NOMBRES RÉELS, FRACTIONS CONTINUES, ET CLASSES DE COMPLEXITÉ

Labhalla Salah, Université de Marrakech
Lombardi Henri, Université de Franche-Comté, Besançon

Résumé : Nous étudions différentes manières de présenter les nombres réels. Nous comparons ces présentations du point de vue des fonctionnelles récursives d'une part, et de celui des classes de complexité d'autre part.
L'impossibilité d'obtenir certaines fonctions sous forme de fonctionnelles récursives est en général facile à établir. Cette impossibilité peut souvent être explicitée (et renforcée) en termes de complexité:
– il existe une suite de faible complexité dont l'image est une suite non récursive
– il existe des objets de faible complexité mais dont les images sont des objets de complexité arbitrairement grande. (le plus souvent la "faible complexité" est celle en temps linéaire ou polynomial)
En outre, certaines présentations des réels équivalentes du point de vue des fonctionnelles récursives se distinguent nettement du point de vue de la complexité.
Nous faisons une étude particulière concernant les développements en fraction continue (dfc). Nous précisons exactement quelle est la partie de l'information disponible dans le dfc d'un réel x qui équivaut à l'information disponible dans sa coupure de Dedekind. Nous montrons également que la somme de 2 réels dont le dfc est calculable en temps polynomial peut être un réel dont le dfc est de complexité arbitrairement grande.
Ce travail confirme que seule une présentation des réels via des suites de rationnels explicitement de Cauchy est adaptée aux calculs avec les réels.

Mots clés : nombres réels, suites de Cauchy, coupures de Dedekind, mesure d'irrationalité, fractions continues, fonctionnelles récursives, fonctionnelles primitives récursives, fonctionnelles en temps polynomial, classes de complexité en temps, **LINTIME**, $\mathcal{P}$

Abstract : We study some representations of real numbers. We compare these representations, on the one hand from the viewpoint of recursive functionals, and of complexity on the other hand.
The impossibility of getting some fonctions as recursive fonctionals is generaly easy. This impossibility may often be explicited (and reinforced) in terms of complexity:
– existence of a sequence of low complexity whose image is not a recursive sequence
– existence of objects of low complexity but whose images have arbitrarily high time complexity (often, the "low complexity" is linear time or polynomial time)
Moreover, some presentations of real numbers that are equivalent from the view point of recursive functionals, are very distinct from the viewpoint of complexity.
We make a particular study of presentations via continued fractions (dfc). We precise exactly what part of information available in the x's dfc is equivalent to the information available in its Dedekind's cut. We show that the sum of two reals whose dfcs are polynomial time computable may be a real whose dfc has time complexity arbirarily high.
This work confirms that the unique representation of real numbers suitable for the ordinary calculus is via explicit Cauchy sequences of rationals.

Key words : real numbers, Cauchy sequences, Dedekind cuts, irrationnality measure, continued fractions, recursive functional, primitive recursive functional, polynomial time functional, Oracle Turing Machine, time complexity, **LINTIME**, $\mathcal{P}$

INTRODUCTION

La notion de réel récursif a été introduite par Turing en 1936 [**Tu**], et étudiée en détail, notamment par Specker [**Spe**] et Rice [**Ric**].
Dans l'article [**Ko1**], Ker I. Ko a introduit et étudié la notion de complexité concernant différentes représentations d'un nombre réel. Pour les présentations via les suites de Cauchy et via les coupures de Dedekind, il a défini les ensembles $\mathbb{R}_{CON}(\mathfrak{C})$ et $\mathbb{R}_{CUT}(\mathfrak{C})$, où $(\mathfrak{C})$ est une classe de complexité arbitraire. Nous utiliserons la notation $\mathbb{R}_{CONV}(\mathfrak{C})$ à la place de $\mathbb{R}_{CON}(\mathfrak{C})$.
Dans l'article [**Lab**], Labhalla a étudié la présentation via les fractions continues et a introduit les ensembles $\mathbb{R}_{CONT}(\mathfrak{C})$. Voir aussi à ce sujet [**Ko2**].

Dans cet article, nous étudions différentes présentations des nombres réels (présentations que nous notons $\mathbb{R}_{CONV}$, $\mathbb{R}_{CUT-}$, $\mathbb{R}_{CUT}$, $\mathbb{R}_{MIR}$, $\mathbb{R}_{CONT}$) en introduisant le point de vue des fonctionnelles récursives.
La présentation $\mathbb{R}_{CONV}$ est basée sur les suites de Cauchy explicitement convergentes.
Les deux présentations $\mathbb{R}_{CUT}$ et $\mathbb{R}_{CUT-}$ sont basées sur les coupures de Dedekind, et apparemment très voisines.
La présentation $\mathbb{R}_{MIR}$ est basée sur les mesures d'irrationalité.
La présentation $\mathbb{R}_{CONT}$ est basée sur les développements en fraction continue.
Nous obtenons des fonctionnelles en temps polynomial pour représenter l'identité de $\mathbb{R}$ dans les cas suivants:

$$\mathbb{R}_{CONT} \longrightarrow \mathbb{R}_{MIR} \longrightarrow \mathbb{R}_{CUT} \longrightarrow \mathbb{R}_{CONV}$$

Nous donnons une version constructive forte du théorème : «aucune partie de $\mathbb{R}_{CONV}$ n'est récursivement décidable».
Nous montrons que $\mathbb{R}_{CUT}$, $\mathbb{R}_{MIR}$ et $\mathbb{R}_{CONT}$ sont des présentations équivalentes du point de vue des fonctionnelles récursives. Par contre, les présentations $\mathbb{R}_{CUT}$ et $\mathbb{R}_{CUT-}$ ne sont pas récursivement équivalentes, et ceci bien que l'on ait : $\mathbb{R}_{CUT}(\mathfrak{C}) = \mathbb{R}_{CUT-}(\mathfrak{C})$ pour toute classe $\mathfrak{C}$ de complexité en temps.
Nous précisons en outre la complexité des fonctionnelles liant $\mathbb{R}_{MIR}$ et $\mathbb{R}_{CONT}$.
L'impossibilité d'obtenir certaines fonctions sous forme de fonctionnelles récursives est en général facile à établir. Cette impossibilité peut souvent être explicitée (et renforcée) en termes de complexité :

- il existe une suite de faible complexité dont l'image est une suite non récursive
- il existe des objets de faible complexité mais dont les images sont des objets de complexité en temps arbitrairement grande.(le plus souvent la "faible complexité" est celle en temps linéaire ou polynomial)

En outre, ce dernier point de vue permet d'établir une nette différence entre des présentations récursivement équivalentes.
Nous donnons différentes versions pour la non récursivité du test « $x \in \mathbb{Q}$? » lorsque x est dans $\mathbb{R}_{CUT}$, $\mathbb{R}_{MIR}$ ou $\mathbb{R}_{CONT}$.
Nous obtenons, pour une classe $\mathfrak{C}$ de complexité en temps arbitraire, les non-inclusions suivantes:

$$\mathbb{R}_{CUT}(\mathfrak{C}) \not\supset \mathbb{R}_{CONV}(\mathbf{LINTIME})$$
$$\mathbb{R}_{MIR}(\mathfrak{C}) \not\supset \mathbb{R}_{CUT}(\mathbf{LINTIME})$$

en outre:

$$\mathbb{R}_{CONT}(\mathcal{P}) \quad \supset \quad \mathbb{R}_{MIR}(\mathcal{P})$$

Nous obtenons également des résultats assez forts de non stabilité pour l'addition: (avec une classe $\mathcal{C}$ de complexité en temps arbitraire)

$$\mathbb{R}_{CUT}(\mathcal{C}) \quad \supset \quad \mathbb{R}_{CUT}(\mathcal{P}) + \mathbb{R}_{CUT}(\mathcal{P})$$
$$\mathbb{R}_{MIR}(\mathcal{C}) \quad \supset \quad \mathbb{R}_{MIR}(\mathcal{P}) + \mathbb{R}_{MIR}(\mathcal{P})$$
$$\mathbb{R}_{CONT}(\mathcal{C}) \quad \supset \quad \mathbb{R}_{CONT}(\mathcal{P}) + \mathbb{R}_{CONT}(\mathcal{P})$$

Concernant les développements en fraction continue (dfc), nous précisons exactement quelle est la partie de l'information disponible dans le dfc d'un réel x qui équivaut à l'information disponible dans sa coupure de Dedekind.
Tous ces résultats renforcent les résultats précédemment obtenus sur le sujet.

Cet article est la version française de [**LL1**], dont les résultats ont été annoncés en [**LL2**] et [**LL3**]. Nous avons, dans cette version française, rajouté quelques explications dans l'introduction de la section 3.2. L'étude a été poursuivie, pour les représentations du type “développement décimal illimité”, dans l'article [**LL4**].

Nous terminons cette introduction par le plan de l'article et par quelques notations que nous utiliserons dans la suite

Plan de l'article

Quelques notations

$\mathbb{N}_1$	ensemble des entiers naturels en unaire
$\mathbb{N}_1^*$	partie du précédent formée des entiers > 0
$\mathbb{N}$	ensemble des entiers naturels en binaire. Du point de vue de la complexité, $\mathbb{N}_1$ est isomorphe à la partie de $\mathbb{N}$ formée des puissances de 2
$\mathbb{Z}$	ensemble des entiers relatifs en binaire.
$\mathbb{Q}$	ensemble des rationnels présentés sous forme d'une fraction avec numérateur et dénominateur en binaire
$\mathbb{Q}^{\mathbb{N}_1}$	ensemble des suites de rationnels, où l'indice est en unaire. En général, les suites seront considérées avec un indice en unaire. Pour plus de précision nous mettons $\mathbb{N}_1$ ou $\mathbb{N}$ en exposant.
$\mathbb{R}$	ensemble "abstrait" des nombres réels.
$\mathbb{R}_{CONV}$	ensemble des réels présentés via des suites de Cauchy (cf. section 2.1).
$\mathbb{R}_{CONV}(\mathfrak{C})$	partie de $\mathbb{R}_{CONV}$ formée des objets de complexité $\mathfrak{C}$ ($\mathfrak{C}$ est une classe de complexité)
$\mathfrak{C}$-suite dans … :	(cf. fin de la section 2.1)
$\mathbb{R}_{CUT}$	ensemble des réels présentés via les coupures de Dedekind (cf. section 2.2).
$\mathbb{R}_{CUT-}$	variante de $\mathbb{R}_{CUT}$ (cf. section 2.2).
$\mathbb{R}_{MIR}$	ensemble des réels présentés via les coupures de Dedekind, mais en explicitant les relations d'inégalité stricte, c.-à-d. en précisant en outre une mesure d'irrationalité (cf. section 2.3).
$\mathbb{R}_{CONT}$	ensemble des réels présentés via les fractions continues (cf. section 2.4).
LINTIME	complexité en temps linéaire (déterministe)
$\mathfrak{P}$	complexité en temps polynomial. Nous utilisons par ailleurs les notations standard **DTIME**(f(n)) et **DSPACE**(f(n))
Pr	"complexité" primitive récursive (rappelons qu'une fonction est primitive récursive si et seulement si elle est en temps primitif récursif)
Rec	classe des fonctions récursives
dfc	développement en fraction continue
dfc pair	dfc fini d'un rationnel a/b : $[a_0; a_1, a_2, ..., a_p]$ avec p pair (donc a_p peut prendre la valeur 1)
Ent(x)	partie entière du réel x
lg(n)	longueur de l'entier n lorsqu'il est écrit en binaire
sg(x)	signe de x (–1 , 0 ou +1)
$x =_{\mathbb{A}} y$	voir fin de la section 1

1. PRÉLIMINAIRES

1.1. Rappels sur les fractions continues. (cf. [Kh])

Soit a_0 un entier et $(a_1, a_2, \ldots\ldots, a_n)$ une suite finie d'entiers strictement positifs. Nous notons par $[a_0; a_1, a_2, \ldots\ldots, a_n]$ la fraction continue finie :

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots\ldots\ldots\ldots + \cfrac{1}{a_n}}}$$

et par $[a_0; a_1, a_2, \ldots\ldots, a_n, \ldots]$ la fraction continue infinie.
Alors chaque nombre irrationnel x a une unique représentation en fraction continue infinie et chaque nombre rationnel x a une unique représentation en fraction continue finie

$$[a_0; a_1, a_2, \ldots\ldots, a_n] \text{ avec } a_n > 1 \text{ si } n \geq 1.$$

En outre $[a_0; a_1, a_2, \ldots\ldots, a_n] = [a_0; a_1, a_2, \ldots\ldots, a_n - 1, 1]$ (avec $n \geq 0$).
On en déduit que tout rationnel x a une unique représentation en fraction continue finie

$$[a_0; a_1, a_2, \ldots\ldots, a_n] \text{ avec } n \text{ pair}.$$

Dans la suite, nous abrégeons "représentation en fraction continue" par **dfc**.

