Measuring Masking Fault-Tolerance

Pablo F. Castro, Pedro R. D'Argenio, Ramiro Demasi, Luciano Putruele

Dependable Systems dTime Talks
October, 2020

Measuring Masking Fault-Tolerance

Pablo F. Castro, Pedro R. D'Argenio,
, Ramiro Demasi, Luciano Putruele

Dependable Systems dTim

October, 2020


Check for updates

Measuring Masking Fault-Tolerance

Pablo F. Castro[1,3](✉), Pedro R. D'Argenio[2,3,4], Ramiro Demasi[2,3], and Luciano Putruele[1,3]

[1] Departamento de Computación, FCEFQyN, Universidad Nacional de Río Cuarto, Río Cuarto, Córdoba, Argentina

{pcastro,lputruele}@dc.exa.unrc.edu.ar

[2] FaMAF, Universidad Nacional de Córdoba, Córdoba, Argentina

{dargenio,rdemasi}@famaf.unc.edu.ar

Investigaciones Científicas y Técnicas (CONICET),

Motivation

```
module NOMINAL

  b : [0..1] init 0;

  [w0]   true -> (b' = 0);
  [w1]   true -> (b' = 1);
  [r0]   b=0  -> true;
  [r1]   b=1  -> true;

endmodule
```

Ideal behaviour

```
module FAULTY

  v : [0..3] init 0;

  [w0]     true -> (v' = 0);
  [w1]     true -> (v' = 3);
  [r0]     v<=1 -> true;
  [r1]     v>=2 -> true;
  [fault] v<3  -> (v' = v+1);
  [fault] v>0  -> (v' = v-1);

endmodule
```

Redundancy

Behaviour of the implementation

A fault is masked when the occurrence of it have no observable consequences

Motivation

```
module NOMINAL

  b : [0..1] init 0;

  [w0]   true -> (b' = 0);
  [w1]   true -> (b' = 1);
  [r0]   b=0  -> true;
  [r1]   b=1  -> true;

endmodule
```

```
module FAULTY

  v : [0..3] init 0;

  [w0]     true -> (v' = 0);
  [w1]     true -> (v' = 3);
  [r0]     v<=1 -> true;
  [r1]     v>=2 -> true;
  [fault] v<3  -> (v' = v+1);
  [fault] v>0  -> (v' = v-1);

endmodule
```

- ¿Can an implementation mask all faults?

Motivation

```
module NOMINAL

  b : [0..1] init 0;

  [w0]   true -> (b' = 0);
  [w1]   true -> (b' = 1);
  [r0]   b=0  -> true;
  [r1]   b=1  -> true;

endmodule
```

```
module FAULTY

  v : [0..5] init 0;

  [w0]     true -> (v' = 0);
  [w1]     true -> (v' = 5);
  [r0]     v<=2 -> true;
  [r1]     v>=3 -> true;
  [fault] v<5  -> (v' = v+1);
  [fault] v>0  -> (v' = v-1);

endmodule
```

- ¿Can an implementation mask all faults?

CONICET UNC UNIVERSITÄT DES SAARLANDES

Motivation

```
module NOMINAL

  b : [0..1] init 0;

  [w0]   true -> (b' = 0);
  [w1]   true -> (b' = 1);
  [r0]   b=0  -> true;
  [r1]   b=1  -> true;

endmodule
```

```
module FAULTY

  v : [0..5] init 0;

  [w0]     true -> (v' = 0);
  [w1]     true -> (v' = 5);
  [r0]     v<=2 -> true;
  [r1]     v>=3 -> true;
  [fault] v<5  -> (v' = v+1);
  [fault] v>0  -> (v' = v-1);

endmodule
```

- ¿Can an implementation mask all faults?
- Given two implementations ¿can we determine which is better on masking?

Motivation

```
module NOMINAL

  b : [0..1] init 0;

  [w0]   true -> (b' = 0);
  [w1]   true -> (b' = 1);
  [r0]   b=0  -> true;
  [r1]   b=1  -> true;

endmodule
```

```
module FAULTY

  v : [0..5] init 0;

  [w0]     true -> (v' = 0);
  [w1]     true -> (v' = 5);
  [r0]     v<=2 -> true;
  [r1]     v>=3 -> true;
  [fault] v<5  -> (v' = v+1);
  [fault] v>0  -> (v' = v-1);

endmodule
```

- ¿Can an implementation mask all faults?
  - Behavioural relation
  - Game characterisation
  - Algorithm
- Given two implementations ¿can we determine which is better on masking?
  - Game based distance
  - Algorithm
  - Tool

CONICET

UNIVERSITÄT DES SAARLANDES

Strong Masking Simulation

Definition 3.1. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ be two transition systems. A' is *strong masking fault-tolerant* with respect to A if there exists a relation $\mathbf{M} \subseteq S \times S'$ between A and A' such that:

(A) $s_0 \, \mathbf{M} \, s'_0$, and

(B) for all $s \in S, s' \in S'$ with $s \, \mathbf{M} \, s'$ and all $e \in \Sigma$ the following holds:

  (1) if $s \xrightarrow{e} t$ then $\exists \, t' \in S' : s' \xrightarrow{e}' t' \wedge t \, \mathbf{M} \, t'$;

  (2) if $s' \xrightarrow{e}' t'$ then $\exists \, t \in S : s \xrightarrow{e} t \wedge t \, \mathbf{M} \, t'$;

  (3) if $s' \xrightarrow{F}' t'$ for some $F \in \mathcal{F}$ then $s \, \mathbf{M} \, t'$.

If such a relation exists we say that A' is a *strong masking fault-tolerant implementation* of A, denoted by $A \preceq_m A'$.

Strong Masking Simulation

Nominal: no faults

Implementation: has faults

Definition 3.1. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ be two transition systems. A' is *strong masking fault-tolerant* with respect to A if there exists a relation $\mathbf{M} \subseteq S \times S'$ between A and A' such that:

(A) $s_0 \,\mathbf{M}\, s'_0$, and

(B) for all $s \in S, s' \in S'$ with $s \,\mathbf{M}\, s'$ and all $e \in \Sigma$ the following holds:

  (1) if $s \xrightarrow{e} t$ then $\exists\, t' \in S' : s' \xrightarrow{e}{}' t' \wedge t \,\mathbf{M}\, t'$;

  (2) if $s' \xrightarrow{e}{}' t'$ then $\exists\, t \in S : s \xrightarrow{e} t \wedge t \,\mathbf{M}\, t'$;

  (3) if $s' \xrightarrow{F}{}' t'$ for some $F \in \mathcal{F}$ then $s \,\mathbf{M}\, t'$.

