PROBABILISTIC RELATIONAL MODELS OF COMPLETE IL-SEMIRINGS

Tsumagari, Norihiro
Research Institute for Mathematical Science, Kyoto University

https://doi.org/10.5109/1495413

出版情報：Bulletin of informatics and cybernetics. 44, pp.87-109, 2012-12. Research Association of Statistical Sciences

PROBABILISTIC RELATIONAL MODELS OF COMPLETE IL-SEMIRINGS

by

Norihiro Tsumagari

Reprinted from the Bulletin of Informatics and Cybernetics Research Association of Statistical Sciences, Vol.44

FUKUOKA, JAPAN
2012

Bulletin of Informatics and Cybernetics, Vol. 44, 2012

PROBABILISTIC RELATIONAL MODELS OF COMPLETE IL-SEMIRINGS

By

Norihiro Tsumagari*

Abstract

This paper studies basic properties of probabilistic multirelations which are generalized the semantic domain of probabilistic systems and then provides two probabilistic models of complete IL-semirings using probabilistic multirelations. Also it is shown that these models need not be models of complete idempotent semirings.

Key Words and Phrases: Semantic domain, Probabilistic systems, Probabilistic multirelations, Complete idempotent left semirings

1. Introduction

In this paper we generalize semantic domain of probabilistic distributed systems. McIver and Weber (2005) 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 and Cauchy-closed. Using probabilistic Kleene algebras, Cohen's separation theorems (cf. Cohen (2000)) are generalised for probabilistic distributed systems and the general separation results are applied to Rabin's solution (cf. Rabin (1982)) to distributed mutual exclusion with bounded waiting (cf. McIver, Cohen, and Morgan (2006)). 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. For that purpose, it is necessary to clarify the algebraic properties of semantic domain of probabilistic systems.

Complete idempotent left semiring (IL-semiring) is introduced by Möller (2004) as a relaxation of complete idempotent semiring (or quantale) related Kleene algebra deeply. In fact, it has already known that every complete idempotent semiring forms a Kleene algebra. Though the relational models of complete IL-semirings are studied by Nishizawa, Tsumagari and Furusawa (2009) using up-closed multirelation which is an extention of binary relations, the probabilistic models of this algebraic structure have

* Research Institute for Mathematical Science, Kyoto University. ntsuma@kurims.kyoto-u.ac.jp

never been discussed. This paper would be the first one to introduce probabilistic models of complete IL-semirings.

By the way, probabilistic programs introduced by McIver et al — in the form of subsets of $(A \cup \{\top\}) \times \mathcal{D}_1(A \cup \{\top\})$ — could be translated to subsets of $A \times \mathcal{D}(A)$ where $\mathcal{D}(A)$ is the set of all probabilistic *sub*-distributions. Using this simple form, we introduce a notion of probabilistic multirelations and study basic properties of them. And then we show that the set of all finitary $\underline{0}$-included down-closed and convex probabilistic multirelations forms a complete IL-semiring preserving all right directed join and the right 0. Additionally we also show that the set of all total $\mathcal{D}_1$-convex probabilistic multirelations forms a complete IL-semiring preserving the right 0.

This paper is organized as follows. Section 2. reminds us the definition of complete idempotent left semiring and shows well-known relational models of it. Section 3. provides basic notions for probabilistic distributions which will appear in this paper. In section 4. we introduce the definition and basic properties of probabilistic multirelation. Section 5. provides a probabilistic model of complete IL-semirings, using finitary $\underline{0}$-included down-closed and convex probabilistic multirelations. Finally we introduce another notion of probabilstic multirelations with the different restrictions and provide another probabilistic model of complete IL-semirings, using total $\mathcal{D}_1$-convex probabilistic multirelations in section 6. and 7..

2. Complete Idempotent Left Semiring

We recall the definition of *idempotent left semirings* introduced by Möller (2004).

Definition 2.1. Let $(K, 0, 1, +, \cdot)$ be a tuple of a set K, two elements 0 and 1 of K, and two binary operations $+$ and $\cdot$ on K. An *idempotent left semiring (IL-semiring)* is a tuple $(K, 0, 1, +, \cdot)$, satisfying the following properties:

1. $(K, +, 0)$ is an idempotent commutative monoid, that is

$$\begin{aligned} 0 + a &= a & (1)\\ a + b &= b + a & (2)\\ a + a &= a & (3)\\ a + (b + c) &= (a + b) + c & (4) \end{aligned}$$

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

$$\begin{aligned} a(bc) &= (ab)c & (5)\\ 1a &= a & (6)\\ a1 &= a & (7) \end{aligned}$$

3. The left semi-distributive laws:

$$\begin{aligned} ab + ac &\leq a(b + c) & (8)\\ ac + bc &= (a + b)c & (9)\\ 0a &= 0 & (10) \end{aligned}$$

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

An IL-semiring $(K, 0, 1, +, \cdot)$ is called complete if it has joins (the least upper bounds).

