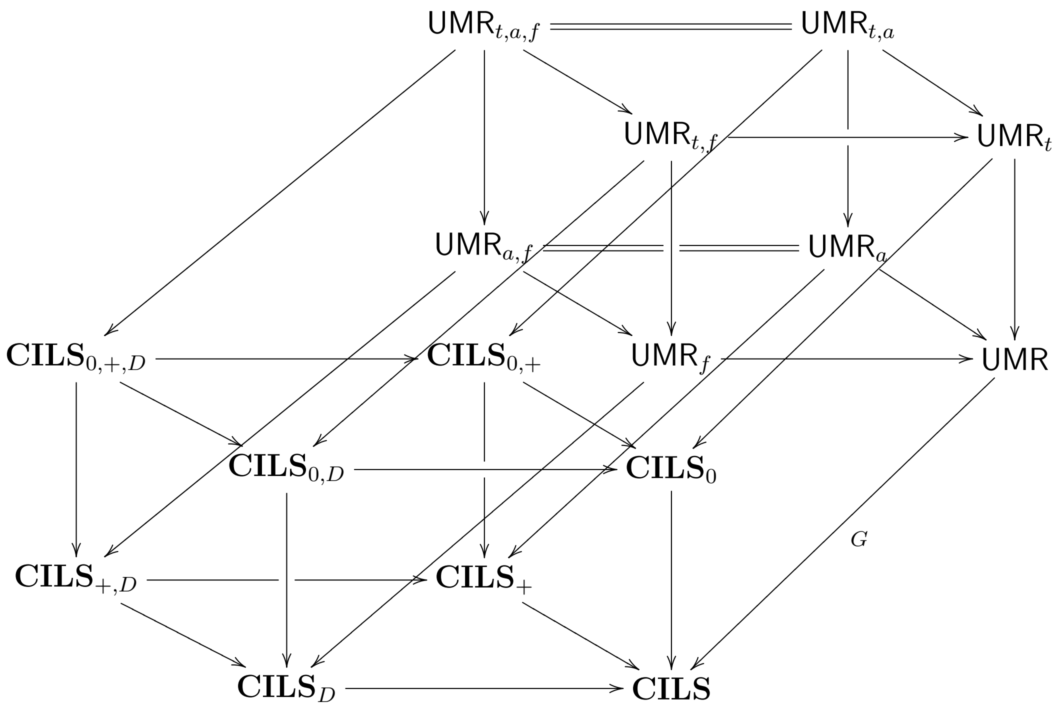

Figure 3.5: The maps from the cube of UMR to the cube of **CILS**

This corollary includes many results about multirelational models of lazy Kleene algebras.

Example 3.5. *$T(A) = \wp(A)$ is a closed type. In this case, T-$\mathsf{UMR}(A)$ is a lazy Kleene algebra. Therefore, the set of up-closed multirelations over A forms a lazy Kleene algebra.*

Example 3.6. *$T(A) = \{X \subseteq A \mid X$ is finite$\}$ is a closed type. Since this type T is finite, T-$\mathsf{UMR}(A)$ is a monodic tree Kleene algebra.*

Example 3.7. *$T(A) = \{X \subseteq A \mid X$ is finite and non-empty$\}$ is a closed type. Since this type T is total and finite, T-$\mathsf{UMR}(A)$ is a probabilistic Kleene algebra.*

Example 3.8. *$T(A) = \{\{a\} \mid a \in A\}$ is a closed type. Since this type T is total, affine, and finite, T-$\mathsf{UMR}(A)$ is a Kleene algebra, Therefore, the set of ordinary binary relations over A forms a Kleene algebra.*

Example 3.9. *We compare the notion of finitary up-closed multirelations with the notion of up-closed multirelations of type $T(A) = \{X \subseteq A \mid X$ is finite$\}$. A finitary up-closed multirelation is not always an up-closed multirelation of this type T over A, since* *the former may include* (a, X) *for an infinite* X*, but the latter must not. Conversely, an up-closed multirelation of type* T *over* A *is not always a finitary up-closed multirelation. However, the set of finitary up-closed multirelations forms a complete IL-semiring and it is isomorphic to* $T\text{-}\mathsf{UMR}(A)$ *as a complete IL-semiring [TNF08b]. The isomorphism maps a finitary up-closed multirelation* R *to* $\{(a, X) \in R \mid X \text{ is finite}\}$ *and an up-closed multirelation* R *of type* T *over* A *to* $\{(a, X) \in A \times \wp(A) \mid \exists Y \subseteq X.(a, Y) \in R\}$*. Therefore, the set of finitary up-closed multirelations also forms a lazy Kleene algebra satisfying the* D*-axiom.*

Example 3.10. $T(A) = \{X \subseteq A \mid X \text{ is non-empty}\}$ *is a closed type. Since this type* T *is total,* $T\text{-}\mathsf{UMR}(A)$ *is a lazy Kleene algebra satisfying the* 0*-axiom.*

Example 3.11. $T(A) = \{\emptyset\} \cup \{\{a\} \mid a \in A\}$ *is a closed type. Since this type* T *is affine,* $T\text{-}\mathsf{UMR}(A)$ *is a lazy Kleene algebra satisfying the* $+$*-axiom.*

3.7 Summary

We studied the relationship between relaxations of Kleene algebras and classes of multirelations.

We extended the notion of multirelations by introducing types of multirelations. For each of eight classes of relaxation of Kleene algebra, we gave a sufficient condition on type T such that the set of up-closed multirelations of type T belongs to the class. In particular, the affineness condition and the totality condition of a type are not only sufficient, but also necessary.

This chapter includes the result that the set of ordinary binary relations forms a Kleene algebra, the set of up-closed multirelations forms a lazy Kleene algebra, the set of up-closed finite multirelations forms a monodic tree Kleene algebra, and the set of total up-closed finite multirelations forms a probabilistic Kleene algebra. The cube consisting of eight conditions of type of multirelation is actually a triangular prism. It is strange but interesting.

Chapter 4

Another Multirelational Model of Complete IL-semiring

In this chapter we study an another multirelational model of complete IL-semirings. We introduce bottomed multirelations given by Weber and McIver [MW05, Web08] as abstract probabilistic programs. And then we show that the set of bottomed multirelations forms complete IL-semiring.

4.1 Overview

Previously, Weber et al [MW05, Web08] studied the relationship between the model of probabilistic systems and its abstract model which consists of (not up-closed) multirelations. In [MW05, Web08] they introduce a multirelational model of probabilistic Kleene algebra under the name of abstract probabilistic programs. And they show that this model and probabilistic Kleene algebra are useful for the counterexamples search for equalities in the model of probabilistic systems. Specifically they proved that satisfiability of inequalities on the set of probabilistic programs is preserved on the set of abstract probabilistic programs in terms of probabilistic Kleene algebra. In this chapter, we introduce the abstract model given by Weber [Web08] in the name of bottomed multirelation and study the basic properties of them. Then we prove that it forms complete IL-semiring preserving all right directed join and the right zero.

This chapter is organized as follows. In section 4.2 we introduce the definition of bottomed multirelation and study the operators on the set of bottomed multirelations. Section 4.3 show a multirelational model of complete IL-semiring consisting of bottomed multirelations.

4.2 Bottomed Multirelation

We treat multirelations in the form of subsets of $A^{\perp} \times \wp_{+}(A^{\perp})$ instead of $A \times \wp(A)$, where a special state $\perp$ is assumed to be not in A, $\wp_{+}(A)$ is the set of all non-empty subsets of A and $A^{\perp}$ is $A \cup \{\perp\}$.

First we introduce unusual order on $\wp_{+}(A^{\perp})$.

Definition 4.1. *For a set A, let X, Y be two non-empty subsets of $A^{\perp}$. Then the order $\sqsubseteq_{\mathcal{A}}$ on $\wp_{+}(A^{\perp})$ is defined by*

$$X \sqsubseteq_{\mathcal{A}} Y \iff X = Y \vee [\perp \in X \wedge X \subseteq Y \cup \{\perp\}] \ .$$

We provide examples of ordered sets with respect to this order for the better understanding.

Example 4.1. *Let A_1 be a singleton set $\{x\}$, and A_2 a set $\{x, y\}$. Figure 4.1 contains the diagrams for two ordered sets, $\wp_{+}(A_1^{\perp})$ and $\wp_{+}(A_2^{\perp})$.*

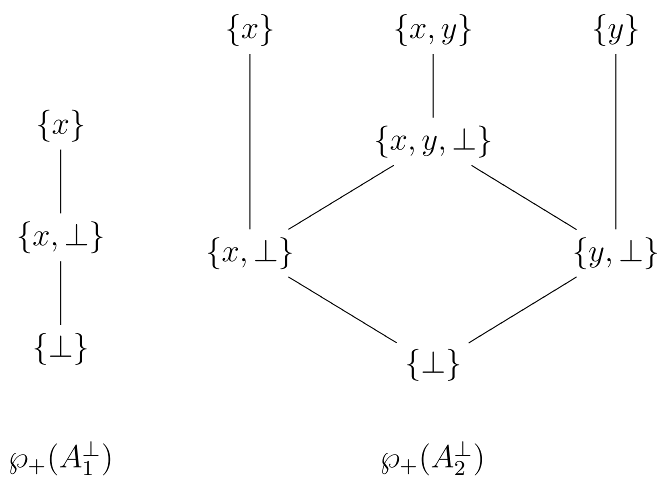

Figure 4.1: The diagrams for two ordered sets

Definition 4.2. *A subset R of $A^{\perp} \times \wp_{+}(A^{\perp})$ satisfying*

$$(\perp, X) \in R \iff X = \{\perp\}$$

is called a bottomed multirelation over a set A.

Next we introduce some restrictions for bottomed multirelations.

Definition 4.3. *A bottomed multirelation $R \subseteq A^{\perp} \times \wp_{+}(A^{\perp})$ is called*

- $\perp$-included *if for each $a \in A^{\perp}$, $(a, \{\perp\}) \in R$.*
- down-closed *if for each $a \in A^{\perp}$, $X, Y \in \wp_{+}(A^{\perp})$,*

$$(a, X) \in R \wedge Y \sqsubseteq_{\mathcal{A}} X \implies (a, Y) \in R \ .$$

- union-closed *if for each $a \in A^{\perp}$, $X, Y \in \wp_{+}(A^{\perp})$,*

$$(a, X), (a, Y) \in R \implies (a, X \cup Y) \in R \ ,$$

- finite *if for each $a \in A^{\perp}$, $X \in \wp_{+}(A^{\perp})$,*

$$(a, X) \in R \implies X \textit{ is finite} \ .$$

We denote $\mathsf{bMR}(A)$ for the set of all $\perp$-included, down- and union-closed, finite and bottomed multirelations over a set A.

We prove that $\mathsf{bMR}(A)$ forms complete IL-semiring preserving the right 0 and all right directed join.

First, we think the least element and the arbitrary join on $\mathsf{bMR}(A)$. The least element 0 on $\mathsf{bMR}(A)$ is given by

$$0 := \{(a, \{\perp\}) \mid a \in A_{\perp}\} \ .$$

We have the following lemma.

Lemma 4.1. *For each subset χ of $\mathsf{bMR}(A)$, the union $\bigcup \chi$ is $\perp$-included, down-closed and finite.*

Proof. Let χ be a subset of $\mathsf{bMR}(A)$. $\bigcup \chi$ is $\perp$-included obviously. If $(a, X) \in \bigcup \chi$ then there exists $Q \in \chi$ such that $(a, X) \in Q$. Then X is finite because $Q$is finite. In addition if $Y \sqsubseteq_{\mathcal{A}} X$ then we have $(a, Y) \in \bigcup \chi$ since Q is down-closed. Therefore $\bigcup \chi$ is finite and down-closed. $\square$

However, $P \cup Q$ need not be union-closed for each $P, Q \in \mathsf{bMR}(A)$.

Example 4.2. *Let A be a set $\{x, y\}$ and $P, Q \in \mathsf{bMR}(A)$ as follows:*

$$\begin{aligned} P &= 0 \cup \{(x, \{y, \bot\}), (y, \{x, \bot\})\} \ , \\ Q &= 0 \cup \{(x, \{x, \bot\}), (y, \{y, \bot\})\} \ . \end{aligned}$$

Then $(x,\ \{x, y, \bot\}) \notin P \cup Q$ though $(x, \{y, \bot\}), (x, \{x, \bot\}) \in P \cup Q$. Therefore $P \cup Q$ is not union-closed.

We introduce the union-closure to construct the binary join on $\mathsf{bMR}(A)$.

Definition 4.4 (Union-closure)**.** *For a bottomed multirelation $R \in \mathsf{bMR}(A)$, the* union closure *$H_u(R)$ of R is defined by*

$$H_u(R) = \left\{(a,\ \bigcup_{i \in I} X_i) \mid a \in A^{\bot} \wedge I \in \wp_f(A^{\bot}) \wedge \forall i \in I.(a, X_i) \in R\right\}.$$

where $\wp_f(A^{\bot})$ is the set of all finite subsets of $A^{\bot}$.

$H_u(R)$ is the smallest union-closed set containing $R \in \mathsf{bMR}(A)$.

Remark 4.1. *H_u is a closure operator on $\mathsf{bMR}(A)$.*

We obtain the following lemma immediately.

Lemma 4.2. *For a bottomed multirelation $R \in \mathsf{bMR}(A)$, $H_u(R)$ is finite (resp. $\bot$-included).*

Lemma 4.3. *For a bottomed multirelation $R \in \mathsf{bMR}(A)$, $H_u(R)$ is down-closed.*

Proof. Let $R \in \mathsf{bMR}(A)$ be down-closed. And assume that $(a, Y) \in H_u(R)$ and $Z \sqsubseteq_{\mathcal{A}} Y$. Then there exists $I \in \wp_f(A^{\bot})$ and $\forall i \in I.(a, X_i) \in R$, and $Y = \bigcup_{i \in I} X_i$. In the case of $Z = Y$, obviously $(a, Z) \in H_u(R)$. Suppose that $Z \neq Y$. Then $\bot \in Z$ and $Z \subseteq \bigcup_{i \in I} X_i \cup \{\bot\}$, that is, for each $x \in Z \backslash \{\bot\}$ there exists $i_x \in I$ such that $x \in X_{i_x}$. We have $(a, \{x, \bot\}) \in R$ for each $x \in Z \backslash \{\bot\}$ since $\{x, \bot\} \sqsubseteq_{\mathcal{A}} X_{i_x}$ and R is down-closed. Therefore $(a, Z) = (a,\ \bigcup_{x \in Z \backslash \{\bot\}} \{x, \bot\}) \in H_u(R)$. □

For each subset χ of $\mathsf{bMR}(A)$, the join $\bigvee \chi$ is given by as follows.

$$\bigvee \chi := H_u(\bigcup \chi)$$

Especially, we denotes $P + Q$ for the binary join of $P, Q \in \mathsf{bMR}(A)$. The operator $+$ is monotone, i.e.,

$$P \subseteq P' \ \wedge \ Q \subseteq Q' \implies P + Q \subseteq P' + Q'$$

for $P, P', Q, Q' \in \mathsf{bMR}(A)$. We immediately obtain that $0 \subseteq P$, $P = 0 + P$, $P + Q = Q + P$, and $P + P = P$ for each $P, Q \in \mathsf{bMR}(A)$.

Lemma 4.4. *The operator $+$ is associative, that is*

$$(P + Q) + R = P + (Q + R)$$

for $P, Q, R \in \mathsf{bMR}(A)$.

Proof. Suppose $P, Q, R \in \mathsf{bMR}(A)$. $(P + Q) + R = P + (Q + R)$ is sufficient to show that $(P + Q) + R \subseteq P + (Q + R)$ since $+$ is commutative. $P + Q \subseteq P + (Q + R)$ and $R \subseteq P + (Q + R)$ hold since $+$ is monotone. Therefore $P + (Q + R)$ is upper bound of $P + Q$ and R. We have $(P + Q) + R = H_u((P + Q) \cup R) \subseteq P + (Q + R)$ by the definition of H_u. □

Therefore the following property holds.

Proposition 4.1. $(\mathsf{bMR}(A), +, 0)$ *is a idempotent commutative monoid.*

For $P, Q \in \mathsf{bMR}(A)$, the composition $P; Q$ is defined as follows.

$$\begin{aligned} &(a, X) \in P; Q \\ &\iff \exists Y \in \wp(A^{\perp}).\ [(a, Y) \in P \wedge \forall y \in Y.\ \exists X_y \in \wp(A^{\perp}).(y, X_y) \in Q \wedge X = \bigcup_{y \in Y} X_y]. \end{aligned}$$

Lemma 4.5. $\mathsf{bMR}(A)$ *is closed under the composition* ;.

Proof. Suppose $P, Q \in \mathsf{bMR}(A)$. We show that $P; Q \in \mathsf{bMR}(A)$.

First we prove that $P; Q$ is $\perp$-included. We immediately have $(a, \{\perp\}) \in P; Q$ since $(a, \{\perp\}) \in P$ and $(\perp, \{\perp\}) \in Q$ for each $a \in A$.

Next, we prove that $P; Q$ is down-closed. Suppose $(a, X) \in P; Q$ and $Z \sqsubseteq_{\mathcal{A}} X$ then there exists $Y \in \wp(A^{\perp})$ such that $(a, Y) \in P$ and $(y, X_y) \in Q$ for each $y \in Y$ and $X = \bigcup_{y \in Y} X_y$. In the case of $Z = X$, obviously $(a, Z) \in P; Q$. Suppose that $Z \neq X$. Then $\perp \in Z$ and $Z \subseteq \bigcup_{y \in Y} X_y \cup \{\perp\}$, that is, for each $x \in Z \backslash \{\perp\}$ there exists $y_x \in Y$ such that $x \in X_{y_x}$. We have $(y_x, \{x, \perp\}) \in Q$ for each $x \in Z \backslash \{\perp\}$ since $\{x, \perp\} \sqsubseteq_{\mathcal{A}} X_{y_x}$ and Q is down-closed. Let $Y' := \{y_x \mid x \in Z \backslash \{\perp\}\} \cup \{\perp\}$. Then we have $(a, Y') \in P$

since $Y' \sqsubseteq_{\mathcal{A}} Y$ and P is down-closed. Let $X_{y_x} := \{x, \perp\}$ Then we have $(y_x, X_{y_x}) \in Q$ for each $y_x \in Y'$. Therefore

$$(a, \bigcup_{y_x \in Y} X_{y_x}) = (a, Z) \in P; Q \ .$$

Finally, we prove that $P; Q$ is union-closed. Assume that $(a, X), (a, X') \in P; Q$.

