# 16 Presburger Arithmetic

Presburger Arithmetic is a simple theory of natural numbers that extends our previous theories of first-order logic with equality. We extend the syntax of first-order logic with equality, add $< \mathbb{N}, 0, S, + >$, but remove all other predicate and function symbols as well as constants. So we only have 0 as constant, the successor function 'S' and addition '+' as function symbols and the equality symbol '=' as predicate symbol.

## 16.1 The axioms

Our axioms are
(1) the rules of first-order logic (e.g. the refinement logic rules)
(2) the axioms $\mathrm{Eq}_1 ... \mathrm{Eq}_3$ of equality (reflexivity, commutativity, transitivity) as well as the equality substitution axiom schemata (mostly for successor and addition).
(3) special axioms of arithmetic

1. $S\,x \neq 0$
2. $S\,x = S\,y \Rightarrow x = y$
3. $x + 0 = x$
4. $x + S\,y = S(x + y)$

**Ind:** $P[0/z] \wedge (\forall x)(P[x/z] \Rightarrow P[S\,x/z]) \Rightarrow (\forall x)(P[x/z])$ *for every formula $P$ with free variable $z$*

The induction axiom can also be expressed as rule scheme

$x : \mathbb{N} \vdash P[x/z]$ `by induction on` $x$ `using` $z.P[z]$
`1.` $\vdash P[0/z]$
`2.` $x : \mathbb{N}$, $P[x/z] \vdash P[S\,x/z]$

**Q: Does this theory have a model?** (Consistency)

In other words, is there an interpretation of $< \mathbb{N}, 0, S, + >$ that satisfies the 5 axioms? Obviously yes, because the *Standard-Interpretation* works out fine. Use the natural numbers as universe, interpret 0 as number zero, $S$ as successor function that increments a number by one, and $+$ as the usual addition. So the axioms make sense.

**Q: Do we miss any axioms of the natural numbers?**

What about commutativity and associativity of addition and other fundamental laws of the natural numbers?
*Example proof*: here is one of the basic laws: $(\forall x) S\,x \neq x$

$\vdash \vdash S\,x \neq x$ `by induction on` $x$ `using z.(S z≠z)`

`1` $\vdash S\,0 \neq 0$ `by Axiom 1 on 0`

`2.` $S\,x \neq x \vdash S\,S\,x \neq S\,x$ `by notR`
`2.1.` $S\,x \neq x, S\,S\,x = S\,x \vdash$ `false by notL 2`
`2.1.1.` $S\,x \neq x, S\,S\,x = S\,x \vdash S\,x = x$ `by RW with Axiom 2 using S x and x`

RW is applying the equality substitution rule

*Example proof*: What about commutativity of addition? $(\forall x, y) x + y = y + x$
The proof is a bit more complex

```
 ⊢ x + y = y + x by induction on x using z.z + y = y + z

 1. ⊢ 0 + y = y + 0  by RW rhs with Axiom 3
 1.1. ⊢ 0 + y = y  by induction on y using z.(0 + z = z)

 1.1.1.  ⊢ 0 + 0 = 0  by RW rhs with Axiom 3
 1.1.1.1.  ⊢ 0 = 0  by Equality (reflexivity)

 1.1.2.  0 + y = y ⊢ 0 + S y = S y  by RW lhs with Axiom 4
 1.1.2.1.  0 + y = y ⊢ S(0 + y) = S y  by lhs with IndHyp
 1.1.2.1.  0 + y = y ⊢ S y = S y  by Equality (reflexivity)

 2.  x + y = y + x  ⊢ S x + y = y + S x RW rhs with Axiom 4
 2.1.  x + y = y + x  ⊢ S x + y = S(y + x) RW rhs with IndHyp
 2.1.1.  x + y = y + x  ⊢ S x + y = S(x + y)
                  by induction on y using z.(S x + y = S(x + y))

 2.1.1.1.  x + y = y + x  ⊢ S x + 0 = S(x + 0) by RW lhs with Axiom 3
 2.1.1.1.1.  x + y = y + x  ⊢ S x = S(x + 0) by RW rhs with Axiom 3
 2.1.1.1.1.1.  x + y = y + x  ⊢ S x = S x by Equality (reflexivity)

 2.1.1.2.  x + y = y + x, S x + y = S(x + y)  ⊢ S x + S y = S(x + S y)
                  by RW rhs with Axiom 4
 2.1.1.2.1.  x + y = y + x, S x + y = S(x + y)  ⊢ S x + S y = S(S(x + y))
                  by RW rhs IndHyp
 2.1.1.2.1.1.  x + y = y + x, S x + y = S(x + y)  ⊢ S x + S y = S(S x + y)
                  by RW rhs Axiom 4
 2.1.1.2.1.1.1  x + y = y + x, S x + y = S(x + y)  ⊢ S x + S y = S x + S y
                  by Equality (reflexivity)
```

