

Non-Interference for Multi-Agent Workflows

Helmut Seidl

Joint work with:

Christian Müller, Bernd Finkbeiner

TU München + U. des Saarlandes

MOD 2019

Lecture 3:

Noninterference via Abstraction

\forall^* FOL as Abstract Domain

Monadic predicates are not enough.

\forall^* FOL as Abstract Domain

Monadic predicates are not enough.

Desirable Invariants

$$\forall x_1, x_2, p, d. \text{Discuss}(a, x, p, d) \leftrightarrow \text{Discuss}'(a, x, p, d)$$

\forall^* FOL as Abstract Domain

Monadic predicates are not enough.

Desirable Invariants

$$\forall x_1, x_2, p, d. \text{Discuss}(a, x, p, d) \leftrightarrow \text{Discuss}'(a, x, p, d)$$

Inference

- ▶ eliminate $\forall A$
- ▶ deal with $\exists x$
- ▶ deal with non-termination

Universal SO-QE

Good News

$$\forall A. F \vee Ax \vee \neg Ay$$

Universal SO-QE

Good News

$$\forall A. F \vee Ax \vee \neg Ay \equiv F \vee (x = y)$$

Universal SO-QE

Good News

$$\forall A. F \vee Ax \vee \neg Ay \equiv F \vee (x = y)$$

Generalization

$$\forall A. F \vee (\exists x. Ayx \wedge G) \vee \neg Azx'$$

Universal SO-QE

Good News

$$\forall A. F \vee Ax \vee \neg Ay \equiv F \vee (x = y)$$

Generalization

$$\begin{aligned} \forall A. F \vee (\exists x. Ayx \wedge G) \vee \neg Azx' \\ \equiv F \vee (y = z) \wedge G[x'/x] \end{aligned}$$

Application: Guarded Substitutions

Only entries

$$Ry := \phi$$

Application: Guarded Substitutions

Only entries

$$Ry := \phi \quad \text{or}$$

$$Ry := \exists x. Azx \wedge \phi$$

Application: Guarded Substitutions

Only entries

$$Ry := \phi \quad \text{or}$$

$$Ry := \exists x. Azx \wedge \phi \quad \text{or}$$

$$Ry := Ry \vee \exists x. Azx \wedge \phi$$

// ϕ quantifierfree

Application: Guarded Substitutions

Only entries

$$Ry := \phi \quad \text{or}$$

$$Ry := \exists x. A_z x \wedge \phi \quad \text{or}$$

$$Ry := Ry \vee \exists x. A_z x \wedge \phi$$

// ϕ quantifierfree

$$\begin{aligned} \text{Discuss}(x_1, x_2, p, d) &:= \exists r_1 r_2. \\ &A_4(x_2, x_1, p, d, r_1, r_1) \wedge \\ &\text{Report}(x_1, p, r_1) \wedge \\ &\text{Report}(x_2, p, r_2) \end{aligned}$$

... is guarded!

Application to Invariant Generation

$$\psi = \forall x, y. \neg S(a, x) \vee \neg R(x, y) \vee S(a, y)$$

Application to Invariant Generation

$$\psi = \forall x, y. \neg S(a, x) \vee \neg R(x, y) \vee S(a, y)$$

$$\theta = \{ S(y_1, y_2) := S(y_1, Sy_2) \vee \\ \exists z. A(y_1, y_2, z) \wedge T(y_1, y_2, z) \}$$

Application to Invariant Generation

$$\psi = \forall x, y. \neg S(a, x) \vee \neg R(x, y) \vee S(a, y)$$

$$\theta = \{ S(y_1, y_2) := S(y_1, Sy_2) \vee \\ \exists z. A(y_1, y_2, z) \wedge T(y_1, y_2, z) \}$$

$$\forall A. (\psi\theta) = \forall A, x, y, z. \neg R(x, y) \vee S(a, y) \vee$$

Application to Invariant Generation

$$\psi = \forall x, y. \neg S(a, x) \vee \neg R(x, y) \vee S(a, y)$$

$$\theta = \{ S(y_1, y_2) := S(y_1, Sy_2) \vee \\ \exists z. A(y_1, y_2, z) \wedge T(y_1, y_2, z) \}$$

$$\forall A. (\psi\theta) = \forall A, x, y, z. \neg R(x, y) \vee S(a, y) \vee \\ \neg S(a, x) \wedge (\neg A(a, x, z) \vee \neg T(a, x, z)) \vee$$

