Analyse de complexité pour un théorème de Hall sur les fractions continues

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

Résumé : Nous donnons dans cet article un traitement algorithmique et controlé en temps polynomial d'un théorème établi par M. Hall en 1947 : tout nombre réel peut s'écrire comme somme de deux nombres irrationnels dont les développements en fraction continue ne contiennent que les entiers 1, 2, 3 ou 4 (sauf éventuellement le premier terme) ..

Mots clés : nombres réels, fractions continues, fonctionnelles récursives, calculabilité en temps polynomial, théorème de Cantor, théorème de Hall

Abstract : We give in this paper a polynomial time controlled version of a theorem of M. Hall : every real number can be written as the sum of two irrational numbers whose dfcs contain only 1, 2 3 or 4..

Key words : real numbers, continued fractions, recursive functionals, polynomial time computability, Cantor theorem, Hall theorem.

Classification AMS : 11A55, 68Q25, 03F60

Introduction

Nous donnons dans cet article un traitement algorithmique et controlé en temps polynomial d'un théorème dû à M. Hall ([Hal] 1947) : tout nombre réel peut s'écrire comme somme de deux nombres irrationnels dont les développements en fraction continue ne contiennent que les entiers 1, 2, 3 ou 4 (sauf éventuellement le premier terme) . Contrairement à Hall (voir également [CF]), nous ne faisons pas appel au théorème de Cantor (toute suite décroissante des fermés bornés non vides de $\mathbb{R}$ admet une intersection non vide). Il s'agit en effet d'un argument non constructif.

En fait, M. Hall donne une preuve où il n'utilise que des majorations de certains rapports, et la preuve devient constructive en utilisant également des minorations des mêmes rapports.

La relation avec le théorème de Cantor est la suivante. Si on considère une suite décroissante explicite d'intervalles non vides $[a_i,b_i]$ on voit intuitivement que l'on ne peut pas en général expliciter un point x de l'intersection à partir de la seule donnée des deux suites (a_i) et (b_i) (révélées par des oracles), alors que c'est tout à fait facile si la longueur $\left| a_i - b_i \right|$ de l'intervalle converge explicitement vers 0 . Nous donnons différentes formes mathématiques de ce résultat négatif dans la section 3 . Lorsque $\left| a_i - b_i \right|$ tend explicitement vers 0 , l'intersection des intervalles est réduite à un seul point, que l'on calcule facilement en fonction des données. On retrouve le phénomène bien connu selon lequel un résultat d'existence classique abstrait devient souvent constructif lorsque l'unicité est assurée.

Notons $\mathbb{R}_{CONV}$ (resp. $\mathbb{R}_{CONT}$) l'ensemble des réels présentés à la Cauchy (resp. via les développements en fraction continue) Nous obtenons comme conséquence de notre explicitation de la preuve de Hall une fonctionnelle calculable en temps $O(n^2)$

$$\mathcal{F} : \mathbb{R}_{CONV} \to \mathbb{R}_{CONT} \times \mathbb{R}_{CONT} \qquad x \mapsto (y,z)$$

avec dans $\mathbb{R}$: $x = y + z$

Nous en déduisons qu'il existe des couples de réels dont le développement en fraction continue est calculable en temps $O(n^2)$ tandis que leur somme peut être de complexité supérieure à une complexité fixée a priori. Ceci améliore des résultats du même style que nous avions donné dans [Lab] et [LL].

Signalons pour terminer cette introdutction que notre attention a été attirée sur le théorème de Hall par l'excellent survey de J. Shallit [Sha].

1) Rappels, définitions

1.1) Rappels sur les fractions continues.

Un exposé de référence sur les développements en fraction continue est le livre de A. Ya Khintchine ([Khi]).

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 :

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

Dans le cas d'une suite infinie, nous notons également $/\, a_0, a_1, a_2, \ldots\ldots, a_n, \ldots /$ 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

$$/\, a_0, a_1, a_2, \ldots\ldots, a_n \,/ \quad \text{avec} \quad a_n > 1 \quad \text{si} \quad n \geq 1.$$

Dans la suite, nous abrégeons “développement en fraction continue” par **dfc**.

Soit $x := /\, a_0, a_1, a_2, \ldots\ldots, a_n, \ldots /$ et $p_n/q_n := /\, a_0, a_1, a_2, \ldots\ldots, a_n \,/$ (on suppose toujours que la fraction p_n/q_n est réduite).

L'entier a_n s'appelle le $n^{ème}$ quotient partiel et la fraction p_n/q_n le $n^{ème}$ convergent du réel x . Alors :

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

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

La fonction homographique associée à un dfc fini est :

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

1.2) Complexité d'algorithmes

Ce paragraphe et le suivant rappellent des définitions données dans [LL], où l'on pourra trouver plus de détails.