Note that in the proof we have shown that 0 is not only neutral to the right of + but also to the left: $0 + x = x$.
Similarly we can prove associativity of addition:
$(\forall x, y, z)(x + (y + z) = (x + y) + z)$ **HOMEWORK!**
So all basic properties of the natural numbers with addition are valid in Presburger Arithmetic.

## 16.2 Properties

### Presburger Arithmetic is decidable

For those interested I recommend a proof in the book of Boolos and Jeffrey, chapter 21 (9 pages), which describes a mechanism for deciding these formulae. Note, that in contrast to arbitrary first-order logic we have fixed the universe to be the set of natural numbers (there is only one model!) and thus limited the scope of quantifiers.
due to the absence of multiplication (BJ section 21)

**Q: Is there more than one interpretation of the axioms of Presburger Arithmetic?**

Obviously yes, but up to isomorphism they are all the same as the standard-interpretation. (no proof)

**Can we express more than addition in Presburger Arithmetic?**

What about predecessor, subtraction, multiplication and other functions?

**Defininition:** Let $\underline{\underline{x}}$ abbreviate $\underbrace{S\,S\,S\,...S\,0}_{x\text{ times}}$.

An n-ary function $f$ can be *represented* in a theory $\mathcal{T}$ if there is an n+1–ary predicate $F$ such that for all $\bar{x}, y$

$f(\bar{x}) = y$ implies $F(\underline{\underline{\bar{x}}}, \underline{\underline{y}})$ is valid and $f(\bar{x}) \neq y$ implies $\neg F(\underline{\underline{\bar{x}}}, \underline{\underline{y}})$ is valid.

We usually drop the underlining or overbars, i.e. use $x$ instead of $\bar{x}$ and $y$ instead of $\underline{\underline{y}}$ if this is unique in the context.

Examples:

- *Predecessor*: $p(x) = y$ iff $(x = 0 \wedge y = 0) \vee S\,y = x$.
  So we choose as representation the predicate $P(x, y) \equiv (x = \underline{\underline{0}} \wedge y = \underline{\underline{0}}) \vee S\,y = x$.

  Now we have to show: $p(x) = y$ implies that $P(\underline{\underline{x}}, \underline{\underline{y}})$ is valid and $p(x) \neq y$ implies that $\neg P(\underline{\underline{x}}, \underline{\underline{y}})$ is valid in Presburger Arithmetic.

  Proof by induction over $x$ (note that this is induction on the meta-level, in this case actually just a case distinction)