Then there exists $Y, Y' \in \wp(A^{\perp})$ such that $(a, Y), (a, Y') \in P$ and there exists $X_y \in \wp(A^{\perp})$ for each $y \in Y$ such that $(y, X_y) \in Q$ for each $y \in Y$ and

$$X = \bigcup_{y \in Y} X_y \ .$$

And also there exists $X'_y \in \wp(A^{\perp})$ for each $y \in Y'$ such that $(y, X'_y) \in Q$ for each $y \in Y'$ and

$$X' = \bigcup_{y \in Y'} X'_y \ .$$

We obtain that $(a,\ Y \cup Y') \in P$ and $(y,\ X_y \cup X'_y) \in Q$ for each $y \in Y \cup Y'$ since P and Q are union-closed — note that $X_y = \emptyset$ for $y \in Y' \backslash Y$ and $X'_y = \emptyset$ for $y \in Y \backslash Y'$. In addition, we have

$$(a, X \cup X') = (a,\ (\bigcup_{y \in Y} X_y) \cup (\bigcup_{y \in Y'} X'_y)) = (a,\ \bigcup_{y \in Y \cup Y'} (X_y \cup X'_y)) \in P; Q \ .$$

Therefore $P; Q$ is union-closed. $\square$

The composition operator is monotone, that is, preserves the inclusion.

Lemma 4.6. *The composition operator* ; *is associative, that is*

$$(P; Q); R = P; (Q; R)$$

for $P, Q, R \in \mathsf{bMR}(A)$.

Proof. First, we show that $(P; Q); R \subseteq P; (Q; R)$ holds. Let $(a, X) \in ((P; Q); R)$. Then there exists $Y \in \wp(A^{\perp})$ such that $(a, Y) \in P; Q$ and $(y, X_y) \in R$ for each $y \in Y$ and $X = \bigcup_{y \in Y} X_y$. And there exists $Z \in \wp(A^{\perp})$ such that $(a, Z) \in P$ and $(z, Y_z) \in Q$ for each $z \in Z$ and $Y = \bigcup_{z \in Z} Y_z$. Then we have $(a, Z) \in P$ and $(z, \bigcup_{y \in Y_z} X_y) \in Q; R$. Therefore

$$X = \bigcup \{X_y \mid y \in \bigcup\nolimits_{z \in Z} Y_z\} = \bigcup_{z \in Z} \bigcup_{y \in Y_z} X_y \in (P; (Q; R))(a) \ .$$

Conversely, if $(a, X) \in P;(Q;R)$, then there exists $Z \in \wp(A^{\perp})$ such that $(a, Z) \in P$ and $(z, X_z) \in Q;R$ for each $z \in Z$ and $X = \bigcup_{z\in Z} X_z$. And there exists $Y_z \in \wp(A^{\perp})$ such that $(z, Y_z) \in Q$ and $(y, X_z^y) \in R$ for each $y \in Y_z$ and $X_z = \bigcup_{y\in Y_z} X_z^y$. Note that

$$X = \bigcup_{z\in Z} \bigcup_{y\in Y_z} X_z^y = \bigcup \left\{ \bigcup_{z\in Z} X_z^y \mid y \in \bigcup_{z\in Z} Y_z \right\} .$$

We have $(y, \bigcup_{z\in Z} X_z^y) \in R$, since Z is finite and R is union-closed. Then we obtain $(a, \bigcup_{z\in Z} Y_z) \in P;Q$. And then we have $(a, \bigcup \{\bigcup_{z\in Z} X_z^y \mid y \in \bigcup_{z\in Z} Y_z\}) \in (P;Q);R$. □

We discuss the zero element and the composition.

Proposition 4.2. *Let $R \in \mathsf{bMR}(A)$. $0;R = 0$ and $R;0 = 0$.*

Proof. We already have $0 \subseteq 0;R$ and $0 \subseteq R;0$ because we already have proved that $0;R$, $R;0$ are $\perp$-included in the lemma 4.2. If $(a, X) \in 0;R$ then there exists $Y \in \wp(A^{\perp})$ such that $(a, Y) \in 0$ and $(y, X_y) \in R$ for each $y \in Y$ and $X = \bigcup_{y\in Y} X_y$. Then $X = \{\perp\}$ since $Y = \{\perp\}$.

If $(a, X) \in 0;R$, then there exists $Y \in \wp(A^{\perp})$ such that $(a, Y) \in 0$ and $(y, X_y) \in R$ for each $y \in Y$ and $X = \bigcup_{y\in Y} X_y$. Then $X = \{\perp\}$ since $Y = \{\perp\}$.

Finally we show that $R;0 \subseteq 0$. If $(a, X) \in R;0$, then there exists $Y \in \wp(A^{\perp})$ such that $(a, Y) \in R$ and $(y, X_y) \in 0$ for each $y \in Y$ and $X = \bigcup_{y\in Y} X_y$. Then X is $\{\perp\}$. □

The identity $1 \in \mathsf{bMR}(A)$ is defined by

$$1 := \{(a, X) \mid a \in A, X \sqsubseteq_{\mathcal{A}} \{a\}\}$$

Lemma 4.7. *The identity satisfies the unit law, that is*

$$1;R = R \textit{ and } R;1 = R$$

for each $R \in \mathsf{bMR}(A)$.

Proof. First, we prove that $1;R = R$. If $(a, X) \in 1;R$ then there exists $Y \in \wp(A^{\perp})$ such that $(a, Y) \in 1$ and $(y, X_y) \in R$ for each $y \in Y$ and $X = \bigcup_{y\in Y} X_y$. It is satisfied that Y is equal to $\{\perp\}$, $\{a, \perp\}$, or $\{a\}$. In the case of $Y = \{\perp\}$, we have $X = \{\perp\}$. That's why obviously $(a, \{\perp\}) \in R$. Assume that $Y = \{a\}$, we have $X = \bigcup_{y\in Y} X_y = X_a$. And then $(a, X) = (a, X_a) \in R$. In the case of $Y = \{a, \perp\}$, we have (a, X_a), $(\perp, \{\perp\}) \in R$, and $X = X_a \cup \{\perp\}$. Then $X \sqsubseteq_{\mathcal{A}} X_a$, so we have $(a, X) \in R$ since R is down-closed.

Conversely, suppose $(a, X) \in R$. Since $(a, \{a\}) \in 1$ we obtain $(a, X) \in 1; R$ immediately.

Next we show that $R; 1 = R$. Suppose $(a, h) \in R; 1$. $Y \in \wp(A^\perp)$ such that $(a, Y) \in R$ and $(y, X_y) \in 1$ for each $y \in Y$ and $X = \bigcup_{y \in Y} X_y$. By the definition of the identity, we have $X_y \sqsubseteq_{\mathcal{A}} \{y\}$ for each $y \in Y$. Then $X = \bigcup_{y \in Y} X_y \sqsubseteq_{\mathcal{A}} Y$. Therefore $(a, X) \in R$ since R is down-closed.

Conversely, assume $(a, X) \in R$. Since $(x, \{x\}) \in 1$ for each $x \in X$, we have $(a, X) = (a, \bigcup_{x \in X} \{x\}) \in R; 1$. □

Lemma 4.6 and 4.7 show the following property.

Proposition 4.3. *A tuple* $(\mathsf{bMR}(A),\ ;,\ 1)$ *is a monoid.*

Next, we consider the left distributivity.

Proposition 4.4. *Let* χ *be a subset of* $\mathsf{bMR}(A)$*. Then*

$$(\bigvee \chi); R = \bigvee_{Q \in \chi} Q; R$$

for each $R \in \mathsf{bMR}(A)$*.*

Proof. Obviously, it is satisfied $\bigvee_{Q \in \chi} Q; R \subseteq (\bigvee \chi); R$ by the monotonicity of the composition ;. We show that $(\bigvee \chi); R \subseteq \bigvee_{Q \in \chi} Q; R$. If $(a, X) \in (\bigvee \chi); R$ then there exists $Y \in \wp(A^\perp)$ such that $(a, Y) \in \bigvee \chi$ and there exists $X_y \subseteq A^\perp$ such that $(y, X_y) \in R$ for each $y \in Y$ and $X = \bigcup_{y \in Y} X_y$. Also, there exists $I \in \wp_f(A^\perp)$ and $Y_i \in \wp(A^\perp)$ for each $i \in I$ such that $(a, Y_i) \in \bigcup \chi$ and $Y = \bigcup_{i \in I} Y_i$. Then there exists $Q_i \in \chi$ satisfying $(a, Y_i) \in Q_i$ for each $i \in I$. We have $(a, \bigcup_{y \in Y_i} X_y) \in Q_i; R$ since $(a, Y_i) \in Q_i$ and $(y, X_y) \in R$ for each $y \in Y_i$. Therefore we have

$$X = \bigcup_{y \in Y} X_y = \bigcup \left\{ X_y \mid y \in \bigcup_{i \in I} Y_i \right\} = \bigcup_{i \in I} \bigcup_{y \in Y_i} X_y \in \left(\bigvee_{Q \in \chi} Q; R \right)(a) \ .$$

□

Then we have $(P + Q); R = P; R + Q; R$ for $P, Q, R \in \mathsf{bMR}(A)$ obviously.

4.3 Another Multirelational Model of Complete IL-semiring

We have already shown that a tuple $(\mathsf{bMR}(A), +, ;, 0, 1, \bigvee)$ is a complete IL-semiring preserving the right zero by the proposition 4.1, 4.2, 4.3 and 4.4. Additionally, this complete IL-semiring also preserves all right directed joins.

Lemma 4.8. *If $\chi \subseteq \mathsf{bMR}(A)$ is directed, $\bigcup_{Q\in\chi} Q$ is union-closed.*

Proof. Assume that $\chi \subseteq (A)$ is directed. We show that $(a, X), (a, X') \in \bigcup_{Q\in\chi} Q$ implies $(a, X \cup X') \in \bigcup_{Q\in\chi} Q$. If $(a, X), (a, X') \in \bigcup_{Q\in\chi} Q$ then there exists $P, P' \in \chi$ such that $(a, X) \in P$, $(a, X') \in P'$. Since χ is directed, there exists $R \in \chi$ such that $P \subseteq R$, $P' \subseteq R$. Therefore $(a, X \cup X') \in R \subseteq \bigcup_{Q\in\chi} Q$ since $(a, X), (a, X') \in R$ and R is union-closed. □

By Proposition 4.1, 4.8, if $\chi \subseteq \mathsf{bMR}(A)$ is directed, $\bigcup_{Q\in\chi} Q$ is $\perp$-included finite down- and union-closed. The fact indicates that the directed join $\bigvee \chi$ of $\chi \subseteq \mathsf{bMR}(A)$ is given by

$$\bigvee \chi = \bigcup_{Q\in\chi} Q \ .$$

Proposition 4.5. *Let χ be a directed subset of $\mathsf{bMR}(A)$. Then*

$$R; \left(\bigvee \chi\right) = \bigvee_{Q\in\chi} R; Q$$

for each $R \in \mathsf{bMR}(A)$.

Proof. Obviously, it is satisfied $\bigvee_{Q\in\chi} R; Q \subseteq R; (\bigvee \chi)$ by the monotonicity of the composition ;. We show that $R; (\bigvee \chi) \subseteq \bigvee_{Q\in\chi} R; Q$.

Assume that $(a, X) \in R; (\bigvee \chi)$. Then there exists $Y \in \wp(A^{\perp})$ such that $(a, Y) \in R$. And also there exists $X_y \in \wp(A^{\perp})$ for each $y \in Y$ such that $(y, X_y) \in \bigvee \chi$ and $X = \bigcup_{y\in Y} X_y$. Since χ is directed, for each $y \in Y$, $(y, X_y) \in \bigvee \chi = \bigcup_{Q\in\chi} Q$, that is, there exists $Q_y \in \chi$ satisfying $(y, X_y) \in Q_y$ for $y \in Y$. Since $\{Q_y \mid y \in Y\}$ is finite and χ is directed, there exists $P \in \chi$ satisfying $Q_y \subseteq P$ for $y \in Y$. Then we have

$$(a, X) = (a, \bigcup_{y\in Y} X_y) \in R; P \subseteq \bigcup_{Q\in\chi} R; Q \ .$$

Therefore $(a, X) \in \bigvee_{Q\in\chi} R; Q$. □

Finally we obtain the following.

Theorem 4.1. *A tuple $(\mathsf{bMR}(A), +, ;, 0, 1, \bigvee)$ is a complete IL-semiring preserving the right zero and all right directed join.*

However, $P; (Q + R) = P; Q + P; R$ need not hold for $P, Q, R \in \mathsf{bMR}(A)$.

Example 4.3. *Consider two bottomed multirelations,*

$$\begin{aligned} R' &= 0 \cup \{(a, W) \mid a \in A, W \sqsubseteq_{\mathcal{A}} \{x, y\}\} \\ Q' &= 0 \cup \{(x, W) \mid W \sqsubseteq_{\mathcal{A}} \{y\}\} \cup \{(y, W) \mid W \sqsubseteq_{\mathcal{A}} \{x\}\} \end{aligned}$$

on $\mathsf{bMR}(\{x, y\})$. *Since* $(x, \{x, y\}) \in R'$ *and* $(x, \{y\}), (y, \{y\}) \in Q' + 1$,

$$(x, \{y\}) \in R'; (Q' + 1).$$

But we have

$$(x, X) \in R'; Q' + R'; 1 \implies X \sqsubseteq_{\mathcal{A}} \{x, y\} \ .$$

Therefore $(x, \{y\}) \notin R'; Q' + R'; 1$.

4.4 Summary

This chapter has discussed bottomed multirelations which are abstract probabilistic programs introduced by Weber and McIver [MW05, Web08]. And we have studied the basic properties of bottomed multirelations, especially the operators of them, and then we have proved that the set of $\perp$-included finite down- and union-closed bottomed multirelations forms a complete IL-semiring preserving the right 0 and all directed join. And we also have shown that a counter example of the right distributivity.

Chapter 5

Probabilistic Models of Complete IL-semiring

This chapter studies basic properties of probabilistic multirelations which are generalized the semantic domain of probabilistic systems and then shows that the set of probabilistic multirelations forms a complete IL-semiring.

5.1 Overview

In this chapter we generalize a semantics of probabilistic distributed systems. McIver et al [MCC06], [MW05] introduced a notion of probabilistic programs in the form of subsets of $(A \cup \{\top\}) \times \mathcal{D}_1(A \cup \{\top\})$ where $\top$ is a special state assumed to be not in A and $\mathcal{D}_1(A)$ is the set of all probabilistic distributions over a set A. And they proved that the set of all probabilistic programs forms a probabilistic Kleene algebra, with three restrictions called up-closed, convex-closed and Cauchy-closed. Actually probabilistic programs in the form of subsets of $(A \cup \{\top\}) \times \mathcal{D}_1(A \cup \{\top\})$ can be translated to subsets of $A \times \mathcal{D}(A)$ where $\mathcal{D}(A)$ is the set of all probabilistic sub-distributions. We use this simple form and introduce a notion of probabilistic multirelations and study basic properties of them. And then we show that the set of all finitary **0**-included down- and convex-closed probabilistic multirelations forms a complete IL-semiring preserving all right directed join and the right 0 — of course, it forms a probabilistic Kleene algebra. Additionally we also show that the set of left-total $\mathcal{D}_1$ convex-closed probabilistic multirelations forms a complete IL-semiring preserving the right 0.

This chapter is organized as follows. Section 5.2 provides basic notions which will appear in this chapter. In section 5.3 we introduce the definition and basic properties of probabilistic multirelation. Section 5.4 provides a probabilistic model of complete IL-semirings, using finitary $\mathbf{0}$-included down- and convex-closed probabilistic multirelations. Finally we provide probabilistic model of complete IL-semirings, using left-total and $\mathcal{D}_1$ convex-closed probabilistic multirelations in section 5.5.

5.2 Preliminaries

A *probabilistic sub-distribution* over a set A is a mapping d from a set A to the interval $[0,1]$ such that $\sum_{a\in A} d(a) \leq 1$. We denote $\mathcal{D}(A)$ for the set of all probabilistic sub-distributions over A. Also a probabilistic sub-distribution d over a set A is simply called probabilistic distribution if d satisfies $\sum_{a\in A} d(a) = 1$. We denote $\mathcal{D}_1(A)$ for the set of all probabilistic distributions over A.

For $d \in \mathcal{D}(A)$, the *support* of d is defined by

$$\mathsf{supp}(d) := \{s \in A \mid d(s) > 0\}$$

If $\mathsf{supp}(d)$ is finite, we call that d is finitary. And $\mathcal{D}_f(A)$ denotes the set of all finitary probabilistic distributions.

The order $\sqsubseteq_{\mathcal{D}}$ on $\mathcal{D}(A)$ is defined by $d \sqsubseteq_{\mathcal{D}} d' \iff \forall a \in A.\ d(a) \leq d'(a)$ for each $d, d' \in \mathcal{D}(A)$.

