Relational verification of probabilistic programs: an algebraic framework

Leandro Gomes
joint work with Patrick Baillot and Marco Gaboardi

GT SCALP meeting 2024

Context and motivation

Formal methodologies aim to prove

- partial correctness
- safety
- liveness
- ...

Context and motivation

Formal methodologies aim to prove

- partial correctness
- safety
- liveness
- ...

Numerous formal verification approaches have surfaced

- Hoare logic
- Dynamic logic
- Temporal logic
- Kleene algebra with tests (KAT)
  - NetKAT - networks
  - CKAT - concurrency
  - TopKAT - incorrectness logic
  - ...
- ...

Context and motivation

Some of the systems to verify have a probabilistic behaviour

- randomized algorithms
- security
- differential privacy
- learning theory
- ...

Context and motivation

Some of the systems to verify have a probabilistic behaviour

- randomized algorithms
- security
- differential privacy
- learning theory
- ...

and need a relational reasoning, e.g. **probabilistic non-interference**

Deterministic methods have been lifted to the probabilistic setting:
probabilistic Relational Hoare logic pRHL

Context and motivation

Some of the systems to verify have a probabilistic behaviour

- randomized algorithms
- security
- differential privacy
- learning theory
- ...

and need a relational reasoning, e.g. **probabilistic non-interference**

Deterministic methods have been lifted to the probabilistic setting: **probabilistic Relational Hoare logic pRHL**

However, it would still be useful to benefit from automation

Goal

Introduce a KAT-like approach for relational reasoning on probabilistic programs

An example of program analysis

OneTimePad(x : *private text*) : *public message*
$key \xleftarrow{\$} Uniform(\{0,1\}^{\frac{1}{2}})$;
$cipher \leftarrow x$ *XOR* key;
return $cipher$;

An example of program analysis

OneTimePad(x : *private text*) : *public message*
$key \xleftarrow{\$} Uniform(\{0,1\}^{\frac{1}{2}})$;
$cipher \leftarrow x$ *XOR* key;
return *cipher*;

Prove that *cipher* does not depend on the private text x:
non-interference

An example of program analysis

OneTimePad(x : *private text*) : *public message*
$key \xleftarrow{\$} Uniform(\{0,1\}^{\frac{1}{2}})$;
$cipher \leftarrow x$ *XOR* key;
return $cipher$;

Prove that *cipher* does not depend on the private text x:
non-interference

How to formally reason about such property?

Guarded Kleene Algebra with Tests (GKAT)

(S. Smolka et al, 2020)

$b, b_1, b_2 \in \mathrm{BExp} ::=$		$c, c_1, c_2 \in \mathrm{Exp} ::=$	
0	**false**	1	**skip**
1	**true**	$a \in \Sigma$	**do** a
$p \in T$	p	$b \in \mathrm{BExp}$	**assert** b
$b_1; b_2$	b_1 **and** b_2	$c_1; c_2$	$c_1; c_2$
$b_1 + b_2$	b_1 **or** b_2	$c_1 +_b c_2$	**if** b **then** c_1 **else** c_2
$\bar{b}$	**not** b	$c^{(b)}$	**while** b **do** c

GKAT example

$$\textit{terms } t \in \texttt{Terms} ::= x \in \texttt{Var} \mid r \in \mathbb{R} \mid t_1 + t_2 \mid t_1 - t_2 \mid t_1 \times t_2$$

$$\textit{distributions } d \in \texttt{Distr}$$

$$\textit{tests } b \in \texttt{Tests} ::= \textbf{false} \mid \textbf{true} \mid t_1 < t_2 \mid t_1 = t_2 \mid \textbf{not } b \mid b_1 \textbf{ and } b_2 \mid b_1 \textbf{ or } b_2$$

$$\textit{commands } c \in \texttt{Comm} ::= \textbf{skip} \mid x \leftarrow t \mid x \overset{\$}{\leftarrow} d \mid c_1; c_2 \mid \textbf{if } b \textbf{ then } c_1 \textbf{ else } c_2 \mid \textbf{while } b \textbf{ do } c$$

