DM #4 — Correction de l'algorithme du PGCD binaire d'automne (avec solutions)

Dans tout cet exercice, bien que ce ne soit pas vraiment nécessaire, on pourra supposer si l'on veut que les calculs arithmétiques ont lieu en précision arbitraire (« dans $\mathbb{N}$ »).

On souhaite prouver la correction totale d'un algorithme de *PGCD binaire*. On commence par analyser un type de boucle apparaissant dans l'algorithme, **où l'on suppose que la valeur initiale de la variable `a` est strictement positive** :

```
1 while (a % 2 == 0)
2 {
3     a = a / 2;
4 }
```

où `a` est de type `unsigned`.
On note a et a' les valeurs prises par la variable `a` en début et en fin d'une itération de la boucle ci-dessus.

1. Prouvez l'invariant de boucle $\mathcal{I}_1 : a > 0$.

Initialisation : Immédiate, par hypothèse sur `a`.
Conservation : On suppose $\mathcal{I}_1$ vrai en début d'une itération. On a donc $a > 0$ (par $\mathcal{I}_1$) et $a \equiv 0 \mod 2$ (par la condition de boucle), d'où $a \geq 2$ et $a' = a \div 2 \geq 1$. La propriété est conservée.

2. Montrez que a est un variant de cette boucle.

La variable `a` est de type `unsigned`, et il s'ensuit que a est toujours un entier.
Minoration : par $\mathcal{I}_1$, a est minoré par une constante.
Stricte décroissance : on a $a' = a \div 2$ et $a > 0$, d'où $a' < a$.

On définit la *valuation 2-adique* d'un entier naturel non nul n, notée $v_2(n)$, comme le nombre d'occurrences du facteur 2 dans la décomposition de n en facteurs premiers. Autrement dit, $v_2(n)$ est l'entier naturel k (éventuellement nul) le plus grand tel que 2^k divise n.
Soit α, α' les valeurs de `a` avant et après l'exécution de la boucle ci-dessus, on veut montrer que $\alpha' = \alpha \div 2^{v_2(\alpha)}$.
Autrement dit, α' est égal à α dont on a « supprimé » tous les éventuels facteurs 2.
Pour montrer cela avec un invariant, on introduit une variable « fantôme » `i` (dont on note i et i' les valeurs en début et fin d'itération) dont le but est de compter le nombre d'itérations dans la boucle. Cette boucle modifiée est alors :

```
1 unsigned i = 0;
2 while (a % 2 == 0)
3 {
4     a = a / 2;
5     i = i + 1;
6 }
```

3. Prouvez l'invariant $\mathcal{I}_3$ suivant : $a \times 2^i = \alpha$

Initialisation : Avant entrée dans la boucle on a $i = 0$ et $a = \alpha$: $\mathcal{I}_3$ est vrai.
Conservation :

$$
\begin{aligned}
a &= 2 \times a' && \text{condition d'entrée \& ligne 4} \\
i' &= i + 1 && \text{ligne 5} \\
a' \times 2^{i'} &= a' \times 2^{i+1} && \text{ci dessus} \\
&= a \times 2^i && \text{ci dessus} \\
&= \alpha && \text{par } \mathcal{I}_3
\end{aligned}
$$

4. Conclure.

Par la condition de sortie de boucle et $\mathcal{I}_1$ on a que α' est non divisible par deux et strictement positif, et par $\mathcal{I}_3$ on a $\alpha' \times 2^i = \alpha$. Par la définition de la valuation 2-adique on a alors $v_2(\alpha) = i$, et le résultat suit.

L'algorithme du PGCD binaire que l'on souhaite analyser utilise en réalité la suite de trois boucles suivantes,

```
1  while ((a % 2 == 0) && (b % 2 == 0))
2  {
3      r = r * 2;
4      a = a / 2;
5      b = b / 2;
6  }
7  while (a % 2 == 0)
8  {
9      a = a / 2;
10 }
11 while (b % 2 == 0)
12 {
13     b = b / 2;
14 }
```

où l'on suppose les variables `a`, `b` et `r` préalablement déclarées, **et `a` et `b` de valeurs strictement positives**. On note α, β, ρ les valeurs initiales de ces variables avant la première boucle, α', β', ρ' leur valeur à la fin de celle-ci, α'', β'', ρ'' à la fin de la seconde, et α''', β''', ρ''' à la fin de la troisième.
L'objectif va être de montrer que :

— $\alpha''' = \alpha \div 2^{v_2(\alpha)}$
— $\beta''' = \beta \div 2^{v_2(\beta)}$
— $\rho''' = \rho \times 2^{\min(v_2(\alpha), v_2(\beta))}$

On commence par la dernière égalité, en constatant que $\rho''' = \rho'$ et qu'il suffit donc d'analyser la première boucle.

