Combination of Uniform Interpolants via Beth Definability

Diego Calvanese[1], **Silvio Ghilardi**[2], Alessandro Gianola[1], Marco Montali[1], Andrey Rivkin[1]

[1] KRDB Research Centre for Knowledge and Data
Free University of Bozen-Bolzano, Italy

[2] Dipartimento di Matematica
Università degli Studi di Milano, Italy

DOCToR 21

July 7, 2021

Outline

Outline

1. Uniform Interpolants: the antefacts
2. Formal Preliminaries
3. Equality Interpolating Condition and Beth Definability
4. The Convex Combined Algorithm
5. The Non-Convex Case: a Counterexample
6. Conclusions

Uniform Interpolants in Propositional Logics

Uniform interpolants were introduced in the context of non-classical logics, starting from the pioneering work by Pitts [1992] who proved that in IPC for every formula $\phi(x, \underline{y})$ there is a formula $\phi_x(\underline{y})$ such that for every further formula $\psi(\underline{y}, \underline{z})$ we have

$$\phi(x, \underline{y}) \vdash \psi(\underline{y}, \underline{z}) \text{ iff } \phi_x(\underline{y}) \vdash \psi(\underline{y}, \underline{z})$$

Uniform Interpolants in Propositional Logics

Uniform interpolants were introduced in the context of non-classical logics, starting from the pioneering work by Pitts [1992] who proved that in IPC for every formula $\phi(x, \underline{y})$ there is a formula $\phi_x(\underline{y})$ such that for every further formula $\psi(\underline{y}, \underline{z})$ we have

$$\phi(x, \underline{y}) \vdash \psi(\underline{y}, \underline{z}) \text{ iff } \phi_x(\underline{y}) \vdash \psi(\underline{y}, \underline{z})$$

In modal logic, uniform interpolants have a *local* and a *global* version, depending on how the entailment $\vdash$ is interpreted.

Uniform Interpolants in Propositional Logics

The local version of uniform interpolation allows an (albeit not faithful) interpretation of the second order propositional calculus into plain propositional calculus, whereas the global version can be used in the axiomatization of model completions for the corresponding classes of algebras.

Uniform Interpolants in Propositional Logics

The local version of uniform interpolation allows an (albeit not faithful) interpretation of the second order propositional calculus into plain propositional calculus, whereas the global version can be used in the axiomatization of model completions for the corresponding classes of algebras.

Uniform interpolants can be sematically connected to some appropriate notion of bisimulation at the level of Kripke models.

Uniform Interpolants in Propositional Logics

The existence of uniform interpolants is an exceptional phenomenon, which is however not so infrequent, as witnessed by a large literature in non-classical logics.

Uniform Interpolants in Propositional Logics

The existence of uniform interpolants is an exceptional phenomenon, which is however not so infrequent, as witnessed by a large literature in non-classical logics.

The main results from the above literature are that uniform interpolants exist for intuitionistic logic and for some modal systems (like the Gödel-Löb system and the S4.Grz system); they do not exist for instance in S4 and K4, whereas for the basic modal system K they exist for the local version but not for the global version (the opposite situation is also well-possible, already in the locally tabular case).

Uniform Interpolants in First Order Theories

In the last decade, also the automated reasoning community (Kapur, Gulwani-Musuvathi) developed an increasing interest in uniform interpolants (sometimes renamed as **covers**), with particular focus on quantifier-free fragments of first-order theories.

Uniform Interpolants in First Order Theories

In the last decade, also the automated reasoning community (Kapur, Gulwani-Musuvathi) developed an increasing interest in uniform interpolants (sometimes renamed as **covers**), with particular focus on quantifier-free fragments of first-order theories.

In such context, uniform interpolants are directly connected with *model completeness* (see below).

Uniform Interpolants in First Order Theories

In the last decade, also the automated reasoning community (Kapur, Gulwani-Musuvathi) developed an increasing interest in uniform interpolants (sometimes renamed as **covers**), with particular focus on quantifier-free fragments of first-order theories.

In such context, uniform interpolants are directly connected with *model completeness* (see below).

Our interest in uniform interpolants for first order theories comes from infinite state model checking applications, in particular from the verification of (Business) Processes enriched with real data (*data-aware processes*).

Verification Applications

Given a state formula ϕ for states $S^{(i)}$, we symbolically define $T^{-1}(S^{(i)})$:

$$Pre(\tau, \phi) \equiv \exists \underline{x}'(\tau(\underline{x}, \underline{x}') \wedge \phi(\underline{x}'))$$

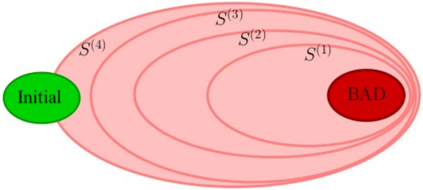
Verification Applications

Given a state formula ϕ for states $S^{(i)}$, we symbolically define $T^{-1}(S^{(i)})$:

$$Pre(\tau, \phi) \equiv \exists \underline{x}' (\tau(\underline{x}, \underline{x}') \wedge \phi(\underline{x}'))$$

Backward-Reachability ($S^{(0)} \equiv$ "bad states")

Safety Check	If $S^{(i)}$ contains an initial, return **unsafe**
Next States	Compute $S^{(i+1)} := S^{(i)} \cup T^{-1}(S^{(i)})$
Fix-Point Check	If $S^{(i+1)} \equiv S^{(i)}$, return **safe**



Verification Applications

Roughly speaking, unsafety of the system means satsifiability of certain existential formulae; thus, one can limit to existentially closed structures and exploit quantifier elimination when model completions exist.

Verification Applications

Roughly speaking, unsafety of the system means satsifiability of certain existential formulae; thus, one can limit to existentially closed structures and exploit quantifier elimination when model completions exist.

This gives a *precise* representation of reachable states, whereas computations of reachable states via ordinary interpolants (McMillan 2006) give overapproximations (to be refined during search).