If such a relation exists we say that A' is a *strong masking fault-tolerant implementation* of A, denoted by $A \preceq_m A'$.

CONICET

UNC

UNIVERSITÄT DES SAARLANDES

Nominal:
no faults

Strong Masking Simulation

Implementation:
has faults

Definition 3.1. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ be two transition systems. A' is *strong masking fault-tolerant* with respect to A if there exists a relation $\mathbf{M} \subseteq S \times S'$ between A and A' such that:

(A) $s_0 \, \mathbf{M} \, s'_0$, and

(B) for all $s \in S, s' \in S'$ with $s \, \mathbf{M} \, s'$ and all $e \in \Sigma$ the following holds:

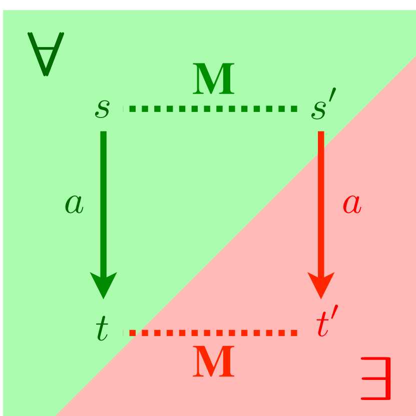
(1) if $s \xrightarrow{e} t$ then $\exists \, t' \in S' : s' \xrightarrow{e}' t' \wedge t \, \mathbf{M} \, t'$;

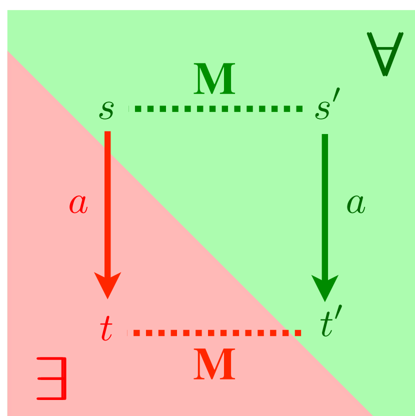
(2) if $s' \xrightarrow{e}' t'$ then $\exists \, t \in S : s \xrightarrow{e} t \wedge t \, \mathbf{M} \, t'$;

(3) if $s' \xrightarrow{F}' t'$ for some $F \in \mathcal{F}$ then $s \, \mathbf{M} \, t'$.

Just like
bisimulation

If such a relation exists we say that A' is a *strong masking fault-tolerant implementation* of A, denoted by $A \preceq_m A'$.





Nominal: no faults

Strong Masking Simulation

Implementation: has faults

Definition 3.1. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ be two transition systems. A' is *strong masking fault-tolerant* with respect to A if there exists a relation $\mathbf{M} \subseteq S \times S'$ between A and A' such that:

(A) $s_0 \,\mathbf{M}\, s'_0$, and

(B) for all $s \in S, s' \in S'$ with $s \,\mathbf{M}\, s'$ and all $e \in \Sigma$ the following holds:

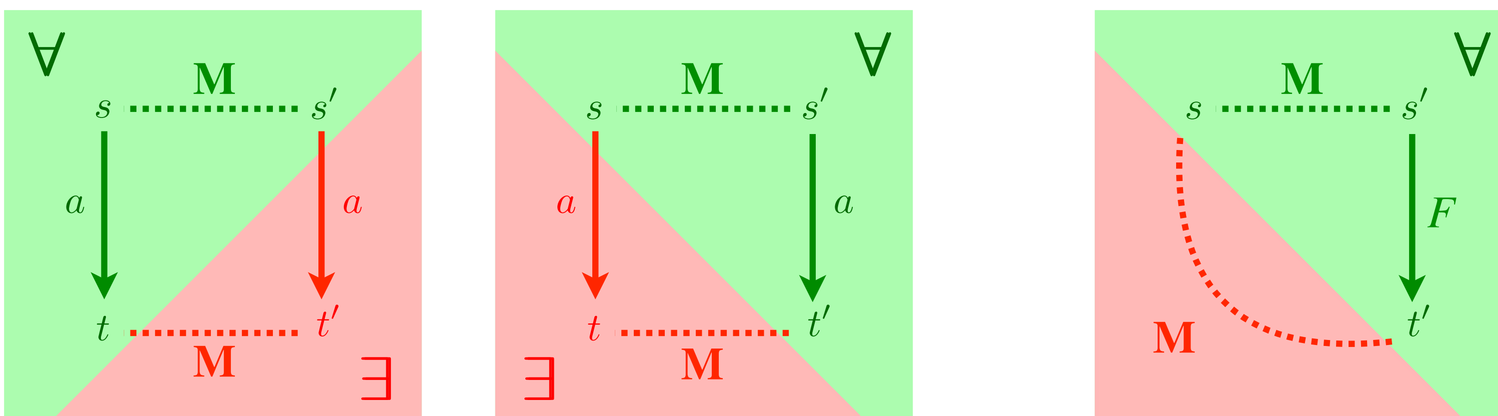
(1) if $s \xrightarrow{e} t$ then $\exists\, t' \in S' : s' \xrightarrow{e}{}' t' \wedge t \,\mathbf{M}\, t'$;

(2) if $s' \xrightarrow{e}{}' t'$ then $\exists\, t \in S : s \xrightarrow{e} t \wedge t \,\mathbf{M}\, t'$;

(3) if $s' \xrightarrow{F}{}' t'$ for some $F \in \mathcal{F}$ then $s \,\mathbf{M}\, t'$.

Just like bisimulation

If such a relation exists we say that A' is a *strong masking fault-tolerant implementation* of A, denoted by $A \preceq_m A'$.



