

# Correction

## MPRI 2-6

Antoine Miné

October 1, 2018

### Problem 1

1. The concrete evaluation gives:

$$\begin{aligned}
 & \text{wrap}[-128, 127](\text{wrap}[0, 255](\{-1, 0, 1\}) + \text{wrap}[0, 255](\{-1, 0, 1\})) \\
 = & \text{wrap}[-128, 127](\{0, 1, 255\} + \{0, 1, 255\}) \\
 = & \text{wrap}[-128, 127](\{0, 1, 2, 255, 256, 510\}) \\
 = & \{-2, -1, 0, 1, 2\}
 \end{aligned}$$

2. We define the optimal  $\text{wrap}[\ell, h]_i^\sharp$  as:

$$\begin{aligned}
 & \text{wrap}[\ell, h]_i^\sharp([a, b]) \\
 = & \alpha_i(\text{wrap}[\ell, h]_i^\sharp(\gamma_i([a, b]))) \\
 = & [\min \{ \text{wrap}[\ell, h](v) \mid v \in [a, b] \}, \max \{ \text{wrap}[\ell, h](v) \mid v \in [a, b] \}]
 \end{aligned}$$

where  $\alpha_i$  and  $\gamma_i$  are the interval abstraction and the interval concretization.

We then have two cases:

- either  $a$  and  $b$  are contained in a single interval of the form  $[\ell + h] + k(h - \ell + 1)$ , i.e., if  $\exists k : \ell + k(h - \ell + 1) \leq a \leq b \leq h + k(h - \ell + 1)$ . In that case,  $\text{wrap}[\ell, h]_i^\sharp([a, b]) = [a - k(h - \ell + 1), b - k(h - \ell + 1)] = [\text{wrap}[\ell, h](a), \text{wrap}[\ell, h](b)]$ ;
- otherwise,  $\text{wrap}[\ell, h]_i^\sharp([a, b]) = [\ell, h]$ , as the interval  $[a, b]$  contains both a point  $x$  such that  $\text{wrap}[\ell, h](x) = \ell$  and a point  $y$  such that  $\text{wrap}[\ell, h](y) = h$ .

The operator is exact if and only if:

- either we are in the first case:  $\exists k : \ell + k(h - \ell + 1) \leq a \leq b \leq h + k(h - \ell + 1)$ ;
- or  $b - a \geq h - \ell$ , which implies  $\{ \text{wrap}[\ell, h](v) \mid v \in [a, b] \} = [\ell, h]$  in the concrete anyway.

An example of non-exact application of the operator is  $\text{wrap}[0, 255]^\sharp([-1, 0]) = [0, 255]$  as, in the concrete, we would get the set  $\{0, 255\}$ .

3. We get:

$$\begin{aligned}
 & \text{wrap}[-128, 127]_i^\sharp(\text{wrap}[0, 255]_i^\sharp(x^\sharp) +_i^\sharp \text{wrap}[0, 255]_i^\sharp(y^\sharp)) \\
 = & \text{wrap}[-128, 127]_i^\sharp(\text{wrap}[0, 255]_i^\sharp([-1, 1]) +_i^\sharp \text{wrap}[0, 255]_i^\sharp(y[-1, 1])) \\
 = & \text{wrap}[-128, 127]_i^\sharp([0, 255] +_i^\sharp [0, 255]) \\
 = & \text{wrap}[-128, 127]_i^\sharp([0, 510]) \\
 = & [-128, 127]
 \end{aligned}$$

The concrete is, by question 1,  $\{-2, -1, 0, 1, 2\}$ . Note that it can be exactly represented as an interval  $[-2, 2]$ , yet, the evaluation of the expression in the interval domain gives a much coarser result:  $[-128, 127]$ . Hence, the abstract result is neither exact nor optimal.

This imprecision is caused by the accumulated loss of precision due to applying several optimal but non-exact operators in sequence (in general, the composition of optimal but non-exact operators is not an optimal operator). In particular, the first applications of  $\text{wrap}[0, 255]_i^\sharp$  results in a non-recoverable loss of precision.

4. The set of values  $V \stackrel{\text{def}}{=} \{0, 1, 4\}$  can be abstracted both as  $x^\sharp \stackrel{\text{def}}{=} [0, 1] + 3\mathbb{Z}$  and as  $y^\sharp \stackrel{\text{def}}{=} [0, 1] + 4\mathbb{Z}$ . Moreover, both abstract values are minimal in  $\mathcal{D}_m$ , i.e., no  $z^\sharp$  such that  $\gamma_m(z^\sharp) \subsetneq \gamma_m(x^\sharp)$  or  $\gamma_m(z^\sharp) \subsetneq \gamma_m(y^\sharp)$  can satisfy  $V \subseteq \gamma_m(z^\sharp)$ . If it existed,  $\alpha_m$  would allow constructing a *unique* minimal element  $\alpha_m(V)$  overapproximating  $V$ .
5. To design an abstraction  $+_m^\sharp$  of  $+$  in  $\mathcal{D}_m$ , we add separately the interval component and the modular component:

$$([a_1, b_1] + k_1\mathbb{Z}) +_m^\sharp ([a_2, b_2] + k_2\mathbb{Z}) \stackrel{\text{def}}{=} [a_1 + a_2, b_1 + b_2] + \text{gcd}(k_1, k_2)\mathbb{Z}$$