Verification Applications

Roughly speaking, unsafety of the system means satsifiability of certain existential formulae; thus, one can limit to existentially closed structures and exploit quantifier elimination when model completions exist.

This gives a *precise* representation of reachable states, whereas computations of reachable states via ordinary interpolants (McMillan 2006) give overapproximations (to be refined during search).

Then uniform interpolants enter into the picture. This might be competitive (as witnessed by our MCMT implementation) even from complexity viewpoint, because only a limited fragment of first-order logic is needed to formalize databases with primary and foreign keys. More details in our journal (MSCS 20) and conferences (BPM 19,20,21) papers.

Specific Contributions from this talk

Theories arising in applications are quite rich, they are often modular combinations of theories modeling processes and data.

Specific Contributions from this talk

Theories arising in applications are quite rich, they are often modular combinations of theories modeling processes and data.

- We supply a general algorithm for computing **combined covers** in case of **convex** component theories.

Specific Contributions from this talk

Theories arising in applications are quite rich, they are often modular combinations of theories modeling processes and data.

- We supply a general algorithm for computing **combined covers** in case of **convex** component theories.
- The **hypothesis** under which this algorithm is correct is the same needed to transfer quantifier-free interpolation: the **equality interpolating condition**.

Specific Contributions from this talk

Theories arising in applications are quite rich, they are often modular combinations of theories modeling processes and data.

- We supply a general algorithm for computing **combined covers** in case of **convex** component theories.
- The **hypothesis** under which this algorithm is correct is the same needed to transfer quantifier-free interpolation: the **equality interpolating condition**.
- We prove that the equality interpolating condition is also **necessary** for transferring covers.

Specific Contributions from this talk

Theories arising in applications are quite rich, they are often modular combinations of theories modeling processes and data.

- We supply a general algorithm for computing **combined covers** in case of **convex** component theories.
- The **hypothesis** under which this algorithm is correct is the same needed to transfer quantifier-free interpolation: the **equality interpolating condition**.
- We prove that the equality interpolating condition is also **necessary** for transferring covers.
- The algorithm relies on the extensive use of the **Beth definability property** for primitive fragments.

Specific Contributions from this talk

Theories arising in applications are quite rich, they are often modular combinations of theories modeling processes and data.

- We supply a general algorithm for computing **combined covers** in case of **convex** component theories.
- The **hypothesis** under which this algorithm is correct is the same needed to transfer quantifier-free interpolation: the **equality interpolating condition**.
- We prove that the equality interpolating condition is also **necessary** for transferring covers.
- The algorithm relies on the extensive use of the **Beth definability property** for primitive fragments.
- **Counterexample** showing **non-transfer** of covers for non-convex theories in general, even in case combined quantifier-free interpolants do exist.

Outline

Preliminaries

Definition

Given a FO theory T and two quantifier-free FO formulae $\alpha(\underline{x}, \underline{y})$, $\beta(\underline{y}, \underline{z})$ such that $\vdash_T \alpha \to \beta$, a **quantifier-free** FO formula $\gamma(\underline{y})$ is a **T-quantifier-free interpolant** if $\vdash_T \alpha \to \gamma$ and $\vdash_T \gamma \to \beta$ hold.

Preliminaries

Definition

Given a FO theory T and two quantifier-free FO formulae $\alpha(\underline{x}, \underline{y})$, $\beta(\underline{y}, \underline{z})$ such that $\vdash_T \alpha \to \beta$, a **quantifier-free** FO formula $\gamma(\underline{y})$ is a T-**quantifier-free interpolant** if $\vdash_T \alpha \to \gamma$ and $\vdash_T \gamma \to \beta$ hold.

If every pair $\alpha(\underline{x}, \underline{y}), \beta(\underline{y}, \underline{z})$ has a quantifier-free interpolant, then T enjoys the quantifier-free interpolation property.

Preliminaries

Definition

Given a FO theory T and two quantifier-free FO formulae $\alpha(\underline{x}, \underline{y})$, $\beta(\underline{y}, \underline{z})$ such that $\vdash_T \alpha \to \beta$, a **quantifier-free** FO formula $\gamma(\underline{y})$ is a **T-quantifier-free interpolant** if $\vdash_T \alpha \to \gamma$ and $\vdash_T \gamma \to \beta$ hold.

If every pair $\alpha(\underline{x}, \underline{y}), \beta(\underline{y}, \underline{z})$ has a quantifier-free interpolant, then T enjoys the quantifier-free interpolation property.

Definition

A theory T is *stably infinite* iff every T-satisfiable **constraint** (conjunction of literals) is satisfiable in an **infinite** model of T.

Preliminaries

Definition

Given a FO theory T and two quantifier-free FO formulae $\alpha(\underline{x}, \underline{y})$, $\beta(\underline{y}, \underline{z})$ such that $\vdash_T \alpha \to \beta$, a **quantifier-free** FO formula $\gamma(\underline{y})$ is a **T-quantifier-free interpolant** if $\vdash_T \alpha \to \gamma$ and $\vdash_T \gamma \to \beta$ hold.

If every pair $\alpha(\underline{x}, \underline{y}), \beta(\underline{y}, \underline{z})$ has a quantifier-free interpolant, then T enjoys the quantifier-free interpolation property.

Definition

A theory T is *stably infinite* iff every T-satisfiable **constraint** is satisfiable in an **infinite** model of T.

Definition

A theory T is *convex* iff for every **constraint** δ, if $T \vdash \delta \to \bigvee_{i=1}^{n} x_i = y_i$ then $T \vdash \delta \to x_i = y_i$ holds for some $i \in \{1, ..., n\}$.

A convex theory is 'almost' stably infinite.

Uniform Quantifier-Free Interpolation (Covers)

Fix a theory T and an existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$.

