Two examples of probabilistic Kleene algebra

Norihiro Tsumagari

Graduate school of Science and Engineering, Kagoshima university

06 . 30 . 2008

RIMS workshop in Kyoto

Outline

- Kleene algebra
- Probabilistic Kleene algebra
- Examples

  Probabilistic Case

  - by McIver and Weber to interpret probabilistic distributive systems

  Up-closed Multi-relations with some restrictions

  - by Furusawa, Tsumagari and Nishizawa, in ”Relations and Kleene Algebra in Computer Science, volume 4988 of LNCS”

Definition

$(K, +, \cdot, {}^*, 0, 1)$ is *Kleene algebra*:

- $(K, +, 0)$ is a commutative idempotent monoid.
- $(K, \cdot, 1)$ is a monoid.
- 0 is zero element with respect to $\cdot$.

$$
\begin{aligned}
ab + ac &= a(b + c) \\
ac + bc &= (a + b)c \\
1 + aa^* &\leq a^* \\
1 + a^*a &\leq a^* \\
ab \leq a &\implies ab^* \leq a \\
ab \leq b &\implies a^*b \leq b
\end{aligned}
$$

Definition

$(K, +, \cdot, ^*, 0, 1)$ is *probabilistic Kleene algebra* :

- $(K, +, 0)$ is a commutative idempotent monoid.
- $(K, \cdot, 1)$ is a monoid.
- 0 is zero element with respect to $\cdot$.

$$ab + ac \cancel{=} \le a(b + c)$$

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

$$1 + aa^* \le a^*$$

$$\cancel{1 + a^*a \le a^*}$$

$$\cancel{ab \le a}\ a(b + 1) \le a \implies ab^* \le a$$

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

Example 1.

Probabilistic case

A.K.McIver and T.Weber

Discrete probability distribution

d is a discrete probability distribution over a set $S^\top$:

$$d : S^\top \to [0,1] \quad s.t. \quad \sum_{k \in S^\top} d(k) = 1$$

where $S^\top = S \cup \{\top\}$ ($\top \notin S$).

The set of discrete probability distributions over $S^\top$: $\overline{S^\top}$

Probabilistic power domain

Probabilistic power domain is $(\overline{S}^{\top}, \sqsubseteq_{\mathcal{D}})$:

$$d \sqsubseteq_{\mathcal{D}} d' \overset{def}{\iff} \forall k \in S; \quad d(k) \geq d'(k)$$

Up Closure

D: a set of distributions,

D is up-closed if

$$d \in D \ \wedge \ d \sqsubseteq_{\mathcal{D}} d' \implies d' \in D;$$

Convex Closure

D: a set of distributions,

D is convex-closed if

$$d, d' \in D \implies d \;{}_p\!\oplus d' \in D;$$

where for $p \in [0, 1]$,

$$(d \;{}_p\!\oplus d')(s) := p \times d(s) + (1 - p) \times d'(s)$$

Cauchy Closure

D: a set of distributions,

D is Cauchy-closed if $\forall d \in \overline{S^{\top}}$

$$\forall \epsilon > 0.\ \exists d_{\epsilon} \in D.\ \mathrm{dist}(d, d_{\epsilon}) < \epsilon \implies d \in D$$

where the distance over $\overline{S^{\top}}$ is defined as

$$\mathrm{dist}(d, d') := \max\{|d(k) - d'(k)| \mid \forall k \in S^{\top}\}$$

Probabilistic Case

A mapping

$$P : S^{\top} \to \wp(\overline{S^{\top}})$$

s.t. $P(\top) = \{\delta_{\top}\}$ and

$\forall s \in S.$ [$P(s)$ is up-, convex-, Cauchy-closed]

where $\delta_{\top}(s) := \begin{cases} 1 & (s = \top) \\ 0 & (s \in S) \end{cases}$

$\mathcal{L}S$ denotes the set of such mappings.

Order on $\mathcal{L}S$

For $P, Q \in \mathcal{L}S$,

$$P \sqsubseteq Q \quad \overset{def}{\Longleftrightarrow} \quad \forall s \in S.\ P(s) \subseteq Q(s)$$

Theorem

$(\mathcal{L}S, +, ;, *, 0, 1)$ *is a probabilistic Kleene algebra.*

(McIver and Weber. 2005)

$$
\begin{aligned}
0(s) &:= \{\delta_\top\} \\
1(s) &:= \lceil\{\delta_s\}\rceil \\
(P+Q)(s) &:= \lceil P(s) \cup Q(s) \rceil \\
(P;Q)(s) &:= \{\sum_{u \in S^\top} d(u) \times f_u \mid d \in P(s) \land f_u \in Q(u)\} \\
P^* &:= \mu X \cdot P; X + 1
\end{aligned}
$$

For $D \subseteq \overline{S^\top}$, $\lceil D \rceil$ is the smallest up-, convex-, Cauchy-closed subset of distributions containing D.

