Simplistic ZFC Formalization

Sebastian Ullrich

April 19, 2014

Contents

theory *ZFC*
imports *HOL*
begin

typedecl *set*

axiomatization
  member :: *set* $\Rightarrow$ *set* $\Rightarrow$ *bool*

notation
  member (*op* :) **and**
  member ((-/ : -) [*51*, *51*] *50*)

abbreviation *not-member* **where**
  not-member x A $\equiv$ ~ (x : A) — non-membership

notation
  not-member (*op* ~:) **and**
  not-member ((-/ ~: -) [*51*, *51*] *50*)

notation (*xsymbols*)
  member (*op* $\in$) **and**
  member ((-/ $\in$ -) [*51*, *51*] *50*) **and**
  not-member (*op* $\notin$) **and**
  not-member ((-/ $\notin$ -) [*51*, *51*] *50*)

1 Zermelo-Fraenkel Axiom System

axiomatization where
  extensionality: $\forall z.\ (z \in x \longleftrightarrow z \in y) \Longrightarrow x = y$ **and**
  foundation: $\exists y.\ y \in x \Longrightarrow \exists y.\ y \in x \wedge (\forall z.\ \neg(z \in x \wedge z \in y))$ **and**
  subset-set: $\exists y.\ \forall z.\ z \in y \longleftrightarrow z \in x \wedge P\ z$ **and**
  empty-set: $\exists y.\ \forall x.\ x \notin y$ **and**
  pair-set: $\exists y.\ \forall x.\ x \in y \longleftrightarrow x = z_1 \vee x = z_2$ **and**
  power-set: $\exists y.\ \forall z.\ z \in y \longleftrightarrow (\forall u.\ u \in z \longrightarrow u \in x)$ **and**
  sum-set: $\exists y.\ \forall z.\ z \in y \longleftrightarrow (\exists u.\ z \in u \wedge u \in x)$

definition *empty* :: *set* ({}) **where**
  $empty \equiv THE\ y.\ \forall x.\ x \notin y$

axiomatization where
  infinity: $\exists w.\ \{\} \in w \wedge (\forall x.\ x \in w \longrightarrow (\exists z.\ z \in w \wedge (\forall u.\ u \in z \longleftrightarrow u \in x \vee u = x)))$ **and**
  replacement: $P\ x\ y \wedge P\ x\ z \longrightarrow y = z \Longrightarrow \exists u.\ (\forall w_1.\ w_1 \in u \longleftrightarrow (\exists w_2.\ w_2 \in a \wedge P\ w_2\ w_1))$

lemma *empty*[*simp*]: $x \notin empty$

proof−
  have $\exists! y.\ \forall x.\ x \notin y$
  proof (*rule ex-ex1I*)
    fix $y\ y'$
    assume $\forall x.\ x \notin y\ \forall x.\ x \notin y'$
    thus $y = y'$ **by** −(*rule extensionality*, *simp*)
  qed (*rule empty-set*)
  hence $\forall x.\ x \notin \{\}$
    unfolding *empty-def*
    by (*rule theI'*)
  thus *?thesis* **..**
qed

Let's try to generalize that for the other introduction axioms.

lemma *exAxiomD1*:
  assumes $\exists y.\ \forall x.\ x \in y \longleftrightarrow P\ x$
  shows $\exists! y.\ \forall x.\ x \in y \longleftrightarrow P\ x$
using *assms*
by (*auto intro*:*extensionality*)

lemma *exAxiomD2*:
  assumes $\exists y.\ \forall x.\ x \in y \longleftrightarrow P\ x$
  shows $x \in (THE\ y.\ \forall x.\ x \in y \longleftrightarrow P\ x) \longleftrightarrow P\ x$
apply (*rule spec*[*of - x*])
by (*rule theI'*[*OF assms*[*THEN exAxiomD1*]])