Application to Invariant Generation

$$\psi = \forall x, y. \neg S(a, x) \vee \neg R(x, y) \vee S(a, y)$$

$$\theta = \{ S(y_1, y_2) := S(y_1, Sy_2) \vee \\ \exists z. A(y_1, y_2, z) \wedge T(y_1, y_2, z) \}$$

$$\forall A. (\psi\theta) = \forall A, x, y, z. \neg R(x, y) \vee S(a, y) \vee \\ \neg S(a, x) \wedge (\neg A(a, x, z) \vee \neg T(a, x, z)) \vee \\ (\exists z. A(a, y, z) \wedge T(a, y, z))$$

Application to Invariant Generation

$$\psi = \forall x, y. \neg S(a, x) \vee \neg R(x, y) \vee S(a, y)$$

$$\theta = \{ S(y_1, y_2) := S(y_1, Sy_2) \vee \\ \exists z. A(y_1, y_2, z) \wedge T(y_1, y_2, z) \}$$

$$\forall A. (\psi\theta) = \forall A, x, y, z. \neg R(x, y) \vee S(a, y) \vee \\ \neg S(a, x) \wedge (\neg A(a, x, z) \vee \neg T(a, x, z)) \vee \\ (\exists z. A(a, y, z) \wedge T(a, y, z))$$

$$= \forall x, y, z. \neg R(x, y) \vee S(a, y) \vee \\ \neg S(a, x) \wedge (\neg T(a, x, z) \vee (x = y))$$

Application to Invariant Generation

$$\psi = \forall x, y. \neg S(a, x) \vee \neg R(x, y) \vee S(a, y)$$

$$\theta = \{ S(y_1, y_2) := S(y_1, Sy_2) \vee \\ \exists z. A(y_1, y_2, z) \wedge T(y_1, y_2, z) \}$$

$$\begin{aligned} \forall A. (\psi\theta) &= \forall A, x, y, z. \neg R(x, y) \vee S(a, y) \vee \\ &\quad \neg S(a, x) \wedge (\neg A(a, x, z) \vee \neg T(a, x, z)) \vee \\ &\quad (\exists z. A(a, y, z) \wedge T(a, y, z)) \\ &= \forall x, y, z. \neg R(x, y) \vee S(a, y) \vee \\ &\quad \neg S(a, x) \wedge (\neg T(a, x, z) \vee (x = y)) \end{aligned}$$

... will FP iteration terminate?

Question

Are there **infinite** sequences

$$\Psi_0 \leftarrow \Psi_1 \leftarrow \Psi_2 \leftarrow \dots$$

// pairwise inequivalent

Question

Are there infinite sequences

$$\Psi_0 \leftarrow \Psi_1 \leftarrow \Psi_2 \leftarrow \dots$$

// pairwise inequivalent

Yes!

Question

Are there **infinite** sequences

$$\Psi_0 \leftarrow \Psi_1 \leftarrow \Psi_2 \leftarrow \dots$$

// pairwise inequivalent

Yes!

$$\phi_0 \equiv \forall x, y. \neg T(x, y) \vee S(x, y)$$

Question

Are there **infinite** sequences

$$\Psi_0 \leftarrow \Psi_1 \leftarrow \Psi_2 \leftarrow \dots$$

// pairwise inequivalent

Yes!

$$\phi_0 \equiv \forall x, y. \neg T(x, y) \vee S(x, y)$$

$$\phi_1 \equiv \forall x, z_1, y. \neg T(x, z_1) \vee \neg T(z_1, y) \vee S(x, y)$$

Question

Are there infinite sequences

$$\Psi_0 \leftarrow \Psi_1 \leftarrow \Psi_2 \leftarrow \dots$$

// pairwise inequivalent

Yes!

$$\phi_0 \equiv \forall x, y. \neg T(x, y) \vee S(x, y)$$

$$\phi_1 \equiv \forall x, z_1, y. \neg T(x, z_1) \vee \neg T(z_1, y) \vee S(x, y)$$

$$\phi_2 \equiv \forall x, z_1, z_2, y. \neg T(x, z_1) \vee \neg T(z_1, z_2) \vee \neg T(z_2, y) \vee S(x, y)$$

...

