Motivation

- Last few lectures: Full first-order logic
Motivation

- **Last few lectures:** Full first-order logic

- First-order logic is very powerful and very general.
Motivation

- Last few lectures: Full first-order logic
- First-order logic is very powerful and very general.
- But in many settings, we have a particular application in mind and do not need the full power of first order logic.
Motivation

- **Last few lectures:** Full first-order logic

- First-order logic is very powerful and very general.

- But in many settings, we have a particular application in mind and do not need the full power of first order logic.

- For instance, instead of general predicates/functions, we might only need an equality predicate or arithmetic operations.
Motivation

- **Last few lectures:** Full first-order logic

- First-order logic is very powerful and very general.

- But in many settings, we have a particular application in mind and do not need the full power of first order logic.

- For instance, instead of general predicates/functions, we might only need an equality predicate or arithmetic operations.

- Also, might want to disallow some interpretations that are allowed in first-order logic.
First-Order Theories

- **First-order theories**: Useful for formalizing and reasoning about particular application domains
  - e.g., involving integers, real numbers, lists, arrays, ...
First-Order Theories

- **First-order theories**: Useful for formalizing and reasoning about particular application domains
  - e.g., involving integers, real numbers, lists, arrays, ...

- **Advantage**: By focusing on particular application domain, can give much more efficient, specialized decision procedures
First-Order Theories

- **First-order theories**: Useful for formalizing and reasoning about particular application domains
  - e.g., involving integers, real numbers, lists, arrays, ...

- **Advantage**: By focusing on particular application domain, can give much more efficient, specialized decision procedures

- **Today**: Talk about what first-order theories are and look at some examples.
First-Order Theories

- **First-order theories**: Useful for formalizing and reasoning about particular application domains
  - e.g., involving integers, real numbers, lists, arrays, ...

- **Advantage**: By focusing on particular application domain, can give much more efficient, specialized decision procedures

- **Today**: Talk about what first-order theories are and look at some examples.

- **Future lectures**: Explore individual first-order theories in more detail and learn about specialized decision procedures
Signature and Axioms of First-Order Theory

- A first-order theory $T$ consists of:

  1. Signature $\Sigma_T$: set of constant, function, and predicate symbols
  2. Axioms $A_T$: A set of FOL sentences over $\Sigma_T$

Sigma $\Sigma$ formula: Formula constructed from symbols of $\Sigma_T$ and variables, logical connectives, and quantifiers.

Example: We could have a theory of heights $T_H$ with signature $\Sigma_H$: \{taller\} and axiom:

$$\forall x, y. \text{taller}(x, y) \rightarrow \neg \text{taller}(y, x)$$

Is $\exists x. \forall z. \text{taller}(x, z) \land \text{taller}(y, w)$ legal $\Sigma_H$ formula? Yes

What about $\exists x. \forall z. \text{taller}(x, z) \land \text{taller}(\text{joe}, \text{tom})$? No
Signature and Axioms of First-Order Theory

- A first-order theory \( T \) consists of:
  1. **Signature** \( \Sigma_T \): set of constant, function, and predicate symbols

Example: We could have a theory of heights \( T_H \) with signature \( \Sigma_H \): \{taller\} and axiom:

\[
\forall x, y. \text{taller}(x, y) \rightarrow \neg \text{taller}(y, x)
\]

Is \( \exists x. \forall z. \text{taller}(x, z) \land \text{taller}(y, w) \) legal \( \Sigma_H \) formula?

Yes

What about \( \exists x. \forall z. \text{taller}(x, z) \land \text{taller}(joe, tom) \)?

No
Signature and Axioms of First-Order Theory

- A first-order theory $T$ consists of:
  1. **Signature $\Sigma_T$**: set of constant, function, and predicate symbols
  2. **Axioms $A_T$**: A set of FOL sentences over $\Sigma_T$
A first-order theory $T$ consists of:

1. **Signature $\Sigma_T$:** set of constant, function, and predicate symbols

2. **Axioms $A_T$:** A set of FOL sentences over $\Sigma_T$

**$\Sigma_T$ formula:** Formula constructed from symbols of $\Sigma_T$ and variables, logical connectives, and quantifiers.
Signature and Axioms of First-Order Theory

- A first-order theory $T$ consists of:
  1. **Signature** $\Sigma_T$: set of constant, function, and predicate symbols
  2. **Axioms** $A_T$: A set of FOL sentences over $\Sigma_T$

- $\Sigma_T$ formula: Formula constructed from symbols of $\Sigma_T$ and variables, logical connectives, and quantifiers.

- **Example:** We could have a theory of heights $T_H$ with signature $\Sigma_H : \{\text{taller}\}$ and axiom:

$$\forall x, y. \text{taller}(x, y) \rightarrow \neg \text{taller}(y, x)$$
Signature and Axioms of First-Order Theory

- A first-order theory $T$ consists of:
  1. **Signature $\Sigma_T$**: set of constant, function, and predicate symbols
  2. **Axioms $A_T$**: A set of FOL sentences over $\Sigma_T$

- **$\Sigma_T$ formula**: Formula constructed from symbols of $\Sigma_T$ and variables, logical connectives, and quantifiers.

- **Example**: We could have a theory of heights $T_H$ with signature $\Sigma_H : \{\text{taller}\}$ and axiom:
  $$\forall x, y. \text{taller}(x, y) \rightarrow \neg\text{taller}(y, x)$$

- **Is $\exists x. \forall z. \text{taller}(x, z) \land \text{taller}(y, w)$ legal $\Sigma_H$ formula?**
Signature and Axioms of First-Order Theory

- A first-order theory $T$ consists of:
  1. **Signature $\Sigma_T$**: set of constant, function, and predicate symbols
  2. **Axioms $A_T$**: A set of FOL sentences over $\Sigma_T$

- $\Sigma_T$ formula: Formula constructed from symbols of $\Sigma_T$ and variables, logical connectives, and quantifiers.

- **Example**: We could have a theory of heights $T_H$ with signature $\Sigma_H : \{\text{taller}\}$ and axiom:

  $$\forall x, y. \text{taller}(x, y) \rightarrow \neg\text{taller}(y, x)$$

- Is $\exists x. \forall z. \text{taller}(x, z) \land \text{taller}(y, w)$ legal $\Sigma_H$ formula? Yes
A first-order theory $T$ consists of:

1. **Signature $\Sigma_T$:** set of constant, function, and predicate symbols

2. **Axioms $A_T$:** A set of FOL sentences over $\Sigma_T$

**$\Sigma_T$ formula:** Formula constructed from symbols of $\Sigma_T$ and variables, logical connectives, and quantifiers.

**Example:** We could have a theory of heights $T_H$ with signature $\Sigma_H : \{\text{taller}\}$ and axiom:

$$\forall x, y. \text{taller}(x, y) \rightarrow \neg\text{taller}(y, x)$$

**Is $\exists x. \forall z. \text{taller}(x, z) \land \text{taller}(y, w)$ legal $\Sigma_H$ formula?** Yes

**What about $\exists x. \forall z. \text{taller}(x, z) \land \text{taller}(\text{joe}, \text{tom})$?**
Signature and Axioms of First-Order Theory

- A first-order theory $T$ consists of:
  1. **Signature $\Sigma_T$**: set of constant, function, and predicate symbols
  2. **Axioms $A_T$**: A set of FOL sentences over $\Sigma_T$

- **$\Sigma_T$ formula**: Formula constructed from symbols of $\Sigma_T$ and variables, logical connectives, and quantifiers.

- **Example**: We could have a theory of heights $T_H$ with signature $\Sigma_H : \{\text{taller}\}$ and axiom:
  \[
  \forall x, y. \text{taller}(x, y) \rightarrow \neg\text{taller}(y, x)
  \]

- Is $\exists x. \forall z. \text{taller}(x, z) \land \text{taller}(y, w)$ legal $\Sigma_H$ formula? Yes

- What about $\exists x. \forall z. \text{taller}(x, z) \land \text{taller}(\text{joe}, \text{tom})$? No
The axioms $A_T$ provide the meaning of symbols in $\Sigma_T$. 

Example: In our theory of heights, axioms define meaning of predicate `taller`

Specifically, axioms ensure that some interpretations legal in standard FOL are not legal in $T$

Example: Consider relation constant `taller`, and $U = \{A, B, C\}$

In FOL, possible interpretation: $I(\text{taller}) : \{\langle A, B \rangle, \langle B, A \rangle\}$

In our theory of heights, this interpretation is not legal b/c does not satisfy axioms
The axioms $A_T$ provide the meaning of symbols in $\Sigma_T$.

Example: In our theory of heights, axioms define meaning of predicate \textit{taller}.
Axioms of First-Order Theory

- The axioms $A_T$ provide the meaning of symbols in $\Sigma_T$.

- **Example:** In our theory of heights, axioms define meaning of predicate $taller$

- Specifically, axioms ensure that some interpretations legal in standard FOL are not legal in $T$
Axioms of First-Order Theory

- The axioms $A_T$ provide the meaning of symbols in $\Sigma_T$.

- **Example:** In our theory of heights, axioms define meaning of predicate `taller`.

- Specifically, axioms ensure that some interpretations legal in standard FOL are not legal in $T$.

- **Example:** Consider relation constant `taller`, and $U = \{A, B, C\}$.
Axioms of First-Order Theory

- The axioms \( A_T \) provide the meaning of symbols in \( \Sigma_T \).

- **Example:** In our theory of heights, axioms define meaning of predicate \( \text{taller} \).

- Specifically, axioms ensure that some interpretations legal in standard FOL are not legal in \( T \).

- **Example:** Consider relation constant \( \text{taller} \), and \( U = \{ A, B, C \} \).

- In FOL, possible interpretation: \( I(\text{taller}) : \{ \langle A, B \rangle, \langle B, A \rangle \} \).
Axioms of First-Order Theory

- The axioms $A_T$ provide the meaning of symbols in $\Sigma_T$.

- **Example:** In our theory of heights, axioms define meaning of predicate $taller$

- Specifically, axioms ensure that some interpretations legal in standard FOL are not legal in $T$

- **Example:** Consider relation constant $taller$, and $U = \{A, B, C\}$

- In FOL, possible interpretation: $I(taller) : \{\langle A, B \rangle, \langle B, A \rangle\}$

- In our theory of heights, this interpretation is not legal b/c does not satisfy axioms
Models of $T$

- A structure $M = \langle U, I \rangle$ is a model of theory $T$, or $T$-model, if $M \models A$ for every $A \in A_T$. 

Example: Consider structure consisting of universe $U = \{A, B\}$ and interpretation $I(taller) : \{\langle A, B \rangle, \langle B, A \rangle\}$.

- Is this a model of $T$? No

Now, consider the same $U$ and interpretation $\langle A, B \rangle$. Is this a model? Yes

Suppose our theory had another axiom: $\forall x, y, z. (taller(x, y) \land taller(y, z) \rightarrow taller(x, z))$.

- Consider $I(taller) : \{\langle A, B \rangle, \langle B, C \rangle\}$. Is $(U, I)$ a model? No
Models of $T$

- A structure $M = \langle U, I \rangle$ is a model of theory $T$, or $T$-model, if $M \models A$ for every $A \in A_T$.

- **Example:** Consider structure consisting of universe $U = \{A, B\}$ and interpretation $I(taller) : \{\langle A, B \rangle, \langle B, A \rangle\}$
Models of $T$

- A structure $M = \langle U, I \rangle$ is a model of theory $T$, or $T$-model, if $M \models A$ for every $A \in A_T$.

- **Example:** Consider structure consisting of universe $U = \{A, B\}$ and interpretation $I(taller) : \{\langle A, B \rangle, \langle B, A \rangle\}$.

- Is this a model of $T$?
Models of $T$

- A structure $M = \langle U, I \rangle$ is a model of theory $T$, or $T$-model, if $M \models A$ for every $A \in A_T$.

- **Example:** Consider structure consisting of universe $U = \{A, B\}$ and interpretation $I(taller) : \{\langle A, B \rangle, \langle B, A \rangle\}$

- Is this a model of $T$? No
Models of $T$

A structure $M = \langle U, I \rangle$ is a model of theory $T$, or $T$-model, if $M \models A$ for every $A \in A_T$.

Example: Consider structure consisting of universe $U = \{A, B\}$ and interpretation $I(taller) : \{\langle A, B\rangle, \langle B, A\rangle\}$

Is this a model of $T$? No

Now, consider same $U$ and interpretation $\langle A, B \rangle$. Is this a model?
Models of $T$

- A structure $M = \langle U, I \rangle$ is a model of theory $T$, or $T$-model, if $M \models A$ for every $A \in A_T$.