- A quantifier-free (qf) formula $\psi(\underline{y})$ is a T-***uniform (qf) interpolant*** (or, T-***cover***) of $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ iff

Uniform Quantifier-Free Interpolation (Covers)

Fix a theory T and an existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$.

- A quantifier-free (qf) formula $\psi(\underline{y})$ is a T-***uniform (qf) interpolant*** (or, T-***cover***) of $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ iff

  (i) $\psi(\underline{y}) \in Res(\exists \underline{e}\, \phi) := \{\theta(\underline{y}, \underline{z}) \mid T \models \phi(\underline{e}, \underline{y}) \rightarrow \theta(\underline{y}, \underline{z})\}$,

KRDB

Uniform Quantifier-Free Interpolation (Covers)

Fix a theory T and an existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$.

- A quantifier-free (qf) formula $\psi(\underline{y})$ is a T-***uniform (qf) interpolant*** (or, T-***cover***) of $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ iff

  (i) $\psi(\underline{y}) \in Res(\exists \underline{e}\, \phi) := \{\theta(\underline{y}, \underline{z}) \mid T \models \phi(\underline{e}, \underline{y}) \to \theta(\underline{y}, \underline{z})\}$,

  (ii) $\psi(\underline{y})$ implies (modulo T) all the formulae in $Res(\exists \underline{e}\, \phi)$.

Uniform Quantifier-Free Interpolation (Covers)

Fix a theory T and an existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$.

- A quantifier-free (qf) formula $\psi(\underline{y})$ is a T-***uniform (qf) interpolant*** (or, T-***cover***) of $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ iff

  (i) $\psi(\underline{y}) \in Res(\exists \underline{e}\, \phi) := \{\theta(\underline{y}, \underline{z}) \mid T \models \phi(\underline{e}, \underline{y}) \to \theta(\underline{y}, \underline{z})\}$,

  (ii) $\psi(\underline{y})$ implies (modulo T) all the formulae in $Res(\exists \underline{e}\, \phi)$.

  We say that a theory T has *uniform (qf) interpolation* iff every existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ has a T-uniform (qf) interpolant.

Uniform Quantifier-Free Interpolation (Covers)

Fix a theory T and an existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$.

- A quantifier-free (qf) formula $\psi(\underline{y})$ is a T-***uniform (qf) interpolant*** (or, T-***cover***) of $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ iff

  (i) $\psi(\underline{y}) \in Res(\exists \underline{e}\, \phi) := \{\theta(\underline{y}, \underline{z}) \mid T \models \phi(\underline{e}, \underline{y}) \to \theta(\underline{y}, \underline{z})\}$,

  (ii) $\psi(\underline{y})$ implies (modulo T) all the formulae in $Res(\exists \underline{e}\, \phi)$.

  We say that a theory T has *uniform (qf) interpolation* iff every existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ has a T-uniform (qf) interpolant.

- A T-cover is, intuitively, the strongest formula implied by $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$.

Uniform Quantifier-Free Interpolation (Covers)

Fix a theory T and an existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$.

- A quantifier-free (qf) formula $\psi(\underline{y})$ is a T-***uniform (qf) interpolant*** (or, T-***cover***) of $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ iff

  (i) $\psi(\underline{y}) \in Res(\exists \underline{e}\, \phi) := \{\theta(\underline{y}, \underline{z}) \mid T \models \phi(\underline{e}, \underline{y}) \to \theta(\underline{y}, \underline{z})\}$,

  (ii) $\psi(\underline{y})$ implies (modulo T) all the formulae in $Res(\exists \underline{e}\, \phi)$.

  We say that a theory T has *uniform (qf) interpolation* iff every existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ has a T-uniform (qf) interpolant.

- A T-cover is, intuitively, the strongest formula implied by $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$.
- In the cover $\psi(\underline{y})$, the variables $\underline{e}$ have been 'eliminated', in some sense.

Uniform Quantifier-Free Interpolation (Covers)

Fix a theory T and an existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$.

- A quantifier-free (qf) formula $\psi(\underline{y})$ is a T-***uniform (qf) interpolant*** (or, T-***cover***) of $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ iff

  (i) $\psi(\underline{y}) \in Res(\exists \underline{e}\, \phi) := \{\theta(\underline{y}, \underline{z}) \mid T \models \phi(\underline{e}, \underline{y}) \to \theta(\underline{y}, \underline{z})\}$,

  (ii) $\psi(\underline{y})$ implies (modulo T) all the formulae in $Res(\exists \underline{e}\, \phi)$.

  We say that a theory T has *uniform (qf) interpolation* iff every existential formula $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ has a T-uniform (qf) interpolant.
- A T-cover is, intuitively, the strongest formula implied by $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$.
- In the cover $\psi(\underline{y})$, the variables $\underline{e}$ have been 'eliminated', in some sense.
- But, in general, $\psi(\underline{y})$ does *not* imply $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$. Hence, usually $\psi(\underline{y})$ and $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ are not T-equivalent.

Uniform Quantifier-Free Interpolation (Covers)

Following SMT-terminology, we call $\mathcal{EUF}(\Sigma)$ the pure equality theory in the (functional) signature Σ.

Uniform Quantifier-Free Interpolation (Covers)

Following SMT-terminology, we call $\mathcal{EUF}(\Sigma)$ the pure equality theory in the (functional) signature Σ.

Uniform (qf) interpolants exists in $\mathcal{EUF}(\Sigma)$: an algorithm using Superposition Calculus is presented in our (CADE 19) paper - journal version in (JAR 21), to appear.

Uniform Quantifier-Free Interpolation (Covers)

Following SMT-terminology, we call $\mathcal{EUF}(\Sigma)$ the pure equality theory in the (functional) signature Σ.

Uniform (qf) interpolants exists in $\mathcal{EUF}(\Sigma)$: an algorithm using Superposition Calculus is presented in our (CADE 19) paper - journal version in (JAR 21), to appear.

