A Quantitative Approach to Non-Interference for Probabilistic Systems

Alessandra Di Pierro
joint work with
Alessandro Aldini

Pisa, 2nd Mefisto Workshop, November 2003
Overview

- Process Algebra
Overview

- Process Algebra
- NI via Process Equivalence
Overview

- Process Algebra
- NI via Process Equivalence
- Measuring NI
Overview

- Process Algebra
- NI via Process Equivalence
- Measuring NI
- An example
Overview

- Process Algebra
- NI via Process Equivalence
- Measuring NI
- An example
- Linear operators and norm
Overview

- Process Algebra
- NI via Process Equivalence
- Measuring NI
- An example
- Linear operators and norm
- Conclusions
A Probabilistic Process Calculus

\[ P ::= 0 \mid \pi.P \mid P +^p P \mid P \parallel^p_P P \mid P\backslash L \mid P/^p_\alpha A, \]
A Probabilistic Process Calculus

\[ P ::= 0 | \pi.P | P +^p P | P \parallel^p_s P | P \setminus L | P /^p_a | A, \]

Action \( \pi \) is drawn from set \( \text{Act} \) and can be an \textit{internal} or \( \tau \) action, an \textit{output} action \( a \), or an \textit{input} action \( a^* \), where \( a \) belongs to the set of visible action types \( \text{AType} \).
A Probabilistic Process Calculus

\[ P ::= 0 \mid \pi.P \mid P +^p P \mid P \mid_s P \mid P \backslash L \mid P /_a^p \mid A, \]

Action \( \pi \) is drawn from set \( \text{Act} \) and can be an \emph{internal} or \( \tau \) action, an \emph{output} action \( a \), or an \emph{input} action \( a_* \), where \( a \) belongs to the set of visible action types \( \text{AType} \).

We denote by \( \mathcal{G} \) the set of finite state, guarded, and closed terms generated by the syntax above.
The model we adopt is a generative-reactive transition system \((G, Act, T)\), whose states are process terms and \(T\) is a probabilistic transition relation.
The model we adopt is a generative-reactive transition system \((G, Act, T)\), whose states are process terms and \(T\) is a probabilistic transition relation.

Input actions, \(RAct\), are treated according to a reactive model, while output and internal actions, \(GAct\), are treated according to a generative model.
Operational Semantics

The model we adopt is a generative-reactive transition system \((G, Act, T)\), whose states are process terms and \(T\) is a probabilistic transition relation.

Input actions, \(RAct\), are treated according to a reactive model, while output and internal actions, \(GAct\), are treated according to a generative model.

We will informally define \(T\) via an example.
Consider the process

\[(a_* + r \ b) \parallel_{\{a,b\}}^p (b_* c + q b_* d)\]
Consider the process

\[(a_\ast + r b) \parallel \{a, b\} (b_\ast . c + q b_\ast . d)\]
$P \setminus L$ prevents the execution of the actions of type in $L \subseteq AType$. It corresponds to process $P \parallel_L 0$. 

A Quantitative Approach to Non-Interference for Probabilistic Systems – p.6/20
Hiding and Restriction

\[ P \setminus L \text{ prevents the execution of the actions of type in } L \subseteq A_{Type}. \text{ It corresponds to process } P \parallel_L 0. \]

\[ P /_a^p \text{ turns actions of type } a \text{ into actions } \tau. \text{ The probability } p \text{ specifies the choice between generative actions } \tau \text{ obtained by hiding reactive actions } a \_ \text{ of } P \text{ and generative actions previously enabled by } P. \]
Hiding and Restriction

\(P \setminus L\) prevents the execution of the actions of type in 
\(L \subseteq AType\). It corresponds to process \(P ||_L 0\).

\(P/\alpha\) turns actions of type \(\alpha\) into actions \(\tau\). The probability \(p\) specifies the choice between generative actions \(\tau\) obtained by hiding reactive actions \(a_*\) of \(P\) and generative actions previously enabled by \(P\).

By hiding \(a_*\) in \(P \triangleq a_* +^q b\) we turn the purely nondeterministic choice into a probabilistic one:
Hiding and Restriction

\( P \setminus L \) prevents the execution of the actions of type in \( L \subseteq AType \). It corresponds to process \( P \parallel_L 0 \).

\( P/\!\!/^p_a \) turns actions of type \( a \) into actions \( \tau \). The probability \( p \) specifies the choice between generative actions \( \tau \) obtained by hiding reactive actions \( a* \) of \( P \) and generative actions previously enabled by \( P \).