GKAT semantics

A **Probabilistic model** of GKAT is a triple

$$i = (S, eval, sat)$$

where:

- **S** is a set of states;
- for each action a, **eval(a)** : $S \to \mathcal{D}(S)$ is a sub-Markov kernel;
- for each test t, **sat(t)** $\subseteq S$

GKAT semantics

A **Probabilistic model** of GKAT is a triple

$$i = (S, eval, sat)$$

where:

- **S** is a set of states;
- for each action a, **eval(a)** : $S \to \mathcal{D}(S)$ is a sub-Markov kernel;
- for each test t, **sat(t)** $\subseteq S$

$$\mathcal{P}_i[\![c]\!] \text{ is a sub-Markov kernell}$$

$$\mathcal{P}_i[\![c_1; c_2]\!](s)(s') := \sum_{s''} \mathcal{P}_i[\![c_1]\!](s)(s'') \times \mathcal{P}_i[\![c_2]\!](s'')(s')$$

GKAT axioms

$$
\begin{array}{rcl}
c +_b c & = & c \\
c_1 +_b c_2 & = & c_2 +_{\bar{b}} c_1 \\
(c_1 +_{b_1} c_2) +_{b_2} c_3 & = & c_1 +_{b_1;b_2} (c_2 +_{b_2} c_3) \\
c_1; c_3 +_b c_2; c_3 & = & (c_1 +_b c_2); c_3 \\
(c_1; c_2); c_3 & = & c_1; (c_2; c_3) \\
0; c & = & 0
\end{array}
\qquad
\begin{array}{rcl}
c; 0 & = & 0 \\
1; c & = & c \\
c; 1 & = & c \\
c^{(b)} & = & c; c^{(b)} +_b 1
\end{array}
$$

GKAT

Proposition

The probabilistic model above **satisfies** *the axioms of GKAT.*

Reason about programs

How to state properties about programs?

In Hoare logic $\{\varphi\}c\{\psi\}$ is translated in KAT $\varphi; c = \varphi; c; \psi$

Reason about programs

How to state properties about programs?

In Hoare logic $\{\varphi\}c\{\psi\}$ is translated in KAT $\varphi; c = \varphi; c; \psi$

How to state **relational** properties about **probabilistic** programs?

In *probabilistic relational Hoare logic (pRHL)*[Barthe *et all* 2009]

The judgment

$$\vdash_i c \sim c' : \phi \Rightarrow \psi$$

is valid in the interpretation $\mathcal{P}_i[\![\cdot]\!]$ if for every (m, m') such that $(m, m') \models \phi$, $\exists \mu \in \mathcal{D}(S^2)$ such that

$$\Pi_1(\mu) = \mathcal{P}_i[\![c]\!](m), \Pi_2(\mu) = \mathcal{P}_i[\![c']\!](m')$$

and

$$\mathit{range}(\mu) = \{(m, m') \in S \mid \mu(m, m') > 0\} \subseteq \psi$$

Reason about programs

How to state properties about programs?

In Hoare logic $\{\varphi\}c\{\psi\}$ is translated in KAT $\varphi; c = \varphi; c; \psi$

How to state **relational** properties about **probabilistic** programs?

In *probabilistic relational Hoare logic (pRHL)*[Barthe *et all* 2009]

The judgment

$$\vdash_i c \sim c' : \phi \Rightarrow \psi$$

is valid in the interpretation $\mathcal{P}_i[\![\cdot]\!]$ if for every (m, m') such that $(m, m') \models \phi$, $\exists \mu \in \mathcal{D}(S^2)$ such that

$$\Pi_1(\mu) = \mathcal{P}_i[\![c]\!](m), \Pi_2(\mu) = \mathcal{P}_i[\![c']\!](m')$$

and

$$\mathit{range}(\mu) = \{(m, m') \in S \mid \mu(m, m') > 0\} \subseteq \psi$$

Bi Guarded Kleene Algebra with Tests (BiGKAT)