Definition 2.2. A *complete IL-semiring* is a tuple $(K, 0, 1, +, \cdot, \bigvee)$ with the following properties:

1. $(K, 0, 1, +, \cdot)$ 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. A typical example of complete IL-semirings is given by multirelations. A *multirelation* over a set A is a subset of $A \times \wp(A)$ where $\wp(A)$ is the powerset of A. A multirelation R is called *up-closed* if $(a, X) \in R \wedge X \subseteq Y \implies (a, Y) \in R$.

Example 2.3. For a set A the set K of all up-closed multirelations over A forms a complete IL-semiring $(K, 0, 1, +, \cdot, \bigvee)$ where

- $R + Q$ 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 $\forall y \in Y.(y, X) \in Q$,
- $1 = \{(a, X) \mid a \in X, X \subseteq A\}$, and
- $\bigvee$ is the union operator.

This example is given by Nishizawa, Tsumagari and Furusawa (2009).

Complete IL-semirings are relaxations of complete I-semirings (or quantales). In fact, a complete IL-semiring could be called a complete I-semiring, satisfying some additional restrictions.

Definition 2.4. 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 2.5. A complete IL-semiring $(K, 0, 1, +, \cdot, \bigvee)$ preserves

- 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 $a \cdot \bigvee S = \bigvee\{a \cdot x \mid x \in S\}$ for each $a \in K$ and each directed $S \subseteq K$,

respectively.

A tuple $(K, 0, 1, +, \cdot, \bigvee)$ is a complete I-semiring (or a quantale) if and only if it is a complete IL-semiring preserving the right 0, the right $+$, and all right directed joins. This fact has shown by Nishizawa, Tsumagari and Furusawa (2009).

Example 2.6. For a set A the set K of all binary relations over A forms a complete IL-semiring $(K, 0, 1, +, \cdot, \bigvee)$ where

- $R + Q$ 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.

Actually this tuple is a complete I-semiring.

3. Probabilistic Distribution

For a set A we denote $\wp_f(A)$ for the set of all finite subsets of A. A *probabilistic sub-distribution* over a set A is a mapping d from a set A to the interval $[0, 1]$ such that $\sum_{a \in A} d(a) \leq 1$ where $\sum_{a \in A} d(a) := \mathsf{sup}\{\sum_{a \in S} d(a) \mid S \in \wp_f(A)\}$. 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 convenience, we often call a sub-distribution simply a distribution.

Also we denote $\mathsf{spt}(d)$ for the *support* of $d \in \mathcal{D}(A)$ defined by

$$\mathsf{spt}(d) := \{a \in A \mid d(a) > 0\}$$

If $\mathsf{spt}(d)$ is finite, d is called *finitary*. And $\mathcal{D}_f(A)$ denotes the set of all finitary probabilistic distributions over A.

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 $\underline{0}$ for the *point distribution at $x \in A$* and the *zero distribution* respectively, defined by

$$\delta_x(a) := \begin{cases} 1 & (a = x) \\ 0 & (a \neq x) \end{cases}, \quad \underline{0}(a) := 0, \quad \text{for each } a \in A \ .$$

Let p be a real number in $[0, 1]$, and d a distribution. Then 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

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

4. Probabilistic Multirelation

The binary multirelations are studied by Rewitzky (2003) and Brink (2006) as a semantic domain of programs. An multirelation over a set A is defined as a subset of $A \times \wp(A)$ but now we define the probabilistic multirelation using $\mathcal{D}$ instead of $\wp$.

DEFINITION 4.1. A *probabilistic multirelation* over a set A is a subset of $A \times \mathcal{D}(A)$.

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

Next we introduce a fundamental restriction for probabilistic multirelations.

DEFINITION 4.2. A probabilistic multirelation R over a set A is *convex* if

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

for each $a \in A$, $d, d' \in \mathcal{D}(A)$ and $p \in [0, 1]$.

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

Next, we introduce three restrictions — *finitary, $\underline{0}$-included and down-closed* — for probabilistic multirelations, and then we provide a probabilistic model of complete IL-semirings. This model is laxer than the model for probabilistic systems given by McIver and Weber (2005), without *Cauchy-closed*.