By hiding \( a* \) in \( P \triangleq a* +^q b \) we turn the purely nondeterministic choice into a probabilistic one: \( P/\!\!/^p_a \equiv \tau +^p b \), is a probabilistic choice between the action \( \tau \) obtained by hiding the action \( a* \) and the action \( b \).
Weak Probabilistic Bisimulation

Define $\text{Prob}(P, \tau^* a, C) =$:

\[
\begin{cases}
1 & \text{if } a = \tau \land P \in C \\
\sum_{Q \in G} \text{Prob}(P, \tau, Q) \cdot \text{Prob}(Q, \tau^*, C) & \text{if } a = \tau \land P \notin C \\
\sum_{Q \in G} \text{Prob}(P, \tau, Q) \cdot \text{Prob}(Q, \tau^* a, C) + \text{Prob}(P, a, C) & \text{if } a \neq \tau
\end{cases}
\]
Weak Probabilistic Bisimulation

Define $\text{Prob}(P, \tau^*a, C) =$:

$$
\begin{cases}
1 & \text{if } a = \tau \land P \in C \\
\sum_{Q \in G} \text{Prob}(P, \tau, Q) \cdot \text{Prob}(Q, \tau^*, C) & \text{if } a = \tau \land P \notin C \\
\sum_{Q \in G} \text{Prob}(P, \tau, Q) \cdot \text{Prob}(Q, \tau^*a, C) + \text{Prob}(P, a, C) & \text{if } a \neq \tau
\end{cases}
$$

An equivalence relation $R \subseteq G \times G$ is a weak probabilistic bisimulation iff, $(P, Q) \in R$ implies $\forall C \in G/R$:

- $\text{Prob}(P, \tau^*a, C) = \text{Prob}(Q, \tau^*a, C) \ \forall a \in G\text{Act}$
- $\text{Prob}(P, a_*, C) = \text{Prob}(Q, a_*, C) \ \forall a_* \in R\text{Act}$. 
Example

Consider $P \triangleq a + \frac{1}{2} b$ and $Q \triangleq \tau.Q + \frac{1}{3} (a + \frac{1}{2} b)$
Consider $P \triangleq a + \frac{1}{2} b$ and $Q \triangleq \tau. Q + \frac{1}{3} (a + \frac{1}{2} b)$

Let $R$ be the relation which determines partition $\{C', [\emptyset]\}$, with $C' = \{P, Q\}$ and $[\emptyset] = \{\emptyset\}$. 
Example

Consider \( P \triangleq a + \frac{1}{2} b \) and \( Q \triangleq \tau.Q + \frac{1}{3} (a + \frac{1}{2} b) \)

Let \( R \) be the relation which determines partition \( \{ C, [0] \} \), with \( C = \{ P, Q \} \) and \( [0] = \{ 0 \} \).

\[ \text{Prob}(P, \tau^* \pi, [0]) = \frac{1}{2}, \text{ with } \pi \in \{ a, b \} \]
Consider $P \triangleq a + \frac{1}{2} b$ and $Q \triangleq \tau.Q + \frac{1}{3} (a + \frac{1}{2} b)$

Let $R$ be the relation which determines partition $\{ C, [0] \}$, with $C = \{ P, Q \}$ and $[0] = \{ 0 \}$.

$$\text{Prob}(P, \tau^* \pi, [0]) = \frac{1}{2}, \text{ with } \pi \in \{ a, b \}$$

$$\text{Prob}(Q, \tau^* a, [0]) = \frac{1}{3} \cdot \text{Prob}(Q, \tau^* a, [0]) + \frac{1}{3},$$
Example

Consider $P \triangleq a + \frac{1}{2} b$ and $Q \triangleq \tau.Q + \frac{1}{3} (a + \frac{1}{2} b)$

Let $R$ be the relation which determines partition $\{ C, [0] \}$, with $C = \{ P, Q \}$ and $[0] = \{ 0 \}$.

$\text{Prob}(P, \tau^* \pi, [0]) = \frac{1}{2}$, with $\pi \in \{ a, b \}$

$\text{Prob}(Q, \tau^* a, [0]) = \frac{1}{3} \cdot \text{Prob}(Q, \tau^* a, [0]) + \frac{1}{3}$,

from which we derive

$\text{Prob}(Q, \tau^* a, [0]) = \frac{1}{2}$. 

