Polite Theories Revisited

Dejan Jovanović and Clark Barrett

New York University

SMT 09, Aug. 2-3, 2009
McGill University, Montreal, Canada

Outline

Outline

The Theory Combination Problem

Combination of Theories

Given individual decision procedures for (quantifier free) first-order theories T_1 and T_2 how can we combine them in a modular fashion into a decision procedure for a theory $T_1 \oplus T_2$?

- The most commonly used method is due to Nelson and Oppen (1979)
- Allows one to decide the combination using decision procedures for T_1 and T_2 as black-boxes

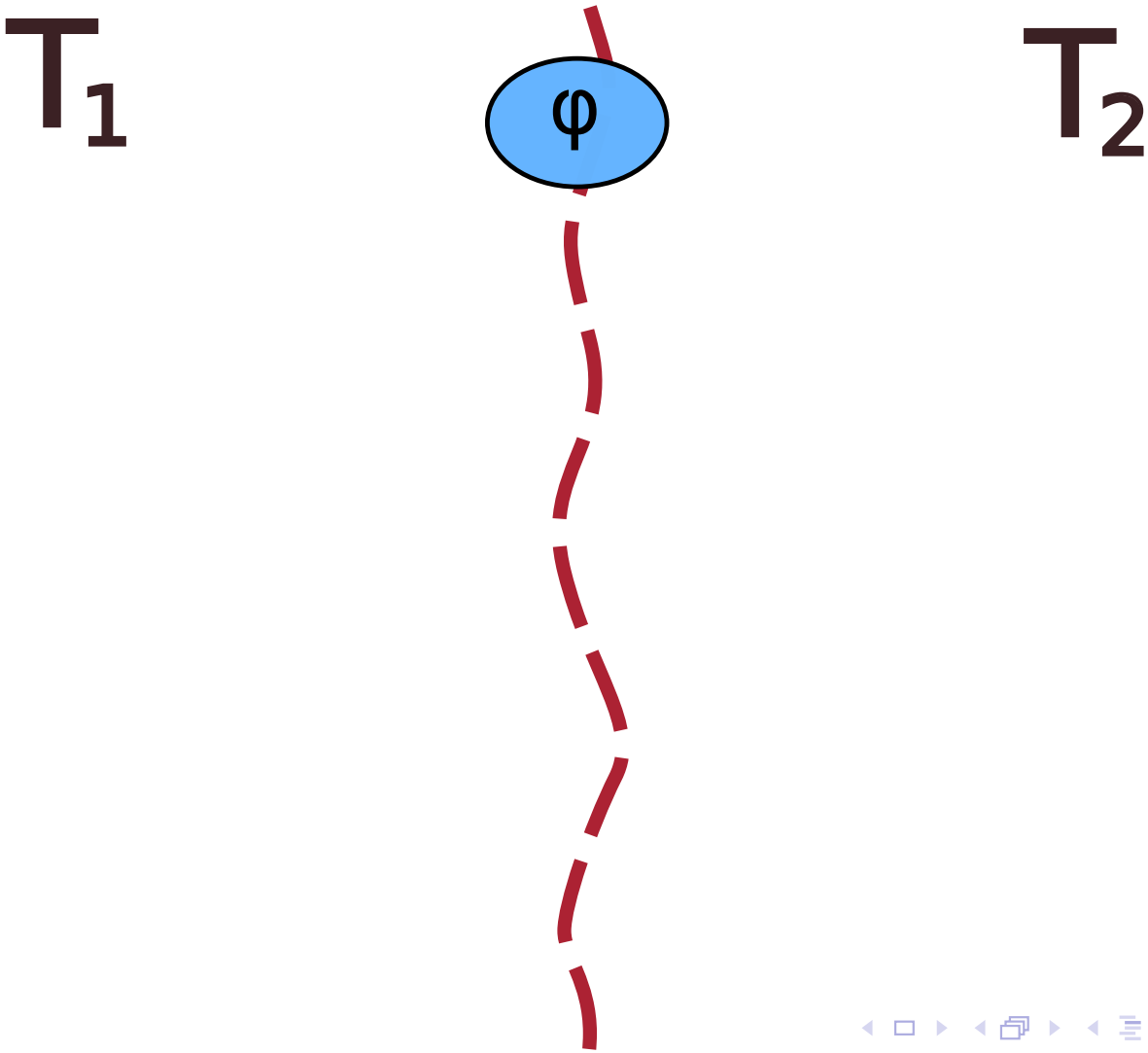
The Theory Combination Problem

Combination of Theories

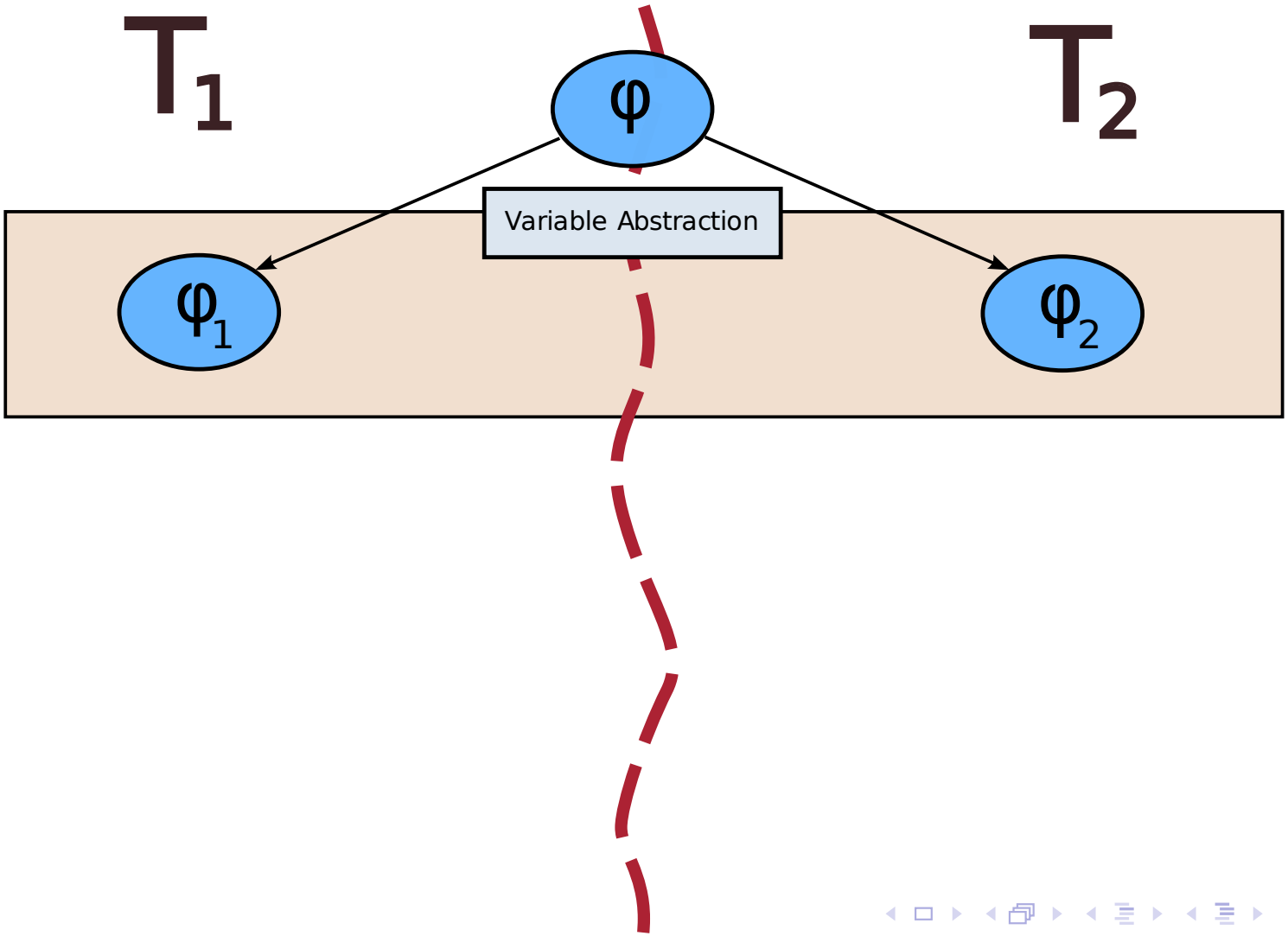
Given individual decision procedures for (quantifier free) first-order theories T_1 and T_2 how can we combine them in a modular fashion into a decision procedure for a theory $T_1 \oplus T_2$?

- The most commonly used method is due to Nelson and Oppen (1979)
- Allows one to decide the combination using decision procedures for T_1 and T_2 as black-boxes

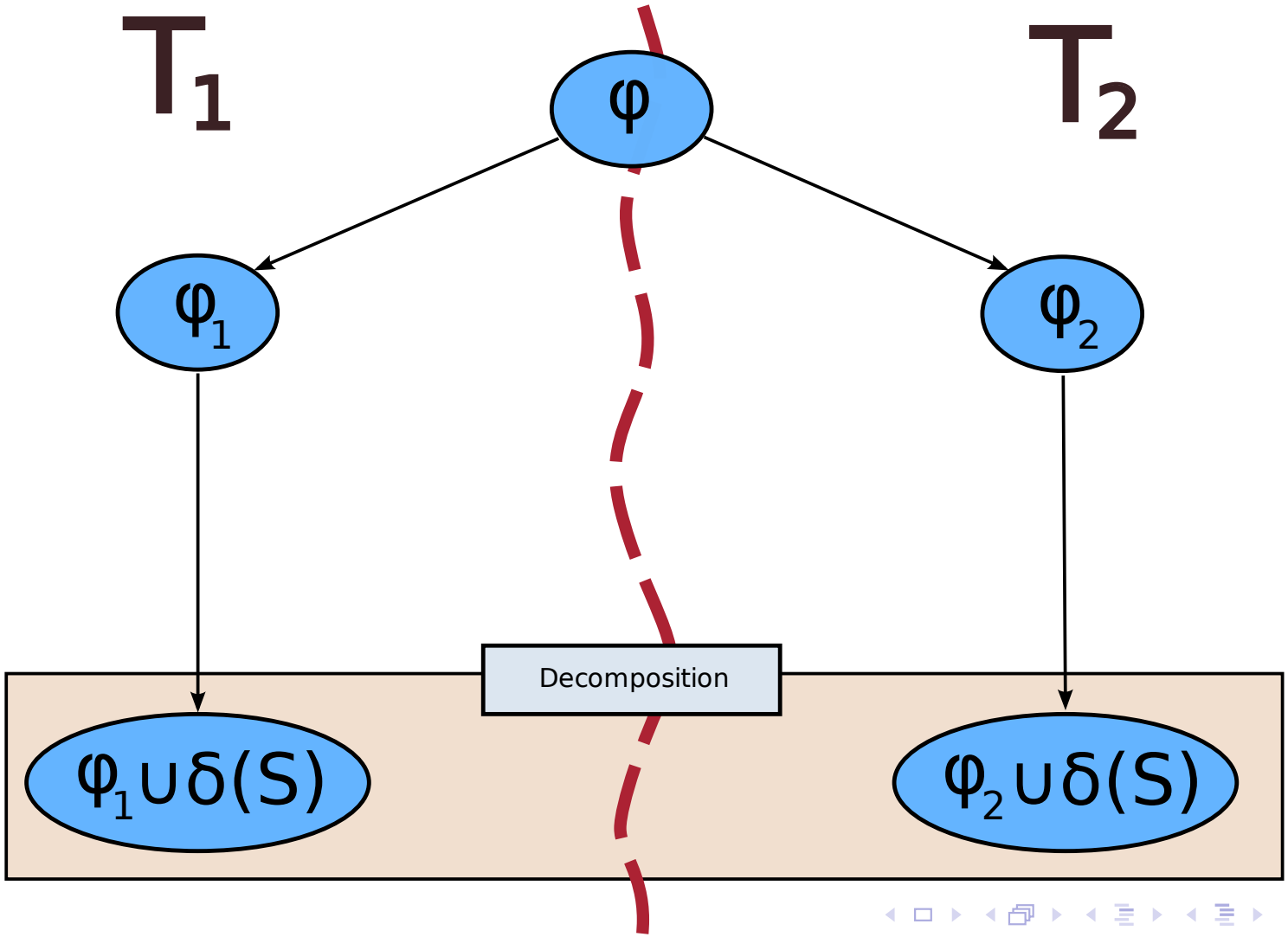
Nelson-Oppen: Idea (1979)