DEFINITION 4.3. A probabilistic multirelation $R \in \mathsf{pMR}(A)$ is called

- *finitary* if $R[a] \subseteq \mathcal{D}_f(A)$ for each $a \in A$,
- *$\underline{0}$-included* if $(a, \underline{0}) \in R$ for each $a \in A$, and
- *down-closed* if $(a, d) \in R \wedge d' \sqsubseteq_{\mathcal{D}} d$ implies $(a, d') \in R$ for each $a \in A$, $d, d' \in \mathcal{D}(A)$.

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

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

LEMMA 4.4. *For each subset χ of $\mathsf{pMR}_{0,d,f}(A)$, the union $\bigcup \chi$ is finitary, $\underline{0}$-included and down-closed.*

PROOF. Let χ be a subset of $\mathsf{pMR}_{0,d,f}(A)$. Obviously $\bigcup \chi$ is finitary and $\underline{0}$-included. 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 for each $P, Q \in \mathsf{pMR}_{0,d,f}(A)$.

EXAMPLE 4.5. Let A be a set $\{x, y\}$ and $P, Q \subseteq A \times \mathcal{D}(A)$ as follows:

$$P = \{(a, d) \mid a \in A,\ d \sqsubseteq_{\mathcal{D}} \delta_x\} \ ,$$
$$Q = \{(a, d) \mid a \in A,\ d \sqsubseteq_{\mathcal{D}} \delta_y\} \ .$$

P and Q are finitary, $\underline{0}$-included, down-closed and convex, that is $P, Q \in \mathsf{pMR}_{0,d,f}(A)$. 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.

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

DEFINITION 4.6. For a probabilistic multirelation $R \in \mathsf{pMR}(A)$, the *convex hull* $H_c(R)$ of R is defined by

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

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

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

We obtain the followings immediately.

LEMMA 4.7. *If $R \in \mathsf{pMR}(A)$ is finitary (resp. $\underline{0}$-included), then $H_c(R)$ is finitary (resp. $\underline{0}$-included).*

LEMMA 4.8. *If $R \in \mathsf{pMR}(A)$ 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 a finite set I, $d \in \mathcal{D}_1(I)$, 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 $h' = \sum_{i \in I} d(i) \cdot F'(i) \in H_c(R)$. □

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

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

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

LEMMA 4.9. *The operator + is associative, that is*

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

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

PROOF. It 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 convex 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 4.10. $(\mathsf{pMR}_{0,d,f}(A), +, \mathit{0})$ *is an idempotent commutative monoid.*

For $X \in \wp(A)$, a mapping $F : X \to \mathcal{D}(A)$ and $Q \in \mathsf{pMR}(A)$, $F \sqsubseteq Q$ denotes that $(u, F(u)) \in Q$ for each $u \in X$.

For $P, Q \in \mathsf{pMR}_{0,d,f}(A)$, the composition $P \cdot Q$ of P and Q is defined by

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

LEMMA 4.11. $\mathsf{pMR}_{0,d,f}(A)$ *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 $\underline{0}$-included. We have $(a, \underline{0}) \in P$ for each $a \in A$. Let $F : A \to \mathcal{D}(A)$ be a mapping such that $F(u) = \underline{0}$ for each $u \in A$. Then $F \sqsubseteq Q$ holds. Therefore

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

We prove that $P \cdot Q$ is finitary. If $(a, h) \in P \cdot Q$ then there exists $d \in P[a]$ and $F : \mathsf{spt}(d) \to \mathcal{D}(A)$ satisfying $F \sqsubseteq Q$ and $h = \sum_{u\in A} d(u)\cdot F(u)$. Then

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

Since $\mathsf{spt}(d)$ and $\mathsf{spt}(F(u))$ are finites sets, then $\mathsf{spt}(h)$ 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

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

Since $d' \sqsubseteq_{\mathcal{D}} d$, $F'(u) \sqsubseteq_{\mathcal{D}} F(u)$ holds for each $u \in A$. So we obtain that $F' \sqsubseteq Q$ 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. Suppose that $h, h' \in (P;Q)[a]$. Then there exists $d, d' \in P[a]$, $F : A \to \mathcal{D}(A)$, and $F' : A \to \mathcal{D}(A)$ such that $h = \sum_{u \in A} d(u) \cdot F(u)$ and $h' = \sum_{u \in A} d'(u) \cdot F'(u)$. Then for each $s \in A$ and $p \in [0,1]$, we obtain that

$$\begin{aligned}(h \ {}_p\!\oplus h')(s) &= p \cdot \sum_{u \in A} d(u) \cdot F(u)(s) + (1-p) \cdot \sum_{u \in A} d'(u) \cdot F'(u)(s) \\ &= \sum_{u \in A} (p \cdot d(u) \cdot F(u)(s) + (1-p) \cdot d'(u) \cdot F'(u)(s)) \ .\end{aligned}$$

