New Insights on the Nelson-Oppen Combination Method

Clark Barrett

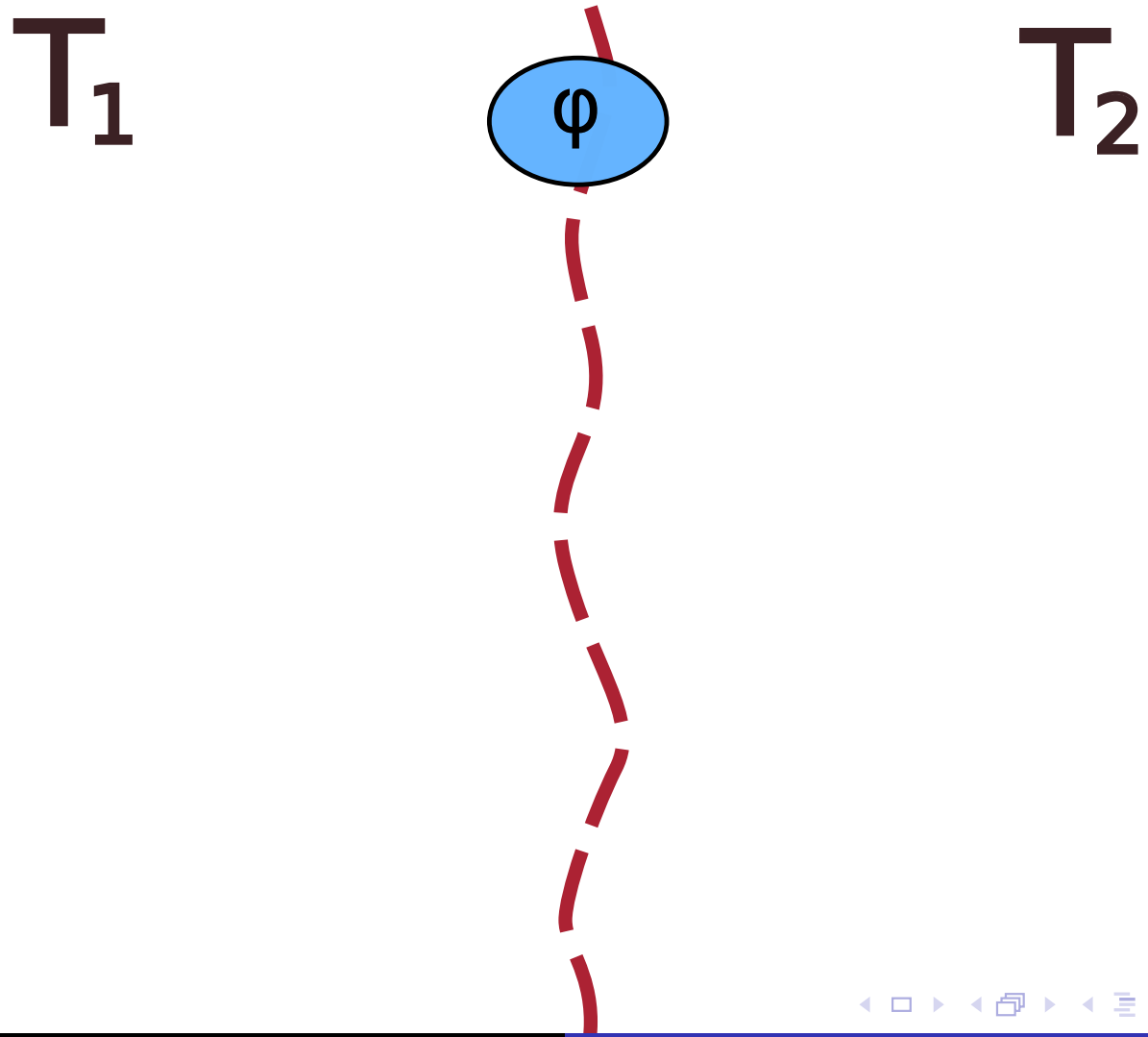
New York University

CS357, Stanford University, Nov 2, 2015

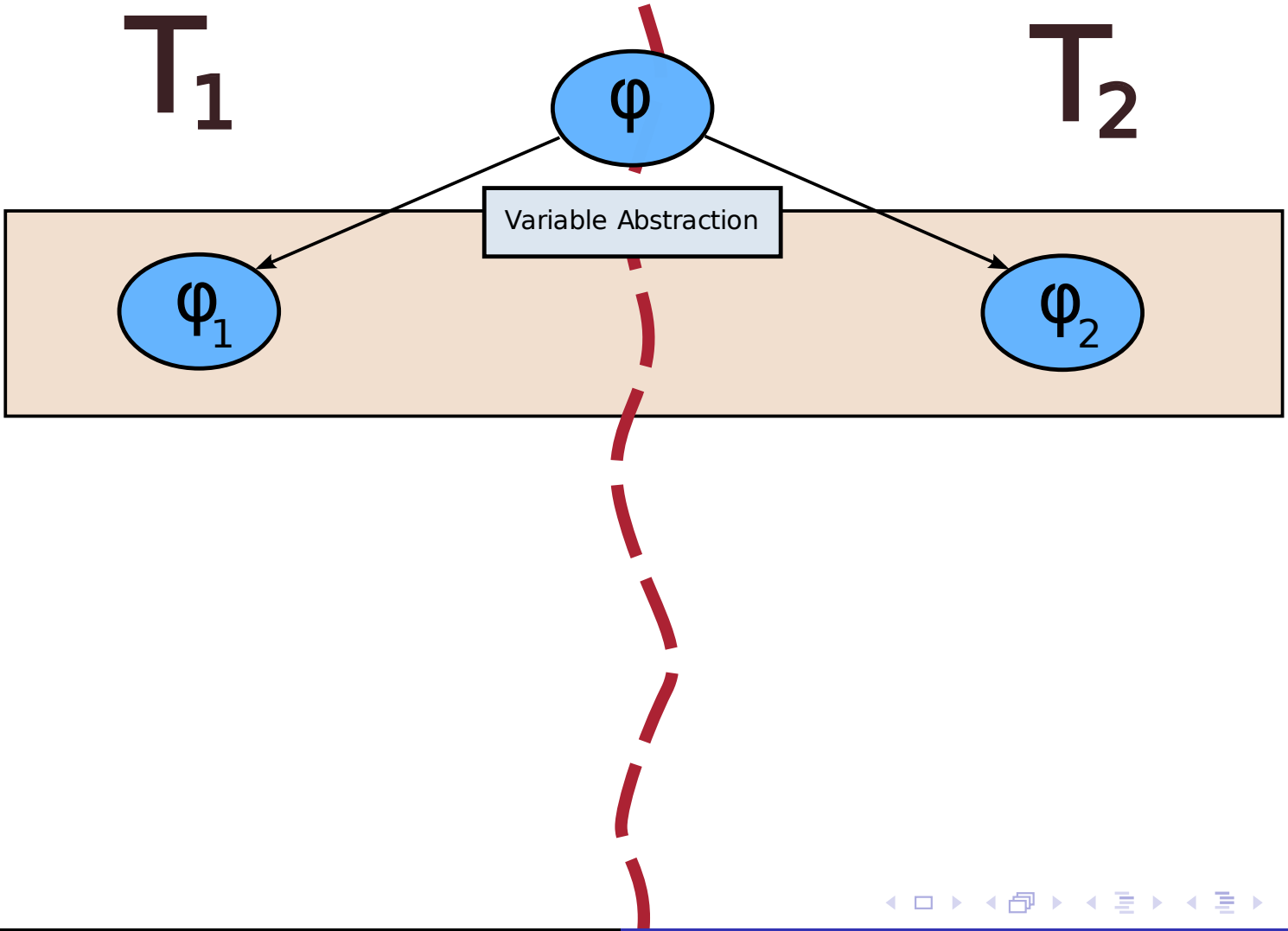
Outline

Outline

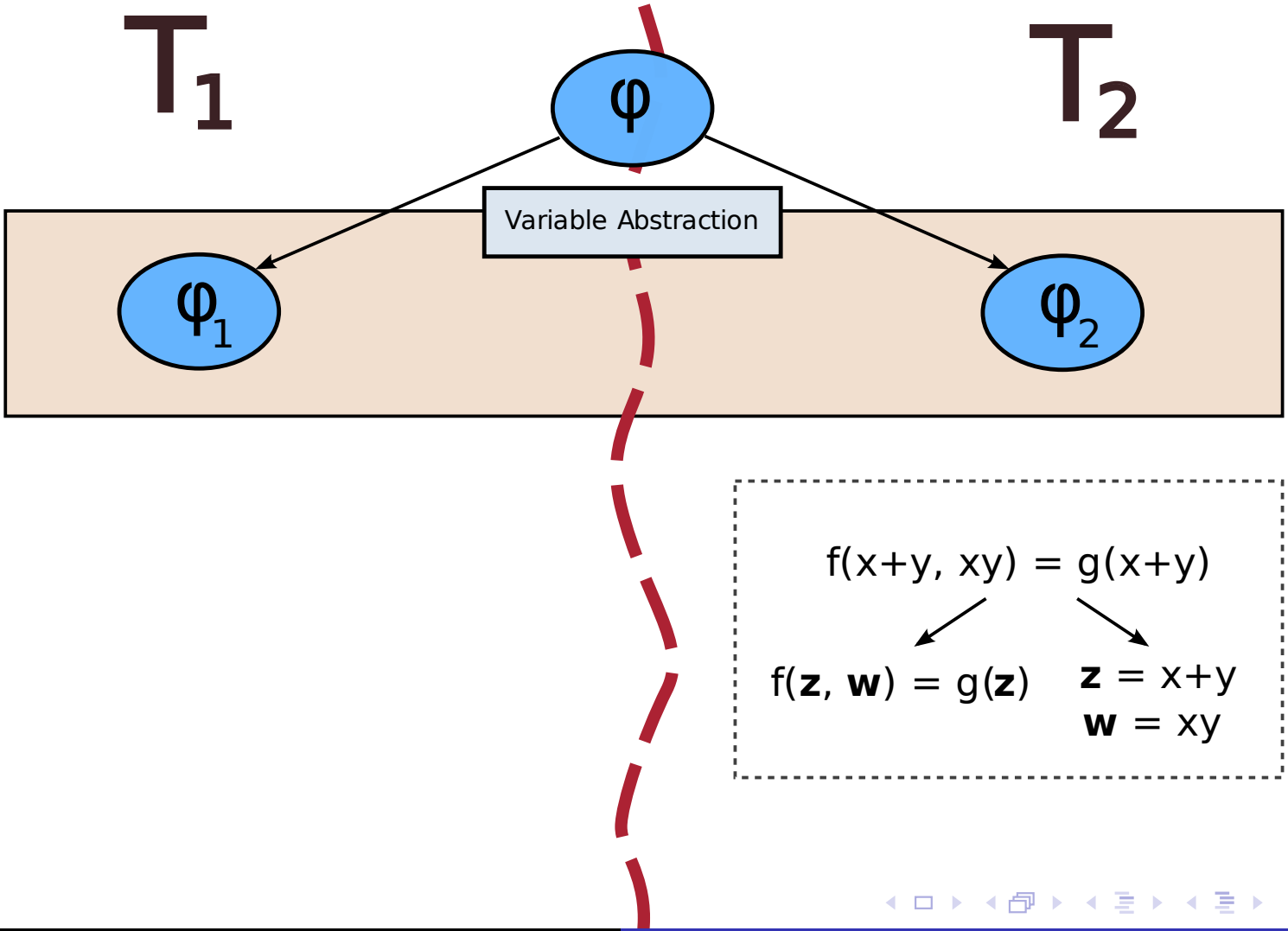
Nelson-Oppen: Idea (1979)



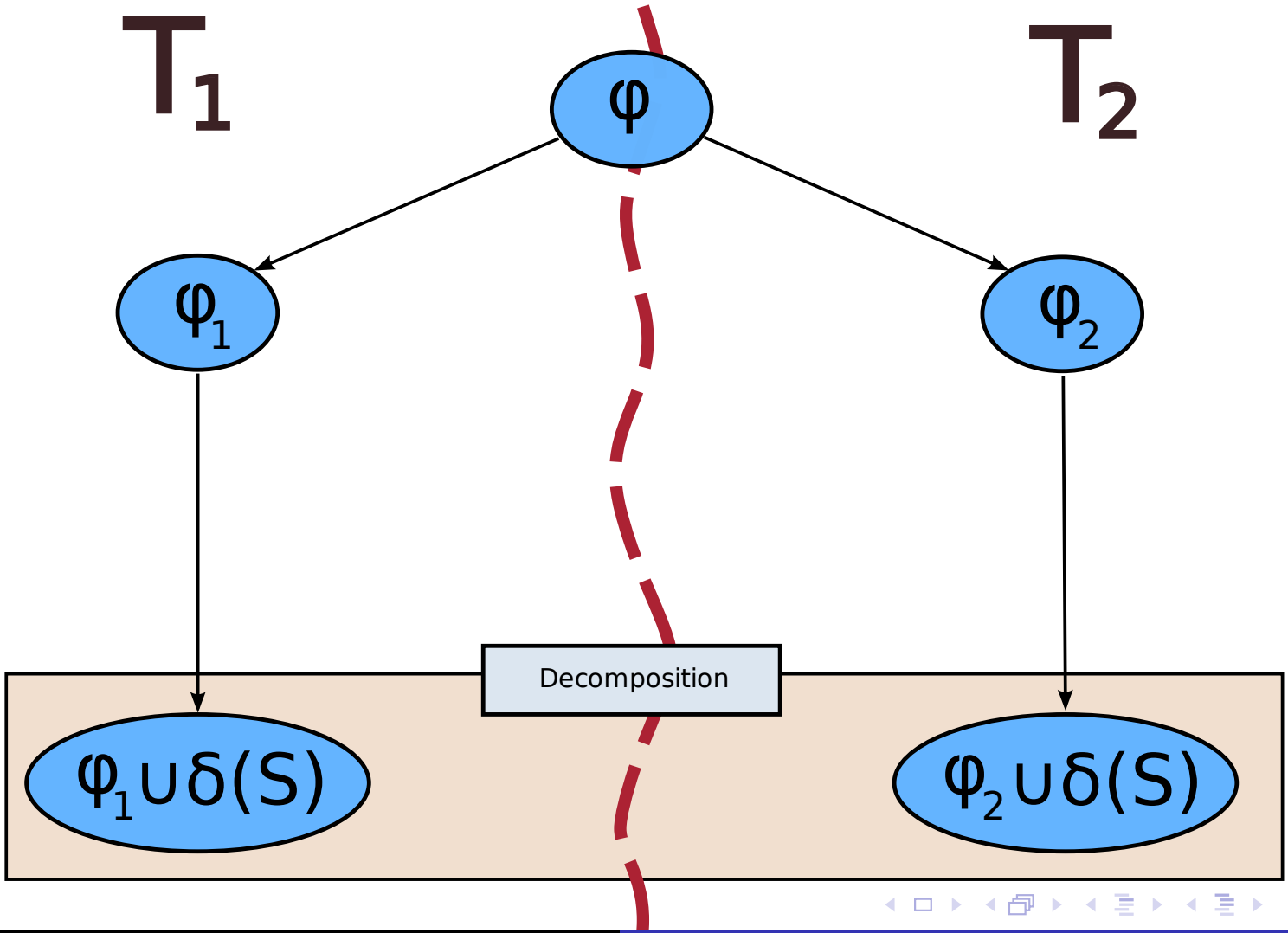
Nelson-Oppen: Idea (1979)