lemma *exAxiomD3*:
  assumes $\exists y.\ \forall x.\ x \in y \longleftrightarrow P\ x\ \ x \in (THE\ y.\ \forall x.\ x \in y \longleftrightarrow P\ x)$
  shows $P\ x$
using *assms exAxiomD2*
by *auto*

lemma *empty'*: $x \notin empty$
apply (*rule exAxiomD2*[*of* λ-. *False*, *simplified*, *folded empty-def*])
by (*rule empty-set*)

lemma[*simp*]: $(\forall x.\ x \notin y) \longleftrightarrow y = \{\}$
by (*auto intro*:*extensionality*)

definition *pair* :: *set* ⇒ *set* ⇒ *set* ({-, -}) **where**
  $pair\ z_1\ z_2 \equiv THE\ y.\ \forall x.\ x \in y \longleftrightarrow x = z_1 \lor x = z_2$

definition *singleton* :: *set* ⇒ *set* ({-}) **where**
  $singleton\ x \equiv \{x, x\}$

definition *sum* :: *set* ⇒ *set* **where**
  $sum\ x \equiv THE\ y.\ \forall z.\ z \in y \longleftrightarrow (\exists u.\ z \in u \land u \in x)$

definition *subset* :: (*set* ⇒ *bool*) ⇒ *set* ⇒ *set* **where**

subset P x ≡ *THE y*. $\forall z.\ z \in y \longleftrightarrow z \in x \wedge P\ z$

syntax
subset :: *pttrn* => *set* ⇒ *bool* => *set* ((*1*{- ∈ -./ -}))
translations
{*z* ∈ *x*. *P*} == *subset* (%*z*. *P*) *x*

definition *Pow* :: *set* ⇒ *set* **where**
Pow x ≡ *THE y*. $\forall z.\ z \in y \longleftrightarrow (\forall u.\ u \in z \longrightarrow u \in x)$

lemma *pair*[*simp*]: $x \in \{z_1, z_2\} \longleftrightarrow x = z_1 \vee x = z_2$
by (*rule exAxiomD2*[*of* $\lambda x.\ x = z_1 \vee x = z_2$, *simplified*, *folded pair-def*]) (*rule pair-set*)

lemma *singleton*[*simp*]: $x \in \{y\} \longleftrightarrow x = y$
by −(*unfold singleton-def*, *simp*)

lemma *sum*[*simp*]: $z \in sum\ x \longleftrightarrow (\exists u.\ z \in u \wedge u \in x)$
by (*rule exAxiomD2*[*of* $\lambda z.\ \exists u.\ z \in u \wedge u \in x$, *simplified*, *folded sum-def*]) (*rule sum-set*)

lemma *subset*[*simp*]: $z \in \{z \in x.\ P\ z\} \longleftrightarrow z \in x \wedge P\ z$
by (*rule exAxiomD2*[*of* $\lambda z.\ z \in x \wedge P\ z$, *simplified*, *folded subset-def*]) (*rule subset-set*)

lemma *Pow*[*simp*]: $z \in Pow\ x \longleftrightarrow (\forall u.\ u \in z \longrightarrow u \in x)$
by (*rule exAxiomD2*[*of* $\lambda z.\ \forall u.\ u \in z \longrightarrow u \in x$, *simplified*, *folded Pow-def*]) (*rule power-set*)

2 Lemmas on Unions and Intersections

definition *union* :: *set* ⇒ *set* ⇒ *set* (**infixl** ∪ *65*) **where**
union x y ≡ *sum* (*pair x y*)

lemma *union*[*simp*]: $z \in a \cup b \longleftrightarrow z \in a \vee z \in b$
by (*auto simp*:*union-def*)

lemma *union-script*: $\exists y.\ \forall z.\ z \in y \longleftrightarrow z \in a \vee z \in b$
by (*rule exI*[*of* - $a \cup b$]) *simp*

definition *intersect* :: *set* ⇒ *set* ⇒ *set* (**infixl** ∩ *70*) **where**
$a \cap b \equiv \{x \in a.\ x \in b\}$