For $u \in A$, let F'' be a mapping from A to $\mathcal{D}(A)$ such that

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

where $q(u) = \dfrac{p \cdot d(u)}{p \cdot d(u) + (1-p) \cdot d'(u)}$. We have $F'' \sqsubseteq Q$ since Q is convex. Then

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

holds. And we have $d \ {}_p\!\oplus d' \in P[a]$ since P is convex. Therefore $P \cdot Q$ is convex. □

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

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

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

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 $F : A \to \mathcal{D}(A)$ satisfying $\forall u \in A.\ (u, F(u)) \in R$ and

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

holds. Also there exists $d' \in P[a]$ and $F' : A \to \mathcal{D}(A)$ such that $F' \sqsubseteq Q$ and

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

holds. Then we have

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

where $F'' : A \to \mathcal{D}(A)$ is defined by

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

Since $F'' \sqsubseteq Q\cdot R$, 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 $F : A \to \mathcal{D}(A)$ 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 $G_u : A \to \mathcal{D}(A)$ satisfying $G_u \sqsubseteq R$ and

$$F(u) = \sum_{t\in A} e_u(t)\cdot G_u(t) \ .$$

Since R is $\underline{0}$-included, $\underline{0} \in R[t]$ for each $t \in A$. For $u \in A$ let $G'_u : A \to \mathcal{D}(A)$ be as follows:

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

Obviously $G'_u \sqsubseteq R$. We have

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

Let $G : A \to \mathcal{D}(A)$ be a mapping satisfying

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

Then we have $G(t) \in R[t]$ for each $t \in A$, since $\mathsf{spt}(d)$ is finite, R is convex and

$$\sum_{u\in \mathsf{spt}(d)} \frac{d(u)\cdot e_u(t)}{\sum_{u\in \mathsf{spt}(d)} d(u)\cdot e_u(t)} = 1 \quad .$$

Let $d' \in \mathcal{D}(A)$ as follows.

$$d'(t) := \sum_{u\in A} d(u)\cdot e_u(t) \quad .$$

Then it holds that $d' \in (P\cdot Q)[a]$. Therefore

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

□

PROPOSITION 4.13. *Let $R \in \mathsf{pMR}_{0,d,f}(A)$. $0\cdot R = 0$ and $R\cdot 0 = 0$*

PROOF. We have $0 \subseteq 0\cdot R$ and $0 \subseteq R\cdot 0$ because it already has been proved that $0\cdot R$ and $R\cdot 0$ are $\underline{0}$-included in the lemma 4.11.

If $(a,h) \in 0\cdot R$, then there exists $d \in 0[a]$ and $F : \mathsf{spt}(d) \to \mathcal{D}(A)$ such that $F \sqsubseteq R$ and $h = \sum_{u\in A} d(u)\cdot F(u)$. Since $d = \underline{0}$ by the definition of 0, we have $h = \sum_{u\in A}\underline{0}(u)\cdot F(u) = \underline{0}$. Therefore $(a,h) = (a,\underline{0}) \in 0$.

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 $F : \mathsf{spt}(d) \to \mathcal{D}(A)$ such that $F \sqsubseteq 0$ and $h = \sum_{u \in A} d(u) \cdot F(u)$. Therefore $h = \sum_{u \in A} d(u) \cdot \underline{0} = \underline{0} \in \mathit{0}[a]$. □

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 4.14. *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 $h = \sum_{u \in A} d(u) \cdot F(u)$ and $F \sqsubseteq R$. Since the definition of $\mathit{1}$, we have

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

Then $(a, F(a)) \in R$ 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 $F : A \to \mathcal{D}(A)$ such that

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

then we have

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

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 $F : A \to \mathcal{D}(A)$ 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 $F(u) \sqsubseteq_{\mathcal{D}} \delta_u$ for each $u \in A$ and

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

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

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

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

□

Lemma 4.12 and 4.14 show the following property.

PROPOSITION 4.15. *A tuple* $(\mathsf{pMR}_{0,d,f}(A), \ \cdot, \ \mathit{1})$ *is a monoid.*

Next, we consider the left distributivity.