Two further algorithms are in (Gianola, G., Kapur CILC 21).

Covers and Model Completions

A *universal* Σ-theory T has a ***model completion*** iff there is a stronger theory $T^* \supseteq T$ (in the same signature Σ) such that (i) every T-model embeds into a model of T^*; (ii) T^* eliminates quantifiers.

Covers and Model Completions

A *universal* Σ-theory T has a ***model completion*** iff there is a stronger theory $T^* \supseteq T$ (in the same signature Σ) such that (i) every T-model embeds into a model of T^*; (ii) T^* eliminates quantifiers.

Theorem (Covers and QE)

Suppose that T is a universal theory. Then, T has a model completion T^* ***iff*** *T has uniform quantifier-free interpolation. If this happens, T^* is axiomatized by the infinitely many sentences $\forall \underline{y}\, (\psi(\underline{y}) \to \exists \underline{e}\, \phi(\underline{e}, \underline{y}))$, where $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ is a primitive formula and ψ is a* ***cover*** *of it.*

Covers and Model Completions

A *universal* Σ-theory T has a ***model completion*** iff there is a stronger theory $T^* \supseteq T$ (in the same signature Σ) such that (i) every T-model embeds into a model of T^*; (ii) T^* eliminates quantifiers.

Theorem (Covers and QE)

Suppose that T is a universal theory. Then, T has a model completion T^* ***iff*** *T has uniform quantifier-free interpolation. If this happens, T^* is axiomatized by the infinitely many sentences $\forall \underline{y}\, (\psi(\underline{y}) \to \exists \underline{e}\, \phi(\underline{e}, \underline{y}))$, where $\exists \underline{e}\, \phi(\underline{e}, \underline{y})$ is a primitive formula and ψ is a* ***cover*** *of it.*

Hence, **computing covers** in a theory T
is **equivalent** to
eliminating quantifiers in its model completion T^*.

Outline

Equality Interpolating Condition

Definition ([YM05])

A convex universal theory T is *equality interpolating* iff for every pair y_1, y_2 of variables and for every pair of *constraints* $\delta_1(\underline{x}, \underline{z}_1, y_1)$, $\delta_2(\underline{x}, \underline{z}_2, y_2)$ such that $T \vdash \delta_1(\underline{x}, \underline{z}_1, y_1) \wedge \delta_2(\underline{x}, \underline{z}_2, y_2) \to y_1 = y_2$, **there exists** a term $t(\underline{x})$ such that $T \vdash \delta_1(\underline{x}, \underline{z}_1, y_1) \wedge \delta_2(\underline{x}, \underline{z}_2, y_2) \to y_1 = t(\underline{x}) \wedge y_2 = t(\underline{x})$.

Equality Interpolating Condition

Definition ([YM05])

A convex universal theory T is *equality interpolating* iff for every pair y_1, y_2 of variables and for every pair of *constraints* $\delta_1(\underline{x}, \underline{z}_1, y_1)$, $\delta_2(\underline{x}, \underline{z}_2, y_2)$ such that $T \vdash \delta_1(\underline{x}, \underline{z}_1, y_1) \wedge \delta_2(\underline{x}, \underline{z}_2, y_2) \to y_1 = y_2$, **there exists** a term $t(\underline{x})$ such that $T \vdash \delta_1(\underline{x}, \underline{z}_1, y_1) \wedge \delta_2(\underline{x}, \underline{z}_2, y_2) \to y_1 = t(\underline{x}) \wedge y_2 = t(\underline{x})$.

Examples of universal **quantifier-free interpolating** and **equality interpolating** theories:

- $\mathcal{EUF}(\Sigma)$, given a signature Σ;
- recursive data theories;
- linear real arithmetics;
- Boolean algebras.

Beth Definability and Equality Interpolating Condition

Equality interpolating can be characterized using Beth definability.

Given a primitive formula $\exists \underline{z} \phi(\underline{x}, \underline{z}, y)$, we say that:

- $\exists \underline{z}\, \phi(\underline{x}, \underline{z}, y)$ *implicitly defines* y in T iff the following formula is T-valid: $\forall y\, \forall y'\, (\exists \underline{z} \phi(\underline{x}, \underline{z}, y) \wedge \exists \underline{z} \phi(\underline{x}, \underline{z}, y') \rightarrow y = y')$;
- $\exists \underline{z} \phi(\underline{x}, \underline{z}, y)$ *explicitly defines* y in T iff there is a term $t(\underline{x})$ such that the formula is T-valid: $\forall y\, (\exists \underline{z} \phi(\underline{x}, \underline{z}, y) \rightarrow y = t(\underline{x}))$;
- a theory T has the ***Beth definability property*** *for primitive formulae* iff whenever a primitive formula $\exists \underline{z}\, \phi(\underline{x}, \underline{z}, y)$ *implicitly* defines the variable y then it also *explicitly* defines it.

Theorem (Key Theorem [BGR14])

A convex theory T having quantifier-free interpolation is ***equality interpolating iff*** *it has the* ***Beth definability property*** *for primitive formulae.*

Strong Amalgamability and Equality Interpolating Condition

It is well-known since the 70's that, for a universal theory, quantifier-free interpolation is equivalent to **amalgamation property**.