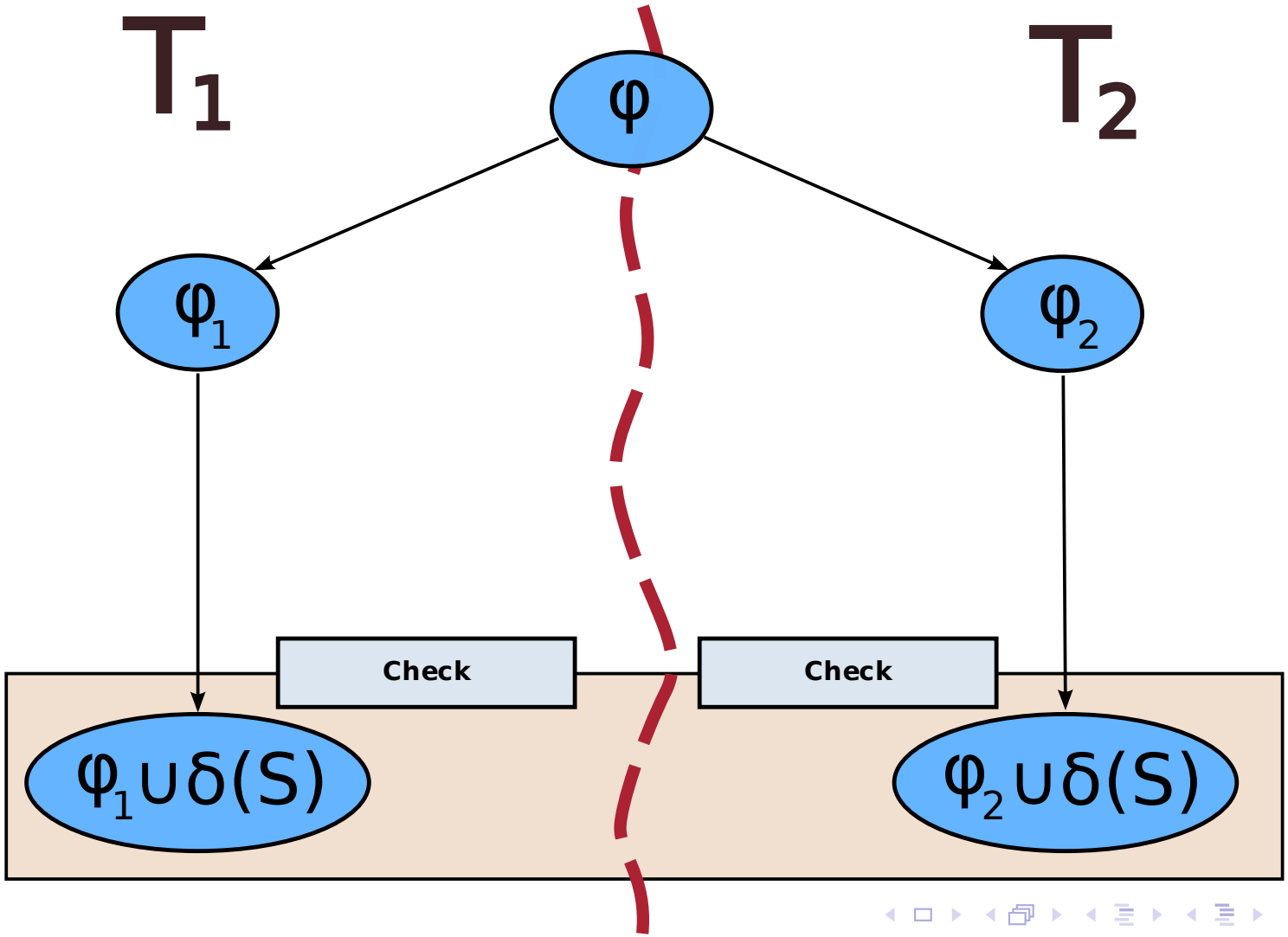
Nelson-Oppen: Idea (1979)



Nelson-Oppen: Idea (1979)



Nelson-Oppen: Idea (1979)



Nelson-Oppen

Does this work?

- Not always
- Nelson (1981), Oppen (1980)

  > *"... each theory is **stably-infinite**, that is, that any quantifier-free formula in the theory has an infinite model if it has any model."*

- Are the theories we want stably-infinite?
- Many are but some are not.
- Most notably, the theory of fixed size bit-vectors – finite!

Nelson-Oppen

Does this work?

- Not always
- Nelson (1981), Oppen (1980)

  > *"... each theory is **stably-infinite**, that is, that any quantifier-free formula in the theory has an infinite model if it has any model."*

- Are the theories we want stably-infinite?
- Many are but some are not.
- Most notably, the theory of fixed size bit-vectors – finite!

Nelson-Oppen

Does this work?

- Not always
- Nelson (1981), Oppen (1980)

  > *"... each theory is **stably-infinite**, that is, that any quantifier-free formula in the theory has an infinite model if it has any model."*

- Are the theories we want stably-infinite?
- Many are but some are not.
- Most notably, the theory of fixed size bit-vectors – finite!

Nelson-Oppen

Does this work?

- Not always
- Nelson (1981), Oppen (1980)

  > *"... each theory is **stably-infinite**, that is, that any quantifier-free formula in the theory has an infinite model if it has any model."*

- Are the theories we want stably-infinite?
- Many are but some are not.
- Most notably, the theory of fixed size bit-vectors – finite!

Arrays and Bitvectors

Combination of arrays with bit-vectors:

1. Theory T_{bv} of bit-vectors of size 1
2. Theory T_{array} of arrays over bit-vectors

Nelson-Oppen

- Consider the following set of UNSAT constraints:

$$a_i \neq a_j, \text{ for } 1 \leq i < j \leq 5 \ .$$

- There are only 4 diferent such arrays:

Arrays and Bitvectors

Combination of arrays with bit-vectors:

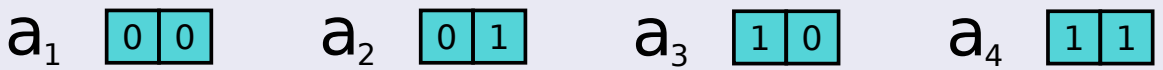
1. Theory T_{bv} of bit-vectors of size 1
2. Theory T_{array} of arrays over bit-vectors

Nelson-Oppen

- Consider the following set of UNSAT constraints:

$$a_i \neq a_j, \text{ for } 1 \leq i < j \leq 5 \ .$$

- There are only 4 diferent such arrays:



Arrays and Bitvectors

Combination of arrays with bit-vectors:

1. Theory T_{bv} of bit-vectors of size 1
2. Theory T_{array} of arrays over bit-vectors

Nelson-Oppen

- Consider the following set of UNSAT constraints:

$$a_i \neq a_j, \text{ for } 1 \leq i < j \leq 5 \ .$$

- Constraints are entirely within the language of T_{array} and there are no shared variables
- Decision procedure for the theory of arrays will tell us that these constraints are SAT

Outline

Polite Theories

An attempt to overcome the requirement of stable-infiniteness while keeping the framework of Nelson and Oppen was presented in

> *S. Ranise, C. Ringeissen, and C.G. Zarba. Combining Data Structures with Nonstably Infinite Theories Using Many-Sorted Logic. In FroCoS 2005, Proceedings. Springer, 2005.*

- The paper introduces the notion of Polite Theories.
- A polite theory can be combined with any other theory.
- Combination method almost the same as Nelson-Oppen.

Politeness

Let Σ be a signature, let $S \subseteq \Sigma^{\mathbb{S}}$ be a set of sorts, and let T be a Σ-theory.

Definition

Theory T is **Polite** with respect to S if

- T is smooth with respect to S, and
- T is finitely witnessable with respect to S.

Smoothness

Let Σ be a signature, let $S = \{s_1, \ldots, s_n\} \subseteq \Sigma^{\mathbb{S}}$ be a set of sorts, and let T be a Σ-theory.

Definition

Theory T is **Smooth** with respect to S if

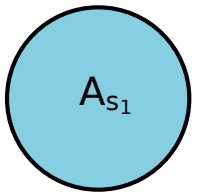
- for every T-satisfiable quantifier-free Σ-formula ϕ
- for every T-interpretation $\mathcal{A}$ satisfying ϕ
- for all cardinals numbers κ_i such that $\kappa_i \geq |A_{s_i}|$
- there exists a T-interpretation $\mathcal{B}$ satisfying ϕ

such that

- $|B_{s_i}| = \kappa_i$, for $i = 1, \ldots, n$.

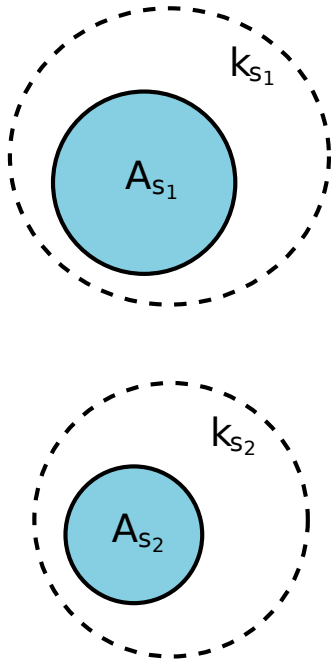
Smoothness

- Let ϕ is satisfiable in $\mathcal{A}$
- Let $|A_{s_1}| \leq \kappa_1$ and $|A_{s_2}| \leq \kappa_2$
- Then ϕ is satisfiable in $\mathcal{B}$ with $|B_{s_1}| = \kappa_1$ and $|B_{s_2}| = \kappa_2$



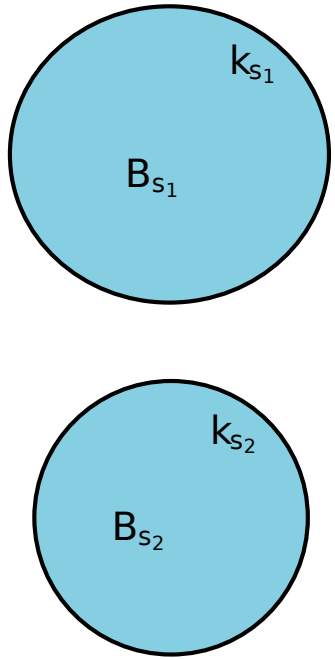
Smoothness

- Let ϕ is satisfiable in $\mathcal{A}$
- Let $|A_{s_1}| \leq \kappa_1$ and $|A_{s_2}| \leq \kappa_2$
- Then ϕ is satisfiable in $\mathcal{B}$ with $|B_{s_1}| = \kappa_1$ and $|B_{s_2}| = \kappa_2$



Smoothness

- Let ϕ is satisfiable in $\mathcal{A}$
- Let $|A_{s_1}| \leq \kappa_1$ and $|A_{s_2}| \leq \kappa_2$
- Then ϕ is satisfiable in $\mathcal{B}$ with $|B_{s_1}| = \kappa_1$ and $|B_{s_2}| = \kappa_2$



Finite Witnessability

Let Σ be a signature, let $S \subseteq \Sigma^{\mathbb{S}}$ be a set of sorts, and let T be a Σ-theory.

