Formal Specification F28FS2, Lecture 2
(Up to section 3.2 of Currie's book.)

Jamie Gabbay

January 27, 2014

Types

Z is a typed language. Example types:

- $\mathbb{Z}$ (integers).
- $\mathbb{N}$ (natural numbers).

We'll see more types in due course.

We can construct types out of other types, or we can declare new basic types like '$PERSON$'.

Variables

x, y, z are variables. Each variable has a type, which describes the possible values we can give a variable.

$x : \mathbb{Z}$ is a integer variable. If we write 'x', we mean 'some possibly negative number'.

$x, y : \mathbb{N}$ are two natural number variables. If we write 'x, y', we mean 'two numbers, both non-negative'.

By the way, is 0 in $\mathbb{N}$? (Answer: page 20 of "The essence of Z", or page 44 of ZBook (Formal Specification and Documentation using Z).)

$x : \mathit{PERSON}$ corresponds to what we say in English "some guy".

Predicates

A predicate is a proposition with variables.

A predicate can be assigned a truth-value, and can contain variables.

So if $x, y : \mathbb{N}$ then

$$x = y + 3$$

is a predicate.

If $x, y : PERSON$ then $x = y$ and $\neg(x = y)$ are predicates.

Predicates

So $x, y : \mathbb{N}$.

- If we decide that $x = 2$ and $y = 1$, then the truth-value of $x = y + 3$ is the truth-value of $2 = 1 + 3$.
- If we decide that $x = 2$ and $y = -1$, then the truth-value of $x = y + 3$ is the truth-value of $2 = (-1) + 3$.

There is a mistake in the last item. What is it?

Quantifiers

We use quantifiers to express general truths.

To assert 'for all x, $x + 1 > 1$' we use a universal or for all quantifier:

$$\forall x : \mathbb{N} \bullet (x + 1 > 1).$$

To assert 'there exists an x, $x + 1 > 1$' we use an existential or there exists quantifier:

$$\exists x : \mathbb{N} \bullet (x + 1 > 1).$$

Quantifiers

Assume a base type *PERSON* and variables $x, y, z : PERSON$.

Assume a binary (2-place) predicate-former *loves* (so $loves(x, y)$ means 'x loves y'). Write down predicates to express the following:

- Everybody loves everybody.
- Everybody loves everybody else (but not necessarily themselves).
- Everybody has somebody who loves them.
- Everybody has somebody else who loves them.
- There is only one person (hint: use equality).

Quantifiers

Assume a base type *PERSON* and variables $x, y, z : PERSON$.
Assume a binary (2-place) predicate-former *loves* (so $loves(x, y)$ means 'x loves y'). Predicates are:

- $\forall x : PERSON \bullet \forall y : PERSON \bullet loves(x, y)$.
- $\forall x : PERSON \bullet \forall y : PERSON \bullet (\neg(y = x) \Rightarrow loves(x, y))$.
- $\forall x : PERSON \bullet \exists y : PERSON \bullet loves(y, x)$.
- Exercise: Everybody has somebody else who loves them.
- Exercise: There is only one person (hint: use equality).

Get the types right

The type of a variable can make a difference:

$$\begin{array}{ll} \forall x : \mathbb{Z} \bullet (x + 2 > 1) & \text{is false} \\ \forall x : \mathbb{N} \bullet (x + 2 > 1) & \text{is true} \end{array}$$

A convenient shorthand

Write

$$\forall x : \mathbb{N} | P \bullet Q$$

for

$$\forall x : \mathbb{N} \bullet (P \Rightarrow Q)$$

Thus,

$$\forall x : \mathbb{N} | x > 5 \bullet x > 5 \quad \text{is true.}$$

Read $|$ as ‘such that’.

Is this true or false?

$$\forall x : \mathbb{N} | x > 5 \bullet \forall y : \mathbb{N} | y < 4 \bullet x^y > y^x.$$

Alternative presentation:

$$\forall x : \mathbb{N} \bullet \forall y : \mathbb{N} \bullet ((x > 5 \wedge y < 4) \Rightarrow x^y > y^x).$$

Syntax

$\forall \langle\text{name}\rangle : \langle\text{type}\rangle\ [\ |\ \langle\text{constraint}\rangle]\ \bullet \langle\text{predicate}\rangle$

This is read as:

"For all $\langle$name$\rangle$ of type $\langle$type$\rangle$
[such that $\langle$constraint$\rangle$], it is true that
$\langle$predicate$\rangle$."

Existential quantifier

Finally, $\exists_1$ means 'there exists a unique'.

$\exists_1 x : \mathbb{N} \bullet x = 25$ is true.

$\exists_1 x : \mathbb{N} \mid x < 6 \land x > 4 \bullet T$ is true (there is just one number less than 6 and more than 4).

$\exists_1 x : \mathbb{Z} \bullet x^2 = 25$ is false.

Exercise: Express $\exists_1$ using $\exists$ and $=$.

Exercise: Express $\exists$ using $\forall$ and $\neg$.

Quantifiers (summarised)

Tell me whether the following are true or false:

- $\forall x : \mathbb{N} | x < 10 \bullet x + 9 > 12$.
- $\exists x : \mathbb{N} | x < 10 \bullet x + 9 > 12$.
- $\exists_1 x : \mathbb{N} | x < 10 \bullet x + 9 > 12$.