Nous notons $\mathbb{N}_1$ l'ensemble des entiers naturels présentés en unaire. Les notations $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$ désignent les ensembles usuels donnés dans une représentation binaire. La notation $\mathbb{D}$ désigne l'ensemble des nombres de la forme $k/2^n$ avec k et n entiers, représentés par les couples $(k,n) \in \mathbb{Z} \times \mathbb{N}_1$. Enfin $\mathbb{D}_n$ est la partie de l'ensemble précédent avec n fixé.

Dans cet article nous traitons d'algorithmes qui acceptent d'une part des entrées dans des ensembles dénombrables codés tels que $\mathbb{N}_1$, $\mathbb{N}$, $\mathbb{Z}$ et $\mathbb{Q}$, et d'autre part des entrées dans des ensembles de fonctions, comme l'ensemble des suites $(x_n)_{n\in \mathbb{N}_1}$ à indices dans $\mathbb{N}_1$ et à valeurs dans $\mathbb{D}$. Une telle entrée est traitée par l'algorithme comme un oracle. Lorsque l'algorithme pose la question «n-ème terme de la suite ?» l'oracle répond x_n. On peut aussi considérer l'oracle comme répondant à la question «terme suivant de la suite ?». La définition de la complexité de tels algorithmes pose quelques problèmes dans le cas général. Néanmoins, dans le cas où on n'utilise que des oracles donnant leur réponse parmi un ensemble fini de valeurs fixées a priori, la complexité en temps est définie en disant que la réponse de l'oracle consomme une unité de temps. Nous n'aurons pas besoin ici de plus de détails concernant la complexité des fonctionnelles récursives définies par nos algorithmes.

1.3) Deux présentations de l'ensemble des réels : à la Cauchy et par fractions continues

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 et notation 1.1 : Nous définirons $\mathbb{R}_{\mathsf{CONV}}$ comme la partie de $\mathbb{Q}^{\mathbb{N}_1}$ formée des suites $(x_n)_{n\in \mathbb{N}_1}$ de rationnels vérifiant la condition: $\left| x_n - x_{n+1} \right| \leq 1/2^{n+1}$

Une classe de complexité $\mathfrak{C}$ étant définie, nous noterons $\mathbb{R}_{\mathsf{CONV}}(\mathfrak{C})$ la partie de $\mathbb{R}_{\mathsf{CONV}}$ formée par les suites $(x_n)_{n\in \mathbb{N}_1}$ de complexité $\mathfrak{C}$.

à un réel x ainsi défini correspond une suite d'intervalles *emboités* $\left[x_n - 1/2^n, x_n + 1/2^n\right]$ contenant x.

Une présentation de $\mathbb{R}$ équivalente à $\mathbb{R}_{\mathsf{CONV}}$ peut être obtenue en demandant que chaque x_n soit un élément de $\mathbb{D}_n$. Par exemple un nombre réel x est codé sous forme d'une série :

$$(c_0 , (a_n)_{n\in \mathbb{N}_1}) \text{ code } x = c_0 + \sum_{i=0}^{\infty} \frac{a_i}{2^{i+1}}$$

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

L'avantage par rapport à la représentation $\mathbb{R}_{\mathsf{CONV}}$ est que *tout* élément de $\mathbb{Z} \times \{-1,0,1\}^{\mathbb{N}_1}$ représente un nombre réel x : aucune condition supplémentaire n'est imposée. Un autre avantage est que la représentation de $\mathbb{R}$ ainsi obtenue est localement compacte (avant même de

passer au quotient par la relation d'égalité). Cela correspond au fait que dans cette représentation, la taille de l'approximation de x à $1/2^n$ près est toujours raisonnable (ce qui n'est pas automatique avec la représentation $\mathbb{R}_{CONV}$). Ainsi cette représentation de $\mathbb{R}$ est très proche de toute implantation informatique raisonnable de la notion de nombre réel (cf. par exemple [KF]).

Définition et notation 1.2 :

Nous noterons $\mathbb{R}_{CONV2}$ cette deuxième représentation de $\mathbb{R}$. Ainsi $\mathbb{R}_{CONV2}$ n'est rien d'autre que $\mathbb{Z} \times \{-1,0,1\}^{\mathbb{N}_1}$ vu comme représentant $\mathbb{R}$ via le codage explicité. Une classe de complexité $\mathfrak{C}$ étant définie, nous noterons $\mathbb{R}_{CONV2}(\mathfrak{C})$ la partie de $\mathbb{R}_{CONV2}$ formée par les couples $(c_0 , (a_n)_{n\in \mathbb{N}_1})$ où la suite $(a_n)_{n\in \mathbb{N}_1}$ est de complexité $\mathfrak{C}$.