Question

Are there **infinite** sequences

$$\Psi_0 \leftarrow \Psi_1 \leftarrow \Psi_2 \leftarrow \dots$$

// pairwise inequivalent

Yes!

$$\phi_0 \equiv \forall x, y. \neg T(x, y) \vee S(x, y)$$

$$\phi_1 \equiv \forall x, z_1, y. \neg T(x, z_1) \vee \neg T(z_1, y) \vee S(x, y)$$

$$\phi_2 \equiv \forall x, z_1, z_2, y. \neg T(x, z_1) \vee \neg T(z_1, z_2) \vee \neg T(z_2, y) \vee S(x, y)$$

...

$$\Psi_h \equiv \phi_1 \wedge \dots \wedge \phi_h$$

Question

Are there infinite sequences

$$\Psi_0 \leftarrow \Psi_1 \leftarrow \Psi_2 \leftarrow \dots$$

// pairwise inequivalent

Yes!

$$\phi_0 \equiv \forall x, y. \neg T(x, y) \vee S(x, y)$$

$$\phi_1 \equiv \forall x, z_1, y. \neg T(x, z_1) \vee \neg T(z_1, y) \vee S(x, y)$$

$$\phi_2 \equiv \forall x, z_1, z_2, y. \neg T(x, z_1) \vee \neg T(z_1, z_2) \vee \neg T(z_2, y) \vee S(x, y)$$

...

$$\Psi_h \equiv \phi_1 \wedge \dots \wedge \phi_h$$

⇒ sequences of strengthenings can be infinite ...

Question

Are there **infinite** sequences

$$\Psi_0 \leftarrow \Psi_1 \leftarrow \Psi_2 \leftarrow \dots$$

// pairwise inequivalent

Yes!

$$\phi_0 \equiv \forall x, y. \neg T(x, y) \vee S(x, y)$$

$$\phi_1 \equiv \forall x, z_1, y. \neg T(x, z_1) \vee \neg T(z_1, y) \vee S(x, y)$$

$$\phi_2 \equiv \forall x, z_1, z_2, y. \neg T(x, z_1) \vee \neg T(z_1, z_2) \vee \neg T(z_2, y) \vee S(x, y)$$

...

$$\Psi_h \equiv \phi_1 \wedge \dots \wedge \phi_h$$

⇒ sequences of strengthenings **can** be infinite ...
besides their conjunction is **FOL definable**.

Gödel 1930

Stratification

- ▶ Often, workflows operate in **levels**
- ▶ Predicates at the next layer only depend on themselves and lower **levels**

Stratification

- ▶ Often, workflows operate in **levels**
- ▶ Predicates at the next layer only depend on themselves and lower **levels**

Example

Author < Conflict
< Assign
< Report
< Discuss

Stratification

- ▶ Often, workflows operate in **levels**
- ▶ Predicates at the next layer only depend on themselves and lower **levels**