We write δ_x and $\mathbf{0}$ for the point distribution at $x \in A$ and the zero distribution. The *point distribution* δ_x *at* $x \in A$ is defined by

$$\delta_x(a) := \begin{cases} 1 & (a = x) \\ 0 & (a \neq x) \end{cases},$$

and the zero distribution $\mathbf{0}$ is defined by $\forall a \in A.\ \mathbf{0}(a) = 0$. For $p \in [0,1]$ and distribution d, we write $p \cdot d$ for the p-weighted distribution of d, defined by $(p \cdot d)(a) = p \cdot d(a)$. Also for $p \in [0,1]$ and distributions $d, d' \in \mathcal{D}(A)$, we write $d\ {}_p\!\oplus d'$ for the

p-weighted sum of d and d', defined by

$$(d\ {}_p\!\oplus d')(a) = p \cdot d(a) + (1-p) \cdot d'(a) \ .$$

5.3 Probabilistic Multirelation

The ordinary binary multirelation over a set A is defined as a subset of $A \times \wp(A)$, but the probabilistic multirelation is defined by $\mathcal{D}(A)$ instead of $\wp(A)$.

Definition 5.1. *A probabilistic multirelation over a set A is a subset of $A \times \mathcal{D}(A)$.*

For each probabilistic multirelation R over A and $a \in A$, we denote $R(a)$ for $\{d \in \mathcal{D}(A) \mid (a, d) \in R\}$.

Next we introduce a fundamental restriction for probabilistic multirelations.

Definition 5.2 (Convex closed)**.** *A probabilistic multirelation R over a set A is called* convex closed *if for each $a \in A$, $d, d' \in \mathcal{D}(A)$ and $p \in [0, 1]$,*

$$(a, d), (a, d') \in R \implies (a, d\ {}_p\!\oplus d') \in R \ .$$

$\mathsf{pMR}(A)$ denotes a set of all convex-closed probabilistic multirelations. The partial order on $\mathsf{pMR}(A)$ is the inclusion $\subseteq$ on sets.

Next, we introduce three restrictions, *finitary,* 0*-included and down-closed* for probabilistic multirelations, and then we show that the probabilistic model forms a complete IL-semiring. The model which appear here is the laxer one of McIver-Morgan's model for probabilistic systems.

Definition 5.3. *A probabilistic multirelation $R \in \mathsf{pMR}(A)$ is called*

- finitary *if for each $a \in A$, $R(a) \subseteq \mathcal{D}_f(A)$.*

- $\mathbf{0}$-included *if for each $a \in A$, $(a, \mathbf{0}) \in R$.*

- down-closed *if for each $a \in A$, $d, d' \in \mathcal{D}(A)$,*

$$(a, d) \in R \land d' \sqsubseteq_{\mathcal{D}} d \implies (a, d') \in R \ .$$

We denote $\mathsf{pMR}_{0,d,f}(A)$ for the set of all finitary 0-included down- and convex-closed probabilistic multirelations over a set A.

We prove that $\mathsf{pMR}_{0,d,f}(A)$ forms complete IL-semiring preserving the right 0 and all right directed join. First, we think the arbitrary join and the least element on $\mathsf{pMR}_{0,d,f}(A)$. We have the following lemma.

Lemma 5.1. *For each subset χ of $\mathsf{pMR}_{0,d,f}(A)$, the union $\bigcup\chi$ is finitary, $\mathbf{0}$-included and down-closed.*

Proof. Let χ be a subset of $\mathsf{pMR}_{0,d,f}(A)$. $\bigcup\chi$ is finitary and $\mathbf{0}$-included obviously. If $(a,d) \in \bigcup\chi$ and $d' \sqsubseteq_{\mathcal{D}} d$, then there exists $Q \in \chi$ such that $(a,d) \in Q$. We have $(a,d') \in Q$ since Q is down-closed. Therefore $(a,d') \in Q \subseteq \bigcup\chi$. □

However, $P \cup Q$ need not be convex-closed for each $P, Q \in \mathsf{pMR}_{0,d,f}(A)$.

Example 5.1. *Let A be a set $\{x,y\}$ and $P, Q \in \mathsf{pMR}_{0,d,f}(A)$ as follows:*

$$\begin{aligned} P &= \{(a,d) \in A \times \mathcal{D}_f(A) \mid d \sqsubseteq_{\mathcal{D}} \delta_x\} \ , \\ Q &= \{(a,d) \in A \times \mathcal{D}_f(A) \mid d \sqsubseteq_{\mathcal{D}} \delta_y\} \ . \end{aligned}$$

P and Q are finitary, 0-included, down-, and convex-closed. Then $(x,\ \delta_x \ {}_{\frac{1}{2}}\!\oplus \delta_y) \notin P \cup Q$ though $(x,\delta_x), (x,\delta_y) \in P \cup Q$. Therefore $P \cup Q$ is not convex-closed.

We introduce the convex hull to construct the binary join on $\mathsf{pMR}_{0,d,f}(A)$.

Definition 5.4 (Convex hull)**.** *For a probabilistic multirelation $R \in \mathsf{pMR}(A)$, the* convex hull *$H_c(R)$ of R is defined by*

$$\left\{(a,\ \sum_{i\in I} d(i)\cdot F(i)) \in A \times \mathcal{D}(A) \mid I \in \wp_f(A),\ d \in \mathcal{D}_1(I),\ F : I \to R(a)\right\} .$$

where $\wp_f(A)$ is the set of all finite subsets of A.

$H_c(R)$ is the smallest convex-closed set containing $R \in \mathsf{pMR}(A)$.

Remark 5.1. *H_c is a closure operator on $\mathsf{pMR}(A)$.*

We obtain the followings immediately.

Lemma 5.2. *If a probabilistic multirelation $R \in \mathsf{pMR}(A)$ is finitary (resp. $\mathbf{0}$-included), then $H_c(R)$ is finitary (resp. $\mathbf{0}$-included).*

Lemma 5.3. *If a probabilistic multirelation $R \in \mathsf{pMR}(A)$ is down-closed, then $H_c(R)$ is down-closed.*

Proof. Let $R \in \mathsf{pMR}(A)$ be down-closed. And assume that $(a, h) \in H_c(R)$ and $h' \sqsubseteq_{\mathcal{D}} h$. Then there exists $I \in \wp(A)$, $d \in \mathcal{D}_1(I)$, and $F : I \to R(a)$ satisfying $h = \sum_{i \in I} d(i) \cdot F(i)$.

We take $F' : I \to R(a)$ as follows

$$F(i)(a) = \begin{cases} \dfrac{d'(a)}{d(a)} F(i)(a) & (d(a) > 0) \\ 0 & (d(a) = 0) \end{cases}$$

Therefore $d' = \sum_{i \in I} d(i) \cdot F'(i) \in H_c(R)$. □

For each subset χ of $\mathsf{pMR}_{0,d,f}(A)$, the join $\bigvee \chi$ is given by as follows.

$$\bigvee \chi := H_c\left(\bigcup \chi\right)$$

Especially, we denotes $P + Q$ for the binary join of $P, Q \in \mathsf{pMR}_{0,d,f}(A)$. The operator $+$ is monotone, i.e.,

$$P \subseteq P' \ \wedge \ Q \subseteq Q' \implies P + Q \subseteq P' + Q'$$

for $P, P', Q, Q' \in \mathsf{pMR}_{0,d,f}(A)$.

The least element 0 on $\mathsf{pMR}_{0,d,f}(A)$ is given by

$$0 := \{(a, \mathbf{0}) \mid a \in A\} \ .$$

We immediately obtain that $0 \subseteq P$, $P = 0 + P$, $P + Q = Q + P$, and $P + P = P$ for each $P, Q \in \mathsf{pMR}_{0,d,f}(A)$.

Lemma 5.4. *The operator + is associative, that is*

$$(P + Q) + R = P + (Q + R)$$

for $P, Q, R \in \mathsf{pMR}_{0,d,f}(A)$.

The proof of the above is similar to Lemma 4.4.

Therefore the following property holds.

Proposition 5.1. $(\mathsf{pMR}_{0,d,f}(A), +, 0)$ *is a idempotent commutative monoid.*

For $P, Q \in \mathsf{pMR}_{0,d,f}(A)$, let the composition $P \cdot Q$ be a set

$$\left\{(a, \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)) \mid (a, d) \in P,\ F : \mathsf{supp}(d) \to \mathcal{D}(A) \text{ s.t. } F \sqsubseteq Q\right\}$$

where $F \sqsubseteq Q \overset{def}{\iff} \forall u \in \mathsf{supp}(d).\ (u, F(u)) \in Q$.

Lemma 5.5. $\mathsf{pMR}_{0,d,f}(A)$ *is closed under the composition* $\cdot$.

Proof. Suppose $P, Q \in \mathsf{pMR}_{0,d,f}(A)$. We show that $P \cdot Q \in \mathsf{pMR}_{0,d,f}(A)$.

First we prove that $P \cdot Q$ is $\mathbf{0}$-included. We have $(a, \mathbf{0}) \in P$ for each $a \in A$. Let $F : A \to \mathcal{D}(A)$ be a mapping such that $F(u) = \mathbf{0}$ for each $u \in A$. Then $F \sqsubseteq Q$ holds. Therefore

$$(a, \mathbf{0}) = (a, \sum_{u \in A} \mathbf{0}(u) \cdot F(u)) \in P \cdot Q\ .$$

We prove that $P \cdot Q$ is finitary. If $(a, h) \in P \cdot Q$ then there exists $d \in P(a)$ and $F : A \to \mathcal{D}(A)$ satisfying $(u, F(u)) \in Q$ for each $u \in A$ and $h = \sum_{u \in A} d(u) \cdot F(u)$. Since

$$\mathsf{supp}(h) = \bigcup_{u \in \mathsf{supp}(d)} \mathsf{supp}(F(u))$$

and $\mathsf{supp}(d)$ and $\mathsf{supp}(F(u))$ are finites sets, then $\mathsf{supp}(h)$ is finite.

Next, we prove that $P \cdot Q$ is down-closed. Suppose $(a, h) \in P \cdot Q$ and $h' \sqsubseteq_{\mathcal{D}} h$ then there exists $d \in P(a)$ and $F : A \to \mathcal{D}(A)$ satisfying $(u, F(u)) \in Q$ for each $u \in A$ and $h = \sum_{u \in A} d(u) \cdot F(u)$. We take $F' : A \to \mathcal{D}(A)$ as follows

$$F'(u)(a) = \begin{cases} \dfrac{d'(a)}{d(a)} \cdot F(u)(a) & (a \in \mathsf{supp}(d)) \\ 0 & (a \notin \mathsf{supp}(d)) \end{cases}$$

Since $d' \sqsubseteq_{\mathcal{D}} d$, for each $u \in A$ $F'(u) \sqsubseteq_{\mathcal{D}} F(u)$ holds. So we obtain that $\forall u \in A.\ (u, F'(u)) \in Q$ by the fact that Q is down-closed. Therefore

$$(a, d') = (a, \sum_{u \in A} d''(u) \cdot F'(u)) \in P \cdot Q\ .$$

$P \cdot Q$ is down-closed.

Finally, we prove that $P \cdot Q$ is convex closed. Suppose that $h, h' \in (P; Q)(a)$. Then there exists $d, d' \in P(a)$, and $F, F' : \mathsf{supp}(d) \to \mathcal{D}(A)$ such that $d = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$,

$d' = \sum_{u \in \mathsf{supp}(d)} d'(u) \cdot F'(u)$. Let $p \in [0,1]$. Then for some $s \in A$,

$$\begin{aligned}(h\ {}_p\!\oplus h')(s) &= p \cdot \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)(s) + (1-p) \cdot \sum_{u \in \mathsf{supp}(d')} d'(u) \cdot F'(u)(s) \\ &= \sum_{u \in \mathsf{supp}(d\ {}_p\!\oplus d')} p \cdot d(u) \cdot F(u)(t) + (1-p) \cdot d'(u) \cdot F'(u)(s) \ .\end{aligned}$$

For $u \in A$, let $F'' : \mathsf{supp}(d\ {}_p\!\oplus d') \to \mathcal{D}(A)$ be a mapping such that

$$F''(u) = F(u)\ {}_{q(u)}\!\oplus F'(u)$$

where $q(u) = \dfrac{p \cdot f(u)}{p \cdot f(u) + (1-p) \cdot f'(u)}$. Since Q is convex-closed, we have $F'' \sqsubseteq Q$.

$$(h\ {}_p\!\oplus h')(s) = \sum_{u \in A} (d\ {}_p\!\oplus d')(u) \cdot F''(u)(s)$$

holds. And we have $d\ {}_p\!\oplus d' \in P(s)$ since P is convex-closed. Therefore $P \cdot Q$ is convex-closed. □

The composition operator is monotone, i.e.,

$$P \subseteq P' \ \wedge\ Q \subseteq Q' \implies P \cdot Q \ \subseteq\ P' \cdot Q'$$

for $P,\ P',\ Q,\ Q' \in \mathsf{pMR}_{0,d,f}(A)$.

Lemma 5.6. *The composition operator $\cdot$ is associative, that is*

$$(P \cdot Q) \cdot R = P \cdot (Q \cdot R)$$

for $P, Q, R \in \mathsf{pMR}_{0,d,f}(A)$.

Proof. For $(P \cdot Q) \cdot R = P \cdot (Q \cdot R)$ it is sufficient to prove $((P \cdot Q) \cdot R)(a) = (P \cdot (Q \cdot R))(a)$ for each $a \in A$. First, we show that the inclusion $((P \cdot Q) \cdot R)(a) \subseteq (P \cdot (Q \cdot R))(a)$ holds. Let $h \in ((P \cdot Q) \cdot R)(a)$. Then there exists $d \in (P \cdot Q)(a)$ and $F : \mathsf{supp}(d) \to \mathcal{D}(A)$ satisfying $\forall u \in A.\ (u, F(u)) \in R$ and $h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$ holds. Also, since $d \in (P \cdot Q)(a)$, there exists $d' \in P(a)$ and $F' : \mathsf{supp}(d') \to \mathcal{D}(A)$ such that $\forall t \in \mathsf{supp}(d').(t, F'(t)) \in Q$, and $d = \sum_{t \in \mathsf{supp}(d')} d'(t) \cdot F'(t)$ holds. Then

$\mathsf{supp}(d) = \bigcup\{\mathsf{supp}(F'(t)) \mid t \in \mathsf{supp}(d')\}$. We have

$$\begin{aligned}
h = & \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u) \\
= & \sum_{u \in \mathsf{supp}(d)} \left(\sum_{t \in \mathsf{supp}(d')} d'(t) \cdot F'(t) \right) (u) \cdot F(u) \\
= & \sum_{u \in \mathsf{supp}(d)} \sum_{t \in \mathsf{supp}(d')} (d'(t) \cdot F'(t)(u) \cdot F(u)) \\
= & \sum_{t \in \mathsf{supp}(d')} \sum_{u \in \mathsf{supp}(d)} (d'(t) \cdot F'(t)(u) \cdot F(u)) \\
= & \sum_{t \in \mathsf{supp}(d')} d'(t) \cdot \left(\sum_{u \in \mathsf{supp}(d)} F'(t)(u) \cdot F(u) \right) \\
= & \sum_{t \in \mathsf{supp}(d')} d'(t) \cdot \left(\sum_{u \in \bigcup_{s \in \mathsf{supp}(d')} \mathsf{supp}(F'(s))} F'(t)(u) \cdot F(u) \right) \\
= & \sum_{t \in \mathsf{supp}(d')} d'(t) \cdot \left(\sum_{u \in \mathsf{supp}(F'(t))} F'(t)(u) \cdot F(u) \right) \\
= & \sum_{t \in \mathsf{supp}(d')} d'(t) \cdot F''(t)
\end{aligned}$$

where

$$F''(t) = \sum_{u \in \mathsf{supp}(F'(t))} F'(t)(u) \cdot F(u) \quad .$$

Since $F''(t) \in (Q \cdot R)(t)$ for each $t \in \mathsf{supp}(d')$, we have $h \in (P \cdot (Q \cdot R))(a)$.