Le fait de tolérer “un chiffre en trop” par rapport à une écriture en base 2 “ordinaire” permet d'obtenir le résultat suivant (cf. Proposition 2.2 dans [LL])

Proposition 1.1 : Les 2 présentations $\mathbb{R}_{CONV}$ et $\mathbb{R}_{CONV2}$ de $\mathbb{R}$ sont équivalentes au sens suivant : il existe deux fonctionnelles à oracle :

$$\mathbb{R}_{CONV2} \to \mathbb{R}_{CONV} \quad \text{et} \quad \mathbb{R}_{CONV} \to \mathbb{R}_{CONV2}$$

qui représentent l'identité de $\mathbb{R}$ et avec les caractéristiques suivantes (en terme de complexité). La première est calculable en temps $O(n)$. La seconde interroge son oracle avec une précision $O(n)$ et termine son calcul en temps $O(r^2)$ où r est la taille de la réponse donnée par l'oracle.

Nous présentons maintenant la définition de l'ensemble $\mathbb{R}_{CONT}$ correspondant à la présentation d'un nombre réel par son développement en fraction continue.

Définition 1.3 : 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. Une classe de complexité $\mathfrak{C}$ étant définie, nous noterons $\mathbb{R}_{CONT}(\mathfrak{C})$ la partie de $\mathbb{R}_{CONT}$ formée par les couples $(e , (f_n))$ où la suite (f_n) est de complexité $\mathfrak{C}$.

Dans [LL], il est démontré qu'il n'existe aucune fonctionnelle récursive de $\mathbb{R}_{CONV}$ vers $\mathbb{R}_{CONT}$ qui représente l'identité de $\mathbb{R}$, et que l'addition de deux réels n'est pas représentable par une fonctionnelle récursive dans la représentation $\mathbb{R}_{CONT}$ (ceci invalide a priori tout algorithme qui prétend calculer à coup sûr la somme de deux réels dans la présentation $\mathbb{R}_{CONT}$).

2) Explicitation d'un nombre réel comme somme de deux développements en fraction continue au moyen d'une fonctionnelle en temps polynomial

Nous donnons dans cette section un traitement algorithmique et controlé en temps polynomial d'un théorème dû à M. Hall ([Hal] 1947) : tout nombre réel peut s'écrire comme somme de deux nombres irrationnels dont les développements en fraction continue ne contiennent que les entiers 1, 2, 3 ou 4 (sauf éventuellement le premier terme égal à la partie entière).

Théorème 2.1 : Il existe une fonctionnelle calculable en temps $O(n^2)$ et qui interroge son oracle $O(n)$ fois :

$$\mathcal{F} : \mathbb{R}_{CONV2} \to \mathbb{R}_{CONT} \times \mathbb{R}_{CONT}$$

Vérifiant : si $x \in \mathbb{R}_{CONV2}$ et $\mathcal{F}(x) = (y,z)$ alors $x =_{\mathbb{R}} y + z$.

En outre les développements en fraction continue y et z ne contiennent que les entiers 1, 2, 3 ou 4 (sauf éventuellement leur premier terme). En conséquence, si x est dans $\mathbb{R}_{CONV2}(O(n^k))$, alors y et z sont dans $\mathbb{R}_{CONT}(O(n^{sup(k,2)}))$.

Remarque : Les mêmes résultats valent en remplaçant $\mathbb{R}_{CONV2}$ par $\mathbb{R}_{CONV}$ (appliquer la proposition 1.1).

preuve> Un réel x est représenté par un élément

$$(c_0,(a_n)_{n\in \mathbb{N}_1}) \in \mathbb{Z} \times \{-1,0,1\}^{\mathbb{N}_1}$$

avec l'égalité :

$$x = c_0 + \sum_{i=0}^{\infty} \frac{a_i}{2^{i+1}}$$

On désire écrire x sous la forme $y + z$ où y et z sont deux irrationnels donnés par leurs dfc. La fonctionnelle que nous voulons construire prend une entrée m dans $\mathbb{N}_1$ (qui spécifie le nombre de termes que l'on veut pour chacun des dfc), et une entrée dans $\mathbb{Z}$ qui est l'entier c_0 pour l'écriture de x dans $\mathbb{R}_{CONV2}$.

Elle interroge l'oracle qui précise x , au moyen de la question « chiffre suivant ? » , et l'oracle délivre le nouveau chiffre $a_n \in \{-1,0,1\}$. La convention naturelle dans ce cadre est de dire que les n premières valeurs a_i , qui permettent de préciser x à $1/2^n$ près, sont obtenues en n unités de temps. La fonctionnelle doit délivrer les m premiers termes des deux dfc de x et y .

En outre la réponse doit être *cohérente* au sens suivant : pour le même nombre réel x avec la même valeur entrée pour c_0 et pour deux valeurs m et $m+k$ en entrée pour le nombre de termes souhaités, si l'oracle répond de la même manière lorsque les mêmes questions lui sont posées, les m premiers termes pour le dfc de y à $m+k$ termes livré par la fonctionnelle sont les mêmes que ceux livrés pour le dfc de y à m termes (et même chose pour z).