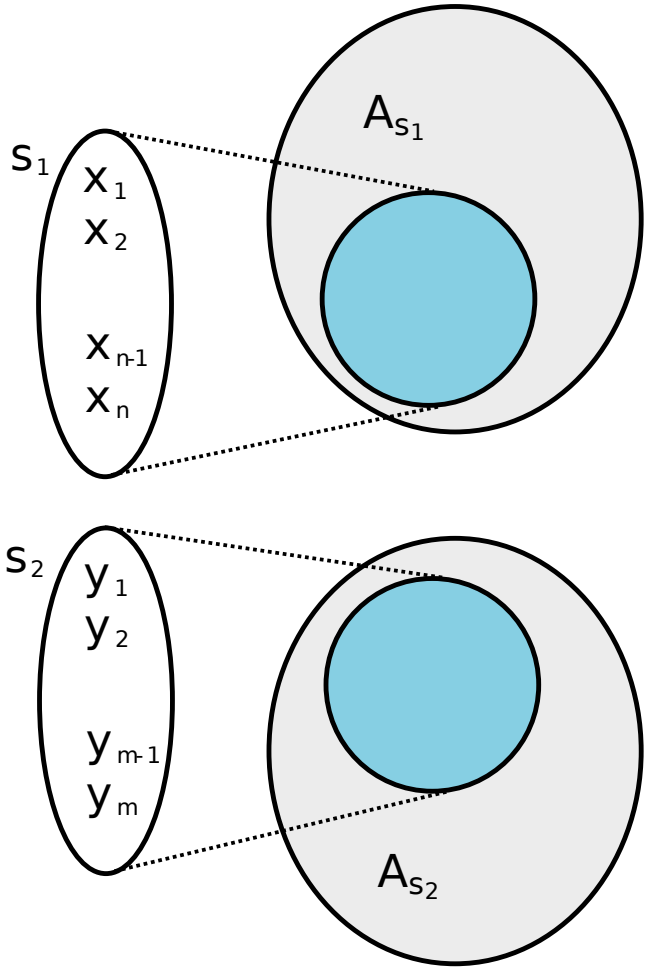
Definition

Theory T is **Finitely Witnessable** with respect to S if there is a computable QF-formula transformation *witness* such that for every QF Σ-formula ϕ and set of variables V with sorts in S

1. ϕ and $(\exists \overrightarrow{v})\psi$ are T-equivalent, where $\psi = \mathit{witness}(\phi)$ and $\overrightarrow{v}$ are the fresh variables, and
2. if $\psi \wedge \delta(V)$ is T-satisfiable then there is a T-interpretation $\mathcal{A}$ such that $A_s = [\mathit{vars}_s(\psi \wedge \delta(V))]^{\mathcal{A}}$ for all $s \in S$.

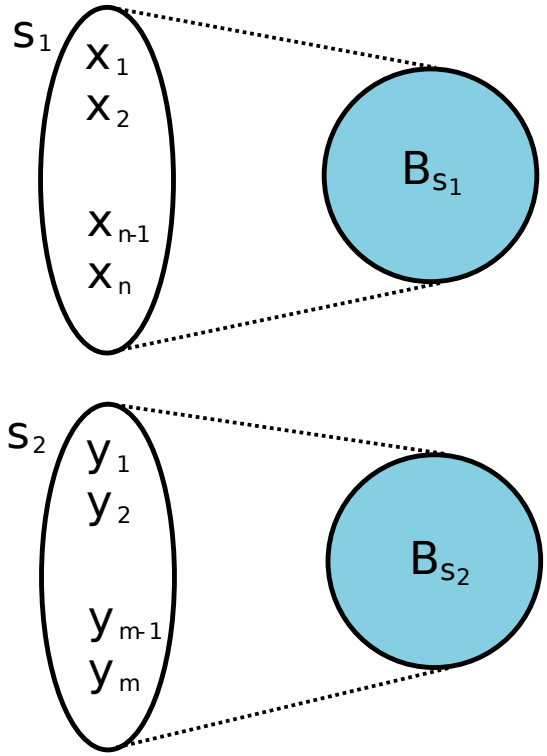
Finite Witnessability

- Let $\psi = \mathit{witness}(\phi)$, V a set of variables and $S = \{s_1, s_2\}$.
- If $\psi \wedge \delta(V)$ is satisfiable in $\mathcal{A}$
- Then $\psi \wedge \delta(V)$ is satisfiable in $\mathcal{B}$ that is witnessed by variables



Finite Witnessability

- Let $\psi = \mathit{witness}(\phi)$, V a set of variables and $S = \{s_1, s_2\}$.
- If $\psi \wedge \delta(V)$ is satisfiable in $\mathcal{A}$
- Then $\psi \wedge \delta(V)$ is satisfiable in $\mathcal{B}$ that is witnessed by variables



Politeness

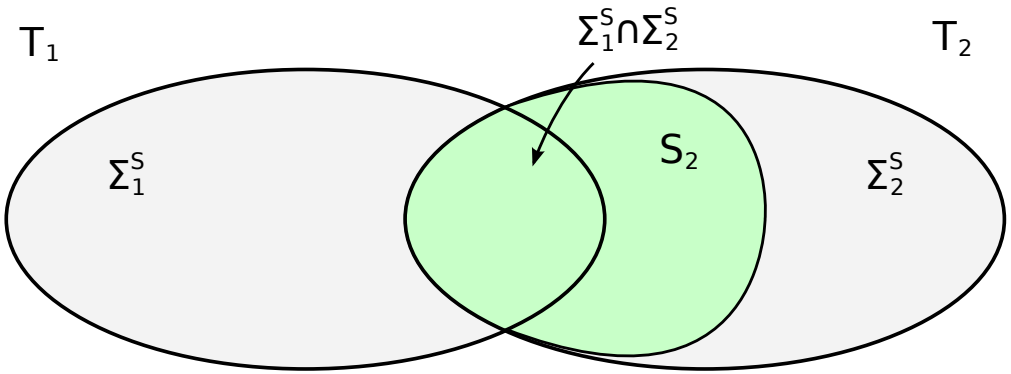
Let Σ be a signature, let $S \subseteq \Sigma^{\mathbb{S}}$ be a set of sorts, and let T be a Σ-theory.

Definition

Theory T is **Polite** with respect to S if

- T is smooth with respect to S, and
- T is finitely witnessable with respect to S.