$(\mu X \cdot -)$ denotes the least fixed point of the function $(\lambda X \cdot -) : \mathcal{L}S \to \mathcal{L}S$

$P;(Q+R) \sqsubseteq P;Q + P;R$ need not hold.

Example

$S = \{x, y\}$, $P, Q \in \mathcal{L}S$

$$P(s) = \{d \mid d(x) \le \tfrac{1}{2}, d(y) \le \tfrac{1}{2}\}$$
$$Q(s) = \{d \mid d(s) = 0\}$$

$$\begin{aligned}
\delta_x &= \tfrac{1}{2} \times \delta_x + \tfrac{1}{2} \times \delta_x + 0 \times \delta_\top && \delta_x \ {}_{\frac{1}{2}}\!\oplus \delta_y \in P(s) \\
&= (\delta_x \ {}_{\frac{1}{2}}\!\oplus \delta_y)(x) \times \delta_x && \delta_x \in 1(x) \subseteq (Q+1)(x) \\
&\quad +(\delta_x \ {}_{\frac{1}{2}}\!\oplus \delta_y)(y) \times \delta_x && \delta_x \in Q(y) \subseteq (Q+1)(y) \\
&\quad +(\delta_x \ {}_{\frac{1}{2}}\!\oplus \delta_y)(\top) \times \delta_\top && \delta_\top \in (Q+1)(\top)
\end{aligned}$$

$$\therefore \forall s \in S.\ \delta_x \in P;(Q+1)(s) \ .$$

(McIver & Weber)

$P;(Q+R) \sqsubseteq P;Q+P;R$ need not hold.

Example

$S=\{x,y\}$, $P,Q \in \mathcal{L}S$

$$P(s)=\{d \mid d(x)\le \tfrac{1}{2}, d(y)\le \tfrac{1}{2}\}$$
$$Q(s)=\{d \mid d(s)=0\}$$

$$\therefore \forall s \in S.\ \delta_x \in P;(Q+1)(s) \ .$$

But, $\delta_x \notin P(s)=(P;1)(s)$ and $\delta_x \notin (P;Q)(s)$

$$(\because \forall d \in (P;Q)(s);\ d(x) \le \tfrac{1}{2})$$

(McIver & Weber)

Example 2.

Up-closed Multirelations

with some restrictions

Furusawa, Tsumagari, Nishizawa

Up-closed Multirelation

A *multirelation* R over a set A :

$$R \subseteq A \times \wp(A)$$

R is *up-closed* if

$$\forall x \in A.\, \forall X, Y \subseteq A.\quad (x, X) \in R \;\wedge\; X \subseteq Y \;\Rightarrow\; (x, Y) \in R$$

The set of up-closed multirelations over A :

$$\mathbf{UMRel}(A)$$

One of the restrictions : "finitary"

Definition

$R \in \mathbf{UMRel}(A)$ is *finitary*:

$$(x, W) \in R$$
$$\Longrightarrow \ \exists\, Z : \text{a finite set. } (Z \subseteq W \wedge (x, Z) \in R).$$

The set of finitary up-closed multirelations over A :

$$\mathbf{UMRel}_f(A)$$

The other restriction : "total"

Definition

$R \in \mathbf{UMRel}(A)$ is *total*:

$$\forall x \in A.(x, \emptyset) \notin R$$

(I.Rewitzky and C. Brink. 2006)

The set of finitary total up-closed multirelations over A :

$$\mathbf{UMRel}_f^+(A)$$

Obvious element of $\mathbf{UMRel}_f^+(A)$

$$\mathbf{0} := \emptyset$$

is in $\mathbf{UMRel}_f^+(A)$.

Union on $\mathbf{UMRel}_f^+(A)$

$\boldsymbol{\Lambda}$: an index set.

For a family $\{R_\lambda \in \mathbf{UMRel}_f^+(A) \mid \lambda \in \boldsymbol{\Lambda}\}$,

$$\bigcup_{\lambda \in \boldsymbol{\Lambda}} R_\lambda$$

is in $\mathbf{UMRel}_f^+(A)$.

Union on $\mathbf{UMRel}_f^+(A)$

Λ : an index set.