PROPOSITION 4.16. *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 $F: A\to\mathcal{D}(A)$ such that $h=\sum_{u\in A} d(u)\cdot F(u)$ 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

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

Therefore $(a,h)\in\bigvee_{Q\in\chi} Q\cdot R$ since

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

for each $i\in I$. □

Also we have $(P+Q)\cdot R = P\cdot R + Q\cdot R$ for $P,Q,R\in\mathsf{pMR}_{0,d,f}(A)$. Therefore, we obtain the following property by Proposition 4.10, 4.13, 4.15 and 4.16.

PROPOSITION 4.17. *A tuple* $(\mathsf{pMR}_{0,d,f}(A), 0, 1, +, \cdot)$ *is an idempotent left semiring.*

5. First Probabilistic Model of Complete IL-semiring

We have already shown that a tuple $(\mathsf{pMR}_{0,d,f}(A), 0, 1, +, \cdot, \bigvee)$ is a complete IL-semiring preserving the right 0 by Proposition 4.13, 4.16 and 4.17. Additionally, it also preserves all right directed joins.

LEMMA 5.1. *If* $\chi\subseteq\mathsf{pMR}_{0,d,f}(A)$ *is directed* $\bigcup_{Q\in\chi} Q$ *is convex.*

PROOF. Assume that $\chi\subseteq\mathsf{pMR}_{0,d,f}(A)$ is directed, and $p\in[0,1]$. 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 $P\subseteq R$ and $P'\subseteq R$. Therefore $(a, d\ {}_p\!\oplus d')\in R\subseteq\bigcup_{Q\in\chi} Q$ since $d,d'\in R[a]$ and R is convex. □

By Proposition 4.4 and Lemma 5.1, $\bigcup_{Q\in\chi}Q$ is $\underline{0}$-included finitary down-closed and convex. This fact indicates that the directed join $\bigvee\chi$ of $\chi \subseteq \mathsf{pMR}_{0,d,f}(A)$ is given by the union of all probabilistic multirelations in χ, that is,

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

Proposition 5.2. *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 $(a,h)\in R\cdot(\bigvee\chi)$.Then there exists $d\in R[a]$, $F\sqsubseteq\bigvee\chi$ such that $h=\sum_{u\in A}d(u)\cdot F(u)$ Since χ is directed,

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

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

$$h=\sum_{u\in A}d(u)\cdot F(u) = \sum_{u\in\mathsf{spt}(d)} d(u)\cdot F(u)\in(R\cdot P)[a]\subseteq\bigcup_{Q\in\chi}(R\cdot Q)[a] \ .$$

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

The following theorem summarises this discussion.

Theorem 5.3. *A tuple $(\mathsf{pMR}_{0,d,f}(A), 0, 1, +, \cdot, \bigvee)$ is a complete IL-semiring preserving all right directed joins and the right* 0.

Using previous results given by Nishizawa, Tsumagari and Furusawa (2009), we also obtain the following lemma from the above theorem.

Lemma 5.4. $\mathsf{pMR}_{0,d,f}(A)$ *forms a lazy Kleene algebra satisfying the 0-axiom and the D-axiom, or a probabilistic Kleene algebra.*

The following example shows that

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

need not hold on $\mathsf{pMR}_{0,d,f}(A)$.

EXAMPLE 5.5. Let A be a set $\{x,y\}$, and $P, Q \in \mathsf{pMR}_{0,d,f}(A)$ be as follows.

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

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

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

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 $(x, \delta_x) \notin P = P \cdot Q + P \cdot \mathit{1}$.

6. Another Probabilistic Multirelation

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 from this section. $\mathsf{pMR}_1(A)$ denotes the set of all probabilistic multirelations in the form of subsets of $A \times \mathcal{D}_1(A)$, that is

$$\mathsf{pMR}_1(A) = \{R \in \mathsf{pMR}(A) \mid \forall a \in A.\ R[a] \subseteq \mathcal{D}_1(A)\}\ .$$

The partial order on $\mathsf{pMR}_1(A)$ is the inclusion relation $\subseteq$.

DEFINITION 6.1. $R \in \mathsf{pMR}_1(A)$ is called

- *total* if
$$R \neq \emptyset \implies \forall a \in A.\ R[a] \neq \emptyset\ .$$
- $\mathcal{D}_1$-*convex* if
$$\sum_{i \in I} d(i) \cdot F(i) \in R[a]$$
for each $a \in A$ where I is a finite set, $d \in \mathcal{D}_1(I)$ and $F : I \to R[a]$.

We denote $\mathsf{pMR}_{t,1}(A)$ for the set of all total $\mathcal{D}_1$-convex 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 for each $P, Q \in \mathsf{pMR}_{t,1}(A)$.