$$
\begin{array}{rcl}
B, B_1, B_2 \in \ddot{\mathrm{B}}\mathrm{Exp} ::= & & \\
\mid & \ddot{0} & \langle 0 \mid 0 \rangle \\
\mid & \ddot{1} & \langle 1 \mid 1 \rangle \\
\mid & P \in \mathbb{P} & p \\
\mid & B_1 \fatsemi B_2 & B_1 \textbf{ and } B_2 \\
\mid & B_1 \oplus B_2 & B_1 \textbf{ or } B_2 \\
\mid & \neg B & \textbf{not } B
\end{array}
$$

$$
\begin{array}{rc}
C, C_1, C_2 \in \ddot{\mathrm{E}}\mathrm{xp} ::= & \\
\mid & A \in \Sigma \\
\mid & \langle c| \\
\mid & |c\rangle \\
\mid & \{c \underset{C}{\mid} c'\} \\
\mid & B \in \ddot{\mathrm{B}}\mathrm{Exp} \\
\mid & C_1 \fatsemi C_2 \\
\mid & C_1 \oplus_B C_2 \\
\mid & C^{(B)}
\end{array}
$$

BiGKAT semantics

A **Probabilistic model** of BiGKAT is a probabilistic interpretation of GKAT $i = (S, eval, sat)$ and two functions $Eval$, Sat
such that:

- for each action A, **Eval(A)** : $S^2 \to \mathcal{D}(S^2)$ is a sub-Markov kernel;
- for each test P, **Sat(P)** $\subseteq S^2$.
- $\overline{\mathcal{P}_i}[\![C]\!] : S^2 \to \mathcal{D}(S^2)$ is a sub-Markov kernell

BiGKAT semantics

A **Probabilistic model** of BiGKAT is a probabilistic interpretation of GKAT $i = (S, eval, sat)$ and two functions $Eval$, Sat
such that:

- for each action A, **Eval(A)** : $S^2 \to \mathcal{D}(S^2)$ is a sub-Markov kernel;
- for each test P, **Sat(P)** $\subseteq S^2$.
- $\overline{\mathcal{P}_i}[\![C]\!] : S^2 \to \mathcal{D}(S^2)$ is a sub-Markov kernell
- $\overline{\mathcal{P}_i}[\![C_1 \fatsemi C_2]\!] = \sum_{(s_1'', s_2'')} \overline{\mathcal{P}_i}[\![C_1]\!](s_1, s_2)(s_1'', s_2'') \times \overline{\mathcal{P}_i}[\![C_2]\!](s_1'', s_2'')(s_1', s_2')$

BiGKAT semantics

A **Probabilistic model** of BiGKAT is a probabilistic interpretation of GKAT $i = (S, eval, sat)$ and two functions $Eval$, Sat
such that:

- for each action A, **Eval(A)** : $S^2 \to \mathcal{D}(S^2)$ is a sub-Markov kernel;
- for each test P, **Sat(P)** $\subseteq S^2$.
- $\overline{\mathcal{P}_i}[\![C]\!] : S^2 \to \mathcal{D}(S^2)$ is a sub-Markov kernell
- $\overline{\mathcal{P}_i}[\![C_1 \fatsemi C_2]\!] = \sum_{(s_1'', s_2'')} \overline{\mathcal{P}_i}[\![C_1]\!](s_1, s_2)(s_1'', s_2'') \times \overline{\mathcal{P}_i}[\![C_2]\!](s_1'', s_2'')(s_1', s_2')$
- $\overline{\mathcal{P}_i}[\![\langle c|]\!] = \mathcal{P}_i[\![c]\!] \times id_S$
- $\overline{\mathcal{P}_i}[\![|c\rangle]\!] = id_S \times \mathcal{P}_i[\![c]\!]$

BiGKAT semantics

A **Probabilistic model** of BiGKAT is a probabilistic interpretation of GKAT $i = (S, eval, sat)$ and two functions $Eval$, Sat
such that:

- for each action A, **Eval(A)** : $S^2 \to \mathcal{D}(S^2)$ is a sub-Markov kernel;
- for each test P, **Sat(P)** $\subseteq S^2$.
- $\overline{\mathcal{P}_i}[\![C]\!] : S^2 \to \mathcal{D}(S^2)$ is a sub-Markov kernell
- $\overline{\mathcal{P}_i}[\![C_1 \fatsemi C_2]\!] = \sum_{(s_1'', s_2'')} \overline{\mathcal{P}_i}[\![C_1]\!](s_1, s_2)(s_1'', s_2'') \times \overline{\mathcal{P}_i}[\![C_2]\!](s_1'', s_2'')(s_1', s_2')$
- $\overline{\mathcal{P}_i}[\![\langle c|]\!] = \mathcal{P}_i[\![c]\!] \times id_S$
- $\overline{\mathcal{P}_i}[\![|c\rangle]\!] = id_S \times \mathcal{P}_i[\![c]\!]$
- $\overline{\mathcal{P}_i}[\![\{c \mid_C c'\}]\!]$ is defined only if $\overline{\mathcal{P}_i}[\![C]\!]$ is defined and if:
  - $\Pi_1(\overline{\mathcal{P}_i}[\![C]\!](s, s')) = \mathcal{P}_i[\![c]\!](s)$
  - $\Pi_2(\overline{\mathcal{P}_i}[\![C]\!](s, s')) = \mathcal{P}_i[\![c']\!](s'), \forall s, s' \in S$
    $\overline{\mathcal{P}_i}[\![\{c \mid_C c'\}]\!] = \overline{\mathcal{P}_i}[\![C]\!]$

BiGKAT theory

$$\langle 0| = |0\rangle = \ddot{0} \tag{1}$$

$$\langle 1| = |1\rangle = \ddot{1} \tag{2}$$

$$\langle b_1 + b_2| = \langle b_1| \oplus \langle b_2| \tag{3}$$

$$\langle \neg b| = \neg\langle b| \tag{4}$$

$$\langle c_1 ; c_2| = \langle c_1| \fatsemi \langle c_2| \tag{5}$$

$$\langle c_1 +_b c_2| = \langle c_1| \oplus_{\langle b|} \langle c_2| \tag{6}$$

$$\langle c^{(b)}| = \langle c|^{\langle b|} \tag{7}$$

BiGKAT theory

$$\langle 0| = |0\rangle = \ddot{0} \tag{1}$$
$$\langle 1| = |1\rangle = \ddot{1} \tag{2}$$
$$\langle b_1 + b_2| = \langle b_1| \oplus \langle b_2| \tag{3}$$
$$\langle \neg b| = \neg\langle b| \tag{4}$$
$$\langle c_1; c_2| = \langle c_1| \fatsemi \langle c_2| \tag{5}$$
$$\langle c_1 +_b c_2| = \langle c_1| \oplus_{\langle b|} \langle c_2| \tag{6}$$
$$\langle c^{(b)}| = \langle c|^{\langle b|} \tag{7}$$

- $\forall_{c_1,c_2 \in \mathsf{Exp}},\ \langle c_1| \fatsemi |c_2\rangle = |c_2\rangle \fatsemi \langle c_1|$

BiGKAT theory

$$\langle 0| = |0\rangle = \ddot{0} \tag{1}$$
$$\langle 1| = |1\rangle = \ddot{1} \tag{2}$$
$$\langle b_1 + b_2| = \langle b_1| \oplus \langle b_2| \tag{3}$$
$$\langle \neg b| = \neg\langle b| \tag{4}$$
$$\langle c_1; c_2| = \langle c_1| \fatsemi \langle c_2| \tag{5}$$
$$\langle c_1 +_b c_2| = \langle c_1| \oplus_{\langle b|} \langle c_2| \tag{6}$$
$$\langle c^{(b)}| = \langle c|^{\langle b|} \tag{7}$$

- $\forall_{c_1,c_2 \in \mathsf{Exp}},\ \langle c_1| \fatsemi |c_2\rangle = |c_2\rangle \fatsemi \langle c_1|$
- $\{c \mid_C c'\} = C$