Consider a partition of $A_{Type}$ into high-level actions, $High$, and low-level actions, $Low$. 
Consider a partition of $AType$ into high-level actions, $High$, and low-level actions, $Low$.

Compare the low-level view of the system in the absence of high-level interactions and the low-level view of the system in the presence of high-level interactions. Formally, check whether:
Consider a partition of $AType$ into high-level actions, $High$, and low-level actions, $Low$.

Compare the low-level view of the system in the absence of high-level interactions and the low-level view of the system in the presence of high-level interactions. Formally, check whether:

$$P \setminus High \approx_{PB} P^{p_1}_{h_1} \cdots p_n_{h_n} \forall p_1, \ldots, p_n \in (0, 1).$$
Examples

\[ P \triangleq h_*(a_0 + b_0) + (a_0 + b_0) \] satisfies the PNI property, since
\[ (a_0 + b_0) \approx_{PB} \tau.(a_0 + b_0) + p(a_0 + b_0) \] for any choice of parameter \( p \) of the hiding operator.
Examples

\[ P \triangleq h_\ast (a_\ast \cdot 0 + b_\ast \cdot 0) + (a_\ast \cdot 0 + b_\ast \cdot 0) \text{ satisfies the} \ PNI \text{ property, since} \\
(a_\ast \cdot 0 + b_\ast \cdot 0) \approx_{PB} \tau (a_\ast \cdot 0 + b_\ast \cdot 0) +^p (a_\ast \cdot 0 + b_\ast \cdot 0) \text{ for any} \\
\text{choice of parameter} \ p \ \text{of the hiding operator.}
\]

Consider \[ P \triangleq a.(h_\ast \cdot 0 + b.0) + b.a.0. \] We have that for \text{any choice of} \ p, \\
\[ a.b.0 + b.a.0 \equiv P \setminus \{h\} \not\approx_{PB} a.(\tau.0 +^p b.0) + b.a.0 \equiv P^p_h. \]

Examples

- $P \triangleq h_\ast (a_\ast.\underline{0} + b_\ast.\underline{0}) + (a_\ast.\underline{0} + b_\ast.\underline{0})$ satisfies the PNI property, since $(a_\ast.\underline{0} + b_\ast.\underline{0}) \approx_{PB} \tau.(a_\ast.\underline{0} + b_\ast.\underline{0}) +^p (a_\ast.\underline{0} + b_\ast.\underline{0})$ for any choice of parameter $p$ of the hiding operator.

- Consider $P \triangleq a.(h_\ast.\underline{0} + b.\underline{0}) + b.a.\underline{0}$. We have that for any choice of $p$, $a.b.\underline{0} + b.a.\underline{0} \equiv P\setminus\{h\} \not\approx_{PB} a.((\tau.\underline{0} +^p b.\underline{0}) + b.a.\underline{0}) \equiv P/_{h}^p$.

- $P \triangleq a.h.b.\underline{0} + (a.b.\underline{0} + a.\underline{0})$ presents a probabilistic information leakage.
Examples

- \( P \overset{\Delta}{=} h_*(a_*0 + b_*0) + (a_*0 + b_*0) \) satisfies the PNI property, since 
  \( (a_*0 + b_*0) \approx_{PB} \tau_*(a_*0 + b_*0) +^p (a_*0 + b_*0) \) for any choice of parameter \( p \) of the hiding operator.

- Consider \( P \overset{\Delta}{=} a.(h_*0 + b.0) + b.a.0 \). We have that for any choice of \( p \),
  \( a.b.0 + b.a.0 \equiv P \setminus \{h\} \not\approx_{PB} a.(\tau.0 +^p b.0) + b.a.0 \equiv P/^p_h \).

- \( P \overset{\Delta}{=} a.h.b.0 + (a.b.0 + a.0) \) presents a probabilistic information leakage. Can we measure it?
Measuring PNI

Intuitive idea: if two processes $P$ and $Q$ are not w.p.b. then for each equivalence relation $R \subseteq \mathcal{G} \times \mathcal{G}$, there exists $C \in \mathcal{G}/R$ and $a \in GAct$ such that

$$\text{Prob}(P, \tau^*a, C) \neq \text{Prob}(Q, \tau^*a, C).$$
Measuring PNI

Intuitive idea: if two processes $P$ and $Q$ are not w.p.b. then for each equivalence relation $R \subseteq \mathcal{G} \times \mathcal{G}$, there exists $C \in \mathcal{G}/R$ and $a \in GA^ct$ such that

$$\text{Prob}(P, \tau^* a, C) \neq \text{Prob}(Q, \tau^* a, C).$$

For each $R$ consider the state where the transition probabilities are maximally different and calculate the difference. Then take the $\inf$ over all $R$. 
Measuring PNI (ctd.)