- **Example:** Consider structure consisting of universe $U = \{A, B\}$ and interpretation $I(taller) : \{\langle A, B \rangle, \langle B, A \rangle\}$

- Is this a model of $T$? **No**

- Now, consider same $U$ and interpretation $\langle A, B \rangle$. Is this a model? **Yes**
Models of $T$

- A structure $M = \langle U, I \rangle$ is a model of theory $T$, or $T$-model, if $M \models A$ for every $A \in A_T$.

- Example: Consider structure consisting of universe $U = \{A, B\}$ and interpretation $I(taller) : \{\langle A, B \rangle, \langle B, A \rangle\}$

- Is this a model of $T$? No

- Now, consider same $U$ and interpretation $\langle A, B \rangle$. Is this a model? Yes

- Suppose our theory had another axiom:

  $$\forall x, y, z. \ (taller(x, y) \land taller(y, z) \rightarrow taller(x, z))$$
Models of $T$

- A structure $M = \langle U, I \rangle$ is a model of theory $T$, or $T$-model, if $M \models A$ for every $A \in A_T$.

- **Example:** Consider structure consisting of universe $U = \{A, B\}$ and interpretation $I(taller) : \{\langle A, B \rangle, \langle B, A \rangle\}$

- Is this a model of $T$? No

- Now, consider same $U$ and interpretation $\langle A, B \rangle$. Is this a model? Yes

- Suppose our theory had another axiom:

  $$\forall x, y, z. (taller(x, y) \land taller(y, z) \rightarrow taller(x, z))$$

- Consider $I(taller) : \{\langle A, B \rangle, \langle B, C \rangle\}$. Is $(U, I)$ a model?
Models of $T$

- A structure $M = \langle U, I \rangle$ is a model of theory $T$, or $T$-model, if $M \models A$ for every $A \in A_T$.

- **Example:** Consider structure consisting of universe $U = \{A, B\}$ and interpretation $I(taller) : \{\langle A, B \rangle, \langle B, A \rangle\}$

- Is this a model of $T$? No

- Now, consider same $U$ and interpretation $\langle A, B \rangle$. Is this a model? Yes

- Suppose our theory had another axiom:
  $$\forall x, y, z. \ (taller(x, y) \land taller(y, z) \rightarrow taller(x, z))$$

- **Consider** $I(taller) : \{\langle A, B \rangle, \langle B, C \rangle\}$. Is $(U, I)$ a model? No
Formula $F$ is satisfiable modulo $T$ if there exists a $T$-model $M$ and variable assignment $\sigma$ such that $M, \sigma \models F$.
Satisfiability and Validity Modulo $T$

- Formula $F$ is **satisfiable modulo** $T$ if there exists a $T$-model $M$ and variable assignment $\sigma$ such that $M, \sigma \models F$

- Formula $F$ is **valid modulo** $T$ if for all $T$-models $M$ and variable assignments $\sigma$, $M, \sigma \models F$
Satisfiability and Validity Modulo $T$

- Formula $F$ is **satisfiable modulo** $T$ if there exists a $T$-model $M$ and variable assignment $\sigma$ such that $M, \sigma \models F$

- Formula $F$ is **valid modulo** $T$ if for all $T$-models $M$ and variable assignments $\sigma$, $M, \sigma \models F$

- **Question**: How is validity modulo $T$ different from FOL-validity?
Satisfiability and Validity Modulo $T$

- Formula $F$ is **satisfiable modulo** $T$ if there exists a $T$-model $M$ and variable assignment $\sigma$ such that $M, \sigma \models F$.

- Formula $F$ is **valid modulo** $T$ if for all $T$-models $M$ and variable assignments $\sigma$, $M, \sigma \models F$.

**Question:** How is validity modulo $T$ different from FOL-validity?

**Answer:** Disregards all structures that do not satisfy theory axioms.
Satisfiability and Validity Modulo $T$

- Formula $F$ is **satisfiable modulo** $T$ if there exists a $T$-model $M$ and variable assignment $\sigma$ such that $M, \sigma \models F$

- Formula $F$ is **valid modulo** $T$ if for all $T$-models $M$ and variable assignments $\sigma$, $M, \sigma \models F$

**Question:** How is validity modulo $T$ different from FOL-validity?

**Answer:** Disregards all structures that do not satisfy theory axioms.

**If a formula $F$ is valid modulo theory $T$, we will write $T \models F$.**
Satisfiability and Validity Modulo $T$

- Formula $F$ is **satisfiable modulo** $T$ if there exists a $T$-model $M$ and variable assignment $\sigma$ such that $M, \sigma \models F$.

- Formula $F$ is **valid modulo** $T$ if for all $T$-models $M$ and variable assignments $\sigma$, $M, \sigma \models F$.

**Question:** How is validity modulo $T$ different from FOL-validity?

**Answer:** Disregards all structures that do not satisfy theory axioms.

- If a formula $F$ is valid modulo theory $T$, we will write $T \models F$.

- Theory $T$ consists of all sentences that are valid in $T$. 
Equivalence Modulo $T$

- Two formulas $F_1$ and $F_2$ are equivalent modulo theory $T$ if for every $T$-model $M$ and for every variable assignment $\sigma$:

$$M, \sigma \models F_1 \text{ iff } M, \sigma \models F_2$$
Equivalence Modulo $T$

- Two formulas $F_1$ and $F_2$ are **equivalent modulo theory $T$** if for every $T$-model $M$ and for every variable assignment $\sigma$:

  $$M, \sigma \models F_1 \text{ iff } M, \sigma \models F_2$$

- Another way of stating equivalence of $F_1$ and $F_2$ modulo $T$:

  $$T \models F_1 \leftrightarrow F_2$$
Two formulas $F_1$ and $F_2$ are equivalent modulo theory $T$ if for every $T$-model $M$ and for every variable assignment $\sigma$:

$$M, \sigma \models F_1 \text{ iff } M, \sigma \models F_2$$

Another way of stating equivalence of $F_1$ and $F_2$ modulo $T$:

$$T \models F_1 \leftrightarrow F_2$$

Example: Consider a theory $T_=$ with predicate symbol $=$ and suppose $A_T$ gives the intended meaning of equality to $=$.
Equivalence Modulo $T$

- Two formulas $F_1$ and $F_2$ are equivalent modulo theory $T$ if for every $T$-model $M$ and for every variable assignment $\sigma$:

$$M, \sigma \models F_1 \text{ iff } M, \sigma \models F_2$$

- Another way of stating equivalence of $F_1$ and $F_2$ modulo $T$:

$$T \models F_1 \leftrightarrow F_2$$

- Example: Consider a theory $T_=$ with predicate symbol $=$ and suppose $A_T$ gives the intended meaning of equality to $=.$

- Are $x = y$ and $y = x$ equivalent modulo $T_=$?
Equivalence Modulo $T$

- Two formulas $F_1$ and $F_2$ are **equivalent modulo theory** $T$ if for every $T$-model $M$ and for every variable assignment $\sigma$:

  \[ M, \sigma \models F_1 \iff M, \sigma \models F_2 \]

- Another way of stating equivalence of $F_1$ and $F_2$ modulo $T$:

  \[ T \models F_1 \leftrightarrow F_2 \]

- **Example:** Consider a theory $T_\equiv$ with predicate symbol $=$ and suppose $A_T$ gives the intended meaning of equality to $=$.

- Are $x = y$ and $y = x$ equivalent modulo $T_\equiv$? Yes
Equivalence Modulo $T$

- Two formulas $F_1$ and $F_2$ are equivalent modulo theory $T$ if for every $T$-model $M$ and for every variable assignment $\sigma$:

  $$M, \sigma \models F_1 \text{ iff } M, \sigma \models F_2$$

- Another way of stating equivalence of $F_1$ and $F_2$ modulo $T$:

  $$T \models F_1 \leftrightarrow F_2$$

- Example: Consider a theory $T_\simeq$ with predicate symbol $\simeq$ and suppose $A_T$ gives the intended meaning of equality to $\simeq$.

- Are $x = y$ and $y = x$ equivalent modulo $T_\simeq$? Yes

- Are they equivalent according to FOL semantics?
Equivalence Modulo $T$

- Two formulas $F_1$ and $F_2$ are **equivalent modulo theory** $T$ if for every $T$-model $M$ and for every variable assignment $\sigma$:

$$M, \sigma \models F_1 \text{ iff } M, \sigma \models F_2$$

- Another way of stating equivalence of $F_1$ and $F_2$ modulo $T$:

$$T \models F_1 \leftrightarrow F_2$$

- **Example:** Consider a theory $T_\leq$ with predicate symbol $\leq$ and suppose $A_T$ gives the intended meaning of equality to $\leq$.

- Are $x = y$ and $y = x$ equivalent modulo $T_\leq$? Yes

- Are they equivalent according to FOL semantics? No
Equivalence Modulo $T$

- Two formulas $F_1$ and $F_2$ are equivalent modulo theory $T$ if for every $T$-model $M$ and for every variable assignment $\sigma$:

$$M, \sigma \models F_1 \iff M, \sigma \models F_2$$

- Another way of stating equivalence of $F_1$ and $F_2$ modulo $T$:

$$T \models F_1 \leftrightarrow F_2$$

- Example: Consider a theory $T_\leq$ with predicate symbol $=$ and suppose $A_T$ gives the intended meaning of equality to $=$.

- Are $x = y$ and $y = x$ equivalent modulo $T_\leq$? Yes

- Are they equivalent according to FOL semantics? No

- Falsifying interpretation:
Equivalence Modulo $T$

- Two formulas $F_1$ and $F_2$ are **equivalent modulo theory** $T$ if for every $T$-model $M$ and for every variable assignment $\sigma$:
  \[
  M, \sigma \models F_1 \iff M, \sigma \models F_2
  \]

- Another way of stating equivalence of $F_1$ and $F_2$ modulo $T$:
  \[
  T \models F_1 \iff F_2
  \]

- **Example:** Consider a theory $T_\equiv$ with predicate symbol $\equiv$ and suppose $A_T$ gives the intended meaning of equality to $\equiv$.

- Are $x = y$ and $y = x$ equivalent modulo $T_\equiv$? **Yes**

- Are they equivalent according to FOL semantics? **No**

- **Falsifying interpretation:** $U = \{\Box, \triangle\}, I(\equiv) : \{\langle \triangle, \Box \rangle\}$
A theory \( T \) is complete if for every sentence \( F \), if \( T \) entails \( F \) or its negation:

\[
T \models F \text{ or } T \models \neg F
\]
Completeness of Theory

- A theory $T$ is complete if for every sentence $F$, if $T$ entails $F$ or its negation:

$$T \models F \text{ or } T \models \neg F$$

- Question: In first-order logic, for every closed formula $F$, is either $F$ or $\neg F$ valid?
Completeness of Theory

- A theory $T$ is complete if for every sentence $F$, if $T$ entails $F$ or its negation:

  $$T \models F \text{ or } T \models \neg F$$

- Question: In first-order logic, for every closed formula $F$, is either $F$ or $\neg F$ valid?

- Answer: No! Consider $p(a)$: Neither $p(a)$ nor $\neg p(a)$ is valid.
Completeness of Theory

- A theory $T$ is **complete** if for every sentence $F$, if $T$ entails $F$ or its negation:
  \[ T \models F \text{ or } T \models \neg F \]

- **Question:** In first-order logic, for every closed formula $F$, is either $F$ or $\neg F$ valid?

- **Answer:** No! Consider $p(a)$: Neither $p(a)$ nor $\neg p(a)$ is valid.

- Consider $U = \{\circ, \star\}$
Completeness of Theory

- A theory $T$ is complete if for every sentence $F$, if $T$ entails $F$ or its negation:

$$T \models F \text{ or } T \models \neg F$$

- **Question:** In first-order logic, for every closed formula $F$, is either $F$ or $\neg F$ valid?

- **Answer:** No! Consider $p(a)$: Neither $p(a)$ nor $\neg p(a)$ is valid.

- Consider $U = \{\circ, \star\}$

- Falsifying interpretation for $p(a)$:
Completeness of Theory

- A theory $T$ is complete if for every sentence $F$, if $T$ entails $F$ or its negation:

  \[ T \models F \text{ or } T \models \neg F \]

- **Question:** In first-order logic, for every closed formula $F$, is either $F$ or $\neg F$ valid?

- **Answer:** No! Consider $p(a)$: Neither $p(a)$ nor $\neg p(a)$ is valid.

- Consider $U = \{\circ, \star\}$

- Falsifying interpretation for $p(a)$: $I(a) = \circ$, $I(p) = \{(\star)\}$
Completeness of Theory

▶ A theory $T$ is complete if for every sentence $F$, if $T$ entails $F$ or its negation:

$$T \models F \text{ or } T \models \neg F$$

▶ Question: In first-order logic, for every closed formula $F$, is either $F$ or $\neg F$ valid?

