Important mathematical jargon : Sets

Very roughly, sets are the mathematicians' data structures.

Informally, we will consider a *set* as a (well-defined, unordered) collection of mathematical objects, called the *elements* (or *members*) of the set.

Notation: $x \notin A$.

Set membership

The symbol '$\in$' known as the *set membership* predicate is central to the theory of sets, and its purpose is to build statements of the form

$$x \in A$$

that are true whenever it is the case that the object x is an element of the set A, and false otherwise.

Defining sets

singleton

The set	of even primes	is	$\{2\}$
	of booleans		$\{\,\mathbf{true}\,,\ \mathbf{false}\,\}$
	$[-2..3]$		$\{-2\,,\,-1\,,\,0\,,\,1\,,\,2\,,\,3\}$

specification

enumeration

$$\{x \in \mathbb{Z} \mid -2 \leq x \leq 3\}$$

$\underline{\underline{NB}}$: $\{\underline{true}, \underline{false}\}$

$= \{\underline{false}, \underline{true}\}$

$$a \in \{x \in A \mid P(x)\} \iff [a \in A \wedge P(a)]$$

Set comprehension

The basic idea behind set comprehension is to define a set by means of a property that precisely characterises all the elements of the set.

Notations:

$$\{x \in A \mid P(x)\} \quad , \quad \{x \in A : P(x)\}$$

$$/\!/$$

$$\{x \mid x \in A \wedge P(x)\}$$

Set equality

Two sets are equal precisely when they have the same elements

Examples:

- $\{x \in \mathbb{N} : 2 \mid x \wedge x \text{ is prime}\} = \{2\}$
- For a positive integer m,
$$\{x \in \mathbb{Z} : m \mid x\} = \{x \in \mathbb{Z} : x \equiv 0 \pmod{m}\}$$
- $\{d \in \mathbb{N} : d \mid 0\} = \mathbb{N}$

$= \{d \in \mathbb{N} : \underline{\text{true}}\}$

Equivalent predicates specify equal sets:

$$\{\, x \in A \mid P(x) \,\} = \{\, x \in A \mid Q(x) \,\}$$

iff

$$\forall x.{}^{\in A}\ \ P(x) \iff Q(x)$$

Example: For a positive integer m,

$$\{\, x \in \mathbb{Z}_m \mid x \text{ has a reciprocal in } \mathbb{Z}_m \,\}$$

$$=$$

$$\{\, x \in \mathbb{Z}_m \mid 1 \text{ is an integer linear combination of } m \text{ and } x \,\}$$

Greatest common divisor

Given a natural number n, the set of its *divisors* is defined by set comprehension as follows

$$D(n) = \{ d \in \mathbb{N} : d \mid n \} \quad .$$

Example 67

1. $D(0) = \mathbb{N}$
2. $D(1224) = \left\{ \begin{array}{c} 1, 2, 3, 4, 6, 8, 9, 12, 17, 18, 24, 34, 36, 51, 68, \\ 72, 102, 136, 153, 204, 306, 408, 612, 1224 \end{array} \right\}$

Remark Sets of divisors are hard to compute. However, the computation of the greatest divisor is straightforward. :)

Going a step further, what about the *common divisors* of pairs of natural numbers? That is, the set

$$\mathrm{CD}(m, n) = \{ d \in \mathbb{N} : d \mid m \wedge d \mid n \}$$

for $m, n \in \mathbb{N}$.

$$\{ d \in \mathbb{N} : d \mid n \wedge d \mid n \}$$
$$= \{ d \in \mathbb{N} : d \mid n \}$$

Example 68

$$\mathrm{CD}(1224, 660) = \{ 1, 2, 3, 4, 6, 12 \}$$

Since $\mathrm{CD}(n, n) = \mathrm{D}(n)$, the computation of common divisors is as hard as that of divisors. But, what about the computation of the *greatest common divisor*?

Lemma 71 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $\mathrm{m} \equiv \mathrm{m}' \pmod{\mathrm{n}}$. *Then,*

$$\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \mathrm{CD}(\mathrm{m}', \mathrm{n}) \ .$$

PROOF:

given m
take $m' = m + n$
Then
$CD(m,n) = CD(m+n, n)$

given m
take $m' = m - n$
Then
$CD(m,n) = CD(m-n, n)$

<u>Assume</u> $\boxed{m \equiv m' \pmod{n}}$ (*) $\Longleftrightarrow$ $m - m' = k \cdot n$ for an int k.

$$CD(m,n) \overset{?}{=} CD(m',n) = \{d \in \mathbb{N} : d \mid m' \wedge d \mid n\}$$

$$\| $$

$$\{d \in \mathbb{N} : d \mid m \wedge d \mid n\}$$

iff $\boxed{\forall d \in \mathbb{N}.\ (d \mid m \wedge d \mid n) \Longleftrightarrow (d \mid m' \wedge d \mid n).}$?