Quelques résultats classiques

Soit $x := [a_0; a_1, a_2, \ldots\ldots, a_n, \ldots]$ et $p_n/q_n := [a_0; a_1, a_2, \ldots\ldots, a_n]$.
L'entier a_n s'appelle le $n^{ème}$ quotient partiel et la fraction p_n/q_n le $n^{ème}$ convergent de x .
Alors :

$$\forall\ n \geq 2 : \qquad p_n = a_n\, p_{n-1} + p_{n-2}\,,\ q_n = a_n\, q_{n-1} + q_{n-2}\,,\ q_n \geq 2^{(n-1)/2}$$

$$L_n(z) = [a_0; a_1, a_2, \ldots\ldots, a_n, z] = \frac{p_n\, z + p_{n-1}}{q_n\, z + q_{n-1}},$$

$$H_n(y) = -\frac{q_{n-1}\, y - p_{n-1}}{q_n\, y + p_n}, \qquad a_{n+1} = \mathrm{Ent}(H_n(x))\,,$$

$$\forall\ n \geq 1 \qquad \frac{1}{q_n(q_n + q_{n+1})} < \left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n\, q_{n+1}}$$

Pour tout entier $n \geq 1$ et tout rationnel a/b tel que $0 < b \leq q_n$ et $a/b \neq p_n/q_n$ on a:

$$\left| x - \frac{a}{b} \right| > \left| x - \frac{p_n}{q_n} \right|$$

Enfin, si y est compris entre x et p_n/q_n alors x et y ont le même dfc jusqu'à l'ordre n , et donc les mêmes convergents jusqu'à p_n/q_n

1.2. Fonctionnelles récursives et complexité.

Nous étudions dans l'article la complexité de certaines fonctionnelles récursives.
Il s'agit de fonctionnelles qui acceptent en entrées

- des objets "discrets" : éléments de $\mathbb{N}_1$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, ..., d'une part,
- et des objets plus complexes tels que:

éléments de $\mathbb{Q}^{\mathbb{Q}}$ ou de $\{-2,-1,0,1,2\}^{\mathbb{N}_1}$,

d'autre part.

Ces objets “complexes” interviennent à titre d'oracles pour une machine de Turing qui calcule la fonctionnelle récursive.

En sortie, la machine de Turing à oracles (MTO) fournit des objets "discrets", mais on peut obtenir par exemple une fonctionnelle de $\mathbb{Q}^{\mathbb{Q}}$ vers $\mathbb{N}^{\mathbb{N}_1}$ sous forme d'une fonctionnelle de $\mathbb{N}_1 \times \mathbb{Q}^{\mathbb{Q}}$ vers $\mathbb{N}$.

Lorsque les oracles d'une MTO fournissent des réponses dont la taille est majorée a priori, nous disons que nous sommes dans le cas "localement compact". Dans ce cas, la définition de la complexité en temps du calcul exécuté est bien connue : le temps de calcul doit être majoré, indépendamment des réponses fournies par l'oracle, par une fonction récursive S(n) où n représente la taille des entrées "discrètes": le calcul est alors dans **DTIME**(S(n)).

Lorsque les oracles d'une MTO fournissent des réponses dont la taille est a priori arbitraire, la complexité en temps de la fonctionnelle est relativement mal définie dans la littérature. Nous ne proposerons pas de définition générale, et nous nous contenterons des 3 notions suivantes, (la dernière restant en partie non précisée):

- celle de fonctionnelle récursive “tout court”
- celle de fonctionnelle (uniformément) primitive récursive (telle que donnée par S. C. Kleene dans [**IM**])
- celle de fonctionnelle (uniformément) en temps polynomial

Explicitons un minimum ces deux dernières notions.

Une fonctionnelle est (uniformément) primitive récursive si elle peut être calculée par un "programme à boucles répéter" (un "loop program" en anglais) utilisant comme seules instructions de base:

- des instructions N := $f(M_1, M_2, ..., M_k)$ où f est une fonction primitive récursive (on pourrait limiter f à quelques fonctions particulièrement simples)
- des instructions "oracle" : N := $g(M_1, M_2, ..., M_j)$ où g désigne un oracle

Les seules boucles d'un "programme à boucles répéter" sont des boucles "**Répéter** N **fois ...**" , où N est une variable du programme, et elles sont éventuellement imbriquées les unes dans les autres.

Concernant les fonctionnelles (uniformément) en temps polynomial, nous ne proposerons pas de définition, mais nous faisons les 2 remarques suivantes:

primo: les fonctionnelles en temps polynomial que nous construisons sont toujours du type très simple qui suit: elles peuvent être calculées par un programme sans aucune boucle dont les instructions de base sont les suivantes:

- des instructions N := $f(M_1, M_2, ..., M_k)$ où f est une fonction calculable en temps polynomial
- des instructions "oracle" :

  N := $g(M_1, M_2, ..., M_j)$ où g désigne un oracle
- des instructions "oracle" : N := (nombre codant la) liste des valeurs h(0), h(1), ..., h(L), où h désigne un oracle acceptant une entrée *en unaire.*

secundo: nous adoptons le critère négatif suivant: s'il existe une suite calculable en temps polynomial dont la fonctionnelle $\mathcal{F}$ donne pour image une suite non calculable en temps

polynomial, alors la fonctionnelle $\mathcal{F}$ n'est sûrement pas (uniformément) calculable en temps polynomial.
Il nous semble clair que toute définition raisonnable de la notion de fonctionnelle uniformément calculable en temps polynomial doit être cohérente avec le "primo" et le "secundo" ci-dessus.
Depuis la parution de la version anglaise, nous avons pris connaissance de la définition tout à fait raisonnable de «fonctionnelle uniformément calculable en temps polynomial» (définie comme appartenant à la classe notée **POLY**) donnée par Mike Townsend dans [**Tow**], alors que la définition proposée par Ko et Friedman dans [**KF**] présente un défaut d'uniformité évident.

Nous terminons par quelques définitions informelles utilisées dans la suite de l'article.

Définitions (plus ou moins informelles)**:**

1) Supposons qu'un ensemble "abstrait" $\mathbb{A}$ soit présenté par un ensemble $\mathcal{Q}$ "concret", c.-à-d. avec lequel la notion de fonctionnelle récursive ait un sens. Nous dirons que 2 éléments x' et x" de $\mathcal{Q}$ sont *égaux dans* $\mathbb{A}$ s'ils représentent le même élément x de $\mathbb{A}$**.** Et nous écrirons $x' =_{\mathbb{A}} x''$.

2) Supposons que 2 ensembles "abstraits" $\mathbb{A}$ et $\mathbb{B}$ soient présentés par 2 ensembles $\mathcal{Q}$ et $\mathcal{B}$ "concrets". Nous dirons qu'une fonctionnelle récursive $\mathcal{F}$ de $\mathcal{Q}$ vers $\mathcal{B}$ est *extensionnelle* ou encore qu'elle *respecte l'égalité* si elle représente une fonction f de $\mathbb{A}$ vers $\mathbb{B}$. On dit alors que la fonction f est *récursivement représentable* (dans les présentations $\mathcal{Q}$ et $\mathcal{B}$ de $\mathbb{A}$ et $\mathbb{B}$). En remplaçant "fonctionnelle récursive" par "fonctionnelle primitive récursive" ou "$\mathcal{P}$-fonctionnelle" , on obtient les notions de *fonction* **Pr**-*représentable* et de *fonction* $\mathcal{P}$-*représentable* .

3) Supposons qu'un ensemble "abstrait" $\mathbb{A}$ soit présenté par deux ensembles $\mathcal{Q}_1$ et $\mathcal{Q}_2$ "concrets". Nous dirons que 2 éléments x_1 et x_2 de $\mathcal{Q}_1$ et $\mathcal{Q}_2$ sont *égaux dans* $\mathbb{A}$ s'ils représentent le même élément x de $\mathbb{A}$. Et nous écrirons $x_1 =_{\mathbb{A}} x_2$. Nous dirons que les deux présentations sont *récursivement équivalentes* (resp. $\mathcal{P}$-*équivalentes,* **Pr**-*équivalentes*) si l'identité de $\mathbb{A}$ est représentable par une fonctionnelle récursive de $\mathcal{Q}_1$ vers $\mathcal{Q}_2$ et par une fonctionnelle récursive de $\mathcal{Q}_2$ vers $\mathcal{Q}_1$. (resp. par une $\mathcal{P}$-fonctionnelle, par une **Pr**-fonctionnelle)

2. QUELQUES PRÉSENTATIONS DES NOMBRES RÉELS à la Cauchy, à la Dedekind, avec mesure d'irrationalité, par les fractions continues.

2.1. Réels à la Cauchy : $\mathbb{R}_{\mathrm{CONV}}$

Du point de vue de la calculabilité, la manière la plus naturelle de présenter un nombre réel x consiste à donner une méthode qui permette de trouver, pour $n \in \mathbb{N}_1$, une approximation rationnelle de x avec la précision $1/2^n$. Cela conduit à la présentation de x via une suite de rationnels $(x_n)_{n\in\mathbb{N}_1}$, convergeant vers x , avec par exemple la condition:

$$\left| x_n - x_m \right| \leq 1/2^n + 1/2^m$$

La condition proposée dans la définition suivante est plus facile à tester.

Définition 2.1 : Nous définirons $\mathbb{R}_{CONV}$ comme la partie de $\mathbb{Q}^{\mathbb{N}_1}$ formée des suites $(x_n)_{n\in\mathbb{N}_1}$ de rationnels vérifiant la condition: $\left| x_n - x_{n+1} \right| \leq 1/2^{n+1}$

Il existe par ailleurs une présentation $\mathcal{P}$-équivalente à $\mathbb{R}_{CONV}$ où un nombre réel x est codé sous forme d'une série :

$$(c_0 , (a_n)_{n\in\mathbb{N}_1}) \text{ code } x = c_0 + \sum_{i=0}^{\infty} \frac{a_i}{4^{i+1}}$$

avec $c_0 \in \mathbb{Z}$ et $(a_n)_{\in\mathbb{N}_1} \in \{-2,-1,0,1,2\}^{\mathbb{N}_1}$

L'avantage est que <u>tout</u> élément de $\mathbb{Z} \times \{-2,-1,0,1,2\}^{\mathbb{N}_1}$ représente un nombre réel x : aucune condition supplémentaire n'est imposée. Le signe de x , s'il est strict, est donné par le premier a_n non nul, et le nombre 0 n'est représenté que par la suite identiquement nulle. Par ailleurs, le fait de tolérer "un chiffre en trop" par rapport à une écriture en base 4 "ordinaire" permet d'obtenir le résultat :

Proposition 2.2 : Les 2 présentations $\mathbb{R}_{CONV}$ et $\mathbb{Z} \times \{-2,-1,0,1,2\}^{\mathbb{N}_1}$ de $\mathbb{R}$ sont $\mathcal{P}$-équivalentes. Nous noterons $\mathbb{R}_{CONV4}$ cette deuxième représentation.

preuve> Soit tout d'abord $(c_0, (a_n)_{n\in\mathbb{N}_1})$ dans $\mathbb{R}_{CONV4} = \mathbb{Z} \times \{-2,-1,0,1,2\}^{\mathbb{N}_1}$ et définissons la suite $(y_n)_{n\in\mathbb{N}_1}$ à valeurs dans $\mathbb{Z}$ par :

$$y_0 = c_0 , \; y_{n+1} = 4.y_n + a_n$$

de sorte que la suite $x_n = y_n/4^n$ converge vers le réel x défini par

$$x = c_0 + \sum_{i=0}^{\infty} \frac{a_i}{4^{i+1}}$$

On a $\left| x_n - x_{n+1} \right| \leq 2/4^{n+1} = 1/2^{2n+1}$, de sorte que la suite représente bien x dans $\mathbb{R}_{CONV}$.
Les entiers n (en unaire) et c_0 (en binaire) étant les entrées, il est clair que le programme (avec utilisation de l'"oracle" (a_n)) qui calcule le dénominateur y_n et le numérateur 4^n de x_n est dans **DTIME**$(O(n^2))$.
Inversement soit $(x_n)_{n\in\mathbb{N}_1}$ un élément de $\mathbb{R}_{CONV}$. Définissons le rationnel x'_n comme le nombre de la forme $y_n/ 4^n$ (avec y_n dans $\mathbb{Z}$) le plus proche de x_{2n+3} (y_n est la partie entière de $1/2 + 4^n . x_{2n+3}$). On a alors les inégalités :

$$\left| x'_n - x_{2n+3} \right| \leq 1/2.4^n , \; \left| x'_{n+1} - x_{2n+5} \right| \leq 1/2.4^{n+1} \text{ et}$$

$$\left| x_{2n+3} - x_{2n+5} \right| \leq 1/2^{2n+4} + 1/2^{2n+5} = (1/16 + 1/32).1/4^n ,$$

d'où on tire:

$$\left| x'_n - x'_{n+1} \right| \leq (23/32).1/4^n < (24/8).1/4^{n+1} = 3/4^{n+1}$$

c.à.d encore $\left| 4.y_n - y_{n+1} \right| < 3$.

Comme $a_n = y_{n+1} - 4.y_n$ est entier, c'est forcément l'un des 5 "chiffres" $-2, -1, 0, 1, 2$.