▶ Answer: No! Consider $p(a)$: Neither $p(a)$ nor $\neg p(a)$ is valid.

▶ Consider $U = \{\circ, \star\}$

▶ Falsifying interpretation for $p(a)$: $I(a) = \circ$, $I(p) = \{\langle \star \rangle\}$

▶ Falsifying interpretation for $\neg p(a)$:
Completeness of Theory

- A theory $T$ is complete if for every sentence $F$, if $T$ entails $F$ or its negation:

$$T \models F \text{ or } T \models \neg F$$

- **Question**: In first-order logic, for every closed formula $F$, is either $F$ or $\neg F$ valid?

- **Answer**: No! Consider $p(a)$: Neither $p(a)$ nor $\neg p(a)$ is valid.

- Consider $U = \{\circ, \star\}$

- Falsifying interpretation for $p(a)$: $I(a) = \circ$, $I(p) = \{\langle \star \rangle\}$

- Falsifying interpretation for $\neg p(a)$: $I(a) = \circ$, $I(p) = \{\langle \circ \rangle\}$
Decidability of Theory

A theory $T$ is **decidable** if for every formula $F$, there exists an algorithm that:

1. always terminates and answers "yes" if $F$ is valid modulo $T$ and
2. terminates and answers "no" if $F$ is not valid modulo $T$
Decidability of Theory

- A theory $T$ is **decidable** if for every formula $F$, there exists an algorithm that:
  1. always terminates and answers "yes" if $F$ is valid modulo $T$ and
  2. terminates and answers "no" if $F$ is not valid modulo $T$

- Unlike full first-order logic, many of the first-order theories we will study are decidable.
Decidability of Theory

- A theory $T$ is **decidable** if for every formula $F$, there exists an algorithm that:
  
  1. always terminates and answers "yes" if $F$ is valid modulo $T$ and
  2. terminates and answers "no" if $F$ is not valid modulo $T$

- Unlike full first-order logic, many of the first-order theories we will study are decidable.

- For those that are not decidable, we are interested in **fragments** of that theory that are decidable.
Fragments of Theories

- A **fragment** of a theory is a syntactically restricted subset of that theory.
Fragments of Theories

- A **fragment** of a theory is a syntactically restricted subset of that theory.

- **Example**: Quantifier-free fragment of a theory $T$ is the set of quantifier-free formulas that are valid modulo $T$. 
Fragments of Theories

- **A fragment** of a theory is a syntactically restricted subset of that theory.

- **Example:** Quantifier-free fragment of a theory \( T \) is the set of quantifier-free formulas that are valid modulo \( T \).

- A fragment of \( T \) is **decidable** if it is decidable whether \( T \models F \) for every formula \( F \) in that fragment.
Fragments of Theories

- A **fragment** of a theory is a syntactically restricted subset of that theory.

- **Example:** Quantifier-free fragment of a theory $T$ is the set of quantifier-free formulas that are valid modulo $T$.

- A fragment of $T$ is **decidable** if it is decidable whether $T \models F$ for every formula $F$ in that fragment.

- For some of the theories we will look at, the full theory is not decidable, but their quantifier-free fragment is (often efficiently) decidable and very useful in practice.
Examples of Theories

- **Remainder of this lecture:** Introduction to commonly-used first-order theories:
Examples of Theories

- **Remainder of this lecture:** Introduction to commonly-used first-order theories:
  1. Theory of equality
  2. Peano Arithmetic
  3. Presburger Arithmetic
  4. Theory of Rationals
  5. Theory of Arrays
Examples of Theories

▶ **Remainder of this lecture:** Introduction to commonly-used first-order theories:

1. Theory of equality
2. Peano Arithmetic
3. Presburger Arithmetic
4. Theory of Rationals
5. Theory of Arrays

▶ In the following lectures, we will further explore these theories and look at decision procedures.
Overview of the Theory of Equality $T_=$

- Extends first-order logic with a "built-in" equality predicate $=$
Overview of the Theory of Equality $T_=$

- Extends first-order logic with a "built-in" equality predicate $=$

- **Signature:**

  $$
  \Sigma_\ =
  : \{=, a, b, c, \cdots, f, g, h, \cdots, p, q, r, \cdots\}
  $$

  - $=\,$, a binary predicate, **interpreted** by axioms.

  - all constant, function, and predicate symbols.
Axioms of the Theory of Equality

- Axioms of $T_=$ define the meaning of equality predicate $=$
Axioms of the Theory of Equality

- Axioms of $T_=$ define the meaning of equality predicate $=$
- Equality is reflexive, symmetric, and transitive:
Axioms of the Theory of Equality

- Axioms of $T_=$ define the meaning of equality predicate $=$

- Equality is reflexive, symmetric, and transitive:

  1. $\forall x. \ x = x$  \hspace{1cm} (reflexivity)
Axioms of the Theory of Equality

- Axioms of $T_=$ define the meaning of equality predicate $=$

- Equality is reflexive, symmetric, and transitive:

  1. $\forall x. x = x$ (reflexivity)

  2. $\forall x, y. x = y \rightarrow y = x$ (symmetry)

  3. $\forall x, y, z. x = y \land y = z \rightarrow x = z$ (transitivity)
Axioms of the Theory of Equality

- Axioms of \( T = \) define the meaning of equality predicate :=

- Equality is reflexive, symmetric, and transitive:

  1. \( \forall x. \ x = x \)  
     \( \text{(reflexivity)} \)

  2. \( \forall x, y. \ x = y \rightarrow y = x \)  
     \( \text{(symmetry)} \)
Axioms of the Theory of Equality

- Axioms of $T_=$ define the meaning of equality predicate $=$

- Equality is reflexive, symmetric, and transitive:

  1. $\forall x. x = x$  \hspace{2cm} (reflexivity)

  2. $\forall x, y. x = y \rightarrow y = x$  \hspace{2cm} (symmetry)

  3. $\forall x, y, z. x = y \land y = z \rightarrow x = z$  \hspace{2cm} (transitivity)
Axioms of the Theory of Equality

- Axioms of $T_=$ define the meaning of equality predicate $=$

- Equality is reflexive, symmetric, and transitive:

  1. $\forall x. \; x = x$  
     \hspace{1cm} \text{(reflexivity)}

  2. $\forall x, y. \; x = y \rightarrow y = x$  
     \hspace{1cm} \text{(symmetry)}

  3. $\forall x, y, z. \; x = y \land y = z \rightarrow x = z$  
     \hspace{1cm} \text{(transitivity)}
Consider universe $U = \{\circ, \bullet\}$. 

Which interpretations of $\models$ are allowed according to axioms?

$I(\models) : \{\langle \circ, \circ \rangle, \langle \bullet, \bullet \rangle\}$?

No, violates reflexivity, transitivity

$I(\models) : \{\langle \circ, \circ \rangle, \langle \circ, \bullet \rangle, \langle \bullet, \bullet \rangle, \langle \bullet, \circ \rangle\}$?

Yes
Consider universe \( U = \{ \circ, \bullet \} \).

Which interpretations of \( = \) are allowed according to axioms?
Example

- Consider universe $U = \{\circ, \bullet\}$.

- Which interpretations of $=$ are allowed according to axioms?
  - $I(=) : \{\langle \circ, \bullet \rangle, \langle \bullet, \circ \rangle\}$?
Example

- Consider universe $U = \{\circ, \bullet\}$.

- Which interpretations of $=$ are allowed according to axioms?
  - $I(=) : \{\langle \circ, \bullet \rangle, \langle \bullet, \circ \rangle\}$? No, violates reflexivity, transitivity
Example

- Consider universe $U = \{\circ, \bullet\}$.

- Which interpretations of $=$ are allowed according to axioms?
  - $I(=) : \{\langle\circ, \bullet\rangle, \langle \bullet, \circ \rangle\}$? No, violates reflexivity, transitivity
  - $I(=) : \{\langle \circ, \circ \rangle, \langle \bullet, \bullet \rangle\}$?
Example

Consider universe $U = \{◦, •\}$.

Which interpretations of $=$ are allowed according to axioms?

- $I(=) : \{\langle◦, •\rangle, \langle•, ◦\rangle\}$? No, violates reflexivity, transitivity

- $I(=) : \{\langle◦, ◦\rangle, \langle•, •\rangle\}$? Yes
Example

- Consider universe $U = \{\circ, \bullet\}$.

- Which interpretations of $=$ are allowed according to axioms?
  - $I(=) : \{\langle \circ, \bullet \rangle, \langle \bullet, \circ \rangle\}$? No, violates reflexivity, transitivity
  - $I(=) : \{\langle \circ, \circ \rangle, \langle \bullet, \bullet \rangle\}$? Yes
  - $I(=) : \{\langle \circ, \circ \rangle, \langle \circ, \bullet \rangle, \langle \bullet, \bullet \rangle, \langle \bullet, \circ \rangle\}$?
Example

- Consider universe \( U = \{\circ, \bullet\} \).

- Which interpretations of \( = \) are allowed according to axioms?
  - \( I(=) : \{\langle \circ, \bullet \rangle, \langle \bullet, \circ \rangle\} \)?
    - No, violates reflexivity, transitivity
  - \( I(=) : \{\langle \circ, \circ \rangle, \langle \bullet, \bullet \rangle\} \)?
    - Yes
  - \( I(=) : \{\langle \circ, \circ \rangle, \langle \circ, \bullet \rangle, \langle \bullet, \bullet \rangle, \langle \bullet, \circ \rangle\} \)?
    - Yes
Axioms of the Theory of Equality, cont.

- **Function congruence:**
  For any \( n \)-ary function \( f \), two terms \( f(\bar{x}) \) and \( f(\bar{y}) \) are equal if \( \bar{x} \) and \( \bar{y} \) are equal:

\[
\forall x_1, \ldots, x_n, y_1, \ldots, y_n. \bigwedge_{i} x_i = y_i \rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)
\]
Axioms of the Theory of Equality, cont.

- **Function congruence:**
  For any $n$-ary function $f$, two terms $f(\vec{x})$ and $f(\vec{y})$ are equal if $\vec{x}$ and $\vec{y}$ are equal:

  $$\forall x_1, \ldots, x_n, y_1, \ldots, y_n. \bigwedge_i x_i = y_i \rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$$

- **Predicate congruence:**
  For any $n$-ary predicate $p$, two formulas $p(\vec{x})$ and $p(\vec{y})$ are equivalent if $\vec{x}$ and $\vec{y}$ are equal:

  $$\forall x_1, \ldots, x_n, y_1, \ldots, y_n. \bigwedge_i x_i = y_i \rightarrow (p(x_1, \ldots, x_n) \leftrightarrow p(y_1, \ldots, y_n))$$
Function/predicate congruence "axioms" stand for a set of axioms, instantiated for each function and predicate symbol.
Congruence and Axiom Schemata

- Function/predicate congruence "axioms" stand for a set of axioms, instantiated for each function and predicate symbol.

- Thus, these are not really axioms, but axiom schemata.
Congruence and Axiom Schemata

- Function/predicate congruence "axioms" stand for a set of axioms, instantiated for each function and predicate symbol.

- Thus, these are not really axioms, but axiom schemata.

- Example: For unary functions $g$ and $h$, function congruence axiom scheme stands for two axioms:
Function/predicate congruence "axioms" stand for a set of axioms, instantiated for each function and predicate symbol.

Thus, these are not really axioms, but axiom schemata.

Example: For unary functions $g$ and $h$, function congruence axiom scheme stands for two axioms:

1. $\forall x, y. (x = y \rightarrow g(x) = g(y))$
Congruence and Axiom Schemata

- Function/predicate congruence "axioms" stand for a set of axioms, instantiated for each function and predicate symbol.

- Thus, these are not really axioms, but axiom schemata.

- Example: For unary functions $g$ and $h$, function congruence axiom scheme stands for two axioms:

  1. $\forall x, y. (x = y \rightarrow g(x) = g(y))$

  2. $\forall x, y. (x = y \rightarrow h(x) = h(y))$
Example

Consider universe \{\circ, \bullet, \star\}, and

\[ I(\equiv) : \{\langle \circ, \circ \rangle, \langle \circ, \bullet \rangle, \langle \bullet, \bullet \rangle, \langle \bullet, \circ \rangle, \langle \star, \star \rangle\} \]
Example

- Consider universe \{\circ, \bullet, \star\}, and

  \[ I(\equiv) : \{\langle\circ, \circ\rangle, \langle\circ, \bullet\rangle, \langle\bullet, \bullet\rangle, \langle\bullet, \circ\rangle, \langle\star, \star\rangle\} \]

- Are the following valid interpretations?
Example

- Consider universe $\{\circ, \bullet, \star\}$, and

$$I(=) : \{\langle \circ, \circ \rangle, \langle \circ, \bullet \rangle, \langle \bullet, \bullet \rangle, \langle \bullet, \circ \rangle, \langle \star, \star \rangle\}$$

- Are the following valid interpretations?
  - $I(f) = \{\bullet \mapsto \circ, \circ \mapsto \star, \star \mapsto \star\}$
  - $I(f) = \{\bullet \mapsto \circ, \circ \mapsto \bullet, \star \mapsto \star\}$
Example

Consider universe $\{\circ, \bullet, \star\}$, and

$$I(=) : \{\langle \circ, \circ \rangle, \langle \circ, \bullet \rangle, \langle \bullet, \bullet \rangle, \langle \bullet, \circ \rangle, \langle \star, \star \rangle\}$$

Are the following valid interpretations?