That's it for Chapter 2 of "The essence of Z". Do exercises 2.5 and 2.6.

Get comfortable with writing propositions now. You can do this by doing the exercises above (and proposing more of your own on `haggis.stackexchange.com`).

Types

Every variable in Z has a type, which you must specify when you declare the variable: $x, y : \mathbb{Z}$.

$\mathbb{Z}$ is a built-in type.

You can declare your own types using a free type definition:

- COLOUR $::=$ red $|$ green $|$ blue.
  This declares a type with three elements.
- So does this: FUEL $::=$ petrol $|$ diesel $|$ electricity.
- So does this: FLAGSTATE $=$ up $|$ down.

Types

You can add a basic type PERSON.

- [PERSON].
- [FLAG].

This just declares a type — and says nothing of what is or is not a person. You can still declare x : PERSON, but where your people come from — that's none of Z's business.

Nested quantifiers (love)

Assume a binary predicate $\text{loves}(x, y)$ on $x, y : \text{PERSON}$. Then:

- $\forall x, y : \text{PERSON} \bullet \text{loves}(x, y)$ is “everybody loves everybody” (as in: make love, not war).
- $\forall x : \text{PERSON} \bullet \exists y : \text{PERSON} \bullet \text{loves}(x, y)$ means “everybody loves somebody” (cf. Elton John 1990: “You Gotta Love Someone”).
- $\exists x : \text{PERSON} \bullet \forall y : \text{PERSON} \bullet \text{loves}(x, y)$ means “there is somebody who loves everybody” (Jesus, Mickey Mouse, Chatty Cathy, ...).
- $\exists x : \text{PERSON} \bullet \exists y : \text{PERSON} \bullet \text{loves}(x, y)$ means “there is somebody who loves somebody” (but it might be themselves; how do you write “there is somebody who loves somebody else”?).

Nested quantifiers (number theory)

Suppose $x, y : \mathbb{N}$. Define $x|y$ (x divides y) by

$$x|y \quad \text{for} \quad \exists z : \mathbb{N} \bullet x * z = y.$$

Then define even(y) to be $2|y$.

Q. How do you write 'y is prime'? (Hint: y is prime when any number dividing it is 1 or y.)

Nested quantifiers (number theory)

prime(y) is

$$\forall x : \mathbb{N} \mid x|y \bullet (x = 1 \vee x = y).$$

Nested quantifiers (number theory)

Q (relatively easy). Goldbach's conjecture: every number greater than 2 is the sum of two primes. Express the conjecture in predicate logic.

Q (hard). Abraham Lincoln is said to have said "You can fool some of the people all of the time, and all of the people some of the time, but you can not fool all of the people all of the time.".

Assuming $x : \mathit{PERSON}$ and modelling time as $t : \mathbb{N}$, and assuming a binary predicate $\mathrm{canFool}(x, t)$, express this in predicate logic.

Signatures

A signature is a collection of type declarations.

Philosophers call this a universe of discourse; down the pub this is called ‘what we’re talking about’.

Sets

Given a type T we can form the powerset $\mathbb{P}\ T$. This is the type of sets of elements from T.

We declare sets as follows:

numset $==$ $\{4, 5, 6, 7, 8, 9\} : \mathbb{P}\mathbb{Z}$

numset $==$ $4..9 : \mathbb{P}\mathbb{Z}$

numset $==$ $\{n : \mathbb{Z} | n \geq 4 \wedge n \leq 9 \bullet n\} : \mathbb{P}\mathbb{Z}$

numset $==$ $\{n : \mathbb{Z} | n \geq 2 \wedge n \leq 7 \bullet n + 2\} : \mathbb{P}\mathbb{Z}$.

(These are all equivalent.)

Sets

If the declared variable is 'naked' after the bullet, we may omit it:

numset $== \{n : \mathbb{Z} | n \geq 4 \wedge n \leq 9\} : \mathbb{P}\mathbb{Z}$

is shorthand for

numset $== \{n : \mathbb{Z} | n \geq 4 \wedge n \leq 9 \bullet n\} : \mathbb{P}\mathbb{Z}$.

Sets

If the predicate is just true, we may omit it:

evens $== \{n : \mathbb{Z} \bullet 2 * n\}$

is shorthand for

evens $== \{n : \mathbb{Z} | T \bullet 2 * n\}$.

The empty set

The emptyset $\emptyset$ (or $\{\}$) means

$\{n : \mathbb{Z} | F \bullet n\}$.

Exercise: Is $\{n : \mathbb{Z} | F \bullet n\}$ equal to $\{n : \mathbb{Z} | F \bullet 2 * n\}$? Why?

Sets vs Types

Sets and types are related; they both 'collect' elements.

Types are primitive. Sets are defined. But there is some overlap:
Given $\mathbb{Z}$, we could define:

$$\begin{aligned} \mathbb{N} &== \{n : \mathbb{Z} | n \geq 0 \bullet n\} : \mathbb{P}\mathbb{N} \\ \mathbb{N}_1 &== \{n : \mathbb{Z} | n \geq 1 \bullet n\} : \mathbb{P}\mathbb{N} \end{aligned}$$

You can do exercise 3.1 of "The essence of Z" now.

That's it for lecture 2!