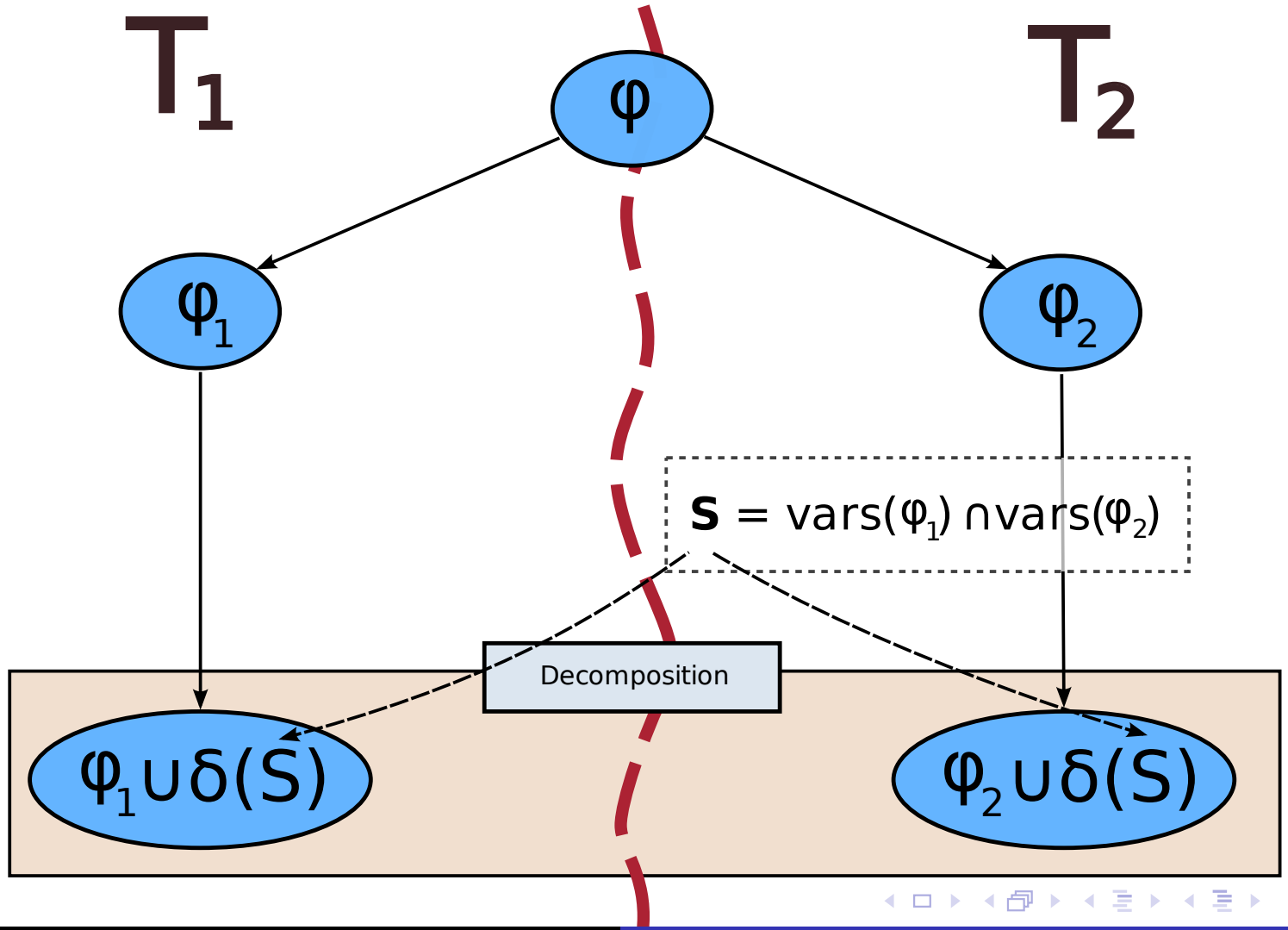
Nelson-Oppen: Idea (1979)



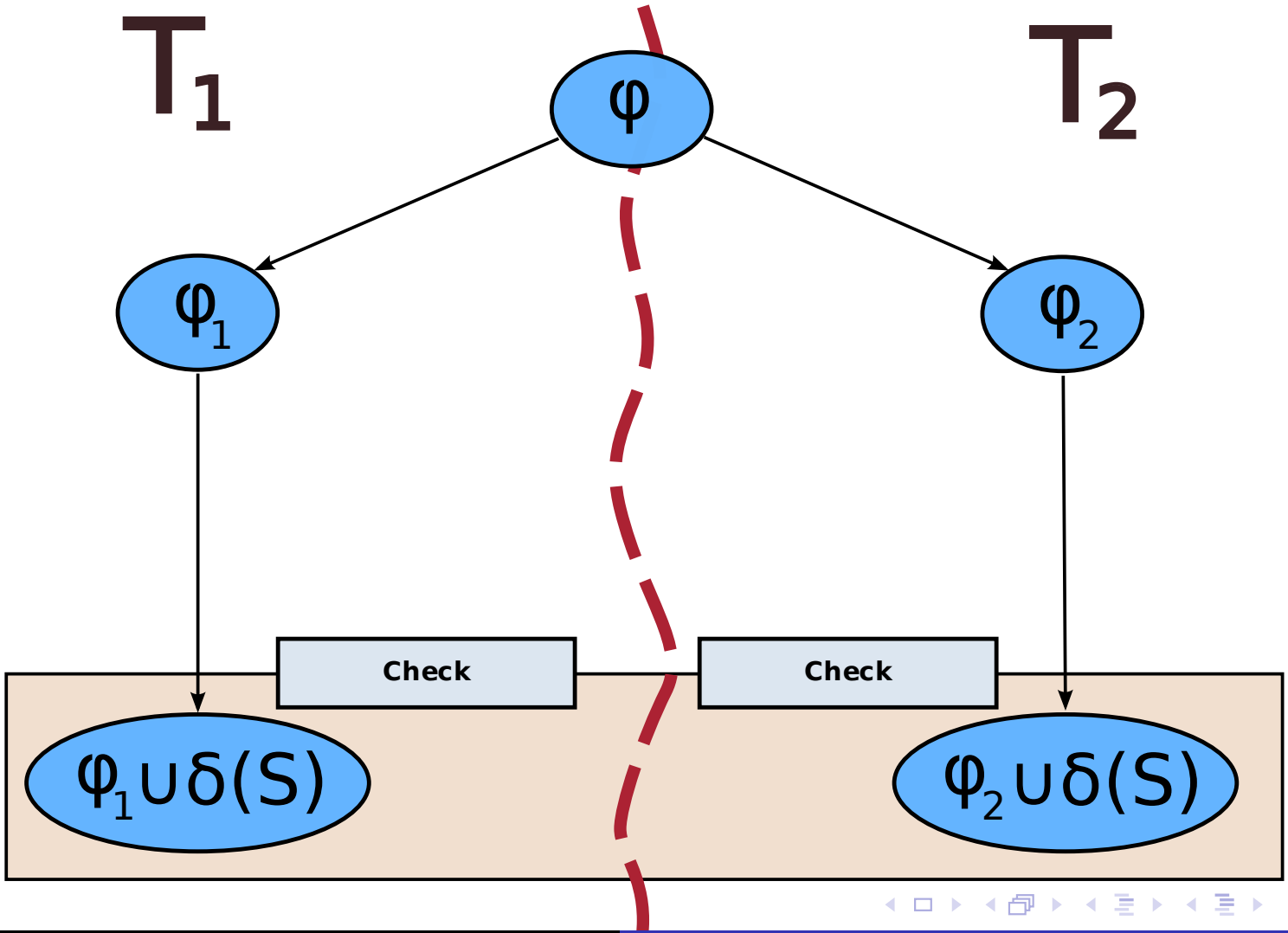
Nelson-Oppen: Idea (1979)



Nelson-Oppen: Idea (1979)



Nelson-Oppen: Idea (1979)



Outline

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 constraints:

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

- There are only 4 different 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 constraints:

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

- There are only 4 different such arrays:

Arrays and Bitvectors

Combination of arrays with bit-vectors:

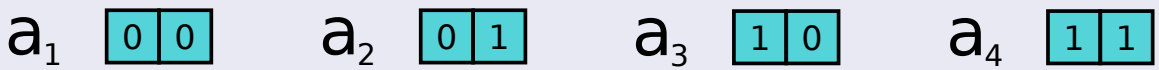
1. Theory T_{bv} of bit-vectors of size 1
2. Theory T_{array} of arrays over bit-vectors

Nelson-Oppen

- Consider the following set of constraints:

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

- There are only 4 different 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 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

Polite Theories

- Polite theories provide an elegant solution (Ranise et al., 2005)
- A polite theory can be combined with any other theory, even if the other theory is not stably-infinite.
- Combination method almost the same as Nelson-Oppen.

Many-Sorted Logic: Syntax

- Signature Σ is a triple (S, F, P) where S is a set of sorts, F is a set of function symbols, P is a set of predicate symbols.
- We denote projections as $\Sigma^{\mathbb{S}}$, $\Sigma^{\mathbb{F}}$, $\Sigma^{\mathbb{P}}$, and the signature union as $\Sigma_1 \cup \Sigma_2 = (S_1 \cup S_2, F_1 \cup F_2, P_1 \cup P_2)$.
- The standard notions of Σ-term, Σ-literal, and Σ-formula.
- For a term (formula) ϕ we use $vars_\sigma(\phi)$ to denote all the variables of the sort $\sigma \in S$.

Many-Sorted Logic: Semantics

- Σ-interpretation $\mathcal{A}$ over set of variable X interprets
  - each sort $\sigma \in \Sigma^{\mathbb{S}}$ as a non-empty domain A_σ
  - each variable in $x \in X$ of sort σ to an element $x^{\mathcal{A}} \in A_\sigma$
  - each function symbol $f \in \Sigma^F$ to a function $f^{\mathcal{A}}$ on the appropriate domains
  - each predicate symbol $p \in \Sigma^P$ to a subset $p^{\mathcal{A}}$ of the appropriate domains
- Σ-structure is a Σ-interpretation over an empty set of variables
- A formula ϕ over a set X of variables is satisfiable if it is true in an Σ-interpretation over X

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

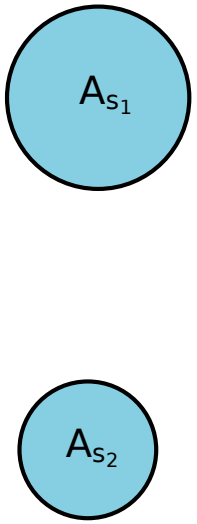
- for every T-satisfiable quantifier-free Σ-formula ϕ
- for every T-interpretation $\mathcal{A}$ satisfying ϕ
- for all cardinals numbers κ_i such that $\kappa_i \geq |A_{s_i}|$
- there exists a T-interpretation $\mathcal{B}$ satisfying ϕ

such that

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

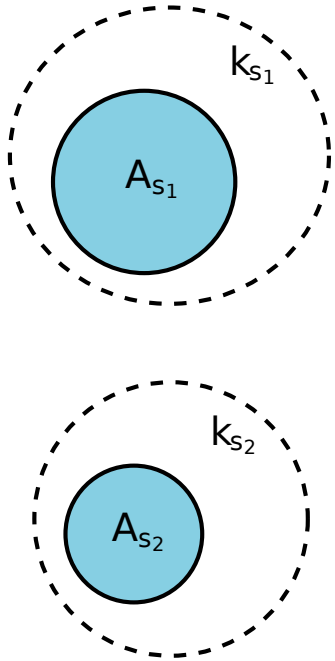
Smoothness

- Let ϕ is satisfiable in $\mathcal{A}$, $S = \{s_1, s_2\}$
- 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 $|B_{s_2}| = \kappa_2$



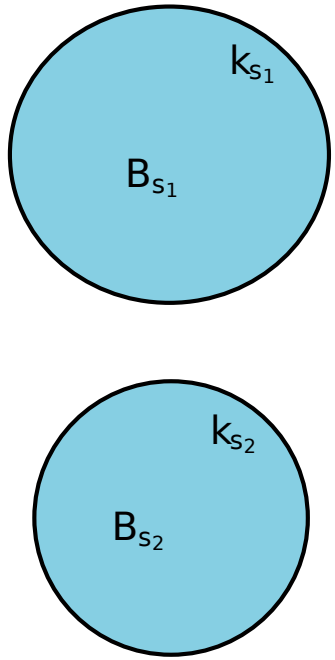
Smoothness

- Let ϕ is satisfiable in $\mathcal{A}$, $S = \{s_1, s_2\}$
- 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 $\mathcal{A}$, $S = \{s_1, s_2\}$
- 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.