BiGKAT theory

$$\langle 0| = |0\rangle = \ddot{0} \tag{1}$$
$$\langle 1| = |1\rangle = \ddot{1} \tag{2}$$
$$\langle b_1 + b_2| = \langle b_1| \oplus \langle b_2| \tag{3}$$
$$\langle \neg b| = \neg\langle b| \tag{4}$$
$$\langle c_1; c_2| = \langle c_1| \fatsemi \langle c_2| \tag{5}$$
$$\langle c_1 +_b c_2| = \langle c_1| \oplus_{\langle b|} \langle c_2| \tag{6}$$
$$\langle c^{(b)}| = \langle c|^{\langle b|} \tag{7}$$

- $\forall_{c_1,c_2 \in \mathsf{Exp}},\ \langle c_1| \fatsemi |c_2\rangle = |c_2\rangle \fatsemi \langle c_1|$
- $\{c \mid_C c'\} = C$
- $\{c_1 \mid_{C_1} c_1'\} \fatsemi \{c_2 \mid_{C_2} c_2'\} = \{c_1; c_2 \mid_{C_1 \fatsemi C_2} c_1'; c_2'\}$

BiGKAT theory

$$\langle 0| = |0\rangle = \ddot{0} \tag{1}$$
$$\langle 1| = |1\rangle = \ddot{1} \tag{2}$$
$$\langle b_1 + b_2| = \langle b_1| \oplus \langle b_2| \tag{3}$$
$$\langle \neg b| = \neg\langle b| \tag{4}$$
$$\langle c_1; c_2| = \langle c_1| \fatsemi \langle c_2| \tag{5}$$
$$\langle c_1 +_b c_2| = \langle c_1| \oplus_{\langle b|} \langle c_2| \tag{6}$$
$$\langle c^{(b)}| = \langle c|^{\langle b|} \tag{7}$$

- $\forall_{c_1,c_2 \in \mathsf{Exp}},\ \langle c_1| \fatsemi |c_2\rangle = |c_2\rangle \fatsemi \langle c_1|$
- $\{c \mid_C c'\} = C$
- $\{c_1 \mid_{C_1} c_1'\} \fatsemi \{c_2 \mid_{C_2} c_2'\} = \{c_1; c_2 \mid_{C_1 \fatsemi C_2} c_1'; c_2'\}$
- Axioms of GKAT

BiGKAT theory

$$\langle 0| = |0\rangle = \ddot{0} \quad (1)$$

$$\langle 1| = |1\rangle = \ddot{1} \quad (2)$$

$$\langle b_1 + b_2| = \langle b_1| \oplus \langle b_2| \quad (3)$$

$$\langle \neg b| = \neg \langle b| \quad (4)$$

$$\langle c_1 ; c_2| = \langle c_1| \fatsemi \langle c_2| \quad (5)$$

$$\langle c_1 +_b c_2| = \langle c_1| \oplus_{\langle b|} \langle c_2| \quad (6)$$

$$\langle c^{(b)}| = \langle c|^{\langle b|} \quad (7)$$

- $\forall_{c_1, c_2 \in \mathsf{Exp}},\ \langle c_1| \fatsemi |c_2\rangle = |c_2\rangle \fatsemi \langle c_1|$
- $\{c \underset{C}{\mid} c'\} = C$
- $\{c_1 \underset{C_1}{\mid} c_1'\} \fatsemi \{c_2 \underset{C_2}{\mid} c_2'\} = \{c_1 ; c_2 \underset{C_1 \fatsemi C_2}{\mid} c_1' ; c_2'\}$
- Axioms of GKAT
- Axioms of GKAT written in the language of BiGKAT expressions (e.g. $C \oplus_B C = C$)