lemma *intersect*[*simp*]: $z \in a \cap b \longleftrightarrow z \in a \wedge z \in b$
by (*simp add*:*intersect-def*)

lemma *intersect-script*: $\exists y.\ \forall z.\ z \in y \longleftrightarrow z \in a \wedge z \in b$

by (*rule subset-set*)

definition *Intersect* :: $(set \Rightarrow bool) \Rightarrow set$ ($\bigcap$- [1000] 999) **where**
$\bigcap P \equiv THE\ y.\ \forall z.\ z \in y \longleftrightarrow (\forall u.\ P\ u \longrightarrow z \in u)$

lemma *Intersect*[*simp*]: $\exists z.\ P\ z \Longrightarrow z \in \bigcap P \longleftrightarrow (\forall u.\ P\ u \longrightarrow z \in u)$
proof (*rule exAxiomD2*[*of* $\lambda z.\ \forall u.\ P\ u \longrightarrow z \in u$, *simplified*, *folded Intersect-def*])
assume $\exists z.\ P\ z$
then obtain z **where**[*simp*]: $P\ z$ **..**
let $?y = \{x \in z.\ \forall u.\ P\ u \longrightarrow x \in u\}$
have $\forall x.\ x \in ?y \longleftrightarrow (\forall u.\ P\ u \longrightarrow x \in u)$ **by** *auto*
thus $\exists y.\ \forall x.\ x \in y \longleftrightarrow (\forall u.\ P\ u \longrightarrow x \in u)$**..**
qed

3 Ordered Pairs

definition *ordered-pair* :: $set \Rightarrow set \Rightarrow set$ ($\langle$-,-$\rangle$) **where**
$\langle a,b\rangle \equiv \{\{a\}, \{a,b\}\}$

lemma *intersect-singleton*[*simp*]: $x \cap \{y\} = (if\ y \in x\ then\ \{y\}\ else\ \{\})$
by (*auto intro*:*extensionality*)

lemma *empty-singleton-neq*[*simp*]: $\{x\} \neq \{\}$
proof
assume *assm*: $\{x\} = \{\}$
have $x \notin \{\}$ **by** *simp*
with *assm* **have** $x \notin \{x\}$ **by** *simp*
thus *False* **by** *simp*
qed

lemma *singleton-eqD*[*dest!*]: $\{x\} = \{y\} \Longrightarrow x = y$
by (*drule arg-cong*[*of* - -$\lambda z.\ y \in z$]) *simp*

lemma *singleton-pair-eqD*[*dest!*]:
assumes $\{x\} = \{y, z\}$
shows $x = y \wedge y = z$
proof−
from *assms* **have** $y \in \{x\} \longleftrightarrow y \in \{y, z\}$ **by** *simp*
hence $x = y$ **by** *simp*
from *assms* **have** $z \in \{x\} \longleftrightarrow z \in \{y, z\}$ **by** *simp*
hence $x = z$ **by** *simp*
with ‹$x = y$› **show** *?thesis* **by** *simp*
qed

lemma *singleton-pair-eqD'*[*dest!*]:
assumes $\{y, z\} = \{x\}$
shows $x = y \wedge y = z$
using *assms*[*symmetric*] **by** (*rule singleton-pair-eqD*)

lemma *pair-singleton*[*simp*]: $\{x,\ x\} = \{x\}$
unfolding *singleton-def* **..**

lemma *pair-eq-fstD*[*dest*!]:
  assumes $\{x{,}y\} = \{x{,}z\}$
  shows $y = z$
using *assms*
proof (*cases* $x = y$)
  case *False*
  from *assms* **have** $y \in \{x{,}y\} \longleftrightarrow y \in \{x{,}z\}$ **by** *simp*
  with *False* **show** *?thesis* **by** *simp*
qed *auto*