The operator is sound because, given  $x_1 = c_1 + k_1n_1$ ,  $x_2 = c_2 + k_2n_2$  where  $c_1 \in [a_1, b_1]$  and  $c_2 \in [a_2, b_2]$ , we have  $x_1 + x_2 = (c_1 + c_2) + (k_1n_1 + k_2n_2)$ , where  $c_1 + c_2 \in [a_1 + a_2, b_1 + b_2] = [a_1, b_1] + [a_2, b_2]$  and  $k_1n_1 + k_2n_2 \in k_1\mathbb{Z} + k_2\mathbb{Z} = \text{gcd}(k_1, k_2)\mathbb{Z}$ . Note that, in this definition,  $\text{gcd}$  is extended to  $\mathbb{N}$  by defining  $\forall x : \text{gcd}(0, x) = \text{gcd}(x, 0) = x$  (similarly to the simple congruence domain seen in the course).

For  $\text{wrap}[\ell, h]_m^\sharp([a, b] + k\mathbb{Z})$  we consider two different cases:

- (a) when the result, in the concrete, can be exactly represented as an interval, we return this interval; this can be checked by ensuring that  $[a, b] + k\mathbb{Z}$  does not cross any boundary in  $\ell + (h - \ell + 1)\mathbb{Z}$ , i.e., that  $[a, b]$  does not cross any boundary in  $\ell + (h - \ell + 1)\mathbb{Z} + k\mathbb{Z} = \ell + \text{gcd}(k, h - \ell + 1)\mathbb{Z}$ ;
- (b) otherwise, we keep the interval component intact and adjust the modular component so that the result corresponds to the argument modulo  $h - \ell + 1$ ; i.e., we add  $(h - \ell + 1)\mathbb{Z}$  to  $[a, b] + k\mathbb{Z}$  to get  $[a, b] + \text{gcd}(h - \ell + 1, k)\mathbb{Z}$ .

We get:

$$\begin{aligned} \text{wrap}[\ell, h]_m^\sharp([a, b] + k\mathbb{Z}) &\stackrel{\text{def}}{=} \\ &\begin{cases} [\text{wrap}[\ell, h](a), \text{wrap}[\ell, h](b)] + 0\mathbb{Z} & \text{if } (\ell + k'\mathbb{Z}) \cap [a + 1, b] = \emptyset \\ [a, b] + k'\mathbb{Z} & \text{otherwise} \end{cases} \\ \text{where } k' &\stackrel{\text{def}}{=} \text{gcd}(k, h - \ell + 1) \end{aligned}$$

In our example, both applications of  $\text{wrap}[0, 255]_m^\sharp$  exercise the second case of the definition, while the application of  $\text{wrap}[-128, 127]_m^\sharp$  exercises the first case. We get:

$$\begin{aligned} &\text{wrap}[-128, 127]_m^\sharp(\text{wrap}[0, 255]_m^\sharp(x^\sharp) +_m^\sharp \text{wrap}[0, 255]_m^\sharp(y^\sharp)) \\ &= \text{wrap}[-128, 127]_m^\sharp(\text{wrap}[0, 255]_m^\sharp([-1, 1] + 0\mathbb{Z}) +_m^\sharp \text{wrap}[0, 255]_m^\sharp(y[-1, 1] + 0\mathbb{Z})) \\ &= \text{wrap}[-128, 127]_m^\sharp([-1, 1] + 256\mathbb{Z} +_m^\sharp [-1, 1] + 256\mathbb{Z}) \\ &= \text{wrap}[-128, 127]_m^\sharp([-2, 2] + 256\mathbb{Z}) \\ &= [-2, 2] \end{aligned}$$

Hence, the result is optimal.

## Problem 2

1. In the concrete, the set  $X \subseteq \mathbb{R}$  of possible values for the variable  $X$  is given by the smallest solution of the equation:

$$X = \{0\} \cup \{ \alpha x + b \mid x \in X, b \in [0, \beta] \}$$

which can be computed using Kleene iterations as:

$$X = \cup_i F^i(\emptyset) \text{ where } F(S) \stackrel{\text{def}}{=} \{0\} \cup \{ \alpha x + b \mid x \in S, b \in [0, \beta] \}$$

We can prove by recurrence on  $i$  that  $F^i(\emptyset) = [0, \sum_{k < i} \alpha^k \beta]$ . The limit of this interval is the following interval, open at its upper bound:  $\cup_i F^i = [0, \sum_k \alpha^k \beta]$ . We have two cases:

- (a) if  $0 \leq \alpha < 1$ , then the limit is  $[0, m[$  where  $m \stackrel{\text{def}}{=} \beta / (1 - \alpha)$ ;
- (b) if  $\alpha \geq 1$ , then the limit is  $[0, +\infty[$ .

