École polytechnique — X2013 — INF412 Fondements de l'informatique

PC5 notée

Sujet proposé par David Monniaux et Bruno Salvy

Cet énoncé comporte deux parties indépendantes et qui pourront être résolues dans n'importe quel ordre.

Dans chaque partie, on pourra, pour répondre à une question, admettre les résultats dont on demande la démonstration aux questions *précédentes*.

Les correcteurs vous remercient d'avance d'écrire lisiblement.

1 Modèles des réels et des complexes

On s'intéresse dans un premier temps aux corps réels ordonnés. La signature est $\mathcal{L} := (\{0,1\},\{+,-,\times\},\{<,=\})$ et les modèles considérés sont égalitaires (l'égalité y est interprêtée comme l'égalité).

Question 1.1. *Donner une formule close sur $\mathcal{L}$ qui soit vraie pour le corps des réels $\mathbb{R}$, mais fausse pour le corps des rationnels $\mathbb{Q}$.*

Question 1.2. *Montrer que les formules atomiques sur $\mathcal{L}$ sont équivalentes par les axiomes des anneaux commutatifs ordonnés (associativité, commutativité, opposé, compatibilité de l'ordre avec les opérations) à l'une des formes $P(x_1,\dots,x_n) < Q(x_1,\dots,x_n)$ ou $P(x_1,\dots,x_n) = Q(x_1,\dots,x_n)$ où P et Q appartiennent à $\mathbb{Z}[X_1,\dots,X_n]$ pour un $n \in \mathbb{N}$.*

Question 1.3. *Donner une formule sans quantificateurs sur $\mathcal{L}$, équivalente sur $\mathbb{R}$ à la formule $\exists x, ax^2+bx+c=0$. (Deux formules sont équivalentes sur une structure si elles ont même valeur de vérité pour toute affectation des variables libres.)*

Le mathématicien polonais Alfred Tarski a donné dans les années 1930–1940 un algorithme prenant en entrée une formule du premier ordre ϕ arbitraire et renvoyant en sortie une formule équivalente à ϕ, mais sans quantificateurs.

Question 1.4. *Déduire de l'existence de cet algorithme que l'on peut tester si une formule close du premier ordre est vraie sur $\mathbb{R}$.*

On dit qu'un sous-ensemble X de $\mathbb{R}^n$ est *définissable* sur une signature $\mathcal{S}$ s'il existe une formule du premier ordre à n variables $\phi(x_1,\dots,x_n)$ sur $\mathcal{S}$ telle que

$$X = \{(a_1,\dots,a_n) \in \mathbb{R}^n \mid \phi(a_1,\dots,a_n) \text{ est vraie.}\}$$

(La définissabilité dans $\mathbb{C}$ se définit de façon analogue en remplaçant $\mathbb{R}$ par $\mathbb{C}$).

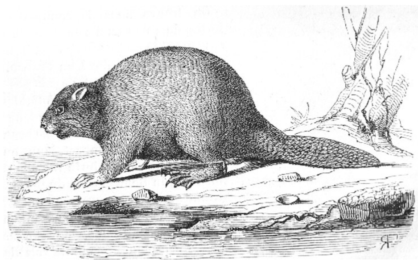
Question 1.5. *Montrer que l'ensemble des points à distance strictement inférieure à 1 de l'hyperbole d'équation $xy=1$ est définissable sur $\mathcal{L}$.*

Question 1.6. *Montrer que l'ensemble $\mathbb{Z}$ des entiers n'est pas définissable sur $\mathcal{L}$.*

Question 1.7. *Montrer que sur la signature $\mathcal{M} := (\{0,1\},\{+,-,\times,\exp\},\{\})$, l'ensemble $\mathbb{Z}$ est définissable comme sous-ensemble du corps $\mathbb{C}$ des complexes avec* exp *interprété comme l'exponentielle.*

2 Le castor affairé

La fonction du « castor affairé » (*busy beaver*) a été introduite en 1962 par Tibor Radó [1]. Considérons les machines de Turing à n états $(1 \ldots n)$, parmi lesquels on distingue un état initial 1 et un état final 0, opérant sur un seul ruban infini dans les deux directions, sur l'alphabet $\{0,1\}$ (le 0 servant de « blanc »). Chaque machine à n états est donc déterminée par une fonction qui à chaque état $1 \leq k \leq n$, et chaque valeur lue $\{0,1\}$, associe une indication de direction dans $\{\leftarrow, \rightarrow\}$, une valeur à écrire dans $\{0,1\}$ et un nouvel état dans $0 \ldots n$.



Le castor, par Alcide Raillet, 1895

Question 2.1. *Donnez le nombre $N(n)$ de machines de Turing à $n \geq 2$ états du type ci-dessus.* (On distinguera les machines identiques à renumérotation des états près, et on comptera toutes les machines, y compris celles qui sont « stupides », par exemple celles qui ont des états non initiaux sur lesquels n'arrivent aucune transition.)

Parmi ces machines, on nomme « castors à n états » les machines qui, sur une entrée entièrement vide (ruban constitué uniquement de 0), terminent (en atteignant l'état final). Le *score* d'un castor est le nombre de 1 écrits sur le ruban à la fin de l'exécution.

Question 2.2. *Montrez que l'ensemble des castors à $n \geq 2$ états est non vide.*

L'ensemble des castors à n états étant non vide (question 2.2) et fini (question 2.1), il admet donc un score maximal, noté $C(n)$. On appelle C *fonction du castor affairé.*

Question 2.3. *Montrez que C est croissante au sens large.*

Nous reprenons la définition de « calculable » de la PC4 : une machine de Turing M calcule une fonction f si, sur une bande comprenant une succession de n chiffres 1 précédés et suivis d'un zéro, avec la tête de lecture sur le chiffre le plus à gauche (le reste de la bande contenant n'importe quoi), la machine termine forcément, en laissant $f(n)$ écrit de la même façon sur la bande et sans avoir changé les valeurs écrites sur la bande à gauche de la position initiale de la tête.

Nous admettons le résultat démontré dans la PC4 que toutes les fonctions primitives récursives (donc toutes les fonctions arithmétiques usuelles) sont calculables avec cette définition, que les fonctions calculables peuvent être composées, etc.

Pour M une machine de Turing, nous notons $|M|$ son nombre d'états.

Question 2.4. *Soit E une machine de Turing calculant une fonction f_E. Prouvez que pour tout n, $C(2n+2+|E|) \geq f_E(n)$.*

Question 2.5. *Déduisez-en que C ne peut être calculable.* (On pourra supposer qu'elle l'est, considérer la fonction $n \mapsto C(3n)$, et appliquer judicieusement certains des résultats des questions précédentes.)

Références

[1] Tibor Radó. On non-computable functions. *Bell System Technical Journal*, 41(3) :877–884, May 1962.