Combination Method

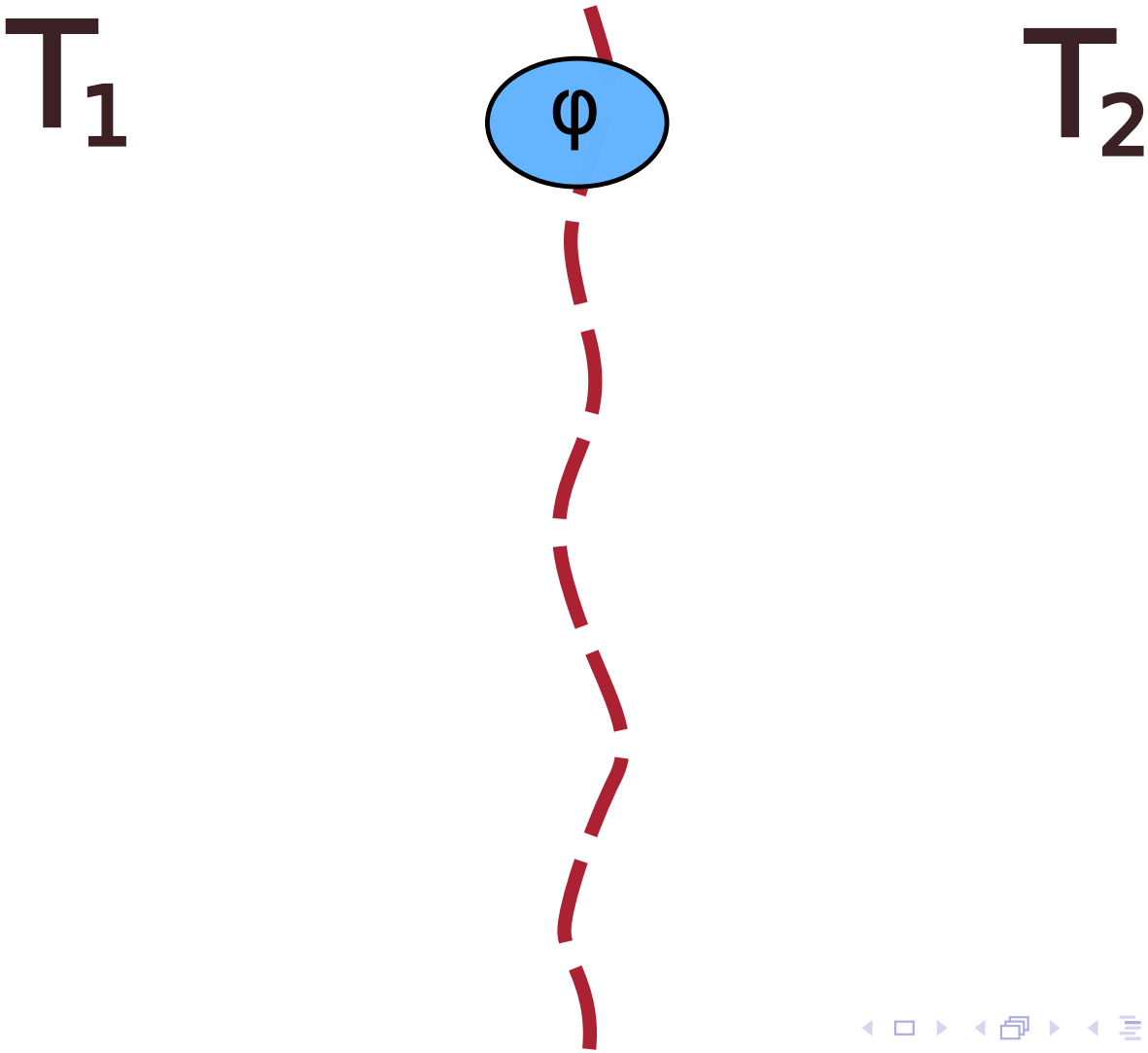


Let T_i be a Σ_i-theory, for $i = 1, 2$, and assume that

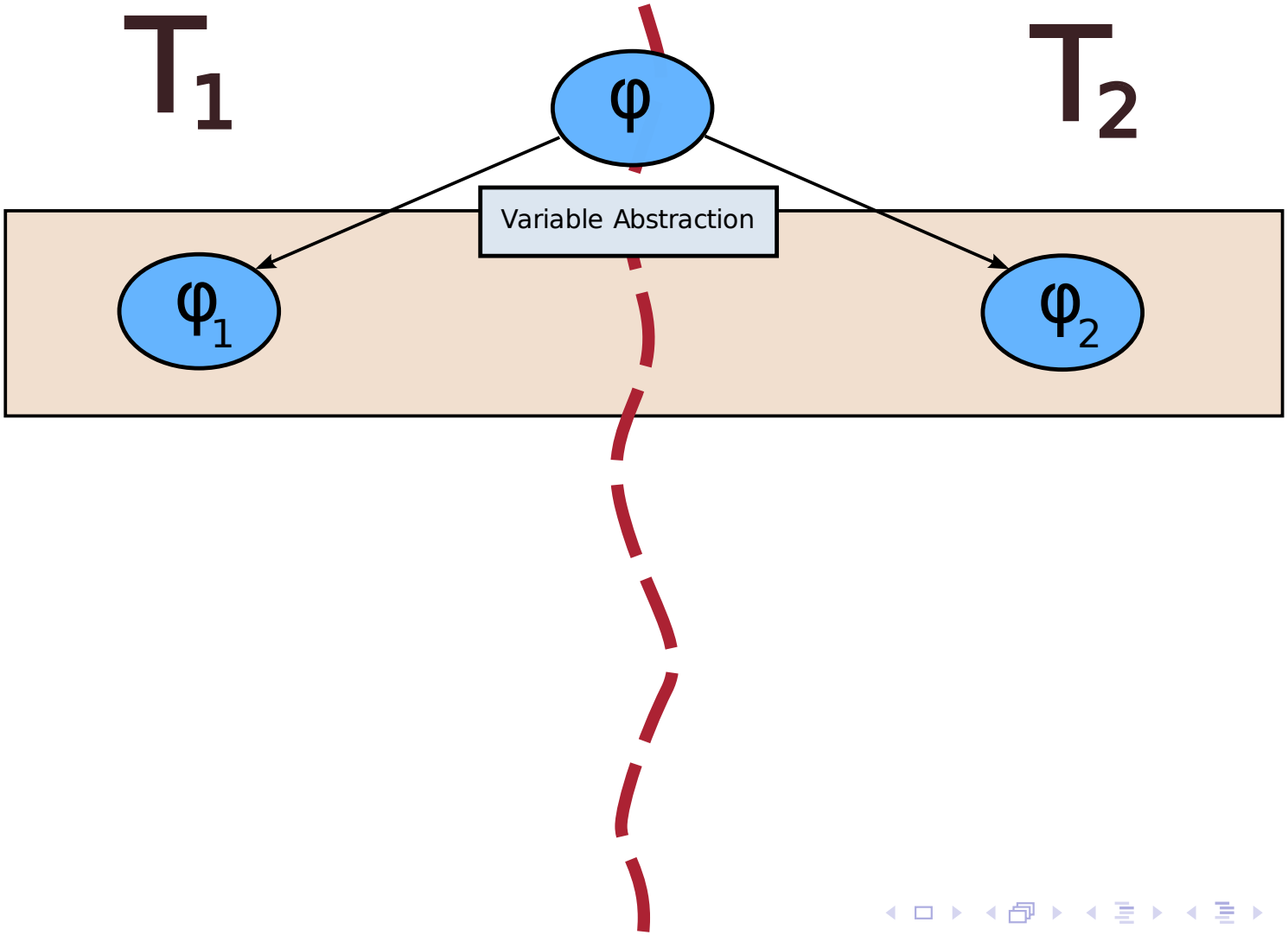
- we know how to decide quantifier-free satisfiability of T_i;
- signatures Σ_i are disjoint;
- T_2 is polite with respect S_2 where $\Sigma_1^{\mathbb{S}} \cap \Sigma_2^{\mathbb{S}} \subseteq S_2$.

Then we can decide $T_1 \oplus T_2$ with a modified Nelson-Oppen method.

