CS 486: Spring 2001
Cornell University
Prof. Robert Constable

April 17 Lecture Notes - Formalization

Semigroups

Last Thursday we discussed the formalization of semigroups.

Semigroup = Set S, operation $\circ$, such that
$\forall x, y, z \in S, \quad x \circ (y \circ z) = (x \circ y) \circ z \quad \underline{\text{Assoc}}$

We formalized that as first-order language with predicates Eq for equality, =; Op for $\circ$; and axioms

$E_1 - E_3$	for equality
Op_1	for total functionality of $Op: \ \forall xy \exists !\, z \ Op(x, y, z)$
assoc	$Op(y, z, u) \wedge Op(x, u, t) \wedge Op(x, y, v) \wedge Op(v, z, s) \supset Eq(t, s)$

Monoids, Groups, Rings and Fields

Today we will extend that to Monoids, Groups, Rings, and Fields. We will first review what these concepts are and then formalize them.

a) *Monoids* are semigroups together with an identity for $\circ$.

  axiom is <u>Id</u>: $\quad \exists !\, i. \quad \forall x \exists S. \quad x \circ i = x \ \wedge \ i \circ x = x$
  or formalized: $\quad \exists !\, i. \quad \forall x \quad Op(x, i, x) \ \wedge \ Op(i, x, x)$

  for $(\mathbb{Z}, +)$ the identity is 0; for $(\mathbb{Z}, *)$ the identity is 1

b) *Groups* are monoids with inverse elements.

  <u>Inv</u> $\forall x \in S.\ \exists \bar{x} \in S.\ x \circ \bar{x} = i \ \wedge \ \bar{x} \circ x = i.$

  Formalized $\forall x \exists \bar{x}.\ Op(x, \bar{x}, i) \wedge Op(\bar{x}, x, i).$

  for $(\mathbb{Z}, +)$ the inverse of x is $-x$
  for $(\mathbb{Z}, *)$ there are no inverses; it is not a group
  for $(\mathbb{Z}_3, *)$ the inverse of 1 is 1, and for 2 it is 2; but 0 doesn't have an inverse

c) *Rings.* There is more to $\mathbb{Z}$ than being a group – this comes from the interplay of two operations, + and $*$. $(\mathbb{Z}, +)$ is a group, $(\mathbb{Z}, *)$ is a monoid, both are *commutative* ($a + b = b + a$; $a * b = b * a$).

  If we put that together, we know that $(\mathbb{Z}, +, *)$ satisfies the following axioms:

	+	$*$
Assoc	A_2	M_2
Comm	A_1	M_1
Id	A_3	M_3
Inv	A_4	—

  (The names $A_1 - A_4$, $M_1 - M_4$ refer to the handout.)

And there is one more axiom about the combination of $+$ and $*$:

$$\forall xyz.\;\; x*(y+z) = x*y + x*z \;\; \textit{Distrib} \text{ (or ``D'' in the handout)}$$

If we put these together we get what is called a ring. Actually for being a ring, it suffices to have $A_1 - A_4, M_2$ and D.

Because of: M_1 $(\mathbb{Z}, +, *)$ is a *commutative ring*
M_3 it is a *ring with unity*

And even more, we know that there is no divisor of zero. If $x * y = 0$ then either $x = 0$ or $y = 0$. A ring that has this property,

$$\forall xy.\;\; x * y = i_+ \supset x = i_+ \vee y = i_+ \;(Z)$$

and M_1 and M_3, is called an *integral domain*. However, since $(\mathbb{Z}, +, *)$ does not satisfy M_4 (Inv for $*$) it is not a field.

d) *Fields.*

$M_4 :\;\; \forall x.\;\; x \neq i_+ \supset \exists\, \bar{x} \in S.\;\; x * \bar{x} = i_* \wedge \bar{x} * x = i_*$

An example for a domain with two operations that is a field is:

$(\mathbb{Q}, +, *)$ with $\bar{x} \equiv \frac{1}{x}$

Notes from Professor Constable's half of lecture:

Connection between logic and boolean rings (relate $t, f, \&, \vee, \supset$ to ring operations).

<u>Boolean ring</u>: ring + idempotence $\quad x \cdot x = x \quad$ <u>note:</u> this is not a boolean algebra

Formalization of basic math is first-order logic

a) from algebraic and ordered structures to natural numbers
b) compare to Peano Arithmetic in Stewart & Tall (assignment next week)

Which axioms do we have to add to *uniquely* describe $\mathbb{Z}$ (up to isomorphism)? I.e., what characteristizes $\mathbb{Z}$, beyond being an integral domain?

- Ordering (discrete linear order!) connected to $+$ and $*$
- Define predicate <u>positive</u> $Pos(Z)$, then $a < b$ is $P(b-a)$

$$\begin{array}{llll} P_1 & \forall xy.\ Pos(x) \wedge Pos(y) & \supset & Pos(x+y) \\ P_2 & \forall xy.\ Pos(x) \wedge Pos(y) & \supset & Pos(x*y) \\ P_3 & \forall x.\ Pos(x) \vee Pos(-x) & \vee & x = 0 \end{array}$$

- Prove the basic laws of $<, +, *$ (monotonicity, strict order, etc.)

  e.g. $\forall xyz.\ x < y \wedge y < z > x < z$.
  <u>Proof</u>: we know $Pos(y-x) \wedge Pos(z-y)$ show $Pos(z-x)$ using P_1 and the ring axioms.

- <u>But</u> we need more than just ordered integral domains to characterize $\mathbb{Z}$ ($\mathbb{Z}_4$ satisfies all these axioms), i.e <u>induction principle</u>:

$$Q(0) \wedge (\forall x > 0.\ \ Q > Q(x+1)) \wedge (\forall x.\ \ x < 0.\ \ Q(x+1) > Q(x)) > \forall x.\ \ Qx$$

$\mathbb{Z}$ is <u>the</u> ordered integral domain with induction.

Define $Nat(x) \equiv Pos(x) \vee x = 0$.