On ne peut par contre exiger que la réponse de la fonctionnelle soit la même pour deux descriptions différentes du même réel x par deux oracles. Autrement dit l'entrée x est bien un élément de $\mathbb{R}_{CONV2}$ et non un élément de $\mathbb{R}$.

Le fait que la fonctionnelle donne des réponses cohérentes résultera de la structure même de l'algorithme, qui produit les m chiffres demandés du dfc de y (et ceux de z) les uns après les autres et non de manière globale.

On supposera dans la suite sans perte de généralité que $x \in J = [0.415, 1.656]$ (il suffit en effet de demander x avec une précision de $1/16$ pour le situer sur un intervalle rationnel de longueur $1/8$ contenu à coup sûr dans un intervalle du type $a + J$ avec a dans $\mathbb{Z}$). La recherche des dfc $/ y_0, y_1, y_2, \ldots\ldots, y_n, \ldots /$ et $/ z_0, z_1, z_2, \ldots\ldots, z_n, \ldots /$ de y et z sera alors initialisée par $y_0 = 0$, $z_0 = 0$.

Nous donnons maintenant un algorithme qui situe à l'étape n°k y et z sur deux intervalles fermés Y_k et $\mathbb{Z}_k$, avec $x \in Y_k + Z_k$.

À l'initialisation (étape n°0) on a :

$Y_0 = Z_0 = [\,/\,0,4,1,4,1,4,\ldots\,/\,,\,/\,0,1,4,1,4,1,\ldots\,/\,] = [\,(\sqrt{2}-1)/2\,,\ 2(\sqrt{2}-1)\,]$
avec $x \in X_0 \subset [0.415,\ 1.656] \subset (Y_0 + Z_0) = [\,(\sqrt{2}-1)\,,\ 4(\sqrt{2}-1)\,]$
Lors de l'étape n°k+1 , un des deux intervalles Y_k et Z_k reste fixe et l'autre diminue.
Le fait de situer y sur Y_k permet de connaître exactement un certain nombre de termes de son dfc, tous compris entre 1 et 4 (à l'exception de $y_0 = 0$). La même chose est valable pour z .
À l'étape n°$k = 15 \times m$ on sera assuré de connaître au moins m termes du dfc de y et m termes du dfc de z . (la preuve est donnée plus loin)
Plus précisément, si $\sigma = [0, u_1, u_2, \ldots\ldots, u_n]$ avec les u_i entre 1 et 4 nous notons :

- F_σ l'intervalle fermé ayant pour extrémités / 0, u_1, u_2,……, u_n, 4,1,4,1,4,1,… / et / 0, u_1, u_2,……, u_n, 1,4,1,4,1,4,… / (intervalles de type 1 chez Hall)
  (le premier nombre est l'extrémité droite si n est pair, gauche sinon)
- G_σ l'intervalle fermé ayant pour extrémités / 0, u_1, u_2,……, u_n, 2,4,1,4,1,4,1,… / et / 0, u_1, u_2,……, u_n, 4,1,4,1,4,1,4,… / (intervalles de type 2 chez Hall)
- H_σ l'intervalle fermé ayant pour extrémités / 0, u_1, u_2,……, u_n, 3,4,1,4,1,4,1,… / et / 0, u_1, u_2,……, u_n, 4,1,4,1,4,1,4,… / (intervalles de type 3 chez Hall)

Tous les intervalles Y_k et Z_k sont de l'un des trois types ci dessus. Lorsque y (par exemple) est situé sur un intervalle F_σ on connaît les termes $[0, y_1, y_2, \ldots\ldots, y_n] = [0, u_1, u_2, \ldots\ldots, u_n]$ de son dfc. S'il est situé sur un intervalle G_σ on sait en outre que y_{n+1} est égal à 2 , 3 ou 4 , et s'il est situé sur un intervalle H_σ on sait en outre que y_{n+1} est égal à 3 ou 4 .

La remarque fondamentale qui permet de faire tourner l'algorithme est la suivante :

- supposons $U = [a,d]$, $V = [e,f]$, $a < b < c < d$, $U' = [a,b]$, $T = [b,c]$ et $U'' = [c,d]$
- si $t = (c - b) = l(T)$ c.-à-d. la longueur du "trou" T est strictement inférieure à $v = (f - e) = l(V)$ c.-à-d. la longueur de V , alors les intervalles $U'+V$ et $U''+V$ se chevauchent sur une longueur $(v - t)$ et leur réunion est égale à $U+V$
- ainsi, si on a un réel x à la Cauchy dans $U+V$, il suffit de le connaître avec une précision meilleure que $(v - t)/2$ pour le situer à coup sûr sur l'un au moins des deux intervalles $U'+V$ et $U''+V$