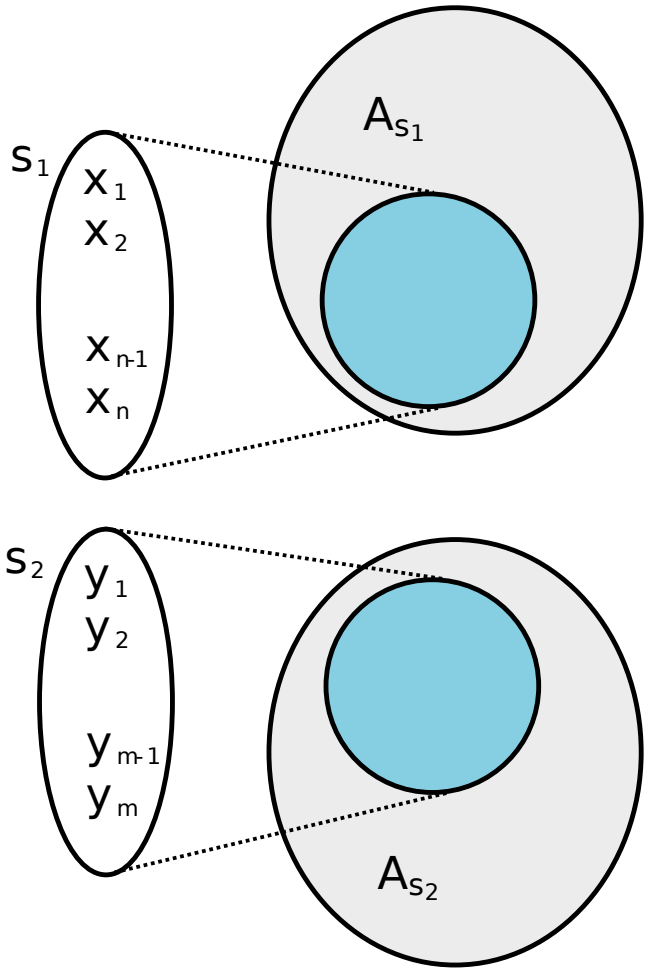
Definition

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 in some T-interpretation $\mathcal{A}$, then there is a T-interpretation $\mathcal{B}$ such that $B_s = [\mathit{vars}_s(\psi \wedge \delta(V))]^{\mathcal{B}}$ for all $s \in S$.

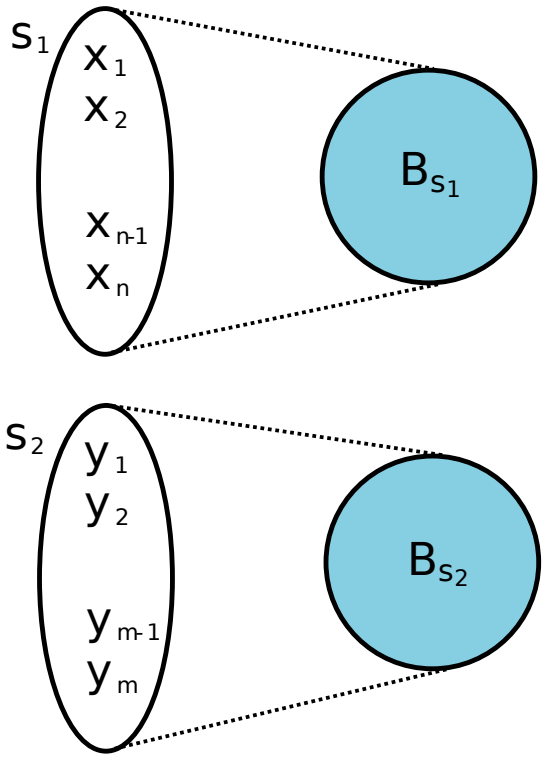
Finite Witnessability

- 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 (Again)

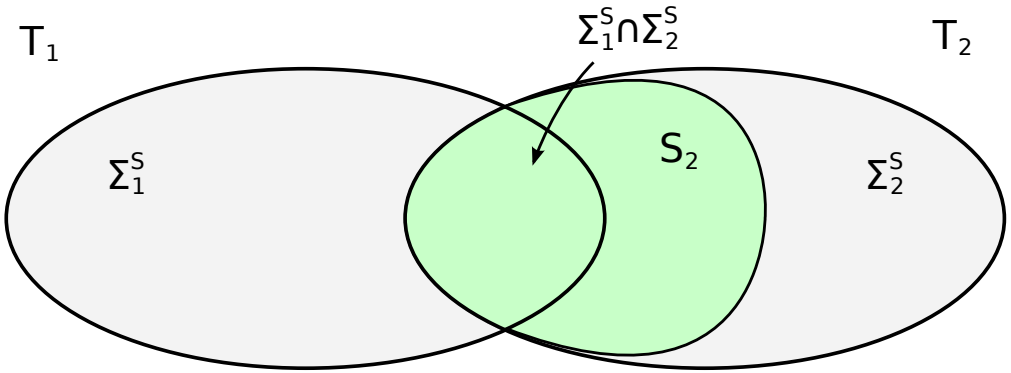
Let Σ be a signature, let $S \subseteq \Sigma^{\mathbb{S}}$ be a set of sorts, and let T be a Σ-theory.

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

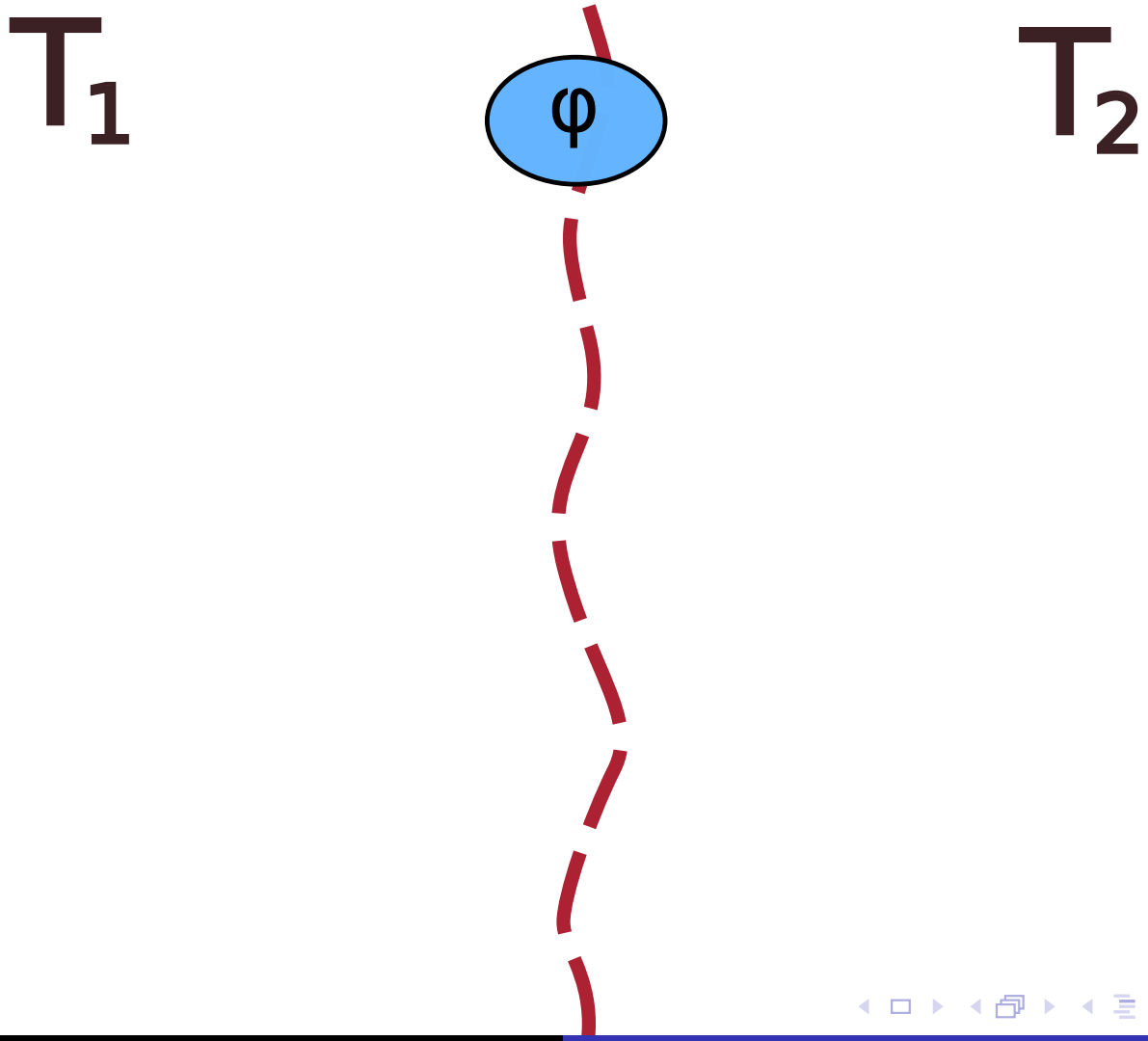


Let T_i be a Σ_i-theory, for $i = 1, 2$, and assume that

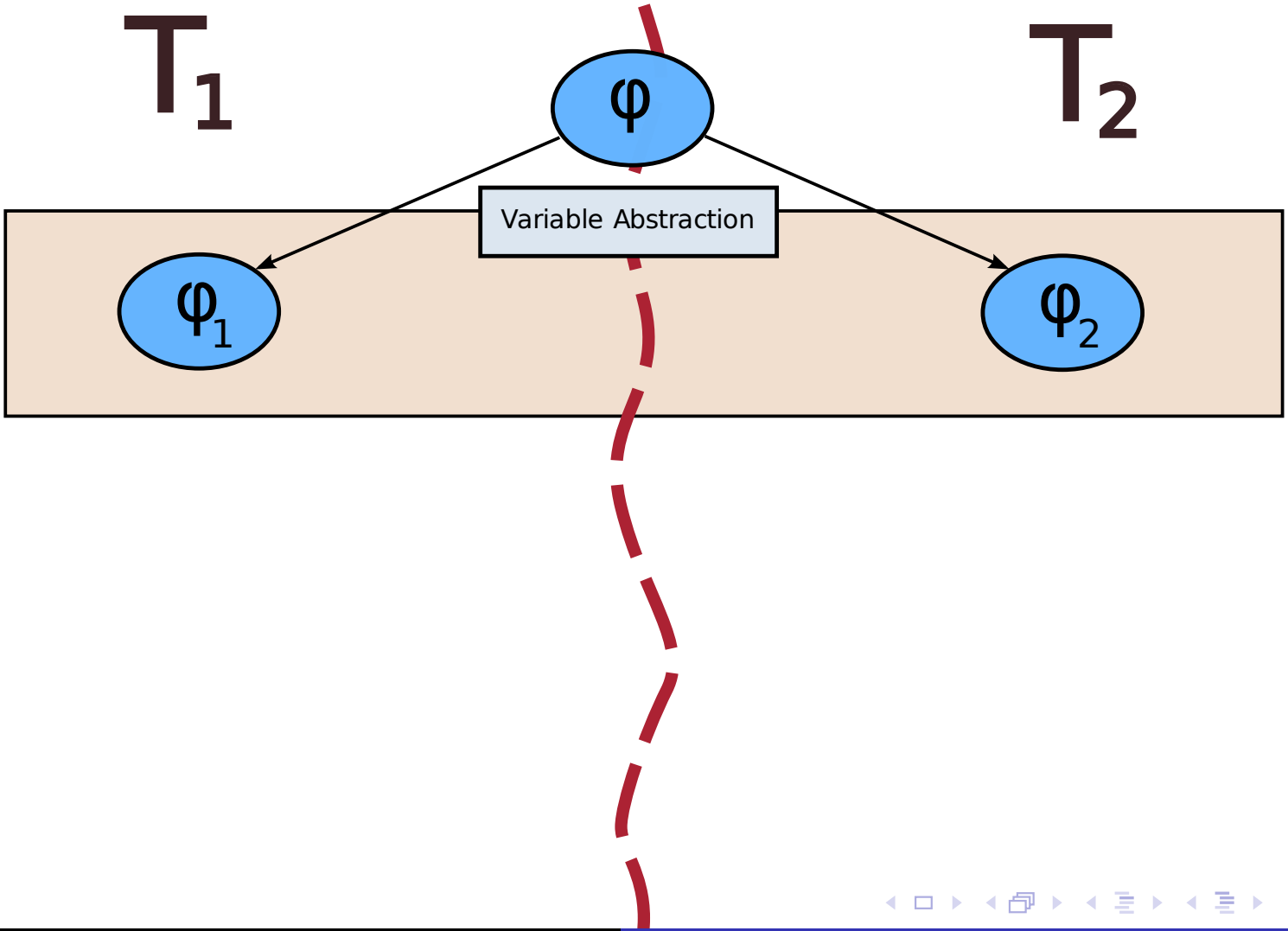
- we know how to decide quantifier-free satisfiability of T_i;
- signatures Σ_i are disjoint (except for sorts);
- T_2 is polite with respect S_2 where $\Sigma_1^{\mathbb{S}} \cap \Sigma_2^{\mathbb{S}} \subseteq S_2$.