Conversely, if $h \in (P \cdot (Q \cdot R))(a)$, then there exists $d \in P(a)$ and $F : \mathsf{supp}(d) \to \mathcal{D}(A)$ satisfying $F(u) \in (Q \cdot R)(u)$ for each $u \in \mathsf{supp}(d)$ and $h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$. In addition, for each $u \in \mathsf{supp}(d)$, there exists $e_u \in Q(u)$ and $G_u : \mathsf{supp}(e_u) \to \mathcal{D}(A)$ satisfying $G_u(t) \in R(t)$ for each $t \in \mathsf{supp}(e_u)$ and $F(u) = \sum_{t \in \mathsf{supp}(e_u)} e_u(t) \cdot G_u(t)$. Then $\mathbf{0} \in R(t)$ for each $t \in A$ since R is 0-included. Let J be a set as follows:

$$J := \bigcup\{\mathsf{supp}(e_u) \mid u \in \mathsf{supp}(d)\} \quad .$$

Also, for $u \in \mathsf{supp}(d)$ let $G'_u : J \to \mathcal{D}(A)$ be as follows:

$$G'_u(t) := \begin{cases} G_u(t) & (t \in \mathsf{supp}(e_u)) \\ \mathbf{0} & (t \notin \mathsf{supp}(e_u)) \end{cases} \quad .$$

We have

$$\begin{aligned}
h &= \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u) \\
&= \sum_{u \in \mathsf{supp}(d)} d(u) \cdot \left(\sum_{t \in \mathsf{supp}(e_u)} e_u(t) \cdot G_u(t) \right) \\
&= \sum_{u \in \mathsf{supp}(d)} d(u) \cdot \left(\sum_{t \in J} e_u(t) \cdot G'_u(t) \right) \\
&= \sum_{u \in \mathsf{supp}(d)} \sum_{t \in J} (d(u) \cdot e_u(t) \cdot G'_u(t)) \\
&= \sum_{t \in J} \sum_{u \in \mathsf{supp}(d)} (d(u) \cdot e_u(t) \cdot G'_u(t)) \\
&= \sum_{t \in J} \left(\left(\sum_{u \in \mathsf{supp}(d)} d(u)\ e_u(t) \right) \cdot \sum_{u \in \mathsf{supp}(d)} \left(\frac{d(u) \cdot e_u(t)}{\sum_{u \in \mathsf{supp}(d)} d(u) \cdot e_u(t)} \cdot G'_u(t) \right) \right)
\end{aligned}$$

Let $G : J \to \mathcal{D}(A)$

$$G(t) := \sum_{u \in \mathsf{supp}(d)} \left(\frac{d(u) \cdot e_u(t)}{\sum_{u \in \mathsf{supp}(d)} d(u) \cdot e_u(t)} \cdot G'_u(t) \right) \quad .$$

Then we have $G(t) \in R(t)$ for each $t \in J$ since $\sum_{u \in \mathsf{supp}(d)} \frac{d(u) \cdot e_u(t)}{\sum_{u \in \mathsf{supp}(d)} d(u) \cdot e_u(t)} = 1$, $\mathsf{supp}(d)$ is finite and $R(t)$ is convex-closed. Let

$$d'(t) := \sum_{u \in \mathsf{supp}(d)} d(u) \cdot e_u(t) \ ,$$

then it holds that $d' \in (P \cdot Q)(a)$ and $\mathsf{supp}(d') = J$. Therefore

$$h = \sum_{t \in \mathsf{supp}(d')} d'(t) \cdot G(t) \in ((P \cdot Q) \cdot R)(a) \ .$$

□

Proposition 5.2. *Let $R \in \mathsf{pMR}_{0,d,f}(A)$. $0 \cdot R = 0$ and $R \cdot 0 = 0$.*

Proof. We already have $0 \subseteq 0 \cdot R$ and $0 \subseteq R \cdot 0$ because we already have proved that $0 \cdot R$ and $R \cdot 0$ are **0**-included in the lemma 5.5. If $(a, h) \in 0 \cdot R$, then there exists

$d \in \mathit{0}(a)$ and $F : \mathsf{supp}(d) \to \mathcal{D}(A)$ such that $h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$. Since $d = \mathbf{0}$ by the definition of $\mathit{0}$, we have

$$h = \sum_{u \in A} \mathbf{0}(u) \cdot F(u) = \mathbf{0}$$

Therefore $(a, h) = (a, \mathbf{0}) \in \mathit{0}$. Finally we show that $R \cdot \mathit{0} \subseteq \mathit{0}$. If $(a, h) \in R \cdot \mathit{0}$, then there exists $d \in R(a)$ and $F : \mathsf{supp}(d) \to \mathcal{D}(A)$ such that $h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$ and $\forall u \in A.\ (u, F(u)) \in 0$. Actually, $h = \sum_{u \in A} d(u) \cdot \mathbf{0} = \mathbf{0} \in 0(a)$. □

The identity $\mathit{1} \in \mathsf{pMR}_{\mathit{0},d,f}(A)$ is defined by

$$\mathit{1} := \{(a, d) \mid a \in A, d \sqsubseteq_{\mathcal{D}} \delta_a\} \ .$$

Lemma 5.7. *The identity satisfies the unit law, that is*

$$\mathit{1} \cdot R = R \text{ and } R \cdot \mathit{1} = R$$

for each $R \in \mathsf{pMR}_{0,d,f}(A)$.

Proof. First, we prove that $\mathit{1} \cdot R = R$. If $(a, h) \in \mathit{1} \cdot R$ then there exist $d \in \mathit{1}(a)$ and $F : A \to \mathcal{D}(A)$ such that $h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$ and $F \sqsubseteq R$. Since the definition of $\mathit{1}$, we have

$$\begin{aligned} h &= \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u) \\ &= d(a) \cdot F(a) \ . \end{aligned}$$

So we have $(a, F(a)) \in R$ and $h \sqsubseteq_{\mathcal{D}} F(a)$. Therefore $(a, h) \in R$ since R is down-closed.

Conversely, suppose $(a, h) \in R$. If we take $F : \mathsf{supp}(h) \to \mathcal{D}(A)$ such that

$$F(u) = \begin{cases} h & (u = a) \\ \mathbf{0} & (u \neq a) \ . \end{cases}$$

Then we have

$$(a, h) = (a, \sum_{u \in \{a\}} \delta_a(u) \cdot F(u)) \in \mathit{1} \cdot R \ .$$

Next we show that $R \cdot \mathit{1} = R$. Suppose $(a, h) \in R \cdot \mathit{1}$. Then there exists $d \in R(a)$ and $F : \mathsf{supp}(d) \to \mathcal{D}(A)$ such that $h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$ and $F \sqsubseteq \mathit{1}$. By the definition of the identity, we have $F(u) \sqsubseteq_{\mathcal{D}} \delta_u$ for each $u \in \mathsf{supp}(d)$ and

$$h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u) \sqsubseteq_{\mathcal{D}} \sum_{u \in \mathsf{supp}(d)} d(u) \cdot \delta_u = d \ .$$

Therefore $(a,h) \in R$ since R is down-closed.

Conversely, assume $(a,h) \in R$. If we take $F : \mathsf{supp}(d) \to \mathcal{D}(A)$ such that $F(u) = \delta_u$ for each $u \in \mathsf{supp}(d)$, then

$$(a,h) = (a, \sum_{u \in \mathsf{supp}(d)} h(u) \cdot F(u)) \in R \cdot 1 \ .$$

□

Lemma 5.6 and 5.7 show the following property.

Proposition 5.3. *A tuple* $(\mathsf{pMR}_{0,d,f}(A),\ \cdot,\ 1)$ *is a monoid.*

Next, we consider the left distributivity.

Proposition 5.4. *Let* χ *be a subset of* $\mathsf{pMR}_{0,d,f}(A)$*. Then*

$$(\bigvee \chi) \cdot R = \bigvee_{Q \in \chi} Q \cdot R$$

for each $R \in \mathsf{pMR}_{0,d,f}(A)$*.*

Proof. Obviously, it is satisfied $\bigvee_{Q\in\chi} Q \cdot R \subseteq (\bigvee \chi) \cdot R$ by the monotonicity of the composition $\cdot$. We show that $(\bigvee \chi) \cdot R \subseteq \bigvee_{Q\in\chi} Q \cdot R$. If $(a,h) \in (\bigvee \chi) \cdot R$ then there exists $d \in (\bigvee \chi)(a)$ and $F : \mathsf{supp}(d) \to \mathcal{D}(A)$ such that $h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$ and $F \sqsubseteq R$. Also, there exists $I \in \wp_f(A)$, $d' \in \mathcal{D}_1(I)$, and $F' : I \to (\bigcup \chi)(a)$ such that $d = \sum_{i\in I} d'(i) \cdot F'(i)$. So, we have

$$\begin{aligned}
h &= \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u) \\
&= \sum_{u \in \mathsf{supp}(d)} \left(\sum_{i\in I} d'(i) \cdot F'(i) \right) (u) \cdot F(u) \\
&= \sum_{u \in \mathsf{supp}(d)} \sum_{i\in I} (d'(i) \cdot F'(i)(u) \cdot F(u)) \\
&= \sum_{i\in I} \sum_{u \in \mathsf{supp}(d)} (d'(i) \cdot F'(i)(u) \cdot F(u)) \\
&= \sum_{i\in I} d'(i) \cdot \left(\sum_{u \in \mathsf{supp}(d)} F'(i)(u) \cdot F(u) \right) \\
&= \sum_{i\in I} d'(i) \cdot \left(\sum_{u \in \bigcup_{t \in \mathsf{supp}(d')} \mathsf{supp}(F'(i))} F'(i)(u) \cdot F(u) \right) \\
&= \sum_{i\in I} d'(i) \cdot \left(\sum_{u \in \mathsf{supp}(F'(i))} F'(i)(u) \cdot F(u) \right)
\end{aligned}$$

Therefore $(a,h) \in \bigvee_{Q\in\chi} Q \cdot R$ because for each $i \in I$,

$$\sum_{u \in \mathsf{supp}(F'(i))} F'(i)(u) \cdot F(u) \in \left(\bigcup_{Q\in\chi} Q \cdot R \right)(a) \ .$$

□

Also we have $(P+Q)\cdot R = P \cdot R + Q \cdot R$ for $P, Q, R \in \mathsf{pMR}_{0,d,f}(A)$.

5.4 Probabilistic Model of Complete IL-semiring

We have already shown that a tuple $(\mathsf{pMR}_{0,d,f}(A), +, \cdot, \mathit{0}, \mathit{1}, \bigvee)$ is a complete IL-semiring preserving the right 0 by Proposition 5.1, 5.2, 5.3 and 5.4. Additionally, it also preserves all right directed joins.

Lemma 5.8. *If $\chi \subseteq \mathsf{pMR}_{0,d,f}(A)$ is directed, $\bigcup_{Q\in\chi} Q$ is convex-closed.*

Proof. Assume that $\chi \subseteq (A)$ is directed, $p \in [0,1]$. We show that $(a,d),(a,d') \in \bigcup_{Q\in\chi} Q$ implies $(a, d \ {}_p\!\oplus\ d') \in \bigcup_{Q\in\chi} Q$. If $(a,d),(a,d') \in \bigcup_{Q\in\chi} Q$ then there exists $P, P' \in \chi$ such that $(a,d) \in P$, $(a,d') \in P'$. Since χ is directed, there exists $R \in \chi$ such that $P \subseteq R$, $P' \subseteq R$. Therefore $(a, d \ {}_p\!\oplus\ d') \in R \subseteq \bigcup_{Q\in\chi} Q$ since $d, d \in R(s)$ and R is convex-closed. □

By Proposition 5.1, 5.8, if $\chi \subseteq \mathsf{pMR}_{0,d,f}(A)$ is directed, $\bigcup_{Q\in\chi} Q$ is 0-included finitary down- and convex-closed. The fact indicates that the directed join $\bigvee \chi$ of $\chi \subseteq \mathsf{pMR}_{0,d,f}(A)$ is given by

$$\left(\bigvee \chi \right)(a) = \bigcup_{Q\in\chi} Q(a) \ .$$

Proposition 5.5. *Let χ be a directed subset of $\mathsf{pMR}_{0,d,f}(A)$. Then*

$$R \cdot \left(\bigvee \chi \right) = \bigvee_{Q\in\chi} R \cdot Q$$

for each $R \in \mathsf{pMR}_{0,d,f}(A)$.

Proof. Obviously, it is satisfied $\bigvee_{Q\in\chi} R\cdot Q \subseteq R \cdot (\bigvee \chi)$ by the monotonicity of the composition $\cdot$. We show that $R \cdot (\bigvee \chi) \subseteq \bigvee_{Q\in\chi} R \cdot Q$.

Assume that $(a, h) \in R; (\bigvee \chi)$.Then there exists $d \in R(a)$, $F \sqsubseteq \bigvee \chi$ such that $h = \sum\limits_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$. Since χ is directed, for each $u \in A$,

$$F(u) \in \left(\bigvee \chi\right)(u) = \bigcup_{Q \in \chi} Q(u) \ ,$$

that is, there exists $Q_u \in \chi$ satisfying $F \sqsubseteq Q_u$ for $u \in A$. Since $\{Q_u \mid u \in \mathsf{supp}(d)\}$ is finite and χ is directed, there exists $P \in \chi$ satisfying $Q_u \subseteq R$ for $u \in \mathsf{supp}(d)$. Then we have

$$h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u) \in R; P(a) \subseteq \left(\bigcup_{Q \in \chi}\right) R; Q(a) \ .$$

Therefore $(a, h) \in \bigvee_{Q \in \chi} R; Q$. □

Finally we proved that

Theorem 5.1. *A tuple* $(\mathsf{pMR}_{0,d,f}(A), +, \cdot, \mathit{0}, \mathit{1}, \bigvee)$ *is a complete IL-semiring preserving all right directed joins and the right* 0.

The following example shows that

$$P \cdot Q + P \cdot R = P \cdot (Q + R)$$

need not hold for $P, Q, R \in \mathsf{pMR}_{0,d,f}(A)$.

Example 5.2. Let A be a set $\{x, y\}$, and $P, Q \in \mathsf{pMR}_{0,d,f}(A)$ be as follows.

$$\begin{aligned} P &= \left\{(a, d) \mid a \in A \wedge \forall u \in A. d(u) \leq \tfrac{1}{2}\right\} \\ Q &= \{(a, d) \mid d(a) = 0\} \end{aligned}$$

Then, we have $(x, \delta_x) \in P; (Q + \mathit{1})$ because

$$\begin{aligned} \delta_x &= \tfrac{1}{2} \cdot \delta_x + \tfrac{1}{2} \cdot \delta_x \\ &= d(x) \cdot \delta_x + d(y) \cdot \delta_x \end{aligned}$$

and $\delta_x \in (Q + \mathit{1})(u)$ for each $u \in A$. On the other hand, we have $P \cdot Q + P \cdot \mathit{1} = P$ since $P \cdot Q \subseteq P$ and $P \cdot \mathit{1} = P$. Therefore $(x, \delta_x) \notin P = P \cdot Q + P \cdot \mathit{1}$.

5.5 Another Probabilistic Model of Complete IL-semiring

The previous probabilistic model of complete idempotent left semirings preserves all right directed join and the right 0. In this section, we study a probabilistic model of complete idempotent left semiring preserving the right 0 and show that this model need not preserve all directed join.

We treat only the subsets of $A \times \mathcal{D}_1(A)$ as probabilistic multirelations in this section. $\mathsf{pMR}_1(A)$ denotes the set of all probabilistic multirelations in the form of the subsets of $A \times \mathcal{D}_1(A)$. The partial order on $\mathsf{pMR}_1(A)$ is the inclusion relation $\subseteq$.

Definition 5.5 (Left-total)**.** *$R \in \mathsf{pMR}(A)$ is called* left-total *if*

$$R \neq \emptyset \implies \forall a \in A.\ R(a) \neq \emptyset\ .$$

Definition 5.6 ($\mathcal{D}_1$-convex closed)**.** *$R \in \mathsf{pMR}_1(A)$ is called $\mathcal{D}_1$-convex closed if for each $a \in A$, $d \in \mathcal{D}_1(A)$, and $F : A \to R(a)$,*

$$\sum_{u \in A} d(u) \cdot F(u) \in R(a)$$

We denote $\mathsf{pMR}_{t,1}(A)$ for a set of all left-total and $\mathcal{D}_1$-convex closed probabilistic multirelations over a set A.

We prove that $\mathsf{pMR}_{t,1}(A)$ forms complete idempotent left semiring preserving the right 0.

First, we think the arbitrary join and the least element on $\mathsf{pMR}_{t,1}(A)$. $P \cup Q$ need not be $\mathcal{D}_1$ convex closed for each $P, Q \in \mathsf{pMR}_{t,1}(A)$.

Example 5.3. Let A be a set $\{x, y\}$ and $P, Q \in \mathsf{pMR}_{t,1}(A)$ be as follows:

$$\begin{aligned} P &= \{(a, \delta_x) \mid a \in A\}\ , \\ Q &= \{(a, \delta_y) \mid a \in A\}\ . \end{aligned}$$

Then $(P \cup Q)(x) = \{\delta_x, \delta_y\}$. Assume that $d \in \mathcal{D}_1(A)$ satisfies $d(x) = d(y) = \dfrac{1}{2}$ and $F : A \to (P \cup Q)(x)$ satisfies $F(x) = \delta_x, F(y) = \delta_y$, then

$$\left(\sum_{i \in A} d(i) \cdot F(i) \right)(x) = d(x)\ \delta_x(x) + d(y)\ \delta_y(x) = \frac{1}{2}$$

Similarly, $\left(\sum_{i \in A} d(i) \cdot F(i)\right)(y) = \dfrac{1}{2}$. Therefore

$$\sum_{i \in A} d(i) \cdot F(i) \notin (P \cup Q)(x) \ .$$

We define the $\mathcal{D}_1$ convex hull to construct the join on $\mathsf{pMR}_{t,1}(A)$.

Definition 5.7 ($\mathcal{D}_1$ convex hull)**.** *For $R \in \mathsf{pMR}_1(A)$, let $H_1(R)$ be a set*

$$\left\{(a,\ \sum_{u \in A} d(u) \cdot F(u)) \mid a \in A,\ d \in \mathcal{D}_1(A),\ F : A \to R(a)\right\}.$$

$H_c(R)$ is the smallest $\mathcal{D}_1$ convex closed set containing $R \in \mathsf{pMR}_1(A)$.

Remark 5.2. *H_c is a closure operator on $\mathsf{pMR}_1(A)$.*

The operator H_c preserves left-totality.

Lemma 5.9. *If $R \in \mathsf{pMR}_1(A)$ is left-total, then $H_c(R)$ is left-total.*

Proof. Assume $H_c(R) \neq \emptyset$. There exists $a \in A$, $d \in \mathcal{D}_1(A)$, and $F : A \to R(a)$ satisfying

$$(a,\ \sum_{u \in A} d(u) \cdot F(u)) \in H_c(R) \ .$$

Then $R \neq \emptyset$ because $(a, F(u)) \in R$ for each $u \in A$. Since R is left-total, there exists $d_a \in \mathcal{D}_1(A)$ such that $(a, d_a) \in R$ for each $a \in A$. Therefore $H_c(R)$ is left-total since $(a, d_a) \in R \subseteq H_c(R)$. □

For each subset χ of $\mathsf{pMR}_{t,1}(A)$, the arbitrary join $\bigvee \chi$ is given by as follows.

$$\bigvee \chi := H_c\left(\bigcup \chi\right)$$

Especially, we write $P + Q$ for the binary join of $P, Q \in \mathsf{pMR}_{t,1}(A)$.

The operator $+$ is monotone, i.e.,

$$P \subseteq P' \ \wedge\ Q \subseteq Q' \implies P + Q \subseteq P' + Q'$$

for $P, P', Q, Q' \in \mathsf{pMR}_{t,1}(A)$.

The least element on $\mathsf{pMR}_{t,1}(A)$ is the emptyset. The emptyset as a probabilistic multirelation will be denoted by $\mathit{0}$. We obtain that $\mathit{0} \subseteq P$, $P = \mathit{0} + P$, $P + Q = Q + P$, and $P + P = P$ for $P, Q \in \mathsf{pMR}_{t,1}(A)$ obviously.

Lemma 5.10. *The operator + is associative, that is*

$$(P+Q)+R = P+(Q+R)$$

for $P, Q, R \in \mathsf{pMR}_{t,1}(A)$.