For a family $\{R_\lambda \in \mathbf{UMRel}_f^+(A) \mid \lambda \in \Lambda\}$,

$$\bigcup_{\lambda \in \Lambda} R_\lambda$$

is in $\mathbf{UMRel}_f^+(A)$.

$R + S$ denotes $R \cup S$ for $R, S \in \mathbf{UMRel}_f^+(A)$

Proposition

$(\mathbf{UMRel}_f^+(A), +, 0)$ *is*
a commutative idempotent monoid.

That is

$$
\begin{aligned}
0 + R &= R \\
R + P &= P + R \\
R + R &= R \\
R + (P + Q) &= (R + P) + Q
\end{aligned}
$$

Composition on Multirelations

For $R, P \in \mathbf{UMRel}_f^+(A)$, the composition $R; P$:

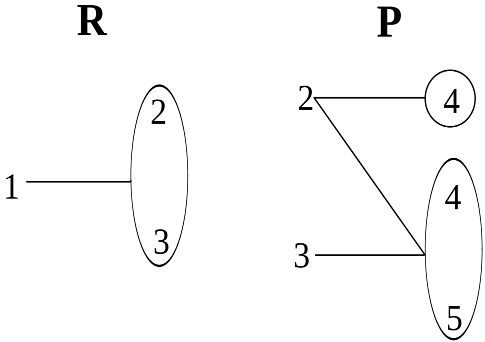
$$
\begin{aligned}
& (x, W) \in R; P \\
\stackrel{def}{\iff} \; & \exists Y \subseteq A. \, ((x, Y) \in R \;\wedge\; \forall y \in Y. (y, W) \in P)
\end{aligned}
$$

Composition on Multirelations

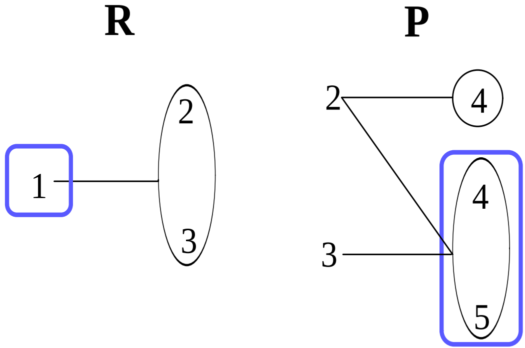
For $R, P \in \mathbf{UMRel}_f^+(A)$, the composition $R; P$:

$$
\begin{aligned}
& (x, W) \in R; P \\
\overset{def}{\iff}\ & \exists Y \subseteq A.\ ((x, Y) \in R \ \wedge\ \underline{\forall y \in Y.(y, W) \in P})
\end{aligned}
$$

$$A = \{1, 2, 3, 4, 5\}$$
$$R = \{(1, W) \mid \{2, 3\} \subseteq W\}$$
$$P = \{(2, W) \mid 4 \in W\} \cup \{(3, W) \mid \{4, 5\} \subseteq W\}$$

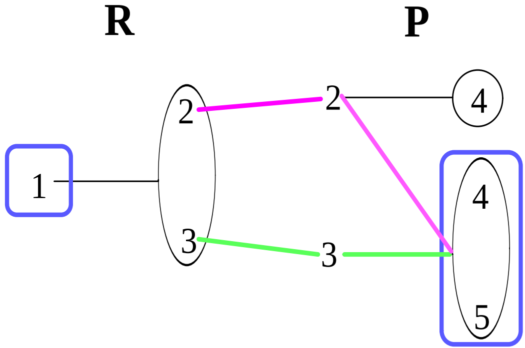


$$A = \{1, 2, 3, 4, 5\}$$
$$R = \{(1, W) \mid \{2, 3\} \subseteq W\}$$
$$P = \{(2, W) \mid 4 \in W\} \cup \{(3, W) \mid \{4, 5\} \subseteq W\}$$



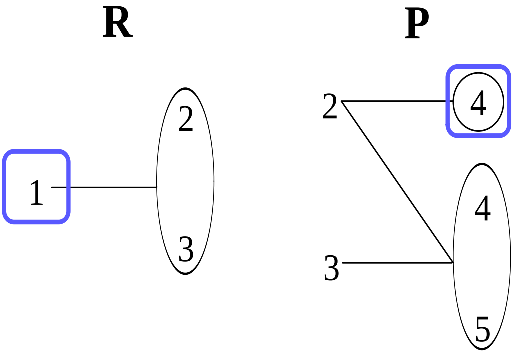
$(1,\{4,5\}) \in R;P$?