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

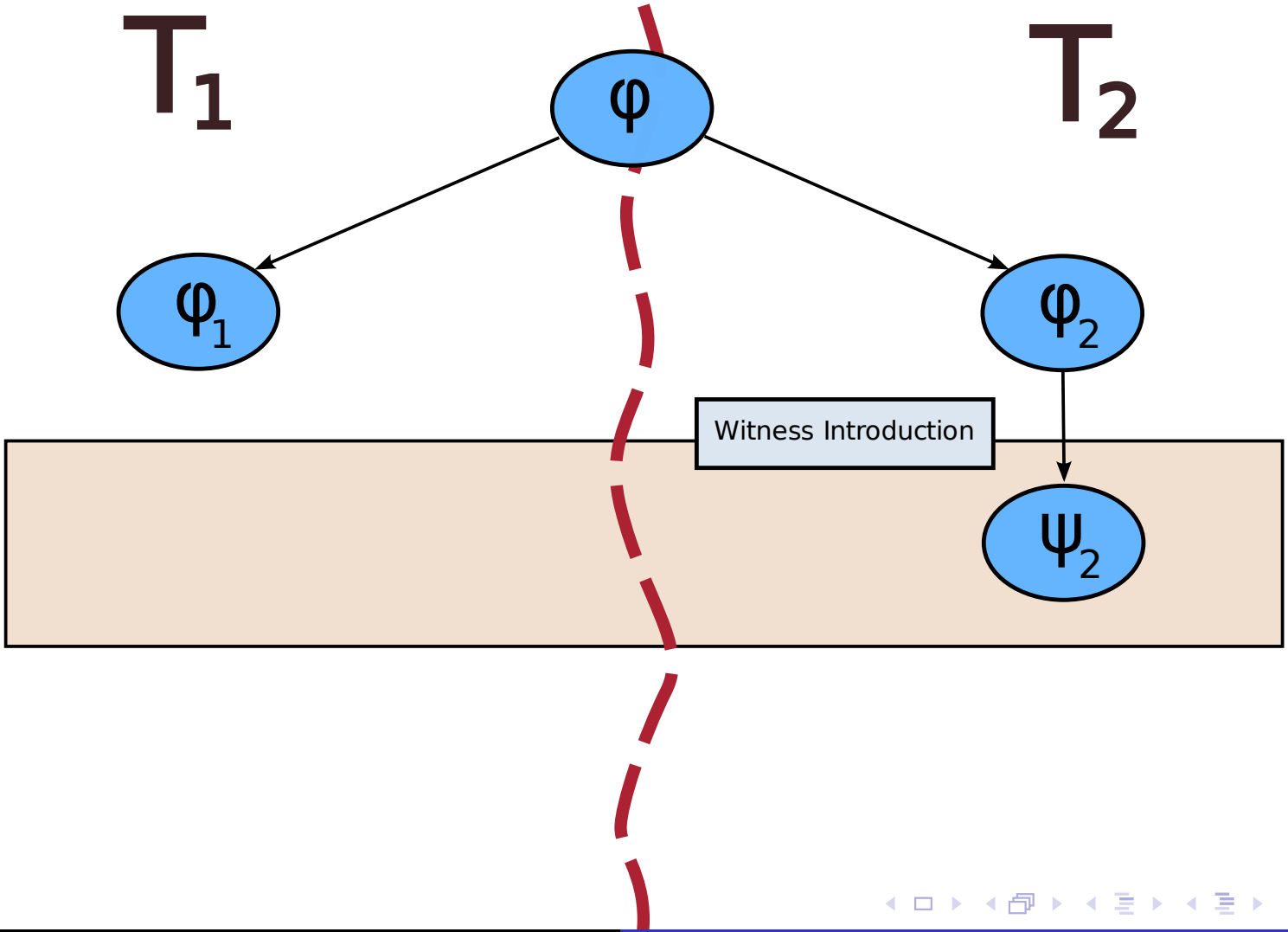
Combination Method



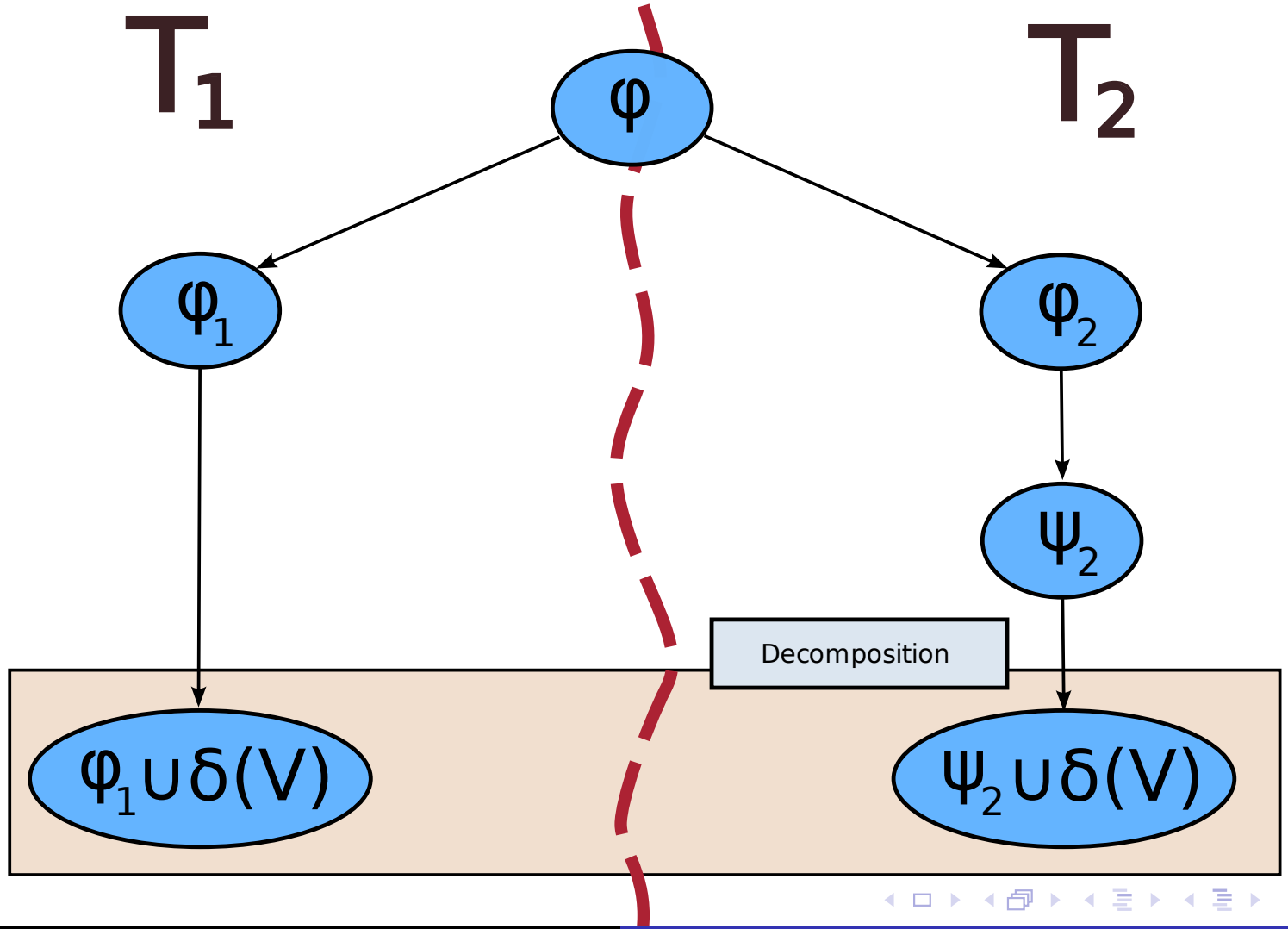
Combination Method



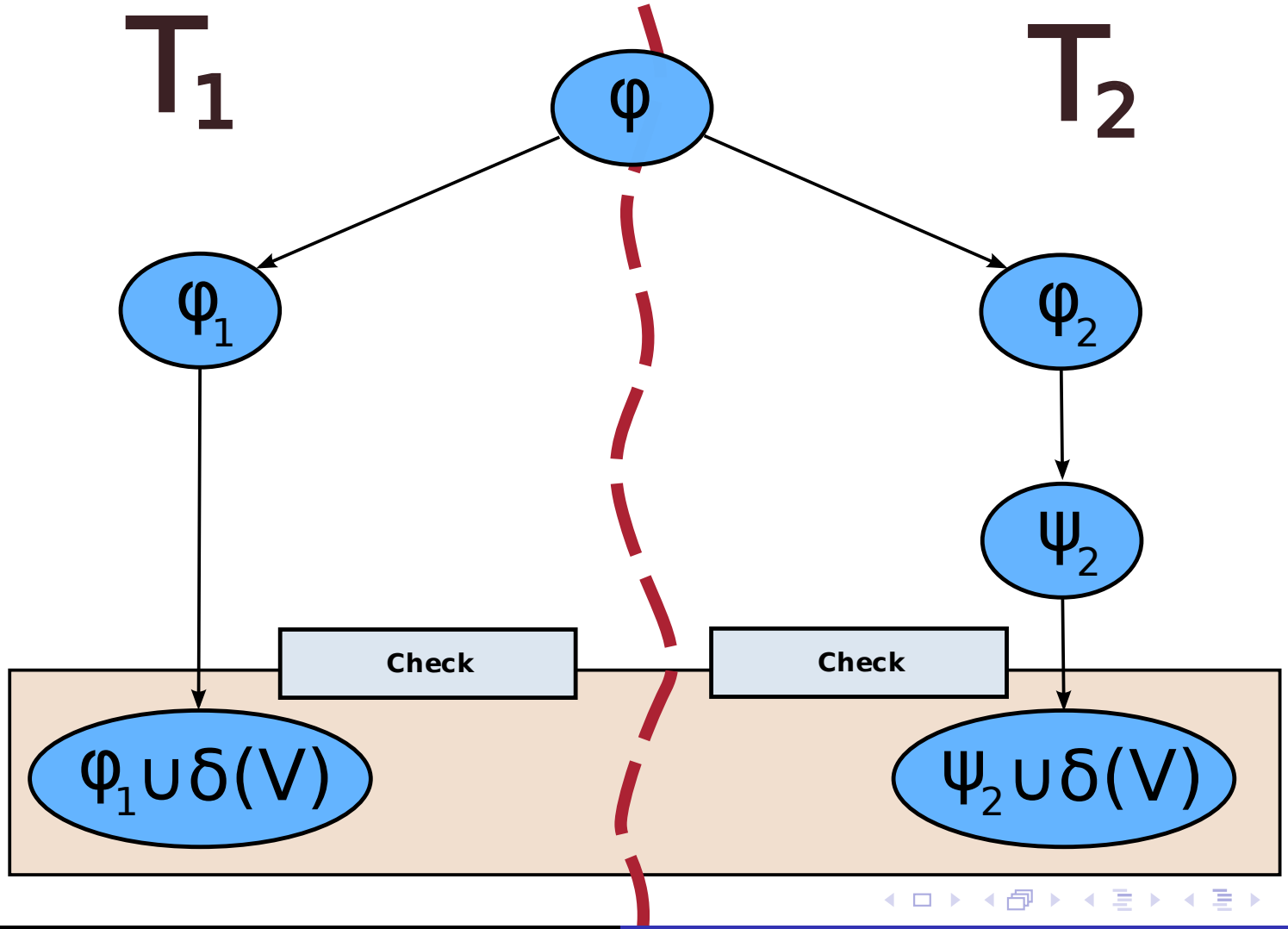
Combination Method



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:

$$a_1 \neq a_2 \longrightarrow (\mathit{read}(a_1, i) \neq \mathit{read}(a_2, i))$$

Outline

Example

Example

Consider this example combining UF and the theory of bit-vectors (here $\times$ is bit-vector multiplication):

$$\bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i) \wedge x_{i+1} = x_i \times x_i)$$

$$\phi_1 : \bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i)) \qquad \phi_2 : \bigwedge_{i=1}^{n-1} (x_{i+1} = x_i \times x_i)$$

$$S = \{x_1, x_2, \ldots, x_n\}$$

$$\phi_1 \wedge \delta(S) \qquad \phi_2 \wedge \delta(S)$$

Example

Example

Consider this example combining UF and the theory of bit-vectors (here $\times$ is bit-vector multiplication):

$$\bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i) \wedge x_{i+1} = x_i \times x_i)$$

$$\phi_1 : \bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i)) \qquad \phi_2 : \bigwedge_{i=1}^{n-1} (x_{i+1} = x_i \times x_i)$$

$$S = \{x_1, x_2, \ldots, x_n\}$$

$$\phi_1 \wedge \delta(S) \qquad \phi_2 \wedge \delta(S)$$

Example

Example

Consider this example combining UF and the theory of bit-vectors (here $\times$ is bit-vector multiplication):

$$\bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i) \wedge x_{i+1} = x_i \times x_i)$$

$$\phi_1 : \bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i)) \qquad \phi_2 : \bigwedge_{i=1}^{n-1} (x_{i+1} = x_i \times x_i)$$

$$S = \{x_1, x_2, \ldots, x_n\}$$

$$\phi_1 \wedge \delta(S) \qquad \phi_2 \wedge \delta(S)$$

Example

Example

Consider this example combining UF and the theory of bit-vectors (here $\times$ is bit-vector multiplication):

$$\bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i) \wedge x_{i+1} = x_i \times x_i)$$

$$\phi_1 : \bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i)) \qquad \phi_2 : \bigwedge_{i=1}^{n-1} (x_{i+1} = x_i \times x_i)$$

$$S = \{x_1, x_2, \ldots, x_n\}$$

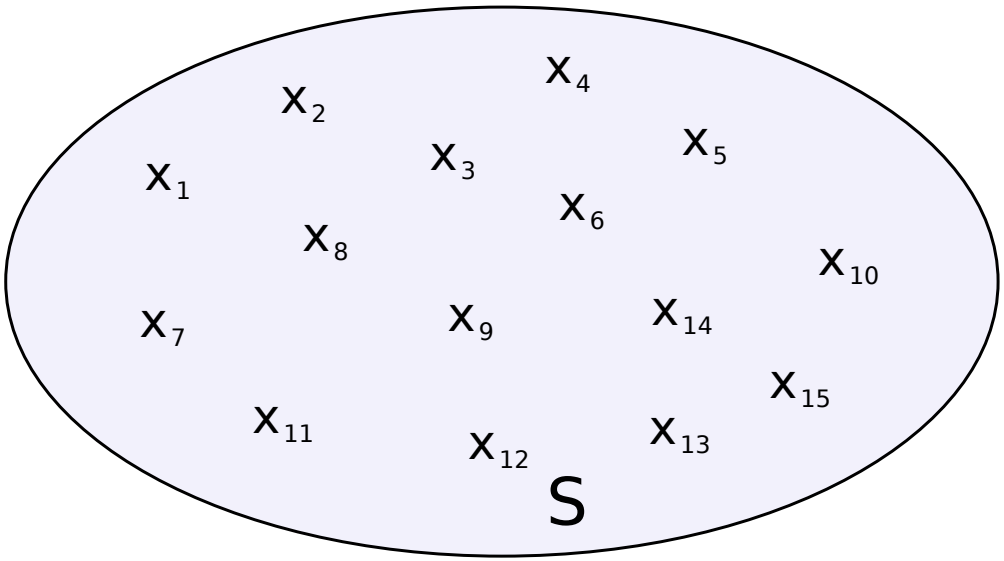
$$\phi_1 \wedge \delta(S) \qquad \phi_2 \wedge \delta(S)$$