Proof. Suppose $P, Q, R \in \mathsf{pMR}_{t,1}(A)$. $(P+Q)+R = P+(Q+R)$ is sufficient to show that $(P+Q)+R \subseteq P+(Q+R)$ since $+$ is commutative. $P+Q \subseteq P+(Q+R)$ and $R \subseteq Q+R \subseteq P+(Q+R)$ hold since $+$ is monotone. Therefore $P+(Q+R)$ is a arbitrarily convex closed set containing $P+Q$ and R. We have $(P+Q)+R = H_c((P+Q) \cup R) \subseteq P+(Q+R)$ by the definition of H_c. □

Therefore the following property holds.

Proposition 5.6. $(\mathsf{pMR}_{t,1}(A), +, \mathit{0})$ is a idempotent commutative monoid.

The composition $P \cdot Q$ of $P, Q \in \mathsf{pMR}_{t,1}(A)$ is defined as follows:

$$\left\{(a,\ \sum_{u \in A} d(u) \cdot F(u)) \mid a \in A, d \in P(a),\ F : A \to \mathcal{D}(A) \text{ s.t. } F \sqsubseteq Q\right\}$$

where $F \sqsubseteq Q \iff \forall u \in A.(u, F(u)) \in Q$.

Lemma 5.11. $\mathsf{pMR}_{t,1}(A)$ *is closed under the composition* $\cdot$.

Proof. We show that $P \cdot Q \in \mathsf{pMR}_{t,1}(A)$ for each $P, Q \in \mathsf{pMR}_{t,1}(A)$.

First we prove that $P \cdot Q$ is left-total. If $P \cdot Q \neq \emptyset$ then there exists $(a, h) \in P \cdot Q$. By the definition of the composition, there exists $d \in P(a)$ and $F : A \to \mathcal{D}_1(A)$ such that

$$h = \sum_{u \in A} d(u) \cdot F(u)$$

and $F \sqsubseteq Q$. We obviously have P is not empty by $d \in P(a)$. Since P is left-total, for each $a \in A$ there exists $d_a \in P(a)$. We also obtain that Q is not empty, because $F : A \to \mathcal{D}_1(A)$ satisfies $F \sqsubseteq Q$. Therefore Q satisfies that for each $u \in A$ there exists $f_u \in \mathcal{D}_1(A)$ such that $(u, f_u) \in Q$ since Q is also left-total. It holds that

$$(a, \sum_{u \in A} d_a(u) \cdot f_u) \in P \cdot Q\ .$$

for each $a \in A$. Therefore $P \cdot Q$ is left-total.

Finally, we prove that $P \cdot Q$ is $\mathcal{D}_1$ convex closed. Suppose $d \in \mathcal{D}_1(A)$ and $F : A \to (P \cdot Q)(a)$. We show that

$$\sum_{i\in A} d(i) \cdot F(i) \in (P \cdot Q)(a) \ .$$

By the assumption, for each $i \in A$ there exists $e_i \in P(a)$ and $G_i : A \to \mathcal{D}_1(A)$ satisfying $G_i \sqsubseteq Q$ and $F(i) = \sum_{u\in A} e_i(u) \cdot G_i(u)$. Then we have

$$\begin{aligned}
\sum_{i\in A} d(i) \cdot F(i) &= \sum_{i\in A} d(i) \cdot \left(\sum_{u\in A} e_i(u) \cdot G_i(u) \right) \\
&= \sum_{i\in A}\sum_{u\in A} \left(d(i)\ e_i(u) \cdot G_i(u) \right) \\
&= \sum_{u\in A}\sum_{i\in A} \left(d(i)\ e_i(b) \cdot G_i(u) \right) \\
&= \sum_{u\in A} \left(\left(\sum_{i\in A} d(i)\ e_i(u) \right) \cdot \sum_{i\in A} \frac{d(i)\ e_i(u)}{\sum_{i\in A} d(i)\ e_i(u)} \cdot G_i(u) \right) \\
&= \sum_{u\in A} d'(u) \cdot G(u)
\end{aligned}$$

where

$$d' = \sum_{i\in A} d(i) \cdot e_i \quad \text{and} \quad G(u) = \sum_{i\in A} \frac{d(i) \cdot e_i(u)}{\sum_{i\in A} (d(i) \cdot e_i(u))} \cdot G_i(u) \ .$$

It holds that $(a, d') \in P$ since P is $\mathcal{D}_1$ convex closed. And also we have $G \sqsubseteq Q$ since Q is $\mathcal{D}_1$ convex closed. Therefore we obtain $\sum_{i\in A} d(i) \cdot F(i) \in (P \cdot Q)(a)$. □

The composition operator is monotone, i.e.,

$$P \subseteq P' \ \wedge \ Q \subseteq Q' \implies P \cdot Q \ \subseteq \ P' \cdot Q'$$

for $P,\ P',\ Q,\ Q' \in \mathsf{pMR}_{t,1}(A)$.

Lemma 5.12. *The composition operator $\cdot$ is associative, that is*

$$(P \cdot Q) \cdot R = P \cdot (Q \cdot R)$$

for $P, Q, R \in \mathsf{pMR}_{t,1}(A)$.

Proof. First, we show that $(P \cdot Q) \cdot R \subseteq P \cdot (Q \cdot R)$ holds. Suppose $(a, h) \in (P \cdot Q) \cdot R$. Then there exists $d \in (P \cdot Q)(a)$ and $F : A \to \mathcal{D}_1(A)$ such that $F \sqsubseteq R$ and $h = \sum_{u \in A} d(u) \cdot F(u)$ holds. Also since $d \in (P \cdot Q)(a)$, there exists $d' \in P(a)$ and $F' : A \to \mathcal{D}_1(A)$ such that $F' \sqsubseteq Q$, and $d = \sum_{t \in A} d'(t) \cdot F'(t)$ holds. We have

$$
\begin{aligned}
h &= \sum_{u \in A} d(u) \cdot F(u) \\
&= \sum_{u \in A} \left(\sum_{t \in A} d'(t) \cdot F'(t) \right) (u) \cdot F(u) \\
&= \sum_{u \in A} \sum_{t \in A} (d'(t) \cdot F'(t)(u) \cdot F(u)) \\
&= \sum_{t \in A} \sum_{u \in A} (d'(t) \cdot F'(t)(u) \cdot F(u)) \\
&= \sum_{t \in A} d'(t) \cdot \left(\sum_{u \in A} F'(t)(u) \cdot F(u) \right) \\
&= \sum_{t \in A} d'(t) \cdot F''(t)
\end{aligned}
$$

where

$$F''(t) = \sum_{u \in A} F'(t)(u) \cdot F(u).$$

Since $F'' \sqsubseteq Q \cdot R$, we have $(a, h) \in P \cdot (Q \cdot R)$.

Conversely, if $(a, h) \in P \cdot (Q \cdot R)$, then there exists $d \in P(a)$ and $F : A \to \mathcal{D}_1(A)$ satisfying $F \sqsubseteq Q \cdot R$ and $h = \sum_{u \in A} d(u) \cdot F(u)$. In addition, for each $u \in A$, there exists $e_u \in Q(u)$ and $G_u : A \to \mathcal{D}_1(A)$ satisfying $G_u \sqsubseteq R$ and $F(u) = \sum_{t \in A} e_u(t) \cdot G_u(t)$. Then there exists $f_t \in R(t)$ for each $t \in A$ since R is non-empty and left-total. We have

$$
\begin{aligned}
h &= \sum_{u \in A} d(u) \cdot F(u) \\
&= \sum_{u \in A} d(u) \cdot \left(\sum_{t \in A} e_u(t) \cdot G_u(t) \right) \\
&= \sum_{u \in A} \sum_{t \in A} (d(u) \cdot e_u(t) \cdot G_u(t)) \\
&= \sum_{t \in A} \sum_{u \in A} (d(u) \cdot e_u(t) \cdot G_u(t)) \\
&= \sum_{t \in A} \left(\left(\sum_{u \in A} d(u) \cdot e_u(t) \right) \cdot \sum_{u \in A} \left(\frac{d(u) \cdot e_u(t)}{\sum_{u \in A} d(u) \cdot e_u(t)} \cdot G_u(t) \right) \right)
\end{aligned}
$$

Let

$$d' := \sum_{u \in A} d(u) \cdot e_u \quad \text{and} \quad G(t) := \sum_{u \in A} \left(\frac{d(u) \cdot e_u(t)}{\sum_{u \in A} d(u) \cdot e_u(t)} \cdot G_u(t) \right) .$$

It is satisfied that $G'_u \sqsubseteq R$. Since $R(t)$ is $\mathcal{D}_1$ convex-closed, we have $G \sqsubseteq R$. Also it holds that $d' \in (P \cdot Q)(a)$. Therefore

$$h = \sum_{t \in A} d'(t) \cdot G(t) \in ((P \cdot Q) \cdot R)(a) .$$

□

Lemma 5.13. *Let $R \in \mathsf{pMR}_{t,1}(A)$. $0 \cdot R = 0$.*

Proof. By the definition of 0, $0 \subseteq 0 \cdot R$ holds obviously.

Conversely, we show that $0 \cdot R = \emptyset$. We have $0(a) = \emptyset$ since $0 = \emptyset$. Assume $(a, h) \in 0 \cdot R$. Then there exists $d \in 0(a)$. However it contradicts the fact that $0(a) = \emptyset$. □

Lemma 5.14. *Let $R \in \mathsf{pMR}_{t,1}(A)$. $R \cdot 0 = 0$.*

Proof. By the definition of 0, $0 \subseteq R \cdot 0$ holds obviously.

Conversely, we show that $R \cdot 0 = \emptyset$. If $(a, h) \in R \cdot 0$, then there exists $d \in R(a)$ and $F : A \to \mathcal{D}_1(A)$ such that $F \sqsubseteq 0$ and $h = \sum_{u \in A} d(u) \cdot F(u)$. However it contradicts the fact that $0 = \emptyset$. □

The identity $1 \in \mathsf{pMR}_{t,1}(A)$ is defined by

$$1 := \{(a, \delta_a) \mid a \in A\} .$$

Lemma 5.15. The identity satisfies the unit law, that is

$$1 \cdot R = R \text{ and } R \cdot 1 = R$$

for each $R \in \mathsf{pMR}_{t,1}(A)$.

Proof. First, we prove that $1 \cdot R = R$. If $(a, h) \in 1 \cdot R$ then there exist $d \in 1(a)$ and $F : A \to \mathcal{D}_1(A)$ such that $F \sqsubseteq R$ and $h = \sum_{u \in A} d(u) \cdot F(u)$. By the definition of the identity, we have

$$\begin{aligned} h &= \sum_{u \in A} d(u) \cdot F(u) \\ &= \sum_{u \in A} \delta_a(u) \cdot F(u) \\ &= F(a) . \end{aligned}$$

Therefore $(a, h) = (a, F(a)) \in R$ since $F \sqsubseteq R$. Conversely, suppose $(a, h) \in R$. Then there exists $f_u \in R(u)$ for each $u \in A$ because R is left-total. Let $F : A \to \mathcal{D}_1(A)$ as follows:

$$F(u) = \begin{cases} h & (u = a) \\ f_u & (u \neq a) \end{cases}$$

Then we have

$$(a, h) = (a, F(a)) = (a, \sum_{u \in A} \delta_a(u) \cdot F(u)) \in \mathit{1} \cdot R \ .$$

Next we show that $R \cdot \mathit{1} = R$. Assume $(a, h) \in R$. Let $F : A \to \mathcal{D}_1(A)$ be a mapping satisfying $F(u) = \delta_u$ for each $u \in A$. Then

$$(a, h) = (a, \sum_{u \in A} h(u) \cdot F(u)) \in R \cdot \mathit{1} \ .$$

Conversely, assume that $(a, h) \in R \cdot \mathit{1}$. Then there exists $d \in R(a)$ and $F : A \to \mathcal{D}_1(A)$ such that

$$h = \sum_{u \in A} d(u) \cdot F(u)$$

and $F \sqsubseteq \mathit{1}$. By the definition of the identity, we have

$$(a, h) = (a, \sum_{u \in A} d(u) \cdot \delta_u) = (a, d) \in R$$

□

Lemma 5.12 and 5.15 show the following property.

Proposition 5.7. *A tuple* $(\mathsf{pMR}_{t,1}(A), \ \cdot, \ \mathit{1})$ *is a monoid.*

Next, we consider the left distributivity.

Lemma 5.16. *Let* χ *is a subset of* $\mathsf{pMR}_{t,1}(A)$*, then*

$$(\bigvee \chi) \cdot R = \bigvee_{Q \in \chi} Q \cdot R$$

for each $R \in \mathsf{pMR}_{t,1}(A)$.

Proof. Obviously, it is satisfied $\bigvee_{Q\in\chi} Q \cdot R \subseteq (\bigvee\chi)\cdot R$ by the monotonicity of the composition. We show that $(\bigvee\chi)\cdot R \subseteq \bigvee_{Q\in\chi} Q\cdot R$. Assume that $(a,h)\in(\bigvee\chi)\cdot R$. If $R=0$, then $(\bigvee\chi)\cdot 0 = 0 \subseteq \bigvee_{Q\in\chi} Q\cdot R$. Suppose that $R\neq 0$. Then there exists $d\in(\bigvee\chi)(a)$ and $F: A\to\mathcal{D}(A)$ satisfying $F\sqsubseteq R$ and $h=\sum\limits_{u\in A} d(u)\cdot F(u)$. In addition, there exists $d'\in\mathcal{D}_1(A)$, and $F': A\to\left(\bigcup\chi\right)(a)$ such that $d=\sum\limits_{i\in A} d'(i)\cdot F'(i)$. So, we have

$$\begin{aligned}
h &= \sum_{u\in A} d(u)\cdot F(u)\\
&= \sum_{u\in A}\left(\sum_{i\in A} d'(i)\cdot F'(i)\right)(u)\cdot F(u)\\
&= \sum_{u\in A}\sum_{i\in A}\left(d'(i)\cdot F'(i)(u)\cdot F(u)\right)\\
&= \sum_{i\in A}\sum_{u\in A}\left(d'(i)\cdot F'(i)(u)\cdot F(u)\right)\\
&= \sum_{i\in A} d'(i)\cdot\left(\sum_{u\in A} F'(i)(u)\cdot F(u)\right)
\end{aligned}$$

Let $G: A\to\left(\bigcup_{Q\in\chi} Q\cdot R\right)(a)$ as $G(i) := \sum\limits_{u\in A} F'(i)(u)\cdot F(u)$. Therefore

$$h=\sum_{i\in A} d'(i)\cdot G(i)\in\bigvee_{Q\in\chi} Q\cdot R\ .$$

□

Also we have $(P+Q)\cdot R = P\cdot R + Q\cdot R$ for $P,Q,R\in\mathsf{pMR}_t(A)$. Therefore, we obtain the following property.

Proposition 5.8. *A tuple* $(\mathsf{pMR}_t(A),+,\cdot,0,1)$ *is an idempotent left semiring.*

$\mathsf{pMR}_t(A)$ forms a complete idempotent left semiring. In addition, we have the following theorem by the lemma 5.14.

Theorem 5.2. *A tuple* $(\mathsf{pMR}_t(A),+,\cdot,0,1,\bigvee)$ *is a complete idempotent left semi-ring preserving the right* 0.

The following example shows that

$$P \cdot Q + P \cdot R = P \cdot (Q + R)$$

need not hold for $P, Q, R \in \mathsf{pMR}_{t,1}(A)$.

Example 5.4. Let A be a set $\{x, y\}$, and $P, Q \in \mathsf{pMR}_{t,1}(A)$ be as follows.

$$\begin{array}{rcl} P & = & \left\{(a, d) \mid a \in A \wedge d(x) = d(y) = \dfrac{1}{2}\right\} \\ Q & = & \{(x, \delta_y), (y, \delta_x)\} \ . \end{array}$$

Then, we have $(x, \delta_x) \in P \cdot (Q + 1)$ because

$$\begin{array}{rcl} \delta_x & = & \dfrac{1}{2} \cdot \delta_x + \dfrac{1}{2} \cdot \delta_x \\ & = & d(x) \cdot \delta_x + d(y) \cdot \delta_x \end{array}$$

and also $\delta_x \in (Q+1)(u)$ for each $u \in A$. On the other hand, we have $P \cdot Q + P \cdot 1 = P$ since $P \cdot Q \subseteq P$ and $P \cdot 1 = P$. Therefore $(x, \delta_x) \notin P = P \cdot Q + P \cdot 1$.

Also for $P, Q \in \mathsf{pMR}_{t,1}(A)$ and directed subset $\chi \subseteq \mathsf{pMR}_{t,1}(A)$,

$$P \cdot \left(\bigvee \chi\right) \ = \ \bigvee_{Q \in \chi} P \cdot Q$$

need not hold.