lemma *ordered-pair-eq*[*simp*]: $\langle x_1{,}x_2\rangle = \langle y_1{,}y_2\rangle \longleftrightarrow x_1 = y_1 \wedge x_2 = y_2$
proof
  assume *assm*: $\langle x_1{,}x_2\rangle = \langle y_1{,}y_2\rangle$
  hence $\{x_1\} \in \langle x_1{,}x_2\rangle \longleftrightarrow \{x_1\} \in \langle y_1{,}y_2\rangle$ **by** *simp*
  hence[*simp*]: $x_1 = y_1$ **by** (*auto simp*:*ordered-pair-def*)
  show $x_1 = y_1 \wedge x_2 = y_2$ **using** *assm*
  proof (*cases* $x_2 = x_1$)
    case *False*
    from *assm* **have** $\{x_1{,}x_2\} \in \langle x_1{,}x_2\rangle \longleftrightarrow \{x_1{,}x_2\} \in \langle y_1{,}y_2\rangle$ **by** *simp*
    with *False* **show** *?thesis* **by** (*auto simp*:*ordered-pair-def*)
  qed (*auto simp*:*ordered-pair-def*)
qed *simp*

4 Relations and Functions

definition *rel* $r \equiv \forall x.\ x \in r \longrightarrow (\exists x_1\ x_2.\ x = \langle x_1{,}x_2\rangle)$
definition *rel''* $r\ a\ b \equiv$ *rel* $r \wedge (\forall x_1\ x_2.\ \langle x_1,\ x_2\rangle \in r \longrightarrow x_1 \in a \wedge x_2 \in b)$
definition *rel'* $r\ s \equiv$ *rel''* $r\ s\ s$
definition *func* $r \equiv$ *rel* $r \wedge (\forall x\ y_1\ y_2.\ \langle x{,}y_1\rangle \in r \wedge \langle x{,}y_2\rangle \in r \longrightarrow y_1 = y_2)$
definition *func'* $f\ a\ b \equiv$ *func* $f \wedge$ *rel''* $f\ a\ b$

4.1 Existence Proofs

definition *singletons* $a \equiv \{b \in$ *Pow* $a.\ \exists x.\ b = \{x\}\}$

lemma *singletons*[*simp*]: $b \in$ *singletons* $a \longleftrightarrow (\exists x.\ b = \{x\} \wedge x \in a)$
by (*auto simp*:*singletons-def*)

definition *pairs* $a\ b \equiv \{c \in$ *Pow* $(a \cup b).\ \exists x\ y.\ c = \{x,\ y\} \wedge x \in a \wedge y \in b\}$

lemma *pairs-correct*[*simp*]: $c \in$ *pairs* $a\ b \longleftrightarrow (\exists x\ y.\ c = \{x,\ y\} \wedge x \in a \wedge y \in b)$
by (*auto simp*:*pairs-def*)

definition *ordered-pairs a b* $\equiv$ $\{c \in Pow\ (Pow\ a \cup Pow\ (a \cup b)).\ \exists\, x\ y.\ c = \langle x,y \rangle \wedge x \in a \wedge y \in b\}$

lemma *ordered-pairs*[*simp*]: $c \in$ *ordered-pairs a b* $\longleftrightarrow (\exists\, x\ y.\ c = \langle x,y \rangle \wedge x \in a \wedge y \in b)$
by (*auto simp add*:*ordered-pairs-def ordered-pair-def*)

definition *rels a b* $\equiv \{r \in Pow$ (*ordered-pairs a b*). *rel r*$\}$

lemma *rels*[*simp*]: $r \in$ *rels a b* $\longleftrightarrow$ *rel''* *r a b*
by (*auto simp*:*rels-def rel-def rel''-def*)

definition *funcs a b* $\equiv \{f \in$ *rels a b*. *func f*$\}$

lemma *funcs*[*simp*]: $f \in$ *funcs a b* $\longleftrightarrow$ *func'* *f a b*
by (*auto simp*:*funcs-def func'-def func-def*)