Complexity of searching for an arrangement

Complexity

Search for a suitable arrangement over the shared variables introduces a heavy layer of complexity:

$$O(\mathcal{T}_1(n)) \oplus O(\mathcal{T}_2(n)) \implies O(2^{n^2} \times (\mathcal{T}_1(n) + \mathcal{T}_2(n))) \ .$$

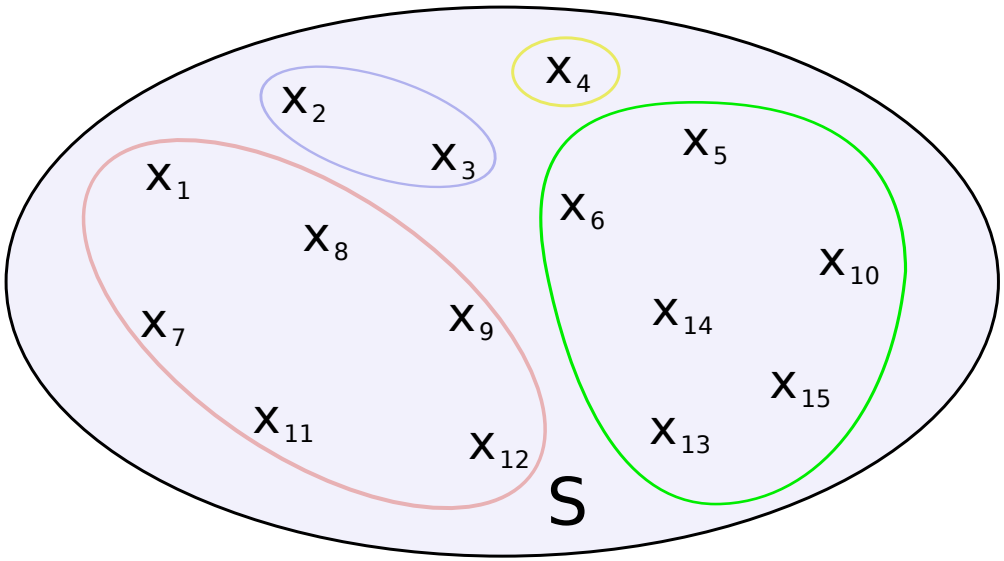


Complexity of searching for an arrangement

Complexity

Search for a suitable arrangement over the shared variables introduces a heavy layer of complexity:

$$O(\mathcal{T}_1(n)) \oplus O(\mathcal{T}_2(n)) \implies O(2^{n^2} \times (\mathcal{T}_1(n) + \mathcal{T}_2(n))) \ .$$



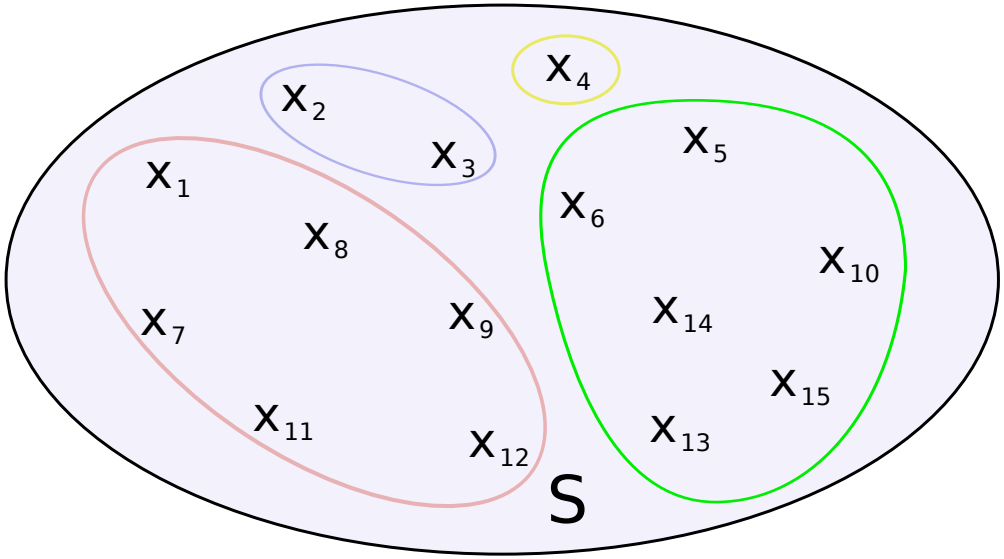
Complexity of searching for an arrangement

Complexity

Search for a suitable arrangement over the shared variables introduces a heavy layer of complexity:

$$O(\mathcal{T}_1(n)) \oplus O(\mathcal{T}_2(n)) \implies O(2^{n^2} \times (\mathcal{T}_1(n) + \mathcal{T}_2(n))) \ .$$

$\phi_1 \cup \delta(S)$



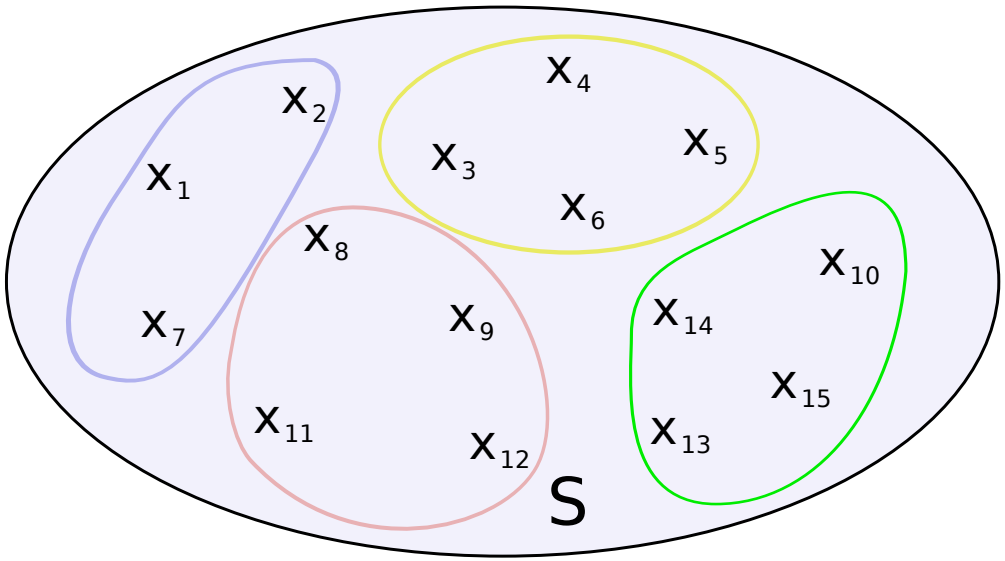
$\phi_2 \cup \delta(S)$

Complexity of searching for an arrangement

Complexity

Search for a suitable arrangement over the shared variables introduces a heavy layer of complexity:

$$O(\mathcal{T}_1(n)) \oplus O(\mathcal{T}_2(n)) \implies O(2^{n^2} \times (\mathcal{T}_1(n) + \mathcal{T}_2(n))) \ .$$



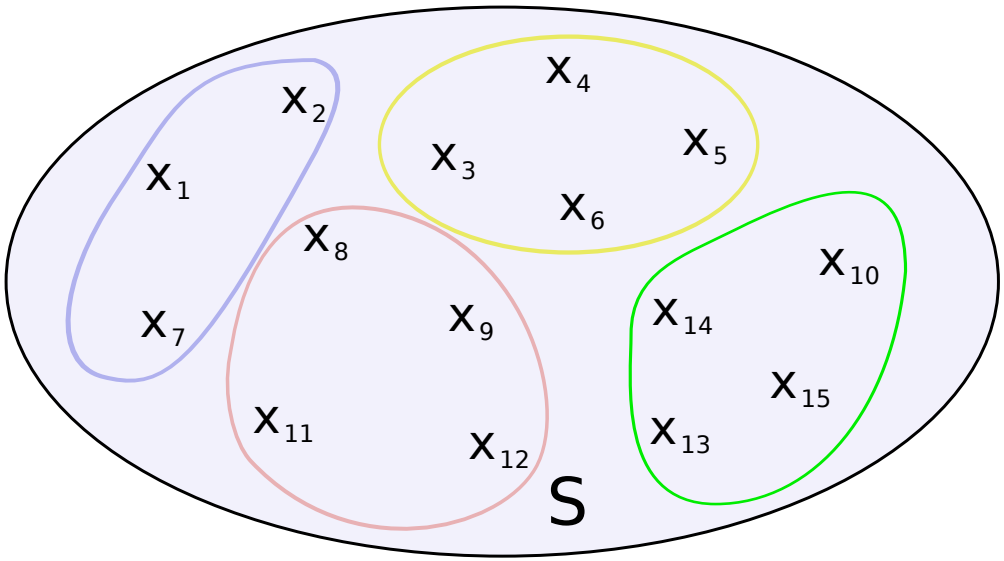
Complexity of searching for an arrangement

Complexity

Search for a suitable arrangement over the shared variables introduces a heavy layer of complexity:

$$O(\mathcal{T}_1(n)) \oplus O(\mathcal{T}_2(n)) \implies O(2^{n^2} \times (\mathcal{T}_1(n) + \mathcal{T}_2(n))) \ .$$

$\phi_1 \cup \delta(S)$



$\phi_2 \cup \delta(S)$

Example

Example

$$\bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i) \wedge x_{i+1} = x_i \times x_i)$$

$$\phi_1 : \bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i)) \qquad \phi_2 : \bigwedge_{i=1}^{n-1} (x_{i+1} = x_i \times x_i)$$

$$S = \{x_1, x_2, \ldots, x_n\}$$

$$\phi_1 \wedge \delta(S) \qquad \phi_2 \wedge \delta(S)$$

Example

Example

But...

We are free to interpret f_i as we wish so there is no need to guess an arrangement.

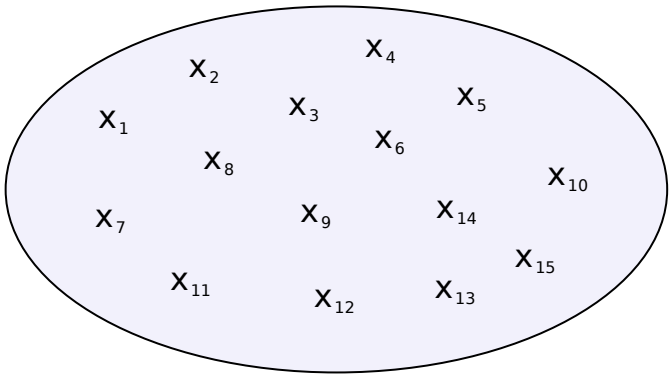
$$\phi_1 : \bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i)) \qquad \phi_2 : \bigwedge_{i=1}^{n-1} (x_{i+1} = x_i \times x_i)$$

$$S = \{x_1, x_2, \ldots, x_n\}$$

$$\phi_1 \wedge \delta(S) \qquad \phi_2 \wedge \delta(S)$$

Arrangements and Care Graphs

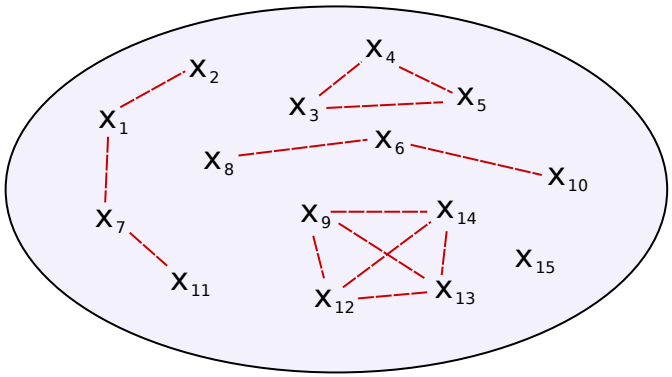
- Instead of guessing an equivalence relation over all the shared variables, we will first identify which pairs of variables a theory cares about (care graph).



- We then only need to consider arrangements δ_G over the graph **G**.
- An arrangement δ_G is the restriction of some equivalence relation to the graph **G**.