Example 5.5. Let $\mathbb{N}$ be a set of all natural numbers, and P be a probabilistic multirelation

$$P = \{(0, d)\} \cup \{(a, \delta_a) \mid a > 0\}$$

where $d \in \mathcal{D}(A)$ satisfies $d(n) = \dfrac{1}{2^{n+1}}$ for each $n \in \mathbb{N}$. For $i \in \mathbb{N}$, let Q_i be

$$Q_i = \{(a, \delta_0 \ {}_p\!\oplus \delta_a) \mid a \leq i, p \in [0, 1]\} \cup \{(b, \delta_b) \mid i < b\} \ .$$

It satisfies that $P \in \mathsf{pMR}_{t,1}(\mathbb{N})$ and $\{Q_i \in \mathsf{pMR}_{t,1}(\mathbb{N}) \mid i \in \mathbb{N}\}$ is directed. Then we have $d \in P(0)$. Let $F : \mathbb{N} \to \mathcal{D}_1(\mathbb{N})$ be a function such that $F(u) = \delta_0$ for each $u \in A$. Then we have $F \sqsubseteq \bigcup_{i \in \mathbb{N}} Q_i$, and $(0, \delta_0) \in P \cdot \left(\bigcup_{i \in \mathbb{N}} Q_i\right) \subseteq P \cdot \left(\bigvee_{i \in \mathbb{N}} Q_i\right)$ because

$$\delta_0 = \sum_{u \in \mathbb{N}} d(u) \cdot F(u) \ .$$

However, we can prove that $(0, \delta_0) \notin \bigvee_{i \in \mathbb{N}} P \cdot Q_i$. We show that

$$(0, \ h) \in \bigvee_{i \in \mathbb{N}} P \cdot Q_i \implies h(0) < 1$$

If $(\omega, h) \in \bigvee_{i\in\mathbb{N}} P \cdot Q_i$, then there exists $d' \in \mathcal{D}_1(\mathbb{N})$ and $F : \mathbb{N} \to \left(\bigcup_{i\in\mathbb{N}} P \cdot Q_i\right)(0)$ such that

$$h = \sum_{j\in\mathbb{N}} d'(j) \cdot F(j) \ .$$

We consider $F(j) \in \left(\bigcup_{i\in\mathbb{N}} P \cdot Q_i\right)(0)$. For $j \in A$, there exists $k_j \in \mathbb{N}$ satisfying $F(j) \in P \cdot Q_{k_j}(0)$. Then there exists $e_j \in P(0)$ and $G_j : A \to \mathcal{D}(A)$ such that

$$F(j) = \sum_{u\in\mathbb{N}} e_j(u) \cdot G_j(u)$$

and $G_j \sqsubseteq Q_{k_j}$. By the definition of P, $e_j = d$ for each $j \in J$. Then we have

$$\begin{aligned}
F(j) &= \sum_{u\in\mathbb{N}} e_j(u) \cdot G_j(u) \\
&= \sum_{u\in\mathbb{N}} d(u) \cdot G_j(u) \\
&= \sum_{u\le k_j} d(u) \cdot G_j(u) + \sum_{u>k_j} d(u) \cdot G_j(u) \\
&= \sum_{u\le k_j} d(u) \cdot (\delta_0 \ {}_{p_u^j}\!\oplus \delta_u) + \sum_{u>k_j} d(u) \cdot \delta_u \ .
\end{aligned}$$

That is, $F(j)(0) = \sum_{u\le k_j} d(u) \cdot p_u^j$. Therefore we obtain $h(\omega) < 1$ because

$$\begin{aligned}
h(\omega) &= \sum_{j\in\mathbb{N}} d'(j) \cdot F(j)(0) \\
&= \sum_{j\in\mathbb{N}} d'(j) \cdot \sum_{u\le k_j} d(u) \cdot p_u^j \\
&\le \sum_{j\in\mathbb{N}} d'(j) \cdot \sum_{u\le k_j} d(u) \\
&= \sum_{j\in\mathbb{N}} d'(j) \cdot \left(1 - \frac{1}{2^{k_j+1}}\right) \\
&< \sum_{j\in\mathbb{N}} d'(j) \\
&= 1 \ .
\end{aligned}$$

5.6 Summary

In this chapter we have introduced a notion of probabilistic multirelations which is generalized semantic domain of probabilistic distributed systems given by McIver et al. And then we proved that the set of all 0-included finitary down- and convex-closed probabilistic multirelations forms a complete IL-semiring preserving all right directed joins and the right zero, and it also forms even a probabilistic Kleene algebra.

Also we have studied another type of probabilistic multirelations, and have proved that the set of all left-total and $\mathcal{D}_1$-convex closed probabilistic multirelations forms a complete IL-semiring preserving the right 0.

Chapter 6

Towards Abstraction for Probabilistic Systems

In this chapter we study the relationship between probabilistic systems and non-probabilistic systems. Specifically we consider a number of Galois connections between probabilistic multirelations and non-probabilistic multirelations.

6.1 Overview

A Galois connection is a particular correspondence between two partially ordered sets, and it appears in a theory, *Abstract Interpretation* formalized by Patrick Cousot et al. Abstract interpretation is a theory of sound approximation of the semantics of computer programs, and it can be viewed as a partial execution of a computer program which gains information about its semantics without performing all the calculations. That is, it guarantees soundness of abstraction.

In previous chapters we have shown a probabilistic model of complete IL-semirings and also two non-probabilistic models of them. Probabilistic model is the set of all finitary 0-included down- and convex-closed probabilistic multirelations. One of non-probabilistic models is the set of all total finitary up-closed multirelations, the other is the set of all $\perp$-included finite down-, and union-closed bottomed multirelations. In addition these two complete IL-semirings preserve all right directed join and the right zero. In this chapter we consider a number of Galois connections between these two complete IL-semirings and compare them from the aspect of which preserve operations with respect to complete IL-semiring.

This chapter is organized as follows. In section 6.2 we recall the definition of Galois connection and related proposition. Section 6.3 and 6.4 study Galois connections between probabilistic multirelations and up-closed multirelations. In section 6.5, we show a Galois connection between probabilistic multirelations and bottomed multirelations.

6.2 Galois Connection

First, we recall the definition of Galois connection and their properties.

Definition 6.1 (Galois connection). *For partially ordered sets $(C, \sqsubseteq)$, $(A, \leq)$, and functions $\alpha : C \to A$, $\gamma : A \to C$, a tuple (C, A, α, γ) is called Galois connection if the following holds for each $c \in C$ and $a \in A$.*

$$\alpha(c) \leq a \iff c \sqsubseteq \gamma(a)$$

If a tuple (C, A, α, γ) is Galis connection, then α is called left-adjoint of γ, conversely γ is called right-adjoint of α.

Corollary 6.1. *For partially ordered sets $(C, \sqsubseteq)$, $(A, \leq)$, and functions $\alpha : C \to A$, $\gamma : A \to C$, a tuple (C, A, α, γ) is called a Galois connection if and only if α and γ are monotone satisfying $\forall c \in C. c \sqsubseteq \gamma(\alpha(c))$ and $\forall a \in A. \alpha(\gamma(a)) \leq a$.*

We introduce a typical example of Galois connections.

Example 6.1. *Let C and A be sets. For two ordered sets $(\wp(C), \subseteq)$, $(\wp(A), \subseteq)$, and a mapping $f : C \to A$, consider two mappings $\alpha : \wp(C) \to \wp(A)$, $\gamma : \wp(A) \to \wp(C)$ as follows:*

$$\begin{array}{rcl} \alpha(X) & := & \{f(x) \mid x \in X\} \\ \gamma(Y) & := & \{x \in C \mid f(x) \in Y\} \ . \end{array}$$

Then $(\wp(C), \wp(A), \alpha, \gamma)$ is a Galois connection.

It is known the following proposition.

Proposition 6.1. *Let $(C, \sqsubseteq)$ and $(A, \leq)$ be partially ordered sets and $\alpha : C \to A$ a function. Assume that C is a complete lattice. Then α preserves arbitrary joins if and only if (C, A, α, γ) is a Galois connection where $\gamma : A \to C$ is defined as follows.*

$$\gamma(a) := \bigvee\{c \in C \mid \alpha(c) \leq a\} \ .$$

6.3 Simple Abstraction to Total Finitary Multirelations

In this section, we study a Galois connection between probabilistic multirelations and total finitary up-closed multirelations. Let $\alpha_{\mathsf{supp}} : \mathsf{pMR}_{0,d,f}(A) \to \mathsf{UMR}_{t,f}(A)$ be a mapping as follows.

$$\alpha_{\mathsf{supp}}(R) := \{(a, W) \mid \exists d \in R(a).[d \neq \mathbf{0} \wedge \mathsf{supp}(d) \subseteq W]\} \ .$$

Obviously $\alpha(R)$ is a total finitary up-closed multirelation. Also the mapping α_{supp} preserves the inclusion $\subseteq$.

We show that α_{supp} is a homomorphism of complete IL-semirings.

Lemma 6.1. α_{supp} *preserves the composition, i.e., for each $P, Q \in \mathsf{pMR}_{0,d,f}(A)$*

$$\alpha_{\mathsf{supp}}(P \cdot Q) = \alpha_{\mathsf{supp}}(P); \alpha_{\mathsf{supp}}(Q)$$

Proof. First we prove that $\alpha_{\mathsf{supp}}(P \cdot Q) \subseteq \alpha_{\mathsf{supp}}(P); \alpha_{\mathsf{supp}}(Q)$. Assume that $(a, W) \in \alpha_{\mathsf{supp}}(P \cdot Q)$. Then there exists $h \in \mathcal{D}(A)$ such that $(a, h) \in P \cdot Q$, $h \neq \mathbf{0}$ and $\mathsf{supp}(h) \subseteq W$. By the definition of the composition, there exists $d \in P(a)$ and the mapping $F : A \to \mathcal{D}(A)$ such that $h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$ and $(u, F(u)) \in Q$ for each $u \in \mathsf{supp}(d)$. We note that $d \neq \mathbf{0}$ because $d = \mathbf{0}$ implies $h = \mathbf{0}$. Then we obtain $(a, \mathsf{supp}(d)) \in \alpha_{\mathsf{supp}}(P)$. For each $u \in \mathsf{supp}(d)$, we have $(u, \mathsf{supp}(F(u))) \in \alpha_{\mathsf{supp}}(Q)$ and

$$\mathsf{supp}(F(u)) \subseteq \bigcup\{\mathsf{supp}(F(u)) \mid u \in \mathsf{supp}(d)\} = \mathsf{supp}(h) \subseteq W \ .$$

Then $(u, W) \in \alpha_{\mathsf{supp}}(Q)$ for each $u \in \mathsf{supp}(d)$ since $\alpha_{\mathsf{supp}}(Q)$ is up-closed. Therefore $(a, W) \in \alpha_{\mathsf{supp}}(P); \alpha_{\mathsf{supp}}(Q)$ by the definition of ;.

Conversely we prove that $\alpha_{\mathsf{supp}}(P);\alpha_{\mathsf{supp}}(Q) \subseteq \alpha_{\mathsf{supp}}(P \cdot Q)$. We have

$$\begin{aligned}
& (a,W) \in \alpha_{\mathsf{supp}}(P);\alpha_{\mathsf{supp}}(Q) \\
\iff & \exists Y \in \wp(A).[(a,Y) \in \alpha_{\mathsf{supp}}(P) \wedge \forall y \in Y.(y,W) \in \alpha_{\mathsf{supp}}(Q)] \\
\iff & \exists Y \in \wp(A).[\exists d \in R(a).[d \neq \mathbf{0} \wedge \mathsf{supp}(d) \subseteq Y] \wedge \\
& \qquad \forall y \in Y.\exists f_y \in Q(y).[f_y \neq \mathbf{0} \wedge \mathsf{supp}(f_y) \subseteq W]] \\
\implies & \exists Y \in \wp(A).[\exists d \in R(a).[d \neq \mathbf{0} \wedge \mathsf{supp}(d) \subseteq Y \wedge \\
& \qquad \forall y \in Y.\exists f_y \in Q(y).[f_y \neq \mathbf{0} \wedge \mathsf{supp}(f_y) \subseteq W]]] \\
\implies & \exists d \in R(a).[d \neq \mathbf{0} \wedge \forall y \in \mathsf{supp}(d).\exists f_y \in Q(y).[f_y \neq \mathbf{0} \wedge \mathsf{supp}(f_y) \subseteq W]] \ .
\end{aligned}$$

Let $F : \mathsf{supp}(d) \to \mathcal{D}(A)$ be a mapping such that $F(y) := f_y$ for each $y \in \mathsf{supp}(d)$. Set $h := \sum_{y \in \mathsf{supp}(d)} d(y) \cdot F(y)$. Then we have $(a,h) \in P \cdot Q$ and $\mathsf{supp}(h) \subseteq W$ since

$$\mathsf{supp}(h) = \bigcup \{\mathsf{supp}(F(y)) \mid y \in \mathsf{supp}(d)\}$$

and $\mathsf{supp}(F(y)) \subseteq W$ for each $y \in \mathsf{supp}(d)$. And we also have $h \neq \mathbf{0}$ since $d \neq \mathbf{0}$ and $F(y) \neq \mathbf{0}$ for each $y \in \mathsf{supp}(d)$. Therefore $(a,W) \in \alpha_{\mathsf{supp}}(P \cdot Q)$. □

Lemma 6.2. α_{supp} *preserves the 0-ary operators, 0 and 1.*

Proof. Obviously $\alpha_{\mathsf{supp}}(\mathit{0}) = \emptyset$ holds by the definition of α_{supp}.

Suppose that $(a,W) \in \alpha_{\mathsf{supp}}(\mathit{1})$. Then there exists $d \in \mathit{1}(a)$ such that $d \neq \mathbf{0}$ and $\mathsf{supp}(d) \subseteq W$. This fact implies $a \in W$. Conversely, if $a \in W$ then $\delta_a \in \mathit{1}(a)$, $\delta_a \neq \mathbf{0}$, and $\mathsf{supp}(\delta_a) \subseteq W$. □

Lemma 6.3. α_{supp} *preserves arbitrary joins, i.e., for each* $\chi \subseteq \mathsf{pMR}_{0,d,f}(A)$

$$\alpha_{\mathsf{supp}}(\bigvee \chi) = \bigcup_{R \in \chi} \alpha_{\mathsf{supp}}(R)$$

Proof. Obviously $\bigcup_{R \in \chi} \alpha_{\mathsf{supp}}(R) \subseteq \alpha_{\mathsf{supp}}(\bigvee \chi)$ since α_{supp} preserves the inclusion.

Conversely, we prove that $\alpha_{\mathsf{supp}}(\bigvee \chi) \subseteq \bigcup_{R \in \chi} \alpha_{\mathsf{supp}}(R)$. Suppose that $(a,W) \in \alpha_{\mathsf{supp}}(\bigvee \chi)$. Then there exists $h \in \mathcal{D}(a)$ such that $(a,h) \in \bigvee \chi$, $h \neq \mathbf{0}$ and $\mathsf{supp}(h) \subseteq W$. By the definition of $\bigvee$, there exists $I \in \wp_f(A)$, $d \in \mathcal{D}_1(I)$, and the mapping $F : I \to (\bigcup \chi)(a)$ such that $h = \sum_{i \in I} d(i) \cdot F(i)$. Then we have

$$\mathsf{supp}(h) = \bigcup \{\mathsf{supp}(F(i)) \mid i \in \mathsf{supp}(d)\} \ .$$

Also for some $i \in \mathsf{supp}(d)$, there exists $R_i \in \chi$ such that $(a, F(i)) \in R_i$. Then we have $(a,W) \in \alpha(R_i)$ since

$$\mathsf{supp}(F(i)) \subseteq \bigcup \{\mathsf{supp}(F(i)) \mid i \in \mathsf{supp}(d)\} = \mathsf{supp}(h) \subseteq W \ .$$

□

We obtain the following proposition by Lemma 6.1, 6.2, 6.3.

Proposition 6.2. α_{supp} *is a homomorphism of complete IL-semirings.*

And we also have a Galois connection by Lemma 6.3

Theorem 6.1. *For a set A, $(\mathsf{pMR}_{0,d,f}(A), \mathsf{UMR}_{t,f}(A), \alpha, \gamma)$ is a Galois connection where $\alpha_{\mathsf{supp}} : \mathsf{pMR}_{0,d,f}(A) \to \mathsf{UMR}_{t,f}(A)$ is defined by*

$$(a, W) \in \alpha_{\mathsf{supp}}(R) \overset{def}{\iff} \exists d \in R(a).[d \neq \mathbf{0} \land \mathsf{supp}(d) \subseteq W] \ .$$

and $\gamma_{\mathsf{supp}} : \mathsf{UMR}_{t,f}(A) \to \mathsf{pMR}_{0,d,f}(A)$ is given as Proposition 6.1.

We have given a Galois connection between $\mathsf{pMR}_{0,d,f}(A)$ and $\mathsf{UMR}_{t,f}(A)$, on the natural way in the sense of using the support supp of probabilistic distributions. However, α_{supp} need not preserve the counter example of the left distributivity though this distributivity need not hold on two complete IL-semiring $\mathsf{pMR}_{0,d,f}(A)$ and $\mathsf{UMR}_{t,f}(A)$.

Example 6.2. *We consider probabilistic multirelations P and Q that appeared in Example 5.2. Then $\alpha_{\mathsf{supp}}(P) = \alpha_{\mathsf{supp}}(Q) = \{(a, W) \mid a \in A \land W \neq \emptyset\}$. We already have shown that $P \cdot (Q + 1) \not\subseteq P \cdot Q + P \cdot 1$. Since $\alpha(P) \subseteq \alpha(P); \alpha(P)$, we have*

$$\begin{aligned}
\alpha_{\mathsf{supp}}(P \cdot (Q + 1)) &= \alpha_{\mathsf{supp}}(P \cdot Q) \\
&= \alpha_{\mathsf{supp}}(P); \alpha_{\mathsf{supp}}(Q) \\
&= \alpha_{\mathsf{supp}}(P); \alpha_{\mathsf{supp}}(P) \\
&= \alpha_{\mathsf{supp}}(P); \alpha_{\mathsf{supp}}(P) + \alpha_{\mathsf{supp}}(P) \\
&= \alpha_{\mathsf{supp}}(P); \alpha_{\mathsf{supp}}(Q) + \alpha_{\mathsf{supp}}(P); \alpha_{\mathsf{supp}}(1) \\
&= \alpha_{\mathsf{supp}}(P \cdot Q + P \cdot 1) \ .
\end{aligned}$$

6.4 Revised Abstraction to Total Finitary Multirelations

Reducing the left distributivity from the definition of complete I-semirings (even Kleene algebras) is a typical relaxation for applying probabilistic systems. In this section, we aim at revised abstraction which preserving the counter example of the left distributivity. Then we revise the mapping $\alpha_{\mathsf{supp}} : \mathsf{pMR}_{0,d,f}(A) \to \mathsf{UMR}_{t,f}(A)$.