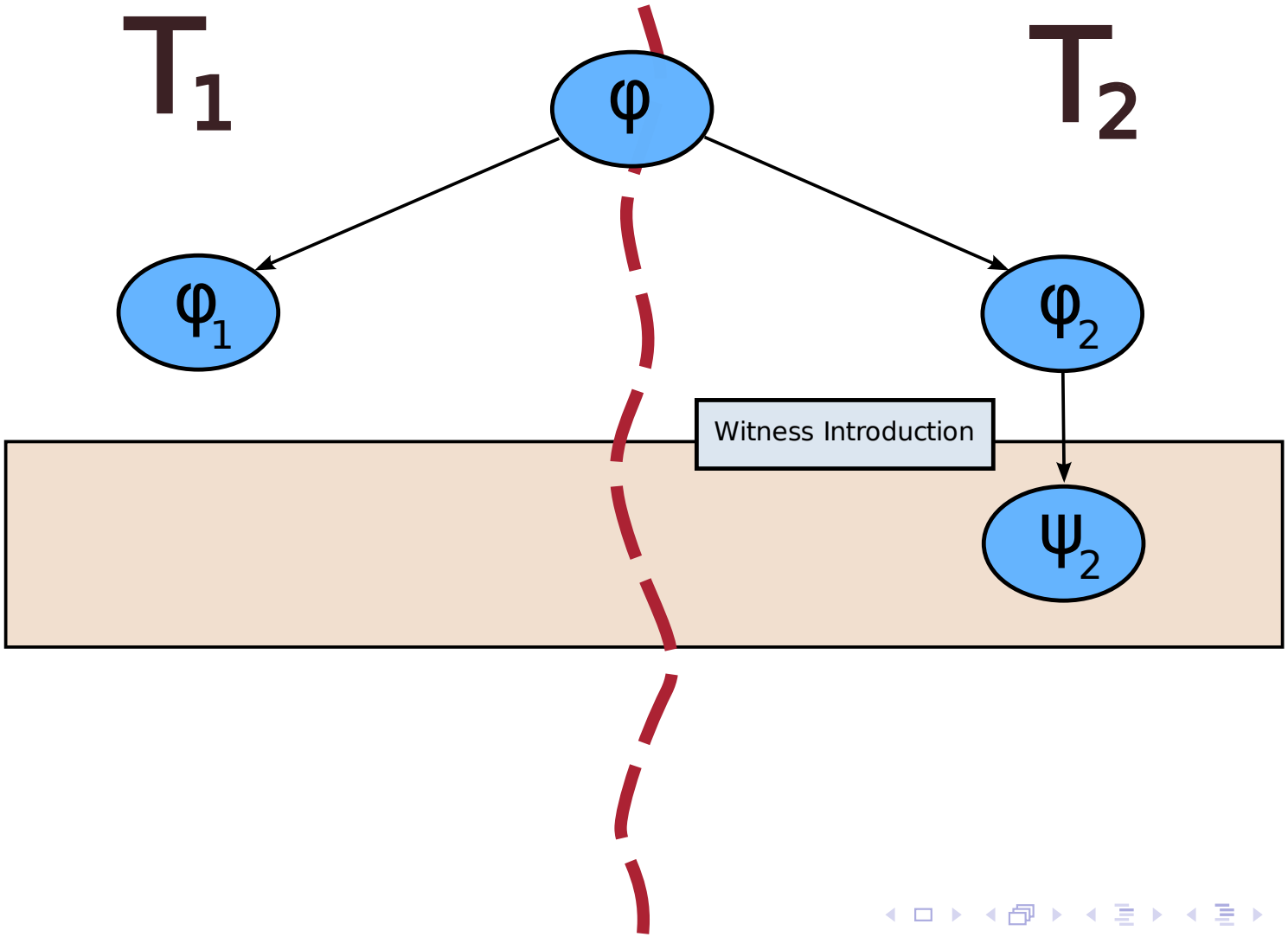
Combination Method



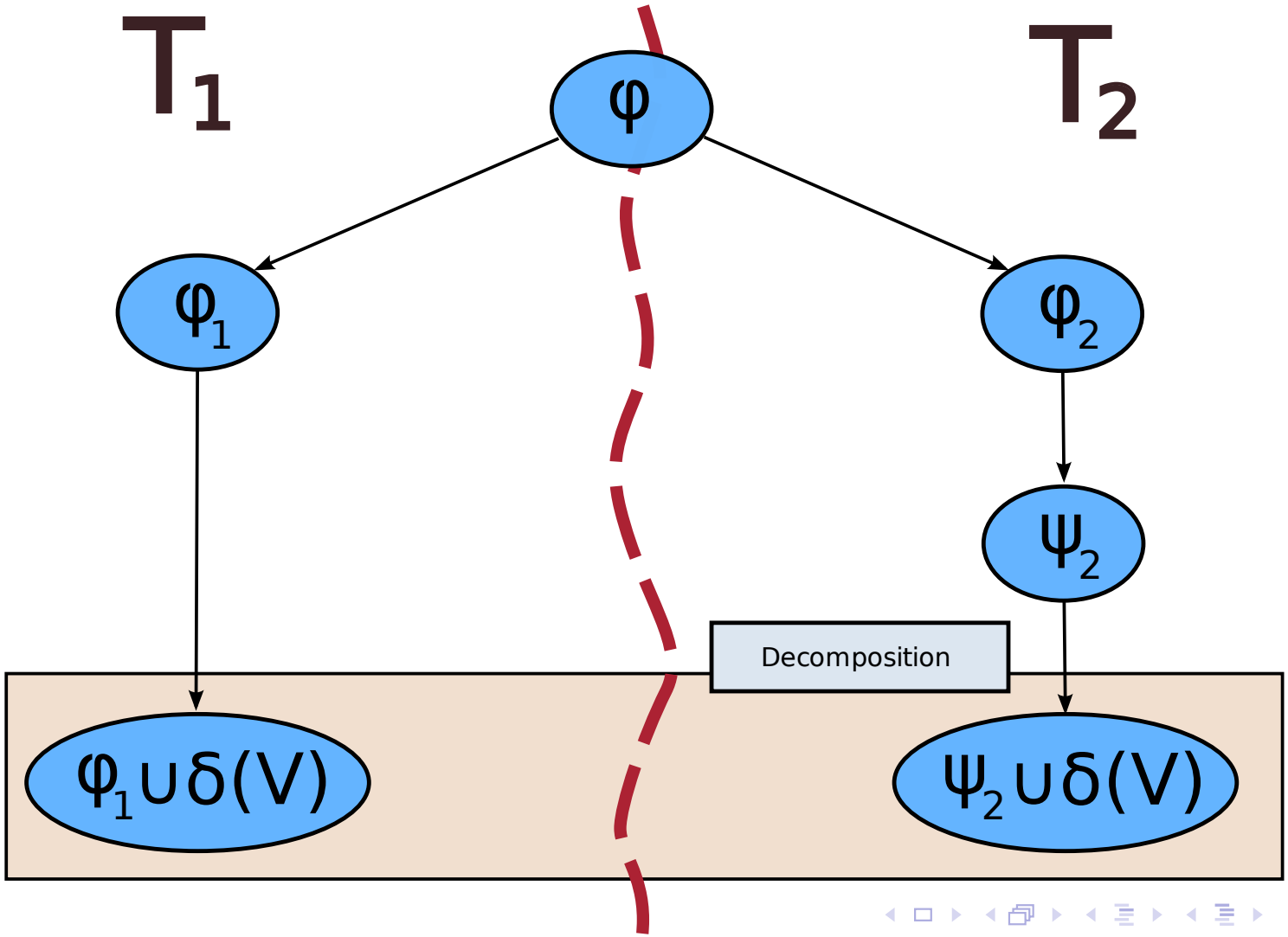
Combination Method



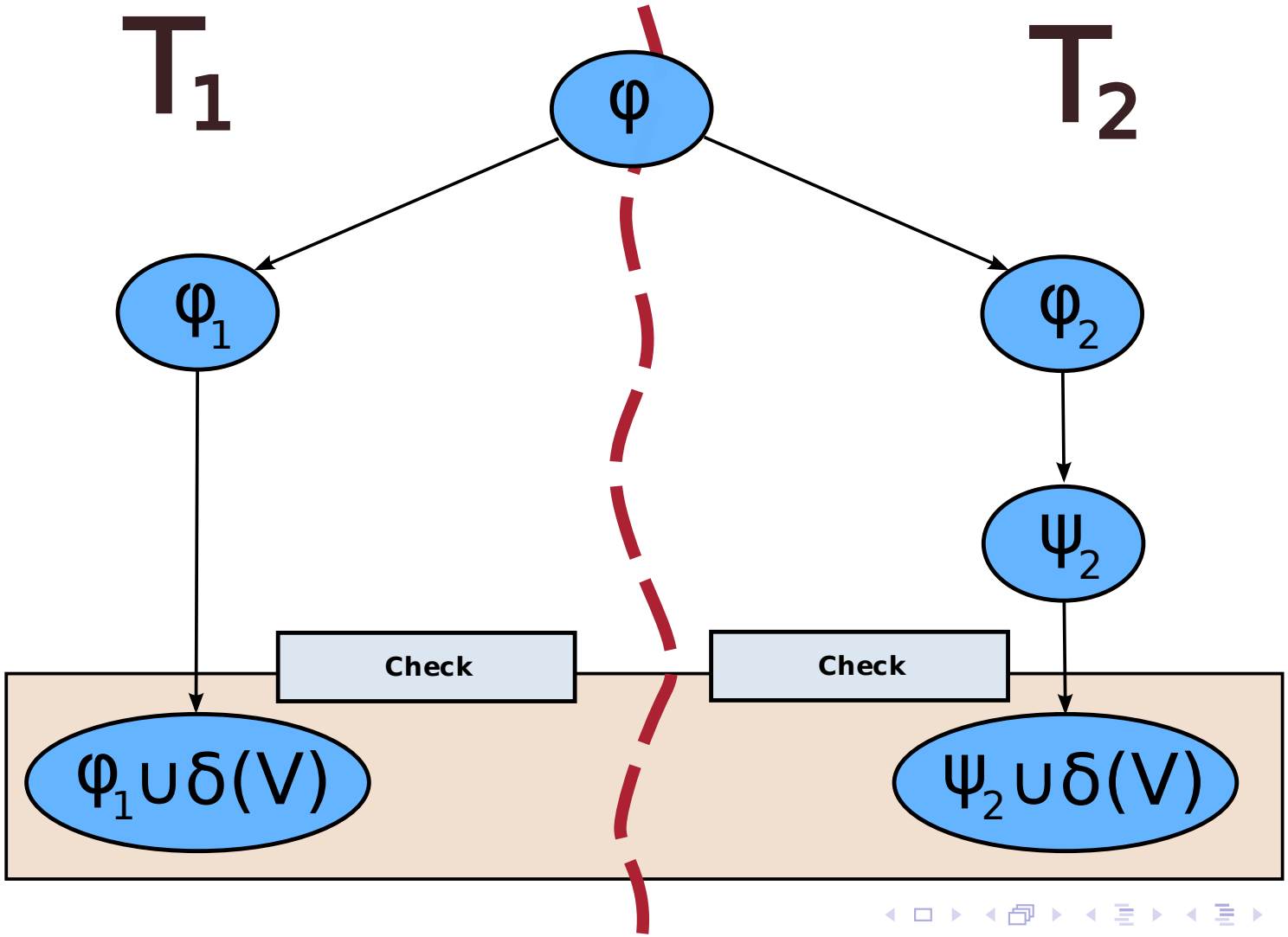
Combination Method



Combination Method



Combination Method



Main Points

- One theory has to be polite with respect to the shared sorts.
- Combination method is not symmetric.
- Implementation is easy – one additional step.
- Proving a theory polite can be hard.

Theory of Arrays

Theory of arrays T_{array} over the sorts $\{\text{array}, \text{index}, \text{elem}\}$ is polite with respect to sorts $\{\text{index}, \text{elem}\}$

Smoothness

We can always extend the model by adding as many index and elem domain points as necessary.

Finitely Witnessable

Witness function simply adds witness indices and elements for disequalities over arrays:

$$a_1 \neq a_2 \longrightarrow (\mathit{read}(a_1, i) = e_1 \wedge \mathit{read}(a_2, i) = e_2 \wedge e_1 \neq e_2)$$

Outline

Preservation of Politeness

We are interested in the following questions:

Is a combination of two polite theories polite?

Theory of two-dimensional arrays.

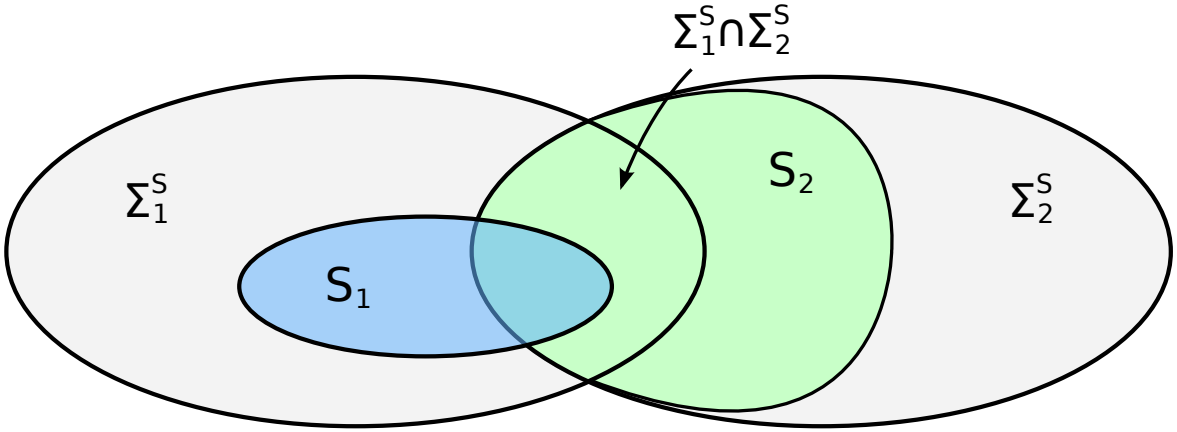
How to combine multiple polite theories?

Theory of n-dimensional arrays.

Is politeness preserved when merging two sorts?

Arrays with elements and indices from the same sort.

Preservation of Politeness



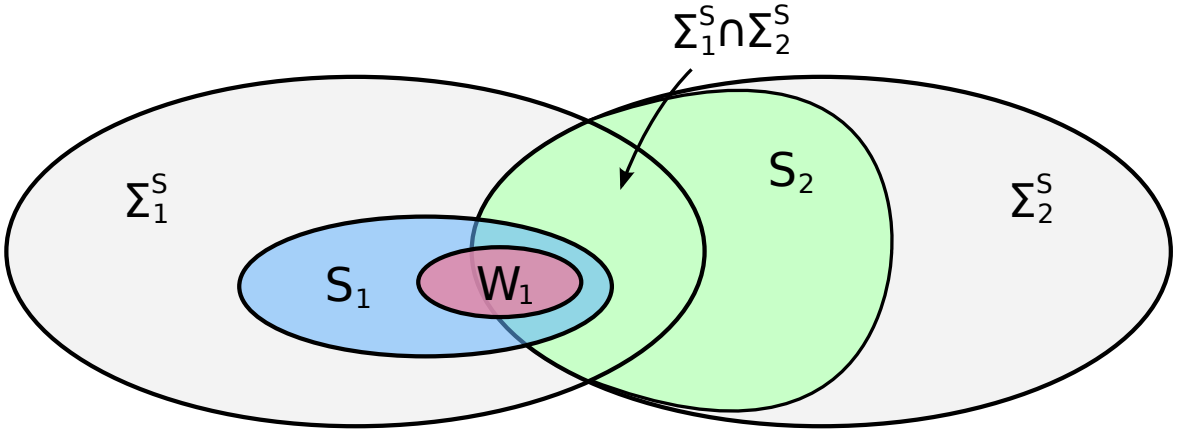
Theorem

Let Σ_1 and Σ_2 be disjoint signatures. If

- *T_i is a Σ_i-theory polite with respect to $S_i \subseteq \Sigma_i^{\mathbb{S}}$,*
- *$witness_1$ only introduces fresh variables in sorts $W_1 \subseteq \Sigma_1^{\mathbb{S}}$,*
- *$\Sigma_1^{\mathbb{S}} \cap \Sigma_2^{\mathbb{S}} \subseteq S_2$ and $W_1 \cap \Sigma_2^{\mathbb{S}} \subseteq S_1$,*

then $T_1 \oplus T_2$ is polite with respect to $S_1 \cup (S_2 \setminus \Sigma_1^{\mathbb{S}})$.

Preservation of Politeness



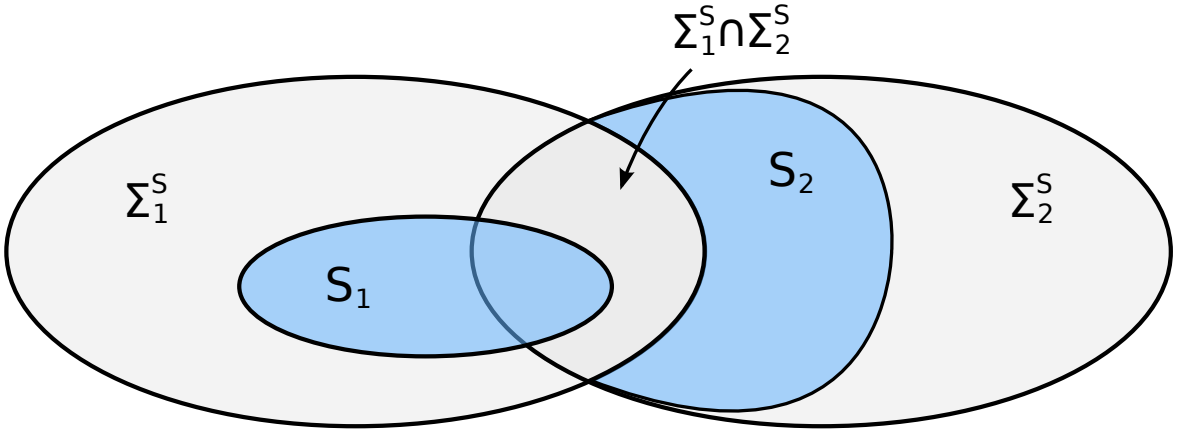
Theorem

Let Σ_1 and Σ_2 be disjoint signatures. If

- *T_i is a Σ_i-theory polite with respect to $S_i \subseteq \Sigma_i^{\mathbb{S}}$,*
- *$witness_1$ only introduces fresh variables in sorts $W_1 \subseteq \Sigma_1^{\mathbb{S}}$,*
- *$\Sigma_1^{\mathbb{S}} \cap \Sigma_2^{\mathbb{S}} \subseteq S_2$ and $W_1 \cap \Sigma_2^{\mathbb{S}} \subseteq S_1$,*

then $T_1 \oplus T_2$ is polite with respect to $S_1 \cup (S_2 \setminus \Sigma_1^{\mathbb{S}})$.