5. Montrez cette égalité, en suivant la même approche qu'aux questions 1 à 4.

On réutilise les mêmes notations qu'aux questions précédentes, étendues à la variable `r`.
La terminaison de la boucle peut se prouver en utilisant indifféremment a ou b comme variant ; la preuve est identique à celle des questions précédentes.
Pour prouver la propriété recherchée, on introduit à nouveau une variable fantôme `i` qui compte le nombre d'itérations effectuées dans la boucle. On a alors l'invariant $\mathcal{I}_5 : r = \rho \times 2^i$ dont l'initialisation est évidente et la conservation se prouve par :

$$\begin{aligned} i' &= i+1 && \text{par définition en tant que variable fantôme} \\ r' &= 2 \times r && \text{ligne 3} \\ &= 2 \times \rho \times 2^i && \text{par } \mathcal{I}_5 \\ &= \rho \times 2^{i'} \end{aligned}$$

Il s'ensuit que $\rho' = \rho \times 2^i$ avec i le nombre d'itérations effectuées dans la boucle, et il suffit de montrer que $i = \min(v_2(\alpha), v_2(\beta))$ pour pouvoir conclure. Pour cela on observe que les invariants $a \times 2^i = \alpha$ et $b \times 2^i = \beta$ sont également valides pour cette boucle (les preuves sont *exactement* les mêmes qu'aux questions précédentes). Par la condition de sortie de boucle on a $v_2(\alpha') = 0$ ou $v_2(\beta') = 0$; supposons sans perte de généralité que $v_2(\alpha') = 0$, alors $i = v_2(\alpha)$. Si $v_2(\beta') = 0$ on a aussi $i = v_2(\beta) = v_2(\alpha) = \min(v_2(\alpha), v_2(\beta))$, sinon $\beta' = \beta \div 2^i$ est divisible par 2 et $v_2(\beta) > i$; on peut conclure dans tous les cas.

6. On note i le nombre d'itérations effectuées par la première boucle. Montrez que $\alpha' \times 2^i = \alpha$ et $\beta' \times 2^i = \beta$.

Déjà fait ci-dessus.

7. Montrez que la seconde boucle termine.

On a déjà montré que la première boucle terminait. Celle-ci admet un invariant similaire à $\mathcal{I}_1$, prouvé de façon identique, et il s'ensuit que $\alpha' > 0$. La seconde boucle possède elle aussi ce même invariant, dont on vient de prouver l'initialisation. Il s'ensuit que a est un variant.

8. On note j le nombre d'itérations effectuées par la seconde boucle. Montrez que $\alpha'' \times 2^j = \alpha'$.

On procède exactement comme précédemment, *via* un invariant $a \times 2^j = \alpha'$ utilisant une variable fantôme j.

9. Montrez qu'on a alors $\alpha'' = \alpha \div 2^{v_2(\alpha)}$.

De $\alpha'' \times 2^j = \alpha'$ et $\alpha' \times 2^i = \alpha$ on déduit $\alpha'' \times 2^j \times 2^i = \alpha$. Par la condition de sortie de boucle on a que α'' n'est pas divisible par deux et est strictement positif, ce qui permet de conclure que $v_2(\alpha) = i + j$, ce qui donne l'égalité recherchée.

10. Conclure.

On a $\alpha''' = \alpha''$ ce qui permet d'obtenir $\alpha''' = \alpha \div 2^{v_2(\alpha)}$, et l'égalité $\beta''' = \beta \div 2^{v_2(\beta)}$ s'obtient en procédant exactement de la même façon.

On considère maintenant la boucle principale de l'algorithme du PGCD binaire :

```
1  unsigned r = 1;
2  while (a > 0 && b > 0)
3  {
4      while ((a % 2 == 0) && (b % 2 == 0))
5      {
6          r = r * 2;
7          a = a / 2;
8          b = b / 2;
9      }
10     while (a % 2 == 0)
11     {
12         a = a / 2;
13     }
14     while (b % 2 == 0)
15     {
16         b = b / 2;
17     }
18
19     if (a < b)
20     {
21         b = b - a;
22     }
23     else
24     {
25         unsigned t = b;
26         b = a - b;
27         a = t;
28     }
29 }
```

où l'on suppose les variables `a` et `b` préalablement déclarées.
On renouvelle nos notations, et utilise a, a', a'' et b, b', b'' pour dénoter les valeurs des variables `a` et `b` au début d'une itération de la boucle, à la ligne 19, et à la fin de l'itération respectivement, ainsi que r et r' pour dénoter les valeurs de la variable `r` en début et fin d'itération.

11. Montrez que $a + b$ est un variant de la boucle principale.

Les variables `a` et `b` sont de type `unsigned`, et il s'ensuit que $a + b$ est toujours un entier.
Minoration : Par la condition de boucle, $a + b > 0$.

Stricte décroissance : Aucune des instructions entre les lignes 6 et 19 ne font croître `a` et `b`, et l'on a donc $a' \leq a$ et $b' \leq b$. On considère ensuite deux cas en fonction de la condition du `if` de la ligne 20 :

— $a' < b'$: dans ce cas $a'' = a'$ et $b'' = b' - a'$, qui est $< b' \leq b$ puisque par les arguments exposés aux questions précédentes l'on a $a' > 0$ (on pourrait également simplement observer que si $a' = 0$, alors $a' < a$, ce qui permettrait aussi de conclure). Il s'ensuit que $a'' + b'' < a + b$.
— $a' \geq b'$: dans ce cas $a'' = b'$ et $b'' = a' - b'$; on a à nouveau $a'' + b'' < a + b$ par exactement les mêmes arguments.