Strong Amalgamability and Equality Interpolating Condition

It is well-known since the 70's that, for a universal theory, quantifier-free interpolation is equivalent to **amalgamation property**. This result can be extended so as to characterize also the equality interpolating condition:

Strong Amalgamability and Equality Interpolating Condition

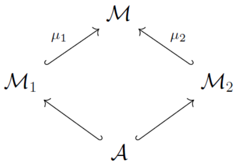
It is well-known since the 70's that, for a universal theory, quantifier-free interpolation is equivalent to **amalgamation property**. This result can be extended so as to characterize also the equality interpolating condition:

Theorem

*[BGR14] The following two conditions are equivalent for a convex universal theory T: (i) T is **equality interpolating** and has **quantifier-free interpolation**; (ii) T has the **strong amalgamation property**.*

Strong Amalgamability and Equality Interpolating Condition

Recall that a universal theory T has the *strong amalgamation property* iff every pair of models $\mathcal{M}_1, \mathcal{M}_2$ of T sharing a common submodel $\mathcal{A}$ can be amalgamated over $\mathcal{A}$ into a model $\mathcal{M}$ in such a way that the $\mathcal{A}$-embeddings μ_1, μ_2 satisfy the following additional condition: if for some m_1, m_2 we have $\mu_1(m_1) = \mu_2(m_2)$, then there exists an element a in $|\mathcal{A}|$ such that $m_1 = a = m_2$.



Transfer of Quantifier-free Interpolants

Theorem (Sufficient Condition [YM05, BGR14])

Let T_1 and T_2 be two universal, convex, stably infinite theories over disjoint signatures Σ_1 and Σ_2. If both T_1 and T_2 are equality interpolating and have quantifier-free interpolation property, then so does $T_1 \cup T_2$.

Transfer of Quantifier-free Interpolants

Theorem (Sufficient Condition [YM05, BGR14])

Let T_1 and T_2 be two universal, convex, stably infinite theories over disjoint signatures Σ_1 and Σ_2. If both T_1 and T_2 are equality interpolating and have quantifier-free interpolation property, then so does $T_1 \cup T_2$.

There is a converse of the previous result:

Theorem (Necessary Condition [BGR14])

Let T be a stably infinite, universal, convex theory admitting quantifier-free interpolation and let Σ be a signature disjoint from the signature of T containing at least a unary predicate symbol. Then, $T \cup \mathcal{EUF}(\Sigma)$ has ***quantifier-free interpolation iff*** *T is* ***equality interpolating****.*

Outline

Convex Theories

- Every Σ_i-theory T_i from now on is ***convex, stably infinite, equality interpolating, universal and admitting a model completion*** T_i^*.

Convex Theories

- Every Σ_i-theory T_i from now on is ***convex, stably infinite, equality interpolating, universal and admitting a model completion*** T_i^*.
- For $i = 1, \dots, n$, we let the formula $\mathtt{ImplDef}^T_{\phi,y_i}(\underline{x})$ be the quantifier-free formula equivalent in T^* to the formula

$$\forall \underline{y}\, \forall \underline{y}' (\phi(\underline{x}, \underline{y}) \land \phi(\underline{x}, \underline{y}') \to y_i = y_i')$$

where the $\underline{y}'$ are renamed copies of the $\underline{y} = y_1, \dots, y_n$.

Convex Theories

- Every Σ_i-theory T_i from now on is ***convex, stably infinite, equality interpolating, universal and admitting a model completion*** T_i^*.
- For $i = 1, \ldots, n$, we let the formula $\texttt{ImplDef}^T_{\phi,y_i}(\underline{x})$ be the quantifier-free formula equivalent in T^* to the formula

$$\forall \underline{y}\, \forall \underline{y}'(\phi(\underline{x}, \underline{y}) \wedge \phi(\underline{x}, \underline{y}') \rightarrow y_i = y_i')$$

where the $\underline{y}'$ are renamed copies of the $\underline{y}$.

The following Lemma supplies terms used as ingredients in the combined covers algorithm:

Lemma (Useful Terms)

Let $L_{i1}(\underline{x}) \vee \cdots \vee L_{ik_i}(\underline{x})$ *be the disjunctive normal form (DNF) of* $\texttt{ImplDef}^T_{\phi,y_i}(\underline{x})$. *Then, for every* $j = 1, \ldots, k_i$, *there is a* $\Sigma(\underline{x})$*-term* $t_{ij}(\underline{x})$ *such that* $T \vdash L_{ij}(\underline{x}) \wedge \phi(\underline{x}, \underline{y}) \rightarrow y_i = t_{ij}$

The terms t_{ij} are obtained thanks to the Beth definability property, that holds because of the Key Theorem.

Computing Combined Covers

- Given a Σ_1-theory T_1 and a Σ_2-theory T_2, we want to compute a $T_1 \cup T_2$-**cover** for $\exists \underline{e}\, \phi(\underline{x}, \underline{e})$ (Initial Formula).

Computing Combined Covers

- Given a Σ_1-theory T_1 and a Σ_2-theory T_2, we want to compute a $T_1 \cup T_2$-**cover** for $\exists \underline{e}\, \phi(\underline{x}, \underline{e})$ (Initial Formula).
- By applying rewriting purification steps, we can assume that ϕ is of the kind $\phi_1 \wedge \phi_2$, where ϕ_i is a Σ_i-formula ($i = 1, 2$).

Computing Combined Covers

- Given a Σ_1-theory T_1 and a Σ_2-theory T_2, we want to compute a $T_1 \cup T_2$-**cover** for $\exists \underline{e}\, \phi(\underline{x}, \underline{e})$ (Initial Formula).
- By applying rewriting purification steps, we can assume that ϕ is of the kind $\phi_1 \wedge \phi_2$, where ϕ_i is a Σ_i-formula $(i = 1, 2)$.
- Assume that ϕ_1 and ϕ_2 contain $e_i \neq e_j$ (for $i \neq j$): guess a partition of the $\underline{e}$ and replace each e_i with the representative element of its equivalence class.

Computing Combined Covers

- Given a Σ_1-theory T_1 and a Σ_2-theory T_2, we want to compute a $T_1 \cup T_2$-**cover** for $\exists \underline{e}\, \phi(\underline{x}, \underline{e})$ (Initial Formula).
- By applying rewriting purification steps, we can assume that ϕ is of the kind $\phi_1 \wedge \phi_2$, where ϕ_i is a Σ_i-formula $(i = 1, 2)$.
- Assume that ϕ_1 and ϕ_2 contain $e_i \neq e_j$ (for $i \neq j$): guess a partition of the $\underline{e}$ and replace each e_i with the representative element of its equivalence class.
- The algorithm employs **acyclic explicit definitions** `ExplDef`$(\underline{z}, \underline{x})$ $\bigwedge_{i=1}^{m} z_i = t_i(z_1, \ldots, z_{i-1}, \underline{x})$ where the term t_i is pure.

