PRESBURGER ARITHMETIC ($T_{\mathbb{N}}$)

THE THEORY OF NATURAL NUMBERS

- Signature, $\Sigma_{\mathbb{N}}$: $0, 1, +, =$
  - $0,1$ are constants
  - $+$ is a binary function
  - $=$ is a binary predicate.
- Axioms:

1. $\forall x.\ \neg(x + 1 = 0)$ (zero)
2. $\forall x, y.\ x + 1 = y + 1 \ \rightarrow\ x = y$ (successor)
3. $F[0]\ \land\ (\forall x.\ F[x] \rightarrow F[x + 1])\ \rightarrow\ \forall x.\ F[x]$ (induction)
4. $\forall x.\ x + 0 = x$ (plus zero)
5. $\forall x, y.\ x + (y + 1) = (x + y) + 1$ (plus successor)

PRESBURGER ARITHMETIC

INTERPRETATION

1. $\forall x.\ \neg(x+1=0)$	(zero)
2. $\forall x, y.\ x+1=y+1 \ \rightarrow\ x=y$	(successor)
3. $F[0] \ \wedge\ (\forall x.\ F[x] \rightarrow F[x+1]) \ \rightarrow\ \forall x.\ F[x]$	(induction)
4. $\forall x.\ x+0=x$	(plus zero)
5. $\forall x, y.\ x+(y+1)=(x+y)+1$	(plus successor)

- The intended $T_{\mathbb{N}}$–interpretation is $\mathbb{N}$, the set of natural numbers
- Does there exist a finite subset of $\mathbb{N}$ which is also a $T_{\mathbb{N}}$–interpretation?
  - Which axiom(s) will be violated by any finite subset?
- Are negative numbers allowed by the axioms?

PRESBURGER ARITHMETIC

EXAMPLES

- Examples of $\Sigma_{\mathbb{N}}$-formulae
  - $\forall x \,.\, \exists y \,.\, x = y + 1$
  - $3x + 5 = 2y$
    - Can be expressed as $(x + x) + (1 + 1 + 1 + 1 + 1) = (y + y)$
  - $\forall x \,.\, \exists y \,.\, x + f(y) = 5$ is not a $\Sigma_{\mathbb{N}}$-formula
- How to express $x < y$ and $x \leq y$?
  - $\exists z \,.\, z \neq 0 \wedge y = x + z$
  - $\exists z \,.\, y = x + z$

PRESBURGER ARITHMETIC

EXPANDING TO THEORY OF INTEGERS

- How to expand the domain to negative numbers?
  - $x + y < 0$
  - Converted to $(x_p - x_n) + (y_p - y_n) < 0$
  - Converted to $x_p + y_p < x_n + y_n$
  - Converted to $\exists z \,.\, z \neq 0 \land x_p + y_p + z = x_n + y_n$

THEORY OF INTEGERS ($T_{\mathbb{Z}}$)

LINEAR INTEGER ARITHMETIC

SIGNATURE:

$$\{\ldots, -2, -1, 0, 1, 2, \ldots\} \cup \{\ldots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \ldots\} \cup \{+, -, =, <, \leq\}$$

- Signature:
  - $\ldots, -2, -1, 0, 1, 2, \ldots$ are constants
  - $\ldots, -3\cdot, -2\cdot, 2\cdot, 3\cdot, \ldots$ are unary functions to represent coefficients of variables
  - $+, -$ are binary functions
  - $=, <, \leq$ are binary predicates.
- Any $T_{\mathbb{Z}}$−formula can be converted to a $T_{\mathbb{N}}$−formula.

PRESBURGER ARITHMETIC

DECIDABILITY

- Validity in quantifier-free fragment of Presgurber Arithmetic is decidable
  - NP-Complete
- Validity in full Presburger Arithmetic is also decidable
  - Super Exponential Complexity : $O(2^{2^n})$
- Conjunctions of quantifier-free linear constraints can be solved efficiently
  - Using Simplex Method or Omega test.
- Presburger Arithmetic is also complete
  - For any closed $T_{\mathbb{N}}-$formula F, either $T_{\mathbb{N}} \vDash F$ or $T_{\mathbb{N}} \vDash \neg F$

THEORY OF EQUALITY ($T_=$)

- One of the simplest first-order theories
  - $\Sigma_=$: All symbols used in FOL and the special symbol $=$
  - Allows uninterpreted functions and predicates, but $=$ is interpreted.
- Axioms of Equality

1. $\forall x.\ x = x$	(reflexivity)
2. $\forall x, y.\ x = y \ \rightarrow \ y = x$	(symmetry)
3. $\forall x, y, z.\ x = y \ \wedge \ y = z \ \rightarrow \ x = z$	(transitivity)