Il est clair que le calcul de y_n (donc aussi celui de a_n ou c_0) est dans **DTIME**$(O(n^2))$ par rapport à l'entrée x_{2n+3} donc aussi en temps polynomial par rapport à l'entrée n lorsqu'on dispose de l'oracle $(x_n)_{n\in\mathbb{N}_1}$ ❑

Remarque : On a un résultat analogue avec par exemple la base 2 et les chiffres –1, 0, 1, (présentation $\mathbb{R}_{CONV2}$) ou plus généralement la base p et au moins $p+1$ chiffres consécutifs. Par exemple si on veut un développement en base 4 d'un nombre x avec les chiffres 1, 2, 3, 4, 5, on rajoute 3 à chaque chiffre après la virgule d'un développement dans $\mathbb{R}_{CONV4}$ du nombre $y = x - 1$, en effet :

$$x - 3.\sum_{i=1}^{\infty} 4^{-i} = x - 1 .$$

Notations :
– $\mathbb{R}_{CONV}(\mathfrak{C})$: une classe de complexité $\mathfrak{C}$ étant définie, nous noterons $\mathbb{R}_{CONV}(\mathfrak{C})$ la partie de $\mathbb{R}_{CONV}$ formée par les suites $(x_n)_{n\in\mathbb{N}_1}$ de complexité $\mathfrak{C}$.
– **$\mathfrak{C}$-suite dans** $\mathbb{R}_{CONV}$: une suite (x^m) dans l'ensemble $\mathbb{R}_{CONV}$ sera appelé une « $\mathfrak{C}$-suite dans $\mathbb{R}_{CONV}$ » si la suite double $(x_{m,n})$ (définie par $(x_{m,n}) = (x^m)_n$), est de complexité $\mathfrak{C}$.

Tous les termes d'une $\mathfrak{C}$-suite dans $\mathbb{R}_{CONV}$ sont dans $\mathbb{R}_{CONV}(\mathfrak{C})$ mais la réciproque n'est naturellement pas valable.

2.2. Réels à la Dedekind : $\mathbb{R}_{CUT}$

Un nombre réel x est dit *calculable au sens de Dedekind* si le test t_x : "comparer le réel x au rationnel q" est effectif (q est la variable, et $t_x(q)$ peut prendre 3 valeurs: –1, 0 ou +1 selon que $q < x$, $q = x$, ou $q > x$).
On obtient la version relativisée de nombre réel *calculable en temps polynomial au sens de Dedekind* en demandant que le test soit faisable en temps polynomial.
Nous pouvons utiliser les coupures de Dedekind pour obtenir une nouvelle présentation des nombres réels, notée $\mathbb{R}_{CUT}$:

Définition 2.3 : Nous définissons l'ensemble $\mathbb{R}_{CUT}$ comme une partie de $\mathbb{Z}\times\{-1,0,+1\}^{\mathbb{Q}}$. Un élément (z,t) de $\mathbb{Z}\times\{-1,0,+1\}^{\mathbb{Q}}$ est dans $\mathbb{R}_{CUT}$ si et seulement si les conditions suivantes sont vérifiées (q et q' sont des rationnels) :

i) la fonction t est croissante et elle prend au plus une fois la valeur 0 ,
ii) $\forall\, q\ (\, t(q) > 0 \quad \Rightarrow \exists\ q' < q\ ,\ t(q') > 0\ )$
$\forall\, q\ (\, t(q) < 0 \quad \Rightarrow \exists\ q' > q\ ,\ t(q') < 0\ )$
iii) $t(z) < 0 < t(z+2)$

Les conditions 1) , 2) et 3) signifient que la fonction t est bien un test t_x correspondant à un nombre réel x . Le fait d'avoir intégré explicitement le minorant z et le majorant $z+2$ dans la définition de $\mathbb{R}_{CUT}$ nous permet d'obtenir sans difficulté le résultat suivant, qui serait faux si z n'intervenait pas dans la définition :

Proposition 2.4 : Il existe une **DTIME**$(O(n^2))$-fonctionnelle de $\mathbb{Z}\times\{-1,0,+1\}^{\mathbb{Q}}$ vers $\mathbb{R}_{CONV}$ dont la restriction à $\mathbb{R}_{CUT}$ représente l'identité de $\mathbb{R}$.

preuve> L'entrée est donnée par $z \in \mathbb{Z}$ et $n \in \mathbb{N}_1$, et on a un oracle dans $\{-1,0,+1\}^{\mathbb{Q}}$. On fait une dichotomie à partir des valeurs initiales z et $z+2$ jusqu'à obtenir une précision de $1/2^{n+2}$. ❑

Notations : $\mathbb{R}_{CUT}(\mathfrak{C})$: analogue de $\mathbb{R}_{CONV}(\mathfrak{C})$. Par exemple $\mathbb{R}_{CUT}(\mathfrak{P})$ représente l'ensemble des réels calculables en temps polynomial au sens de Dedekind.
On définit également les $\mathfrak{C}$-suites dans $\mathbb{R}_{CUT}$ de manière analogue aux $\mathfrak{C}$-suites dans $\mathbb{R}_{CONV}$.

Une variante : On peut considérer un test $t^{-}_{x}(q)$ qui ne prend que les valeurs -1 ou $+1$ selon que $x < q$ ou $x \geq q$. Cela conduit à définir un ensemble $\mathbb{R}_{CUT-}$ comme une partie convenable de $\mathbb{Z} \times \{-1,+1\}^{\mathbb{Q}}$. Nous ne prendrons pas la peine d'expliciter les conditions analogues à celles données à la définition 2.3.

2.3. Réels avec mesure d'irrationalité : $\mathbb{R}_{MIR}$

Le test t_x, s'il est effectif, nous permet de décider si un rationnel q est distinct de x. Lorsque c'est le cas, ceci doit pouvoir être explicité en <u>calculant</u> un rationnel q' situé entre x et q. Nous obtenons ainsi une version plus explicite des coupures de Dedekind.

Définition 2.5 :

a) Nous appellerons *mesure d'irrationalité du nombre réel* x une fonction μ de $\mathbb{Q}$ vers $\mathbb{Q}$ qui vérifie les 3 conditions suivantes:

$\mu(q) = q$ si $q = x$, $x < \mu(q) < q$ si $x < q$, et $x > \mu(q) > q$ si $x > q$

b) Nous appellerons *mesure d'irrationalité sans signe du nombre réel* x une fonction η de $\mathbb{N}$ vers $\mathbb{N}$ telle que, pour tout rationnel p/q (avec $q > 0$) on ait :

$$x \neq p/q \Rightarrow |x - p/q| > 1/\eta(q)$$

Lorsque x est irrationnel, la "mesure d'irrationalité sans signe" est à très peu près la mesure d'irrationalité au sens classique .
Nous pouvons utiliser les mesures d'irrationalité pour obtenir une nouvelle présentation des nombres réels:

Définition 2.6 : Nous définirons $\mathbb{R}_{MIR}$ comme une partie de $\mathbb{Z} \times \mathbb{Q}^{\mathbb{Q}}$.

Un élément (z , μ) de $\mathbb{Z} \times \mathbb{Q}^{\mathbb{Q}}$ est dans $\mathbb{R}_{MIR}$ si et seulement si les conditions suivantes sont vérifiées: (avec q, q', r dans $\mathbb{Q}$)

i) $\mu(q) \leq q < r \Rightarrow \mu(r) < r$; $\quad q < r \leq \mu(r) \Rightarrow q < \mu(q)$

ii) $q < \mu(q) = q' \Rightarrow q' < \mu(q')$; $\quad q > \mu(q) = q' \Rightarrow q' > \mu(q')$

iii) $z < \mu(z) < \mu(z+2) < z+2$

Théorème 2.7 : Les 2 présentations $\mathbb{R}_{CUT}$ et $\mathbb{R}_{MIR}$ de $\mathbb{R}$ sont récursivement équivalentes**.**
Plus précisément:

a) Il existe une $\mathfrak{P}$-fonctionnelle de $\mathbb{Z} \times \mathbb{Q}^{\mathbb{Q}}$ vers $\mathbb{Z} \times \{-1,0,+1\}^{\mathbb{Q}}$ dont la restriction à $\mathbb{R}_{MIR}$ représente l'identité de $\mathbb{R}$ (l'ensemble $\mathbb{R}$ étant représenté par $\mathbb{R}_{MIR}$ (source) et $\mathbb{R}_{CUT}$ (image))

b) Il existe une fonctionnelle récursive partielle de $\mathbb{Z} \times \{-1,0,+1\}^{\mathbb{Q}}$ vers $\mathbb{Z} \times \mathbb{Q}^{\mathbb{Q}}$ dont la restriction à $\mathbb{R}_{CUT}$ représente l'identité de $\mathbb{R}$ (l'ensemble $\mathbb{R}$ étant représenté par $\mathbb{R}_{CUT}$ et $\mathbb{R}_{MIR}$)

preuve> a) immédiate: on compare q et $\mu(q)$
b) supposons par exemple $t(q) < 0$; on initialise $q' := q+1$, puis on fait $q' := (q+q')/2$ jusqu'à ce que $t(q') < 0$.
Notons que cette procédure peut boucler sans fin si l'oracle ne répond pas conformément à un élément de $\mathbb{R}_{CUT}$ ❑

Remarques:
Le fait que la fonctionnelle est beaucoup moins bonne dans le sens $\mathbb{R}_{CUT} \longrightarrow \mathbb{R}_{MIR}$ se traduira en terme de complexité (cf. section 4)
Pour qu'un réel x soit dans $\mathbb{R}_{MIR}(\mathcal{P})$ il faut et il suffit qu'il soit dans $\mathbb{R}_{CONV}(\mathcal{P})$ et qu'il possède une mesure d'irrationalité sans signe majorée par une fonction $n \mapsto 2^{P(\mathbf{lg}(n))}$, où P est un polynome. Résultat analogue avec **PSPACE** .
De même, pour qu'un réel x soit dans $\mathbb{R}_{MIR}(\mathbf{Pr})$ il faut et il suffit qu'il soit dans $\mathbb{R}_{CONV}(\mathbf{Pr})$ et qu'il possède une mesure d'irrationalité sans signe primitive récursive.

2.4. Réels par fractions continues : $\mathbb{R}_{CONT}$

On examine maintenant la présentation via les fractions continues. Un nombre réel irrationnel x possède un développement en fraction continue illimité $n \longrightarrow a_n(x)$ qui peut être considéré comme un élément de $\mathbb{Z} \times \mathbb{N}^{\mathbb{N}_1^*}$. Par ailleurs un nombre rationnel possède un développement en fraction continue fini, qui peut être prolongé par des 0 de manière purement conventionnelle. Enfin, nous remarquons qu'un nombre réel représenté par un élément calculable de $\mathbb{R}_{MIR}$ ne peut pas être ipso facto testé rationnel ou irrationnel. Tout ceci conduit à penser raisonnable la définition suivante, dans laquelle les rationnels et les irrationnels ne sont pas nettement séparés a priori les uns des autres.

Définition 2.8 : Nous définirons $\mathbb{R}_{CONT}$ comme égal à $\mathbb{Z} \times \mathbb{N}^{\mathbb{N}_1^*}$. Tout élément (e,f) de $\mathbb{R}_{CONT}$ représente un nombre réel x dont le développement en fraction continue est donné par la suite (e, f(1), f(2), ...) en convenant d'arrêter au premier f(i) nul s'il en existe.

Remarque : Chaque nombre rationnel est donc représenté, avec ses deux dfc possibles, une infinité de fois. Un irrationnel n'est par contre représenté qu'une seule fois.

Théorème 2.9 : Les deux présentations $\mathbb{R}_{CONT}$ et $\mathbb{R}_{MIR}$ de $\mathbb{R}$ sont **Pr**-équivalentes **.** Plus précisément:

a) Il existe une $\mathcal{P}$-fonctionnelle de $\mathbb{R}_{CONT}$ vers $\mathbb{R}_{MIR}$ qui représente l'identité de $\mathbb{R}$
b) Il existe une **Pr**-fonctionnelle de $\mathbb{Z} \times \mathbb{Q}^{\mathbb{Q}}$ vers $\mathbb{R}_{CONT}$ dont la restriction à $\mathbb{R}_{MIR}$ représente l'identité de $\mathbb{R}$.)

preuve> Voyons d'abord la fonctionnelle de $\mathbb{R}_{CONT}$ vers $\mathbb{R}_{MIR}$.
Nous utilisons les inégalités donnés dans les préliminaires.