$$A = \{1, 2, 3, 4, 5\}$$
$$R = \{(1, W) \mid \{2, 3\} \subseteq W\}$$
$$P = \{(2, W) \mid 4 \in W\} \cup \{(3, W) \mid \{4, 5\} \subseteq W\}$$



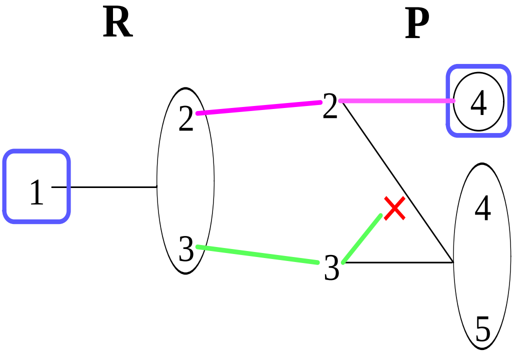
$(1,\{4,5\}) \in R;P$?   Yes!

$$A = \{1,2,3,4,5\}$$
$$R = \{(1,W) \mid \{2,3\} \subseteq W\}$$
$$P = \{(2,W) \mid 4 \in W\} \cup \{(3,W) \mid \{4,5\} \subseteq W\}$$



$(1,\{4\}) \in R;P$?

$$A = \{1, 2, 3, 4, 5\}$$
$$R = \{(1, W) \mid \{2, 3\} \subseteq W\}$$
$$P = \{(2, W) \mid 4 \in W\} \cup \{(3, W) \mid \{4, 5\} \subseteq W\}$$



$(1,\{4\}) \in R;P$?

No!

Proposition

$(\mathbf{UMRel}_f^+(A), ;, 0)$ *satisfies*

$$\begin{aligned} 0; R &= 0 \\ R; 0 &= 0 \end{aligned}$$

"Total" is needed for "$R; 0 \subseteq 0$".

Example

$A = \{x\}$, then $(x, \emptyset) \in \nabla = A \times \wp(A)$.
For all $W \subseteq A$,

$$(x, \emptyset) \in \nabla \;\wedge\; \forall y \in \emptyset.(y, W) \in 0.$$

Therefore $\nabla; 0 = \nabla$.

$$\nabla; 0 \nsubseteq 0.$$

Proposition

- *The operator* $;$ *is monotone, i.e.*

$$R \subseteq R' \wedge P \subseteq P' \Rightarrow R; P \subseteq R'; P'$$

- $\mathbf{UMRel}_f^+(A)$ *is closed under the composition* $;$.
- *The composition* $;$ *is associative on* $\mathbf{UMRel}_f^+(A)$*, i.e.*

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

The *identity* $\mathbf{1} \in \mathbf{UMRel}_f^+(A)$

$$\mathbf{1} \;:=\; \{(x, W) \mid x \in W\}$$

is in $\mathbf{UMRel}_f^+(A)$.

Proposition

$(\mathbf{UMRel}_f^+(A), ;, 1)$ *is a monoid.*

That is

$$\begin{aligned} P; (Q; R) &= (P; Q); R \\ 1; R &= R \\ R; 1 &= R \end{aligned}$$

Distribute law

Proposition

For $P, Q, R \in \mathbf{UMRel}_f^+(A)$,

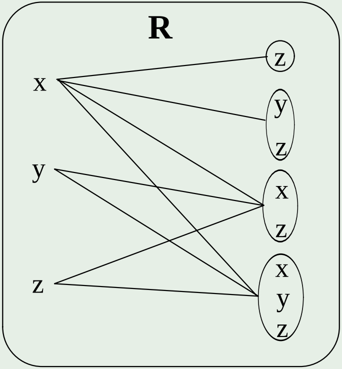
$$
\begin{aligned}
P; R + Q; R &= (P+Q); R \\
R; P + R; Q &\subseteq R; (P+Q)\ .
\end{aligned}
$$

$R; (P + Q) \subseteq R; P + R; Q$ need not hold.

Example

$R \in$ **UMRel**$(\{x, y, z\})$;

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

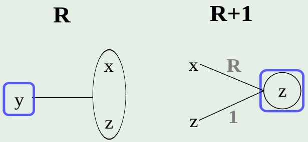


$R; (P+Q) \subseteq R; P + R; Q$ need not hold.

Example

$R \in$ **UMRel**$(\{x, y, z\})$;

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

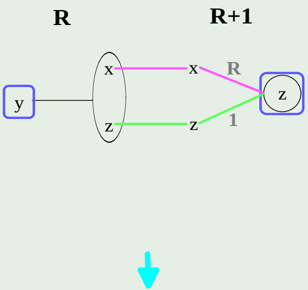


$R; (P + Q) \subseteq R; P + R; Q$ need not hold.