Computing Combined Covers

- Given a Σ_1-theory T_1 and a Σ_2-theory T_2, we want to compute a $T_1 \cup T_2$-**cover** for $\exists \underline{e}\, \phi(\underline{x}, \underline{e})$ (Initial Formula).
- By applying rewriting purification steps, we can assume that ϕ is of the kind $\phi_1 \wedge \phi_2$, where ϕ_i is a Σ_i-formula $(i = 1, 2)$.
- Assume that ϕ_1 and ϕ_2 contain $e_i \neq e_j$ (for $i \neq j$): guess a partition of the $\underline{e}$ and replace each e_i with the representative element of its equivalence class.
- The algorithm employs **acyclic explicit definitions** $\texttt{ExplDef}(\underline{z}, \underline{x})$ $\bigwedge_{i=1}^{m} z_i = t_i(z_1, \ldots, z_{i-1}, \underline{x})$ where the term t_i is pure.
- A *working formula* is $\exists \underline{z}\, (\texttt{ExplDef}(\underline{z}, \underline{x}) \wedge \exists \underline{e}\, (\psi_1(\underline{x}, \underline{z}, \underline{e}) \wedge \psi_2(\underline{x}, \underline{z}, \underline{e})))$, where ψ_i is a Σ_i-formula $(i = 1, 2)$ and $\underline{x}$ are called *parameters*, $\underline{z}$ *defined variables* and $\underline{e}$ *(truly) existential variables*. ψ_1, ψ_2 always contain the literals $e_i \neq e_j$ (for distinct e_i, e_j from $\underline{e}$) as a conjunct.

Computing Combined Covers

- Given a Σ_1-theory T_1 and a Σ_2-theory T_2, we want to compute a $T_1 \cup T_2$-**cover** for $\exists \underline{e}\, \phi(\underline{x}, \underline{e})$ (Initial Formula).
- By applying rewriting purification steps, we can assume that ϕ is of the kind $\phi_1 \wedge \phi_2$, where ϕ_i is a Σ_i-formula $(i = 1, 2)$.
- Assume that ϕ_1 and ϕ_2 contain $e_i \neq e_j$ (for $i \neq j$): guess a partition of the $\underline{e}$ and replace each e_i with the representative element of its equivalence class.
- The algorithm employs **acyclic explicit definitions** $\texttt{ExplDef}(\underline{z}, \underline{x})$ $\bigwedge_{i=1}^{m} z_i = t_i(z_1, \dots, z_{i-1}, \underline{x})$ where the term t_i is pure.
- A *working formula* is $\exists \underline{z}\, (\texttt{ExplDef}(\underline{z}, \underline{x}) \wedge \exists \underline{e}\, (\psi_1(\underline{x}, \underline{z}, \underline{e}) \wedge \psi_2(\underline{x}, \underline{z}, \underline{e})))$, where ψ_i is a Σ_i-formula $(i = 1, 2)$ and $\underline{x}$ are called *parameters*, $\underline{z}$ *defined variables* and $\underline{e}$ *(truly) existential variables*. ψ_1, ψ_2 always contain the literals $e_i \neq e_j$ (for distinct e_i, e_j from $\underline{e}$) as a conjunct.
- A working formula is *terminal* iff for every $e_i \in \underline{e}$

$$T_1 \vdash \psi_1 \to \neg \texttt{ImplDef}^{T_1}_{\psi_1, e_i}(\underline{x}, \underline{z}) \text{ and } T_2 \vdash \psi_2 \to \neg \texttt{ImplDef}^{T_2}_{\psi_2, e_i}(\underline{x}, \underline{z})$$

Combined Covers Algorithm

Lemma (Main Lemma)

*Every **working formula** is equivalent (modulo $T_1 \cup T_2$) to a disjunction of **terminal** **working formulae**.*

Combined Covers Algorithm

Lemma (Main Lemma)

Every ***working formula*** *is equivalent (modulo $T_1 \cup T_2$) to a disjunction of* ***terminal working formulae****.*

Start from an Initial Formula. The non-deterministic procedure to compute the terminal working formulae applies one of the following **alternatives**:

(1) Add to ψ_1 a disjunct from the DNF of $\bigwedge_{e_i \in \underline{e}} \neg \mathtt{ImplDef}^{T_1}_{\psi_1, e_i}(\underline{x}, \underline{z})$ and to ψ_2 a disjunct from the DNF of $\bigwedge_{e_i \in \underline{e}} \neg \mathtt{ImplDef}^{T_2}_{\psi_2, e_i}(\underline{x}, \underline{z})$;

(2.i) Select $e_i \in \underline{e}$ and $h \in \{1, 2\}$; then add to ψ_h a disjunct L_{ij} from the DNF of $\mathtt{ImplDef}^{T_h}_{\psi_h, e_i}(\underline{x}, \underline{z})$; add $e_i = t_{ij}$ (where t_{ij} is the term mentioned in **Useful Terms Lemma**) to $\mathtt{ExplDef}(\underline{z}, \underline{x})$; the variable e_i becomes *defined*.