Nous avons comme donnée le rationnel a/b , et nous disposons d'un oracle pour le réel x dans $\mathbb{R}_{CONT}$.
Nous allons calculer des convergents successifs du nombre réel x . Si au cours du calcul, x s'avère être rationnel (une réponse "f(n)" de l'oracle est 0) la comparaison de x à a/b est immédiate. On peut donc supposer, pour simplifier l'exposé, que ce cas ne se présente pas.
Le programme consiste alors en ceci:

- calculer $k = 1+2\mathbf{lg}(b)$, et demander à l'oracle la liste des $k+1$ premiers quotients partiels
- calculer les convergents successifs p_0/q_0 , p_1/q_1 , ..., p_n/q_n jusqu'à ce que $q_n \geq b$ (on a $n \leq k$)
- calculer q_{n+1}
- le nombre rationnel $\mu(a/b)$ strictement compris entre x et a/b est alors:

$$a/b + \varepsilon / q_n (q_n + q_{n+1}) \text{ où } \varepsilon \text{ est le signe de } (a/b - p_n/q_n)$$

Voyons maintenant la fonctionnelle de $\mathbb{R}_{MIR}$ vers $\mathbb{R}_{CONT}$.
Nous avons comme données : l'entier z (x est sur l'intervalle $]\, z, z+2\, [$) et l'entier n ; et nous disposons d'un oracle pour le réel x dans $\mathbb{R}_{MIR}$.
Nous voulons calculer le $n^{ième}$ quotient partiel de x . Si, en cours de calcul, le nombre x s'avère rationnel, le résultat est alors immédiat. Nous supposerons donc pour simplifier que ce cas ne se produit pas.
Le calcul se fait par une récurrence simple, (en utilisant l'oracle). Le 1^{er} quotient partiel, la partie entière e de x, est $z+1$ ou z (on demande $\mu(z+1)$ pour décider).
On calcule les convergents successifs au fur et à mesure que sont trouvés les quotients partiels. Si le dernier convergent trouvé est p_j/q_j , on interroge l'oracle pour p_j/q_j , qui donne une réponse "$r_j = \mu(p_j/q_j)$". Donc $a_{j+1} \leq Ent(H_j(r_j))$. On calcule alors a_{j+1} par dichotomie, en comparant x à $L_j(m_i)$ pour des entiers m_i compris entre 1 et $Ent(H_j(r_j))$. ❑

Remarque : Dans la démonstration précédente, la procédure uniformément primitive récursive n'est pas "uniformément en temps polynomial" parce que les variables du programme qui contiennent p_{j-1}, p_j, q_{j-1}, q_j voient leur taille augmenter de manière mal controlée au cours des boucles successives (passage de j à $j+1$).
On a d'ailleurs le résultat suivant (cf.[**Lab**]) :

Proposition 2.10:

On peut construire un élément de $\mathbb{R}_{MIR}(\mathcal{P})$ qui n'est pas dans $\mathbb{R}_{CONT}(\mathcal{P})$.

preuve> Soit en effet le réel x dont le développement en fraction continue est donné par :

$$a_0(x) = 1 \qquad a_n(x) = 2.2^{2^n}$$

Il est clair que x n'est pas dans $\mathbb{R}_{CONT}(\mathcal{P})$.
Par contre, pour tout rationnel a/b la recherche de l'entier k tel que

$$2^{k-1} \leq \mathbf{lg}(b) < 2^k \text{ (d'où } a_k \leq b^2)$$

coûte $O(\mathbf{lg}(b))$ et on a :

$$q_k = a_k q_{k-1} + q_{k-2} \leq \prod_{i=1}^{k} (1 + a_i) < 2.2^{2^{k+1}}$$

ce qui donne

$$\left| x - \frac{a}{b} \right| > \left| x - \frac{p_k}{q_k} \right| \geq \frac{1}{q_k(q_k + q_{k+1})} > \frac{1}{8\, b^{12}}$$

Ceci majore convenablement la mesure d'irrationalité sans signe de x .
En outre, x est dans $\mathbb{R}_{CUT}(\mathcal{P})$ puisque $x - a/b$ a le même signe que $p_k/q_k - a/b$ (a fortiori x est dans $\mathbb{R}_{CONV}(\mathcal{P})$) . ❑

3. IMPOSSIBILITÉ DE REPRÉSENTER RÉCURSIVEMENT CERTAINES FONCTIONS ET CERTAINS TESTS "ÉLÉMENTAIRES"

3.1. Impossibilités via des fonctionnelles récursives

Remarque préliminaire: Considérons une fonctionnelle récursive qui traite "en entrée" un élément $x = (x_n)_{n \in \mathbb{N}_1} \in \mathbb{Q}^{\mathbb{N}_1}$ dans $\mathbb{R}_{CONV}$.
Cela signifie, au niveau du programme qui calcule cette fonctionnelle, la consultation d'un oracle (à la question, " n ? ", il répond : " x_n ").
Supposons que le programme ait donné un résultat avec l'oracle x , et que le plus grand entier n pour lequel l'oracle ait été interrogé soit k :
alors on peut construire un oracle y qui répondrait de la même manière aux questions qui ont été posées à x et qui correspond à un réel arbitraire de l'intervalle $[x_k - 1/2^k, x_k + 1/2^k]$. Avec ce nouvel oracle, le programme aboutit au même résultat.
Notons en particulier que l'oracle qui répondrait: " x_n " à toute question " n ? " où $n \leq k$, et : " x_k " à toute question " n ? " où $n \geq k$ provoquerait le même calcul que l'oracle (x_n) .

Proposition 3.1 :

a) Les tests $x = 0$? , $x > 0$? ne sont pas récursifs pour $x \in \mathbb{R}_{CONV}$.
b) Le test $x \in \mathbb{Q}$? n'est pas récursif pour $x \in \mathbb{R}_{CONV}$, $\mathbb{R}_{CUT}$, $\mathbb{R}_{MIR}$ ou $\mathbb{R}_{CONT}$.

Proposition 3.2 : L'identité de $\mathbb{R}$ n'est pas récursivement représentable pour les présentations $\mathbb{R}_{CONV}$ (source) et $\mathbb{R}_{CUT}$ (image) de $\mathbb{R}$. (même résultat avec $\mathbb{R}_{CUT-}$, $\mathbb{R}_{MIR}$ ou $\mathbb{R}_{CONT}$ à la place de $\mathbb{R}_{CUT}$)

preuve> Prenons tout d'abord le cas du test $x = 0$? avec x dans $\mathbb{R}_{CONV}$: la fonctionnelle récursive ne connaît x que via des valeurs rationnelles approchées. Considérons la réponse fournie par la fonctionnelle lorsque l'oracle répond 0 chaque fois qu'on lui demande une valeur approchée de x . Comme le programme n'interroge qu'un nombre fini de valeurs approchées, la seule information disponible sur x est du type "x est sur tel intervalle" (non réduit à un point). La réponse fournie, si elle est juste pour x nul, est fausse pour tous les autres réels de l'intervalle en question, et vice versa.
Même type de raisonnement pour les tests $x > 0$? , $x \leq 0$? , $x \in \mathbb{Q}$? avec x dans $\mathbb{R}_{CONV}$.
Pour le test "$x \in \mathbb{Q}$?" avec x dans $\mathbb{R}_{CUT}$ on considère un oracle qui répond comme $\sqrt{2}$. Lorsque le programme calculant la fonctionnelle a fourni un résultat, un nombre fini de

comparaisons à des rationnels ont eu lieu. Mais tout réel d'un certain intervalle rationnel entourant $\sqrt{2}$ aurait donné les mêmes réponses aux questions posées: la fonctionnelle se trompe donc, soit pour les rationnels, soit pour les irrationnels de cet intervalle.
La proposition 3.2 est conséquence immédiate de la proposition 3.1(a). ❑

Remarques : commentaires sur la proposition 3.1(b)

1) Il existe néanmoins une fonctionnelle récursive de source $\mathbb{R}_{CUT}$ non partout définie qui répond "oui" lorsque $x \in \mathbb{Q}$ et ne répond rien dans le cas contraire.

2) Bien que tout point rationnel soit un point isolé de $\mathbb{R}_{CONT}$ pour sa métrique "naturelle"[1], l'ensemble des rationnels est une partie dense de $\mathbb{R}_{CONT}$. Ceci explique que $\mathbb{R}_{CONT}$ ne soit pas récursivement équivalent à la réunion disjointe des rationnels (sur lesquels $\mathbb{R}_{CONT}$ induit une topologie discrète) et des irrationnels (qui est un sous-espace complet).

Le théorème suivant est une généralisation de la proposition 3.1(a), on peut le lire «aucune partie de $\mathbb{R}$ n'est récursivement décidable au sens de $\mathbb{R}_{CONV}$ (hormis le vide et le plein)»; la formulation du théorème est plus constructive et la preuve qui en est fournie ici est constructive.

Théorème 3.3 :

Soient $a, b \in \mathbb{R}_{CONV}$ et $\mathcal{F}$ une fonctionnelle récursive de $\mathbb{R}_{CONV}$ vers $\{0, 1\}$ avec
$\mathcal{F}(a) = 0$ et $\mathcal{F}(b) = 1$.

Alors on peut construire a' et b' dans $\mathbb{R}_{CONV}$ tels que :
$\mathcal{F}(a') = 0$, $\mathcal{F}(b') = 1$ et $a' =_{\mathbb{R}} b'$.

preuve> On sait que le résultat $\mathcal{F}(a) = 0$ est obtenu par le programme calculant la fonctionnelle $\mathcal{F}$ à partir d'un nombre fini d'approximations rationnelles de a. Soit k le dernier indice pour lequel a_k est interrogé lors du calcul de $\mathcal{F}(a)$. Notons a^1 la suite obtenue à partir de (a_n) en prenant, à partir due l'indice k, tous les termes égaux à a_k, et notons a^2 la suite constante dont tous les termes sont égaux à a_k. Les suites a^1 et a^2 représentent dans $\mathbb{R}_{CONV}$ le nombre rationnel a_k. Si $\mathcal{F}(a^2) = 1$, la construction est terminée, avec $a' = a^1$ et $b' = a^2$.
Supposons donc $\mathcal{F}(a^2) = 0$.
On procède avec b de la même manière, de sorte qu'on est ramené au cas où $\mathcal{F}(b^2) = 1$, avec a^2 et b^2 qui sont des "rationnels de $\mathbb{R}_{CONV}$" c.-à-d. des suites constantes.
Supposons par exemple $b^2 > a^2$: on construit alors par dichotomie 2 suites (a^n) et (b^n) de "rationnels de $\mathbb{R}_{CONV}$" vérifiant :

$\mathcal{F}(a^n) = 0$, $\mathcal{F}(b^n) = 1$, $b^n - a^n = (b^2 - a^2)/2^{n-2}$,
$b^{n-1} - b^n = 0$ ou $(b^2 - a^2)/2^{n-2}$,
$a^n - a^{n-1} = 0$ ou $(b^2 - a^2)/2^{n-2}$.

Considérons alors les éléments $\tilde{a}$ et $\tilde{b}$ de $\mathbb{R}_{CONV}$ définis par

$\tilde{a}_n$ = (valeur constante de la suite a^{n+r}) et $\tilde{b}_n$ = (valeur constante de la suite b^{n+r}), où $r \geq 2$ vérifie: $b^2 - a^2 \leq 2^{r-2}$.

Si $\mathcal{F}(\tilde{a}) = 0$ et $\mathcal{F}(\tilde{b}) = 1$ la construction est terminée avec $a' = \tilde{a}$ et $b' = \tilde{b}$.

---

[1] La distance "naturelle" de 2 développements en fraction continue est à très peu près: 1/[1+numéro du premier nombre distinct dans les 2 dfc]. La seule modification à apporter consiste, dans le cas des dfc de rationnel, à remplacer un dfc d'un rationnel se terminant par 1 par le dfc du même rationnel ne se terminant pas par 1. On vérifie sans peine que cette distance est donnée par une fonctionnelle récursive à valeurs dans $\mathbb{R}_{CONV}$.

Sinon supposons par exemple $\mathcal{F}(\tilde{a}) = 1$. Soit j le dernier indice pour lequel $\tilde{a}_j$ est interrogé par le programme qui calcule $\mathcal{F}(\tilde{a})$. Soit alors $a' = a^{j+r}$ (suite constante) et b' la suite qui commence comme $\tilde{a}$ et est constante à partir du rang j . La construction est terminée. ❑

Proposition 3.4 : Les représentations $\mathbb{R}_{CUT}$ et $\mathbb{R}_{CUT-}$ de $\mathbb{R}$ ne sont pas récursivement équivalentes. L'identité de $\mathbb{R}$ n'est pas récursivement représentable pour les présentations $\mathbb{R}_{CUT-}$ (source) et $\mathbb{R}_{CUT}$ (image) de $\mathbb{R}$

preuve> Il suffit de montrer que le test $x = 0$? n'est pas réalisable par une fonctionnelle récursive pour x dans $\mathbb{R}_{CUT-}$.
Or, l'information disponible sur le réel x donné comme élément de $\mathbb{R}_{CUT-}$, après qu'un nombre fini de tests aient été réalisés, est du type $x \in]\, q\, ,\, r\,]$ avec q et r rationnels. Il est clair que l'égalité de x à 0 ne peut être déduite d'une information de ce type. La fonctionnelle cherchant à répondre à la question $x = 0$? , se trompe donc sûrement, soit pour 0 soit pour les réels d'un intervalle $]\, q\, ,\, 0\,]$ ❑

Remarque: Le résultat affirmé en proposition 3.4 peut sembler surprenant. Pour un réel x irrationnel, les fonctions t_x et $t_{\bar{x}}$ sont égales, et pour un réel x rationnel, les fonctions $t_{\bar{x}}$ et t_x ne diffèrent qu'au point x . En particulier les fonctions t_x et $t_{\bar{x}}$ ont forcément la même complexité.