Let $d \in \mathbb{N}$.

$(\Rightarrow)$ <u>Assume</u>: ③ $d \mid m$ and ④ $d \mid n$

<u>RTP</u> ①: $d \mid m' \overset{\text{by}(*)}{=\!=} m + (-k) \cdot n$

So ③ & ④ imply ①.

② <u>RTP</u>: $d \mid n$

Holds by ④.

$(\Leftarrow)$

Analogous.

$\boxtimes$

Lemma 73 *For all positive integers* m *and* n,

$$\mathrm{CD}(m,n) = \begin{cases} \mathrm{D}(n) & \text{, if } n \mid m \\ \mathrm{CD}\big(n, \mathrm{rem}(m,n)\big) & \text{, otherwise} \end{cases}$$

① If $n \mid m$ then $m = k \cdot n$ for an int k.

$\mathrm{CD}(m,n) = \mathrm{CD}(k \cdot n, n) = \mathrm{D}(n)$.

② If $n \nmid m$ Then $\mathrm{rem}(m,n) \neq 0$.

$\mathrm{rem}(m,n) \equiv m \pmod n$

$\mathrm{CD}(m,n) = \mathrm{CD}(n, \mathrm{rem}(m,n))$.

Lemma 73 *For all positive integers* m *and* n*,*

$$\mathrm{CD}(m,n) = \begin{cases} \mathrm{D}(n) & \text{, \textit{if} } n \mid m \\ \mathrm{CD}\big(n, \mathrm{rem}(m,n)\big) & \text{, \textit{otherwise}} \end{cases}$$

Since a positive integer n is the greatest divisor in $\mathrm{D}(n)$, the lemma suggests a recursive procedure:

$$\mathrm{gcd}(m,n) = \begin{cases} n & \text{, if } n \mid m \\ \mathrm{gcd}\,\big(n, \mathrm{rem}(m,n)\big) & \text{, otherwise} \end{cases}$$

$$\begin{bmatrix} \mathrm{gcd}(n, m-n) & \text{if } m \geq n \\ \mathrm{gcd}(m, n-m) & \text{if } n \geq m \end{bmatrix}$$

for computing the *greatest common divisor*, of two positive integers m and n. This is

Euclid's Algorithm

gcd

```
fun gcd( m , n )
  =  let
       val ( q , r ) = divalg( m , n )
     in
       if r = 0 then n
       else gcd( n , r )
     end
```

Example 74 ($\mathrm{gcd}(13, 34) = 1$)

$$\begin{aligned}
\mathrm{gcd}(13, 34) &= \mathrm{gcd}(34, 13) \\
&= \mathrm{gcd}(13, 8) \\
&= \mathrm{gcd}(8, 5) \\
&= \mathrm{gcd}(5, 3) \\
&= \mathrm{gcd}(3, 2) \\
&= \mathrm{gcd}(2, 1) \\
&= 1
\end{aligned}$$

NB If $\mathtt{gcd}$ terminates on input (m, n) with output $\mathtt{gcd}(m, n)$ then $\mathrm{CD}(m, n) = \mathrm{D}\big(\mathtt{gcd}(m, n)\big)$.

CD(m,n) may be expressed as the divisors of a unique number.

Proposition 75 *For all natural numbers* m, n *and* a, b*, if* $\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \mathrm{D}(\mathrm{a})$ *and* $\mathrm{CD}(\mathrm{m}, \mathrm{n}) = \mathrm{D}(\mathrm{b})$ *then* $\mathrm{a} = \mathrm{b}$*.*

Idea: $CD(m,n) = D(a)$, $CD(m,n) = D(b)$ $\Longrightarrow$ $a \mid b$ and $b \mid a \Longrightarrow a = b$.

Proposition 75 *For all natural numbers* m, n *and* a, b, *if* $\mathrm{CD}(m,n) = \mathrm{D}(a)$ *and* $\mathrm{CD}(m,n) = \mathrm{D}(b)$ *then* $a = b$.

Proposition 76 *For all natural numbers* m, n *and* k, *the following statements are equivalent:*

1. $\mathrm{CD}(m,n) = \mathrm{D}(k)$.
2.
   - $k \mid m \;\wedge\; k \mid n$, *and*
   - *for all natural numbers* d, $d \mid m \;\wedge\; d \mid n \implies d \mid k$.

defines greatest common divisors.

(1) $\forall d \in \mathbb{N}.\ (d \mid m \wedge d \mid n) \iff (d \mid k)$

(2) (i) $k \mid m \wedge k \mid n$

(ii) $\forall d \in \mathbb{N}.\ (d \mid m \wedge d \mid n) \implies d \mid k$

Exercise:

Show equivalence.