Strong Masking Simulation

Nominal: no faults

Implementation: has faults

Definition 3.1. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ be two transition systems. A' is *strong masking fault-tolerant* with respect to A if there exists a relation $\mathbf{M} \subseteq S \times S'$ between A and A' such that:

(A) $s_0 \,\mathbf{M}\, s'_0$, and

(B) for all $s \in S, s' \in S'$ with $s \,\mathbf{M}\, s'$ and all $e \in \Sigma$ the following holds:

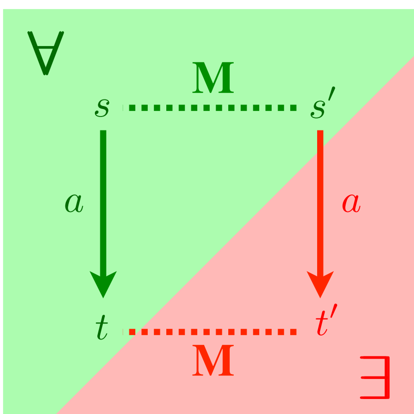
(1) if $s \xrightarrow{e} t$ then $\exists\, t' \in S' : s' \xrightarrow{e}{}' t' \wedge t \,\mathbf{M}\, t'$;

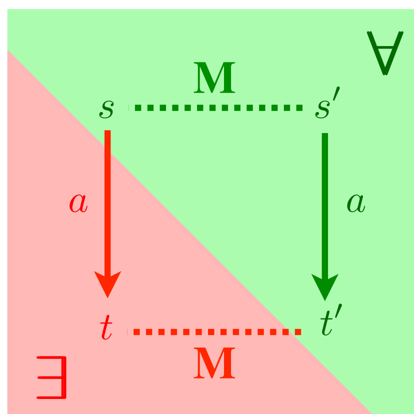
(2) if $s' \xrightarrow{e}{}' t'$ then $\exists\, t \in S : s \xrightarrow{e} t \wedge t \,\mathbf{M}\, t'$;

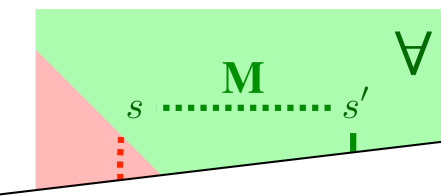
(3) if $s' \xrightarrow{F}{}' t'$ for some $F \in \mathcal{F}$ then $s \,\mathbf{M}\, t'$.

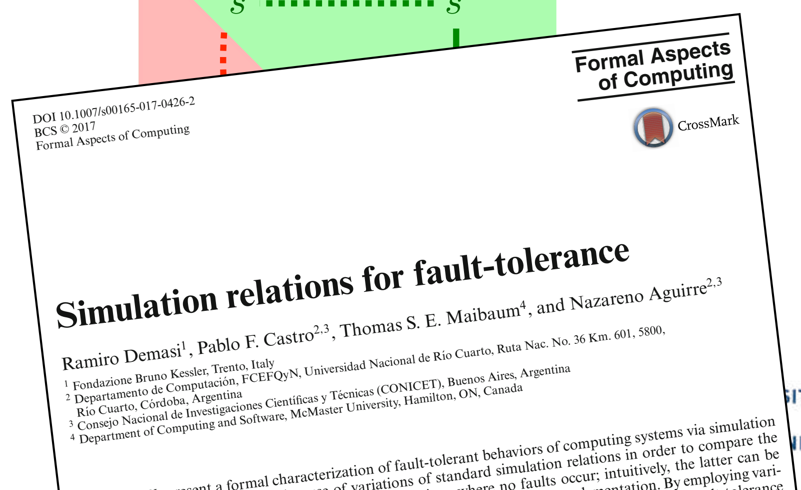
Just like bisimulation

If such a relation exists we say that A' is a *strong masking fault-tolerant implementation* of A, denoted by $A \preceq_m A'$.








DOI 10.1007/s00165-017-0426-2
BCS © 2017
Formal Aspects of Computing

Formal Aspects of Computing

CrossMark

Simulation relations for fault-tolerance

Ramiro Demasi[1], Pablo F. Castro[2,3], Thomas S. E. Maibaum[4], and Nazareno Aguirre[2,3]

[1] Fondazione Bruno Kessler, Trento, Italy
[2] Departamento de Computación, FCEFQyN, Universidad Nacional de Río Cuarto, Ruta Nac. No. 36 Km. 601, 5800, Río Cuarto, Córdoba, Argentina
[3] Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Buenos Aires, Argentina
[4] Department of Computing and Software, McMaster University, Hamilton, ON, Canada

Abstract. We present a formal characterization of fault-tolerant behaviors of computing systems via simulation

CONICET

Strong Masking Simulation

```
module NOMINAL

  b : [0..1] init 0;

  [w0]   true -> (b' = 0);
  [w1]   true -> (b' = 1);
  [r0]   b=0  -> true;
  [r1]   b=1  -> true;

endmodule
```

```
module FAULTY

  v : [0..3] init 0;

  [w0]     true -> (v' = 0);
  [w1]     true -> (v' = 3);
  [r0]     v<=1 -> true;
  [r1]     v>=2 -> true;
  [fault] v<3  -> (v' = v+1);
  [fault] v>0  -> (v' = v-1);

endmodule
```

$$\texttt{NOMINAL} \not\preceq_m \texttt{FAULTY}$$

Strong Masking Simulation

```
module NOMINAL

  b : [0..1] init 0;

  [w0]   true -> (b' = 0);
  [w1]   true -> (b' = 1);
  [r0]   b=0  -> true;
  [r1]   b=1  -> true;

endmodule
```

```
module FAULTY_BOUNDED

  v : [0..3] init 0;
  f : [0..1] init 0;

  [w0]    true -> (v' = 0);
  [w1]    true -> (v' = 3);
  [r0]    v<=1 -> true;
  [r1]    v>=2 -> true;
  [fault] (v<3) & (f<1) -> (v' = v+1) &
                           (f' = f+1);
  [fault] (v>0) & (f<1) -> (v' = v-1) &
                           (f' = f+1);

endmodule
```

$$\mathbf{M} = \{\langle b, (v, f)\rangle \mid 2b \leq v \leq 2b + 1\}$$

$$\texttt{NOMINAL} \preceq_m \texttt{FAULTY\_BOUNDED}$$

Weak Masking Simulation

Definition 3.2. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ be two transition systems with Σ possibly containing τ. A' is *weak masking fault-tolerant* with respect to A if there is a relation $\mathbf{M} \subseteq S \times S'$ between A and A' such that:

(A) $s_0 \, \mathbf{M} \, s'_0$

(B) for all $s \in S, s' \in S'$ with $s \, \mathbf{M} \, s'$ and all $e \in \Sigma \cup \{\tau\}$ the following holds:

(1) if $s \xrightarrow{e} t$ then $\exists \, t' \in S' : s' \stackrel{e}{\Rightarrow}' t' \wedge t \, \mathbf{M} \, t'$;

(2) if $s' \xrightarrow{e}' t'$ then $\exists \, t \in S : s \stackrel{e}{\Rightarrow} t \wedge t \, \mathbf{M} \, t'$;

(3) if $s' \xrightarrow{F}' t'$ for some $F \in \mathcal{F}$ then $s \, \mathbf{M} \, t'$.

If such a relation exists, we say that A' is a *weak masking fault-tolerant implementation* of A, denoted by $A \preceq^w_m A'$.

CONICET UNC UNIVERSITÄT DES SAARLANDES

Weak Masking Simulation

Equivalently

Definition 3.2. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ be two transition systems with Σ possibly containing τ. A' is *weak masking fault-tolerant* with respect to A if there is a relation $\mathbf{M} \subseteq S \times S'$ between A and A' such that:

(A) $s_0 \, \mathbf{M} \, s'_0$

(B) for all $s \in S, s' \in S'$ with $s \, \mathbf{M} \, s'$ and all $e \in \Sigma \cup \{\tau\}$ the following holds:

  (1) if $s \stackrel{e}{\Rightarrow} t$ then $\exists\, t' \in S' : s' \stackrel{e}{\Rightarrow}' t' \wedge t \, \mathbf{M} \, t'$;

  (2) if $s' \stackrel{e}{\Rightarrow}' t'$ then $\exists\, t \in S : s \stackrel{e}{\Rightarrow} t \wedge t \, \mathbf{M} \, t'$;

  (3) if $s' \xrightarrow{F}' t'$ for some $F \in \mathcal{F}$ then $s \, \mathbf{M} \, t'$.

If such a relation exists, we say that A' is a *weak masking fault-tolerant implementation* of A, denoted by $A \preceq_m^w A'$.

Hence,
every result for strong also applies to weak by replacing de strong transition relation by the weak one (except for faults)

CONICET UNC UNIVERSITÄT DES SAARLANDES

Masking Simulation Game

Definition 3.5. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ two transition systems. The *strong masking game graph* $\mathcal{G}_{A,A'} = \langle V^G, V_{\mathrm{R}}, V_{\mathrm{V}}, E^G, {v_0}^G \rangle$ for two players is defined as follows:

- $V^G = (S \times (\Sigma^1 \cup \Sigma^2_{\mathcal{F}} \cup \{\#\}) \times S' \times \{\mathrm{R}, \mathrm{V}\}) \cup \{v_{err}\}$
- The initial state is $v_0^G = \langle s_0, \#, s'_0, \mathrm{R} \rangle$, where the Refuter starts playing
- The Refuter's states are $V_{\mathrm{R}} = \{(s, \#, s', \mathrm{R}) \mid s \in S \wedge s' \in S'\} \cup \{v_{err}\}$
- The Verifier's states are $V_{\mathrm{V}} = \{(s, \sigma, s', \mathrm{V}) \mid s \in S \wedge s' \in S' \wedge \sigma \in (\Sigma^1 \cup \Sigma^2_{\mathcal{F}})\}$

and E^G is the minimal set satisfying:

- $\{((s, \#, s', \mathrm{R}), (t, \sigma^1, s', \mathrm{V})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \#, s', \mathrm{R}), (s, \sigma^2, t', \mathrm{V})) \mid \exists\, \sigma \in \Sigma_{\mathcal{F}} : s' \xrightarrow{\sigma}' t'\} \subseteq E^G$,
- $\{((s, \sigma^2, s', \mathrm{V}), (t, \#, s', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \sigma^1, s', \mathrm{V}), (s, \#, t', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s' \xrightarrow{\sigma}' t'\} \subseteq E^G$,
- $\{((s, F^2, s', \mathrm{V}), (s, \#, s', \mathrm{R}))\} \subseteq E^G$, for any $F \in \mathcal{F}$.
- If there is no outgoing transition from some state v, then, we additionally assume $(v, v_{err}) \in E^G$ and $(v_{err}, v_{err}) \in E^G$.

Masking Simulation Game

Definition 3.5. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ two transition systems. The *strong masking game graph* $\mathcal{G}_{A,A'} = \langle V^G, V_{\mathrm{R}}, V_{\mathrm{V}}, E^G, {v_0}^G \rangle$ for two players is defined as follows:

- $V^G = (S \times (\Sigma^1 \cup \Sigma^2_{\mathcal{F}} \cup \{\#\}) \times S' \times \{\mathrm{R}, \mathrm{V}\}) \cup \{v_{err}\}$
- The initial state is $v_0^G = \langle s_0, \#, s'_0, \mathrm{R} \rangle$, where the Refuter starts playing
- The Refuter's states are $V_{\mathrm{R}} = \{(s, \#, s', \mathrm{R}) \mid s \in S \land s' \in S'\} \cup \{v_{err}\}$
- The Verifier's states are $V_{\mathrm{V}} = \{(s, \sigma, s', \mathrm{V}) \mid s \in S \land s' \in S' \land \sigma \in (\Sigma^1 \cup \Sigma^2_{\mathcal{F}})\}$

and E^G is the minimal set satisfying:

- $\{((s, \#, s', \mathrm{R}), (t, \sigma^1, s', \mathrm{V})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \#, s', \mathrm{R}), (s, \sigma^2, t', \mathrm{V})) \mid \exists\, \sigma \in \Sigma_{\mathcal{F}} : s' \xrightarrow{\sigma}{}' t'\} \subseteq E^G$,
- $\{((s, \sigma^2, s', \mathrm{V}), (t, \#, s', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \sigma^1, s', \mathrm{V}), (s, \#, t', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s' \xrightarrow{\sigma}{}' t'\} \subseteq E^G$,
- $\{((s, F^2, s', \mathrm{V}), (s, \#, s', \mathrm{R}))\} \subseteq E^G$, for any $F \in \mathcal{F}$.
- If there is no outgoing transition from some state v, then, we additionally assume $(v, v_{err}) \in E^G$ and $(v_{err}, v_{err}) \in E^G$.