Dans une situation de ce type, avec $\{U,V\} = \{Y_k,Z_k\}$ et $x \in U+V$, l'algorithme garde V et remplace U par U' ou U'' en fonction de la valeur approchée de x révélée par l'oracle.
Chaque intervalle U (de type 1, 2 ou 3) contient un trou T conformément à la description suivante :

- $F_\sigma = F_{\sigma'} \cup T_{\sigma,1} \cup G_\sigma$ où $\sigma' = [0, u_1, u_2, \ldots\ldots, u_n, 1]$
  (le fait que $F_{\sigma'}$ est une partie droite ou gauche de l'intervalle F_σ dépend de la parité de n)

- $G_\sigma = F_{\sigma''} \cup T_{\sigma,2} \cup H_\sigma$ où $\sigma'' = [0, u_1, u_2, \ldots\ldots, u_n, 2]$
- $H_\sigma = F_{\sigma'''} \cup T_{\sigma,3} \cup F_{\sigma''''}$ où $\sigma''' = [0, u_1, u_2, \ldots\ldots, u_n, 3]$,
  $\sigma'''' = [0, u_1, u_2, \ldots\ldots, u_n, 4]$

Notez que dans chaque cas l'intervalle ouvert correspondant au trou contient uniquement des réels dont au moins un terme du dfc est ≥ 5 . Ainsi, enlever le trou ne supprime aucun dfc composé uniquement de termes égaux à 1 , 2 , 3 ou 4 . En fait dans l'algorithme, on remplace U par U' ou par U'' et donc on enlève plus que le trou, mais cela n'a pas d'importance dans la mesure où nous travaillons avec un réel bien précis en entrée.
Récapitulons.

Lorsque Y_k (ou Z_k) diminue et est remplacé par Y_{k+1} (ou Z_{k+1}) on a les remplacements suivants qui sont possibles

- un intervalle F_σ donne ou bien l'intervalle $F_{\sigma'}$ avec $\sigma' = [0, u_1, u_2, \ldots\ldots, u_n, 1]$ ou bien l'intervalle G_σ :
- un intervalle G_σ donne ou bien l'intervalle $F_{\sigma''}$ avec $\sigma'' = [0, u_1, u_2, \ldots\ldots, u_n, 2]$ ou bien l'intervalle H_σ :
- un intervalle H_σ donne ou bien l'intervalle $F_{\sigma'''}$ avec $\sigma''' = [0, u_1, u_2, \ldots\ldots, u_n, 3]$ ou bien l'intervalle $F_{\sigma''''}$ avec $\sigma'''' = [0, u_1, u_2, \ldots\ldots, u_n, 4]$:

La règle qui permet de savoir quel est celui des deux intervalles Y_k ou Z_k qui diminue à l'étape k+1 est la suivante : l'intervalle qui diminue est celui pour lequel le trou est le plus grand. M. Hall a établi (voir plus loin quelques précisions), que le trou d'un intervalle de type 1, 2 ou 3 est toujours strictement plus petit que les deux autres morceaux.
On voit alors de proche en proche que le trou de l'intervalle qui diminue est toujours strictement plus petit que l'intervalle qui reste fixe. Nous pouvons donc écrire :

étape n° k+1: ($l(B)$ dénote la longueur d'un intervalle B)
Calculer la longueur du trou de Y_k et celle du trou de Z_k. Soit U l'intervalle ayant le plus grand trou, et V l'autre. écrivons $U = U' \cup T \cup U''$. Demander à l'oracle le nombre de chiffres supplémentaires nécessaires pour situer x sur un intervalle $X_{k+1} \subset X_k$ de longueur $l(X_{k+1}) \le l(V) - l(T)$. L'intervalle X_{k+1} est certainement contenu dans $U'+V$ ou dans $U''+V$. On teste si le premier cas se produit. Si oui, on remplace U par U'. Sinon on remplace U par U''. Dans tous les cas on garde V.

Pour que la procédure soit bien controlée (en temps polynomial) il faut des estimations précises concernant les rapports entre les intervalles concernés. Mr. M. Hall ayant fait l'essentiel du travail, il ne reste plus qu'à donner le résultat des calculs et à faire quelques commentaires appropriés.
M. Hall a évalué précisément les rapports $l(T)/l(U')$ et $l(T)/l(U'')$ pour chacun des trois types d'intervalle.
Il trouve par exemple que

$$l(T_{\sigma,1})/l(F_{\sigma'}) = (4-3\xi)(\xi+\varepsilon)/(3\xi-3)(\xi+1+\varepsilon) \text{ avec}$$

$$\xi = /\,1,4,1,4,1,4,1,\ldots\,/ = (1+\sqrt{2})/2 \qquad \text{et} \qquad \varepsilon = q_{n-1}/q_n \text{ où}$$

$$/\,0, u_1, u_2, \ldots\ldots, u_n, \zeta\,/ = \frac{p_n\,\zeta + p_{n-1}}{q_n\,\zeta + q_{n-1}},$$