- $I(f) = \{\bullet \mapsto \circ, \circ \mapsto \star, \star \mapsto \star\}$ No
Example

Consider universe \{◦, ●, ⋆\}, and

\[ I(=) : \{ ⟨◦, ◦⟩, ⟨◦, ●⟩, ⟨●, ●⟩, ⟨●, ◦⟩, ⟨⋆, ⋆⟩ \} \]

- Are the following valid interpretations?
  - \[ I(f) = \{ ● \mapsto ◦, ◦ \mapsto ⋆, ⋆ \mapsto ⋆ \} \text{ No} \]
  - \[ I(f) = \{ ● \mapsto ●, ◦ \mapsto ●, ⋆ \mapsto ● \} \]
Example

Consider universe \(\{\circ, \bullet, \star\}\), and

\[
I(\equiv) : \{\langle \circ, \circ \rangle, \langle \circ, \bullet \rangle, \langle \bullet, \bullet \rangle, \langle \bullet, \circ \rangle, \langle \star, \star \rangle\}
\]

Are the following valid interpretations?

- \(I(f) = \{\bullet \mapsto \circ, \circ \mapsto \star, \star \mapsto \star\}\) No

- \(I(f) = \{\bullet \mapsto \bullet, \circ \mapsto \bullet, \star \mapsto \bullet\}\) Yes
Example

- Consider universe \{\text{o}, \text{•}, \text{*}\}, and

\[
I(\equiv) : \{\langle\text{o}, \text{o}\rangle, \langle\text{o}, \text{•}\rangle, \langle\text{•}, \text{•}\rangle, \langle\text{•}, \text{o}\rangle, \langle\text{*}, \text{*}\rangle\}
\]

- Are the following valid interpretations?

  - \(I(f) = \{\text{•} \mapsto \text{o}, \text{o} \mapsto \text{*}, \text{*} \mapsto \text{*}\}\) No

  - \(I(f) = \{\text{•} \mapsto \text{•}, \text{o} \mapsto \text{•}, \text{*} \mapsto \text{•}\}\) Yes

  - \(I(f) = \{\text{•} \mapsto \text{o}, \text{o} \mapsto \text{•}, \text{*} \mapsto \text{*}\}\)

Vijay Ganesh (Original notes from Isil Dillig), ECE750T-28: Computer-aided Reasoning for Software Engineering Lecture 9: Overview of First-Order Theories
Example

Consider universe \(\{\circ, \bullet, \star\}\), and

\[
I(=) : \{\langle \circ, \circ \rangle, \langle \circ, \bullet \rangle, \langle \bullet, \bullet \rangle, \langle \bullet, \circ \rangle, \langle \star, \star \rangle\}
\]

Are the following valid interpretations?

- \(I(f) = \{\bullet \mapsto \circ, \circ \mapsto \star, \star \mapsto \star\}\) No
- \(I(f) = \{\bullet \mapsto \bullet, \circ \mapsto \bullet, \star \mapsto \bullet\}\) Yes
- \(I(f) = \{\bullet \mapsto \circ, \circ \mapsto \bullet, \star \mapsto \star\}\) Yes
Proving Validity in $T$ using Semantic Arguments

- Semantic argument method can be used to prove $T$ validity.
Proving Validity in $T_\equiv$ using Semantic Arguments

- Semantic argument method can be used to prove $T_\equiv$ validity.

- As before, assume formula is $T_\equiv$ invalid, i.e., there exists a $T_\equiv$ model $M$ and variable assignment $\sigma$ such that $M, \sigma \not\models F$. 
Proving Validity in $T$ using Semantic Arguments

- Semantic argument method can be used to prove $T$ validity.

- As before, assume formula is $T$ invalid, i.e., there exists a $T$ model $M$ and variable assignment $\sigma$ such that $M, \sigma \not\models F$.

- In addition to proof rules for FOL, our proof can also use axioms of $T$. 
Proving Validity in $T_\models$ using Semantic Arguments

- Semantic argument method can be used to prove $T_\models$ validity.

- As before, assume formula is $T_\models$ invalid, i.e., there exists a $T_\models$ model $M$ and variable assignment $\sigma$ such that $M, \sigma \not\models F$.

- In addition to proof rules for FOL, our proof can also use axioms of $T_\models$.

- If we derive contradiction in every branch, formula is valid modulo $T_\models$. 
Example

Prove

\[ F : a = b \land b = c \rightarrow g(f(a), b) = g(f(c), a) \quad T_E\text{-valid}. \]
Example

Prove

\[ F : \ a = b \land b = c \rightarrow g(f(a), b) = g(f(c), a) \quad T_E\text{-valid.} \]

1. \( M, \sigma \not\models F \)

assumption
Example

Prove

\[ F : \ a = b \land b = c \rightarrow g(f(a), b) = g(f(c), a) \quad T_E\text{-valid.} \]

1. \[ M, \sigma \not\models F \quad \text{assumption} \]
2. \[ M, \sigma \models a = b \land b = c \quad 1, \rightarrow \]
3. \[ M, \sigma \not\models g(f(a), b) = g(f(c), a) \quad 1, \rightarrow \]
Example

Prove

\[ F : \ a = b \land b = c \rightarrow g(f(a), b) = g(f(c), a) \quad T_E\text{-valid.} \]

1. \( M, \sigma \not\models F \) assumption
2. \( M, \sigma \models a = b \land b = c \) 1, \( \rightarrow \)
3. \( M, \sigma \not\models g(f(a), b) = g(f(c), a) \) 1, \( \rightarrow \)
4. \( M, \sigma \models a = b \) 2, \( \land \)
5. \( M, \sigma \models b = c \) 2, \( \land \)
Example

Prove

\[ F : a = b \land b = c \rightarrow g(f(a), b) = g(f(c), a) \quad T_E\text{-valid.} \]

1. \( M, \sigma \not\models F \) \hspace{1cm} \text{assumption}
2. \( M, \sigma \models a = b \land b = c \) \hspace{1cm} 1, \rightarrow
3. \( M, \sigma \not\models g(f(a), b) = g(f(c), a) \) \hspace{1cm} 1, \rightarrow
4. \( M, \sigma \models a = b \) \hspace{1cm} 2, \land
5. \( M, \sigma \models b = c \) \hspace{1cm} 2, \land
6. \( M, \sigma \models a = c \) \hspace{1cm} 4, 5, (transitivity)
Example

Prove

\[ F : \ a = b \land b = c \rightarrow g(f(a), b) = g(f(c), a) \quad T_E\text{-valid.} \]

1. \( M, \sigma \not\models F \)
   assumption
2. \( M, \sigma \models a = b \land b = c \)
   1, \( \rightarrow \)
3. \( M, \sigma \not\models g(f(a), b) = g(f(c), a) \)
   1, \( \rightarrow \)
4. \( M, \sigma \models a = b \)
   2, \( \land \)
5. \( M, \sigma \models b = c \)
   2, \( \land \)
6. \( M, \sigma \models a = c \)
   4, 5, (transitivity)
7. \( M, \sigma \models f(a) = f(c) \)
   6, (congruence)
Example

Prove

\[ F : a = b \land b = c \rightarrow g(f(a), b) = g(f(c), a) \quad TE\text{-valid.} \]

\begin{align*}
1. & \quad M, \sigma \not\models F \quad \text{assumption} \\
2. & \quad M, \sigma \models a = b \land b = c \quad 1, \rightarrow \\
3. & \quad M, \sigma \not\models g(f(a), b) = g(f(c), a) \quad 1, \rightarrow \\
4. & \quad M, \sigma \models a = b \quad 2, \land \\
5. & \quad M, \sigma \models b = c \quad 2, \land \\
6. & \quad M, \sigma \models a = c \quad 4, 5, \text{(transitivity)} \\
7. & \quad M, \sigma \models f(a) = f(c) \quad 6, \text{(congruence)} \\
8. & \quad M, \sigma \models b = a \quad 6, \text{(symmetry)}
\end{align*}
Example

Prove

\[ F : a = b \land b = c \rightarrow g(f(a), b) = g(f(c), a) \quad T_E\text{-valid.} \]

1. \( M, \sigma \not\models F \) assumption
2. \( M, \sigma \models a = b \land b = c \) 1, \( \rightarrow \)
3. \( M, \sigma \not\models g(f(a), b) = g(f(c), a) \) 1, \( \rightarrow \)
4. \( M, \sigma \models a = b \) 2, \( \land \)
5. \( M, \sigma \models b = c \) 2, \( \land \)
6. \( M, \sigma \models a = c \) 4, 5, (transitivity)
7. \( M, \sigma \models f(a) = f(c) \) 6, (congruence)
8. \( M, \sigma \models b = a \) 6, (symmetry)
9. \( M, \sigma \models g(f(a), b) = g(f(c), a) \) 7, 8, (congruence)
Example

Prove

\[ F : \; a = b \land b = c \rightarrow g(f(a), b) = g(f(c), a) \quad T_E\text{-valid.} \]

1. \( M, \sigma \not\models F \) \hspace{1cm} \text{assumption}
2. \( M, \sigma \models a = b \land b = c \) \hspace{1cm} 1, \rightarrow
3. \( M, \sigma \not\models g(f(a), b) = g(f(c), a) \) \hspace{1cm} 1, \rightarrow
4. \( M, \sigma \models a = b \) \hspace{1cm} 2, \land
5. \( M, \sigma \models b = c \) \hspace{1cm} 2, \land
6. \( M, \sigma \models a = c \) \hspace{1cm} 4, 5, (transitivity)
7. \( M, \sigma \models f(a) = f(c) \) \hspace{1cm} 6, (congruence)
8. \( M, \sigma \models b = a \) \hspace{1cm} 6, (symmetry)
9. \( M, \sigma \models g(f(a), b) = g(f(c), a) \) \hspace{1cm} 7, 8, (congruence)
10. \( M, \sigma \models \bot \) \hspace{1cm} 3, 9
Decidability and Completeness Results for $T_=$

- Is the full theory of equality decidable?
Decidability and Completeness Results for $T$$_=$

- Is the full theory of equality decidable?
  - No, because it is an extension of FOL

- No, because it is an extension of FOL
Decidability and Completeness Results for $T_=$

- Is the full theory of equality decidable?
  - No, because it is an extension of FOL

- However, quantifier-free fragment of $T_=$ is decidable
Decidability and Completeness Results for $T_=$

- Is the full theory of equality decidable?
  - No, because it is an extension of FOL
- However, quantifier-free fragment of $T_=$ is decidable
- Is $T_=$ complete? (i.e., for any $F$, $T_= \models F$ or $T_= \models \neg F$?)
Decidability and Completeness Results for $T_=$

- Is the full theory of equality decidable?
  - No, because it is an extension of FOL

- However, quantifier-free fragment of $T_=$ is decidable

- Is $T_=$ complete? (i.e., for any $F$, $T_\models F$ or $T_\models \neg F$?)
  - No! $T_\not\models f(a) = b$ and $T_\not\models f(a) \neq b$
There are three major logical first-order theories involving natural numbers and arithmetic.

- Peano arithmetic: Allows multiplication and addition over natural numbers.
- Presburger arithmetic: Allows only addition over natural numbers.
- Theory of integers: Equivalent in expressiveness to Presburger arithmetic, but more convenient notation.
Theories Involving Natural Numbers and Integers

- There are three major logical first-order theories involving natural numbers and arithmetic.

- Peano arithmetic: Allows multiplication and addition over natural numbers
Theories Involving Natural Numbers and Integers

- There are three major logical first-order theories involving natural numbers and arithmetic.
  - **Peano arithmetic**: Allows multiplication and addition over natural numbers
  - **Presburger arithmetic**: Allows only addition over natural numbers
Theories Involving Natural Numbers and Integers

- There are three major logical first-order theories involving natural numbers and arithmetic.