KRDB

Combined Covers Algorithm

Lemma (Main Lemma)

*Every **working formula** is equivalent (modulo $T_1 \cup T_2$) to a disjunction of **terminal working formulae**.*

Start from an Initial Formula. The non-deterministic procedure to compute the terminal working formulae applies one of the following **alternatives**:

(1) Add to ψ_1 a disjunct from the DNF of $\bigwedge_{e_i \in \underline{e}} \neg \mathtt{ImplDef}^{T_1}_{\psi_1, e_i}(\underline{x}, \underline{z})$ and to ψ_2 a disjunct from the DNF of $\bigwedge_{e_i \in \underline{e}} \neg \mathtt{ImplDef}^{T_2}_{\psi_2, e_i}(\underline{x}, \underline{z})$;

(2.i) Select $e_i \in \underline{e}$ and $h \in \{1, 2\}$; then add to ψ_h a disjunct L_{ij} from the DNF of $\mathtt{ImplDef}^{T_h}_{\psi_h, e_i}(\underline{x}, \underline{z})$; add $e_i = t_{ij}$ (where t_{ij} is the term mentioned in **Useful Terms Lemma**) to $\mathtt{ExplDef}(\underline{z}, \underline{x})$; the variable e_i becomes *defined*.

The output is the disjunction of all possible outcomes.

Transfer of covers

Proposition

*A **cover** of a terminal working formula can be obtained by unravelling the explicit definitions of the variables* $\underline{z}$ *from* $\exists \underline{z}\,(\mathtt{ExplDef}(\underline{z}, \underline{x}) \wedge \theta_1(\underline{x}, \underline{z}) \wedge \theta_2(\underline{x}, \underline{z}))$*, where* $\theta_1(\underline{x}, \underline{z})$ *is the* T_1*-**cover** of* $\exists \underline{e} \psi_1(\underline{x}, \underline{z}, \underline{e})$ *and* $\theta_2(\underline{x}, \underline{z})$ *is the* T_2*-**cover** of* $\exists \underline{e} \psi_2(\underline{x}, \underline{z}, \underline{e})$*.*

Transfer of covers

Proposition

A ***cover*** *of a terminal working formula can be obtained by unravelling the explicit definitions of the variables* $\underline{z}$ *from* $\exists \underline{z}\ (\texttt{ExplDef}(\underline{z}, \underline{x}) \wedge \theta_1(\underline{x}, \underline{z}) \wedge \theta_2(\underline{x}, \underline{z}))$, *where* $\theta_1(\underline{x}, \underline{z})$ *is the* T_1*-**cover** of* $\exists \underline{e} \psi_1(\underline{x}, \underline{z}, \underline{e})$ *and* $\theta_2(\underline{x}, \underline{z})$ *is the* T_2*-**cover** of* $\exists \underline{e} \psi_2(\underline{x}, \underline{z}, \underline{e})$.

From the Main Lemma, the previous Proposition and the 'Covers and QE' Theorem, we get:

Transfer of covers

Proposition

*A **cover** of a terminal working formula can be obtained by unravelling the explicit definitions of the variables* $\underline{z}$ *from* $\exists \underline{z}\ (\texttt{ExplDef}(\underline{z}, \underline{x}) \wedge \theta_1(\underline{x}, \underline{z}) \wedge \theta_2(\underline{x}, \underline{z}))$, *where* $\theta_1(\underline{x}, \underline{z})$ *is the* T_1***-cover*** *of* $\exists \underline{e} \psi_1(\underline{x}, \underline{z}, \underline{e})$ *and* $\theta_2(\underline{x}, \underline{z})$ *is the* T_2***-cover*** *of* $\exists \underline{e} \psi_2(\underline{x}, \underline{z}, \underline{e})$.

From the Main Lemma, the previous Proposition and the 'Covers and QE' Theorem, we get:

Theorem

Let T_1, T_2 *be* ***convex, stably infinite, equality interpolating, universal theories over disjoint signatures admitting a model completion****. Then* $T_1 \cup T_2$ *admits a model completion too. Covers in* $T_1 \cup T_2$ *can be effectively* ***computed*** *as shown above.*

Combined Algorithm: an Example

Let T_1 be $\mathcal{EUF}(\Sigma)$ and T_2 be linear real arithmetic.

Combined Algorithm: an Example

Let T_1 be $\mathcal{EUF}(\Sigma)$ and T_2 be linear real arithmetic.

Covers are computed in real arithmetic by **quantifier elimination**, whereas for $\mathcal{EUF}(\Sigma)$ one can apply the **superposition-based algorithm** from [CGG$^+$19].

Combined Algorithm: an Example

Let T_1 be $\mathcal{EUF}(\Sigma)$ and T_2 be linear real arithmetic.

Covers are computed in real arithmetic by **quantifier elimination**, whereas for $\mathcal{EUF}(\Sigma)$ one can apply the **superposition-based algorithm** from [CGG+19].

Consider the formula:

$$\exists e_1 \cdots \exists e_4 \quad \begin{pmatrix} e_1 = f(x_1) \ \wedge \ e_2 = f(x_2) \wedge \\ \wedge \ f(e_3) = e_3 \ \wedge \ \ f(e_4) = x_1 \wedge \\ \wedge \ x_1 + e_1 \leq e_3 \ \wedge \ e_3 \leq x_2 + e_2 \ \wedge \ e_4 = x_2 + e_3 \end{pmatrix}$$

Combined Algorithm: an Example

Let T_1 be $\mathcal{EUF}(\Sigma)$ and T_2 be linear real arithmetic.
Covers are computed in real arithmetic by **quantifier elimination**, whereas for $\mathcal{EUF}(\Sigma)$ one can apply the **superposition-based algorithm** from [CGG$^+$19].
Consider the formula:

$$\exists e_1 \cdots \exists e_4 \quad \begin{pmatrix} e_1 = f(x_1) \ \wedge \ e_2 = f(x_2) \wedge \\ \wedge \ f(e_3) = e_3 \ \wedge \ \ f(e_4) = x_1 \wedge \\ \wedge \ x_1 + e_1 \leq e_3 \ \wedge \ e_3 \leq x_2 + e_2 \ \wedge \ e_4 = x_2 + e_3 \end{pmatrix}$$