Example

Author < Conflict
< Assign
< Report
< Discuss

Guarded stratified — the ϕ are of lower level

Workflow

$\text{Conflict}(x, p) := \text{Author}(x, p) \vee A_2(x, p);$

// A_2 input predicate

$\text{Assign}(x, p) := \neg \text{Conflict}(x, p);$

// strategy of pc chair

$\text{Report}(x, p, r) := \text{Assign}(x, p) \wedge I(x, p, r)$

while (*) $\text{Discuss}(x_1, x_2, p, d) := \exists r_1 r_2.$

$\text{Report}(x_1, p, r_1) \wedge$

$\text{Report}(x_2, p, r_2) \wedge$

$A_4(x_2, x_1, p, d, r_1, r_2)$

Workflow

$\text{Conflict}(x, p) := \text{Author}(x, p) \vee A_2(x, p);$

// A_2 input predicate

$\text{Assign}(x, p) := \neg \text{Conflict}(x, p);$

// strategy of pc chair

$\text{Report}(x, p, r) := \text{Assign}(x, p) \wedge I(x, p, r)$

while (*) $\text{Discuss}(x_1, x_2, p, d) := \exists r_1 r_2.$

$\text{Report}(x_1, p, r_1) \wedge$

$\text{Report}(x_2, p, r_2) \wedge$

$A_4(x_2, x_1, p, d, r_1, r_2)$

... is guarded and stratified!

Central Termination Theorem

Central Termination Theorem

Fixpoint iteration for guarded stratified FOTS terminates.

Central Termination Theorem

Fixpoint iteration for guarded stratified FOTS terminates.

The result is the **weakest** inductive strengthening of /

Central Termination Theorem

Fixpoint iteration for guarded stratified FOTS terminates.

The result is the **weakest** inductive strengthening of I which again is in \forall^* FOL.

Central Termination Theorem

Fixpoint iteration for guarded stratified FOTS terminates.

The result is the **weakest** inductive strengthening of I which again is in \forall^* FOL.

Application to PNID ?

Central Termination Theorem

Fixpoint iteration for guarded stratified FOTS terminates.
The result is the **weakest** inductive strengthening of I
which again is in \forall^* FOL.

Application to PNID ?

\implies **Stubborn** PNID for guarded stratified FOTS is decidable.

PNID with Causal Agents

$$\text{Informed}(x) := \text{Informed}(x) \vee \bigvee_R \exists z. Rxz \not\leftrightarrow R'xz$$

PNID with Causal Agents

$$\text{Informed}(x) := \text{Informed}(x) \vee \bigvee_R \exists z. Rxz \not\leftrightarrow R'xz$$

... cannot be ordered.

PNID with Causal Agents

$$\text{Informed}(x) := \text{Informed}(x) \vee \bigvee_R \exists z. Rxz \not\leftrightarrow R'xz$$

... cannot be ordered.

Modified rule

$$\text{Informed}(x) := A(x)$$

PNID with Causal Agents

$$\text{Informed}(x) := \text{Informed}(x) \vee \bigvee_R \exists z. Rxz \not\leftrightarrow R'xz$$

... cannot be ordered.

Modified rule

$$\text{Informed}(x) := A(x)$$

$$\text{err} := \text{err} \vee \exists x. A(x) \wedge \bigwedge_R \forall z. Rxz \leftrightarrow R'xz$$

PNID with Causal Agents

$$\text{Informed}(x) := \text{Informed}(x) \vee \bigvee_R \exists z. Rxz \not\leftrightarrow R'xz$$

... cannot be ordered.

Modified rule

$$\text{Informed}(x) := A(x)$$

$$\text{err} := \text{err} \vee \exists x. A(x) \wedge \bigwedge_R \forall z. Rxz \leftrightarrow R'xz$$

- ▶ **err** receives highest, **Informed** lowest level
- ▶ Self-composition becomes guarded stratified!

Result

For guarded stratified FOTS, **causal** PNID is decidable.

Result

For guarded stratified FOTS, **causal** PNID is decidable.

Not every FOTS is **guarded stratified**.

⇒ a fallback method is required!

Result

For guarded stratified FOTS, **causal** PNID is decidable.

Not every FOTS is **guarded stratified**.

⇒ a fallback method is required!