Arrangements and Care Graphs

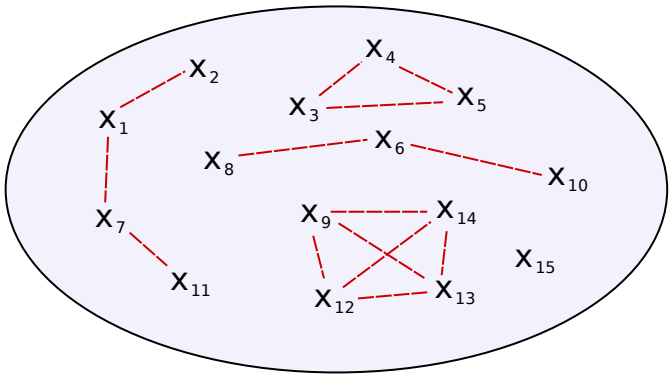
- Instead of guessing an equivalence relation over all the shared variables, we will first identify which pairs of variables a theory cares about (care graph).



- We then only need to consider arrangements δ_G over the graph **G**.
- An arrangement δ_G is the restriction of some equivalence relation to the graph **G**.

Arrangements and Care Graphs

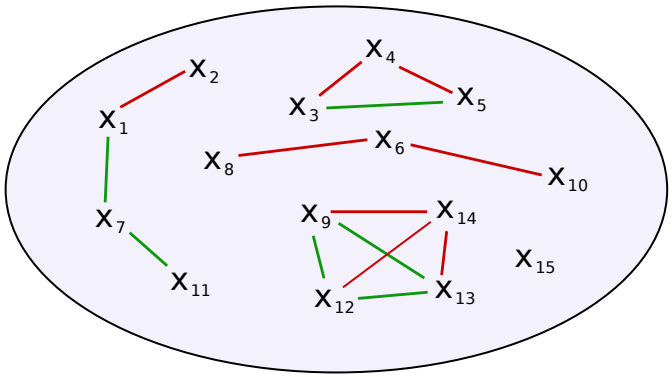
- Instead of guessing an equivalence relation over all the shared variables, we will first identify which pairs of variables a theory cares about (care graph).



- We then only need to consider arrangements $\delta_{\mathbf{G}}$ over the graph **G**.
- An arrangement $\delta_{\mathbf{G}}$ is the restriction of some equivalence relation to the graph **G**.

Arrangements and Care Graphs

- Instead of guessing an equivalence relation over all the shared variables, we will first identify which pairs of variables a theory cares about (care graph).



- We then only need to consider arrangements $\delta_{\mathbf{G}}$ over the graph **G**.
- An arrangement $\delta_{\mathbf{G}}$ is the restriction of some equivalence relation to the graph **G**.

Equality Propagation

Definition (Equality Propagator)

An equality propagator $\mathfrak{P}_T^{=}[\![\cdot]\!]$ for a theory T, for every set V of variables, maps a set of T-literals ϕ into a set of equalities and dis-equalities between variables in V:

$$\mathcal{E} = \mathfrak{P}_T^{=}[\![V]\!](\phi) = \{x_1 = y_1, x_2 = y_2, \ldots, x_m = y_m\} \cup \{z_1 \neq w_1, z_2 \neq w_2, \ldots, z_n \neq w_n\} \ ,$$

where $vars(\mathcal{E}) \subseteq V$ and

1. $\phi \implies \mathcal{E}$ is valid in T, and
2. $\mathfrak{P}_T^{=}[\![V]\!]$ is monotone, i.e. $\mathfrak{P}_T^{=}[\![V]\!](\phi) \subseteq \mathfrak{P}_T^{=}[\![V]\!](\phi \cup \psi)$.

Equality Propagation

Given two theory propagators:

1. $\mathfrak{P}^{=}_{T_1}[\![\cdot]\!]$ for theory T_1
2. $\mathfrak{P}^{=}_{T_1}[\![\cdot]\!]$ for theory T_2

we can construct a theory propagator $\mathfrak{P}^{=}_{T}[\![\cdot]\!]$ for the combined theory $T = T_1 \oplus T_2$

$$\mathfrak{P}^{=}_{T}[\![V]\!](\phi) = (\mathfrak{P}^{=}_{T_1}[\![V]\!] \oplus \mathfrak{P}^{=}_{T_2}[\![V]\!])(\phi) = \psi_1^* \cup \psi_2^* \ ,$$

where $\langle \psi_1^*, \psi_2^* \rangle$ is the least fixpoint of the following operator

$$\mathfrak{P}^{=}_{T}[\![V]\!]\langle \psi_1, \psi_2 \rangle = \left\langle \mathfrak{P}^{=}_{T_1}[\![V]\!](\phi_1 \cup \psi_2), \mathfrak{P}^{=}_{T_2}[\![V]\!](\phi_2 \cup \psi_1) \right\rangle \ .$$

Equality Propagation

Given two theory propagators:

1. $\mathfrak{P}^{=}_{T_1}[\![\cdot]\!]$ for theory T
2. $\mathfrak{P}^{=}_{T_1}[\![\cdot]\!]$ for theory T

we can construct a the nbined theory $T = T_1 \oplus T_2$

$$\mathfrak{P}^{=}_{T}[\![V]\!](\phi) = (\mathfrak{P} \quad ,$$

where $\langle \psi_1^*, \psi_2^* \rangle$ is the le ator

$$\mathfrak{P}^{=}_{T}[\![V]\!]\langle \psi_1, \psi_2 \rangle = \langle \quad _1) \rangle \quad .$$

Propagation

$\psi_1^1 : P_1(\varphi_1)$ $\psi_2^1 : P_2(\varphi_2)$

Equality Propagation

Given two theory propagators:

1. $\mathfrak{P}^{=}_{T_1}[\![\cdot]\!]$ for theory T
2. $\mathfrak{P}^{=}_{T_1}[\![\cdot]\!]$ for theory T

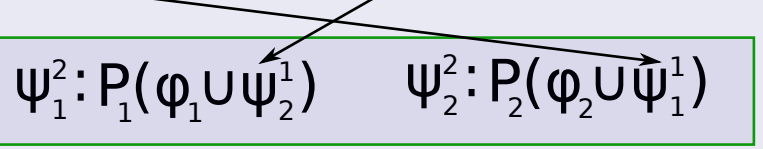
we can construct a the nbined theory $T = T_1 \oplus T_2$

$$\mathfrak{P}^{=}_{T}[\![V]\!](\phi) = (\mathfrak{P} \quad ,$$

where $\langle \psi_1^*, \psi_2^* \rangle$ is the le ator

$$\mathfrak{P}^{=}_{T}[\![V]\!]\langle \psi_1, \psi_2 \rangle = \langle \quad _1) \rangle \quad .$$

Propagation



Equality Propagation

Given two theory propagators:

1. $\mathfrak{P}^{=}_{T_1}[\![\cdot]\!]$ for theory T
2. $\mathfrak{P}^{=}_{T_1}[\![\cdot]\!]$ for theory T

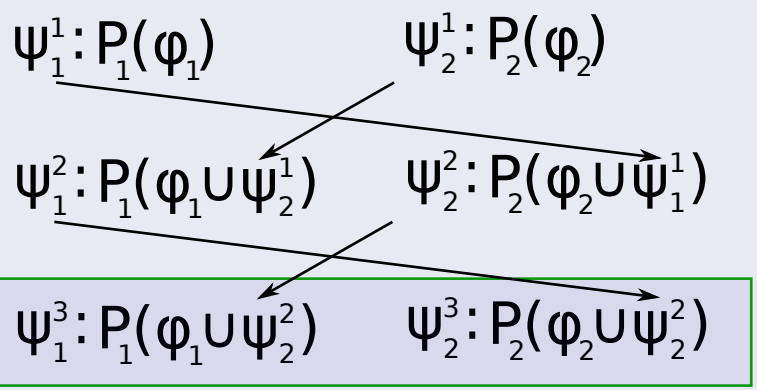
we can construct a the nbined theory $T = T_1 \oplus T_2$

$$\mathfrak{P}^{=}_{T}[\![V]\!](\phi) = (\mathfrak{P} \quad ,$$

where $\langle \psi_1^*, \psi_2^* \rangle$ is the le ator

$$\mathfrak{P}^{=}_{T}[\![V]\!]\langle \psi_1, \psi_2 \rangle = \langle \quad \rangle \quad .$$

Propagation



Equality Propagation

Given two theory propagators:

1. $\mathfrak{P}^{=}_{T_1}[\![\cdot]\!]$ for theory T_1
2. $\mathfrak{P}^{=}_{T_2}[\![\cdot]\!]$ for theory T_2

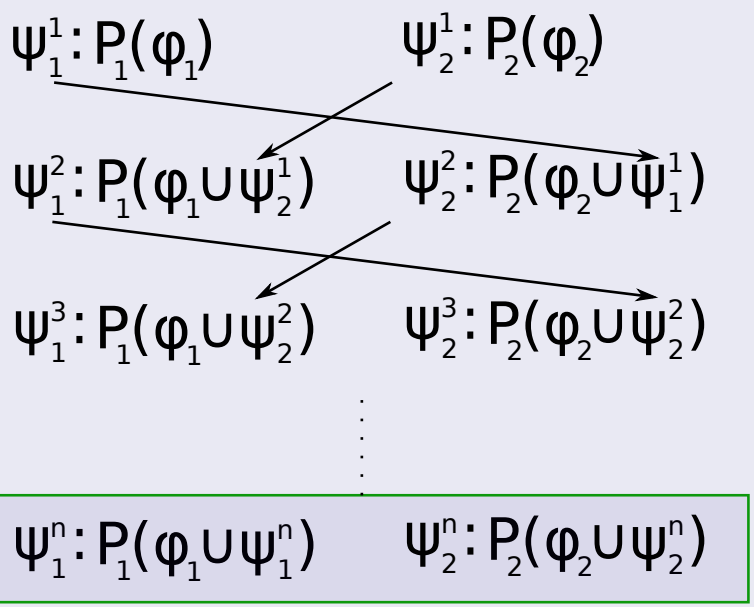
we can construct a the … nbined theory $T = T_1 \oplus T_2$

$$\mathfrak{P}^{=}_{T}[\![V]\!](\phi) = (\mathfrak{P} \ldots ,$$

where $\langle \psi_1^*, \psi_2^* \rangle$ is the le … ator

$$\mathfrak{P}^{=}_{T}[\![V]\!]\langle \psi_1, \psi_2 \rangle = \langle \ldots \rangle .$$

Propagation



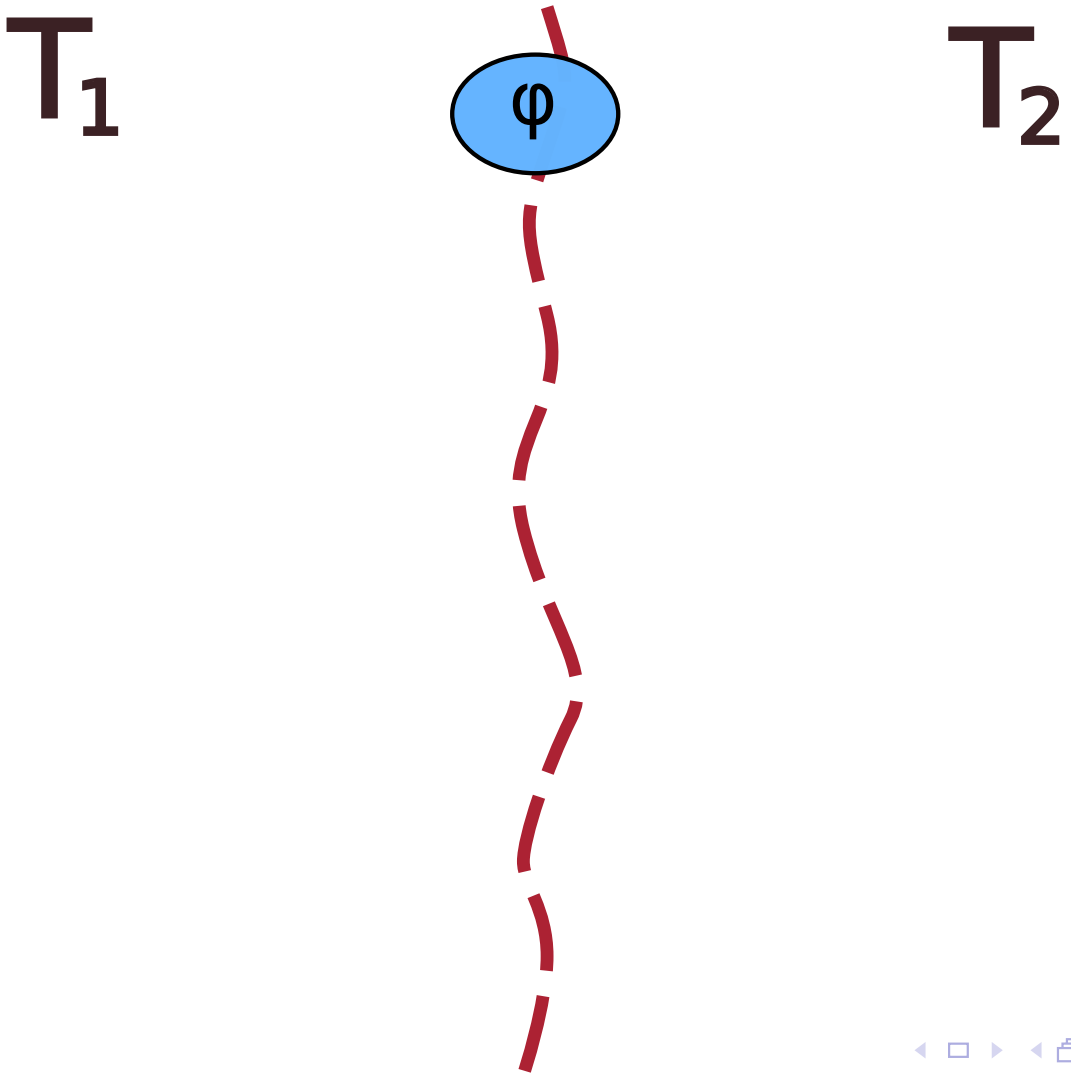
Care Function

Definition (Care Function)