Applying exhaustively Step (1) and Step (2.i), we get:

$$\begin{aligned} & [x_2 = 0 \ \wedge \ f(x_1) = x_1 \ \wedge \ x_1 \leq 0 \ \wedge \ x_1 \leq f(0)] \vee \\ & \vee \ [x_1 + f(x_1) < x_2 + f(x_2) \ \wedge \ x_2 \neq 0] \vee \\ & \vee \begin{bmatrix} x_2 \neq 0 \wedge x_1 + f(x_1) = x_2 + f(x_2) \ \wedge \ f(2x_2 + f(x_2)) = x_1 \wedge \\ \wedge f(x_1 + f(x_1)) = x_1 + f(x_1) \end{bmatrix} \end{aligned}$$

Equality Interpolating is a necessary condition

Equality interpolating is a **necessary condition** for a transfer result, in the sense that it is already required for minimal combinations with signatures adding *uninterpreted symbols*:

Equality Interpolating is a necessary condition

Equality interpolating is a **necessary condition** for a transfer result, in the sense that it is already required for minimal combinations with signatures adding *uninterpreted symbols*:

Theorem

Let T be a convex, stably infinite, universal theory admitting a model completion and let Σ be a signature disjoint from the signature of T containing at least a unary predicate symbol. Then $T \cup \mathcal{EUF}(\Sigma)$ admits a model completion ***iff*** *T is equality interpolating.*

Equality Interpolating is a necessary condition

Equality interpolating is a **necessary condition** for a transfer result, in the sense that it is already required for minimal combinations with signatures adding *uninterpreted symbols*:

Theorem

Let T be a convex, stably infinite, universal theory admitting a model completion and let Σ be a signature disjoint from the signature of T containing at least a unary predicate symbol. Then $T \cup \mathcal{EUF}(\Sigma)$ admits a model completion ***iff*** *T is equality interpolating.*

The necessity can be easily deduced from the Necessity Theorem for **Equality Interpolating**.

Outline

Non-transfer of Covers in the Non-convex case

Convexity hypothesis cannot be eliminated.

Non-transfer of Covers in the Non-convex case

Convexity hypothesis cannot be eliminated.
Consider the **cover transfer** for $T_1 \cup T_2$, where:

- $T_1 :=$ integer difference logic $\mathcal{IDL}$ (integer numbers with successor and predecessor, 0 and the strict order $<$): it is *not* convex, but it satisfies the equality interpolating condition for non-convex theories.
- $T_2 := \mathcal{EUF}(\Sigma_f)$, where Σ_f has only one unary free function symbol f (not belonging to the signature of T_1).

Non-transfer of Covers in the Non-convex case

Convexity hypothesis cannot be eliminated.
Consider the **cover transfer** for $T_1 \cup T_2$, where:

- $T_1 :=$ integer difference logic $\mathcal{IDL}$ (integer numbers with successor and predecessor, 0 and the strict order $<$): it is *not* convex, but it satisfies the equality interpolating condition for non-convex theories.
- $T_2 := \mathcal{EUF}(\Sigma_f)$, where Σ_f has only one unary free function symbol f (not belonging to the signature of T_1).

Proposition

*Let T_1, T_2 be as above; the formula $\exists e\ (0 < e \wedge e < x \wedge f(e) = 0)$ does **not** have a cover in $T_1 \cup T_2$.*

Non-transfer of Covers in the Non-convex case

Convexity hypothesis cannot be eliminated.
Consider the **cover transfer** for $T_1 \cup T_2$, where:

- $T_1 :=$ integer difference logic $\mathcal{IDL}$ (integer numbers with successor and predecessor, 0 and the strict order $<$): it is *not* convex, but it satisfies the equality interpolating condition for non-convex theories.
- $T_2 := \mathcal{EUF}(\Sigma_f)$, where Σ_f has only one unary free function symbol f (not belonging to the signature of T_1).

Proposition

Let T_1, T_2 be as above; the formula $\exists e\ (0 < e \wedge e < x \wedge f(e) = 0)$ does ***not*** *have a cover in $T_1 \cup T_2$.*

The counterexample still applies when replacing integer difference logic with *linear integer arithmetics*.

Outline

Conclusions

- Problem of **combined covers.**

Conclusions

- Problem of **combined covers.**
- Sufficient and necessary conditions for transferring covers to **combinations** in the *convex* case.

Conclusions

- Problem of **combined covers.**
- Sufficient and necessary conditions for transferring covers to **combinations** in the *convex* case.
- General method and algorithm for computing **combined covers** for *convex* theories, based on the use of Beth definability.

Conclusions

- Problem of **combined covers.**
- Sufficient and necessary conditions for transferring covers to **combinations** in the *convex* case.
- General method and algorithm for computing **combined covers** for *convex* theories, based on the use of Beth definability.
- Non-transfer of covers in the *non-convex* case, in general.

Future Work

- Investigate **cover transfer** for 'tame' theory combinations (*codomain* sorts are shared): already available in the ArXiv version;
- **Cover transfer** properties for non-disjoint signatures combinations.

References

R. Bruttomesso, S. Ghilardi, and S. Ranise.
Quantifier-free interpolation in combinations of equality interpolating theories.
ACM Trans. Comput. Log., 15(1):5:1–5:34, 2014.

D. Calvanese, S. Ghilardi, A. Gianola, M. Montali, and A. Rivkin.
Model completeness, covers and superposition.
In *Proc. of CADE*, volume 11716 of *LNCS*. Springer, 2019.

S. Gulwani and M. Musuvathi.
Cover algorithms and their combination.
In *Proc. of ESOP, Held as Part of ETAPS*, pages 193–207, 2008.

D. Kapur.
Nonlinear polynomials, interpolants and invariant generation for system analysis.
In *Proc. of ISSAC*, 2017.

G. Yorsh and M. Musuvathi.
A combination method for generating interpolants.
In *Proc. of CADE-20*, LNCS, pages 353–368. 2005.

THANKS FOR YOUR ATTENTION!