Approach

- ▶ **abstract** existentials
- ▶ complement verification attempt with attempt to falsify

Abstracting Existentials

Every $\forall^*\exists^*$ formula can be strengthened \forall^* FOL:

$$\forall x, y. \exists z. R(x, y, z) \quad \leftarrow$$

Abstracting Existentials

Every $\forall^*\exists^*$ formula can be strengthened \forall^* FOL:

$$\forall x, y. \exists z. R(x, y, z) \quad \leftarrow$$

$$\forall x, y. R(x, y, x) \vee R(x, y, y) \vee R(x, y, a)$$

Abstracting Existentials

Every $\forall^*\exists^*$ formula can be strengthened \forall^* FOL:

$$\forall x, y. \exists z. R(x, y, z) \quad \leftarrow \\ \forall x, y. R(x, y, x) \vee R(x, y, y) \vee R(x, y, a)$$

- ▶ Use as Skolem functions x, y and constant a
- ▶ Take the disjunction over the results

Abstracting Existentials

Every $\forall^*\exists^*$ formula can be strengthened \forall^* FOL:

$$\forall x, y. \exists z. R(x, y, z) \quad \leftarrow \\ \forall x, y. R(x, y, x) \vee R(x, y, y) \vee R(x, y, a)$$

- ▶ Use as **Skolem functions** x, y and constant a
- ▶ Take the disjunction over the results

This strengthening is the **best** possible — at least for formulas from $\forall^*\exists^*$ FOL.

Disproving Invariant

Symbolic Execution for Universes up to Size h

Disproving Invariant

Symbolic Execution for Universes up to Size h

- ▶ Introduce FO variables $y_1 \dots y_h$;

Disproving Invariant

Symbolic Execution for Universes up to Size h

- ▶ Introduce FO variables $y_1 \dots y_h$;
- ▶ Replace $\forall x.\phi$ with $\bigwedge_j \phi[y_j/x]$;
- ▶ Replace $\exists x.\phi$ with $\bigvee_j \phi[y_j/x]$;

$$\Psi \equiv \forall x.\exists y.P(x, y)$$

$$\Psi \equiv \forall x. \exists y. P(x, y)$$

becomes

$$\Psi_2^\# \equiv (P(y_1, y_1) \vee P(y_1, y_2)) \wedge (P(y_2, y_1) \vee P(y_2, y_2))$$

$$\Psi \equiv \forall x. \exists y. P(x, y)$$

becomes

$$\Psi_2^\# \equiv (P(y_1, y_1) \vee P(y_1, y_2)) \wedge (P(y_2, y_1) \vee P(y_2, y_2))$$

Neither $\Psi \rightarrow \Psi_2^\#$ nor $\Psi_2^\# \rightarrow \Psi$ holds ...

$$\Psi \equiv \forall x. \exists y. P(x, y)$$

becomes

$$\Psi_2^\# \equiv (P(y_1, y_1) \vee P(y_1, y_2)) \wedge (P(y_2, y_1) \vee P(y_2, y_2))$$

Neither $\Psi \rightarrow \Psi_2^\#$ nor $\Psi_2^\# \rightarrow \Psi$ holds ...

But

$$\Psi \wedge D_2 \leftrightarrow \Psi_2^\# \quad \text{where}$$

$$D_2 \equiv \forall x. (x = y_1) \vee (x = y_2)$$

Disproving Invariant

Symbolic Execution for Universes up to Size h

- ▶ Introduce FO variables $y_1 \dots y_h$;
- ▶ Replace $\forall x.\phi$ with $\bigwedge_j \phi[y_j/x]$;
- ▶ Replace $\exists x.\phi$ with $\bigvee_j \phi[y_j/x]$;

Disproving Invariant

Symbolic Execution for Universes up to Size h

- ▶ Introduce FO variables $y_1 \dots y_h$;
- ▶ Replace $\forall x.\phi$ with $\bigwedge_j \phi[y_j/x]$;
- ▶ Replace $\exists x.\phi$ with $\bigvee_j \phi[y_j/x]$;
- ▶ Iterate

Disproving Invariant

Symbolic Execution for Universes up to Size h

- ▶ Introduce FO variables $y_1 \dots y_h$;
- ▶ Replace $\forall x.\phi$ with $\bigwedge_j \phi[y_j/x]$;
- ▶ Replace $\exists x.\phi$ with $\bigvee_j \phi[y_j/x]$;
- ▶ Iterate
- ▶ Thereby, **eliminate** SO quantifiers ...