In the following, we will consider only the first case.

2. An interval  $[0, m']$  is an inductive invariant if and only if it is a post-fixpoint of  $F$ , i.e.:  $F([0, m']) \subseteq [0, m']$ . As  $F([0, m']) = [0, \alpha m' + \beta]$ , we deduce that  $[0, m']$  is an inductive invariant if and only if  $\alpha m' + \beta \leq m'$ , i.e.,  $m' \geq \beta / (1 - \alpha) = m$ .
3. An analysis using the interval domain and the widening with threshold set  $T$  will find the smallest interval inductive invariant whose upper bound is in  $T$ . By the answer to the previous question, it will thus find an interval of the form  $[0, m']$  where  $m' \stackrel{\text{def}}{=} \min \{ m' \in T \mid m' \geq \beta / (1 - \alpha) \}$ .

In order to find a bounded interval invariant, it is necessary and sufficient to ensure that  $T$  contains a value greater than or equal to  $\beta / (1 - \alpha)$  and strictly smaller than  $+\infty$ .

The most precise invariant representable in the interval domain is  $[0, \beta / (1 - \alpha)]$  (as we cannot represent open intervals). In order to find the most precise interval invariant, it is necessary and sufficient to have  $\beta / (1 - \alpha) \in T$ .

4. Assume that the result of an interval analysis is the interval  $[0, a]$  where  $a \neq +\infty$ .  
A first decreasing iteration will give  $F([0, a]) = [0, \alpha a + \beta]$ . We know, by the previous question that  $a \geq \beta / (1 - \alpha)$ ; this implies  $a(1 - \alpha) \geq \beta$  and then  $a \geq \alpha a + \beta$ . We thus get  $F([0, a]) \subseteq [0, a]$ . When the invariant is not optimal, i.e.,  $a > \beta / (1 - \alpha)$  the inclusion is strict. By using decreasing iterations, we can compute a sequence  $F^i([0, a])$  that converges to the optimal invariant  $[0, \beta / (1 - \alpha)]$ . The decreasing sequence of intervals is infinite, so, a narrowing must be used to converge in finite time (possibly to an interval between the optimal  $[0, \beta / (1 - \alpha)]$  and the original invariant found  $[0, a]$ ).

5. The first increasing iterates in the interval domain are:

$$\begin{aligned} F^0(\emptyset) &= \emptyset \\ F^1(\emptyset) &= [0, 0] \\ F^2(\emptyset) &= [0, \beta] \\ F^3(\emptyset) &= [0, \alpha\beta + \beta] \end{aligned}$$

Denoting  $x_i$  the upper bound of  $F^i(\emptyset)$ , we get that  $\beta = x_2$  and  $\alpha = (x_3 - \beta)/\beta = x_3/x_2 - 1$ . The exact concrete bound is then  $\beta/(1 - \alpha) = (x_2)^2/(2x_2 - x_3)$ .

We can modify the classic interval widening to check, after iteration 3, the stability of  $(x_2)^2/(2x_2 - x_3)$ . The new widening takes, as parameter, in addition to the two last iterates, the iteration count  $i$ . More precisely, the increasing sequence of intervals computed will now be  $X_{i+1} = X_i \nabla_i F(X_i)$  where, at iteration  $i$ , the widening is defined as:

$$[a, b] \nabla_i [c, d] \stackrel{\text{def}}{=} \begin{cases} [c, d] & \text{if } c \leq a = b \leq d \\ [0, b^2/(2b - d)] & \text{if } a = c = 0 \wedge b^2/(2b - d) \geq b, d \wedge i = 2 \\ [a, b] \nabla [c, d] & \text{otherwise} \end{cases}$$

where  $\nabla$  is the classic interval widening:

$$[a, b] \nabla [c, d] \stackrel{\text{def}}{=} \left[ \begin{cases} a & \text{if } a \leq c \\ -\infty & \text{otherwise} \end{cases}, \begin{cases} b & \text{if } b \geq d \\ +\infty & \text{otherwise} \end{cases} \right]$$

The first case  $c \leq a = b \leq d$  ensures that, at iteration 1, when the upper bound goes from 0 to  $\beta$ , it is not immediately widened to  $+\infty$ . The second case ensures that, at iteration 2, the limit  $\beta/(1 - \alpha) = b^2/(2b - d)$  is chosen as upper bound, if it is sound (test  $a = c = 0 \wedge b^2/(2b - d) \geq b, d$ ). The soundness of  $\nabla$  completes the soundness proof of  $\nabla_i$ . To prove the termination, it is sufficient to remark that a strictly increasing sequence will keep applying  $\nabla$  after a certain iterate, and so, the sequence terminates by the termination property of  $\nabla$ .