CONICET
UNC
UNIVERSITÄT DES SAARLANDES

Masking Simulation Game

Definition 3.5. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ two transition systems. The *strong masking game graph* $\mathcal{G}_{A,A'} = \langle V^G, V_{\mathrm{R}}, V_{\mathrm{V}}, E^G, {v_0}^G \rangle$ for two players is defined as follows:

- $V^G = (S \times (\Sigma^1 \cup \Sigma^2_{\mathcal{F}} \cup \{\#\}) \times S' \times \{\mathrm{R}, \mathrm{V}\}) \cup \{v_{err}\}$
- The initial state is $v_0^G = \langle s_0, \#, s'_0, \mathrm{R} \rangle$, where the Refuter starts playing
- The Refuter's states are $V_{\mathrm{R}} = \{(s, \#, s', \mathrm{R}) \mid s \in S \wedge s' \in S'\} \cup \{v_{err}\}$
- The Verifier's states are $V_{\mathrm{V}} = \{(s, \sigma, s', \mathrm{V}) \mid s \in S \wedge s' \in S' \wedge \sigma \in (\Sigma^1 \cup \Sigma^2_{\mathcal{F}})\}$

and E^G is the minimal set satisfying:

- $\{((s, \#, s', \mathrm{R}), (t, \sigma^1, s', \mathrm{V})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \#, s', \mathrm{R}), (s, \sigma^2, t', \mathrm{V})) \mid \exists\, \sigma \in \Sigma_{\mathcal{F}} : s' \xrightarrow{\sigma}{}' t'\} \subseteq E^G$,
- $\{((s, \sigma^2, s', \mathrm{V}), (t, \#, s', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \sigma^1, s', \mathrm{V}), (s, \#, t', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s' \xrightarrow{\sigma}{}' t'\} \subseteq E^G$,
- $\{((s, F^2, s', \mathrm{V}), (s, \#, s', \mathrm{R}))\} \subseteq E^G$, for any $F \in \mathcal{F}$.
- If there is no outgoing transition from some state v, then, we additionally assume $(v, v_{err}) \in E^G$ and $(v_{err}, v_{err}) \in E^G$.

Masking Simulation Game

Definition 3.5. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ two transition systems. The *strong masking game graph* $\mathcal{G}_{A,A'} = \langle V^G, V_{\mathrm{R}}, V_{\mathrm{V}}, E^G, {v_0}^G \rangle$ for two players is defined as follows:

- $V^G = (S \times (\Sigma^1 \cup \Sigma^2_{\mathcal{F}} \cup \{\#\}) \times S' \times \{\mathrm{R}, \mathrm{V}\}) \cup \{v_{err}\}$
- The initial state is $v_0^G = \langle s_0, \#, s'_0, \mathrm{R} \rangle$, where the Refuter starts playing
- The Refuter's states are $V_{\mathrm{R}} = \{(s, \#, s', \mathrm{R}) \mid s \in S \wedge s' \in S'\} \cup \{v_{err}\}$
- The Verifier's states are $V_{\mathrm{V}} = \{(s, \sigma, s', \mathrm{V}) \mid s \in S \wedge s' \in S' \wedge \sigma \in (\Sigma^1 \cup \Sigma^2_{\mathcal{F}})\}$

and E^G is the minimal set satisfying:

- $\{((s, \#, s', \mathrm{R}), (t, \sigma^1, s', \mathrm{V})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \#, s', \mathrm{R}), (s, \sigma^2, t', \mathrm{V})) \mid \exists\, \sigma \in \Sigma_{\mathcal{F}} : s' \xrightarrow{\sigma}' t'\} \subseteq E^G$,
- $\{((s, \sigma^2, s', \mathrm{V}), (t, \#, s', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \sigma^1, s', \mathrm{V}), (s, \#, t', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s' \xrightarrow{\sigma}' t'\} \subseteq E^G$,
- $\{((s, F^2, s', \mathrm{V}), (s, \#, s', \mathrm{R}))\} \subseteq E^G$, for any $F \in \mathcal{F}$.
- If there is no outgoing transition from some state v, then, we additionally assume $(v, v_{err}) \in E^G$ and $(v_{err}, v_{err}) \in E^G$.

Masking Simulation Game

Definition 3.5. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ two transition systems. The *strong masking game graph* $\mathcal{G}_{A,A'} = \langle V^G, V_{\mathrm{R}}, V_{\mathrm{V}}, E^G, {v_0}^G \rangle$ for two players is defined as follows:

- $V^G = (S \times (\Sigma^1 \cup \Sigma^2_{\mathcal{F}} \cup \{\#\}) \times S' \times \{\mathrm{R}, \mathrm{V}\}) \cup \{v_{err}\}$
- The initial state is $v_0^G = \langle s_0, \#, s'_0, \mathrm{R} \rangle$, where the Refuter starts playing
- The Refuter's states are $V_{\mathrm{R}} = \{(s, \#, s', \mathrm{R}) \mid s \in S \wedge s' \in S'\} \cup \{v_{err}\}$
- The Verifier's states are $V_{\mathrm{V}} = \{(s, \sigma, s', \mathrm{V}) \mid s \in S \wedge s' \in S' \wedge \sigma \in (\Sigma^1 \cup \Sigma^2_{\mathcal{F}})\}$

and E^G is the minimal set satisfying:

- $\{((s, \#, s', \mathrm{R}), (t, \sigma^1, s', \mathrm{V})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \#, s', \mathrm{R}), (s, \sigma^2, t', \mathrm{V})) \mid \exists\, \sigma \in \Sigma_{\mathcal{F}} : s' \xrightarrow{\sigma}{}' t'\} \subseteq E^G$,
- $\{((s, \sigma^2, s', \mathrm{V}), (t, \#, s', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \sigma^1, s', \mathrm{V}), (s, \#, t', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s' \xrightarrow{\sigma}{}' t'\} \subseteq E^G$,
- $\{((s, F^2, s', \mathrm{V}), (s, \#, s', \mathrm{R}))\} \subseteq E^G$, for any $F \in \mathcal{F}$.
- If there is no outgoing transition from some state v, then, we additionally assume $(v, v_{err}) \in E^G$ and $(v_{err}, v_{err}) \in E^G$.