Comme $q_n = u_n\, q_{n-1} + q_{n-2}$, et puisque dans la situation présente les u_i sont compris entre 1 et 4, on a $1/5 < \varepsilon < 1$.
De là on déduit $0.356 < l(T_{\sigma,1})/l(F_{\sigma'}) < 0.420$.
On établit facilement à partir des calculs de Hall le tableau suivant :

on notera
mi = (min(l(U'),l(U''))/l(U) , ma = (max(l(U'),l(U''))/l(U)
type 1
0.356 < l(T)/l(U') < 0.420 , 2.384 < l(U')/l(T) < 2.807
0.297 < l(T)/l(U'') < 0.359 , 2.792 < l(U'')/l(T) < 3.360
0.139 < l(T)/l(U) < 0.162 , 6.176 < l(U)/l(T) < 7.167
0.388 < mi < ma < 0.545 , 1.834 < 1/ma < 1/mi < 2.573

```
type 2
 0.430 < l(T)/l(U') < 0.465   ,  2.152 < l(U')/l(T)  < 2.323
 0.355 < l(T)/l(U") < 0.388   ,  2.578 < l(U")/l(T)  < 2.813
 0.162 <  l(T)/l(U) < 0.175   ,  5.720 <  l(U)/l(T)  < 6.136
 0.350 <   mi < ma  < 0.493   ,  2.030 < 1/ma < 1/mi < 2.854
type 3
 0.471 < l(T)/l(U') < 0.493   ,  2.030 < l(U')/l(T)  < 2.123
 0.735 < l(T)/l(U") < 0.761   ,  1.314 < l(U")/l(T)  < 1.360
 0.223 <  l(T)/l(U) < 0.231   ,  4.344 <  l(U)/l(T)  < 4.483
 0.293 <   mi < ma  < 0.489   ,  2.046 < 1/ma < 1/mi < 3.412
```

On en déduit maintenant une majoration et une minoration du rapport des longueurs des trous de Y_k et de Z_k. Ce rapport de longueur oscille autour de 1. S'il est plus grand que 1 il va diminuer jusqu'à devenir inférieur à 1 puis réaugmenter tout de suite après. Le minimum de ce rapport est donc obtenu en disant : on passe d'un rapport ≥ 1 à un rapport < 1 en faisant un trou dans un intervalle et en gardant la partie qui doit rester, et on regarde la longueur du trou dans le nouvel intervalle. Le minimum qu'on puisse atteindre est donc minoré par :

$$\text{le minimum des } \texttt{mi} \times \frac{\text{mini des } \texttt{l(T)/l(U)}}{\text{maxi des } \texttt{l(T)/l(U)}} > 0.293 \times 0.139 / 0.231 > 0.176$$

On a donc : $0.176 <$ rapport des longueurs des trous < 5.672

Nous apprécions ensuite combien de fois au maximum on peut faire successivement des trous du même coté. Quand on fait un trou d'un coté, la longueur de l'intervalle est au moins divisée par le minimum des `1/ma`, donc au moins par 1.834. Par ailleurs le rapport du trou à l'intervalle est, sur celui de départ, au moins de 0.139 et sur celui d'arrivée au plus de 0.231. On doit donc regarder en combien d'étapes de division par 1.834 on passe de $5.672 \times 0.231 / 0.139$ (qui est majoré par 9.43) à moins que 1, le calcul donne :

$$(1.834)^4 > 11.31 > 9.43 > 6.169 > (1.834)^3$$

On obtient donc que la pire des choses qu'il puisse arriver est qu'il y ait systématiquement quatre fois plus de trous d'un coté (celui de y par exemple) que de l'autre. Au moins 1/5 du nombre total d'étapes est donc consacré à préciser y (la même chose vaut pour z). Par ailleurs on gagne un terme du dfc de y en au pire trois étapes du coté y. Donc, au pire toutes les 15 étapes on gagne au moins un terme du dfc de y (et au moins un terme du dfc de z). Ainsi le nombre d'étapes nécessaires k est majoré par $15 \times m$.(1)

Il nous reste maintenant à voir que pour k étapes de calcul, le temps consommé pour calculer Y_k et Z_k est en $O(k^2)$.

Une minoration de la longueur du plus petit intervalle qui puisse être produit en k étapes est donnée par $l(F_\sigma)$ avec $\sigma = [0, 4, 4, \ldots, 4]$ (avec k termes 4) qui est minoré par $1/5^k$.

Par ailleurs, cherchons une minoration du rapport de la longueur de V (l'intervalle qui ne bouge pas) à la longueur de T (le plus grand des trous). Ce rapport est minimum la première fois qu'on fait un trou du coté U. à l'étape précédente, le trou T' était de l'autre coté et de longueur $l(T') \geq l(T)$. Donc $l(V)/l(T) \geq l(V)/l(T')$ et ce dernier rapport est un rapport du type l(U')/l(T) ou l(U")/l(T) dans le tableau ci-dessus, donc il est minoré par 1.314.