Preservation of Politeness



Theorem

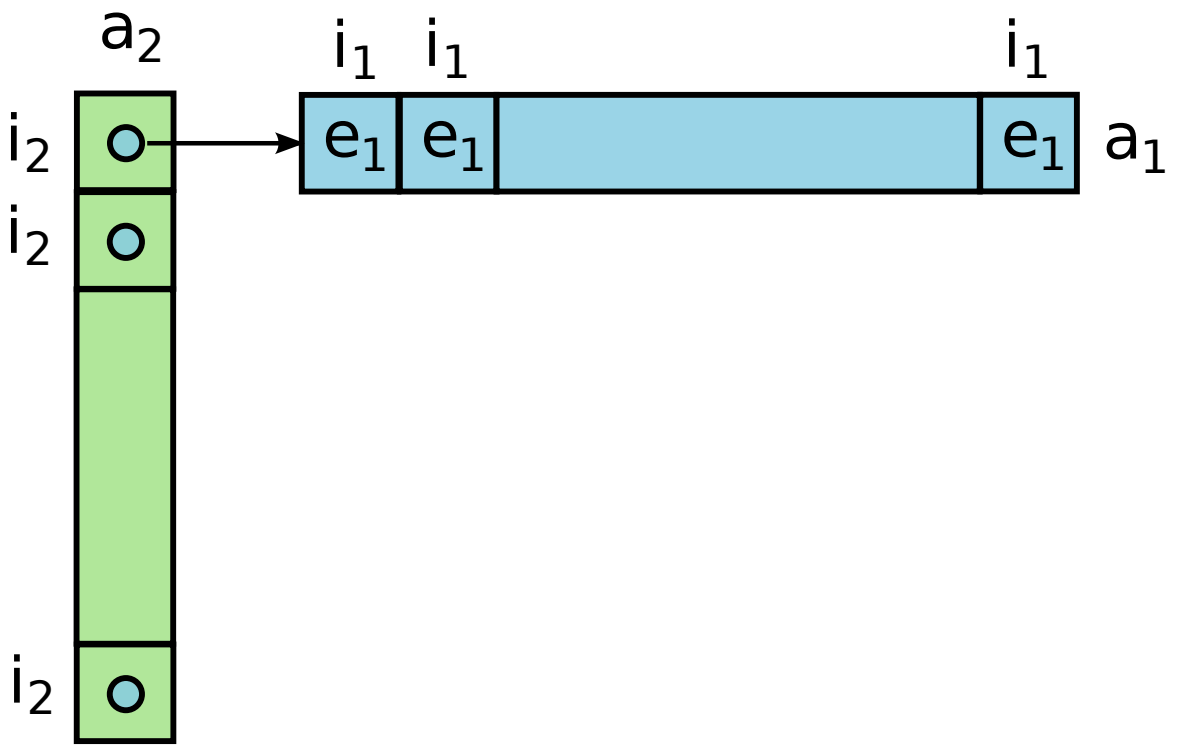
Let Σ_1 and Σ_2 be disjoint signatures. If

- *T_i is a Σ_i-theory polite with respect to $S_i \subseteq \Sigma_i^{\mathbb{S}}$,*
- *$witness_1$ only introduces fresh variables in sorts $W_1 \subseteq \Sigma_1^{\mathbb{S}}$,*
- *$\Sigma_1^{\mathbb{S}} \cap \Sigma_2^{\mathbb{S}} \subseteq S_2$ and $W_1 \cap \Sigma_2^{\mathbb{S}} \subseteq S_1$,*

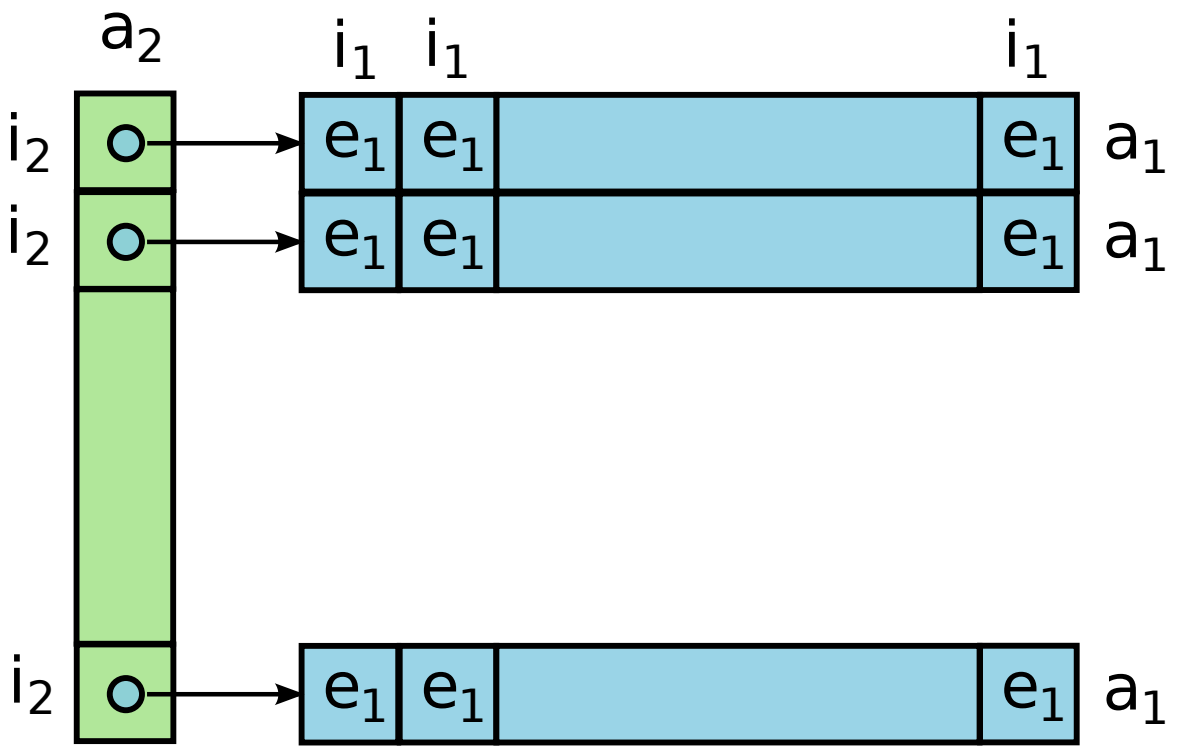
then $T_1 \oplus T_2$ is polite with respect to $S_1 \cup (S_2 \setminus \Sigma_1^{\mathbb{S}})$.

Theory of Arrays

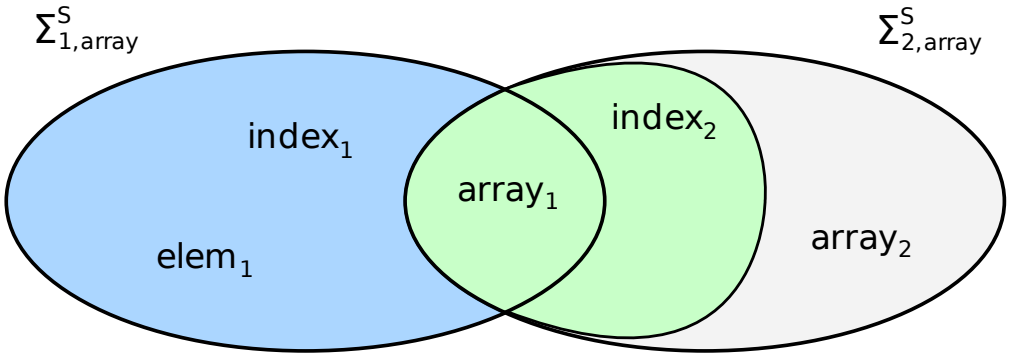
Theory of Arrays



Theory of Arrays



Theory of Arrays

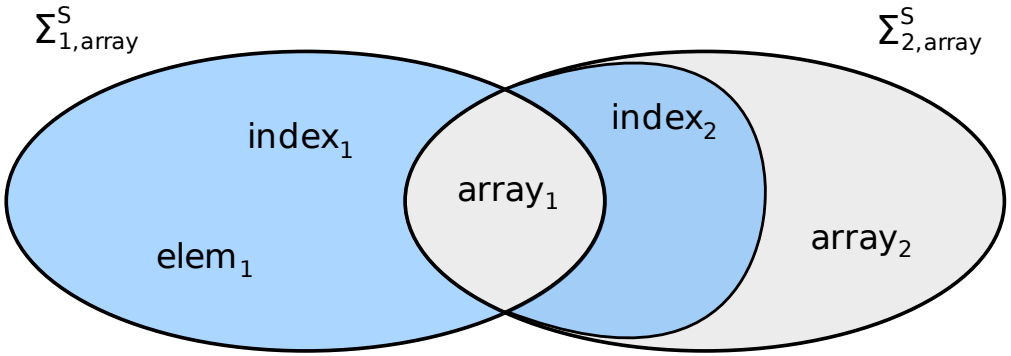


- Two theories of arrays

$$T_{1,\text{array}} : \Sigma^{\mathbb{S}}_{1,\text{array}} = \{\text{array}_1, \text{index}_1, \text{elem}_1\} \ ,$$
$$T_{2,\text{array}} : \Sigma^{\mathbb{S}}_{2,\text{array}} = \{\text{array}_2, \text{index}_2, \text{array}_1\} \ .$$

- Combined theory is the theory of two-dimensional arrays
- Polite with respect to sorts of indices and elements
- How about *n*-dimensional arrays?

Theory of Arrays

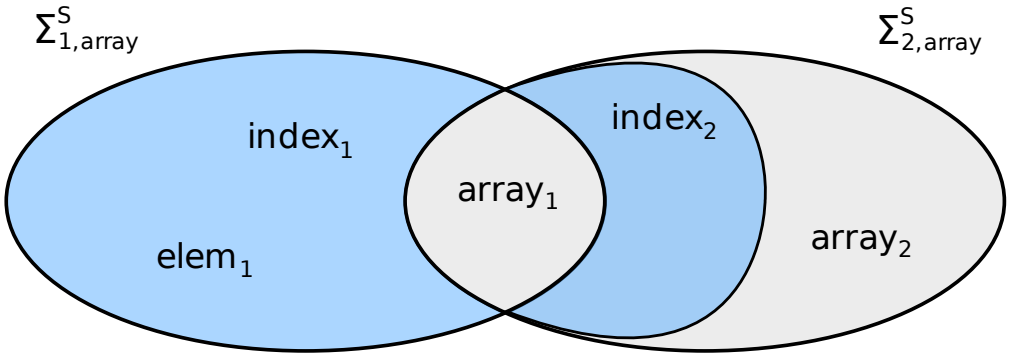


- Two theories of arrays

$$T_{1,\text{array}} : \Sigma^{\mathbb{S}}_{1,\text{array}} = \{\text{array}_1, \text{index}_1, \text{elem}_1\} \ ,$$
$$T_{2,\text{array}} : \Sigma^{\mathbb{S}}_{2,\text{array}} = \{\text{array}_2, \text{index}_2, \text{array}_1\} \ .$$

- Combined theory is the theory of two-dimensional arrays
- Polite with respect to sorts of indices and elements
- How about *n*-dimensional arrays?