Masking Simulation Game

Definition 3.5. Let $A = \langle S, \Sigma, \rightarrow, s_0 \rangle$ and $A' = \langle S', \Sigma_{\mathcal{F}}, \rightarrow', s'_0 \rangle$ two transition systems. The *strong masking game graph* $\mathcal{G}_{A,A'} = \langle V^G, V_{\mathrm{R}}, V_{\mathrm{V}}, E^G, {v_0}^G \rangle$ for two players is defined as follows:

- $V^G = (S \times (\Sigma^1 \cup \Sigma^2_{\mathcal{F}} \cup \{\#\}) \times S' \times \{\mathrm{R}, \mathrm{V}\}) \cup \{v_{err}\}$
- The initial state is $v_0^G = \langle s_0, \#, s'_0, \mathrm{R} \rangle$, where the Refuter starts playing
- The Refuter's states are $V_{\mathrm{R}} = \{(s, \#, s', \mathrm{R}) \mid s \in S \wedge s' \in S'\} \cup \{v_{err}\}$
- The Verifier's states are $V_{\mathrm{V}} = \{(s, \sigma, s', \mathrm{V}) \mid s \in S \wedge s' \in S' \wedge \sigma \in (\Sigma^1 \cup \Sigma^2_{\mathcal{F}})\}$

and E^G is the minimal set satisfying:

- $\{((s, \#, s', \mathrm{R}), (t, \sigma^1, s', \mathrm{V})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \#, s', \mathrm{R}), (s, \sigma^2, t', \mathrm{V})) \mid \exists\, \sigma \in \Sigma_{\mathcal{F}} : s' \xrightarrow{\sigma}' t'\} \subseteq E^G$,
- $\{((s, \sigma^2, s', \mathrm{V}), (t, \#, s', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s \xrightarrow{\sigma} t\} \subseteq E^G$,
- $\{((s, \sigma^1, s', \mathrm{V}), (s, \#, t', \mathrm{R})) \mid \exists\, \sigma \in \Sigma : s' \xrightarrow{\sigma}' t'\} \subseteq E^G$,
- $\{((s, F^2, s', \mathrm{V}), (s, \#, s', \mathrm{R}))\} \subseteq E^G$, for any $F \in \mathcal{F}$.
- If there is no outgoing transition from some state v, then, we additionally assume $(v, v_{err}) \in E^G$ and $(v_{err}, v_{err}) \in E^G$.

We are in the presence of a masking simulation iff the Verifier has a winning strategy (i.e. the Refuter is not able to lead the Verifier to the error state)

Masking Simulation Game (Algorithm)

Definition 3.9. Given a strong masking game graph $\mathcal{G}_{A,A'}$, the sets U_i^j (for $i, j \geq 0$) are defined as follows:

$$U_i^0 = U_0^j = \emptyset,$$

$$U_1^1 = \{v_{err}\},$$

$$U_{i+1}^{j+1} = \{v' \mid v' \in V_{\mathrm{R}} \wedge \mathrm{post}(v') \cap U_{i+1}^j \neq \emptyset\}$$
$$\cup \{v' \mid v' \in V_{\mathrm{V}} \wedge \mathrm{post}(v') \subseteq \bigcup_{i' \leq i+1, j' \leq j} U_{i'}^{j'} \wedge \mathrm{post}(v') \cap U_{i+1}^j \neq \emptyset \wedge \mathrm{pr}_1(v') \notin \mathcal{F}\}$$
$$\cup \{v' \mid v' \in V_{\mathrm{V}} \wedge \mathrm{post}(v') \subseteq \bigcup_{i' \leq i, j' \leq j} U_{i'}^{j'} \wedge \mathrm{post}(v') \cap U_i^j \neq \emptyset \wedge \mathrm{pr}_1(v') \in \mathcal{F}\}$$

Furthermore, $U^k = \bigcup_{i \geq 0} U_i^k$ and $U = \bigcup_{k \geq 0} U^k$.

Fix-point calculation

Lemma 3.10. *The Refuter has a winning strategy in $\mathcal{G}_{A,A'}$ (or $\mathcal{G}^W_{A,A'}$) iff $v_0^G \in U$*

CONICET

UNC

UNIVERSITÄT DES SAARLANDES

Back to the example

Which solution is better?

```
module NOMINAL

  b : [0..1] init 0;

  [w0]   true -> (b' = 0);
  [w1]   true -> (b' = 1);
  [r0]   b=0  -> true;
  [r1]   b=1  -> true;

endmodule
```

```
module FAULTY

  v : [0..3] init 0;

  [w0]     true -> (v' = 0);
  [w1]     true -> (v' = 3);
  [r0]     v<=1 -> true;
  [r1]     v>=2 -> true;
  [fault] v<3  -> (v' = v+1);
  [fault] v>0  -> (v' = v-1);

endmodule
```

```
module FAULTY

  v : [0..5] init 0;

  [w0]     true -> (v' = 0);
  [w1]     true -> (v' = 5);
  [r0]     v<=2 -> true;
  [r1]     v>=3 -> true;
  [fault] v<5  -> (v' = v+1);
  [fault] v>0  -> (v' = v-1);

endmodule
```

Back to the example

```
module NOMINAL

  b : [0..1] init 0;

  [w0]   true -> (b' = 0);
  [w1]   true -> (b' = 1);
  [r0]   b=0  -> true;
  [r1]   b=1  -> true;

endmodule
```

Which solution is better?

```
module FAULTY_BOUNDED

  v : [0..3] init 0;
  f : [0..1] init 0;

  [w0]    true -> (v' = 0);
  [w1]    true -> (v' = 3);
  [r0]    v<=1 -> true;
  [r1]    v>=2 -> true;
  [fault] (v<3) & (f<1) -> (v' = v+1) &
                           (f' = f+1);
  [fault] (v>0) & (f<1) -> (v' = v-1) &
                           (f' = f+1);

endmodule
```

```
module FAULTY_BOUNDED

  v : [0..5] init 0;
  f : [0..2] init 0;

  [w0]    true -> (v' = 0);
  [w1]    true -> (v' = 5);
  [r0]    v<=2 -> true;
  [r1]    v>=3 -> true;
  [fault] (v<3) & (f<2) -> (v' = v+1) &
                           (f' = f+1);
  [fault] (v>0) & (f<2) -> (v' = v-1) &
                           (f' = f+1);

endmodule
```

Add the counting artifact and check masking simulation

Back to the example

Which solution is better?