Formally, define

$$\delta_{\bar{p}} = \sup_{a \in G\text{Act}} | \text{Prob}(P \setminus \text{High}, \tau^* a, C) - \text{Prob}(P/\bar{h}_P, \tau^* a, C) |,$$

where $$R \subseteq G \times G$$ is an equivalence relation, $$\bar{p} = p_1, \ldots, p_n$$, and $$\bar{h}^P = h_1^P, \ldots, h_n^P$$. 
Measuring PNI (ctd.)

Formally, define

$$\delta_{\bar{p}} = \sup_{a \in GAct} \left| \text{Prob}(P \setminus \text{High}, \tau^* a, C) - \text{Prob}(P/\bar{h}_P, \tau^* a, C) \right|,$$

where \( R \subseteq G \times G \) is an equivalence relation, \( \bar{p} = p_1, \ldots, p_n \),

and \( \bar{h}_P = h_1^P, \ldots, h_n^P \).

A measure for PNI is given by

$$\varepsilon_{\bar{p}} = \inf_{R} \{ \delta_{\bar{p}} \mid p_i \in (0, 1), 1 \leq i \leq n \},$$

where the parameter \( \bar{p} \) represents the attack.
Measuring PNI: An Example

Consider $P \triangleq a.(h \cdot 0 + b.0) + b.a.\emptyset$. Then

$$a.b.\emptyset + b.a.\emptyset \equiv P \backslash \{h\} \not\approx_{PB} a.(\tau.\emptyset + p \cdot b.0) + b.a.\emptyset \equiv P/h^p.$$

We show that $\varepsilon_p = \frac{1}{2}p$. 
Measuring PNI: An Example

Consider $P \triangleq a.(h_\ast.0 + b.0) + b.a.0$. Then

$$a.b.0 + b.a.0 \equiv P \setminus \{h\} \not\equiv_{PB} a.(\tau.0 + p b.0) + b.a.0 \equiv P/p^h.$$  

We show that $\varepsilon_p = \frac{1}{2}p$.

Parameter $p$ determines how easy is to distinguish the two behaviours $P_1$ and $P_2$ for a low-level user.
Measuring PNI: An Example

Consider \( P \triangleq a.(h \cdot 0 + b.0) + b.a.0 \). Then
\[
a.b.0 + b.a.0 \equiv P \setminus \{h\} \not\cong_{PB} a.((\tau.0 + p b.0) + b.a.0) \equiv P/_{h}^{p}.
\]

We show that \( \varepsilon_{p} = \frac{1}{2}p \).

Parameter \( p \) determines how easy is to distinguish the two behaviours \( P_{1} \) and \( P_{2} \) for a low-level user.

Clearly, if \( p \) tends to 1, \( \delta_{p} \) is maximal: it is easier to distinguish \( P_{1} \) and \( P_{2} \). Thus the corresponding \( H \) is the best attacker.
Measuring PNI: An Example (ctd.)
Measuring PNI: An Example (ctd.)

For $R_1 = \{\{1, 1\}'\}, \{2, 3, 2', 3'\}, C = \{4, 5, 6, 4', 5'\}$, and $R_2 = \{\{1, 1\}'\}, \{2\}, \{2'\}, \{3, 3'\}, C = \{4, 5, 6, 4', 5'\}$:
Measuring PNI: An Example (ctd.)

For $R_1 = \{\{1, 1'\}, \{2, 3, 2', 3'\}, C = \{4, 5, 6, 4', 5'\}\}$, and $R_2 = \{\{1, 1'\}, \{2\}, \{2'\}, \{3, 3'\}, C = \{4, 5, 6, 4', 5'\}\}$:

$$\delta^R_\mu = \|\text{Prob}(P \setminus \{h\}, a, C) - \text{Prob}(P / h, a, C)\| = 0 - \frac{p}{2} = \frac{p}{2},$$
Measuring PNI: An Example (ctd.)