EXAMPLE 6.2. Let A be a set $\{x,y\}$ and $P, Q \subseteq A \times \mathcal{D}_1(A)$ be as follows:

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

Then P and Q are total and $\mathcal{D}_1$-convex. Obviously we have $(P \cup Q)[x] = \{\delta_x, \delta_y\}$. Let $\mathbf{2}$ be $\{0, 1\}$. Assume that $d \in \mathcal{D}_1(\mathbf{2})$ satisfies $d(0) = d(1) = \frac{1}{2}$ and $F : \mathbf{2} \to (P \cup Q)[x]$ satisfies $F(0) = \delta_x, F(1) = \delta_y$, then

$$\sum_{i \in 2} d(i) \cdot F(i) = d(0) \cdot F(0) + d(1) \cdot F(1) = \frac{1}{2} \cdot \delta_x + \frac{1}{2} \cdot \delta_y = \delta_x \;{}_{\frac{1}{2}}\!\oplus \delta_y$$

Therefore $P \cup Q$ is not $\mathcal{D}_1$-convex since $\delta_x \;{}_{\frac{1}{2}}\!\oplus \delta_y \notin (P \cup Q)[x]$.

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

Definition 6.3. For a total $\mathcal{D}_1$-convex probabilistic multirelation $R \in \mathsf{pMR}_1(A)$, the $\mathcal{D}_1$-convex hull $H_1(R)$ of R is defined by

$$\left\{ (a, \sum_{i \in I} d(i) \cdot F(i)) \mid I : \text{finite set},\ d \in \mathcal{D}_1(I),\ F : I \to R[a] \right\}.$$

$H_1(R)$ is the smallest $\mathcal{D}_1$-convex set containing $R \in \mathsf{pMR}_1(A)$.

Remark. H_1 is a closure operator on $\mathsf{pMR}_1(A)$.

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

$$\bigvee \chi := H_1 \left(\bigcup \chi \right)$$

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 $\emptyset$. Obviously it holds that $\emptyset \subseteq P$, $P = \emptyset + P$, $P + Q = Q + P$, and $P + P = P$ for $P, Q \in \mathsf{pMR}_{t,1}(A)$.

Lemma 6.4. *The operator $+$ is associative, that is*

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

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

Proof. It 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 $\mathcal{D}_1$-convex set containing $P + Q$ and R. We have $(P + Q) + R = H_1((P + Q) \cup R) \subseteq P + (Q + R)$ by the definition of H_1. $\square$

Therefore the following property holds.

Proposition 6.5. $(\mathsf{pMR}_{t,1}(A), +, \emptyset)$ is an idempotent commutative monoid.

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

$$\left\{ \left(a,\ \sum_{u \in A} d(u) \cdot F(u) \right) \mid d \in P[a],\ F : A \to \mathcal{D}_1(A) \text{ s.t. } F \sqsubseteq Q \right\} .$$

LEMMA 6.6. $\mathsf{pMR}_{t,1}(A)$ *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 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 total, there exists $d \in P[a]$ for each $a \in A$. 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 total. It holds that

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

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

Finally, we prove that $P \cdot Q$ is $\mathcal{D}_1$ convex. Let I be a finite set, $d \in \mathcal{D}_1(I)$ and $F : I \to (P \cdot Q)[a]$. We show that

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

By the assumption, for each $i \in I$ 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

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

where

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

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

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

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

Then 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 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 is $\mathcal{D}_1$-convex, 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 6.8. *Let* $R \in \mathsf{pMR}_{t,1}(A)$. $\emptyset\cdot R = \emptyset$

PROOF. By the definition of $\emptyset$, $\emptyset \subseteq \emptyset\cdot R$ holds obviously. Conversely, we show that $\emptyset\cdot R = \emptyset$. Assume $(a,h)\in\emptyset\cdot R$. Then there exists $d\in\emptyset[a]$. However it contradicts the fact that $\emptyset[a]=\emptyset$. □

LEMMA 6.9. *Let* $R \in \mathsf{pMR}_{t,1}(A)$. $R\cdot\emptyset = \emptyset$

PROOF. It holds that $\emptyset \subseteq R\cdot\emptyset$ obviously. Conversely, we show that $R\cdot\emptyset = \emptyset$. If $(a,h)\in R\cdot\emptyset$, then there exists $d\in R[a]$ and $F : A\to\mathcal{D}_1(A)$ such that $F\sqsubseteq\emptyset$ and $h=\sum_{u\in A} d(u)\cdot F(u)$. However there is no such mapping F. □

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

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

LEMMA 6.10. The identity satisfies the unit law, that is

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

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

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 $F : A \to \mathcal{D}_1(A)$ such that $F \sqsubseteq R$ and $h = \sum_{u \in A} d(u) \cdot F(u)$. By the definition of the identity, we have

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

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 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 6.7 and 6.10 show the following property.