Proposition 3.5 : Soit c un nombre irrationnel. Alors le test « $x = c$? » n'est pas donné par une fonctionnelle récursive pour x dans $\mathbb{R}_{CUT}$, $\mathbb{R}_{MIR}$ ou $\mathbb{R}_{CONT}$.

Proposition 3.6 : Soit une fonction f de $\mathbb{R}$ vers $\mathbb{R}$ strictement monotone sur un intervalle rationnel $[\, a\, ,\, b\,]$ et donnant pour image d'un irrationnel c de $[\, a\, ,\, b\,]$ un nombre rationnel $d = f(c)$: alors la fonction f n'est pas récursivement représentable dans $\mathbb{R}_{CUT}$ (même résultat pour $\mathbb{R}_{MIR}$ et $\mathbb{R}_{CONT}$).

Proposition 3.7 : Les fonctions $x \mapsto x^2$, $(x,y) \mapsto x.y$, $(x,y) \mapsto x + y$, $x \mapsto \exp(x)$ etc... ne sont pas récursivement représentables dans $\mathbb{R}_{CUT}$ (même résultat pour $\mathbb{R}_{MIR}$ et $\mathbb{R}_{CONT}$).

preuve> Proposition 3.5 : considérons la réponse donnée par la fonctionnelle lorsque l'oracle "x" répond de la même manière que "c". Après un nombre fini d'interrogations de l'oracle, l'information dont on dispose sur x est son appartenance à un intervalle rationnel, non réduit à un point puisque c est irrationnel. La réponse fournie par la fonctionnelle est donc mauvaise, soit pour c soit pour tous les autres réels de l'intervalle en question.
La proposition 3.6 est alors immédiate.
Pour la proposition 3.7 , on applique la 3.6 avec un irrationnel convenable. (dans le 1^{er} exemple on peut prendre $\sqrt{2}$; le $2^{ème}$ se déduit du 1^{er} ; dans le $3^{ème}$ exemple on peut prendre, y étant fixé égal à $\sqrt{2}$, $-\sqrt{2}$ pour la variable x etc ...) ❑

3.2. Impossibilités via des fonctions récursives

Introduction

Certaines parties de $\mathbb{R}_{CONV}$ telles $\mathbb{R}_{CONV}(\mathcal{P})$ ou $\mathbb{R}_{CONV}(\mathbf{Pr})$ peuvent être facilement énumérées de manière effective. (cf. alinéa suivant) Elles peuvent alors être "traitées" au moyen de fonctions récursives (au lieu de fonctionnelles récursives) .

On a démontré au paragraphe précédent que certaines fonctions de $\mathbb{R}$ vers $\mathbb{R}$ (ou de $\mathbb{R}\times\mathbb{R}$ vers $\mathbb{R}$) ne sont pas représentables par des <u>fonctionnelles</u> récursives lorsqu'on adopte certaines présentations de $\mathbb{R}$ en source et image.

On pourrait espérer néanmoins que certaines de ces fonctions soient représentables par des <u>fonctions</u> récursives lorsqu'on considère leur restriction à une partie de $\mathbb{R}$ énumérée de manière effective (par exemple $\mathbb{R}_{CONV}(\mathcal{P})$). Le but de la section 3.2 est de déjouer cet espoir, du moins en ce qui concerne la classe $\mathcal{P}$.

On peut penser que les résultats négatifs obtenus resteraient les mêmes en remplaçant $\mathcal{P}$ par **LINTIME**.

Enumération effective de $\mathbb{R}_{CONV}(\mathcal{P})$

Soit $(\varphi_k)_{k\in\mathbb{N}}$ une énumération effective des fonctions récursives partielles de $\mathbb{N}_1$ vers $\{-1,0,1\}$ (k est le numéro de Gödel de la machine de Turing qui calcule la fonction partielle φ_k). Si P est un polynome $P(n) := n^a + b$ (avec a, b entiers), le couple (φ_k , P) définit une fonction ψ_k de $\mathbb{N}_1$ vers $\{-1,0,1\}$ calculable en temps polynomial:

$\psi_k(n) :=$ $\varphi_k(n)$ si le programme a terminé le calcul en moins de P(n) étapes
0 sinon

On peut alors énumérer les triplets (z, φ_k , P) où $z \in \mathbb{Z}$, ce qui donne une énumération effective de $\mathbb{R}_{CONV}(\mathcal{P})$; le triplet (z, φ_k , P) représentant le réel :

$$x := z + \sum_i (\psi_k(i)/2^{i+1})$$

La même méthode donne des énumérations effectives de $\mathbb{R}_{CONV}(\mathbf{Pr})$, $\mathbb{R}_{CONT}(\mathcal{P})$, $\mathbb{R}_{CONT}(\mathbf{Pr})$ ou de $\mathbb{R}_{MIR}(\mathbf{Pr})$ via $\mathbb{R}_{CONT}(\mathbf{Pr})$ (cf. théorème 2.9).
Ces énumérations effectives sont définies avec trop peu de précision pour pouvoir conférer aux ensembles correspondants une structure intrinsèque de calculabilité au sens de la complexité. Néanmoins cela suffit à conférer à ces ensembles une structure de calculabilité au sens des fonctions récursives. C'est ainsi que la phrase

$$\text{« f : } \mathbb{R}_{CONV}(\mathcal{P}) \longrightarrow \mathbb{N} \text{ est une fonction récursive »}$$

prend un sens précis et indépendant de la numérotation de Gödel choisie pour les machines de Turing.

Nous avons en vue des résultats négatifs et nous utiliserons systématiquement le critère suivant pour la non récursivité de f dans la phrase ci-dessus :

Critère de non récursivité : Soit f une fonction de $\mathbb{R}_{CONV}(\mathcal{P})$ vers $\mathbb{N}$. S'il existe une $\mathcal{P}$-suite dans $\mathbb{R}_{CONV}$, $(x^m)_{m\in\mathbb{N}_1}$, telle que la suite $(f(x^m))_{m\in\mathbb{N}_1}$ soit non récursive, alors la fonction f est elle-même non récursive.

On appliquera dans la suite ce critère avec d'autres ensembles que $\mathbb{N}$ à l'arrivée.

Notons qu'on pourrait dans le critère remplacer la $\mathcal{P}$-suite dans $\mathbb{R}_{CONV}$ par suite récursive dans $\mathbb{R}_{CONV}$ dont tous les éléments sont dans $\mathbb{R}_{CONV}(\mathcal{P})$ et telle que la majoration polynomiale du temps de calcul de $n \mapsto x^m{}_n$ dépende récursivement de m. Nous n'aurons cependant pas besoin de ce raffinement.

Quid de $\mathbb{R}_{CONV}$ (Rec) ou $\mathbb{R}_{CUT}(\mathcal{P})$?

En ce qui concerne $\mathbb{R}_{CONV}$(**Rec**) ou $\mathbb{R}_{CUT}(\mathcal{P})$, ou même $\mathbb{R}_{MIR}(\mathcal{P})$, la procédure d'énumération obtenue ci-dessus pour $\mathbb{R}_{CONV}(\mathcal{P})$ ne fonctionne plus aussi bien. Par exemple avec $\mathbb{R}_{CONV}$(**Rec**), l'ensemble des couples (z, φ_k) peut être énuméré, mais l'ensemble des indices k pour lesquels la fonction partielle φ_k est totale n'est pas récursivement énumérable. On a un problème analogue avec $\mathbb{R}_{CUT}(\mathcal{P})$ qui tient à la difficulté de tester si une fonction t est dans $\mathbb{R}_{CUT}$ ou pas.

Lorsque nous énonçons quelque chose du genre (cf. propositions 3.9 et 3.10):

> « Il n'existe pas de fonction récursive de $\mathbb{R}_{CUT}(\mathcal{P})$ vers $\mathbb{A}$ telle que .... »

cela a alors précisément la signification suivante:

> « Supposons avoir énuméré de manière effective une partie de $\mathbb{Z} \times \{-1,0,+1\}^{\mathbb{Q}}$ contenant $\mathbb{R}_{CUT}(\mathcal{P})$, alors, via cette énumération, il n'existe pas de fonction récursive vers $\mathbb{A}$ telle que .... »

En fait le même critère de non récursivité s'applique dans ce cas, ce qui explique que les démonstrations de non récursivité soient toutes bâties sur le même modèle.

Une suite de réels intéressante

Nous utilisons une suite récursive dans $\mathbb{R}_{CONV}$, formée de réels tous rationnels, mais qui n'est pourtant pas une suite récursive dans $\mathbb{Q}$.

Soit $(u_n)_{n\in\mathbb{N}_1}$: $\mathbb{N}_1 \longrightarrow \mathbb{N}_1$ une suite **LINTIME** ayant pour image une partie U récursivement énumérable mais non récursive de $\mathbb{N}_1$.

On définit:

$w(n,p) :=$ $1/2^n$ si n est le premier entier m vérifiant $u_m = p$
0 sinon

Il est clair que $w : \mathbb{N}_1 \times \mathbb{N}_1 \longrightarrow \mathbb{Q}$ est dans **DTIME**$(O(n^2))$

On définit alors la suite de réels $(v_n)_{n\in\mathbb{N}_1}$:

$$v_n = \sum_{i=0}^{\infty} w(k,p)$$

On obtient alors facilement les résultats suivants.

Proposition 3.8 :

a) la suite $(v_p)_{p\in\mathbb{N}_1}$ est une **DTIME**$(O(n^2))$-suite dans $\mathbb{R}_{CONV}$
b) le test: " $v_p > 0$? " n'est pas récursif
c) la suite $(v_p)_{p\in\mathbb{N}_1}$ n'est pas une suite récursive dans $\mathbb{Q}$
d) la suite $(v_p)_{p\in\mathbb{N}_1}$ n'est pas une suite récursive dans $\mathbb{R}_{CUT}$ (ni dans $\mathbb{R}_{MIR}$ ou $\mathbb{R}_{CONT}$)
e) la restriction à $\mathbb{R}_{CONV}(\mathcal{P})$ de l'identité de $\mathbb{R}$ n'est pas représentable par une fonction récursive de $\mathbb{R}_{CONV}(\mathcal{P})$ vers $\mathbb{R}_{CUT}$ (de même vers $\mathbb{R}_{MIR}$, ou vers $\mathbb{R}_{CONT}$)

f) les tests $x > 0$?, $x \leq 0$?, $x \in \mathbb{Q}$? ne sont pas récursifs pour $x \in \mathbb{R}_{CONV}(\mathcal{P})$

preuve> Pour le b) : on a: $v_p > 0$ si et seulement si $p \in U$.
Les c), d), e) s'en déduisent immédiatement
Dans f) pour le test $x \in \mathbb{Q}$? on considère la suite $(\sqrt{2}.v_p)_{p\in\mathbb{N}_1}$ ❑

Proposition 3.9 :

a) La suite $(y_p)_{p\in\mathbb{N}_1} = (\sqrt{2} + v_p)_{p\in\mathbb{N}_1}$ est une $\mathcal{P}$-suite dans $\mathbb{R}_{MIR}$
b) Il n'existe pas de fonction récursive de $\mathbb{R}_{MIR}(\mathcal{P})$ vers $\mathbb{R}_{MIR}$ qui représente la fonction $x \mapsto x^2 : \mathbb{R} \longrightarrow \mathbb{R}$
c) Il n'existe pas de fonction récursive de $\mathbb{R}_{MIR}(\mathcal{P}) \times \mathbb{R}_{MIR}(\mathcal{P})$ vers $\mathbb{R}_{MIR}$ qui représente l'addition dans $\mathbb{R}$
d) Mêmes résultats avec $\mathbb{R}_{CUT}$ à la place de $\mathbb{R}_{MIR}$.

preuve> Pour le a): on part de l'inégalité $\left| a/b - \sqrt{2} \right| > 1/4b^2$.
La suite $\sqrt{2} + v_p$ est une **DTIME**$(O(n^2))$-suite dans $\mathbb{R}_{CONV}$.
Il reste à minorer $\left| a/b - v_p - \sqrt{2} \right|$.
Pour cela on calcule $u_1, \ldots, u_m$ jusqu'à ce que : $2^{m-1} \leq 8b^2 < 2^m$
– si on a trouvé une valeur m_0 pour laquelle $u_{m_0} = p$ (alors $v_p = 1/2^{m_0}$ avec $2^{m_0} \leq 8b^2$), on obtient : $\left| a/b - v_p - \sqrt{2} \right| > 1/64.b^5$.
– sinon $v_p < 1/8.b^2$ donc $\left| a/b - v_p - \sqrt{2} \right| > 1/8.b^2$
Ainsi $\sqrt{2} + v_p$ est une **DTIME**$(O(n^2))$-suite dans $\mathbb{R}_{MIR}$.
Le b) résulte du a) puisque la comparaison de y_p^2 à 2 n'est pas récursive.
Le c) résulte aussi de a): on rajoute $-\sqrt{2}$ (qui est dans $\mathbb{R}_{MIR}(\mathcal{P})$) à la $\mathcal{P}$-suite dans $\mathbb{R}_{MIR}$: $(\sqrt{2} + v_p)_{p\in\mathbb{N}_1}$ ❑