For $R_1 = \{\{1, 1'\}, \{2, 3, 2', 3'\}, C = \{4, 5, 6, 4', 5'\}\}$, and $R_2 = \{\{1, 1'\}, \{2\}, \{2'\}, \{3, 3'\}, C = \{4, 5, 6, 4', 5'\}\}$:

$$\delta^R_p = \| \text{Prob}(P\{h\}, a, C) - \text{Prob}(P/\{h\}, a, C)\| = 0 - \frac{p}{2} = \frac{p}{2},$$

$$\delta^R_p = \| \text{Prob}(P\{h\}, a, [2]) - \text{Prob}(P/\{h\}, a, [2])\| = 0 - \frac{1}{2} = \frac{1}{2}.$$
Measuring PNI: An Example (ctd.)

For $R_1 = \{\{1, 1'\}, \{2, 3, 2', 3'\}, C = \{4, 5, 6, 4', 5'\}\}$, and $R_2 = \{\{1, 1'\}, \{2\}, \{2'\}, \{3, 3'\}, C = \{4, 5, 6, 4', 5'\}\}$:

\[
\delta^R_p = ||\text{Prob}(P\{h\}, a, C) - \text{Prob}(P/P_h^p, a, C)|| = 0 - \frac{p}{2} = \frac{p}{2},
\]

\[
\delta^R_p = ||\text{Prob}(P\{h\}, a, [2]) - \text{Prob}(P/P_h^p, a, [2])|| = 0 - \frac{1}{2} = \frac{1}{2}.
\]

\[
\varepsilon_p = \inf\{\frac{p}{2}, \frac{1}{2}\} = \frac{p}{2}.
\]
Matrix Representation

For probabilistic relations $R \subseteq X \times [0, 1] \times X$ define:

$$(M_R)_{xy} = \begin{cases} 
  w & \text{iff } (x, w, y) \in R \\
  0 & \text{otherwise}
\end{cases}$$
Matrix Representation

For probabilistic relations $R \subseteq X \times [0, 1] \times X$ define:

$$(M_R)_{xy} = \begin{cases} 
\sum w & \text{iff } (x, w, y) \in R \\
0 & \text{otherwise}
\end{cases}$$
Matrix Representation

For probabilistic relations $R \subseteq X \times [0, 1] \times X$ define:

$$\begin{align*}
(M_R)_{xy} &= \begin{cases} 
  w & \text{iff } (x, w, y) \in R \\
  0 & \text{otherwise}
\end{cases}
\end{align*}$$

For labelled relations $L \subseteq X \times A \times [0, 1] \times X$ define:

$$L|_a = \{(x, w, y) \mid (x, a, w, y) \in L\}$$

and then:

$$M_L = \bigoplus_{a \in A} M_{L|_a}$$
Example

A Quantitative Approach to Non-Interference for Probabilistic Systems – p.16/20
Example

\[ M(A) = M_a(A) \oplus M_b(A) \]
Example

\[ M(A) = \begin{pmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix} \]
Example

\[
\begin{align*}
\text{M}(A) &= \begin{pmatrix}
0 & \frac{1}{2} \\
0 & 0 \\
0 & 0 \\
\frac{1}{2} & 0 \\
0 & 0
\end{pmatrix}
\end{align*}
\]
Example

\[ \frac{1}{2} : a \]

\[ \frac{1}{2} : b \]

\[ M(A) = \begin{pmatrix}
0 & \frac{1}{2} & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{2} & 0 \\
0 & 0 & 0 & 0 \\
\end{pmatrix} \]
Example

\[ \bullet 1 \xrightarrow{1/2:a} 1/2:b \rightarrow 2 \xrightarrow{1/2:a} 1:\tau \]
$M(A) = M_a(A) \oplus M_b(A) \oplus M_\tau(A)$
Example

\[ M(A) = \begin{pmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \]
We extend the single step operator \( M = \bigoplus_{a \in \text{Act}} M_a \) to encode transitions on strings \( \sigma \in \text{Act}^* \):

\[
S_\sigma = M_{a_1} M_{a_2} \cdots M_{a_n}, \quad S_\varepsilon = I.
\]
We extend the single step operator $M = \bigoplus_{a \in Act} M_a$ to encode transitions on strings $\sigma \in Act^*$:

$$S_\sigma = M_{a_1} M_{a_2} \ldots M_{a_n}, S_\varepsilon = I.$$ 

We can then contract for all $n, m \in \mathbb{N}$ and $a \in Act$

$$M_\alpha(n, m) = S_{\tau^n \alpha \tau^m}.$$
We extend the single step operator \( M = \bigoplus_{a \in \text{Act}} M_a \) to encode transitions on strings \( \sigma \in \text{Act}^* \):

\[
S_\sigma = M_{a_1} M_{a_2} \ldots M_{a_n}, S_{\varepsilon} = I.
\]

