Peano Arithmetic

The theory PA

Definition. For a formula φ its $\forall$-*closure*, notation $\mathrm{cl}(\varphi)$, is

$$\forall\vec{x}.\varphi \equiv \forall x_1 \ldots x_n.\varphi \equiv \forall x_1(\ldots(\forall x_n.\varphi)..)$$

where $\mathrm{FV}(\varphi) = \{\vec{x}\}$

Definition. Peano Arithmetic is the first order theory with equality in the language with signature $\langle 2, 2, 0, 0; 2\rangle$

The function symbols are denoted by $+, \times, 0, 1$

Alternatively one could take $\langle 2, 2, 1, 0; 2\rangle$ and write $+, \times, S, 0$

Axioms of PA are the closures of	alternatively
$x + 1 \neq 0$	$S(x) \neq 0$
$x + 1 = y + 1 \rightarrow x = y$	$S(x) = S(y) \rightarrow x = y$
$[\varphi(0) \wedge \forall y.(\varphi(y) \rightarrow \varphi(y + 1))] \rightarrow \forall y.\varphi(y)$	$[\varphi(0) \wedge \forall y.(\varphi(y) \rightarrow \varphi(S(y)))] \rightarrow \forall y.\varphi(y)$
$x + 0 = x, x + (y + 1) = (x + y) + 1$	$x + 0 = x, x + S(y) = S(x + y)$
$x \times 0 = 0, x \times (y + 1) = (x \times y) + x$	$x \times 0 = 0, x \times S(y) = (x \times y) + x$

Basically this is in second order logic

We axiomatize $\langle \mathbb{N}, S, 0 \rangle$

$$
\begin{array}{rcl}
 & & 0 \in \mathbb{N} \\
x \in \mathbb{N} & \rightarrow & S(x) \in \mathbb{N} \\
 & & 0 \neq S(x) \\
S(x) = S(y) & \rightarrow & x = y \\
\forall X \subseteq \mathbb{N}.[\,0 \in X \ \&\ \forall y.[y \in X \rightarrow S(y) \in X] & \rightarrow & X = \mathbb{N}\,]
\end{array}
$$

The operations $+, \times$ are defined by

$$
\begin{array}{rcl|rcl}
x + 0 & = & x & x \times 0 & = & 0 \\
x + S(y) & = & S(x + y) & x \times S(y) & = & (x \times y) + x
\end{array}
$$

First results: arithmetic

$$
\begin{array}{lrcl}
\mathsf{PA} \vdash & x = 0 & \vee & \exists y. x = S(y) \\
\mathsf{PA} \vdash & x + (y + z) & = & (x + y) + z \\
\mathsf{PA} \vdash & x + y & = & y + x \\
\mathsf{PA} \vdash & x \times (y \times z) & = & (x \times y) \times z \\
\mathsf{PA} \vdash & x \times y & = & y \times x \\
\mathsf{PA} \vdash & x \times (y + z) & = & x \times y + x \times z \\
\mathsf{PA} \vdash & z \neq 0 \wedge x \times z = y \times z & \to & x = y \\
\mathsf{PA} \vdash & x \times 1 & = & x
\end{array}
$$

Order

Define $x < y := \exists z. x + S(z) = y$. Then

PA $\vdash x \not< x$

PA $\vdash x < y \wedge y < z \rightarrow x < z$

PA $\vdash x < y \vee x = y \vee y < x$

PA $\vdash x < y \rightarrow (y = S(x) \vee S(x) < y)$

PA $\vdash x < S(x)$

PA $\vdash \exists w. \varphi(w) \rightarrow \exists y. [\psi(y) \wedge \forall x < y. \neg\psi(x)]$ *least number principle*

Define $x \leq y := x < y \vee x = y$

PA $\vdash \forall w[\underbrace{\forall y{<}w. \psi(y)}_{\text{induction hypothesis}} \rightarrow \psi(w)] \rightarrow \forall w. \psi(w)$

This is *course of value induction*

Proof of course of value induction

By ($\to$-I) suffices to show

$$\forall w[\forall y{<}w.\psi(y) \to \psi(w)] \vdash_{\mathsf{PA}} \forall w.\psi(w)$$

We prove something stronger (induction loading)

$$\forall w[\forall y{<}w.\psi(y) \to \psi(w)] \vdash_{\mathsf{PA}} \forall w \forall y{<}w.\psi(y)$$

Case $w = 0$, that is $\forall y{<}0.\psi(y)$. Trivial, as $y \not< 0$.