  1. For $x = 0$ we have $p(x) = 0$.
     Thus $y = 0$ implies that $P(\underline{\underline{0}}, \underline{\underline{y}}) \equiv (\underline{\underline{0}} = \underline{\underline{0}} \wedge \underline{\underline{0}} = \underline{\underline{0}}) \vee S\,\underline{\underline{0}} = \underline{\underline{0}}$ is valid (reflexivity left)
     $y \neq 0$ implies that $\neg P(\underline{\underline{0}}, \underline{\underline{y}}) \equiv \neg(\underline{\underline{0}} = \underline{\underline{0}} \wedge \underline{\underline{y}} = \underline{\underline{0}}) \vee S\,\underline{\underline{y}} = \underline{\underline{0}}$ is valid because $\underline{\underline{\mathrm{y}}}$ has the form $S\,...0$. Applying Axiom 1 makes both disjuncts false and thus their negation true.
  2. Assume our claim holds for $x = n$
     For $x = n + 1$ we have $p(x) = n$, and $\underline{\underline{x}} = S\,\underline{\underline{n}}$
     Thus $y = n$ implies that $P(S\,\underline{\underline{n}}, \underline{\underline{y}}) \equiv (S\,\underline{\underline{n}} = \underline{\underline{0}} \wedge \underline{\underline{y}} = \underline{\underline{0}}) \vee S\,\underline{\underline{n}} = S\,\underline{\underline{n}}$ is valid (using reflexivity right)
     $y \neq n$ implies that $\neg P(S\,\underline{\underline{n}}, \underline{\underline{y}}) \equiv \neg(S\,\underline{\underline{n}} = \underline{\underline{0}} \wedge \underline{\underline{y}} = \underline{\underline{0}}) \vee S\,\underline{\underline{y}} = S\,\underline{\underline{n}}$ is valid. The left disjunct is false because of $S\,\underline{\underline{n}} \neq \underline{\underline{0}}$ (Axiom 1) and the right disjunct is either $S\,S\,\underline{\underline{n+i}} = S\,\underline{\underline{n}}$ if $y > n$ or $S\,\underline{\underline{y}} = S\,S\,\underline{\underline{y+j}}$ if $y < n$. Both cases can be proven false in Presburger Arithmetic by repeatedly applying Axiom 2 until we reach $S\,\underline{\underline{i}} = 0$ or $0 = S\,\underline{\underline{j}}$ which is false according to Axiom 1 (or axiom 1 and the transitivity of equality).

  So, although the representation in itself was easy to find, the proof of its correctness is by no means trivial. Not however, that in order to prove the validity of $P$ or $\neg P$ we did not use the induction axiom of Presburger Arithmetic but only axioms 1 and 2 and an induction for reasoning about provability OUTSIDE of Presburger Arithmetic. This insight will be very important when we will later remove the induction axiom in the theory $\mathcal{Q}$

  From now on I only present the predicates

- *Subtraction*: $x - y = z$ iff $(x < y \wedge z = 0) \vee y + z = x$

  $x < y$ abbreviates $\exists z. S(x + z) = y$

- *Projection* $p_i^n(x_1, ..x_n) := x_i$

  $p_i^n(x_1, ..x_n) = y$ iff $y = x_i$ is valid

- *Composition* h(x) := f(g(x): f,g represented by F and G

  h(x) = y iff $\exists z. G(x, z) \wedge F(z, y)$ valid

- *Minimization*: g(x) := $\mu_y$[f(x,y)=0]: f(x,y)=t represented by $F(x, y, t)$

  g(x) = z iff $(\forall y)(y \leq z \Rightarrow \exists t.[F(x, y, t) \wedge t = 0 \Leftrightarrow y = z])$

  This is the unrestricted loop or search

  *Representation of* $\leq$:

  x$\leq$y $\equiv$ $\exists z. x + z = y$

*See Boolos-Jeffrey chapter 14 for the proofs that these representations are actually correct.*
So this is pretty powerful, since we have unrestricted loops. What about other functions like multiplication?
$x * y = z$ iff .....????
We would need inductive function definition (or primitive recursion) to do that and actually, we can't. If we could, we would have the full power of recursive functions.
*For those of you who are interested: The chapter 14 in the book of Boolos-Jeffrey proves that all recursive functions can be expressed without primitive recursion if instead you have multiplication. So if multiplication could be represented in Presburger Arithmetic, we could express all the computable functions in Presburger Arithmetic. This again would make Presburger Arithmetic undecidable as there are predicates about recursive functions that are not decidable (such as the halting problem or searching for the root of an arbitrary recursive function).*
So something is missing, ad we need to add at least multiplication to express all of arithmetic.