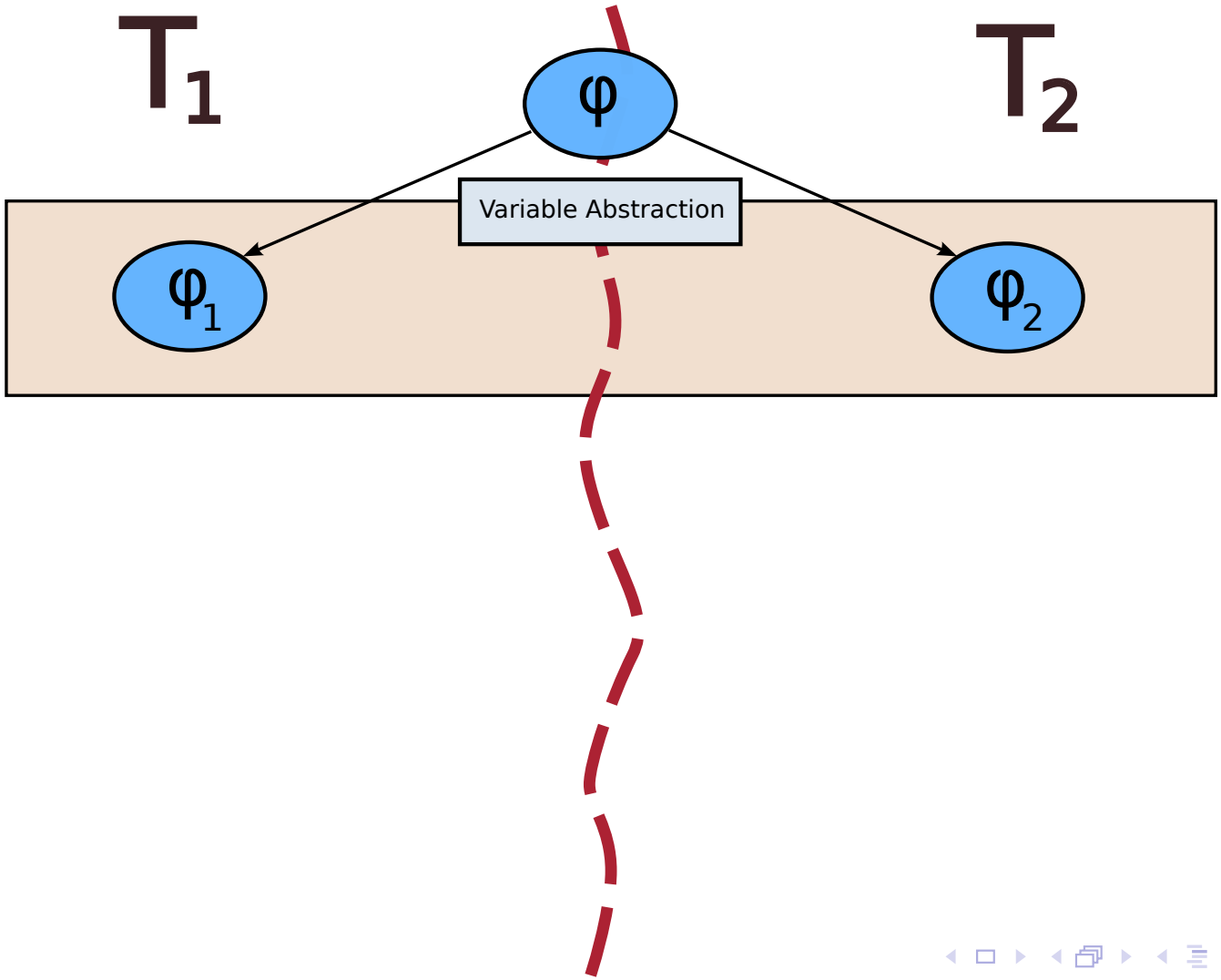
For a theory T we call a function $\mathfrak{C}[\![\cdot]\!]$ a care function for T with respect to a T-equality propagator $\mathfrak{P}^{=}_{T}[\![\cdot]\!]$ when for every set V of variables and every set ϕ of T-literals

1. $\mathfrak{C}[\![V]\!]$ maps ϕ to a care graph $\mathbf{G} = \langle V, E \rangle$.
2. if $x = y$ or $x \neq y$ are in $\mathfrak{P}^{=}_{T}[\![V]\!](\phi)$ then $(x, y) \notin E$;
3. if $\mathbf{G} = \langle V, \emptyset \rangle$ and ϕ is T-satisfiable then, for any arrangement δ_V such that $\mathfrak{P}^{=}_{T}[\![V]\!](\phi) \subseteq \delta_V$, it holds that $\phi \cup \delta_V$ is also T-satisfiable.