Theory of Arrays



- Two theories of arrays

$$T_{1,\text{array}} : \Sigma^{\mathbb{S}}_{1,\text{array}} = \{\text{array}_1, \text{index}_1, \text{elem}_1\} \ ,$$
$$T_{2,\text{array}} : \Sigma^{\mathbb{S}}_{2,\text{array}} = \{\text{array}_2, \text{index}_2, \text{array}_1\} \ .$$

- Combined theory is the theory of two-dimensional arrays
- Polite with respect to sorts of indices and elements
- How about *n*-dimensional arrays?

Combination of Multiple Polite Theories

Theorem

Let T_i be a Σ_i-theory, for $1 \leq i \leq n$. Assume that

- *T_i is decidable (QF fragment),*
- *T_i is polite with respect to S_i,*
- *T_i and T_j can be combined via previous theorem, for $i < j$,*

then $T_1 \oplus \cdots \oplus T_n$ is decidable and polite with respect to

$$S = \bigcup_{j=1}^{n} (S_j \setminus (\bigcup_{i<j} \Sigma_i^{\mathbb{S}})) \ .$$

Multi-Dimensional Arrays

- Different layers in the theory of n-dimensional arrays

$$T_{\text{array},1} : \Sigma^{\mathbb{S}}_{\text{array},1} = \{\text{array}_1, \text{index}_1, \text{elem}_1\} \ ,$$
$$T_{\text{array},k} : \Sigma^{\mathbb{S}}_{\text{array},k} = \{\text{array}_k, \text{index}_k, \text{array}_{k-1}\} \ .$$

- The theories satisfy the assumption of the previous theorem and we can combine them into the full theory

$$T_{\text{array}} = T_{\text{array},1} \oplus T_{\text{array},2} \oplus \cdots \oplus T_{\text{array},n} \ .$$

- Resulting theory is polite with respect to the union of all indices and elements

$$S = \{\text{index}_1, \text{index}_2, \ldots, \text{index}_n, \text{elem}_1\} \ .$$

Multi-Dimensional Arrays

- Different layers in the theory of n-dimensional arrays

$$T_{\text{array},1} : \Sigma^{\mathbb{S}}_{\text{array},1} = \{\text{array}_1, \textbf{index}_1, \textbf{elem}_1\} \ ,$$
$$T_{\text{array},k} : \Sigma^{\mathbb{S}}_{\text{array},k} = \{\text{array}_k, \textbf{index}_k, \textbf{array}_{k-1}\} \ .$$

- The theories satisfy the assumption of the previous theorem and we can combine them into the full theory

$$T_{\text{array}} = T_{\text{array},1} \oplus T_{\text{array},2} \oplus \cdots \oplus T_{\text{array},n} \ .$$

- Resulting theory is polite with respect to the union of all indices and elements

$$S = \{\text{index}_1, \text{index}_2, \ldots, \text{index}_n, \text{elem}_1\} \ .$$

Multi-Dimensional Arrays

- Different layers in the theory of n-dimensional arrays

$$T_{\text{array},1} : \Sigma^{\mathbb{S}}_{\text{array},1} = \{\text{array}_1, \textbf{index}_1, \textbf{elem}_1\} \ ,$$
$$T_{\text{array},k} : \Sigma^{\mathbb{S}}_{\text{array},k} = \{\text{array}_k, \textbf{index}_k, \textbf{array}_{k-1}\} \ .$$

- The theories satisfy the assumption of the previous theorem and we can combine them into the full theory

$$T_{\text{array}} = T_{\text{array},1} \oplus T_{\text{array},2} \oplus \cdots \oplus T_{\text{array},n} \ .$$

- Resulting theory is polite with respect to the union of all indices and elements

$$S = \{\text{index}_1, \text{index}_2, \ldots, \text{index}_n, \text{elem}_1\} \ .$$

Multi-Dimensional Arrays

- Different layers in the theory of n-dimensional arrays

$$T_{\text{array},1} : \Sigma^{\mathbb{S}}_{\text{array},1} = \{\text{array}_1, \textbf{index}_1, \textbf{elem}_1\} \ ,$$
$$T_{\text{array},k} : \Sigma^{\mathbb{S}}_{\text{array},k} = \{\text{array}_k, \textbf{index}_k, \textbf{array}_{k-1}\} \ .$$

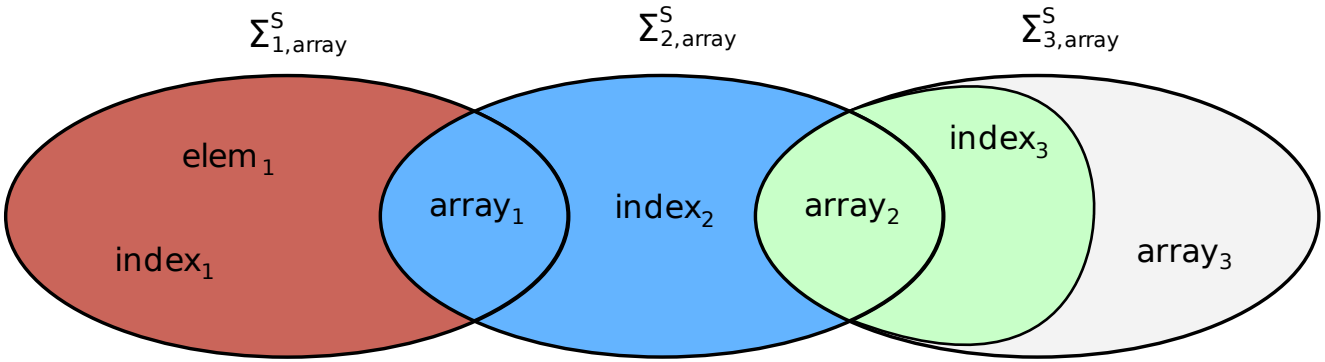
- The theories satisfy the assumption of the previous theorem and we can combine them into the full theory

$$T_{\text{array}} = T_{\text{array},1} \oplus T_{\text{array},2} \oplus \cdots \oplus T_{\text{array},n} \ .$$

- Resulting theory is polite with respect to the union of all indices and elements

$$S = \{\text{index}_1, \text{index}_2, \ldots, \text{index}_n, \text{elem}_1\} \ .$$

Multi-Dimensional Arrays



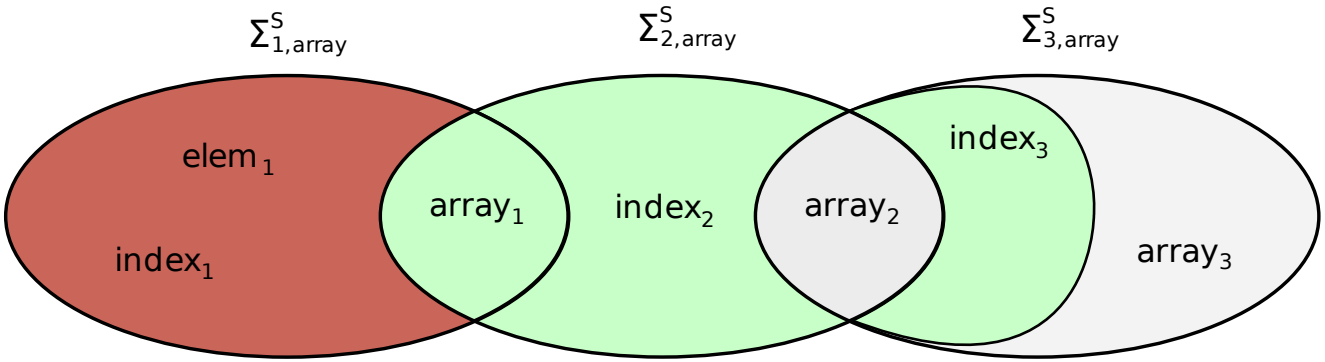
- The theories satisfy the assumption of the previous theorem and we can combine them into the full theory

$$T_{\text{array}} = T_{\text{array},1} \oplus T_{\text{array},2} \oplus \cdots \oplus T_{\text{array},n} \ .$$

- Resulting theory is polite with respect to the union of all indices and elements

$$S = \{\text{index}_1, \text{index}_2, \ldots, \text{index}_n, \text{elem}_1\} \ .$$

Multi-Dimensional Arrays



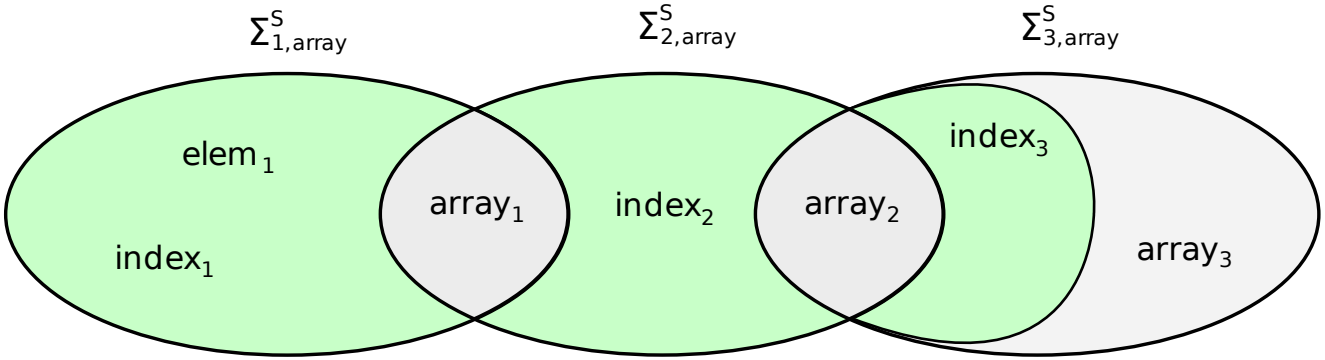
- The theories satisfy the assumption of the previous theorem and we can combine them into the full theory

$$T_{\text{array}} = T_{\text{array},1} \oplus T_{\text{array},2} \oplus \cdots \oplus T_{\text{array},n} \ .$$

- Resulting theory is polite with respect to the union of all indices and elements

$$S = \{\text{index}_1, \text{index}_2, \ldots, \text{index}_n, \text{elem}_1\} \ .$$

Multi-Dimensional Arrays



- The theories satisfy the assumption of the previous theorem and we can combine them into the full theory

$$T_{\text{array}} = T_{\text{array},1} \oplus T_{\text{array},2} \oplus \cdots \oplus T_{\text{array},n} \ .$$

- Resulting theory is polite with respect to the union of all indices and elements

$$S = \{\text{index}_1, \text{index}_2, \ldots, \text{index}_n, \text{elem}_1\} \ .$$

Merging of Sorts

- We know that the theory of arrays

$$T_{\text{array}} : \Sigma^{\mathbb{S}}_{\text{array}} = \{\text{array}, \text{index}, \text{elem}\}$$

  is polite with respect to $\{\text{index}, \text{elem}\}$.
- What if we want a theory where indices and elements are of the same sort? For example

$$T_{\text{array(bv)}} : \Sigma^{\mathbb{S}}_{\text{array(bv)}} = \{\text{array}, \text{bv}\}$$

- This is a different theory, where we can express facts like $\mathit{read}(a, i) \neq i$

Merging of Sorts

Definition (Signature Instantiation)

Let $\Sigma = (S, F, P)$ be a signature. We call $\Sigma_s^{s_1=s_2} = (S', F', P')$ a signature instantiation by sort equality $s_1 = s_2$, for sorts $s_1, s_2 \in S$ and $s \notin S$, if the following holds:

- $S' = S \setminus \{s_1, s_2\} \cup \{s\}$;
- F' contains the same function symbols as F except that we replace s_1 and s_2 with s in every arity;
- P' contains the same predicate symbols as P except that we replace s_1 and s_2 with s in every arity.