---

1 Une analyse plus détaillée permettrait sans doute d'améliorer un peu ce résultat, mais ce n'est pas nécessaire à notre propos.

Ainsi le rapport de la longueur de V (l'intervalle qui ne bouge pas) à la longueur de T (le plus grand des trous) est minoré par 1.314 . Cela signifie que la longueur de chevauchement de U'+V avec U"+V est au moins $0.314 \times l(V)$. En conséquence il ne faudra jamais interroger x avec une précision meilleure que $0.15/5^k$. Ainsi l'oracle n'est pas interrogé plus de $3k+4$ fois. Les calculs à faire sont essentiellement ceux des coefficients des fonctions homographiques

$$\zeta \mapsto / 0, y_1, y_2, \ldots\ldots, y_{s(k)}, \zeta / \quad \text{et} \quad \zeta \mapsto / 0, z_1, z_2, \ldots\ldots, z_{s'(k)}, \zeta /$$

à partir desquels sont calculés les intervalles Y_k et Z_k ainsi que les trous de ces intervalles. Tout ce calcul est donc facilement en $O(k^2)$. ❑

Le corollaire suivant du théorème 2.1 améliore un théorème donné dans [LL]. En outre, la méthode donnée ici est plus simple.

Corollaire 2.2 : Pour toute fonction récursive croissante T , il existe deux nombres réels y , z dans $\mathbb{R}_{\mathsf{CONT}}(O(n^2))$ mais dont la somme n'est pas dans $\mathbb{R}_{\mathsf{CONT}}(\mathbf{DTIME}(T(n)))$

La preuve du corollaire utilise le théorème suivant démontré dans [LL] (théorème 2.1).

Théorème 2.3 : Pour toute fonction récursive croissante $T(n)$ il existe un nombre réel x qui est dans $\mathbb{R}_{\mathsf{CONV}}(\mathbf{LINTIME})$ mais pas dans $\mathbb{R}_{\mathsf{CUT}}(\mathbf{DTIME}(T(n)))$, et a fortiori n'est pas dans $\mathbb{R}_{\mathsf{CONT}}(\mathbf{DTIME}(T(n)))$.

preuve du corollaire 2.2 > Par le théorème 2.3 on produit un x qui est dans $\mathbb{R}_{\mathsf{CONV}}(O(n))$ mais pas dans $\mathbb{R}_{\mathsf{CONT}}(\mathbf{DTIME}(T(n)))$. Par le théorème 2.1 on produit à partir de x des éléments y et z dans $\mathbb{R}_{\mathsf{CONT}}(O(n^2))$ et dont la somme est égale à x . ❑

Remarque : Toutes les majorations du type $O(n^2)$ dans cet article sont sans doute remplaçables par des majorations du type «Quasilineartime» c.-à-d. $\cup_k O(n.\log(n)^k)$, en utilisant les techniques de multiplication rapide d'entiers.

3) Le caractère non constructif du théorème de Cantor

Nous considérons la version affaiblie suivante du théorème de Cantor

(CaT) étant données deux suites de réels (a_n) et (b_n) avec :

$$\forall\, n \quad (a_n \le a_{n+1} \ , \ \ a_n \le b_n \ \text{ et } \ b_{n+1} \le b_n \ )$$

il existe un réel x avec $a_n \le x \le b_n$ pour tout n

En mathématiques constructives (cf. [BR]) ce théorème peut être «infirmé» de la façon suivante. On fournit un «contre-exemple brouwerien» en considérant une suite fugitive (u_n) (c.-à-d. une suite infinie prenant uniquement les valeurs 0 et 1 mais au plus une fois la valeur 1). à partir de cette suite fugitive, on fabrique la suite

$$a_n = \Sigma_{i=0,\ldots,n}\, u_{2i} \ ,$$

qui est une suite croissante (au sens large) prenant ses valeurs dans $\{0,1\}$ et la suite

$$b_n = (1 - \Sigma_{i=0,\ldots,n}\, u_{2i+1})$$

qui est une suite décroissante (au sens large) prenant ses valeurs dans $\{0,1\}$. En outre on a pour tout n : $a_n \le b_n$. Si la valeur 1 est prise par u_m alors les intervalles $[a_{m+k} , b_{m+k}]$ sont réduits au singleton $\{1\}$ ou $\{0\}$ selon que m est pair ou impair.