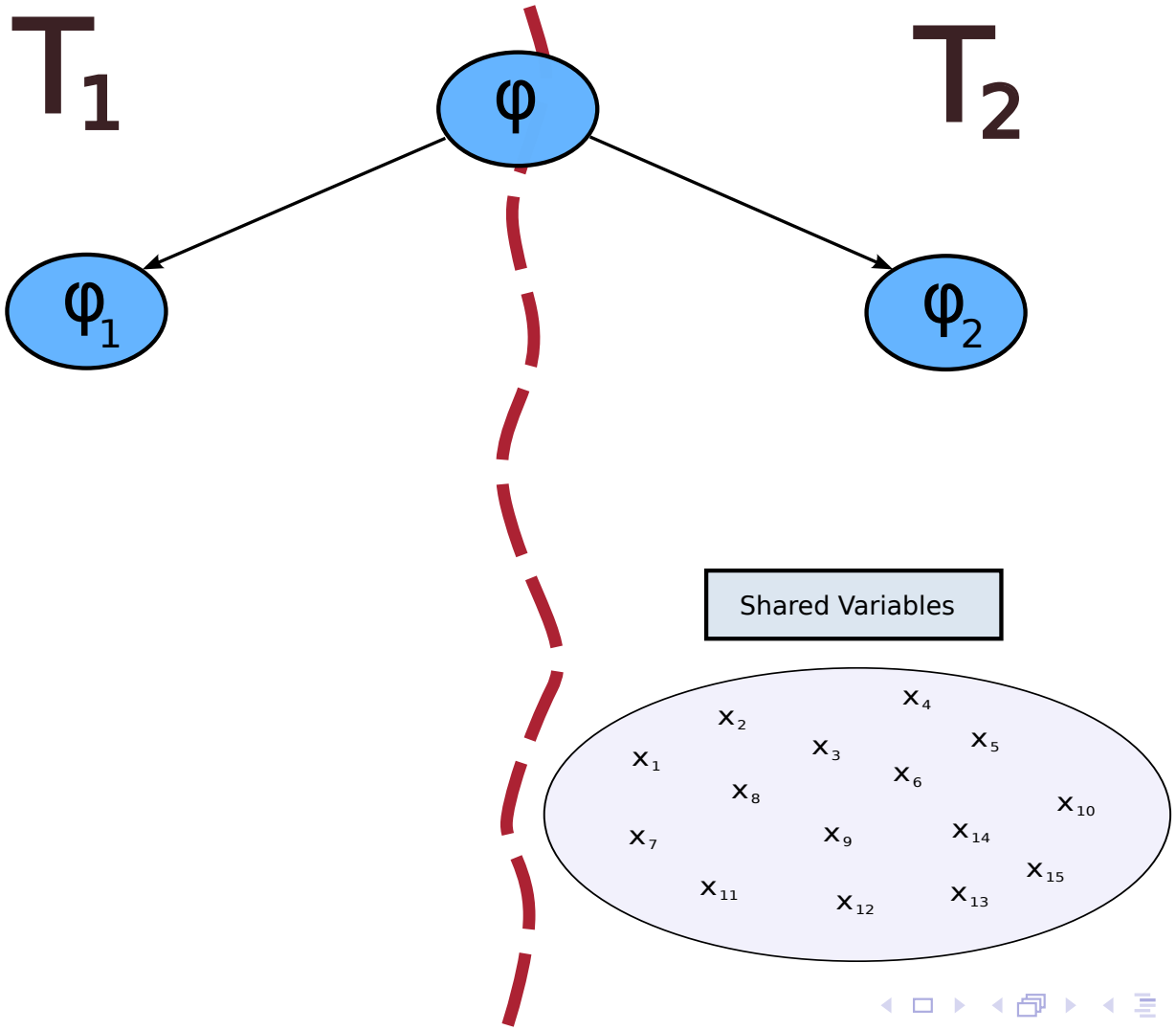
Combination Method



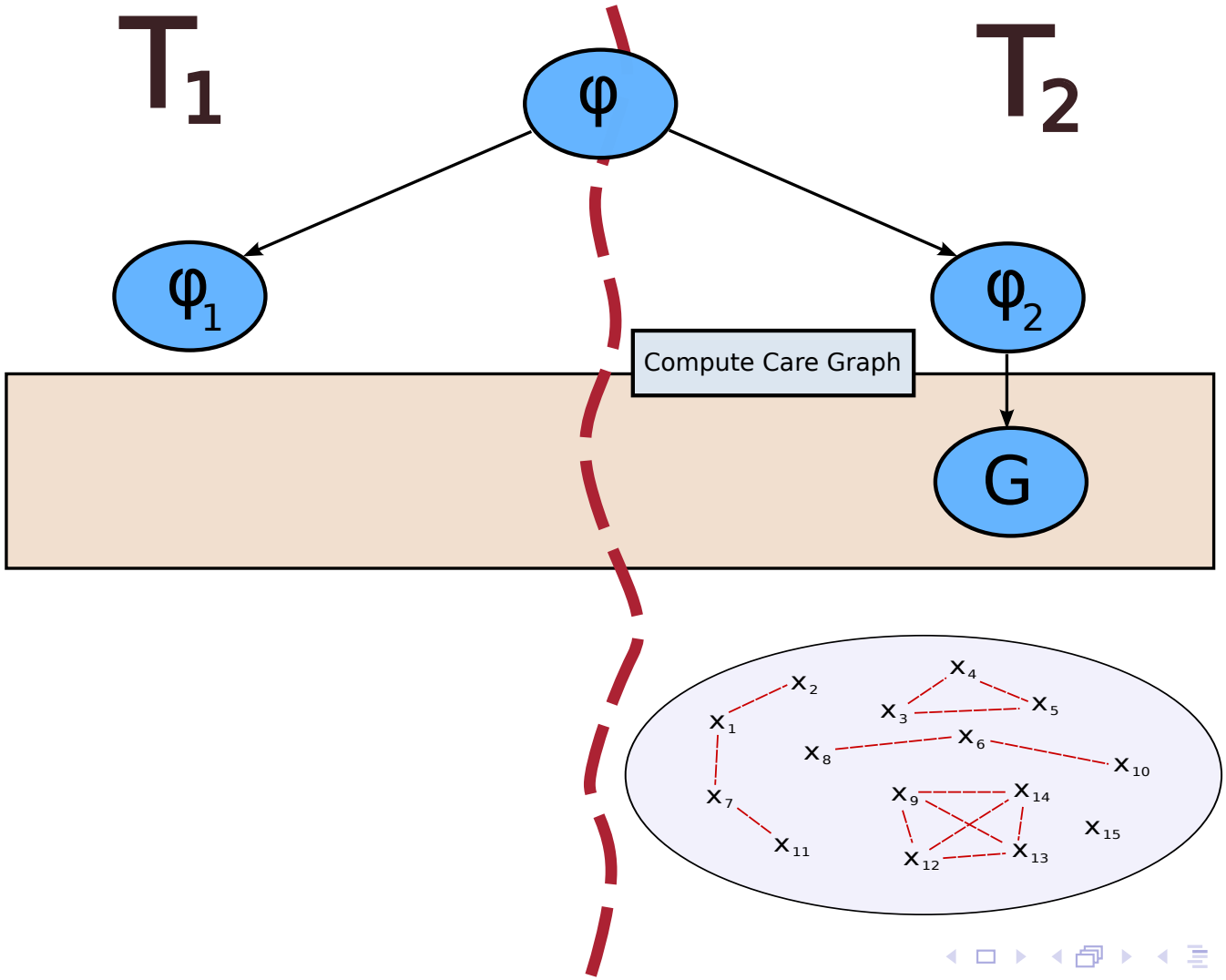
Combination Method



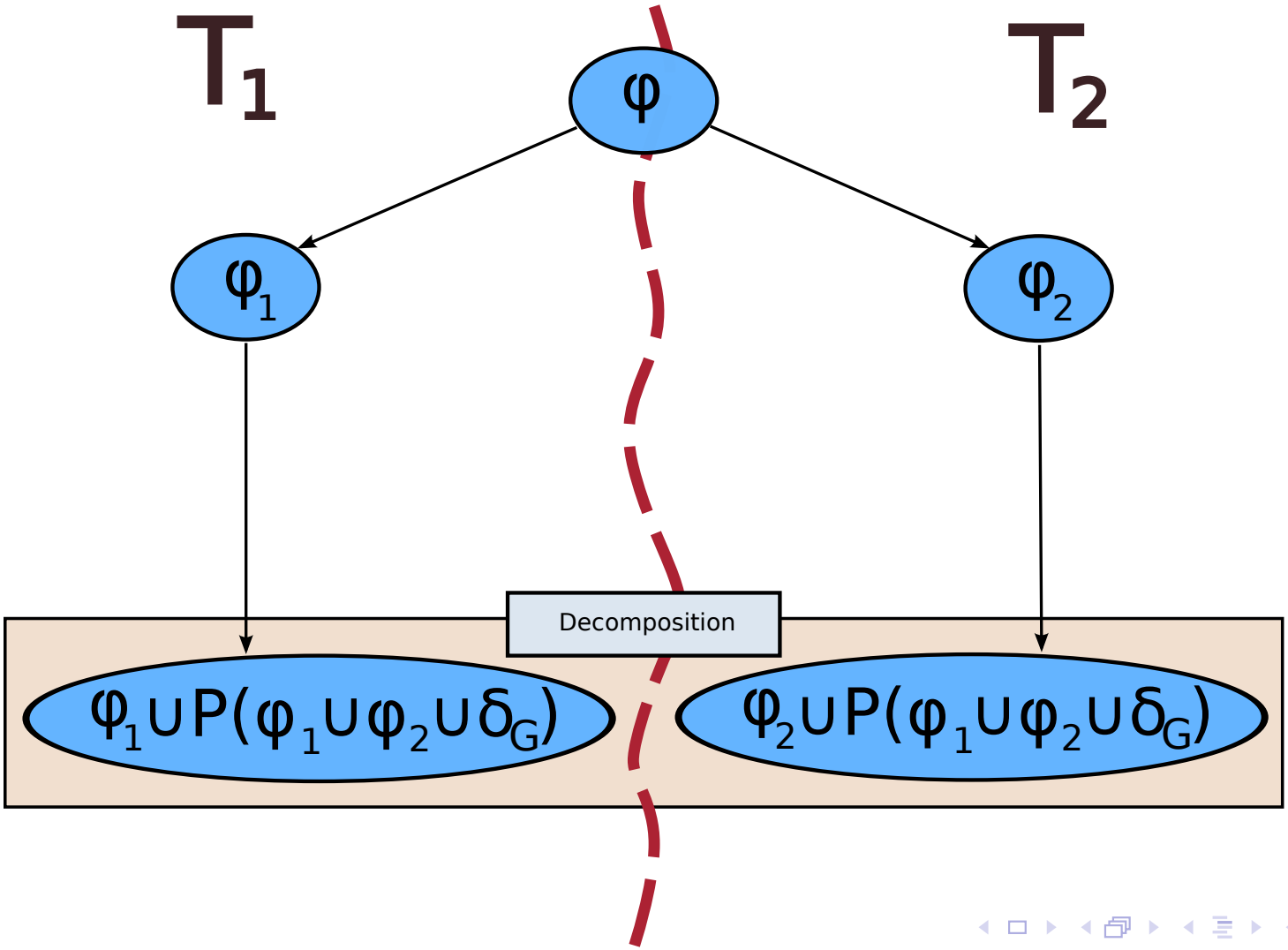
Combination Method



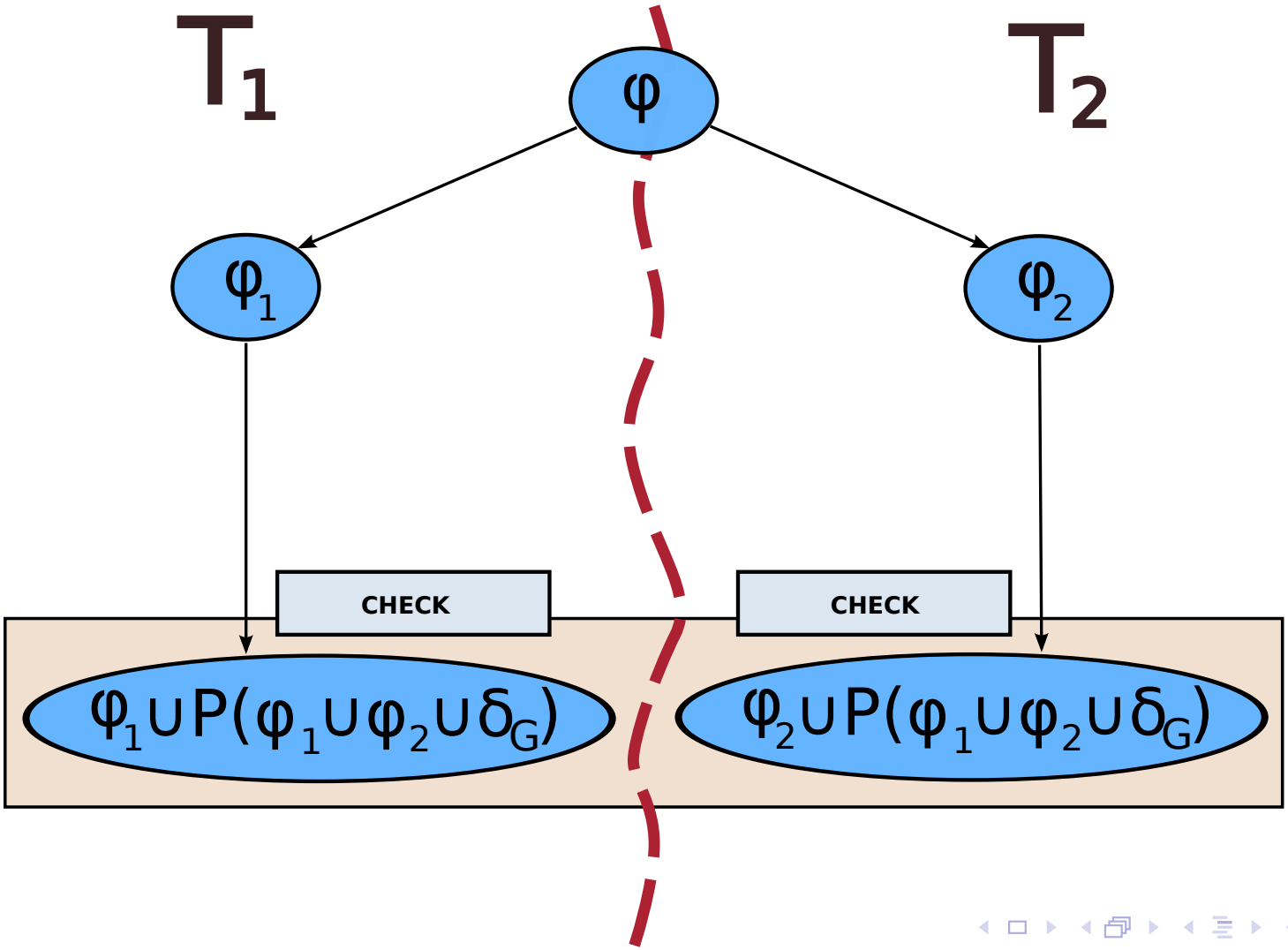
Combination Method



Combination Method



Combination Method



Theorem

Let T_1 and T_2 be two signature-disjoint stably-infinite theories equipped with equality propagators $\mathfrak{P}^{=}_{T_i}[\![\cdot]\!]$. Additionally, let T_2 be equipped with a care function $\mathfrak{C}_{T_2}[\![\cdot]\!]$ operating with respect to $\mathfrak{P}^{=}_{T_2}[\![\cdot]\!]$. Let ϕ be a set of literals with $V = vars(\phi_1) \cap vars(\phi_2)$. Then following are equivalent

1. *ϕ is T-satisfiable;*
2. *there exists a care graph $\mathbf{G}_2$ and an arrangement $\delta_{\mathbf{G}_2}$ over $\mathbf{G}_2$ such that $\mathbf{G}_2$ is a fix-point solution of*

$$\mathbf{G} = \mathbf{G} \cup \mathfrak{C}_{T_2}[\![V]\!](\phi_2 \cup \mathfrak{P}^{=}_{T}[\![V]\!](\phi_1 \cup \phi_2 \cup \delta_{\mathbf{G}})) \ ,$$

and such that the following sets are T_1- and T_2-satisfiable respectively:

$$\phi_1 \cup \mathfrak{P}^{=}_{T}[\![V]\!](\phi_1 \cup \phi_2 \cup \delta_{\mathbf{G}_2}) \ , \quad \phi_2 \cup \mathfrak{P}^{=}_{T}[\![V]\!](\phi_1 \cup \phi_2 \cup \delta_{\mathbf{G}_2}) \ .$$

Combination Method

- Equality propagation is explicit in the method
- The new method is asymmetric – only one theory computes the care graph
- Using trivial care functions and propagators the method reduces to standard Nelson-Oppen
- Easily combines with polite theory extension of Nelson-Oppen
- Care functions and propagators need to be devised for the theories

Theory of Uninterpreted Functions

- Conjunctions of literals the theory can be decided in polynomial time by congruence closure algorithms
- We make use of insights from these algorithms in defining both the equality propagator and the care function
- For simplicity, we assume that the formulas contain no predicate symbols, i.e. literals are

$$x = y, \quad x \neq y, \quad x = f(y_1, \ldots y_n) \ .$$

Equality Propagator

- Let ϕ be a set of literals, V a set of variables, and let $\sim_c$ be the smallest congruence relation over terms in ϕ containing $\{ (x,t) \mid x = t \in \phi \}$.
- We define a dis-equality relation $\neq_c$ as the smallest relation satisfying

$$x \neq y \in \phi \Longrightarrow x \neq_c y \ ,$$
$$x \sim_c x' \wedge y \sim_c y' \wedge x' \neq y' \Longrightarrow x \neq_c y \ .$$

- We define the equality propagator as

$$\mathfrak{P}^{=}_{\mathtt{euf}}[\![V]\!](\phi) = \{ x = y \mid x, y \in V \wedge x \sim_c y \} \cup \{ x \neq y \mid x, y \in V \wedge x \neq_c y \} \ .$$

Equality Propagator

- Let ϕ be a set of literals, V a set of variables, and let $\sim_c$ be the smallest congruence relation over terms in ϕ containing
- \
r
- \

Example

Given the set of literals

$$\phi = \{ x = z,\ y = f(a),\ z \neq f(a) \} \ ,$$

the equality propagator $\mathfrak{P}^{=}_{\mathtt{euf}}[\![\cdot]\!]$ would return

$$\mathfrak{P}^{=}_{\mathtt{euf}}[\![x, y]\!](\phi) = \{ x = x,\ y = y,\ x \neq y,\ y \neq x \} \ .$$

$$\begin{aligned}\mathfrak{P}^{=}_{\mathtt{euf}}[\![V]\!](\phi) = &\{ x = y \mid x, y \in V \wedge x \sim_c y \} \cup \\ &\{ x \neq y \mid x, y \in V \wedge x \neq_c y \} \ .\end{aligned}$$

Care Function

- Let V be a set of variables and let ϕ be a set of literals
- Assume that ϕ only contains function symbols from

$$F = \{f_1, f_2, \ldots, f_n\} \ .$$

- Using the relation $\sim_c$ from before, for each $f \in F$ let E_f be a set of pairs from V such that $(x, y) \in E_f$ iff:
  1. $x \in V$ and $y \in V$,
  2. $\neg(x \sim_c y)$ and $\neg(x \neq_c y)$
  3. there exist terms $t_1 = f(x_1, \ldots, x_i, \ldots, x_k)$ and $t_2 = f(y_1, \ldots, y_i, \ldots, y_k)$ in ϕ such that:
     1. for some $1 \leq i \leq k$, $x \sim_c x_i$ and $y \sim_c y_i$;
     2. $\neg(t_1 \sim_c t_2)$; and for $1 \leq j \leq k$, $\neg(x_j \neq_c y_j)$.

  Let the care-graph edges be $E = \bigcup_{f \in F} E_f$ and define the care function as:

$$\mathfrak{C}_{\mathtt{euf}}[\![V]\!](\phi) = \mathbf{G} = \langle V, E \rangle \ .$$

Care Function

- Let V be a set of variables and let ϕ be a set of literals
- Assume that ϕ only contains function symbols from

- Us
a s
  1.
  2.
  3.

Example

Given the set of literals

$$\phi = \{ x_f = f(x),\ y_f = f(y) \}$$

with $V = \{x, x_f, y, y_f\}$, the care function would return

$$\mathfrak{C}_{\mathtt{euf}}[\![V]\!](\phi) = \mathbf{G} = \langle V, \{(x, y)\} \rangle \ .$$

Let the care-graph edges be $E = \bigcup_{f \in F} E_f$ and define the care function as:

$$\mathfrak{C}_{\mathtt{euf}}[\![V]\!](\phi) = \mathbf{G} = \langle V, E \rangle \ .$$

Example

Example

$$\phi_1 : \bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i)) \qquad \phi_2 : \bigwedge_{i=1}^{n-1} (x_{i+1} = x_i \times x_i)$$

$$V = \{x_1, x_2, \ldots, x_n\}$$
$$\mathfrak{C}_{\mathtt{euf}}[\![V]\!](\phi_1) = \mathbf{G} = \langle V, \emptyset \rangle \ .$$

Example

Example

$$\phi_1 : \bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i)) \qquad \phi_2 : \bigwedge_{i=1}^{n-1} (x_{i+1} = x_i \times x_i)$$

$$V = \{x_1, x_2, \ldots, x_n\}$$
$$\mathfrak{C}_{\mathtt{euf}}[\![V]\!](\phi_1) = \mathbf{G} = \langle V, \emptyset \rangle \ .$$

Example

Example

$$\phi_1 : \bigwedge_{i=1}^{n-1} (x_{i+1} = f_i(x_i)) \qquad \phi_2 : \bigwedge_{i=1}^{n-1} (x_{i+1} = x_i \times x_i)$$

$$V = \{x_1, x_2, \ldots, x_n\}$$
$$\mathfrak{C}_{\mathtt{euf}}[\![V]\!](\phi_1) = \mathbf{G} = \langle V, \emptyset \rangle \ .$$

Thus, no sharing is needed for this example. It is sufficient to check ϕ_1 and ϕ_2 separately.

- There is also a care function for the theory of arrays.
- Similar to uninterpreted functions – arrays can be seen as functions with a twist

Conclusion

- New insights extend classic Nelson-Oppen
- Not radical departures: correctness relies on same basic ideas as Nelson-Oppen
- However, one key difference: *asymmetry* is key to both of these extensions
- Perhaps this says something about the kinds of theories we are using: some are self-contained and some are parameterized
- Parametric theories manage the combination