Example

$R \in$ **UMRel**$(\{x, y, z\})$;

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



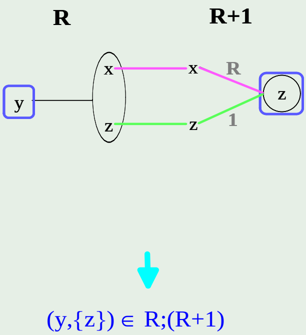
$(y, \{z\}) \in R;(R+1)$

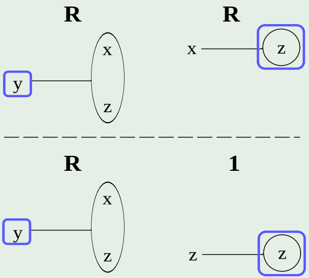
$R;(P+Q) \subseteq R;P + R;Q$ need not hold.

Example

$R \in \mathbf{UMRel}(\{x,y,z\})$;

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



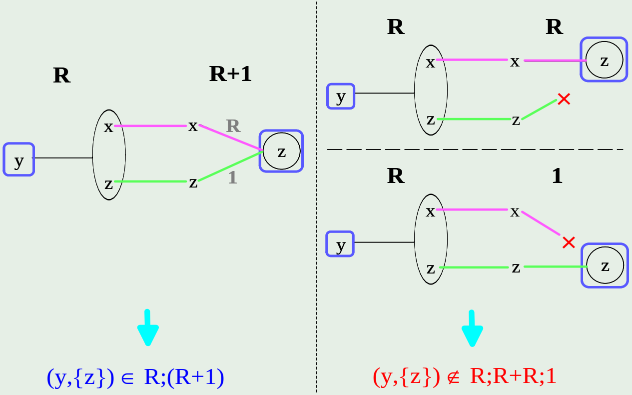


$R; (P + Q) \subseteq R; P + R; Q$ need not hold.

Example

$R \in$ **UMRel**$(\{x, y, z\})$;

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



The star operator *

For $R \in \mathbf{UMRel}_f^+(A)$, a mapping φ_R on $\mathbf{UMRel}_f^+(A)$ is

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

For $R \in \mathbf{UMRel}_f^+(A)$, a mapping φ_R on $\mathbf{UMRel}_f^+(A)$ is

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

The operator * on $\mathbf{UMRel}_f^+(A)$:

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

The star operator *

Proposition

$(\mathbf{UMRel}_f^+(A), +, ;, ^*, 0, 1)$ *satisfies the following conditions:*

$$
\begin{aligned}
1 + R; R^* &\subseteq R^* \\
P; (R + 1) \subseteq P &\Longrightarrow P; R^* \subseteq P \\
R; P \subseteq P &\Longrightarrow R^*; P \subseteq P \ .
\end{aligned}
$$

Proposition

$(\mathbf{UMRel}_f^+(A), +, ;, {}^*, 0, 1)$ *satisfies the following conditions:*

$$
\begin{array}{rcl}
1 + R; R^* & \subseteq & R^* \\
P; (R + 1) \subseteq P & \Longrightarrow & P; R^* \subseteq P \\
R; P \subseteq P & \Longrightarrow & R^*; P \subseteq P \ .
\end{array}
$$

Note :

R^* is the reflexive transitive closure of $R \in \mathbf{UMRel}_f^+(A)$.

"Finitary" is needed for
"$P; (R + 1) \subseteq P \Rightarrow P; R^* \subseteq P$".

Example

$P, R \in \mathbf{UMRel}(\mathbb{N})$;

$$\begin{aligned} P &= \{(n, W) \mid W \text{ is an infinite set.}\} \\ R &= \{(n, W) \mid \exists m \in W. n \leq m + 1\} \end{aligned}$$

In this case $P; (R + 1) \subseteq P$.
For a natural number n,

$$(n, \{0\}) \in P; R^*, \text{ but } (n, \{0\}) \notin P.$$

(K.Nishizawa)

Theorem

$$(\mathbf{UMRel}_f^+(A), +, ;, ^*, 0, 1)$$

is a Probabilistic Kleene algebra.

(H.Furusawa, N.Tsumagari, K.Nishizawa. 2008)

Current Interest

$\mathcal{LS}$ and $\mathbf{UMRel}_f^+(A)$ form probabilistic Kleene algebra, respectively.

What is the relationship of them?