Le fait de savoir déterminer, pour ces deux suites (a_n) et (b_n) un réel x conforme au théorème de Cantor avec une précision meilleure que $1/4$ implique donc qu'on sait déterminer, pour toute suite fugitive (u_n), si l'unique valeur éventuelle de m pour laquelle $u_m = 1$ est avec m pair ou avec m impair. Ce principe non constructif est appelé **LLPO** ce qu'on peut traduire en français par *mini principe d'omniscience*([2]).
Ainsi on a le théorème constructif

Théorème 3.1 : **CaT** $\Rightarrow$ **LLPO**

ce qui invalide **CaT** .
à partir de ce style de réfutation, on peut toujours donner deux versions récursives du caractère non constructif du théorème concerné (ici **CaT**).
La première version est en termes de fonctionnelle.

Proposition 3.2 : Il n'existe pas de fonctionnelle récursive qui, à partir de deux suites de réels (a_n) et (b_n) vérifiant les hypothèses de **CaT** et introduites par des oracles, donne en sortie un réel x vérifiant la conclusion de **CaT** .

preuve> Le premier oracle en entrée donne, pour la question (n,k), un rationnel approchant a_n à $1/2^k$. Le deuxième oracle fait le même travail pour la suite (b_n). Sur l'entrée m la fonctionnelle devrait calculer un rationnel x_m avec la condition de cohérence :

$$\left| x_m - x_{m+1} \right| \leq 1/2^{m+1}$$

Faisons calculer à la fonctionnelle le résultat lorsque le premier oracle répond toujours 0 et le second toujours 1, avec l'entrée $m = 2$. Supposons que les oracles ne soient interrogés que jusqu'à $n = N$. La réponse donnée par la fonctionnelle exclut nécessairement une des deux solutions $x = 0$ ou $x = 1$. Supposons sans perte de généralité que $x = 0$ soit exclu. Il suffit de modifier le deuxième oracle pour $n \geq N+1$ et de lui faire sortir maintenant la réponse 0 pour voir que la fonctionnelle s'est trompée. ❑

La deuxième version est en termes de suites récursives.

Proposition 3.3 : Il existe deux suites récursives doubles de réels $(a_{n,h})$ et $(b_{n,h})$ vérifiant, pour h fixé, les hypothèses de **CaT** , et telles qu'il n'existe aucune suite récursive de réels (x_h) où x_h vérifie, pour chaque h, la conclusion de **CaT** .

preuve> On utilise deux parties A et B de $\mathbb{N}$ récurivement énumérables disjointes mais récursivement inséparables, pour recopier le contre-exemple brouwerien donné dans la preuve du théorème 3.1 . Soit M_A (resp. M_B) une machine de Turing qui reconnait A (resp. B). On pose

- $u_{2n,h} = 1$ si M_A certifie que $h \in A$ en exactement n étapes de calcul,
  $u_{2n,h} = 0$ sinon
- $u_{2n+1,h} = 0$ si M_B certifie que $h \in B$ en exactement n étapes de calcul,
  $u_{2n+1,h} = 1$ sinon

Pour h fixé, la suite $n \mapsto u_{n,h}$ est fugitive, elle est toujours nulle si $h \notin A \cup B$, elle prend la valeur 1 pour un indice pair si $h \in A$ et elle prend la valeur 1 pour un indice impair si

---

[2] Il est équivalent au principe suivant (cf. [BR]) : $\forall\ x \in \mathbb{R}\ \ (x \geq 0 \ \text{ou}\ x \leq 0)$ (avec pour $\mathbb{R}$ l'ensemble des réels à la Cauchy)

$h \in B$. On fabrique les suites $n \mapsto a_{n,h}$ et $n \mapsto b_{n,h}$ à partir de la suite $n \mapsto u_{n,h}$ comme dans le contre-exemple brouwerien. La fin est laissée au lecteur ou à la lectrice. ❑

La méthode des contre-exemples brouweriens donne donc, dans un langage intuitif, l'essence des contre-exemples donnés en mathématiques récursives, un peu de la même manière que les preuves en analyse non-standard donnent l'essence des preuves correspondantes en analyse classique.

Henri LOMBARDI
Laboratoire de Mathématiques
URA CNRS 741
Université de Franche-Comté
25030 BESANCON Cédex
FRANCE
email : hl@grenet.fr

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

Bibliographie

[BR] Bridges D., Richman F. : *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press (1987).

[CF] Cusik T., Flahive M. : *The Markhoff and Lagrange spectra.* Maths Suveys and Monographs vol 30. Édité par l'AMS. (1989). Voir p 47-51

[Hal] Hall M. *On the sum and the product of two continuous fractions* . Annals of Math. 48 (2), p 966-993. (1947).

[KF82] Ker-I. KO, Harvey Friedman : *Computational complexity of real functions* Theoretical Computer Science 20, p 323-352 (1982).

[Khi] A. Ya Khintchine. *Continued fractions* . P. Noordhoff Ltd. Netherlands (1963).

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

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

[Sha] Shallit. J. : *Real numbers with bounded partial quotients : a survey*. L'Enseignement Mathématique. 38. p 151-187 (1992).