Needless to say that this is an ad-hoc solution and prone to error

```
module NOMINAL

  b : [0..1] init 0;

  [w0]   true -> (b' = 0);
  [w1]   true -> (b' = 1);
  [r0]   b=0  -> true;
  [r1]   b=1  -> true;

endmodule
```

```
module FAULTY_BOUNDED

  v : [0..3] init 0;
  f : [0..1] init 0;

  [w0]     true -> (v' = 0);
  [w1]     true -> (v' = 3);
  [r0]     v<=1 -> true;
  [r1]     v>=2 -> true;
  [fault] (v<3) & (f<1) -> (v' = v+1) &
                           (f' = f+1);
  [fault] (v>0) & (f<1) -> (v' = v-1) &
                           (f' = f+1);

endmodule
```

```
module FAULTY_BOUNDED

  v : [0..5] init 0;
  f : [0..2] init 0;

  [w0]     true -> (v' = 0);
  [w1]     true -> (v' = 5);
  [r0]     v<=2 -> true;
  [r1]     v>=3 -> true;
  [fault] (v<3) & (f<2) -> (v' = v+1) &
                           (f' = f+1);
  [fault] (v>0) & (f<2) -> (v' = v-1) &
                           (f' = f+1);

endmodule
```

Add the counting artifact and check masking simulation

CONICET

UNC

UNIVERSITÄT DES SAARLANDES

Quantitative Masking Game

The quantitaive masking game $\mathcal{Q}_{A,A'}$ is defined by extending the masking game with the reward function

$$\mathrm{r}((s,\sigma,s',X)) = \begin{cases} (1,0) & \text{if } \sigma \in \mathcal{F} \\ (0,0) & \text{otherwise} \end{cases} \qquad \mathrm{r}(v_{err}) = (0,1)$$

Take a play $\rho = \rho_0\rho_1\rho_2,\ldots$ and let $\mathrm{r}(\rho_i) = (a_i, b_i)$ for all $i \geq 0$. We define the masking payoff function by:

$$f_m(\rho) = \lim_{n\to\infty} \frac{b_n}{1 + \sum_{i=0}^{n} a_i}$$

CONICET UNC UNIVERSITÄT DES SAARLANDES

Quantitative Masking Game

The quantitaive masking game $\mathcal{Q}_{A,A'}$ is defined by extending the masking game with the reward function

$$\mathrm{r}((s,\sigma,s',X)) = \begin{cases} (1,0) & \text{if } \sigma \in \mathcal{F} \\ (0,0) & \text{otherwise} \end{cases} \qquad \mathrm{r}(v_{err}) = (0,1)$$

Take a play $\rho = \rho_0\rho_1\rho_2,\dots$ and let $\mathrm{r}(\rho_i) = (a_i, b_i)$ for all $i \geq 0$. We define the masking payoff function by:

$$f_m(\rho) = \lim_{n\to\infty} \frac{b_n}{1 + \sum_{i=0}^{n} a_i}$$

$$f_m(\rho) = \begin{cases} 0 & \text{if } v_{err} \text{ is not in } \rho \\ \dfrac{1}{\text{number of faults before } v_{err}} & \text{otherwise} \end{cases}$$

Quantitative Masking Game

The masking distance is defined by the value of the game:

$$\begin{aligned}\delta_m(A, A') \stackrel{\text{def}}{=} \text{val}(\mathcal{Q}_{A,A'}) &= \inf_{\pi_V \in \Pi_V} \sup_{\pi_R \in \Pi_R} f_m(\text{out}(\pi_R, \pi_V)) \\ &= \sup_{\pi_R \in \Pi_R} \inf_{\pi_V \in \Pi_V} f_m(\text{out}(\pi_R, \pi_V))\end{aligned}$$

CONICET UNC UNIVERSITÄT DES SAARLANDES

Quantitative Masking Game

The masking distance is defined by the value of the game:

$$\delta_m(A, A') \stackrel{\text{def}}{=} \text{val}(\mathcal{Q}_{A,A'}) = \inf_{\pi_V \in \Pi_V} \sup_{\pi_R \in \Pi_R} f_m(\text{out}(\pi_R, \pi_V))$$

$$= \sup_{\pi_R \in \Pi_R} \inf_{\pi_V \in \Pi_V} f_m(\text{out}(\pi_R, \pi_V))$$

this equality is guaranteed by a theorem

Theorem: $\delta_m(A, A') = 0$ iff $A \preceq_m A'$

Quantitative Masking Game (algorithm)

Definition 3.9. Given a strong masking game graph $\mathcal{G}_{A,A'}$, the sets U_i^j (for $i, j \geq 0$) are defined as follows:

$$U_i^0 = U_0^j = \emptyset,$$

$$U_1^1 = \{v_{err}\},$$

$$U_{i+1}^{j+1} = \{v' \mid v' \in V_{\mathrm{R}} \wedge \mathrm{post}(v') \cap U_{i+1}^{j} \neq \emptyset\}$$

$$\cup \{v' \mid v' \in V_{\mathrm{V}} \wedge \mathrm{post}(v') \subseteq \bigcup_{i' \leq i+1, j' \leq j} U_{i'}^{j'} \wedge \mathrm{post}(v') \cap U_{i+1}^{j} \neq \emptyset \wedge \mathrm{pr}_1(v') \notin \mathcal{F}\}$$

$$\cup \{v' \mid v' \in V_{\mathrm{V}} \wedge \mathrm{post}(v') \subseteq \bigcup_{i' \leq i, j' \leq j} U_{i'}^{j'} \wedge \mathrm{post}(v') \cap U_{i}^{j} \neq \emptyset \wedge \mathrm{pr}_1(v') \in \mathcal{F}\}$$

Furthermore, $U^k = \bigcup_{i \geq 0} U_i^k$ and $U = \bigcup_{k \geq 0} U^k$.