BiGKAT theory

$$\langle 0| = |0\rangle = \ddot{0} \quad (1)$$

$$\langle 1| = |1\rangle = \ddot{1} \quad (2)$$

$$\langle b_1 + b_2| = \langle b_1| \oplus \langle b_2| \quad (3)$$

$$\langle \neg b| = \neg\langle b| \quad (4)$$

$$\langle c_1; c_2| = \langle c_1| \fatsemi \langle c_2| \quad (5)$$

$$\langle c_1 +_b c_2| = \langle c_1| \oplus_{\langle b|} \langle c_2| \quad (6)$$

$$\langle c^{(b)}| = \langle c|^{\langle b|} \quad (7)$$

- $\forall_{c_1,c_2 \in \mathsf{Exp}},\ \langle c_1| \fatsemi |c_2\rangle = |c_2\rangle \fatsemi \langle c_1|$
- $\{c \underset{C}{\mid} c'\} = C$
- $\{c_1 \underset{C_1}{\mid} c_1'\} \fatsemi \{c_2 \underset{C_2}{\mid} c_2'\} = \{c_1; c_2 \underset{C_1 \fatsemi C_2}{\mid} c_1'; c_2'\}$
- Axioms of GKAT
- Axioms of GKAT written in the language of BiGKAT expressions (e.g. $C \oplus_B C = C$)
- ...

BiGKAT

Proposition

The probabilistic interpretation $\overline{\mathcal{P}_i}[\![.]\!]$ *of BiGKAT satisfies all the axioms of the theory of BiGKAT.*

Example

$key \xleftarrow{\$} Uniform(\{0,1\}^{\frac{1}{2}});$
$cipher \leftarrow x \ XOR \ key;$
$return \ cipher;$

$$c \quad = \quad (z \xleftarrow{\$} d); (y \leftarrow x \ XOR \ z)$$

Example

$key \xleftarrow{\$} Uniform(\{0,1\}^{\frac{1}{2}})$;
$cipher \leftarrow x \; XOR \; key$;
return $cipher$;

$$c \quad = \quad (z \xleftarrow{\$} d); (y \leftarrow x \; XOR \; z)$$

In pRHL, prove:

$$\vdash c \sim c' : \top \Rightarrow [y = y']$$

Example

$key \xleftarrow{\$} Uniform(\{0,1\}^{\frac{1}{2}})$;
$cipher \leftarrow x \; XOR \; key$;
return $cipher$;

$$c \quad = \quad (z \xleftarrow{\$} d); (y \leftarrow x \; XOR \; z)$$

In pRHL, prove:

$$\vdash c \sim c' : \top \Rightarrow [y = y']$$

In BiGKAT we prove:

$$\{c \underset{C}{\mid} c'\} = \{c \underset{C}{\mid} c'\} \fatsemi [y = y']$$

Example

$$\ddot{\mathbf{1}} = B \oplus_B \bar{B}$$

$$\begin{aligned}
\{c \underset{C}{\mid} c'\} &= \{z \xleftarrow{\$} d \underset{C_1}{\mid} z' \xleftarrow{\$} d'\}\langle y \leftarrow x \; XOR \; z \mid y' \leftarrow x' \; XOR \; z'\rangle \\
&= ([x = x'] \oplus_{[x=x']} [x \neq x'])\{z \xleftarrow{\$} d \underset{C_1}{\mid} z' \xleftarrow{\$} d'\}\langle y \leftarrow x \; XOR \; z \mid y' \leftarrow x' \; XOR \; z'\rangle
\end{aligned}$$

Example

$$(C_1 +_B C_2) \fatsemi C_3 = C_1 \fatsemi C_3 +_B C_2 \fatsemi C_3$$

$$\begin{aligned}
\{c \mid_{C} c'\} &= \{z \xleftarrow{\$} d \mid_{C_1} z' \xleftarrow{\$} d'\}\langle y \leftarrow x \; XOR \; z \mid y' \leftarrow x' \; XOR \; z'\rangle \\
&= ([x = x'] \oplus_{[x=x']} [x \neq x'])\{z \xleftarrow{\$} d \mid_{C_1} z' \xleftarrow{\$} d'\}\langle y \leftarrow x \; XOR \; z \mid y' \leftarrow x' \; XOR \; z'\rangle \\
&= [x = x']\{z \xleftarrow{\$} d \mid_{C_1} z' \xleftarrow{\$} d'\}\langle y \leftarrow \; x \; XOR \; z \mid y' \leftarrow \; x' \; XOR \; z'\rangle \\
&\quad \oplus_{[x=x']}[x \neq x']\{z \xleftarrow{\$} d \mid_{C_1} z' \xleftarrow{\$} d'\}\langle y \leftarrow \; x \; XOR \; z \mid y' \leftarrow \; x' \; XOR \; z'\rangle
\end{aligned}$$