AXIOMS OF EQUALITY

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

$$\forall \overline{x}, \overline{y}. \left(\bigwedge_{i=1}^{n} x_i = y_i \right) \rightarrow f(\overline{x}) = f(\overline{y})$$

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

$$\forall \overline{x}, \overline{y}. \left(\bigwedge_{i=1}^{n} x_i = y_i \right) \rightarrow (p(\overline{x}) \leftrightarrow p(\overline{y}))$$

AXIOMS OF EQUALITY

- Function Congruence and Predicate Congruence are actually Axiom Schemes, which can be instantiated with any function or predicate to get axioms.
  - Similar to the induction axiom scheme in Presburger arithmetic.
- For example, for a unary function g, the function congruence axiom is:
  - $\forall x, y \,.\, x = y \rightarrow g(x) = g(y)$

SEMANTIC ARGUMENT METHOD IN $T_=$

- We can use the semantic argument method to prove validity modulo $T_=$.
- Along with the usual proof rules, axioms of equality can be used to derive facts.
- As usual, we look for a contradiction in all branches.

EXAMPLE

Prove that $F : a = b \wedge b = c \rightarrow g(f(a), b) = g(f(c), a)$ is valid

1.	I	$\not\models$	F	assumption
2.	I	$\models$	$a = b \ \wedge \ b = c$	1, $\rightarrow$
3.	I	$\not\models$	$g(f(a), b) = g(f(c), a)$	1, $\rightarrow$
4.	I	$\models$	$a = b$	2, $\wedge$
5.	I	$\models$	$b = c$	2, $\wedge$
6.	I	$\models$	$a = c$	4, 5, (transitivity)
7.	I	$\models$	$f(a) = f(c)$	6, (function congruence)
8.	I	$\models$	$b = a$	4, (symmetry)
9.	I	$\models$	$g(f(a), b) = g(f(c), a)$	7, 8 (function congruence)
10.	I	$\models$	$\perp$	3, 9

DECIDABILITY OF VALIDITY IN $T_=$

- $T_=$ being an extension of FOL, the validity problem is clearly undecidable.
- However, validaty in the quantifier-free fragment of $T_=$ is decidable, but NP-complete.
- Conjunctions of quantifier-free equality constraints can be solved efficiently.
  - Congruence closure algorithm can be used to decide satisfiability of conjunctions of equality constraints in polynomial time

THEORY OF RATIONALS

- Theory of Rationals ($T_{\mathbb{Q}}$)
  - Also called Linear Real Arithmetic.
  - Same symbols as Presburger arithmetic, but many more axioms.
    - Interpretation is $\mathbb{R}$.
  - Example: $\exists x\,.\; 2x = 3$. Satisfiable in $T_{\mathbb{Q}}$.
    - Is it satisfiable in $T_{\mathbb{Z}}$?
  - Conjunctive quantifier-free fragment is efficiently decidable in polynomial time.

THEORIES ABOUT DATA STRUCTURES

- So far, we have looked at theories of numbers and arithmetic.
- But, we can also formalize behaviour of data structures using theories.
  - Very useful for automated verification

THEORY OF ARRAYS (T_A)

- Signature, $\Sigma_A : \{ \cdot [\cdot], \cdot \langle \cdot \triangleleft \cdot \rangle, = \}$
- $a[i]$ is a binary function
    - Read array a at index i
    - Returns the value read.
- $a\langle i \triangleleft v \rangle$ is a ternary function
    - Write value v at index i in array a
    - Returns the modified array.
- $=$ is a binary predicate

EXAMPLES

- $(a\langle 2 \lhd 5\rangle)[2] = 5$
  - Write the value 5 at index 2 in array a, then from the resulting array, the value at index 2 is 5.
- $(a\langle 2 \lhd 5\rangle)[2] = 3$
  - Write the value 5 at index 2 in array a, then from the resulting array, the value at index 2 is 3.
- According to the usual semantics of arrays, which of the formulae is valid/sat/unsat?

AXIOMS OF T_A

- The axioms of T_A include reflexivity, symmetry and transitivity axioms of $T_=$.
- Array Congruence:
  - $\forall a, i, j \,.\, i = j \rightarrow a[i] = a[j]$
- Read over Write 1:
  - $\forall a, i, j, v \,.\, i = j \rightarrow a\langle i \triangleleft v \rangle[j] = v$
- Read over Write 2:
  - $\forall a, i, j, v \,.\, i \neq j \rightarrow a\langle i \triangleleft v \rangle[j] = a[j]$