- **Peano arithmetic**: Allows multiplication and addition over natural numbers

- **Presburger arithmetic**: Allows only addition over natural numbers

- **Theory of integers**: Equivalent in expressiveness to Presburger arithmetic, but more convenient notation
The theory of Peano arithmetic $T_{PA}$ has signature:

$$\Sigma_{PA} : \{0, 1, +, \cdot, =\}$$

- $0, 1$ are constants
- $+, \cdot$ binary functions
- $=$ is a binary predicate
Peano Arithmetic Examples

- **Question**: Is the following a well-formed formula in $T_{PA}$?

$$x + y = 1 \lor f(x) = 1 + 1$$
Question: Is the following a well-formed formula in $T_{PA}$?

\[ x + y = 1 \lor f(x) = 1 + 1 \]

No because contains function symbol $f$
Question: Is the following a well-formed formula in $T_{PA}$?

$$x + y = 1 \lor f(x) = 1 + 1$$

No because contains function symbol $f$

What about $\forall x. \exists y. \exists z. x + y = 1 \lor z \cdot x = 1 + 1$?

No!

But can be rewritten to equivalent $T_{PA}$ formula:

$$(1 + 1) \cdot x = y$$
Question: Is the following a well-formed formula in $T_{PA}$?

$$x + y = 1 \lor f(x) = 1 + 1$$

No because contains function symbol $f$

What about $\forall x. \exists y. \exists z. x + y = 1 \lor z \cdot x = 1 + 1$? Yes!
Peano Arithmetic Examples

- **Question**: Is the following a well-formed formula in $T_{PA}$?

  \[ x + y = 1 \lor f(x) = 1 + 1 \]

  - No because contains function symbol $f$

- What about $\forall x. \exists y. \exists z. x + y = 1 \lor z \cdot x = 1 + 1$? Yes!

- What about $2x = y$?
Peano Arithmetic Examples

- **Question:** Is the following a well-formed formula in $T_{PA}$?

$$x + y = 1 \lor f(x) = 1 + 1$$

- No because contains function symbol $f$

- What about $\forall x. \exists y. \exists z. x + y = 1 \lor z \cdot x = 1 + 1$? **Yes!**

- What about $2x = y$? **No!**
Peano Arithmetic Examples

- **Question:** Is the following a well-formed formula in $T_{PA}$?

  \[ x + y = 1 \lor f(x) = 1 + 1 \]

- No because contains function symbol $f$

- What about $\forall x. \exists y. \exists z. x + y = 1 \lor z \cdot x = 1 + 1$? Yes!

- What about $2x = y$? No!

- But can be rewritten to equivalent $T_{PA}$ formula:
Peano Arithmetic Examples

▷ **Question:** Is the following a well-formed formula in $T_{PA}$?

\[ x + y = 1 \lor f(x) = 1 + 1 \]

▷ No because contains function symbol $f$

▷ What about $\forall x. \exists y. \exists z. x + y = 1 \lor z \cdot x = 1 + 1$? Yes!

▷ What about $2x = y$? No!

▷ But can be rewritten to equivalent $T_{PA}$ formula:

\[ (1 + 1) \cdot x = y \]
Axioms of Peano Arithmetic

- Signature of $T_{PA}$ is: $\Sigma_{PA} : \{0, 1, +, \cdot, =\}$; but these are just symbols with no prior meaning!
Axioms of Peano Arithmetic

- Signature of $T_{PA}$ is: $\Sigma_{PA} : \{0, 1, +, \cdot, =\}$; but these are just symbols with no prior meaning!

- Without axioms, we can find satisfying interpretation for $1 + 1 = 1$
Axioms of Peano Arithmetic

- Signature of $T_{PA}$ is: $\Sigma_{PA} : \{0, 1, +, \cdot, =\}$; but these are just symbols with no prior meaning!

- Without axioms, we can find satisfying interpretation for $1 + 1 = 1$

- Axioms of $T_{PA}$ will give the intended meaning of these symbols
Axioms of Peano Arithmetic

- Signature of $T_{PA}$ is: $\Sigma_{PA} : \{0, 1, +, \cdot, =\}$; but these are just symbols with no prior meaning!

- Without axioms, we can find satisfying interpretation for $1 + 1 = 1$

- Axioms of $T_{PA}$ will give the intended meaning of these symbols

- Axioms introduced by 19th century Italian mathematician Giuseppe Peano
Axioms of Peano Arithmetic

- Signature of $T_{PA}$ is: $\Sigma_{PA} : \{0, 1, +, \cdot, =\}$; but these are just symbols with no prior meaning!

- Without axioms, we can find satisfying interpretation for $1 + 1 = 1$

- Axioms of $T_{PA}$ will give the intended meaning of these symbols

- Axioms introduced by 19th century Italian mathematician Giuseppe Peano

- Unchanged since then, used to investigate consistency and completeness of number theory
The Axioms

- Includes equality axioms, reflexivity, symmetry, and transitivity
The Axioms

- Includes equality axioms, reflexivity, symmetry, and transitivity

- In addition, axioms to give meaning to remaining symbols:
  1. \( \forall x. \neg (x + 1 = 0) \): 0 minimal element of \( \mathbb{N} \) (zero)
  2. \( \forall x. x + 0 = x \): 0 identity for addition (plus zero)
  3. \( \forall x. x \cdot 0 = 0 \) (times zero)
  4. \( \forall x, y. x + 1 = y + 1 \rightarrow x = y \) (successor)
  5. \( \forall x, y. x + (y + 1) = (x + y) + 1 \) (plus successor)
  6. \( \forall x, y. x \cdot (y + 1) = x \cdot y + x \) (times successor)
The Axioms

- Includes equality axioms, reflexivity, symmetry, and transitivity

- In addition, axioms to give meaning to remaining symbols:

  1. $\forall x. \neg (x + 1 = 0)$: 0 minimal element of $\mathbb{N}$ (zero)
The Axioms

- Includes equality axioms, reflexivity, symmetry, and transitivity

- In addition, axioms to give meaning to remaining symbols:
  1. \( \forall x. \neg(x + 1 = 0) \): 0 minimal element of \( \mathbb{N} \)  
   (zero)
  2. \( \forall x. x + 0 = x \): 0 identity for addition  
   (plus zero)
The Axioms

▶ Includes equality axioms, reflexivity, symmetry, and transitivity

▶ In addition, axioms to give meaning to remaining symbols:

1. $\forall x. \neg (x + 1 = 0)$: 0 minimal element of $\mathbb{N}$ (zero)

2. $\forall x. x + 0 = x$: 0 identity for addition (plus zero)

3. $\forall x. x \cdot 0 = 0$ (times zero)
The Axioms

- Includes equality axioms, reflexivity, symmetry, and transitivity

- In addition, axioms to give meaning to remaining symbols:
  1. \( \forall x. \neg(x + 1 = 0) \): 0 minimal element of \( \mathbb{N} \) (zero)
  2. \( \forall x. x + 0 = x \): 0 identity for addition (plus zero)
  3. \( \forall x. x \cdot 0 = 0 \) (times zero)
  4. \( \forall x, y. x + 1 = y + 1 \rightarrow x = y \) (successor)
The Axioms

- Includes equality axioms, reflexivity, symmetry, and transitivity

- In addition, axioms to give meaning to remaining symbols:

  1. \( \forall x. (x + 1 \neq 0) \): 0 minimal element of \( \mathbb{N} \) (zero)

  2. \( \forall x. x + 0 = x \): 0 identity for addition (plus zero)

  3. \( \forall x. x \cdot 0 = 0 \) (times zero)

  4. \( \forall x, y. x + 1 = y + 1 \rightarrow x = y \) (successor)

  5. \( \forall x, y. x + (y + 1) = (x + y) + 1 \) (plus successor)
The Axioms

- Includes equality axioms, reflexivity, symmetry, and transitivity

- In addition, axioms to give meaning to remaining symbols:

1. $\forall x. \neg(x + 1 = 0)$: $0$ minimal element of $\mathbb{N}$ (zero)

2. $\forall x. x + 0 = x$: $0$ identity for addition (plus zero)

3. $\forall x. x \cdot 0 = 0$ (times zero)

4. $\forall x, y. x + 1 = y + 1 \rightarrow x = y$ (successor)

5. $\forall x, y. x + (y + 1) = (x + y) + 1$ (plus successor)

6. $\forall x, y. x \cdot (y + 1) = x \cdot y + x$ (times successor)
One last axiom schema for induction:

\[(F[0] \land (\forall x. F[x] \rightarrow F[x + 1])) \rightarrow \forall x. F[x]\]
Last Axiom

- One last axiom schema for induction:

\[ (F[0] \land (\forall x. F[x] \rightarrow F[x + 1])) \rightarrow \forall x. F[x] \]

- Axiom schema because \( F \) stands for any \( T_{PA} \) formula
One last axiom schema for induction:

\[(F[0] \land (\forall x. F[x] \rightarrow F[x + 1])) \rightarrow \forall x. F[x]\]

- Axiom schema because \(F\) stands for any \(T_{PA}\) formula
- States that any valid interpretation must obey induction:
Last Axiom

- One last axiom schema for induction:

\[
(F[0] \land (\forall x. F[x] \rightarrow F[x + 1])) \rightarrow \forall x. F[x]
\]

- Axiom schema because \( F \) stands for any \( T_{PA} \) formula

- States that any valid interpretation must obey induction:

- If an interpretation satisfies \( F[0] \) and \( \forall x. F[x] \rightarrow F[x + 1] \), then must also satisfy \( \forall x. F[x] \)
Inequalities and Peano Arithmetic

- The theory of Peano arithmetic doesn’t have inequality symbols $<, \leq, <, \geq$
Inequalities and Peano Arithmetic

- The theory of Peano arithmetic doesn’t have inequality symbols $<, \leq, <, \geq$

- But all of these are expressible in $T_{PA}$
Inequalities and Peano Arithmetic

- The theory of Peano arithmetic doesn’t have inequality symbols $<, \leq, <, \geq$

- But all of these are expressible in $T_{PA}$

- **Example:** How can we express $x \cdot y \geq z$ in $T_{PA}$?
Inequalities and Peano Arithmetic

- The theory of Peano arithmetic doesn’t have inequality symbols $<, \leq, <, \geq$

- But all of these are expressible in $T_{PA}$

- **Example:** How can we express $x \cdot y \geq z$ in $T_{PA}$?

  $\exists w. x \cdot y = z + w$
Inequalities and Peano Arithmetic

- The theory of Peano arithmetic doesn’t have inequality symbols $<, \leq, <, \geq$

- But all of these are expressible in $T_{PA}$

- **Example:** How can we express $x \cdot y \geq z$ in $T_{PA}$?

  $$\exists w. x \cdot y = z + w$$

- **Example:** How can we express $x \cdot y < z$ in $T_{PA}$?
Inequalities and Peano Arithmetic

- The theory of Peano arithmetic doesn’t have inequality symbols $<, \leq, <, \geq$.
- But all of these are expressible in $T_{PA}$.

**Example:** How can we express $x \cdot y \geq z$ in $T_{PA}$?

$$\exists w. \ x \cdot y = z + w$$

**Example:** How can we express $x \cdot y < z$ in $T_{PA}$?

$$\exists w. \ w \neq 0 \land x \cdot y + w = z$$
Decidability and Completeness Results for Peano Arithmetic

- Validity in full $T_{PA}$ is undecidable. (Gödel)
Decidability and Completeness Results for Peano Arithmetic

- Validity in full $T_{PA}$ is undecidable. (Gödel)

- Validity in even the quantifier-free fragment of $T_{PA}$ is undecidable. (Matiyasevitch, 1970)
Decidability and Completeness Results for Peano Arithmetic

- Validity in full $T_{PA}$ is undecidable. (Gödel)

- Validity in even the quantifier-free fragment of $T_{PA}$ is undecidable. (Matiyasevitch, 1970)

- $T_{PA}$ is also incomplete. (Gödel)
Decidability and Completeness Results for Peano Arithmetic

- Validity in full $T_{PA}$ is undecidable. (Gödel)

- Validity in even the quantifier-free fragment of $T_{PA}$ is undecidable. (Matiyasevitch, 1970)

- $T_{PA}$ is also incomplete. (Gödel)

- Implication of this: There are valid propositions of number theory that are not valid according to $T_{PA}$
Decidability and Completeness Results for Peano Arithmetic

- Validity in full $T_{PA}$ is undecidable. (Gödel)

- Validity in even the quantifier-free fragment of $T_{PA}$ is undecidable. (Matiyasevitch, 1970)

- $T_{PA}$ is also incomplete. (Gödel)

- Implication of this: There are valid propositions of number theory that are not valid according to $T_{PA}$

- To get decidability and completeness, we need to drop multiplication!
The theory of Presburger arithmetic $T_N$ has signature:

$$\Sigma_N : \{0, 1, +, =\}$$
Presburger Arithmetic

- The theory of Presburger arithmetic $T_N$ has signature:

  $$\Sigma_N : \{0, 1, +, =\}$$

- Axioms define meaning of symbols:
The theory of Presburger arithmetic $T_N$ has signature:

$$\Sigma_N : \{0, 1, +, =\}$$

Axioms define meaning of symbols:

1. $\forall x. \neg(x + 1 = 0)$ (zero)
2. $\forall x. x + 0 = x$ (plus zero)
3. $\forall x, y. x + 1 = y + 1 \rightarrow x = y$ (successor)
4. $\forall x, y. x + (y + 1) = (x + y) + 1$ (plus successor)
5. $F[0] \land (\forall x. F[x] \rightarrow F[x + 1]) \rightarrow \forall x. F[x]$ (induction)
Decidability and Completeness Results for Presburger Arithmetic

- Validity in quantifier-free fragment of Presburger arithmetic is decidable (coNP-complete).