5 Natural Numbers

definition *succ* :: *set* $\Rightarrow$ *set* ((-$^+$) [*1000*] *999*) **where**
$a^+ \equiv a \cup \{a\}$

definition *zero* :: *set* (*0*) **where** *0* $\equiv \{\}$

definition *Ded a* $\equiv 0 \in a \wedge (\forall\, x.\ x \in a \longrightarrow x^+ \in a)$

lemma *icanhazded*: $\exists\, a.$ *Ded a*
proof−
  thm *infinity*
  from *infinity* **obtain** *a* **where** *inf*: $\{\} \in a$
    $\forall\, x.\ x \in a \longrightarrow (\exists\, z.\ z \in a \wedge (\forall\, u.\ (u \in z) = (u \in x \vee u = x)))$ **by** *auto*
  have $\forall\, x.\ x \in a \longrightarrow x^+ \in a$
  proof (*rule*, *rule*)
    fix *x*
    assume $x \in a$
    with *inf* **obtain** *z* **where** *z*: $z \in a\ \forall\, u.\ u \in z \longleftrightarrow u \in x \vee u = x$ **by** *auto*
    from *this*(*2*) **have**[*simp*]: $z = x \cup \{x\}$
    by (*auto intro*:*extensionality*)
    with *z*(*1*) **show** $x^+ \in a$ **by** (*auto simp*:*succ-def*)
  qed
  with *inf*(*1*) **show** *?thesis* **by** (*auto simp add*:*Ded-def zero-def*)
qed

definition *nats* :: *set* ($\mathbb{N}$) **where** $\mathbb{N} \equiv \bigcap$ *Ded*

lemma *nats*: $n \in \mathbb{N} \longleftrightarrow (\forall\, a.$ *Ded a* $\longrightarrow n \in a)$
unfolding *nats-def*
by (*rule Intersect*) (*rule icanhazded*)

5.1 Peano's Axioms

lemma *ax-zero*: $0 \in \mathbb{N}$
by (*simp add*:*nats Ded-def*)

lemma *ax-succ*: $n \in \mathbb{N} \Longrightarrow n^+ \in \mathbb{N}$
by (*simp add*:*nats Ded-def*)

lemma *nonempty-member*[*simp*]: $x \neq \{\} \longleftrightarrow (\exists\, y.\ y \in x)$
by (*rule ccontr*) *simp*

lemma *union-nonempty*[*simp*]: $x \neq \{\} \vee y \neq \{\} \Longrightarrow x \cup y \neq \{\}$
by *auto*

lemma *ax-succ-neq-zero*: $n \in \mathbb{N} \Longrightarrow n^+ \neq 0$
by (*simp add*:*succ-def zero-def*)

lemma *ax-succ-inj*:
  assumes $n \in \mathbb{N}$ $m \in \mathbb{N}$ $n^+ = m^+$
  shows $n = m$
proof−
  from *assms*(*3*) **have** $m \in n \cup \{n\}$ **by** (*simp add*:*succ-def*)
  hence *m*: $n = m \vee m \in n$ **by** *auto*
  from *assms*(*3*)[*symmetric*] **have** $n \in m \cup \{m\}$ **by** (*simp add*:*succ-def*)
  hence *n*: $n = m \vee n \in m$ **by** *auto*

  from *n m foundation*[*of* $\{n,m\}$]
  show *?thesis* **by** *auto*
qed

definition *subseteq* :: *set* ⇒ *set* ⇒ *bool* (- ⊆ - *50*) **where**
  $x \subseteq y \equiv \forall\, z.\ z \in x \longrightarrow z \in y$

lemma *ax-trivial*: $[\![0 \in x; \forall\, y.\ y \in x \longrightarrow y^+ \in x]\!] \Longrightarrow \mathbb{N} \subseteq x$
by (*simp add*:*subseteq-def nats Ded-def*)

end