Proposition 6.11. *A tuple* $(\mathsf{pMR}_{t,1}(A),\ \cdot,\ \mathit{1})$ *is a monoid.*

Next, we consider the left distributivity.

Proposition 6.12. *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 $R=\emptyset$, then $(\bigvee\chi)\cdot\emptyset=\emptyset\subseteq\bigvee_{Q\in\chi}Q\cdot R$. Suppose that $R\neq 0$. Then there exists $d\in(\bigvee\chi)[a]$ and $F:A\to\mathcal{D}(A)$ such that $F\sqsubseteq R$ and $h=\sum_{u\in A}d(u)\cdot F(u)$. In addition, there exists $d'\in\mathcal{D}_1(A)$, and $F':A\to(\bigcup\chi)\,[a]$ such that

$$d=\sum_{i\in A}d'(i)\cdot F'(i)\ .$$

So we have

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

Let G be a mapping from A to $\left(\bigcup_{Q\in\chi}Q\cdot R\right)[a]$ such that

$$G(i):=\sum_{u\in A}F'(i)(u)\cdot F(u)\ .$$

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

From the above we obtain $(P+Q)\cdot R=P\cdot R+Q\cdot R$ for $P,Q,R\in\mathsf{pMR}_{t,1}(A)$. Therefore, we obtain the following property by Proposition 6.11.

PROPOSITION 6.13. *A tuple* $(\mathsf{pMR}_{t,1}(A),\emptyset,1,+,\cdot)$ *is an idempotent left semiring.*

7. Second Probabilistic Model of Complete IL-semiring

We have already shown that a tuple $(\mathsf{pMR}_{t,1}(A),\emptyset,1,+,\cdot,\bigvee)$ is a complete IL-semiring by Proposition 6.12 and 6.13. In addition, we have the following theorem by Lemma 6.9.

THEOREM 7.1. *A tuple* $(\mathsf{pMR}_{t,1}(A),\emptyset,1,+,\cdot,\bigvee)$ *is a complete IL-semiring preserving the right* 0.

Using previous results given by Nishizawa, Tsumagari and Furusawa (2009), we also obtain the following lemma from the above theorem.

LEMMA 7.2. $\mathsf{pMR}_{t,1}(A)$ *forms a lazy Kleene algebra satisfying the 0-axiom.*

The following example shows that complete IL-semiring $\mathsf{pMR}_{t,1}(A)$ need not preserve the right $+$, that is

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

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

EXAMPLE 7.3. Let A be a set $\{x, y\}$, and P, Q probabilistic multirelations such that

$$\begin{aligned} P &= \left\{(a,\ \delta_x\ {}_{\frac{1}{2}}\!\oplus \delta_y) \mid a \in A\right\} \\ Q &= \{(x, \delta_y), (y, \delta_x)\} \ . \end{aligned}$$

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

We have $(x, \delta_x) \in P \cdot (Q + 1)$ since

$$\delta_x = \sum_{u \in A} (\delta_x\ {}_{\frac{1}{2}}\!\oplus \delta_y)(u) \cdot \delta_x$$

and $\delta_x \in (Q + 1)[u]$ 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 $(x, \delta_x) \notin P = P \cdot Q + P \cdot 1$.

In addition, complete IL-semiring $\mathsf{pMR}_{t,1}(A)$ need not preserve all right directed join, that is,

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

need not hold for $P, Q \in \mathsf{pMR}_{t,1}(A)$ and directed subset $\chi \subseteq \mathsf{pMR}_{t,1}(A)$.

EXAMPLE 7.4. Let $\mathbb{N}$ be a set of all natural numbers, and P a probabilistic multirelation

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

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

$$Q_i = \{(a,\ \delta_0\ {}_p\!\oplus \delta_1) \mid a \le i,\ p \in [0, 1]\} \cup \{(a,\ \delta_1) \mid i < a\} \ .$$

Then it holds 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.