- Presburger arithmetic is also complete: For any sentence $F$, $\mathcal{T_N} |= F$ or $\mathcal{T_N} |= \neg F$.

- Admits quantifier elimination: For any formula $F$ in $\mathcal{T_N}$, there exists an equivalent quantifier-free formula $F'$. 
Decidability and Completeness Results for Presburger Arithmetic

- Validity in quantifier-free fragment of Presburger arithmetic is decidable (coNP-complete).

- Validity in full Presburger arithmetic is also decidable (Presburger, 1929)
Decidability and Completeness Results for Presburger Arithmetic

- Validity in quantifier-free fragment of Presburger arithmetic is decidable (coNP-complete).
- Validity in full Presburger arithmetic is also decidable (Presburger, 1929)
- But super exponential complexity: $O(2^{2^n})$
Decidability and Completeness Results for Presburger Arithmetic

- Validity in quantifier-free fragment of Presburger arithmetic is decidable (coNP-complete).

- Validity in full Presburger arithmetic is also decidable (Presburger, 1929)

- But super exponential complexity: $O(2^{2^n})$

- Presburger arithmetic is also complete: For any sentence $F$, $T_N \models F$ or $T_N \models \neg F$
Decidability and Completeness Results for Presburger Arithmetic

- Validity in quantifier-free fragment of Presburger arithmetic is decidable (coNP-complete).

- Validity in full Presburger arithmetic is also decidable (Presburger, 1929)

- But super exponential complexity: $O(2^{2^n})$

- Presburger arithmetic is also complete: For any sentence $F$, $T_N \models F$ or $T_N \models \neg F$

- Admits quantifier elimination: For any formula $F$ in $T_N$, there exists an equivalent quantifier-free formula $F'$. 
Theory of Integers $T_\mathbb{Z}$

- Signature:

\[ \Sigma_\mathbb{Z} : \{ \ldots, -2, -1, 0, 1, 2, \ldots, -3, -2, 2, 3, \ldots, +, -, =, > \} \]
Theory of Integers $T_{\mathbb{Z}}$

- **Signature:**
  \[ \Sigma_{\mathbb{Z}} : \{ \ldots, -2, -1, 0, 1, 2, \ldots, -3 \cdot, -2 \cdot, 2 \cdot, 3 \cdot, \ldots, +, -, =, > \} \]

- Also referred to as the theory of **linear arithmetic over integers**
Theory of Integers $T_{\mathbb{Z}}$

- **Signature:**

$$\Sigma_{\mathbb{Z}} \colon \{ \ldots, -2, -1, 0, 1, 2, \ldots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \ldots, +, -, =, > \}$$

- Also referred to as the theory of **linear arithmetic over integers**

- Equivalent in expressiveness to Presburger arithmetic:

Since reducible to $T_{\mathbb{N}}$, we won’t axiomatize it

Decidable, admits quantifier elimination

Quantifier-free fragment NP-complete, full theory:
Theory of Integers $T_{\mathbb{Z}}$

- Signature:

  $$\Sigma_{\mathbb{Z}} : \{ \ldots, -2, -1, 0, 1, 2, \ldots, -3, -2, 2, 3, \ldots, +, -, =, > \}$$

- Also referred to as the theory of linear arithmetic over integers

- Equivalent in expressiveness to Presburger arithmetic:
  1. For every $T_{\mathbb{Z}}$ formula, there exists equisatisfiable $T_{\mathbb{N}}$ formula
Theory of Integers \( T_{\mathbb{Z}} \)

- Signature:

  \[ \Sigma_{\mathbb{Z}} : \{ \ldots, -2, -1, 0, 1, 2, \ldots, -3n, -2n, 2n, 3n, \ldots, +, -, =, > \} \]

- Also referred to as the theory of \textit{linear arithmetic over integers}

- Equivalent in expressiveness to Presburger arithmetic:
  1. For every \( T_{\mathbb{Z}} \) formula, there exists equisatisfiable \( T_{\mathbb{N}} \) formula
  2. For every \( T_{\mathbb{N}} \) formula, there exists equisatisfiable \( T_{\mathbb{Z}} \) formula
Theory of Integers $T_\mathbb{Z}$

- Signature:

  \[ \Sigma_\mathbb{Z} : \{ \ldots, -2, -1, 0, 1, 2, \ldots, -3 \cdot, -2 \cdot, 2 \cdot, 3 \cdot, \ldots, +, -, =, > \} \]

- Also referred to as the theory of linear arithmetic over integers

- Equivalent in expressiveness to Presburger arithmetic:
  1. For every $T_\mathbb{Z}$ formula, there exists equisatisfiable $T_\mathbb{N}$ formula
  2. For every $T_\mathbb{N}$ formula, there exists equisatisfiable $T_\mathbb{Z}$ formula

- Since reducible to $T_\mathbb{N}$, we won’t axiomatize it
Theory of Integers $T_{\mathbb{Z}}$

- Signature:
  \[ \Sigma_{\mathbb{Z}} : \{ \ldots, -2, -1, 0, 1, 2, \ldots, -3, -2, 2, 3, \ldots, +, -, =, > \} \]

- Also referred to as the theory of linear arithmetic over integers

- Equivalent in expressiveness to Presburger arithmetic:
  1. For every $T_{\mathbb{Z}}$ formula, there exists equisatisfiable $T_{\mathbb{N}}$ formula
  2. For every $T_{\mathbb{N}}$ formula, there exists equisatisfiable $T_{\mathbb{Z}}$ formula

- Since reducible to $T_{\mathbb{N}}$, we won’t axiomatize it

- Decidable, admits quantifier elimination
Theory of Integers $T\mathbb{Z}$

- **Signature:**
  \[
  \Sigma_{\mathbb{Z}} : \{ \ldots, -2, -1, 0, 1, 2, \ldots, -3, -2, 2, 3, \ldots, +, -, =, > \}
  \]

- Also referred to as the theory of **linear arithmetic over integers**

- Equivalent in expressiveness to Presburger arithmetic:
  1. For every $T_{\mathbb{Z}}$ formula, there exists equisatisfiable $T_{\mathbb{N}}$ formula
  2. For every $T_{\mathbb{N}}$ formula, there exists equisatisfiable $T_{\mathbb{Z}}$ formula

- Since reducible to $T_{\mathbb{N}}$, we won’t axiomatize it

- Decidable, admits quantifier elimination

- Quantifier-free fragment NP-complete, full theory: $O(2^{2^{2^{2^{2^n}}}})$
Theory of Rationals

- So far, looked at theories involving arithmetic over integers
Theory of Rationals

- So far, looked at theories involving arithmetic over integers

- Next: the theory of rationals $T_{\mathbb{Q}}$, which is much more efficiently decidable
Theory of Rationals

- So far, looked at theories involving arithmetic over integers
- **Next:** the theory of rationals $T_\mathbb{Q}$, which is much more efficiently decidable
- Defined by signature:

$$\Sigma_\mathbb{Q} : \{0, 1, +, -, =, \geq\}$$
Theory of Rationals

- So far, looked at theories involving arithmetic over integers

- **Next:** the theory of rationals $T_\mathbb{Q}$, which is much more efficiently decidable

- Defined by signature:

  \[ \Sigma_\mathbb{Q} : \{ 0, 1, +, -, =, \geq \} \]

- Signature does not allow strict inequality, but easy to express:

  \[ \forall x, y. \exists z. x + y > z \]
Theory of Rationals

- So far, looked at theories involving arithmetic over integers

- Next: the theory of rationals $T_{\mathbb{Q}}$, which is much more efficiently decidable

- Defined by signature:

$$
\Sigma_{\mathbb{Q}} : \{0, 1, +, -, =, \geq\}
$$

- Signature does not allow strict inequality, but easy to express:

$$
\forall x, y. \exists z. x + y > z \Rightarrow \forall x, y. \exists z. \neg(x + y = z) \land x + y \geq z
$$
Distinction between Theory of Rationals and Presburger Arithmetic

- $T_Q$ has too many axioms, so we won’t discuss them
Distinction between Theory of Rationals and Presburger Arithmetic

- $T_Q$ has too many axioms, so we won’t discuss them

- Distinction between $T_Z$ and $T_Q$: Rational numbers do not satisfy $T_Z$ axioms, but they satisfy $T_Q$ axioms
Distinction between Theory of Rationals and Presburger Arithmetic

- $T_Q$ has too many axioms, so we won’t discuss them

- Distinction between $T_Z$ and $T_Q$: Rational numbers do not satisfy $T_Z$ axioms, but they satisfy $T_Q$ axioms

- Example: $\exists x. (1 + 1)x = 1 + 1 + 1$ Is this formula valid in $T_Q$?
Distinction between Theory of Rationals and Presburger Arithmetic

- $T_Q$ has too many axioms, so we won’t discuss them

- Distinction between $T_Z$ and $T_Q$: Rational numbers do not satisfy $T_Z$ axioms, but they satisfy $T_Q$ axioms

- Example: $\exists x. (1 + 1)x = 1 + 1 + 1$ Is this formula valid in $T_Q$? Yes
Distinction between Theory of Rationals and Presburger Arithmetic

- $T_Q$ has too many axioms, so we won’t discuss them

- Distinction between $T_Z$ and $T_Q$: Rational numbers do not satisfy $T_Z$ axioms, but they satisfy $T_Q$ axioms

- Example: $\exists x. (1 + 1)x = 1 + 1 + 1$ Is this formula valid in $T_Q$? Yes

- Is it valid in $T_Z$?
Distinction between Theory of Rationals and Presburger Arithmetic

- $T_Q$ has too many axioms, so we won’t discuss them

- Distinction between $T_Z$ and $T_Q$: Rational numbers do not satisfy $T_Z$ axioms, but they satisfy $T_Q$ axioms

- Example: $\exists x. (1 + 1)x = 1 + 1 + 1$ Is this formula valid in $T_Q$? Yes

- Is it valid in $T_Z$? No
Distinction between Theory of Rationals and Presburger Arithmetic

- $T_{Q}$ has too many axioms, so we won’t discuss them

- Distinction between $T_{Z}$ and $T_{Q}$: Rational numbers do not satisfy $T_{Z}$ axioms, but they satisfy $T_{Q}$ axioms

- Example: $\exists x. (1 + 1)x = 1 + 1 + 1$ Is this formula valid in $T_{Q}$? Yes

- Is it valid in $T_{Z}$? No

- In general, every formula valid in $T_{Z}$ is valid in $T_{Q}$, but not vice versa
Decidability and Complexity Results for $T_Q$

- Full theory of rationals is **decidable**
Decidability and Complexity Results for $T_Q$

- Full theory of rationals is **decidable**

- High-time complexity: $O(2^{2kn})$ ($k$: some positive integer)
Decidability and Complexity Results for $T_\mathbb{Q}$

- Full theory of rationals is decidable

- High-time complexity: $O(2^{2^{kn}})$ ($k$: some positive integer)

- Conjunctive quantifier-free fragment efficiently decidable (polynomial time)
Decidability and Complexity Results for $T_{\mathbb{Q}}$

- Full theory of rationals is decidable
- High-time complexity: $O(2^{2kn})$ ($k$ some positive integer)
- Conjunctive quantifier-free fragment efficiently decidable (polynomial time)
- Next week, will look at technique for deciding satisfiability of qff $T_{\mathbb{Q}}$ formula (Simplex)
Theories about Data Structures

- So far, we only considered first-order theories involving numbers and arithmetic
Theories about Data Structures

- So far, we only considered first-order theories involving numbers and arithmetic.

- There are also theories that formalize data structures used in programming: e.g., arrays, lists, pointers, bitvectors etc.
Theories about Data Structures

- So far, we only considered first-order theories involving numbers and arithmetic

- There are also theories that formalize data structures used in programming: e.g., arrays, lists, pointers, bitvectors etc.

- We’ll look at one example: theory of arrays
Theories about Data Structures

- So far, we only considered first-order theories involving numbers and arithmetic.

- There are also theories that formalize data structures used in programming: e.g., arrays, lists, pointers, bitvectors etc.