Example

Now we need to define the sub-Markov kernel C_1. Consider the two Markov kernels (corresponding to two couplings):

$$C_{id}(m, m') = \frac{1}{2}\delta_{m[z \leftarrow 0], m'[z' \leftarrow 0]} + \frac{1}{2}\delta_{m[z \leftarrow 1], m'[z' \leftarrow 1]}$$

$$C_{neg}(m, m') = \frac{1}{2}\delta_{m[z \leftarrow 0], m'[z' \leftarrow 1]} + \frac{1}{2}\delta_{m[z \leftarrow 1], m'[z' \leftarrow 0]}$$

Example

Now we need to define the sub-Markov kernel C_1. Consider the two Markov kernels (corresponding to two couplings):

$$C_{id}(m, m') = \frac{1}{2}\delta_{m[z\leftarrow 0], m'[z'\leftarrow 0]} + \frac{1}{2}\delta_{m[z\leftarrow 1], m'[z'\leftarrow 1]}$$
$$C_{neg}(m, m') = \frac{1}{2}\delta_{m[z\leftarrow 0], m'[z'\leftarrow 1]} + \frac{1}{2}\delta_{m[z\leftarrow 1], m'[z'\leftarrow 0]}$$

We have:

$$C_{id} = C_{id} \fatsemi [z = z']$$
$$C_{neg} = C_{neg} \fatsemi [z \neq z']$$

Example

Now we need to define the sub-Markov kernel C_1. Consider the two Markov kernels (corresponding to two couplings):

$$C_{id}(m, m') = \tfrac{1}{2}\delta_{m[z\leftarrow 0],m'[z'\leftarrow 0]} + \tfrac{1}{2}\delta_{m[z\leftarrow 1],m'[z'\leftarrow 1]}$$
$$C_{neg}(m, m') = \tfrac{1}{2}\delta_{m[z\leftarrow 0],m'[z'\leftarrow 1]} + \tfrac{1}{2}\delta_{m[z\leftarrow 1],m'[z'\leftarrow 0]}$$

We have:

$$C_{id} = C_{id} \fatsemi [z = z']$$
$$C_{neg} = C_{neg} \fatsemi [z \neq z']$$

We can then define C_1 as $C_1 = C_{id} \oplus_{[x=x']} C_{neg}$

Example

$$C_1 = C_{id} \oplus_{[x=x']} C_{neg}$$

$$\begin{array}{rl} & C_1\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \\ = & (C_{id} \oplus_{[x=x']} C_{neg})\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \end{array}$$

Example

$$C_1 = C_{id} \oplus_{[x=x']} C_{neg}$$

$$\begin{array}{rl} & C_1\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \\ = & (C_{id} \oplus_{[x=x']} C_{neg})\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \end{array}$$

Example

$$C_{id} = C_{id}[z = z']$$

$$\begin{array}{rl} & [x = x']C_{id}\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \\ = & [x = x']C_{id}[z = z']\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \end{array}$$

Example

C_{id} does not change x, x'

$$
\begin{array}{rl}
 & [x = x']C_{id}\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z'\rangle \\
= & [x = x'][z = z']C_{id}\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z'\rangle \\
= & [x = x'][x = x'][z = z']C_{id}\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z'\rangle
\end{array}
$$

Example

XOR properties

$$
\begin{aligned}
& [x = x']C_{id}\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z'\rangle \\
= \quad & [x = x']C_{id}[z = z']\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z'\rangle \\
= \quad & [x = x']C_{id}[x = x'][z = z']\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z'\rangle \\
= \quad & [x = x']C_{id}[x = x'][z = z'][x \ XOR \ z = x' \ XOR \ z']\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z'\rangle
\end{aligned}
$$