Let $\alpha_1 : \mathsf{pMR}_{0,d,f}(A) \to \mathsf{UMR}_{t,f}(A)$ be a mapping as follows.

$$\alpha_1(R) := \{(a, W) \mid \exists d \in R(a).[d \in \mathcal{D}_1(A) \land \mathsf{supp}(d) \subseteq W]\} \ .$$

In the above definition, we restrict the sum of probabilities of the distribution to 1, from the definition of α_{supp}.

The mapping α_1 preserves the inclusion $\subseteq$.

We show that α_1 is a homomorphism of complete IL-semirings. The required proofs are similar to Lemma 6.1, 6.2, 6.3.

Lemma 6.4. *α_1 preserves the composition, i.e., for each $P, Q \in \mathsf{pMR}_{0,d,f}(A)$*

$$\alpha_1(P \cdot Q) = \alpha_1(P); \alpha_1(Q)$$

Proof. First we prove that $\alpha_1(P \cdot Q) \subseteq \alpha_1(P); \alpha_1(Q)$. Assume that $(a, W) \in \alpha_1(P \cdot Q)$. Then there exists $h \in \mathcal{D}_1(A)$ such that $(a, h) \in P \cdot Q$ and $\mathsf{supp}(h) \subseteq W$. By the definition of the composition, there exists $d \in P(a)$ and the mapping $F : A \to \mathcal{D}(A)$ such that $h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$ and $(u, F(u)) \in Q$ for each $u \in \mathsf{supp}(d)$. Then we obtain $(a, \mathsf{supp}(d)) \in \alpha_1(P)$. For each $u \in \mathsf{supp}(d)$, we have $(u, \mathsf{supp}(F(u))) \in \alpha_1(Q)$ and

$$\mathsf{supp}(F(u)) \subseteq \bigcup\{\mathsf{supp}(F(u)) \mid u \in \mathsf{supp}(d)\} = \mathsf{supp}(h) \subseteq W \ .$$

Then $(u, W) \in \alpha_1(Q)$ for each $u \in \mathsf{supp}(d)$ since $\alpha_1(Q)$ is up-closed. Therefore $(a, W) \in \alpha_1(P); \alpha_1(Q)$ by the definition of ;.

Conversely we prove that $\alpha_1(P); \alpha_1(Q) \subseteq \alpha_1(P \cdot Q)$. We have

$$\begin{aligned}
& (a, W) \in \alpha_1(P); \alpha_1(Q) \\
\iff\ & \exists Y \in \wp(A).[(a, Y) \in \alpha_1(P) \wedge \forall y \in Y.(y, W) \in \alpha_1(Q)] \\
\iff\ & \exists Y \in \wp(A).[\exists d \in R(a).[d \in \mathcal{D}_1(A) \wedge \mathsf{supp}(d) \subseteq Y] \wedge \\
& \qquad \forall y \in Y.\exists f_y \in Q(y).[f_y \in \mathcal{D}_1(A) \wedge \mathsf{supp}(f_y) \subseteq W]] \\
\implies\ & \exists Y \in \wp(A).[\exists d \in R(a).[d \in \mathcal{D}_1(A) \wedge \mathsf{supp}(d) \subseteq Y \wedge \\
& \qquad \forall y \in Y.\exists f_y \in Q(y).[f_y \in \mathcal{D}_1(A) \wedge \mathsf{supp}(f_y) \subseteq W]]] \\
\implies\ & \exists d \in P(a).[d \in \mathcal{D}_1(A) \wedge \\
& \qquad \forall y \in \mathsf{supp}(d).\exists f_y \in Q(y).[f_y \in \mathcal{D}_1(A) \wedge \mathsf{supp}(f_y) \subseteq W]] \ .
\end{aligned}$$

Let $F : \mathsf{supp}(d) \to \mathcal{D}_1(A)$ be a mapping such that $F(y) := f_y$ for each $y \in \mathsf{supp}(d)$. Set $h := \sum_{y \in \mathsf{supp}(d)} d(y) \cdot F(y)$. Then we have $(a, h) \in P \cdot Q$ and $\mathsf{supp}(h) \subseteq W$ since $\mathsf{supp}(h) = \bigcup\{\mathsf{supp}(F(y)) \mid y \in \mathsf{supp}(d)\}$ and $\mathsf{supp}(F(y)) \subseteq W$ for each $y \in \mathsf{supp}(d)$. Also we have $h \in \mathcal{D}_1(A)$ since $d \in \mathcal{D}_1(A)$ and $F(y) \in \mathcal{D}_1(A)$ for each $y \in \mathsf{supp}(d)$. Therefore $(a, W) \in \alpha_1(P \cdot Q)$. $\square$

Lemma 6.5. *α_1 preserves the 0-ary operators, 0 and 1.*

Proof. Obviously $\alpha_1(\mathit{0}) = \emptyset$ holds by the definition of α_1.

Suppose that $(a, W) \in \alpha_1(\mathit{1})$. Then there exists $d \in \mathit{1}(a)$ such that $d \in \mathcal{D}_1(A)$ and $\mathsf{supp}(d) \subseteq W$. This fact implies $d = \delta_a$ and $a \in W$. Conversely, if $a \in W$ then $\delta_a \in \mathit{1}(a)$, $\delta_a \neq \mathbf{0}$, and $\mathsf{supp}(\delta_a) \subseteq W$. □

Lemma 6.6. *α_1 preserves arbitrary joins, i.e., for each $\chi \subseteq \mathsf{pMR}_{0,d,f}(A)$*

$$\alpha_1(\bigvee \chi) = \bigcup_{R \in \chi} \alpha_1(R)$$

Proof. Obviously $\bigcup_{R\in\chi} \alpha_1(R) \subseteq \alpha_1(\bigvee \chi)$ since α_1 preserves the inclusion.

Conversely, we prove that $\alpha_1(\bigvee \chi) \subseteq \bigcup_{R\in\chi} \alpha_1(R)$. Suppose that $(a, W) \in \alpha_1(\bigvee \chi)$. Then there exists $h \in \mathcal{D}_1(A)$ such that $(a, h) \in \bigvee \chi$ and $\mathsf{supp}(h) \subseteq W$. By the definition of $\bigvee$, there exists $I \in \wp_f(A)$, $d \in \mathcal{D}_1(I)$, and the mapping $F : I \to (\bigcup \chi)\,(a)$ such that $h = \sum_{i\in I} d(i)\cdot F(i)$. Then we have $\mathsf{supp}(h) = \bigcup\{\mathsf{supp}(F(i)) \mid i \in \mathsf{supp}(d)\}$. Note that $F(i) \in \mathcal{D}_1(A)$. For each $i \in \mathsf{supp}(d)$, there exists $R_i \in \chi$ such that $(a, F(i)) \in R_i$. Then we have $(a, W) \in \alpha_1(R_i)$ since

$$\mathsf{supp}(F(i)) \subseteq \bigcup\{\mathsf{supp}(F(i)) \mid i \in \mathsf{supp}(d)\} = \mathsf{supp}(h) \subseteq W \ .$$

Therefore $(a, W) \in \bigcup_{R\in\chi} \alpha_1(R)$. □

We obtain the following proposition by Lemma 6.4, 6.5, 6.6.

Proposition 6.3. *α_1 is a homomorphism of complete IL-semirings.*

And we also have a Galois connection by Lemma 6.6

Theorem 6.2. *For a set A, $(\mathsf{pMR}_{0,d,f}(A), \mathsf{UMR}_{t,f}(A), \alpha_1, \gamma)$ is a Galois connection where $\alpha_1 : \mathsf{pMR}_{0,d,f}(A) \to \mathsf{UMR}_{t,f}(A)$ is defined by*

$$(a, W) \in \alpha_1(R) \overset{def}{\iff} \exists d \in R(a).[d \in \mathcal{D}_1(A) \wedge \mathsf{supp}(d) \subseteq W] \ .$$

and $\gamma_{\mathsf{supp}} : \mathsf{UMR}_{t,f}(A) \to \mathsf{pMR}_{0,d,f}(A)$ is given as Proposition 6.1.

We have given second Galois connection between $\mathsf{pMR}_{0,d,f}(A)$ and $\mathsf{UMR}_{t,f}(A)$ revising a mapping α_{supp}. And then α_1 preserves a counter example of the left distributivity unlike in the case of α_{supp}.

Example 6.3. *We consider probabilistic multirelations P and Q that appeared in Example 5.2. Then*

$$\begin{aligned}
\alpha_1(P) &= \{(a, \{x, y\}) \mid a \in A\} \textit{ and },\\
\alpha_1(Q) &= \{(x, \{y\}), (x, \{x, y\}), (y, \{x\}), (y, \{x, y\})\} \ .
\end{aligned}$$

We already have shown that $(x, \delta_x) \in P \cdot Q + P \cdot 1$ *though* $(x, \delta_x) \in P \cdot (Q + 1)$ *in Example 5.2. Since* α_1 *is the homomorphism of complete IL-semirings,*

$$\begin{aligned}
&\alpha_1(P \cdot (Q + 1)) = \alpha_1(P); (\alpha_1(Q) \cup \alpha_1(1)) \textit{ and}\\
&\alpha_1(P \cdot Q + R \cdot 1) = \alpha_1(P); \alpha_1(Q) \cup \alpha_1(P); \alpha_1(1) \ .
\end{aligned}$$

We have $(x, \{x\}) \in \alpha_1(P); (\alpha_1(Q) \cup \alpha_1(1))$ *since* $(x, \{x, y\}) \in \alpha_1(P)$, $(x, \{x\}) \in \alpha_1(1)$ *and* $(x, \{y\}) \in \alpha_1(Q)$. *However* $(x, \{x\})$ *is not in* $\alpha_1(P); \alpha_1(Q)$ *and* $\alpha_1(P); \alpha_1(1)$.

The following example show that γ_1 need not be a homomorphism of **CILS**. Note that $\gamma_1(1) = \bigvee\{R \mid \alpha_1(R) \subseteq 1\}$.

Example 6.4. *We consider a probabilistic multirelation*

$$R = \left\{(a, d) \mid a \in A \wedge \forall u \in A.d(u) \leq \tfrac{1}{2}\right\}$$

on a set $A := \{x, y\}$. *Then we have* $R \subseteq \gamma_1(1)$ *since*

$$\alpha_1(R) = \{(x, \{x, y\}), (y, \{x, y\})\} \subseteq 1 \ .$$

However $R \not\subseteq 1$. *Therefore* $\gamma_1(1) \not\subseteq 1$.

6.5 Abstraction to Bottomed Multirelations

In this section we introduce a Galois connection between probabilistic multirelations and bottomed multirelations. And then we discuss the difference from Galois connections in the previous sections.

Let $\beta : \mathsf{pMR}_{0,d,f}(A) \to \mathsf{bMR}(A)$ be a mapping as follows.

$$\begin{aligned}
\beta(R) \quad = \quad & \{(a, \mathsf{supp}(d)^{\perp}) \mid (a, d) \in R \wedge d \notin \mathcal{D}_1(A)\}\\
& \cup\{(a, \mathsf{supp}(d)) \mid (a, d) \in R \wedge d \in \mathcal{D}_1(A)\} \cup \{(\perp.\{\perp\})\}
\end{aligned}$$

The mapping β preserves the inclusion $\subseteq$. $\beta(R)$ is $\perp$-included finite down- and union-closed. First we prepare the following lemma before proving that β is a homomorphism of complete IL-semirings.

Lemma 6.7. *The mapping* $\beta : \mathsf{pMR}_{0,d,f}(A) \to \mathsf{bMR}(A)$ *satisfies the followings.*

$$(a, W) \in \beta(R) \implies \exists d \in R(a).\ W \sqsubseteq_{\mathcal{A}} \mathsf{supp}(d) \quad \textit{for each } a \in A \textit{ and } W \in \wp(A^{\perp}).$$

Proof. Assume that $(a, W) \in \beta(R)$. Then there exists $d \in R(a) \backslash \mathcal{D}_1(A)$ such that $W = \mathsf{supp}(d)^{\perp}$, or there exists $d \in R(a) \cap \mathcal{D}_1(A)$ such that $W = \mathsf{supp}(d)$. In these two case, we have $W \sqsubseteq_{\mathcal{A}} \mathsf{supp}(d)$. $\square$

Next we show that β preserves the composition on complete IL-semiring.

Lemma 6.8. *β preserves the composition, i.e., for each $P, Q \in \mathsf{pMR}_{0,d,f}(A)$*

$$\beta(P \cdot Q) = \beta(P); \beta(Q)$$

Proof. First we prove that $\beta(P \cdot Q) \subseteq \beta(P); \beta(Q)$. Assume that $(a, W) \in \beta(P \cdot Q)$. If $a = \perp$ then $(a, W) = (\perp, \{\perp\}) \in \beta(P); \beta(Q)$ obviously. If $a \neq \perp$ then there exists $h \in (P \cdot Q)(a)$ such that $h \in \mathcal{D}_1(A)$ and $W = \mathsf{supp}(h)$ or, $h \notin \mathcal{D}_1(A)$ and $W = \mathsf{supp}(h)^{\perp}$. By the definition of the composition on probabilistic multirelations, there exists $d \in P(a)$ and the mapping $F : A \to \mathcal{D}(A)$ such that $h = \sum_{u \in \mathsf{supp}(d)} d(u) \cdot F(u)$ and $(u, F(u)) \in Q$ for each $u \in \mathsf{supp}(d)$. If $h \in \mathcal{D}_1(A)$ and $W = \mathsf{supp}(h)$, then $(a, \mathsf{supp}(d)) \in \beta(P)$ and $(u, \mathsf{supp}(F(u))) \in \beta(Q)$ for each $u \in \mathsf{supp}(d)$ since $h \in \mathcal{D}_1(A)$ implies $d \in \mathcal{D}_1(A)$ and $F(u) \in \mathcal{D}_1(A)$ for each $u \in \mathsf{supp}(d)$. Therefore

$$(a, W) = \left(a, \bigcup_{u \in \mathsf{supp}(d)} \mathsf{supp}(F(u))\right) \in \beta(P); \beta(Q)$$

by the definition of the composition ; on bottomed multirelations. Assume that $h \notin \mathcal{D}_1(A)$ and $W = \mathsf{supp}(h)^{\perp}$. We have $(a, \mathsf{supp}(d)^{\perp}) \in \beta(P)$. Since $(\perp, \{\perp\}) \in \beta(A)$ and $(u, F(u)) \in \beta(Q)$ for each $u \in \mathsf{supp}(d)$, we obtain

$$(a, W) = (a, \mathsf{supp}(h)^{\perp}) = \left(a, \bigcup_{u \in \mathsf{supp}(d)} \mathsf{supp}(F(u)) \cup \{\perp\}\right) \in \beta(P); \beta(Q)\ .$$

Conversely we prove that $\beta(P); \beta(Q) \subseteq \beta(P \cdot Q)$. Assume that $(a, W) \in \beta(P); \beta(Q)$. If $a = \perp$ then $(a, W) = (\perp, \{\perp\}) \in \beta(P \cdot Q)$ obviously. If $a \neq \perp$ then there exists $Y \in \wp(A^{\perp})$ such that

$$(a, Y) \in \beta(P)\ \land\ \forall y \in Y. \exists X_y \in \wp(A^{\perp}). \left[(y, X_y) \in \beta(Q) \land W = \bigcup_{y \in Y} X_y\right]$$

By Lemma 6.7, there exists $d \in P(a)$ such that $Y \sqsubseteq_{\mathcal{A}} \mathsf{supp}(d)$, and also exists $f_y \in Q(y)$ such that $X_y \sqsubseteq_{\mathcal{A}} \mathsf{supp}(f_y)$ for each $y \in Y \backslash \{\perp\}$. Let $F : \mathsf{supp}(d) \to \mathcal{D}(A)$ be a mapping such that $F(y) := f_y$ for each $y \in \mathsf{supp}(d)$. Set $h := \sum_{y \in \mathsf{supp}(d)} d(y) \cdot F(y)$. Then we have $(a, h) \in P \cdot Q$. If $\perp \notin W$ then $\perp \notin X_y$ for each $y \in Y$, and $\perp \notin Y$. Since $Y = \mathsf{supp}(d)$ and $X_y = \mathsf{supp}(f_y)$ for each $y \in Y$,

$$W = \bigcup_{y \in Y} X_y = \bigcup_{y \in \mathsf{supp}(d)} \mathsf{supp}(F(y)) = \mathsf{supp}(h) \ .$$

Therefore $(a, W) \in \beta(P \cdot Q)$.

If $\perp \in W$ then there exists $y \in Y$ such that $\perp \in X_y$. And then

$$W = \bigcup_{y \in Y} X_y = \{\perp\} \cup \bigcup_{y \in Y \setminus \{\perp\}} X_y = \{\perp\} \cup \bigcup_{y \in \mathsf{supp}(d)} \mathsf{supp}(F(y)) = \mathsf{supp}(h)^{\perp} \ .$$

Therefore $(a, W) \in \beta(P \cdot Q)$ since $W \sqsubseteq_{\mathcal{A}} \mathsf{supp}(h)^{\perp}$. □

Lemma 6.9. *β preserves the 0-ary operators, 0 and 1.*

Proof. Obviously $\beta(\mathit{0}) = \{(a, \{\perp\}) \mid a \in A^{\perp}\}$ holds by the definition of β.

Assume that $(a, W) \in \beta(\mathit{1})$. Then there exists $d \in \mathit{1}(a) \cap \mathcal{D}_1(A)$ and $W = \mathsf{supp}(d)$, or $d \in \mathit{1}(a) \backslash \mathcal{D}_1(A)$ and $W = \mathsf{supp}(d)^{\perp}$. In both case $(a, W) \in 1$. Conversely, if $W \sqsubseteq_{\mathcal{A}} \{a\}$ then $W = \{a\}$, $\{a, \perp\}$, $\{\perp\}$. In the case of $W = \{a\}$, $\delta_a \in \mathit{1}(a) \cap \mathcal{D}_1(A)$ and $\{a\} = \mathsf{supp}(\delta_a)$. In the case of $W = \{a, \perp\}$ and $W = \{\perp\}$, we have $\frac{1}{2}\delta_a, \mathbf{0} \in \mathit{1}(a) \backslash \mathcal{D}_1(A)$, $\{a, \perp\} = \mathsf{supp}(\frac{1}{2}\delta_a)^{\perp}$, and $\{\perp\} = \mathsf{supp}(\mathbf{0})^{\perp}$ □

Lemma 6.10. *β preserves arbitrary joins, i.e., for each $\chi \subseteq \mathsf{pMR}_{0,d,f}(A)$*

$$\beta(\bigvee \chi) = \bigvee\nolimits_{R \in \chi} \beta(R)$$

Proof. Obviously $\bigvee_{R \in \chi} \beta(R) \subseteq \beta(\bigvee \chi)$ since β preserves the inclusion.