- We’ll look at one example: theory of arrays.

- Sometimes used in software verification.
Theory of Arrays

Signature

\[ \Sigma: \{[·], ⟨· ⪯ ·⟩, =\} \]

where

- \( a[i] \) binary function –
  read array \( a \) at index \( i \) ("read\((a,i)\)"")

- \( a ⟨i ⪯ v⟩ \) ternary function –
  write value \( v \) to index \( i \) of array \( a \) ("write\((a,i,e)\)"")

- \( a⟨i ⪯ v⟩ \) represents the resulting array after writing value \( v \) at index \( i \)
Example Formulas in Theory of Arrays

- Example: \((a \langle 2 < 5 \rangle)[2] = 5\)

  - Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 5”
Example Formulas in Theory of Arrays

- **Example:** \((a \langle 2 \triangleleft 5 \rangle)[2] = 5\)

- Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 5”

- **Example:** \((a \langle 2 \triangleleft 5 \rangle)[2] = 3\)

- Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 3”

According to the usual semantics of array read and write, is the first formula valid/satisfiable/unsat? **Valid**

What about second formula? **Unsat**
Example Formulas in Theory of Arrays

► Example: \((a\langle 2 \leftarrow 5\rangle)[2] = 5\)

► Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 5”

► Example: \((a\langle 2 \leftarrow 5\rangle)[2] = 3\)

► Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 3”

► According to the usual semantics of array read and write, is the first formula valid/satisfiable/unsat?
Example Formulas in Theory of Arrays

Example: \((a\langle 2 \triangleleft 5 \rangle)[2] = 5\)

Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 5”

Example: \((a\langle 2 \triangleleft 5 \rangle)[2] = 3\)

Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 3”

According to the usual semantics of array read and write, is the first formula valid/satisfiable/unsat? Valid
Example Formulas in Theory of Arrays

- **Example:** \((a\langle 2 \triangleleft 5\rangle)[2] = 5\)

  Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 5”

- **Example:** \((a\langle 2 \triangleleft 5\rangle)[2] = 3\)

  Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 3”

- According to the usual semantics of array read and write, is the first formula valid/satisfiable/unsat? **Valid**

- What about second formula?
Example Formulas in Theory of Arrays

- **Example:** \((a \langle 2 \triangleright 5 \rangle)[2] = 5\)

  - Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 5”

- **Example:** \((a \langle 2 \triangleright 5 \rangle)[2] = 3\)

  - Says: “The value stored at position 2 of an array to whose second position we wrote the value 5 is 3”

- According to the usual semantics of array read and write, is the first formula valid/satisfiable/unsat? **Valid**

- What about second formula? **Unsat**
Axioms of $T_A$

- To define "intended semantics of array read and write", we need to provide axioms of $T_A$. 

1. $\forall a, i, j. i = j \rightarrow a[i] = a[j]$ (array congruence)

2. $\forall a, v, i, j. i = j \rightarrow a\langle i\leftarrow v \rangle[j] = v$ (read-over-write 1)

3. $\forall a, v, i, j. i \neq j \rightarrow a\langle i\leftarrow v \rangle[j] = a[j]$ (read-over-write 2)
Axioms of $T_A$

- To define "intended semantics of array read and write", we need to provide axioms of $T_A$.

- Axioms of $T_A$ include reflexivity, symmetry, and transitivity.
Axioms of $T_A$

- To define "intended semantics of array read and write", we need to provide axioms of $T_A$.

- Axioms of $T_A$ include reflexivity, symmetry, and transitivity

- In addition, they include axioms unique to arrays:
Axioms of $T_A$

- To define "intended semantics of array read and write", we need to provide axioms of $T_A$.

- Axioms of $T_A$ include reflexivity, symmetry, and transitivity.

- In addition, they include axioms unique to arrays:
  1. $\forall a, i, j. \ i = j \rightarrow a[i] = a[j]$  
     (array congruence)
Axioms of $T_A$

- To define "intended semantics of array read and write", we need to provide axioms of $T_A$.

- Axioms of $T_A$ include reflexivity, symmetry, and transitivity.

- In addition, they include axioms unique to arrays:
  1. $\forall a, i, j. \ i = j \rightarrow a[i] = a[j]$ (array congruence)
  2. $\forall a, v, i, j. \ i = j \rightarrow a(i \triangleleft v)[j] = v$ (read-over-write 1)
To define "intended semantics of array read and write", we need to provide axioms of $T_A$.

Axioms of $T_A$ include reflexivity, symmetry, and transitivity.

In addition, they include axioms unique to arrays:

1. $\forall a, i, j. \ i = j \rightarrow a[i] = a[j]$ (array congruence)

2. $\forall a, v, i, j. \ i = j \rightarrow a(i \triangleleft v)[j] = v$ (read-over-write 1)

3. $\forall a, v, i, j. \ i \neq j \rightarrow a(i \triangleleft v)[j] = a[j]$ (read-over-write 2)
Example

Is the following $T_A$ formula valid?

$$F : a[i] = e \rightarrow (\forall j. a(i \triangleleft e)[j] = a[j])$$
Example

- Is the following $T_A$ formula valid?

$$F : a[i] = e \rightarrow (\forall j. \ a\langle i \triangleleft e\rangle[j] = a[j])$$

- Yes! For any $j \neq i$, $a\langle i \triangleleft e\rangle[j] = a[j]$ according to read-over-write 2 axiom. For any $j = i$, old value of $j$ was already $e$, so its value didn’t change.
Example

- Is the following $T_A$ formula valid?
  
  \[ F : a[i] = e \rightarrow (\forall j. \ a\langle i \triangleleft e\rangle[j] = a[j]) \]

- Yes! For any $j \neq i$, $a\langle i \triangleleft e\rangle[j] = a[j]$ according to read-over-write 2 axiom. For any $j = i$, old value of $j$ was already $e$, so its value didn’t change.

- Let’s prove its validity using the semantic argument method.
Example

- Is the following $T_A$ formula valid?

$$F : a[i] = e \rightarrow (\forall j. a(i \triangleleft e)[j] = a[j])$$

- Yes! For any $j \neq i$, $a(i \triangleleft e)[j] = a[j]$ according to read-over-write 2 axiom.
  For any $j = i$, old value of $j$ was already $e$, so its value didn’t change

- Let’s prove its validity using the semantic argument method

- Assume there exists a model $M$ and variable assignment $\sigma$ that does not satisfy $F$ and derive contradiction.
Example cont.

1. \( M, \sigma \not\models a[i] = e \rightarrow (\forall j. a(i < e)[j] = a[j]) \) assumption
Example cont.

1. \( M, \sigma \not\models a[i] = e \rightarrow (\forall j. a(i < e)[j] = a[j]) \) \hspace{1cm} \text{assumption}

2. \( M, \sigma \models a[i] = e \) \hspace{1cm} 1, \rightarrow
Example cont.

1. \( M, \sigma \not\models a[i] = e \rightarrow (\forall j. a\langle i < e\rangle[j] = a[j]) \) assumption

2. \( M, \sigma \models a[i] = e \)

3. \( M, \sigma \not\models \forall j. a\langle i < e\rangle[j] = a[j] \)

4. \( M, \sigma[j \mapsto k] \not\models a\langle i < e\rangle[j] = a[j] \)

5. \( M, \sigma[j \mapsto k] \models i = j \)

6. \( M, \sigma[j \mapsto k] \not\models a\langle i < e\rangle[j] = a[j] \)

7. \( M, \sigma[j \mapsto k] \models a[i] = a[j] \)

8. \( M, \sigma[j \mapsto k] \models a\langle i < e\rangle[j] = e \)

9. \( M, \sigma[j \mapsto k] \models a\langle i < e\rangle[j] = a[i] \)

10. \( M, \sigma[j \mapsto k] \models a\langle i < e\rangle[j] = a[j] \) trans
Example cont.

1. \( M, \sigma \not\models a[i] = e \rightarrow (\forall j. a\langle i \triangleleft e\rangle[j] = a[j]) \) \hspace{1cm} \text{assumption}

2. \( M, \sigma \models a[i] = e \) \hspace{1cm} 1, \rightarrow

3. \( M, \sigma \not\models \forall j. a\langle i \triangleleft e\rangle[j] = a[j] \) \hspace{1cm} 1, \rightarrow

4. \( M, \sigma[j \mapsto k] \not\models a\langle i \triangleleft e\rangle[j] = a[j] \) \hspace{1cm} 3, \forall
Example cont.

1. \( M, \sigma \not \models a[i] = e \rightarrow (\forall j. a\langle i \triangleleft e \rangle[j] = a[j]) \)  
   assumption

2. \( M, \sigma \models a[i] = e \)

3. \( M, \sigma \not \models \forall j. a\langle i \triangleleft e \rangle[j] = a[j] \)

4. \( M, {\sigma}[j \mapsto k] \not \models a\langle i \triangleleft e \rangle[j] = a[j] \)

5. \( M, {\sigma}[j \mapsto k] \models a\langle i \triangleleft e \rangle[j] \neq a[j] \)

1, \( \rightarrow \)

3, \( \forall \)

4, \( \neg \)
Example cont.

1. \( M, \sigma \not\models a[i] = e \to (\forall j. a\langle i < e\rangle[j] = a[j]) \)  
   \text{assumption}

2. \( M, \sigma \models a[i] = e \)  
   1, \( \rightarrow \)

3. \( M, \sigma \not\models \forall j. a\langle i < e\rangle[j] = a[j] \)  
   1, \( \rightarrow \)

4. \( M, \sigma[j \mapsto k] \not\models a\langle i < e\rangle[j] = a[j] \)  
   3, \( \forall \)

5. \( M, \sigma[j \mapsto k] \models a\langle i < e\rangle[j] \neq a[j] \)  
   4, \( \neg \)

6. \( M, \sigma[j \mapsto k] \models i = j \)  
   5, r-o-w 2
Example cont.

1. \[ M, \sigma \not\equiv a[i] = e \rightarrow (\forall j. a\langle i < e\rangle[j] = a[j]) \] assumption
2. \[ M, \sigma \models a[i] = e \] 1, \(\rightarrow\)
3. \[ M, \sigma \not\equiv \forall j. a\langle i < e\rangle[j] = a[j] \] 1, \(\rightarrow\)
4. \[ M, \sigma[j \mapsto k] \not\equiv a\langle i < e\rangle[j] = a[j] \] 3, \(\forall\)
5. \[ M, \sigma[j \mapsto k] \models a\langle i < e\rangle[j] \neq a[j] \] 4, \(\neg\)
6. \[ M, \sigma[j \mapsto k] \models i = j \] 5, r-o-w 2
7. \[ M, \sigma[j \mapsto k] \models a[i] = a[j] \] 6, cong
Example cont.

1. \( M, \sigma \not\models a[i] = e \rightarrow (\forall j. a(i < e)[j] = a[j]) \) \hspace{1cm} \text{assumption}

2. \( M, \sigma \models a[i] = e \)

3. \( M, \sigma \not\models \forall j. a(i < e)[j] = a[j] \)

4. \( M, \sigma[j \mapsto k] \not\models a(i < e)[j] = a[j] \)

5. \( M, \sigma[j \mapsto k] \models a(i < e)[j] \neq a[j] \)

6. \( M, \sigma[j \mapsto k] \models i = j \)

7. \( M, \sigma[j \mapsto k] \models a[i] = a[j] \)

8. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = e \)

9. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

10. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

11. \( M, \sigma[j \mapsto k] \models \bot \)

12. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

13. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

14. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

15. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

16. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

17. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

18. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

19. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

20. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

21. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

22. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

23. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

24. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

25. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

26. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

27. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

28. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

29. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

30. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

31. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

32. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

33. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

34. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

35. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

36. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

37. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

38. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

39. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

40. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

41. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

42. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

43. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

44. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

45. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)

46. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)
Example cont.

<table>
<thead>
<tr>
<th>Step</th>
<th>Assumption/Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>( M, \sigma \not\models a[i] = e \rightarrow (\forall j. a(i \triangleleft e)[j] = a[j]) )</td>
</tr>
<tr>
<td>2.</td>
<td>( M, \sigma \models a[i] = e )</td>
</tr>
<tr>
<td>3.</td>
<td>( M, \sigma \not\models \forall j. a(i \triangleleft e)[j] = a[j] )</td>
</tr>
<tr>
<td>4.</td>
<td>( M, \sigma[j \mapsto k] \not\models a(i \triangleleft e)[j] = a[j] )</td>
</tr>
<tr>
<td>5.</td>
<td>( M, \sigma[j \mapsto k] \models a[i] = a[j] )</td>
</tr>
<tr>
<td>6.</td>
<td>( M, \sigma[j \mapsto k] \models i = j )</td>
</tr>
<tr>
<td>7.</td>
<td>( M, \sigma[j \mapsto k] \models a[i] = a[j] )</td>
</tr>
<tr>
<td>8.</td>
<td>( M, \sigma[j \mapsto k] \models a(i \triangleleft e)[j] = e )</td>
</tr>
<tr>
<td>9.</td>
<td>( M, \sigma[j \mapsto k] \models a(i \triangleleft e)[j] = a[i] )</td>
</tr>
</tbody>
</table>
Example cont.