Proposition 3.10 : Le test $x \in \mathbb{Q}$? n'est pas donné par un test récursif lorsque $x \in \mathbb{R}_{CUT}(\mathcal{P})$ (ou $\mathbb{R}_{MIR}(\mathcal{P})$, ou $\mathbb{R}_{CONT}(\mathcal{P})$)

preuve> Il suffit de le démontrer pour $\mathbb{R}_{CONT}(\mathcal{P})$. Considérons la $\mathcal{P}$-suite dans $\mathbb{R}_{CONT}$, $(x^p)_{p\in\mathbb{N}_1}$, définie par :

$$a_{n+1}(x^p) := \left| u_n - p \right|,\ a_0(x^p) := 1$$

On a $x^p \in \mathbb{Q}$ si et seulement si "p est de la forme u_n" ($p \in U$).
Ce test n'est donc pas récursif, alors que (x^p) est une $\mathcal{P}$-suite dans $\mathbb{R}_{CONT}$. ❑

Une fonctionnelle intéressante

Nous utilisons une fonctionnelle en temps polynomial qui permet d'exprimer un réel à la Cauchy comme somme de 2 réels à la Dedekind. Cette fonctionnelle n'est pas extensionnelle et ne correspond donc à aucune fonction de $\mathbb{R}$ vers $\mathbb{R}^2$

Théorème 3.11 : Il existe une fonctionnelle en temps polynomial :

$$\mathcal{F} : \mathbb{R}_{CONV} \longrightarrow \mathbb{R}_{MIR} \times \mathbb{R}_{MIR}$$

Vérifiant : si $x \in \mathbb{R}_{CONV}$ et $\mathcal{F}(x) = (s,t)$ alors $x =_{\mathbb{R}} s + t$.

preuve> Utilisons la présentation suivante $\mathcal{P}$-équivalente à $\mathbb{R}_{CONV}$: un réel x est représenté par un élément

$$(c_0,(a_n)_{n\in\mathbb{N}_1^*}) \in \mathbb{Z} \times \{1,2,3\}^{\mathbb{N}_1^*}$$

avec l'égalité :

$$x = c_0 + \sum_{i=0}^{\infty} \frac{a_i}{2^i}$$

L'idée est d'écrire a_i sous forme $t_i + s_i$ avec l'un des deux égal à 0 ; de plus on choisit les t_i nuls sur des intervalles de longueur régulièrement croissante : le réel t obtenu est alors suffisamment irrationnel. Plus précisément on définit :

$t_i = a_i$ si $i \in [(2n)^2,(2n+1)^2[$, $t_i = 0$ sinon

$s_i = a_i$ si $i \in [(2n+1)^2,(2n+2)^2[$, $s_i = 0$ sinon

La fonctionnelle $\mathcal{G} : x \mapsto (s,t)$ de $\mathbb{R}_{CONV}$ vers $\mathbb{R}_{CONV} \times \mathbb{R}_{CONV}$ est évidemment en temps polynomial : on calcule sur l'entrée $i \in \mathbb{N}_1$ la partie entière $m = Ent(\sqrt{i})$, puis, selon qu'on calcule s ou t et selon la parité de m on donne la sortie 0 ou a_i (qui est obtenu en questionnant l'oracle $(a_n)_{n\in\mathbb{N}_1}$).

Il s'agit de voir que cette fonctionnelle se factorise par $\mathbb{R}_{MIR} \times \mathbb{R}_{MIR}$ selon le schéma :

$$\begin{array}{ccccc} R_{CONV} & \longrightarrow & \mathcal{F} & \longrightarrow & R_{MIR} \times R_{MIR} \\ & \mathcal{G} \searrow & & & \downarrow \text{ canonique} \\ & & \mathbb{R}_{CONV} \times \mathbb{R}_{CONV} & & \end{array}$$

Raisonnons pour le calcul de s : il s'agit donc, à partir de l'entrée $a/b \in \mathbb{Q}$ et en utilisant l'oracle $(s_n)_{n\in\mathbb{N}_1}$ de calculer en temps polynomial un rationnel a'/b' situé entre a/b et s . Pour cela il nous suffit d'établir une inégalité : $|\, a/b - s \,| > 1/2^{P(\mathbf{lg}(b))}$ où P est un polynome:

on note $$s(k) = x = c_0 + \sum_{i=0}^{4k^2} \frac{s_i}{2^i}$$

et posons $k = \mathbf{lg}(b)$, alors :

si $\frac{a}{b} = s(k)$ on a $$\left| s - \frac{a}{b} \right| = \sum_{4k^2+4k+1}^{\infty} \frac{s_i}{2^i}$$

et par suite

$$\left| s - \frac{a}{b} \right| > \frac{1}{2^{4k^2+4k+1}}$$

sinon on a

$$\left| s(k) - \frac{a}{b} \right| > \frac{1}{b.2^{4k^2}} > \frac{1}{2^{4k^2+4k+1}}$$

et on a $$\left| s - s(k) \right| = \sum_{4k^2+4k+1}^{\infty} \frac{s_i}{2^i} \leq \frac{3}{2^{4k^2+4k}}$$

En utilisant l'inégalité triangulaire on obtient

$$\left| s - \frac{a}{b} \right| > \frac{1}{2^{4k^2+4k}} \qquad \square$$

On en déduit immédiatement :

Proposition 3.12 :

a) Il n'existe pas de fonction récursive
$$\mathbb{R}_{MIR}(\mathcal{P}) \times \mathbb{R}_{MIR}(\mathcal{P}) \longrightarrow \mathbb{R}_{MIR}$$
qui représente l'addition dans $\mathbb{R}$

b) même résultat avec
$$\mathbb{R}_{CUT}(\mathcal{P}) \times \mathbb{R}_{CUT}(\mathcal{P}) \longrightarrow \mathbb{R}_{CUT}$$

c) même résultat avec
$$\mathbb{R}_{CONT}(\mathbf{Pr}) \times \mathbb{R}_{CONT}(\mathbf{Pr}) \longrightarrow \mathbb{R}_{CONT}$$

preuve> (a) En composant cette fonction et la fonctionnelle du théorème 3.11 on contredirait la proposition 3.8(f)

(b) Même raisonnement.

(c) Pour $\mathbb{R}_{CONT}$, utiliser le fait que $\mathbb{R}_{CONT}$ et $\mathbb{R}_{MIR}$ sont **Pr**-équivalents $\square$

4. OBJETS DE FAIBLE COMPLEXITÉ AYANT UNE IMAGE D'UNE COMPLEXITÉ ARBITRAIREMENT GRANDE

Dans la suite, nous utilisons un "lemme fondamental" pour construire des réels convenables. Rappelons tout d'abord la version en unaire du théorème de hiérarchie et un lemme sur les fonctions constructibles en temps.

Théorème de hiérarchie (en unaire) :

Soient T_1 et T_2 deux fonctions récursives de $\mathbb{N}$ vers $\mathbb{N}^*$ vérifiant:

- T_1 est constructible en temps avec $T_1(n) \geq 2^n$
- $T_2(n) \geq n$
- $T_2(n) \cdot \log(T_2(n)) / T_1(n)$ tend vers 0

Alors, il existe une partie A de $\mathbb{N}_1$ qui est dans **DTIME**$(T_1(n))$ mais pas dans **DTIME**$(T_2(n))$

Lemme :

a) Si S et T sont deux fonctions constructibles en temps alors la composée de S et T est également constructible en temps

b) Si S est constructible en temps et vérifie: $S(n) \geq 2.n$,
alors la fonction U construite par récurrence à partir de S :
$U(1) := a \quad U(n+1) := S(U(n))$
est également constructible en temps

Lemme fondamental : Pour toute fonction récursive croissante V il existe une fonction U constructible en temps , et une partie A de $\mathbb{N}_1$, de fonction caractéristique χ_A vérifiant :

- $\chi_A(n)$ est calculable en temps $U(n)$
- $\chi_A(n+1)$ n'est pas calculable en temps $V(U(n))$

(autrement dit $A \in$ **DTIME**$(U(n))$ mais $1 + A \notin$ **DTIME**$(V(U(n)))$

preuve> On majore V par une fonction croissante S constructible en temps. Il suffit d'établir le lemme avec S. Soit U la fonction définie par:

$U(1) := 1$; $U(n+1) := 2^{S(U(n))}$

Alors, d'après le théorème de hiérarchie en unaire et le lemme, il existe une partie A de $\mathbb{N}_1$ reconnaissable en temps U mais pas en temps $\log_2(U)$ c.-à-d. :

$\chi_A(n)$ est calculable en temps $U(n)$, mais $\chi_A(n+1)$ n'est pas calculable en temps $S(U(n))$ ❑

Théorème 4.1 : Pour toute fonction récursive croissante $T(n)$ il existe un nombre réel x qui est dans $\mathbb{R}_{CONV}$(**LINTIME**) mais pas dans $\mathbb{R}_{CUT}$(**DTIME**$(T(n))$)

preuve> Soit $V(n) := T(2n)$, et U construite à partir de V comme dans le lemme fondamental. Soit x défini par :

$$x := \sum_{i=0}^{\infty} \frac{2\chi_A(i) - 1}{2^{U(i)}}$$

Pour tout entier $n \in \mathbb{N}_1$ la recherche de l'entier $k \in \mathbb{N}_1$ tel que $U(k) \le n < U(k+1)$ coûte $O(n)$.

Soit $$d_n := \sum_{i=0}^{k} \frac{2\chi_A(i) - 1}{2^{U(i)}}$$

Alors (d_n) (en tant que suite de rationnels, avec $n \in \mathbb{N}_1$) est dans **LINTIME** et on a la majoration :

$$\left| x - d_n \right| \le \frac{1}{2^{U(k+1)}} < \frac{1}{2^n}$$

Et donc x est dans $\mathbb{R}_{CONV}$(**LINTIME**) .

Mais le signe de $x - d_n$ est donné par $\chi_A(k+1)$, qui n'est pas calculable en temps $T(2U(k))$; et la taille de d_n est majorée par $2\,U(k)$ ❑

Dans le corollaire qui suit $\mathbb{R}_{CONV2}$(**LINTIME**) désigne la partie **LINTIME** de $\mathbb{Z} \times \{-1,0,1\}^{\mathbb{N}_1}$. L'ensemble $\mathbb{R}_{CONV2}$(**LINTIME**) est énumérable de la même manière que $\mathbb{R}_{CONV2}(\mathcal{P})$ (traité au début de la section 3.2, et $\mathcal{P}$-équivalent à $\mathbb{R}_{CONV}(\mathcal{P})$).

On notera les "inclusions":

$\mathbb{R}_{CONV2}$(**LINTIME**) $\subset$ $\mathbb{R}_{CONV}$(**DTIME**$(O(n^2))$

$\mathbb{R}_{CONV}$(**LINTIME**) $\subset$ $\mathbb{R}_{CONV2}$(**DTIME**$(O(n^{1+\varepsilon}))$ avec ε arbitrairement petit

Corollaire 4.2 : Il n'existe pas de fonction récursive de $\mathbb{R}_{CONV2}$(**LINTIME**) vers $\mathbb{R}_{CUT}$ qui représente l'identité de $\mathbb{R}$. (cela renforce la résultat obtenu à la proposition 3.8(f))

Théorème 4.3 : Pour toute fonction récursive croissante $T(n)$ il existe un nombre réel x qui est dans $\mathbb{R}_{CUT}$(**LINTIME**) mais pas dans $\mathbb{R}_{MIR}$(**DTIME**$(T(n))$)

preuve> Soit S une fonction constructible en temps avec S(n) > T(2n)+n+1.
Définissons alors la fonction U par récurrence:

U(1):=1 , U(n+1):=S(U(n)).

