Analysis and Verification of Software
Homework 4

due by March 17, 2015

The congruence domain consists of abstract values denoted, $a\mathbb{Z} + b$, Where $b \in \mathbb{Z}$ and $a \in \mathbb{N}$. We will call a the *modulo* and b the *remainder*.

The lattice operators $\sqcup$ and $\sqcap$ are defined as follows (due to [Gra89]).

$$
\begin{aligned}
&(a\mathbb{Z} + b) \sqcup (a'\mathbb{Z} + b') = gcd\{a, a', |b - b'|\}\mathbb{Z} + min\{b, b'\} \\
&(a\mathbb{Z} + b) \sqcap (a'\mathbb{Z} + b') = lcm\{a, a'\}\mathbb{Z} + b'' \text{ if } b \equiv b' \mod gcd\{a, a'\} \\
&(a\mathbb{Z} + b) \sqcap (a'\mathbb{Z} + b') = \perp \text{ otherwise.}
\end{aligned}
$$

where $b'' \equiv b \mod a$ and $b'' \equiv b' \mod a'$. Other cases follows from the lattice axioms.

The abstraction and concretization maps for this domain are defined as follows:

$$
\begin{aligned}
&\alpha(\{n\}) = 0\mathbb{Z} + n \\
&\alpha(M) = gcd\{|b - b'| | b, b' \in M\}\mathbb{Z} + min\{b | b \in M\} \quad \gamma(a\mathbb{Z} + b) = \{an + b | \forall n \in \mathbb{Z}\} \\
&\gamma(\top) = 1\mathbb{Z} + 0 = \mathbb{Z} \\
&\gamma(\perp) = \varnothing
\end{aligned}
$$

In words the set $\gamma(a\mathbb{Z} + b)$ contains all integers that are congruent to b modulo a.

Examples

- The element (2Z +1) represents the odd integers:
  … -7, -5, -3, -1, 1, 3, 5, 7,…
- The element (3Z +2) represents the integers:
  … -4, -1, 2, 5, 8, 11, 14,…
- The element (5Z +0) represents the integers:
  … -15, -10, -5, 0, 5, 10, 15, 20…

- The basic operators on the congruence domain are defined in the table below:

Operator	Congruence
$\sqcup$	$(a\mathbb{Z}+b)\sqcup(a'\mathbb{Z}+b') = \gcd\{a,a',b-b'\}\mathbb{Z}+\min(b,b')$
$\sqcap$	$(a\mathbb{Z}+b)\sqcap(a'\mathbb{Z}+b') = \mathrm{cond}(b\equiv b' \bmod \gcd(a,a'), \mathrm{lcm}(a,a')\mathbb{Z}+b'', \perp)$
$\sqsubseteq$	$(a\mathbb{Z}+b)\sqsubseteq(a'\mathbb{Z}+b') \Leftrightarrow a'\vert a$ and $b\equiv b' \bmod a'$
$\hat{+}$	$(a\mathbb{Z}+b)\hat{+}(a'\mathbb{Z}+b') = \gcd(a,a')\mathbb{Z}+(b+b')$
Elements	
$\top$	$\mathbb{Z}$ (that is, $a=1, b=0$)
$\perp$	$\varnothing$
Galois connection	
α	$\alpha(k) = 0\mathbb{Z}+k$
γ	$\gamma(a\mathbb{Z}+b) = \{ak+b \vert k\in\mathbb{Z}\}$ if $a\neq 0$ $\gamma(a\mathbb{Z}+b) = \{b\}$ if $a=0$

Let $a\mathbb{Z}+b$ and $a'\mathbb{Z}+b'$ be two non-bottom abstract values. Then

$$(a\mathbb{Z}+b)(a'\mathbb{Z}+b') = gcd\{aa', ab', a'b\}\mathbb{Z}+bb'$$

is a correct approximation of multiplication.

Exercise 1

- Depict the Venn diagram of the congruence domain.
  Its elements are (aZ+b) where if a != 0, then b<a.

  (of course, as it is an infinite domain, you can just represent a part of it!)

- For each operation (sum, difference, multiplication, lub, and glb) discuss the result of the application of the definition above to the case (13Z + 5) and (5Z + 2)

Exercise 2

- Is the domain of congruences a complete lattice?

If your answer is YES, prove it!

If your answer is NO, show a counterexample!

Exercise 3

- Does the domain of congruences satisfy the ascending chain condition ACC?

If your answer is YES, prove it!

If your answer is NO, show a counterexample!

Exercise 4

- Consider the following program:

```
f(x) =
    y=1
    while (x > 0) {
        y = x * y
        x = x - 1
    }
```

- Compute the concrete semantics of this program, and its abstract semantics on the congruence domain.