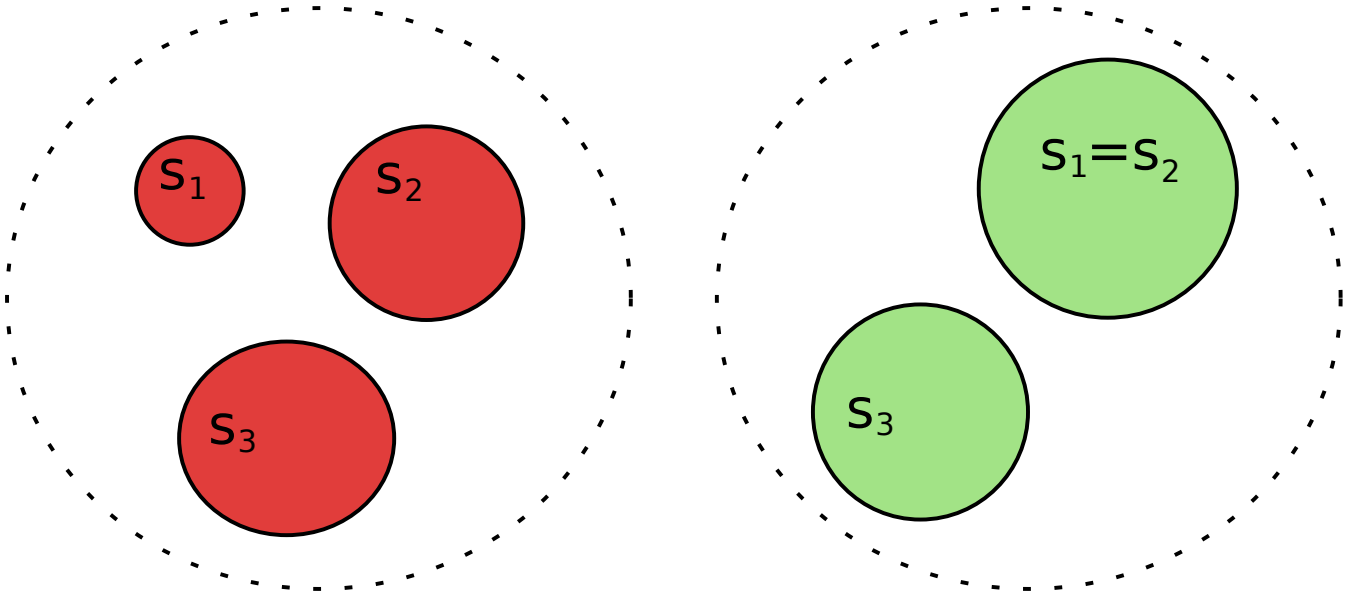
Merging of Sorts

Definition (Theory Instantiation)

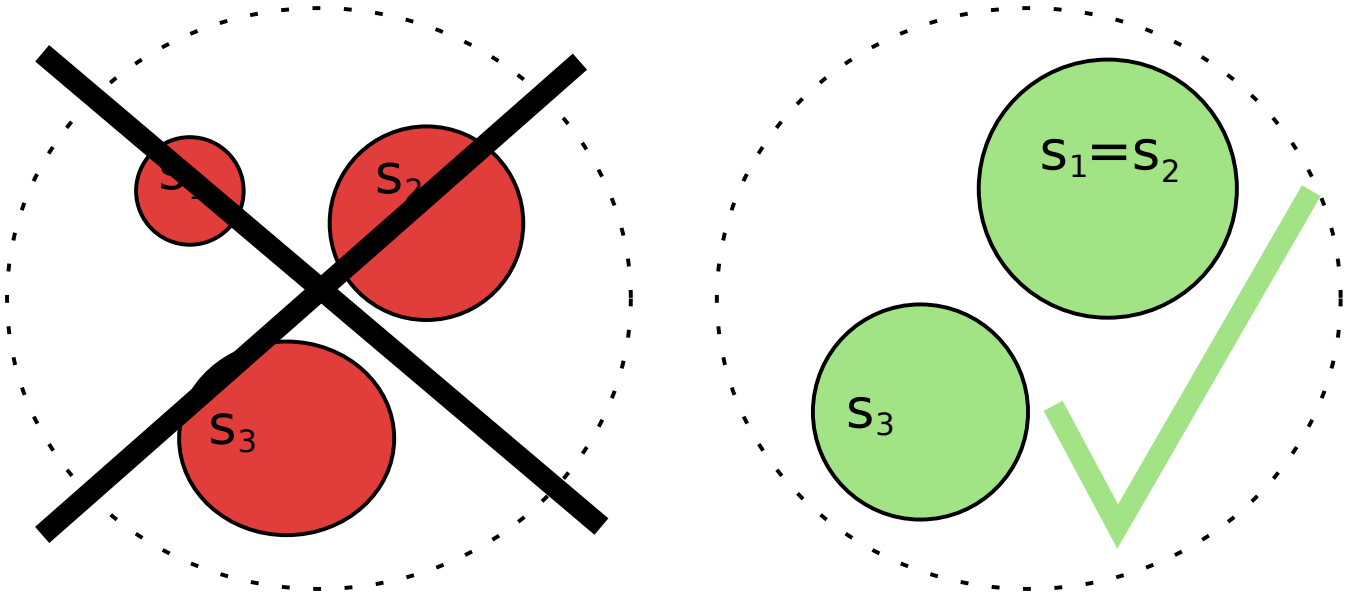
Let Σ be a signature and $T = (\Sigma, \mathbf{A})$ be a Σ-theory. We call a theory $T_s^{s_1=s_2} = \left(\Sigma_s^{s_1=s_2}, \mathbf{B}\right)$ a theory instantiated by sort equality $s_1 = s_2$, for sorts $s_1, s_2 \in \Sigma^{\mathbb{S}}$ and $s \notin \Sigma^{\mathbb{S}}$, when $\mathcal{B} \in \mathbf{B}$ iff there exists an $\mathcal{A} \in \mathbf{A}$ such that

- $B_s = A_{s_1} = A_{s_2}$,
- $B_\sigma = A_\sigma$, for $\sigma \neq s$,
- all predicate and function symbols are interpreted in $\mathcal{B}$ exactly as they are interpreted in $\mathcal{A}$.

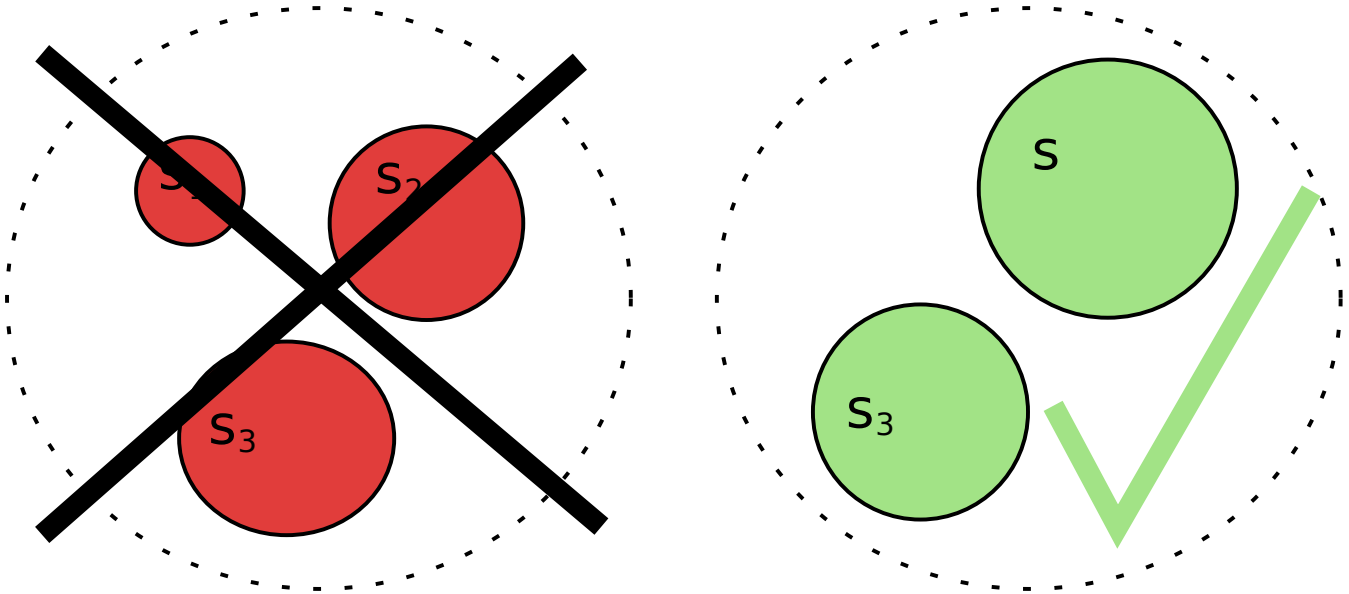
Merging of Sorts



Merging of Sorts



Merging of Sorts



Merging of Sorts

Theorem

Let Σ be a signature, $s_1, s_2 \in \Sigma^{\mathbb{S}}$, and $s \notin \Sigma^{\mathbb{S}}$. If Σ-theory T is polite with respect to S, where $s_1, s_2 \in S$, then $T_s^{s_1=s_2}$ is polite with respect to $(S \setminus \{s_1, s_2\}) \cup \{s\}$.

Arrays over Bit-Vectors

- Theory of n-dimensional arrays

$$T_{\text{array}} = T_{\text{array},1} \oplus T_{\text{array},2} \oplus \cdots \oplus T_{\text{array},n} \ .$$

is polite with respect to the sorts of indices and elements

$$S = \{\text{index}_1, \text{index}_2, \ldots, \text{index}_n, \text{elem}_1\} \ .$$

- We can now equate all the indices and elements to obtain a theory of arrays

$$T_{\text{array(bv)}} = \left(T_{\text{array}}\right)_{\text{bv}}^{\text{elem}_1 = \text{index}_1 = \cdots = \text{index}_n}$$

that is polite with respect to the sort of bv.

Arrays over Bit-Vectors

- Theory of n-dimensional arrays

$$T_{\text{array}} = T_{\text{array},1} \oplus T_{\text{array},2} \oplus \cdots \oplus T_{\text{array},n} \ .$$

is polite with respect to the sorts of indices and elements

$$S = \{\text{index}_1, \text{index}_2, \ldots, \text{index}_n, \text{elem}_1\} \ .$$

- We can now equate all the indices and elements to obtain a theory of arrays

$$T_{\text{array(bv)}} = \left(T_{\text{array}}\right)_{\text{bv}}^{\text{elem}_1 = \text{index}_1 = \cdots = \text{index}_n}$$

that is polite with respect to the sort of bv.

Conclusion

The presented results allow us to reason about polite theories modularly. We have shown the following:

- Politeness is preserved under polite combination.
- A combination theorem for multiple polite theories.
- Politeness is preserved when merging polite sorts.
- All results are applicable in practice, as shown on the theory of arrays.

Thank You

Questions?