Module I41, Licence Informatique 2

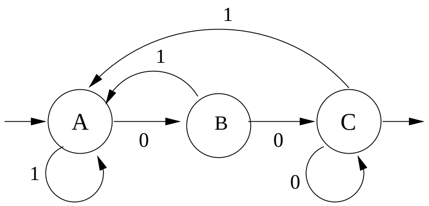
27 juillet 2006

Le sujet est composé d'un problème et deux exercices indépendants à traiter en moins de deux heures. Tous les documents sont autorisés. Vous êtes invités à remettre une copie claire, concise, sans rature ni surcharge. Il est par ailleurs inutile de recopier l'énoncé... Le barème est donné à titre indicatif, la note finale tiendra compte de la présentation générale de la copie.

EXERCICES

[1] Automates [4 pts]

Considérons l'automate $\mathcal{A}$ sur l'alphabet $A = \{0, 1\}$:



(a) Les mots ε, 1100, 1001, 1010, 1111 et 1000 sont-il reconnus par l'automate $\mathcal{A}$?

(b) Donner l'expression la plus simple du langage $00^* + \varepsilon$.

(c) Déterminer le langage $\mathcal{L}(\mathcal{A})$ par la méthode des équations de langage.

(d) Si les mots de A^* sont la représentation en base 2 des entiers naturels, quelle est la propriété arithmétique des mots reconnus par l'automate ?

```
Algorithme PGCD-Additif( a,b : entier)
données
  début
    tant que (0 < b) ∧ (0 < a) faire
        si (a < b) alors
            b ← b − a
        sinon
            a ← a − b
        finsi
    fintq
    retourner(a + b)
  fin
```

Figure 1: Algorithme du PGCD additif.

[2] Logique de Hoare [2 pts]

Soient p et q deux propositions logiques. On suppose que p et q sont deux invariants de l'instruction itérative :

`tant que` b `faire` S `ftq`

Montrer que $(p \wedge q)$ est invariant de cette boucle.

PROBLEME

Soient a et b deux entiers quelconques. On rappelle que le PGCD de a et de b est le plus grand entier d qui divise à la fois a et b. On sait qu'il existe un algorithme efficace pour le déterminer. L'objectif de ce problème concerne le calcul de PGCD en mode additif, pour des implantations sur des machines privées des opérations de réduction modulaire.

[3] Implantation [3 pts]

(a) Donner une implantation itérative en langage C de l'algorithme de la figure (1).

(b) Donner une implantation récursive en langage C de l'algorithme de la figure (1).

[4] Arithmétique [2 pts]

Soient a et b deux entiers positifs ou nul. Par définition, $\text{PGCD}(a, b) = \text{PGCD}(b, a)$.

(a) Montrer que si $a > 0$ alors $\text{PGCD}(a, 0) = a$.

(b) Montrer que si $a > b$ alors $\text{PGCD}(a, b) = \text{PGCD}(b, a - b)$.

[5] Preuve partielle [4 pts]

Soient a et b deux entiers positifs ou nul.Par définition, $\text{PGCD}(a, b) = \text{PGCD}(b, a)$.

(a) Montrer $a \geq 0$ est un invariant de boucle de l'algorithme du PGCDadditif.

(b) Est-ce que $a > 0$ est un autre invariant ?

(c) Soit γ un entier. Montrer que $\text{PGCD}(a, b) = \gamma$ invariant de boucle.

(d) Soient α et β les valeurs initiales des paramètres a et b. Faire une preuve partielle pour établir que le résultat de l'algorithme du PGCD additif est bien $\text{PGCD}(\alpha, \beta)$.

[6] Preuve d'arrêt [3 pts]

(a) Proposer un variant de boucle pertinent. PGCD additif.

(b) Faire une preuve d'arrêt.

[7] Temps de calcul [3 pts]

Soient $\alpha > 0$ et β deux entiers naturels, on note $i(\alpha, \beta)$ le nombre d'itérations de l'algorithme du PGCD additif pour initialisé par $a = \alpha$ et $b = \beta$.

(a) On suppose $\alpha > \beta$, et on note q et ρ les quotient et reste de la division euclidienne de α par β. Exprimer $i(\alpha, \beta)$ en fonction de q et $i(\beta, \rho)$.

(b) Soient q_1, q_2,... les quotients successifs, obtenus par l'algorithme d'Euclide pour calculer le PGCD des entiers α et β. Établir

$$i(\alpha, \beta) = \sum_{i=1}^{n} q_i.$$

(c) Déterminer les valeurs $0 < \beta < 144$ qui maximisent $i(144, \beta)$.

(d) Déterminer les valeurs $0 < \beta < 144$ qui minimisent $i(144, \beta)$.