12. Conclure sur la terminaison de cette boucle.

On a déjà montré aux questions précédentes que les trois boucles internes des lignes 4 à 17 terminaient à condition que $a > 0$ et $b > 0$, et ces deux conditions sont garanties par la condition d'entrée de la boucle principale. Il s'ensuit que chaque itération de la boucle principale termine, et l'existence d'un variant pour celle-ci permet de conclure.

Soit x, y deux entiers naturels, on utilise ci-dessous la notation $x \wedge y$ pour désigner le PGCD de x et y (défini comme le plus grand entier naturel k divisant x et y).

13. Montrez que $r \times a \wedge b = r' \times a' \wedge b'$.

On note $\mathcal{P}$ l'ensemble des nombres premiers, et pour tout $p \in \mathcal{P}$ on définit la *valuation p-adique* d'un entier naturel non nul n de façon analogue à la valuation 2-adique, c'est à dire que $v_p(n)$ est le plus grand entier naturel k (éventuellement nul) tel que 2^k divise n.
On a alors que les décompositions en facteurs premiers de a et b sont données par :

— $a = \prod_{p \in \mathcal{P}} p^{v_p(a)}$
— $b = \prod_{p \in \mathcal{P}} p^{v_p(b)}$

Par l'analyse conclue à la question 10 on a aussi :

— $a' = \prod_{p \in \mathcal{P} \setminus \{2\}} p^{v_p(a)}$
— $b' = \prod_{p \in \mathcal{P} \setminus \{2\}} p^{v_p(b)}$

Par définition du PGCD et ci-dessus, on a :

— $a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$
— $a' \wedge b' = \prod_{p \in \mathcal{P} \setminus \{2\}} p^{\min(v_p(a), v_p(b))}$

d'où $a \wedge b = 2^{\min(v_2(a), v_2(b))} \times a' \wedge b'$.
Enfin par la question 5 on a $r' = r \times 2^{\min(v_2(a), v_2(b))}$, ce qui permet de conclure.

14. Montrez que $a' \wedge b' = a'' \wedge b''$.

Le test de la ligne 19 garantit que chacun des calculs effectués aux lignes 21 et 26 sont exacts (sans *underflow*) ; on a alors deux cas possibles : $a'' = a'$ & $b'' = b' - a'$ ou $a'' = b'$ & $b'' = a' - b'$, et l'on peut conclure par le fait que pour $x \geq y$ entiers naturels l'on a $x \wedge y = x - y \wedge y$.

On considère enfin l'algorithme du PGCD binaire au complet :

```
1  unsigned bgcd(unsigned a, unsigned b)
2  {
3      unsigned r = 1;
4      while (a > 0 && b > 0)
5      {
6          while ((a % 2 == 0) && (b % 2) == 0)
7          {
8              r *= 2;
9              a /= 2;
10             b /= 2;
11         }
12         while (a % 2 == 0)
13         {
14             a /= 2;
15         }
```

```
16          while (b % 2 == 0)
17          {
18              b /= 2;
19          }
20
21          if (a < b)
22          {
23              b = b - a;
24          }
25          else
26          {
27              unsigned t = b;
28              b = a - b;
29              a = t;
30          }
31      }
32
33      if (a > 0)
34      {
35          return a * r;
36      }
37      else
38      {
39          return b * r:
40      }
41  }
```

15. Prouvez la correction totale de cet algorithme.

On note α et β les valeurs initiales des arguments `a` et `b`.
On va d'abord montrer la correction partielle, en utilisant l'invariant de boucle $\mathcal{I}_{15}$: $r \times a \wedge b = \alpha \wedge \beta$.
Initialisation : Triviale.
Conservation : On suppose $\mathcal{I}_{15}$ vrai en début d'une itération. En réutilisant les notations a, a', a'', b, b', b'', r, r' précédentes, la combinaison des questions 13 & 14 donne $r' \times a'' \wedge b'' = r \times a \wedge b$, ce qui par hypothèse $\mathcal{I}_{15}$ vaut $\alpha \times \beta$. La propriété est conservée.

Par $\mathcal{I}_{15}$, les valeurs r, a, b atteintes par les variables `r`, `a`, `b` en sortie de boucle sont telles que $r \times a \wedge b = \alpha \wedge \beta$. Par la condition de sortie de boucle, l'on a également $a = 0$ ou $b = 0$, et donc $a \wedge b = \max(a, b)$. Le test de la ligne 33 fait que la fonction renvoie précisément $r \times \max(a, b)$, ce qui permet de conclure quant à la correction partielle.

La boucle de la ligne 4, et donc la fonction termine par la question 12, ce qui permet de conclure quant à la correction totale.