Conversely, we prove that $\beta(\bigvee \chi) \subseteq \bigvee_{R \in \chi} \beta(R)$. Suppose that $(a, W) \in \beta(\bigvee \chi)$. If $a = \perp$ then obviously $(a, W) = (\perp, \{\perp\}) \in \bigvee_{R \in \chi} \beta(R)$. If $a \neq \perp$ then there exists $h \in (\bigvee \chi)(a)$ such that $W = \mathsf{supp}(h)$ and $h \in \mathcal{D}_1(A)$, or $W = \mathsf{supp}(h)^{\perp}$ and $h \notin \mathcal{D}_1(A)$. In the former case, there exists $I \in \wp_f(A)$, $d \in \mathcal{D}_1(I)$, and the mapping $F : I \to (\bigcup \chi)(a)$ such that $h = \sum_{i \in I} d(i) \cdot F(i)$ by the definition of $\bigvee$. For each $i \in \mathsf{supp}(d)$, there exists $R_i \in \chi$ such that $(a, F(i)) \in R_i$. Since $F(i) \in \mathcal{D}_1(A)$ for all $i \in I$, $(a, \mathsf{supp}(F(i))) \in \bigcup_{i \in I} \beta(R_i)$. Therefore

$$(a, W) = (a, \mathsf{supp}(h)) = \Big(a, \ \bigcup\nolimits_{i \in I} \mathsf{supp}(F(i))\Big) \in \bigvee\nolimits_{R \in \chi} \beta(R) \ .$$

In the latter case, the proof is similar to the above, only differs for including $\perp$. □

We obtain the following proposition by Lemma 6.8, 6.9, 6.10.

Proposition 6.4. *β is a homomorphism of complete IL-semirings.*

And we also have a Galois connection by Lemma 6.10

Theorem 6.3. *For a set A, $(\mathsf{pMR}_{0,d,f}(A), \mathsf{bMR}(A), \beta, \gamma)$ is a Galois connection where $\beta : \mathsf{pMR}_{0,d,f}(A) \to \mathsf{bMR}(A)$ is defined by*

$$\begin{array}{rcl}\beta(R) & = & \{(a, \mathsf{supp}(d)^{\perp}) \mid (a,d) \in R \wedge d \notin \mathcal{D}_1(A)\} \\ & & \cup\{(a, \mathsf{supp}(d)) \mid (a,d) \in R \wedge d \in \mathcal{D}_1(A)\} \cup \{(\perp.\{\perp\})\}\end{array}$$

and $\gamma : \mathsf{bMR}(A) \to \mathsf{pMR}_{0,d,f}(A)$ is given as Proposition 6.1.

We have given a Galois connection between $\mathsf{pMR}_{0,d,f}(A)$ and $\mathsf{bMR}(A)$. And then β preserves a counter example of the right distributivity as in the case of α_1.

Example 6.5. *We consider probabilistic multirelations P and Q that appeared in Example 5.2. Then*

$$\begin{array}{l}\beta(P) = 0 \cup \{(a, W) \mid a \in A, W \sqsubseteq_{\mathcal{A}} \{x, y\}\} \text{ and },\\ \beta(Q) = 0 \cup \{(x, W) \mid W \sqsubseteq_{\mathcal{A}} \{y\}\} \cup \{(y, W) \mid W \sqsubseteq_{\mathcal{A}} \{x\}\} \ .\end{array}$$

We already have shown that $(x, \delta_x) \in P \cdot Q + P \cdot 1$ though $(x, \delta_x) \in P \cdot (Q + 1)$ in Example 5.2. Since β is the homomorphism of complete IL-semirings,

$$\begin{array}{l}\beta(P \cdot (Q + 1)) = \beta(P); (\beta(Q) \cup \beta(1)) \text{ and}\\ \beta(P \cdot Q + R \cdot 1) = \beta(P); \beta(Q) \cup \beta(P); \beta(1) \ .\end{array}$$

We have $(x, \{x\}) \in \beta(P); (\beta(Q) \cup \beta(1))$ since $(x, \{x, y\}) \in \beta(P)$, $(x, \{x\}) \in \beta(1)$ and $(x, \{y\}) \in \beta(Q)$. However $(x, \{x\})$ is not in $\beta(P); \beta(Q)$ and $\beta(P); \beta(1)$.

In the previous section we show that $\gamma_1 : \mathsf{UMR}_{t,f}(A) \to \mathsf{pMR}_{0,d,f}(A)$ need not preserve the identity, however γ preserve.

Proposition 6.5. *The mapping $\gamma : \mathsf{bMR}(A) \to \mathsf{pMR}_{0,d,f}(A)$ satisfies $\gamma(1) = 1$.*

Proof. Note that $\gamma(1) = \bigvee\{R \mid \beta(R) \subseteq 1\}$. For proof of $\gamma(1) \subseteq 1$, it is sufficient to prove that $\beta(R) \subseteq 1$ implies $R \subseteq 1$. Assume that $\beta(R) \subseteq 1$ and $(a, d) \in R$. Then we obtain $d \sqsubseteq_{\mathcal{D}} \delta_a$. Therefore $(a, d) \in 1$. Conversely we have $1 \subseteq \gamma(1)$ since $\beta(1) \subseteq 1$ and $\big(\mathsf{pMR}_{0,d,f}(A), \mathsf{bMR}(A), \beta, \gamma\big)$ is a Galois connection. □

$$\mathsf{pMR}_{0,d,f}(A) \underset{\gamma_{\mathsf{supp}}}{\overset{\alpha_{\mathsf{supp}}}{\rightleftarrows}} \mathsf{UMR}_{t,f}(A) \quad (\perp)$$

$$\mathsf{pMR}_{0,d,f}(A) \underset{\gamma_1}{\overset{\alpha_1}{\rightleftarrows}} \mathsf{UMR}_{t,f}(A) \quad (\perp)$$

$$\mathsf{pMR}_{0,d,f}(A) \underset{\gamma}{\overset{\beta}{\rightleftarrows}} \mathsf{bMR}(A) \quad (\perp)$$

Figure 6.1: Three Galois connections between probabilistic multirelations and non-probabilistic multirelations

6.6 Summary

This chapter has studied the relationship between probabilistic multirelations and non-probabilistic multirelations. We proposed three Galois connections (Fig.6.1) between probabilistic systems and non-probabilistic systems, providing join-preserving mappings from probabilistic multirelations to non-probabilistic multirelations. First one using α_{supp} is given on the natural way in the sense of using the support supp. However α_{supp} need not preserve a counter example of the right distributivity though reducing the right distributivity from the definition of complete I-semirings (even of Kleene algebras) is a typical relaxation for applying probabilistic systems. Second one using α_1 seems to be better than first one because α_1 preserves a counter example of the right distributivity. On the other hand, we have given a Galois connection $\big(\mathsf{pMR}_{0,d,f}(\_), \mathsf{bMR}(\_), \beta, \gamma\big)$ between probabilistic multirelations and bottomed multirelations. The mapping β preserves a counter example of the right distributivity and even γ preserves the identity 1. In that sense the last one seems to be better than the others. It is an opened problem whether or not γ preserves the composition ;.

Summary

The aim of this thesis is to provide a path to abstraction between probabilistic systems and non-probabilistic systems in order to put the verification methods for probabilistic systems into practical use. The contribution of this thesis as follows:

1. We studied up-closed multirelations carefully. Then we have shown that classes of up-closed multirelations provide models of three weaker variants of Kleene algebra: the set of up-closed multirelations forms a lazy Kleene algebra [Moe04], the set of finitary up-closed multirelations forms a monodic tree Kleene algebra [TF06], the set of finitary total up-closed multirelations forms a probabilistic Kleene algebra [MCC06, MW05].

2. We refined the above results. We extend the notion of multirelations introducing types of multirelations. We define a cube consisting of eight classes of lazy Kleene algebras, by introducing three axioms. We also define a cube consisting of eight classes of complete IL-semirings. Then we show a correspondence between types of up-closed multirelations and classes of lazy Kleene algebras via classes of complete IL-semirings.

3. We showed an another multirelational model of complete IL-semirings, using bottomed multirelations. Though it is known that this model forms a probabilistic Kleene algebra [MW05, Web08], we have obtained that proof by providing that the set of all $\perp$-included finite, down- and union-closed multirelations forms a complete IL-semiring preserving all directed joins and the right 0.

4. We give a notion of probabilistic multirelations as a generalization of semantic domain of probabilistic distributed systems introduced by McIver et al [MCC06, MW05]. Then we showed that the set of 0-included finitary down- and convex-closed probabilistic multirelations forms a complete IL-semiring preserving all right directed joins and the right zero. And we also showed that the left distributivity need not hold in this complete IL-semiring.

5. We proposed three Galois connections between probabilistic systems and non-probabilistic systems, providing join-preserving mappings from probabilistic multirelations to non-probabilistic multirelations. First one using α_{supp} is given on the natural way in the sense of using the support supp of probabilistic distributions. However α_{supp} need not preserve the counter example of the left distributivity though reducing the left distributivity from the definition of complete I-semirings [Moe04] (even of Kleene algebras) is a typical relaxation for applying probabilistic systems. Second one using α_1 seems to be better than first one because α_1 preserves a counter example of the left distributivity. These two Galois connections use the mappings to total, finitary and up-closed multirelations. But third Galois connection uses the mapping β to $\perp$-included finite down- and union-closed bottomed multirelations. This one seems to be better than the others because β preserves a counter example of the left distributivity and the right adjoint γ of β preserves the identity on bottomed multirelations.

Finally we offer future prospects with respect to our research.

- The paper [Moe04] extends the notion of lazy Kleene algebras to treat both finite and infinite streams, by adding the notion of meets and greatest fixed points. We are also going to extend our cube by adding conditions about meets and greatest fixed points. We showed that if a complete IL-semiring preserves all right directed joins, then it forms a lazy Kleene algebra satisfying the D-axiom. However, the converse direction has not been proved yet. It is future work.

- As we described in 5, we provided Galois connections as a path to abstraction between probabilistic systems and non-probabilistic systems in order to enable the verification method (using probabilistic Kleene algebra) to be put into practical use. To make use of our results, we have to experiment on abstract models consisting of multirelations, and to check whether or not these models are useful against some kinds of verification problems.

- Kleene algebra is known as a sound and complete axiomatization of regular expressions. However, it is still open problems what sound and complete models of three weaker variants of Kleene algebra are. On the other hand, we are interested in "Kleene algebra"-like axiomatization of complicated system like probabilistic transition systems or quantum systems.

Bibliography

[Coh00] Ernie Cohen. Separation and Reduction. In R. Backhouse and J. N. Oliveira, editors, *Mathematics of Program Construction, volume 1837 of LNCS*, pp. 45–59. Springer, 2000.

[Cou00] Patrick Cousot. Abstract interpretation based formal methods and future challenges. In R. Wilhelm, editor, *Informatics - 10 Years Back, 10 Years Ahead, volume 2000 of LNCS*, pp. 138-156. Springer-Verlag, 2001.

[DMS06] Jules Desharnais, Bernhard Möller, and Georg Struth. Kleene algebra with domain. ACM Trans. Comput. Log. 7(4): 798-833 (2006).

[Dij00] R.M.Dijkstra. Computation Calculus – bridging a formalization gap. Science of Computer Programming 37, 3 - 36, 2000.

[FNT09] H. Furusawa, K. Nishizawa and N. Tsumagari. Multirelational Models of Lazy, Monodic Tree, and Probabilistic Kleene Algebras, In *Bulletin of Informatics and Cybernetics*, volume 41, pp. 11–24, Research Association of Statistical Sciences, 2009.

[FTN08] H. Furusawa, N. Tsumagari, and K. Nishizawa. A Non-Probabilistic Relational Model of Probabilistic Kleene Algebras. In Berghammer,R., Möller, B. and Struth, G., eds., *Relations and Kleene Algebra in Computer Science, volume 4988 of LNCS*, pp. 110–122. Springer, 2008.

[Gor03] Valentin Goranko. The Basic Algebra of Game Equivalences. *Studia Logica 75(2)*, pp. 221–238, 2003.

[IEC98] `IEC 61508` : Functional Safety of Electrical / Electronic / Programmable Electronic Safety Related Systems. 1998-2000.

[Koz94] Dexter Kozen. A Completeness Theorem for Kleene Algebras and the Algebra of Regular Events. *Information and Computation, 110*, pp. 366–390, 1994.

[Koz97] Dexter Kozen. Kleene Algebra with Tests. ACM Trans. Program. Lang. Syst. 19(3): 427-443 (1997).

[MCR04] C. Martin, S. Curtis, and I. Rewitzky. Modelling Nondeterminism. In Dexter Kozen, editor, *Mathematics of Program Construction, volume 3125 of LNCS*, pp. 228–251. Springer, 2004.

[MCC06] Annabelle McIver, Ernie Cohen, and Carroll Morgan. Using Probabilistic Kleene Algebra for Protocol Verification. In R.A. Schmidt, editor, *Relations and Kleene Algebra in Computer Science, volume 4136 of LNCS*, pp. 296–310. Springer, 2006.

[MM05] Annabelle McIver and Carroll Morgan. *Abstraction, Refinement and Proof for Probabilistic Systems*. Springer, 2005.

[MW05] Annabelle McIver and Tjark Weber. Towards Automated Proof Support for Probabilistic Distributed Systems. In G. Sutcliffe and A. Voronkov, editors, *Proceedings of Logic for Programming, Artificial Intelligence, and Reasoning, volume 3835 of LNAI*, pp. 534–548. Springer, 2005.

[Moe04] Bernhard Möller. Lazy Kleene Algebra. In Dexter Kozen, editor, *Mathematics of Program Construction, volume 3125 of LNCS*. Springer, 2004.

[Mor] The project "Specification and Development of Probabilistic Systems", produced by C. Morgan, et al.
`http://www.cse.unsw.edu.au/~carrollm/probs/index.html`

[NTF09] K. Nishizawa, N. Tsumagari and H. Furusawa: The cube of Kleene algebras and the triangular prism of multirelations. In Berghammer, R., Jaoua, A., Möller, B., eds., *Relations and Kleene Algebra in Computer Science.* LNCS, vol. 5827, pp. 276–290, Springer, 2009.

[Par85] Rohit Parikh. The Logic of Games. *Annals of Discrete Mathematics 24*, pp. 111–140, 1985.

[PP03] M. Pauly and R. Parikh. Game Logic - An Overview. *Studia Logica 75(2)*, pp. 165–182, 2003.

[PMC] Model checker `PRISM` `http://www.prismmodelchecker.org/`

[Rab82] M. Rabin. N-Process Mutual Exclusion with Bounded Waiting by 4 log2 N- Valued Shared Variable. JCSS 25(1): 66-75. 1982.

[Rew03] Ingrid Rewitzky. Binary Multirelations. In H. de Swart, E. Orlowska, G. Schmidt, and M. Roubens, editors, *Theory and Applications of Relational Structures as Knowledge Instruments, volume 2929 of LNCS*, pp. 256–271. Springer, 2003.

[RB06] I. Rewitzky and C. Brink. Monotone Predicate Transformers as Up-Closed Multirelations. In R.A. Schmidt, editor, *Relations and Kleene Algebra in Computer Science, volume 4136 of LNCS*, pp. 311–327. Springer, 2006.

[TF06] T. Takai and H. Furusawa. Monodic Tree Kleene Algebra. *Relations and Kleene Algebra in Computer Science, volume 4136 of LNCS*, pp. 402–416, 2006.

[TF08] T. Takai and H. Furusawa. List of Errors of [TF06] available at `http://www.sci.kagoshima-u.ac.jp/~furusawa/person/Papers/correct_monodic_kleene_algebra.pdf` (2008).

[TNF08a] N. Tsumagari, K. Nishizawa, and H. Furusawa. Multirelational Model of Lazy Kleene Algebra. In Berghammer, R., Möller, B., and Struth, G., eds., Relations and Kleene Algebra in Computer Science. PhD Programme at RelMiCS10/AKA5, Frauenworth, Germany, April 7 - April 11 2008, Proceedings, Technical Report, Institut für Informatik, Universität Augsburg, Germany. 2008.

[TNF08b] N. Tsumagari, K. Nishizawa, and H. Furusawa. On Reflexive Transitive Closure of Binary Multirelations. In Participants' Proceedings of Hinokuni Jouhou Symposium. Information Processing Society of Japan, Kyushu Chapter, 2008 (in Japanese).

[TNF09] N. Tsumagari, K. Nishizawa, and H. Furusawa. Construction of Transitive Closure of Binary Multirelations. In *Reports of the Faculty of Science, Kagoshima University*, Vol.42 pp. 1–9, 2009 (in Japanese).

[Ven03] Yde Venema. Representation of Game Algebras. *Studia Logica 75(2)*, pp. 239–256, 2003.

[Web08] Tjark Weber: SAT-based Finite Model Generation for Higher-Order Logic, Ph.D. thesis: Institut für Informatik, Technische Universität München, Germany, 2008.

[Wri02] J. von Wright. From Kleene algebra to refinement algebra. In E. Boiten and B. Möller, editors, *Mathematics of Program Construction, volume 2386 of LNCS*, pp. 233–262. Springer, 2002.

[Wri04] J. von Wright. Towards a Refinement Algebra. Science of Computer Programming 51, pp. 23–45. 2004.