Disproving Invariant

Symbolic Execution for Universes up to Size h

- ▶ Introduce FO variables $y_1 \dots y_h$;
- ▶ Replace $\forall x.\phi$ with $\bigwedge_j \phi[y_j/x]$;
- ▶ Replace $\exists x.\phi$ with $\bigvee_j \phi[y_j/x]$;
- ▶ Iterate
- ▶ Thereby, **eliminate** SO quantifiers ...

\implies iteration terminates

\implies invariants in universes upto size h are decidable.

Proving Invariant

- ▶ Keep universal FO quantifiers!
- ▶ Introduce FO variables y_1, \dots, y_h .
Strengthen **existential** FO quantifiers!

$$\psi \equiv \forall x.\exists z.P(x, z)$$

$$\psi \equiv \forall x. \exists z. P(x, z)$$

becomes

$$\psi_{\exists,2}^{\#} \equiv \forall x. P(x, x) \vee P(x, y_1) \vee P(x, y_2)$$

$$\Psi \equiv \forall x. \exists z. P(x, z)$$

becomes

$$\begin{aligned} \Psi_{\exists,2}^{\#} &\equiv \forall x. P(x, x) \vee P(x, y_1) \vee P(x, y_2) \\ &\rightarrow \Psi \end{aligned}$$

$$\Psi \equiv \forall x. \exists z. P(x, z)$$

becomes

$$\begin{aligned} \Psi_{\exists,2}^{\#} &\equiv \forall x. P(x, x) \vee P(x, y_1) \vee P(x, y_2) \\ &\rightarrow \Psi \end{aligned}$$

where

$$\Psi \wedge D_2 \leftrightarrow \Psi_{\exists,2}^{\#} \wedge D_2$$

Proving Invariant

- ▶ Keep universal FO quantifiers!
- ▶ Introduce FO variables y_1, \dots, y_h .
Strengthen **existential** FO quantifiers!

Proving Invariant

- ▶ Keep universal FO quantifiers!
- ▶ Introduce FO variables y_1, \dots, y_h .
Strengthen **existential** FO quantifiers!
- ▶ Iterate!

Proving Invariant

- ▶ Keep universal FO quantifiers!
- ▶ Introduce FO variables y_1, \dots, y_h .
Strengthen **existential** FO quantifiers!
- ▶ Iterate!

⇒ terminates — whenever result is **FO definable**

⇒ either proves invariant or provides counterexample of size $> h$

Proving Invariant

- ▶ Keep universal FO quantifiers!
- ▶ Introduce FO variables y_1, \dots, y_h .
Strengthen **existential** FO quantifiers!
- ▶ Iterate!

⇒ terminates — whenever result is **FO definable**

⇒ either proves invariant or provides counterexample of size $> h$

⇒ **guaranteed** CEGAR loop!

Summary

- ▶ We identified another class of FOTS where MC as well as PNID is decidable.

Summary

- ▶ We identified another class of FOTS where MC as well as PNID is decidable.
- ▶ **Abstraction** of existentials allows to iteratively strengthen universal invariants.
Termination is guaranteed when the resulting infinite conjunction is FO definable.

Summary

- ▶ We identified another class of FOTS where MC as well as PNID is decidable.
- ▶ **Abstraction** of existentials allows to iteratively strengthen universal invariants. Termination is guaranteed when the resulting infinite conjunction is FO definable.
- ▶ **Symbolic evaluation** allows to find/exclude counter examples up to size h .

Summary

- ▶ We identified another class of FOTS where MC as well as PNID is decidable.
- ▶ **Abstraction** of existentials allows to iteratively strengthen universal invariants. Termination is guaranteed when the resulting infinite conjunction is FO definable.
- ▶ **Symbolic evaluation** allows to find/exclude counter examples up to size h .

This enables the construction of a **CEGAR** loop where after each iteration, the attained invariant is guaranteed to hold up to larger universes.