Case $w + 1$, that is $\forall y{<}w.\psi(y) \to \forall y{<}(w + 1).\psi(y)$.

From $\forall y{<}w.\psi(y)$ and $\forall w[\forall y{<}w.\psi(y) \to \psi(w)]$ we get $\psi(w)$.

But then indeed $\forall y{<}(w + 1).\psi(y)$,

as $y < (w + 1) \leftrightarrow y < w \vee y = w$. ■

Simple number theory

PA $\vdash \forall xy.(y \neq 0 \to \exists a \exists b{<}y.[x = ay + b])$

Definition

$$
\begin{aligned}
x|y &:= \exists z.(xz = y) \\
\mathrm{irred}(x) &:= \forall d{<}x[d|x \to d = 1] \\
\mathrm{prime}(x) &:= x{>}1 \wedge \forall yz[x|yz \to x|y \vee x|z]
\end{aligned}
$$

Proposition PA $\vdash \forall x{>}1.[\mathrm{irred}(x) \ \leftrightarrow \ \mathrm{prime}(x)]$

Proposition PA $\vdash \forall x{>}1 \exists v.(\mathrm{prime}(v) \wedge v|x)$

Exercise Prove 'There are infinitely many primes'

That is PA $\vdash \forall x \exists y{>}x.\mathrm{prime}(y)$

Powers

Define

$$
\begin{aligned}
\mathrm{pow}(x, v) \quad &:= \quad x{\geq}1 \wedge \mathrm{prime}(v) \wedge \forall w{\leq}x.[w{>}1 \wedge w|x \rightarrow v|w] \\
&\Leftrightarrow \quad \text{“}\exists k.x = v^k \wedge \mathrm{prime}(v)\text{”} \\
\mathrm{pp}(x) \quad &:= \quad \exists v{\leq}x.\mathrm{pow}(x, v) \\
&\Leftrightarrow \quad \text{“}\exists v \exists k.x = v^k \wedge \mathrm{prime}(v)\text{”}
\end{aligned}
$$

Definitional extensions

Let $\vec{x} = x_1, \ldots, x_n$. Suppose we can show

$$\mathsf{PA} \vdash \forall \vec{x}\, \exists ! y. \varphi(\vec{x}, y)$$

We can introduce a new function symbol f_φ of arity n and postulate

$$\forall \vec{x}. \varphi(\vec{x}, f_\varphi(\vec{x}))$$

Theorem. This *definitional extension* of PA is equally strong as PA.

Proof idea. Systematically translate

$$\psi(f(\vec{x}))$$

by

$$\exists y. [\varphi(\vec{x}, y) \wedge \psi(y)]. \blacksquare$$

For example we can do this for $\varphi(x_1, x_2)$

$$[(y = 0 \wedge x_1 < x_2) \vee x_1 = y + x_2]$$

For the resulting $f_\varphi(x_1, x_2)$ we write $x_1 \dot{-} x_2 :=$ if $x_1 \geq x_2$ then $x_1 - x_2$ else 0

A new function

Define

$$x \upharpoonright v := v^{\max\{k \in \mathbb{N} | v^k | x\}}$$

$$\begin{aligned} 5 \upharpoonright 3 &= 1 \\ 6 \upharpoonright 3 &= 3 \\ 18 \upharpoonright 3 &= 9 \\ 54 \upharpoonright 3 &= 27 \end{aligned}$$

We can use $\upharpoonright$ in PA since $\upharpoonright = f_\varphi$ with

$$\varphi(x, v, y) := [\mathrm{pow}(y, v) \wedge y | x \wedge yv \not| x]$$

where we have to check the $\forall\exists!$-condition for φ

Known functions

For

$$\psi(x,y,z) \quad := \quad xy \neq 0 \wedge x|z \wedge y|z \wedge \forall v.[x|v \wedge y|v \rightarrow z|v] \\ \vee[xy = 0 \wedge z = 0]$$

we get $f_\psi = \mathrm{lcm}$

Similarly

$$\chi(x,y,z) := z|x \wedge z|y \wedge \forall v.[v|x \wedge v|y \rightarrow v|z] \wedge [xy = 0 \rightarrow z = 0]$$

gives $f_\chi = \mathrm{gcd}$

Provable results

PA ⊢ $x|y \leftrightarrow \forall v{\leq}x.[\mathrm{pp}(v) \wedge v|x \rightarrow v|y]$ (4.1.4)

PA ⊢ $\forall x, y{\geq}1 \exists a{\leq}y \exists b{\leq}x.[ax = by + \mathrm{gcd}(x, y)]$ (4.1.6, Bézout)