Magistère d'Informatique 2007-2008
ENS de Cachan
Langages formels

TD 14

–

Fonctions séquentielles

Exercice 1

Dans cet exercice, on considère deux représentations des entiers en base 2 (ou plus généralement en base β) : la représentation *classique* (avec le bit de poids fort en premier) et la représentation *inverse* (avec le bit de poids faible en premier).

1. Donner un automate séquentiel qui réalise la multiplication par 3 en base 2 (représentation inverse).
2. Donner un automate séquentiel qui réalise la division entière par 3 en base 2 (représentation classique).
3. On définit l'opérateur comparaison comme la fonction prenant en argument deux entiers x et y en représentation inverse et qui renvoie $\top$ si $x \geq y$ et $\perp$ sinon. Donner un automate séquentiel qui réalise la comparaison (on suppose que les codages de x et y ont même longueur).
4. On définit la soustraction comme la fonction prenant deux entiers x et y en représentation inverse et qui renvoie l'entier $x - y$ en base 2 inverse si $x \geq y$ et le caractère # en dernier sinon. Donner un automate séquentiel qui réalise la soustraction.
5. Donner un automate séquentiel qui reconnaît l'ensemble des représentations classiques d'entiers vérifiant $2x + 3y \equiv 1$ [6]. De même pour $\{x \mid \exists y.\ 2x + 3y \equiv 1\ [6]\}$.

Exercice 2

1. Soit $\beta_1 : \{x, y\}^* \to A^*$ le morphisme défini par $\beta_1(x) = a$ et $\beta_1(y) = aba$. La relation β_1^{-1} est-elle une fonction séquentielle ?
2. Même question avec $\beta_2 : \{x, y, z\}^* \to A^*$ défini par $\beta_2(x) = ab$, $\beta_2(y) = abb$ et $\beta_2(z) = baab$.
3. Généralisation. Soit X un sous-ensemble fini de A^* ; X est dit *préfixe* si aucun mot de X n'est préfixe d'aucun autre mot de X. Soit $B = \{x_1, \ldots, x_n\}$ un ensemble en bijection avec X ; cette bijection induit un morphisme $\beta : B^* \to A^*$. Par définition, X est un code si ce morphisme est injectif. Un code X est dit *à délai de déchiffrage d* si quand un mot $f = x_1 \ldots x_{d+1} \in X^{d+1}$ est *préfixe* (en temps que mot de A^*) d'un mot $g = y_1 \ldots y_r \in X^*$, alors on a $x_1 = y_1$.

(a) Vérifier qu'un code préfixe est un code à délai de déchiffrage 0.

(b) Donner un exemple de code qui n'est pas à délai de déchiffrage fini.

(c) Montrer que si X est préfixe, β^{-1} est une fonction séquentielle pure.

(d) Montrer que si X est un code à délai de déchiffrage fini, β^{-1} est une fonction séquentielle.

(e) Réciproquement, montrer que si β^{-1} est une fonction séquentielle, alors X est un code à délai de déchiffrage fini.

On a ainsi démontré :
Proposition Soit $\beta : B^* \to A^*$ un morphisme. L'ensemble $X = \beta(B)$ est un code à délai de déchiffrage fini si et seulement si β^{-1} est une fonction séquentielle.

Exercice 3

On considère les fonctions affines de la forme $\psi(x_1, \ldots, x_n) = a_0 + \sum_{i=1}^{i=n} a_i x_i$ où les a_i sont des entiers naturels, et les x_i des variables à valeurs dans $\mathbb{N}$. On appelle formule atomique une formule de la forme $f(\psi_1, \psi_2)$, avec ψ_1 et ψ_2 des fonctions affines et f un opérateur de comparaison du type $<$, $\leq$, $=$, $>$, $\geq$ ou $\equiv [b]$ pour $b \in \mathbb{N}$ fixé.

On définit l'ensemble des formules de Presbürger comme l'ensemble obtenu à partir des formules atomiques en le fermant par combinaison booléenne (opérateurs $\wedge$, $\vee$ et $\neg$) et par quantification existentielle ($\exists$) et universelle ($\forall$).

L'objectif de cet exercice est de montrer que les formules de Presbürger sont reconnaissables par automate, *i.e.* que pour toute formule de Presbürger ϕ, il existe un automate fini $\mathcal{A}_\phi$ qui reconnaisse exactement les codages en binaire renversés satisfaisant la formule ϕ.

1. Montrer que toute fonction affine est séquentielle.
2. Montrer que l'on peut supposer que l'opérateur de comparaison est toujours $=$.
3. Etant données deux fonctions affines ψ_1 et ψ_2 à variables $x_1, \ldots, x_n$ et $y_1, \ldots, y_m$, montrer que le langage

   $$L := \{(\overline{x_1}^2, \ldots, \overline{x_n}^2, \overline{y_1}^2, \ldots, \overline{y_m}^2) \mid \psi_1(\overline{x_1}^2, \ldots, \overline{x_n}^2) = \psi_2(\overline{y_1}^2, \ldots, \overline{y_m}^2)$$

   est reconnaissable ($\overline{u}^2$ dénote le codage binaire renversé de $u \in \mathbb{N}$).
4. Conclure.