Quantitative Masking Game (algorithm)

Definition 3.9. Given a strong masking game graph $\mathcal{G}_{A,A'}$, the sets U_i^j (for $i, j \geq 0$) are defined as follows:

indicates that the error state is reached after at most *i*-1 faults

$$U_i^0 = U_0^j = \emptyset,$$

$$U_1^1 = \{v_{err}\},$$

$$U_{i+1}^{j+1} = \{v' \mid v' \in V_{\mathrm{R}} \wedge \mathrm{post}(v') \cap U_{i+1}^j \neq \emptyset\}$$
$$\cup \{v' \mid v' \in V_{\mathrm{V}} \wedge \mathrm{post}(v') \subseteq \textstyle\bigcup_{i' \leq i+1, j' \leq j} U_{i'}^{j'} \wedge \mathrm{post}(v') \cap U_{i+1}^j \neq \emptyset \wedge \mathrm{pr}_1(v') \notin \mathcal{F}\}$$
$$\cup \{v' \mid v' \in V_{\mathrm{V}} \wedge \mathrm{post}(v') \subseteq \textstyle\bigcup_{i' \leq i, j' \leq j} U_{i'}^{j'} \wedge \mathrm{post}(v') \cap U_i^j \neq \emptyset \wedge \mathrm{pr}_1(v') \in \mathcal{F}\}$$

Furthermore, $U^k = \bigcup_{i \geq 0} U_i^k$ and $U = \bigcup_{k \geq 0} U^k$.

Quantitative Masking Game (algorithm)

Definition 3.9. Given a strong masking game graph $\mathcal{G}_{A,A'}$, the sets U_i^j (for $i, j \geq 0$) are defined as follows:

$$U_i^0 = U_0^j = \emptyset,$$

$$U_1^1 = \{v_{err}\},$$

$$U_{i+1}^{j+1} = \{v' \mid v' \in V_R \wedge \text{post}(v') \cap U_{i+1}^j \neq \emptyset\}$$

$$\cup \{v' \mid v' \in V_V \wedge \text{post}(v') \subseteq \textstyle\bigcup_{i' \leq i+1, j' \leq j} U_{i'}^{j'} \wedge \text{post}(v') \cap U_{i+1}^j \neq \emptyset \wedge \text{pr}_1(v') \notin \mathcal{F}\}$$

$$\cup \{v' \mid v' \in V_V \wedge \text{post}(v') \subseteq \textstyle\bigcup_{i' \leq i, j' \leq j} U_{i'}^{j'} \wedge \text{post}(v') \cap U_i^j \neq \emptyset \wedge \text{pr}_1(v') \in \mathcal{F}\}$$

Furthermore, $U^k = \bigcup_{i \geq 0} U_i^k$ and $U = \bigcup_{k \geq 0} U^k$.

indicates that the error state is reached after at most i-1 faults

Theorem:

$$\delta_m(A, A') = \begin{cases} \dfrac{1}{\min\{i \mid v_0^G \in U_i^j\}} & \text{if } v_0^G \in U \\ 0 & \text{otherwise} \end{cases}$$

CONICET UNC UNIVERSITÄT DES SAARLANDES

Everybody loves tables!

- Tool MaskD (developed by Luciano)
- Complexity (general):

  $\mathcal{O}(|E^G| * \log |V^G|)$

- Weak case requires reflexive-transitive construction, so add

  $\mathcal{O}(\max(|S|, |S'|)^{2.3727})$

- Complexity (deterministic)

  $\mathcal{O}(|E^G|)$

Shortest weighted path

Case Study	Redundancy	Masking Distance	Time	Time(Det)
Redundant Memory Cell	3 bits	0.333	0.7s	0.6s
	5 bits	0.25	2.5s	1.9s
	7 bits	0.2	7.2s	5.7s
	9 bits	0.167	1m.4s	1m11s
	11 bits	0.143	28m27s	26m10s
N-Modular Redundancy	3 modules	0.333	0.6s	0.5s
	5 modules	0.25	1.2s	0.7s
	7 modules	0.2	5.6s	3.8s
	9 modules	0.167	2m55s	2m32s
	11 modules	0.143	75m17s	72m48s
Dining Philosophers	2 phils	0.5	0.6s	0.6s
	3 phils	0.333	1.9s	0.9s
	4 phils	0.25	5.9s	2.6s
	5 phils	0.2	25.3s	24.1s
	6 phils	0.167	19m.23s	11m39s
Byzantine Generals	3 generals	0.5	0.9s	–
	4 generals	0.333	17.1s	–
	5 generals	0.333	429m54s	–
Raft LRCC (5)	1 follower	0	0.7s	0.8s
	2 followers	0	5.6s	3.6s
	3 followers	0	49m.50s	37m.53s
BRP(1)	1 retransm.	0.333	0.7s	–
	5 retransm.	0.143	0.8s	–
	10 retransm.	0.083	1.3s	–
	20 retransm.	0.045	3.9s	–
	40 retransm.	0.024	4.8s	–
BRP(5)	1 retransm.	0.333	4.2s	–
	5 retransm.	0.143	4.8s	–
	10 retransm.	0.083	6.1s	–
	20 retransm.	0.045	8.7s	–
	40 retransm.	0.024	18.6s	–
BRP(10)	1 retransm.	0.333	4.7s	–
	5 retransm.	0.143	6.4s	–
	10 retransm.	0.083	10.1s	–
	20 retransm.	0.045	20.5s	–
	40 retransm.	0.024	1m.9s	–

CONICET

Measuring Masking Fault-Tolerance

Pablo F. Castro, Pedro R. D'Argenio, Ramiro Demasi, Luciano Putruele

Dependable Systems dTime Talks
October, 2020