1. \( M, \sigma \models a[i] = e \rightarrow (\forall j. a(i < e)[j] = a[j]) \) assumption
2. \( M, \sigma \models a[i] = e \)
3. \( M, \sigma \models \forall j. a(i < e)[j] = a[j] \)
4. \( M, \sigma[j \mapsto k] \models a[i] = a[j] \)
5. \( M, \sigma[j \mapsto k] \models a(i < e)[j] \neq a[j] \)
6. \( M, \sigma[j \mapsto k] \models i = j \)
7. \( M, \sigma[j \mapsto k] \models a[i] = a[j] \)
8. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = e \)
9. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[i] \)
10. \( M, \sigma[j \mapsto k] \models a(i < e)[j] = a[j] \)
Example cont.

1. \( M, \sigma \not\models a[i] = e \rightarrow (\forall j. a\langle i \triangleleft e\rangle[j] = a[j]) \) assumption
2. \( M, \sigma \models a[i] = e \) 1, →
3. \( M, \sigma \not\models \forall j. a\langle i \triangleleft e\rangle[j] = a[j] \) 1, →
4. \( M, \sigma[j \mapsto k] \not\models a[i] = e \) 3, ∀
5. \( M, \sigma[j \mapsto k] \models a[i] = a[j] \) 4, ¬
6. \( M, \sigma[j \mapsto k] \models i = j \) 5, r-o-w 2
7. \( M, \sigma[j \mapsto k] \models a[i] = a[j] \) 6, cong
8. \( M, \sigma[j \mapsto k] \models a\langle i \triangleleft e\rangle[j] = e \) 6, r-o-w 1
9. \( M, \sigma[j \mapsto k] \models a\langle i \triangleleft e\rangle[j] = a[i] \) 2,8,trans
10. \( M, \sigma[j \mapsto k] \models a\langle i \triangleleft e\rangle[j] = a[j] \) 9,7,trans
11. \( M, \sigma[j \mapsto k] \models \bot \) 5,10
Decidability Results for $T_A$

- The full theory of arrays is not decidable.
Decidability Results for $T_A$

- The full theory of arrays is not decidable.
- The quantifier-free fragment of $T_A$ is decidable.
Decidability Results for $T_A$

- The full theory of arrays is not decidable.
- The quantifier-free fragment of $T_A$ is decidable.
- Unfortunately, the quantifier-free fragment is not sufficiently expressive in many contexts.

Example: array property fragment (disallows nested arrays, restrictions on where quantified variables can occur)
Decidability Results for $T_A$

- The full theory of arrays is not decidable.

- The quantifier-free fragment of $T_A$ is decidable.

- Unfortunately, the quantifier-free fragment is not sufficiently expressive in many contexts.

- Thus, people have studied other richer fragments that are still decidable.
Decidability Results for $T_A$

- The full theory of arrays is not decidable.
- The quantifier-free fragment of $T_A$ is decidable.
- Unfortunately, the quantifier-free fragment is not sufficiently expressive in many contexts.
- Thus, people have studied other richer fragments that are still decidable.
- **Example:** array property fragment (disallows nested arrays, restrictions on where quantified variables can occur)
So far, we only talked about individual first-order theories.
Combination of Theories

- So far, we only talked about individual first-order theories.
- Examples: $T_\equiv$, $T_{PA}$, $T_Z$, $T_A$, ...
Combination of Theories

- So far, we only talked about individual first-order theories.

- Examples: $T_e$, $T_{PA}$, $T_Z$, $T_A$, ...

- But in many applications, we need combined reasoning about several of these theories.
So far, we only talked about individual first-order theories.

Examples: $T_\approx$, $T_{PA}$, $T_Z$, $T_A$, …

But in many applications, we need combined reasoning about several of these theories.

Example: The formula $f(x) + 3 = y$ isn’t a well-formed formula in any individual theory, but belongs to combined theory $T_Z \cup T_\approx$
Combined Theories

- Given two theories $T_1$ and $T_2$ that have the $=$ predicate, we define a combined theory $T_1 \cup T_2$.
Combined Theories

- Given two theories $T_1$ and $T_2$ that have the $=$ predicate, we define a combined theory $T_1 \cup T_2$

- Signature of $T_1 \cup T_2$: $\Sigma_1 \cup \Sigma_2$
Combined Theories

- Given two theories $T_1$ and $T_2$ that have the $=$ predicate, we define a combined theory $T_1 \cup T_2$

- Signature of $T_1 \cup T_2$: $\Sigma_1 \cup \Sigma_2$

- Axioms of $T_1 \cup T_2$: $A_1 \cup A_2$
Given two theories $T_1$ and $T_2$ that have the $=$ predicate, we define a combined theory $T_1 \cup T_2$.

- **Signature of** $T_1 \cup T_2$: $\Sigma_1 \cup \Sigma_2$

- **Axioms of** $T_1 \cup T_2$: $A_1 \cup A_2$

- **Is this a well-formed $T_1 \cup T_2$ formula?**

$$1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$$
Combined Theories

- Given two theories $T_1$ and $T_2$ that have the $=$ predicate, we define a combined theory $T_1 \cup T_2$

- Signature of $T_1 \cup T_2$: $\Sigma_1 \cup \Sigma_2$

- Axioms of $T_1 \cup T_2$: $A_1 \cup A_2$

- Is this a well-formed $T_\leq \cup T_\mathbb{Z}$ formula? Yes

$$1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$$
Combined Theories

- Given two theories \( T_1 \) and \( T_2 \) that have the = predicate, we define a combined theory \( T_1 \cup T_2 \)

- Signature of \( T_1 \cup T_2 \): \( \Sigma_1 \cup \Sigma_2 \)

- Axioms of \( T_1 \cup T_2 \): \( A_1 \cup A_2 \)

- Is this a well-formed \( T_1 \cup T_2 \) formula? Yes

\[
1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)
\]

- Is this formula satisfiable according to axioms \( A_{\mathbb{Z}} \cup A_{=} \)?
Combined Theories

- Given two theories $T_1$ and $T_2$ that have the $=$ predicate, we define a combined theory $T_1 \cup T_2$

- Signature of $T_1 \cup T_2$: $\Sigma_1 \cup \Sigma_2$

- Axioms of $T_1 \cup T_2$: $A_1 \cup A_2$

- Is this a well-formed $T_= \cup T_\mathbb{Z}$ formula? Yes

$$1 \leq x \land x \leq 2 \land f(x) \neq f(1) \land f(x) \neq f(2)$$

- Is this formula satisfiable according to axioms $A_\mathbb{Z} \cup A_=$? No
Given decision procedures for individual theories $T_1$ and $T_2$, can we decide satisfiability of formulas in $T_1 \cup T_2$?

In the early 80s, Nelson and Oppen showed this is possible.

Specifically, if

1. quantifier-free fragment of $T_1$ is decidable
2. quantifier-free fragment of $T_2$ is decidable
3. and $T_1$ and $T_2$ meet certain technical requirements

then quantifier-free fragment of $T_1 \cup T_2$ is also decidable.

Also, given decision procedures for $T_1$ and $T_2$, Nelson and Oppen’s technique allows deciding satisfiability of $T_1 \cup T_2$. 
Decision Procedures for Combined Theories

- Given decision procedures for individual theories $T_1$ and $T_2$, can we decide satisfiability of formulas in $T_1 \cup T_2$?

- In the early 80s, Nelson and Oppen showed this is possible.

Specifically, if

1. quantifier-free fragment of $T_1$ is decidable
2. quantifier-free fragment of $T_2$ is decidable
3. and $T_1$ and $T_2$ meet certain technical requirements

then quantifier-free fragment of $T_1 \cup T_2$ is also decidable.
Decision Procedures for Combined Theories

- Given decision procedures for individual theories \( T_1 \) and \( T_2 \), can we decide satisfiability of formulas in \( T_1 \cup T_2 \)?

- In the early 80s, Nelson and Oppen showed this is possible

- Specifically, if

- quantifier-free fragment of \( T_1 \) is decidable
- quantifier-free fragment of \( T_2 \) is decidable
- and \( T_1 \) and \( T_2 \) meet certain technical requirements
- then quantifier-free fragment of \( T_1 \cup T_2 \) is also decidable

Also, given decision procedures for \( T_1 \) and \( T_2 \), Nelson and Oppen's technique allows deciding satisfiability of \( T_1 \cup T_2 \).
Decision Procedures for Combined Theories

- Given decision procedures for individual theories $T_1$ and $T_2$, can we decide satisfiability of formulas in $T_1 \cup T_2$?

- In the early 80s, Nelson and Oppen showed this is possible

- Specifically, if
  1. quantifier-free fragment of $T_1$ is decidable

Decision Procedures for Combined Theories

- Given decision procedures for individual theories $T_1$ and $T_2$, can we decide satisfiability of formulas in $T_1 \cup T_2$?

- In the early 80s, Nelson and Oppen showed this is possible

- Specifically, if
  1. quantifier-free fragment of $T_1$ is decidable
  2. quantifier-free fragment of $T_2$ is decidable
Decision Procedures for Combined Theories

- Given decision procedures for individual theories $T_1$ and $T_2$, can we decide satisfiability of formulas in $T_1 \cup T_2$?

- In the early 80s, Nelson and Oppen showed this is possible

- Specifically, if
  1. quantifier-free fragment of $T_1$ is decidable
  2. quantifier-free fragment of $T_2$ is decidable
  3. and $T_1$ and $T_2$ meet certain technical requirements
Given decision procedures for individual theories $T_1$ and $T_2$, can we decide satisfiability of formulas in $T_1 \cup T_2$?

In the early 80s, Nelson and Oppen showed this is possible.

Specifically, if

1. quantifier-free fragment of $T_1$ is decidable
2. quantifier-free fragment of $T_2$ is decidable
3. and $T_1$ and $T_2$ meet certain technical requirements

then quantifier-free fragment of $T_1 \cup T_2$ is also decidable.
Decision Procedures for Combined Theories

- Given decision procedures for individual theories $T_1$ and $T_2$, can we decide satisfiability of formulas in $T_1 \cup T_2$?

- In the early 80s, Nelson and Oppen showed this is possible

- Specifically, if
  1. quantifier-free fragment of $T_1$ is decidable
  2. quantifier-free fragment of $T_2$ is decidable
  3. and $T_1$ and $T_2$ meet certain technical requirements

- then quantifier-free fragment of $T_1 \cup T_2$ is also decidable

- Also, given decision procedures for $T_1$ and $T_2$, Nelson and Oppen’s technique allows deciding satisfiability $T_1 \cup T_2$
Plan for Next Few Lectures

- We’ll talk about decision procedures for some interesting first-order theories

- Next lecture: Quantifier-free theory of equality
- Later: Theory of rationals, Presburger arithmetic

- Initially, we’ll only focus on decision procedures for formulas without disjunctions
- Ok because we can always convert to DNF to deal with disjunctions – just not very efficient!
- Later in the course, we’ll see about how to handle disjunctions much more efficiently
Plan for Next Few Lectures

- We’ll talk about decision procedures for some interesting first order-theories

- Next lecture: Quantifier-free theory of equality
Plan for Next Few Lectures

- We’ll talk about decision procedures for some interesting first order-theories

- **Next lecture:** Quantifier-free theory of equality

- Later: Theory of rationals, Presburger arithmetic
Plan for Next Few Lectures

- We’ll talk about decision procedures for some interesting first order-theories

- **Next lecture:** Quantifier-free theory of equality

- Later: Theory of rationals, Presburger arithmetic

- Initially, we’ll only focus on decision procedures for formulas without disjunctions
Plan for Next Few Lectures

- We’ll talk about decision procedures for some interesting first order-theories

- **Next lecture**: Quantifier-free theory of equality

- Later: Theory of rationals, Presburger arithmetic

- Initially, we’ll only focus on decision procedures for formulas without disjunctions

- Ok because we can always convert to DNF to deal with disjunctions – just not very efficient!
Plan for Next Few Lectures

- We’ll talk about decision procedures for some interesting first order-theories

- **Next lecture:** Quantifier-free theory of equality

- Later: Theory of rationals, Presburger arithmetic

- Initially, we’ll only focus on decision procedures for formulas without disjunctions

- Ok because we can always convert to DNF to deal with disjunctions – just not very efficient!

- Later in the course, we’ll see about how to handle disjunctions much more efficiently