Example

XOR properties

$$
\begin{aligned}
& [x = x']C_{id}\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \\
= \quad & [x = x']C_{id}[z = z']\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \\
= \quad & [x = x']C_{id}[x = x'][z = z']\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \\
= \quad & [x = x']C_{id}[x = x'][z = z'][x \ XOR \ z = x' \ XOR \ z']\langle \ldots \mid \ldots \rangle [y = y']
\end{aligned}
$$

Example

reverse steps

$$
\begin{aligned}
& [x = x']\, C_{id}\, \langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \\
= \quad & [x = x']\, C_{id}\, [z = z']\, \langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \\
= \quad & [x = x']\, C_{id}\, [x = x']\, [z = z']\, \langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle \\
= \quad & [x = x']\, C_{id}\, [x = x']\, [z = z']\, [x \ XOR \ z = x' \ XOR \ z']\, \langle \ldots \mid \ldots \rangle\, [y = y'] \\
= \quad & [x = x']\, C_{id}\, \langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle\, [y = y']
\end{aligned}
$$

Example

Analogously for C_{neg} with $[x \neq x']$:

$$[x \neq x']C_{neg}\langle y \leftarrow x \ XOR \ z \mid y' \leftarrow x' \ XOR \ z' \rangle [y = y']$$

Example

Analogously for C_{neg} with $[x \neq x']$:

$$[x \neq x']C_{neg}\langle y \leftarrow x \; XOR \; z \mid y' \leftarrow x' \; XOR \; z'\rangle[y = y']$$

By combining the two we obtain:

$$C_1\langle y \leftarrow x \; XOR \; z \mid y' \leftarrow x' \; XOR \; z'\rangle = C_1\langle y \leftarrow x \; XOR \; z \mid y' \leftarrow x' \; XOR \; z'\rangle[y = y']$$

Expressiveness of BiGKAT

The pRHL judgment

$$\vdash_i c \sim c' : \phi \Rightarrow \psi$$

is encoded as

$$\exists C \in \ddot{\mathsf{Exp}},\ \phi \fatsemi \{c \mid_C c'\} = \phi \fatsemi \{c \mid_C c'\} \fatsemi \psi$$

Expressiveness of BiGKAT

The pRHL judgment

$$\vdash_i c \sim c' : \phi \Rightarrow \psi$$

is encoded as

$$\exists C \in \ddot{\mathsf{Exp}},\ \phi \fatsemi \{c \mid_C c'\} = \phi \fatsemi \{c \mid_C c'\} \fatsemi \psi$$

Sequence rule (Barthe *et all* 2009)

$$\frac{\vdash_i c_1 \sim c_1' : \phi \Rightarrow \psi \quad \vdash_i c_2 \sim c_2' : \psi \Rightarrow \xi}{\vdash_i c_1; c_2 \sim c_1'; c_2' : \phi \Rightarrow \xi}$$

is encoded in BiGKAT as:

$$\phi \fatsemi \{c_1 \mid_{C_1} c_1'\} = \phi \fatsemi \{c_1 \mid_{C_1} c_1'\} \fatsemi \psi \ \wedge\ \psi \fatsemi \{c_2 \mid_{C_2} c_2'\} = \psi \fatsemi \{c_2 \mid_{C_2} c_2'\} \fatsemi \xi$$

$$\Rightarrow \phi \fatsemi \{c_1; c_2 \mid_{C_1 \fatsemi C_2} c_1'; c_2'\} = \phi \fatsemi \{c_1; c_2 \mid_{C_1 \fatsemi C_2} c_1'; c_2'\} \fatsemi \xi$$

Encoding of pRHL in BiGKAT

Theorem

The encoding of the pRHL rules (without the while rule) can be derived in BiGKAT.

Conclusions and future work

- Reason about **differential privacy**, which requires to include (ϵ, δ): develop aBiGKAT to encode apRHL;
- Reason about a **while** language;
- Consider a language with both nondeterminism and probabilities;