On raisonne avec le nombre réel y défini par :

$$y := \sum_{i=0}^{\infty} \frac{1}{2^{U(i)}}$$

Montrons que y est dans $\mathbb{R}_{CUT}$(**LINTIME**) .
Pour tout rationnel a/b , nous cherchons un entier k tel que

$$2^{U(k)-U(k-1)-1} \leq b < 2^{U(k+1)-U(k)-1}$$

ce qui coûte O(**lg**(b)) . On pose

$$e_k := \sum_{i=0}^{k} \frac{1}{2^{U(i)}}$$

On ne peut avoir $e_k \leq a/b < y$, car sinon

$$\frac{1}{b\,2^{U(k)}} \leq \frac{a}{b} - e_k < y - e_k \leq \frac{1}{2^{U(k+1)-1}}$$

ce qui impliquerait $b > 2^{U(k+1)-U(k)-1}$: contradiction .
On a donc: $a/b < y \Leftrightarrow a/b \leq e_k$
Montrons maintenant que y n'est pas dans $\mathbb{R}_{MIR}$(**DTIME**(T(n))) :

$$y - e_k \leq \frac{1}{2^{U(k+1)-1}} \quad \Rightarrow \quad \left| \mu(e_k) - e_k \right| < \frac{1}{2^{U(k+1)-1}}$$

ce qui implique:

dénominateur de $\mu(e_k) \geq 2^{U(k+1)-U(k)-1}$,
donc taille de $\mu(e_k) \geq U(k+1) - U(k) - 1$
et $U(k+1) > T(2U(k)) + U(k) + 1$
mais la taille de e_k est majorée par $2\,U(k)$ ❑

Remarque : On ne peut pas déduire du théorème 4.3 un résultat négatif analogue au corollaire 4.2 du théorème 4.1 : c'est parce que $\mathbb{R}_{CUT}$(**LINTIME**) ne peut pas être énuméré de manière effective (contrairement à $\mathbb{R}_{CONV2}$(**LINTIME**))

Théorème 4.4 : Pour toute fonction récursive croissante T(n) il existe deux nombres réels s et t qui sont dans $\mathbb{R}_{MIR}(\mathcal{P})$ mais dont la somme n'est pas dans $\mathbb{R}_{CUT}$(**DTIME**(T(n))) (et a fortiori n'est pas dans $\mathbb{R}_{MIR}$(**DTIME**(T(n))))

preuve> On écrit le nombre x construit au théorème 4.1 sous forme s + t , conformément à la construction décrite au théorème 3.11 ; x est dans $\mathbb{R}_{CONV}$(**LINTIME**) donc s et t sont dans $\mathbb{R}_{MIR}(\mathcal{P})$ ❑

Remarque: En fait s et t sont dans $\mathbb{R}_{MIR}$ (**DTIME**($O(n^3)$))

5. ÉTUDE DETAILLÉE DE LA PRÉSENTATION VIA LES FRACTIONS CONTINUES

5.1. Comparaison de $\mathbb{R}_{CONT}$ *et* $\mathbb{R}_{CUT}$

Notations :
Si f est une fonction de $\mathbb{N}_1^*$ vers $\mathbb{N}$, nous appellerons *sous-graphe de* f la partie sous le graphe de f, c.-à-d. l'ensemble des couples (n, m) de $\mathbb{N}_1^* \times \mathbb{N}$ vérifiant $m \leq f(n)$, et nous noterons Σf la fonction de $\mathbb{N}_1^*$ vers $\mathbb{N}$ définie par:

$$\Sigma f(n) := \sum_{i=1}^{n} f(n)$$

Le théorème qui va suivre affirme que, du point de vue "temps polynomial", il revient au même de se donner la coupure de Dedekind d'un réel x ou de se donner le sous-graphe de Σf, où f(n) est le $n^{ème}$ quotient partiel de la fraction continue de x.
Ceci nous conduit à adopter la notation $\mathbb{R}_{CONTSOUS}$ pour une nouvelle présentation de $\mathbb{R}$:

> $\mathbb{R}_{CONTSOUS}$ est la partie de $\mathbb{Z} \times \{0,1\}^{\mathbb{N}_1^* \times \mathbb{N}}$ formée par les couples (e, g) où g est la fonction caratéristique du sous-graphe d'une fonction croissante de $\mathbb{N}_1^*$ vers $\mathbb{N}$: un tel couple représente le même réel x que celui représenté dans $\mathbb{R}_{CONT}$ par le couple (e,f), où f(1) := g(1) et f(n) := g(n) – g(n–1) pour n > 1.

La complexité d'une fonction f de $\mathbb{N}_1^*$ vers $\mathbb{N}$ peut être appréhendée sous deux aspects : la complexité du sous-graphe de Σf d'une part, le taux de croissance de Σf d'autre part. Il est clair que le passage d'une fonction f au sous-graphe de Σf est donné par une $\mathcal{P}$-fonctionnelle. Le théorème qui suit précise donc quelle est la partie de l'information disponible dans $\mathbb{R}_{CONT}$ qui est utilisée dans $\mathbb{R}_{CUT}$.

Théorème 5.1 :

> $\mathbb{R}_{CUT}$ et $\mathbb{R}_{CONTSOUS}$ sont deux présentations $\mathcal{P}$-équivalentes de $\mathbb{R}$. Plus précisément :
> a) Il existe une $\mathcal{P}$-fonctionnelle de $\mathbb{Z} \times \{-1,0,1\}^{\mathbb{Q}}$ vers $\mathbb{Z} \times \{0,1\}^{\mathbb{N}_1^* \times \mathbb{N}}$ qui envoie $\mathbb{R}_{CUT}$ dans $\mathbb{R}_{CONTSOUS}$ et dont la restriction à $\mathbb{R}_{CUT}$ représente l'identité de $\mathbb{R}$
> b) Il existe une $\mathcal{P}$-fonctionnelle de $\mathbb{Z} \times \{0,1\}^{\mathbb{N}_1^* \times \mathbb{N}}$ vers $\mathbb{Z} \times \{-1,0,1\}^{\mathbb{Q}}$ qui envoie $\mathbb{R}_{CONTSOUS}$ dans $\mathbb{R}_{CUT}$ et dont la restriction à $\mathbb{R}_{CONTSOUS}$ représente l'identité de $\mathbb{R}$.

preuve> Soit tout d'abord un élément (z,t) de $\mathbb{Z} \times \{-1,0,1\}^{\mathbb{Q}}$. Cela signifie que nous avons une donnée z et un oracle t. Nous allons décrire une fonctionnelle en temps polynomial (temps majoré indépendamment des sorties de l'oracle) qui, lorsque (z,t) est dans $\mathbb{R}_{CUT}$, calcule le sous-graphe du dfc du réel x représenté par (z,t). Nous avons donc une $2^{ème}$ donnée: un couple (n,m) dans $\mathbb{N}_1^* \times \mathbb{N}$ pour lequel il nous faut décider si $m \leq \Sigma f(n)$, avec $f(n) = a_n(x)$ (lorsque (z,t) est convenable).
Nous allons raisonner en supposant (z,t) dans $\mathbb{R}_{CUT}$, mais le lecteur pourra vérifier que l'hypothèse n'est pas nécessaire pour la majoration du temps de calcul.
Tout d'abord la partie entière e de x est z+1 ou z (on demande t(z+1) pour décider).
Le principe est de faire successivement les calculs:

- tester $m \le f(1)$?, si la réponse est oui: terminé, sinon calculer f(1)
- tester $m \le \Sigma f(2)$?, si la réponse est oui: terminé, sinon calculer f(2)
etc ...
- tester $m \le \Sigma f(k)$?, si la réponse est oui: terminé, sinon calculer f(k)
..... jusqu'à ce que $k=n$ (si on n'est pas arrêté avant)
Posons $m_0 := m$
On a tout d'abord : $m_0 \le f(1) \Leftrightarrow 1/m_0 \ge x_1 := x - e \Leftrightarrow e + 1/m_0 \ge x$
On interroge donc l'oracle pour $e + 1/m_0$.
Si la réponse est: $x \le e + 1/m_0$, on a terminé, puisque $m_0 \le f(1) \le \Sigma f(k)$. Sinon, on dispose du majorant m_0 de $f(1)$ qui va nous permettre de calculer $f(1)$ par dichotomie dans $\mathbb{N}$ à partir des valeurs initiales 1 et m_0. Ceci nécessite d'interroger au maximum **lg**(m) fois l'oracle pour des valeurs $e + 1/m_{0,i}$ où $m_{0,i}$ est entre 1 et m_0.
Supposons maintenant avoir obtenu "$m > \Sigma f(k)$" et avoir calculé $f(k)$ avec $k < n$.
On pose $m_k := m - \Sigma f(k)$. On a calculé par la même occasion les convergents p_{k-1}/q_{k-1} et p_k/q_k . On connaît donc la fonction homographique H_k telle que $Ent(H_k(x)) = f(k+1)$, ainsi que la fonction homographique réciproque L_k . On a alors :

$$m \le \Sigma f(k+1) \Leftrightarrow m_k \le f(k+1) \Leftrightarrow m_k \le H_k(x) \Leftrightarrow x \perp L_k(m_k)$$

où $\perp$ représente $\le$ ou $\ge$ selon la parité de k .
On interroge donc l'oracle pour $L_k(m_k)$. Si $m \le \Sigma f(k+1)$ on sait que $m \le \Sigma f(n)$. Dans le cas contraire on calcule $f(k+1)$ par dichotomie puisqu'on dispose du majorant m_k pour $f(k+1)$, ce qui nécessite d'interroger l'oracle pour "peu de" valeurs $L_k(m_{k,i})$ où $m_{k,i}$ est entre 1 et m_k .
Il est clair que les m_k, p_k et q_k restent de taille polynomialement majorée en fonction de la taille des données n , m et z . Et donc que le temps de calcul peut être polynomialement majoré indépendamment des réponses données par l'oracle. (Remarquons en passant que si (z,t) n'est pas dans $\mathbb{R}_{CUT}$, les réponses données par l'algorithme ci-dessus peuvent très bien ne pas correspondre au sous graphe d'une fonction croissante).

Passons à la fonctionnelle dans l'autre sens.
Nous avons comme données : un rationnel a/b , la partie entière e de x, et nous disposons d'un oracle pour le sousgraphe de Σf (où le dfc de x est $[e; f(1), f(2), ... , f(n),....]$. Il nous faut comparer x à a/b.
Nous commençons par remarquer que la donnée a/b peut être traduite sous forme de dfc $[c_0; c_1, ..., c_k]$ (où $c_k \ge 2$ si $k \ge 1$).
Notons également que si nous connaissons un réel y dans $\mathbb{R}_{CONT}$:
$y = [a_0; a_1, ..., a_n, ...]$, la comparaison de y à a/b peut être obtenue directement à partir des dfc selon l'algorithme suivant:

Si $\exists\, j < k$ tel que $a_j \ne c_j$ soit i le premier indice, **alors**:
  si $a_i = 0$ $\quad sg(a/b - y) := (-1)^{i+1}$
  sinon $\quad sg(a/b - y) := (-1)^{i+1}\, sg(a_i - c_i)$
sinon
  si $a_k \le c_k - 2$ $\quad sg(a/b - y) := (-1)^k$
  si $a_k > c_k$ $\quad sg(a/b - y) := (-1)^{k+1}$
  si $a_k = c_k$
    si $a_{k+1} = 0$ $\quad a/b = y \quad (sg(a/b - y) := 0)$

sinon $sg(a/b - y) := (-1)^k$

si $a_k = c_k - 1$

si $a_{k+1} = 1$ **et** $a_{k+2} = 0$ $a/b = y$ ($sg(a/b - y) := 0$)

sinon $sg(a/b - y) = (-1)^{k+1}$

En ce qui concerne x, nous connaissons seulement le sous graphe de Σf, mais nous pouvons procéder de proche en proche comme suit:

comparer e et c_0 :
si $e \neq c_0$ comparer x à a/b selon l'algorithme ci-dessus
sinon
tester : $c_1 \leq f(1)$? , et : $c_1 - 1 \leq f(1)$? pour connaître $sg(c_1 - f(1))$:
si $c_1 \neq f(1)$ comparer x à a/b selon l'algorithme ci–dessus
sinon
on sait que $f(1) = c_1$ et on peut connaître $sg(c_2 - f(2))$ en testant :
$c_1 + c_2 \leq \Sigma f(2)$? , et : $c_1 + c_2 - 1 \leq \Sigma f(2)$? :
si $c_2 \neq f(2)$ comparer x à a/b selon l'algorithme ci–dessus **etc...**
NB : si on arrive jusqu'à l'indice k il faudra en outre tester
$f(k) = c_k - 1$ et $f(k+1) = 1$?

L'ensemble du calcul est polynomialement majoré en temps à partir de la taille des données ❑

5.2. Taux de croissance du développement en fraction continue et mesure d'irrationalité

Nous avons indiqué au début de la section 5.1 que la complexité d'une fonction

$$f : \mathbb{N}_1 \longrightarrow \mathbb{N}$$

pouvait être appréhendée sous deux aspects:

- la complexité du sous-graphe de de Σf
- le taux de croissance de Σf

Pour $[e, f(1), f(2), ...]$ dans $\mathbb{R}_{CONT}$ nous avons explicité la complexité du sous-graphe de Σf, en la reliant à celle de la coupure de Dedekind du réel correspondant x. Nous allons maintenant obtenir une interprétation du taux de croissance de Σf en termes de la mesure d'irrationalité sans signe de x.