Note that $(i, \delta_0) \in Q_i$ for each $i \in \mathbb{N}$. Let $F : \mathbb{N} \to \mathcal{D}_1(\mathbb{N})$ be a function such that $F(i) = \delta_0$ for each $i \in \mathbb{N}$. Then $\delta_0 = \sum_{i \in \mathbb{N}} d(i) \cdot F(i)$. Since $d \in P[0]$ and $F \sqsubseteq \bigvee_{i \in \mathbb{N}} Q_i$, we have

$$(0, \delta_0) \in P \cdot \left(\bigvee_{i \in \mathbb{N}} Q_i\right) \ .$$

Now we prove that $(0, \delta_0) \notin \bigvee_{i \in \mathbb{N}} P \cdot Q_i$. It is sufficient to show that

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

If $(0, h) \in \bigvee_{i \in \mathbb{N}} P \cdot Q_i$, then there exists a finite set J, $e \in \mathcal{D}_1(J)$ and a mapping $F : J \to \left(\bigcup_{i \in \mathbb{N}} P \cdot Q_i\right)[0]$ such that

$$h = \sum_{j \in J} e(j) \cdot F(j) \ .$$

We consider $F(j) \in \left(\bigcup_{i\in\mathbb{N}} P \cdot Q_i\right)[0]$. For $j \in J$, there exists $k_j \in \mathbb{N}$ satisfying $F(j) \in P \cdot Q_{k_j}[0]$. Then there exists $d_j \in P[0]$ and $G_j : \mathbb{N} \to \mathcal{D}_1(\mathbb{N})$ such that

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

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

$$\begin{aligned} F(j) &= \sum_{u\in\mathbb{N}} d_j(u) \cdot G_j(u) \\ &= \sum_{u\in\mathbb{N}} d(u) \cdot G_j(u) \\ &= \sum_{u\le k_j} d(u) \cdot G_j(u) + \sum_{u>k_j} d(u) \cdot G_j(u) \\ &= \sum_{u\le k_j} d(u) \cdot (\delta_0 \ {}_{p_u^j}\!\oplus \delta_1) + \sum_{u>k_j} d(u) \cdot \delta_1 \ . \end{aligned}$$

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

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

Therefore $(0, \delta_0) \notin \bigvee_{i\in\mathbb{N}} P \cdot Q_i$ though $(0, \delta_0) \in P \cdot (\bigvee_{i\in\mathbb{N}} Q_i)$.

8. Conclusion

In this paper we provided two probabilistic relational models of complete IL-semirings. At first 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 $\mathsf{pMR}_{0,d,f}(A)$ — *the set of all finitary $\underline{0}$-included down-closed and convex 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.

In addition we have studied another type of probabilistic multirelations, and have proved that $\mathsf{pMR}_{t,1}(A)$ — *the set of all total $\mathcal{D}_1$-convex probabilistic multirelations* — forms a complete IL-semiring preserving the right 0.

Acknowledgement

The author is grateful to the anonymous referee for his careful reading and helpful comments, and wish to thank Assoc. Prof. Hitoshi Furusawa for his valuable comments on this work. This work was supported by Global COE, Kyoto University.

References

Cohen, E. (2000). Separation and Reduction. In Backhouse, R., and Oliveira, J.N., eds., *Mathematics of Program Construction, vol. 1837 of LNCS*, 45–59. Springer.

McIver, A., Cohen, E., and Morgan, C. (2006). Using Probabilistic Kleene Algebra for Protocol Verification. In Schmidt, R.A., ed.,*Relations and Kleene Algebra in Computer Science*, vol. 4136 of LNCS, 296-310. Springer.

McIver, A. and Weber, T. (2005). Towards Automated Proof Support for Probabilistic Distributed Systems. In Sutcliffe, G. and Voronkov, A., eds., *Proceedings of Logic for Programming, Artificial Intelligence, and Reasoning*, volume 3835 of LNAI, 534-548. Springer.

Möller, B. (2004). Lazy Kleene Algebra. In Kozen, D., ed., *Mathematics of Program Construction*, volume 3125 of LNCS, 252-273. Springer.

Nishizawa, K., Tsumagari, N., Furusawa, H. (2009). 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*, vol. 5827 of LNCS, 276-290. Springer.

Rabin, M. (1982). N-Process Mutual Exclusion with Bounded Waiting by 4 log2 N-Valued Shared Variable. JCSS 25(1): 66-75.

Rewitzky, I. (2003). Binary Multirelations. In de Swart, H., Orlowska, E., Schmidt, G., and Roubens, M., eds., *Theory and Applications of Relational Structures as Knowledge Instruments*, volume 2929 of LNCS, 256-271. Springer.

Rewitzky, I. and Brink, C. (2006). Monotone Predicate Transformers as Up-Closed Multirelations. In Schmidt, R.A., ed., *Relations and Kleene Algebra in Computer Science*, volume 4136 of LNCS, 311-327. Springer.

Received August 30, 2012
Revised November 15, 2012