We can then contract for all \( n, m \in \mathbb{N} \) and \( a \in \text{Act} \)

\[
M_\alpha(n, m) = S_{\tau^n \alpha \tau^m}.
\]

Given an equivalence relation \( R \subseteq \mathcal{G} \times \mathcal{G}, C \in \mathcal{G}/R \) and \( \sigma \in \text{Act}^* \), we calculate \( \text{Prob}(P, \sigma, C) \) by

\[
P_{\sigma}(K) = S_\sigma K.
\]
Transition probabilities $\text{Prob}(P, \Lambda, C)$ for some set of words $\Lambda \subseteq \text{Act}^*$ are defined via the operator $P_\Lambda : V(G) \leftrightarrow V(G/R)$.
Transition probabilities \( \text{Prob}(P, \Lambda, C) \) for some set of words \( \Lambda \subseteq \text{Act}^* \) are defined via the operator \( P_\Lambda : \mathcal{V}(G) \mapsto \mathcal{V}(G/R) : \)

\[
(P_\Lambda)_{P,C} = \sum_{a \in \text{Act}, Q \in \mathcal{G}} (P_a)_{PQ} \cdot (P_{\Lambda/a})_{QC}
\]

\[
(P_\Lambda)_{P,C} = 1 \text{ if } P \in C \text{ for all } \Lambda \text{ with } \varepsilon \in \Lambda.
\]
Measure as Operator Norm

Under the basic assumption that for \( P \in \mathcal{G} \), the two sub-models \( P_1 \equiv P \setminus \text{High} \) and \( P_2 \equiv P /^{P_1}_{h_1} \ldots /^{P_n}_{h_n} \) are fully generative, i.e. do not include reactive actions, we can measure the NI property of \( P \) by
Measure as Operator Norm

Under the basic assumption that for $P \in \mathcal{G}$, the two sub-models $P_1 \equiv P \setminus \text{High}$ and $P_2 \equiv P / P_1^{h_1} \ldots / P_n^{h_n}$ are fully generative, i.e. do not include reactive actions, we can measure the NI property of $P$ by

$$
\varepsilon_P = \inf_{K_P, K_Q} \| P_{\tau^* a \tau^*} (K_P) - P_{\tau^* a \tau^*} (K_Q) \|_\infty,
$$

for all $a \in \mathcal{G}Act$
Measure as Operator Norm

Under the basic assumption that for $P \in \mathcal{G}$, the two sub-models $P_1 \equiv P \setminus \text{High}$ and $P_2 \equiv P / P_{h_1} \ldots / P_{h_n}$ are fully generative, i.e. do not include reactive actions, we can measure the NI property of $P$ by

$$\varepsilon_P = \inf_{K_P, K_Q} \| P_{\tau^* a \tau^*}(K_P) - P_{\tau^* a \tau^*}(K_Q) \|_\infty,$$

for all $a \in GAct$

where for a linear operators $M$ on $\mathcal{V}$

$$\| M \|_\infty = \sup_{\bar{x} \in \mathcal{V}} \frac{\| M(\bar{x}) \|}{\| \bar{x} \|} = \sup_{\| \bar{x} \| = 1} \| M(\bar{x}) \|.$$
Conclusions

The construction of safe bounds for $\delta$ gives a quantification of the behavioural “similarity” of processes as a means for establishing a “confidentiality level”.
Conclusions

The construction of safe bounds for $\delta$ gives a quantification of the behavioural “similarity” of processes as a means for establishing a “confidentiality level”.

The value of $\delta$ corresponds to the distinguishability of processes via certain statistical tests. It gives an estimate of the number of tests an attacker needs in order to obtain some confidential information.
Conclusions

The construction of safe bounds for $\delta$ gives a quantification of the behavioural “similarity” of processes as a means for establishing a “confidentiality level”.

The value of $\delta$ corresponds to the distinguishability of processes via certain statistical tests. It gives an estimate of the number of tests an attacker needs in order to obtain some confidential information.

The interaction of a system $P$ with a high-user $H$ forced by the hiding operation can be analysed in order to formalise a notion of best attacker.