Tout d'abord précisons que nous utiliserons une *mesure d'irrationalité sans signe <u>en unaire</u>* pour le réel x, c.-à-d. précisément :

une fonction <u>croissante</u> $\varphi : \mathbb{N}_1 \longrightarrow \mathbb{N}_1$ telle que l'on ait pour tout rationnel p/q :

$$|x - p/q| > 1/2^{\varphi(\mathbf{lg}(q))}$$

Proposition 5.2 :

a) Si φ est une mesure d'irrationalité sans signe en unaire pour un réel x donné dans $\mathbb{R}_{CONT}$ sous forme $[e, f(1), f(2), ...]$, alors on a pour tout n :

$$\mathbf{lg}(f(n+1)) \leq \psi(n.\mathbf{lg}(\Sigma f(n))) \quad (1)$$

b) Inversement, si une fonction ψ croissante vérifie l'inégalité (1) ci-dessus, alors on obtient une mesure d'irrationalité sans signe en unaire pour le réel x en posant :

$$\varphi(n) := 3 + 2n + 2\psi(2n^2) + \psi((1+2n)(1+n+\psi(2n^2))$$

En particulier φ est polynomialement majorée si et seulement si ψ est polynomialement majorée

preuve> On note p_n/q_n les convergents successifs de x . On a les inégalités:

$$\mathbf{lg}(\Sigma f(n)) \le \mathbf{lg}(q_n) \le n\,\mathbf{lg}(\Sigma f(n))$$

$$2\,\mathbf{lg}(q_n) \ge n-1$$

$$\frac{1}{q_n(q_n+q_{n+1})} < \left| x - \frac{p_n}{q_n} \right| \le \frac{1}{q_n\,q_{n+1}} \qquad (2)$$

$$\left| x - \frac{p}{q} \right| > \left| x - \frac{p_n}{q_n} \right| \text{ où } n \text{ est le premier indice tel que } q_n > q \qquad (3)$$

Si φ est donnée, on a: $\mathbf{lg}(f(n+1)) \le \mathbf{lg}(q_{n+1}) \le \varphi(\mathbf{lg}(q_n))$ d'après (2)
Comme φ est croissante, on a $\varphi(\mathbf{lg}(q_n)) \le \varphi(n.\mathbf{lg}(\Sigma f(n))$, d'où l'inégalité (1).
Inversement, si ψ vérifie l'inégalité (1) , alors d'après (2) et (3) on a:

$$\mathbf{lg}(q_n.(q_n+q_{n+1})) \le 2\,\mathbf{lg}(q_n) + \mathbf{lg}(2+f(n+1)) \le 2\,\mathbf{lg}(q_n) + 1 + \psi(n.\mathbf{lg}(\Sigma f(n)))$$

D'où :

$$\mathbf{lg}(q_n) \le \mathbf{lg}(q_{n-1}) + \mathbf{lg}(1+f(n)) \le \mathbf{lg}(q) + 1 + \psi((n-1).\mathbf{lg}(\Sigma f(n-1))$$
$$\le \mathbf{lg}(q) + 1 + \psi(2\,\mathbf{lg}(q)^2)$$

on réutilise

$$\mathbf{lg}(\Sigma f(n)) \le \mathbf{lg}(q_n)$$

et on obtient l'égalité de la proposition 5.2(b) ❑

5.3. Non stabilité de $\mathbb{R}_{\mathsf{CONT}}(\mathcal{P})$ pour l'addition

Fractions continues à la Shallit

Pour construire 2 réels dans $\mathbb{R}_{\mathsf{CONT}}(\mathcal{P})$ dont la somme n'est pas dans $\mathbb{R}_{\mathsf{CONT}}(\mathbf{DTIME}(T(n))$ où T est une fonction récursive croissante donnée, nous utilisons les fractions continues découvertes par Jeffrey Shallit [**Sha**].

Hypothèses communes pour le Théorème de Shallit et le lemme qui suit :
Soit $T : \mathbb{N}_1 \longrightarrow \mathbb{N}_1$ une fonction croissante vérifiant

$T(n+1) \ge 2T(n)$ pour tout entier $n \ge n_0$,

et soit $d(n) := T(n+1) - 2\,T(n)$.

On pose

$$B(u,n) := \sum_{k=0}^{n} \frac{1}{u^{T(k)}} \quad \text{où u est un entier} \ge 2$$

Théorème de Shallit :

Si $n \ge n_0$ et $B(u,n) = [a_0, \ldots, a_p]$, où on a choisi le développement en fraction continue avec p pair (a_p peut donc être égal à 1), alors:

$$B(u,n+1) = [a_0, \ldots, a_p, u^{d(n)}-1, 1, a_p-1, a_{p-1}, \ldots, a_1] \quad (*)$$

(*) (où une écriture $[a_0, \ldots, b, c, 0, d, e, \ldots]$ se contracte en $[a_0, \ldots, b, c+d, e, \ldots]$)

Par suite, lorsque $n_0 = 0$, $T(0) \ge 1$, et $d(n) \ge 1$ pour tout n , la fraction continue de $B(u,\infty)$ est donnée par:

$$[0, v-1, 1, u^{d(0)}-1, v, u^{d(1)}-1, 1, v-1, u^{d(0)}-1, 1, v-1, u^{d(2)}-1, ...]$$

où $v = u^{T(0)}$ et sans aucune "contraction". On remarque alors que les seuls quotients partiels sont $v-1$, v, 1, et les $u^{d(i)}-1$, et donc $B(u,\infty)$ est à quotients partiels bornés si et seulement si les $u^{d(i)}$ sont bornés.
On en déduit le lemme suivant.

Lemme : Si $n_0 = 0$, $T(0) \geq 1$, $d(n) \geq 1$ (pour tout n), et si la fonction $n \mapsto d(\mathbf{lg}(n))$: $\mathbb{N}_1 \longrightarrow \mathbb{N}_1$, est calculable en temps polynomial, alors le dfc de $B(u,\infty)$ est calculable en temps polynomial.

preuve> Soit n un entier en unaire, on cherche à calculer le $n^{ème}$ quotient partiel de $B(u,\infty)$.
On calcule le dfc pair

$$[0; u^{T(0)}-1, 1, u^{d(0)}-1, u^{T(0)}]$$

de $B(u,1)$, où on a $u^{T(0)}-1 \geq 1$; puis les dfc pairs de $B(u,2)$, ... , $B(u,k)$ par application répétée du théorème de Shallit, sans jamais aucune contraction, jusqu'à ce que le dernier indice du dfc obtenu dépasse $n+1$.
A chaque étape, le dfc voit son dernier indice multiplié par 2. On s'arrête donc à un $k < \mathbf{lg}(n)+1$.
La taille des dfc successifs reste majorée par un polynome fixé en n. Le temps de calcul pour chaque étape est convenablement majoré : on calcule $m = d(i)$ en unaire, d'où on déduit u^m en binaire, et il reste juste un travail de recopie (2 fois) du dfc précédent. ❑

Remarque : Les hypothèses du lemme pourraient être affaiblies.

Le théorème suivant résout une conjecture dans [**Ko2**].

Théorème 5.3 :

Pour toute fonction récursive croissante T, il existe deux nombres réels x, y dans $\mathbb{R}_{CONT}(\mathcal{P})$ mais dont la somme n'est pas dans $\mathbb{R}_{MIR}(\mathbf{DTIME}(T(n)))$
(ni dans $\mathbb{R}_{CONT}(\mathbf{DTIME}(T(n)))$ donc)

preuve>
Soit $S : \mathbb{N}_1 \longrightarrow \mathbb{N}_1$ une fonction constructible en temps vérifiant :
- $S(n) \geq n$ pour tout n, et
- le test " k est-il de la forme $S(j)$? " (où k est en unaire) est en temps polynomial.

Soit $d : \mathbb{N}_1 \longrightarrow \mathbb{N}_1$ une fonction calculable en temps polynomial avec $d(n) \geq 2$ pour tout n.
Soit $T_1 : \mathbb{N}_1 \longrightarrow \mathbb{N}_1$ une fonction telle que:
- $T_1(0) \geq 2$
- $T_1(n+1) - 2\,T_1(n) = d(n)$

On pose $T_2(k) := T_1(S(k))$ et on définit les nombres réels x et y :

$$x := \sum_{k=0}^{\infty} \frac{1}{2^{T_1(k)}} \quad , \qquad y := \sum_{k=0}^{\infty} \frac{1}{2^{T_2(k)}}$$

Posons $z := x + y$, on a alors :

$$z := \sum_{k=0}^{\infty} \frac{1}{2^{T_3(k)}} \quad \text{où} \quad T_3(k) = \begin{cases} T_1(k) - 1 & \text{si } k = S(j) \\ T_1(k) & \text{sinon} \end{cases}$$

On a donc pour la fonction T_3 :

– $T_3(0) \geq 1$

– $T_3(n+1) - 2\,T_3(n) = d_3(n)$ avec $d_3(n) \geq 1$ pour tout n

De plus d_3 est calculable en temps polynomial puisque:

– $d_3(n) = \begin{cases} d(n) & \text{si } n \text{ et } n+1 \text{ ne sont pas de la forme } S(j) \\ d(n)+2 & \text{si } n \text{ est de la forme } S(j) \\ d(n)-1 & \text{si } n+1 \text{ est de la forme } S(j) \end{cases}$

Donc x et z ont un dfc calculable en temps polynomial. Donc $-x$ a également un dfc calculable en temps polynomial. Par contre le dfc de $y = z + (-x)$ n'est pas dans $\mathbb{R}_{MIR}(\mathbf{DTIME}(T(n)))$ pour peu que l'on ait l'inégalité :

$$T_2(k+1) \geq T(2.T_2(k)) + T_2(k) + 1$$ (voir preuve du théorème 4.3).

Il suffit pour cela de choisir S de manière que :

$$S(k+1) \geq T(2.T_1(S(k))) + T_1(S(k)) + 1$$ ❑

On déduit du théorème 5.3 une amélioration de la proposition 3.12(c).

Proposition 5.4 : Il n'existe pas de fonction récursive

$$\mathbb{R}_{CONT}(\mathcal{P}) \times \mathbb{R}_{CONT}(\mathcal{P}) \longrightarrow \mathbb{R}_{CONT}$$

qui représente l'addition dans $\mathbb{R}$.

preuve> Soit $\varphi : \mathbb{N} \longrightarrow \mathbb{R}_{CONT}(\mathcal{P})$ une énumération effective de $\mathbb{R}_{CONT}(\mathcal{P})$. Une fonction récursive ϕ de $\mathbb{R}_{CONT}(\mathcal{P}) \times \mathbb{R}_{CONT}(\mathcal{P})$ vers $\mathbb{R}_{CONT}$ est alors donnée, via l'énumération φ , par deux fonctions récursives

$$\phi_1 : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Z} \ , \ \phi_2 : \mathbb{N} \times \mathbb{N} \times \mathbb{N}_1 \longrightarrow \mathbb{N} \ ,$$

telles que le dfc de $\phi(\varphi(i),\varphi(j))$ est

$$[\, \phi_1(i,j) \,;\, \phi_2(i,j,1) \,,\, \phi_2(i,j,2) \,,\ \text{etc.} \,]$$

La fonction récursive ϕ_2 a une complexité en temps S . Si i et j sont fixés, le dfc de $\phi(\varphi(i),\varphi(j))$ a alors une complexité en temps bornée par $S(C_{ij} + n)$. Mais il existe une fonction récursive T croissant plus vite que toutes les fonctions $n \mapsto S(C+n)$. D'où une contradiction avec le théorème 5.3. ❑

Henri LOMBARDI
UFR des Sciences et Techniques
Laboratoire de Mathématiques
Université de Franche-Comté
25030 BESANCON Cédex
FRANCE

Salah LABHALLA
Département de Mathématiques
Université de Marrakech
Bd de SAFI. BP S 15
MARRAKECH
MAROC

Bibliographie

[IM] S.C Kleene Introduction to Metamathematics 1952

[Kh] A. Ya Khintchine. Continued fractions . P. Noordhoff Ltd. Netherlands 1963

[KF] Ker-I. KO, Harvey Friedman : Computational complexity of real functions Theoretical Computer Science 20, (1982), 323-352 .

[Ko1] Ker I. KO. On the definitions of some complexity classes of real numbers. Math System Theory 16 , 95-109 , 1983.

[Ko2] Ker-I Ko On the continued fraction representation of computable real numbers. Theoretical Computer Science 47 (3), 299-313 (1986) . Correction dans TCS 54 (2,3), 341-343 (1987) .

[Lab] S. Labhalla. Complexité du calcul du développement d'un nombre réel en fraction continue. Theoretical Computer Science 83, 219-235 (1991) .

[LL1] Labhalla S., Lombardi H. : Real numbers, continued fractions, and complexity classes. Annals of Pure and Applied Logic 50, 1-28 (1990).

[LL2] Labhalla S., Lombardi H. : Comparaison des complexités des nombres réels dans différentes représentations (à la Cauchy, à la Dedekind, par fractions continues). C.R.A.S. Paris, t. 310, Série I, p 483-488, 1990.

[LL3] Labhalla S., Lombardi H. : Comparaison des nombres réels du point de vue des fonctionnelles récursives. C.R.A.S-Paris, t 311, Série I, p 229-234, 1990.

[LL4] Labhalla S., Lombardi H. : Représentations des nombres réels par développements en base entière et complexité. Theoretical Computer Science 88, 171-182 (1991)

[Ric] H. G. Rice. Recursive real numbers, Proc. Amer. Math. Soc. 5, 784-791 (1954) .

[Sha] Jeffrey O. Shallit. : Simple continued fractions for some irrational numbers II. Journal of Number Theory 14 , 228-231, 1982

[Spe] E. Specker Nicht Konstructive beweisbare Saltze der analysis. J. of Symbolic Logic 14, 145-158, 1949

[Tow] Townsend, M. : Complexity for type-2 relations. Notre Dame Journal of Formal Logic 31 (2), 241-262, 1990

[Tu] A. M. Turing. On computable numbers, with an application to the Entscheidungs problem . Proc London Math Soc 42, 230-265, 1937