Espaces métriques rationnellement présentés et complexité, le cas de l'espace des fonctions réelles uniformément continues sur un intervalle compact

S. Labhalla
Dépt. de Mathématiques
Univ. de Marrakech, Maroc
labhalla@ucam.ac.ma

H. Lombardi
Dépt. de Mathématiques
Univ. de Franche-Comté, France
Henri.Lombardi@univ-fcomte.fr

E. Moutai
Dépt. de Mathématiques
Univ. de Marrakech, Maroc

1er Mars 1999

Résumé : Nous définissons la notion de *présentation rationnelle d'un espace métrique complet* comme moyen d'étude des espaces métriques et des fonctions continues du point de vue de la complexité algorithmique. Nous étudions dans ce cadre différentes manières de présenter l'espace $\mathbf{C}[0,1]$ des fonctions réelles uniformément continues sur l'intervalle $[0,1]$, muni de la norme usuelle : $\| f \|_\infty = \mathbf{Sup}\{| f(x) |;\ 0 \leq x \leq 1\}$. Ceci nous permet de faire une comparaison de nature globale entre les notions de complexité attachées à ces présentations. En particulier, nous obtenons une généralisation des résultats de Hoover concernant le *théorème d'approximation de Weierstrass en temps polynomial*. Nous obtenons également une généralisation des résultats de Ker-I Ko, H. Friedman et N. Müller concernant les fonctions analytiques calculables en temps polynomial.

Mots clés : Espaces métriques, Fonctions réelles, Machine de Turing, Circuit booléen, Circuit semilinéaire binaire, Circuit arithmétique, Complexité algorithmique, Théorème d'approximation de Weierstrass, Classe de Gevrey, Séries de Chebyshev.

Abstract : We define the notion of *rational presentation of a complete metric space*, in order to study metric spaces from the algorithmic complexity point of view. In this setting, we study some representations of the space $\mathbf{C}[0,1]$ of uniformly continuous real functions over [0,1] with the usual norm : $\| f \|_\infty = \mathbf{Sup}\{| f(x) |;\ 0 \leq x \leq 1\}$. This allows us to have a comparison of global kind between complexity notions attached to these presentations. In particular, we get a generalization of Hoover's results concerning the *Weierstrass approximation theorem in polynomial time*. We get also a generalization of previous results on analytic functions which are computable in polynomial time.

Key words : Metric spaces, Real functions, Turing Machine, Boolean circuit, Binary semi-linear circuit, Arithmetic circuit, Algorithmic complexity, Weierstrass approximation theorem,

Gevrey class, Chebyshev series.

Introduction

Notons $\mathbf{C}[0,1]$ l'espace des fonctions réelles uniformément continues sur l'intervalle $[0,1]$. Dans [15], Ker-I. Ko et Friedman ont introduit et étudié la notion de complexité des fonctions réelles, définie via une machine de Turing à oracle.
Dans l'article [13], Hoover a étudié les présentations de l'espace $\mathbf{C}[0,1]$ via les circuits booléens et circuits arithmétiques.
Dans ces deux articles la complexité dans l'espace $\mathbf{C}[0,1]$ est étudiée "point par point".
Autrement dit, sont définies des phrases comme :

- f est un $\mathcal{P}$-point au sens de Ker-I. Ko et Friedman
- f est un $\mathcal{P}$-point au sens des circuits booléens.
- f est un $\mathcal{P}$-point au sens des circuits arithmétiques.

Ko et Friedman ont étudié les propriétés des $\mathcal{P}$-points (au sens de Ker-I. Ko et Friedman). Hoover a montré que les $\mathcal{P}$-points au sens des circuits arithmétiques sont les mêmes que les $\mathcal{P}$-points au sens de Ker-I. Ko et Friedman.

Dans cet article, nous étudions différentes présentations de l'ensemble $\mathbf{C}[0,1]$ en nous basant sur la notion de *présentation rationnelle d'un espace métrique complet*. Ceci nous permet de faire une comparaison de nature globale entre les notions de complexité attachées à différentes présentations.

Après quelques préliminaires dans la section 1, la section 2 contient essentiellement une exposition de ce qui nous semble être une problématique naturelle concernant les questions de complexité relatives aux espaces métriques complets séparables.

Usuellement un espace métrique contient des objets de nature infinie (le paradigme étant un nombre réel défini à la Cauchy), ce qui exclut une présentation informatique directe (c.-à-d. codée sur un alphabet fini) de ces objets.
Pour contourner cette difficulté, on procède comme il est usuel pour l'espace $\mathbb{R}$. On considère une partie dense Y de l'espace métrique considéré X, qui soit suffisamment simple pour que

- ses éléments puissent être codés comme (certains) mots sur un alphabet fini fixé.
- la fonction distance restreinte à Y soit calculable, c.-à-d. donnée par une fonction calculable :

$$\delta : Y \times Y \times \mathbb{N}_1 \to \mathbb{Q} \qquad \text{avec} \qquad \mid d_X(x,y) - \delta(x,y,n) \mid \leq 1/2^n$$

L'espace X apparaît alors comme le séparé-complété de Y.
On dira que le codage proposé pour Y et la description proposée pour la fonction distance constituent une *présentation rationnelle* de l'espace métrique X.
Il est à noter qu'on n'envisage pas de traiter des espaces métriques non complets, pour lesquels les difficultés de codage semblent insurmontables, et pour lesquels on ne peut pratiquement rien démontrer de sérieux en analyse constructive.
Pareillement les espaces métriques traités sont "à base dénombrable" (on dit aussi "séparables").

Les espaces métriques étudiés en analyse constructive (cf. [5]) sont très souvent définis via une présentation rationnelle de ce type, ou au moins faciles à définir selon ce schéma. Le problème qui se pose est en général de définir constructivement une partie dénombrable dense de l'espace considéré. C'est évidemment impossible pour des espaces de Banach classiques non

séparables du style L^∞, mais justement, ces espaces ne sont pas traitables sous leur forme classique par les méthodes constructives. Le problème est plus délicat pour des espaces qui sont classiquement séparables mais pour lesquels il n'y a pas de procédé naturel constructif qui donne une partie dénombrable dense. Par exemple c'est le cas pour un sous-espace fermé arbitraire d'un espace complet séparable, et c'est encore le cas pour certains espaces de fonctions continues.

La présentation en unaire et la présentation en binaire de $\mathbb{Z}$ ne sont pas équivalentes du point de vue la complexité en temps polynomial. La présentation en unaire est une présentation naturelle de $\mathbb{Z}$ comme groupe tandis que la présentation en binaire est une présentation naturelle de $\mathbb{Z}$ comme anneau. On peut se poser des questions analogues concernant les espaces métriques classiques usuels.

La première question qui se pose est la comparaison des différentes présentations d'un espace métrique usuel. Notez que la présentation usuelle de $\mathbb{R}$ est considérée comme la seule naturelle et que c'est à partir de cette présentation de $\mathbb{R}$ qu'est définie la complexité d'une présentation (Y_1, δ_1) de X ou la complexité de l'application Id_X de (Y_1, δ_1) vers (Y_2, δ_2) lorsqu'on compare deux présentations distinctes de X.

La question qui se pose ensuite est celle de la complexité des fonctions continues calculables entre espaces métriques. S'il y a une notion naturelle de complexité des fonctions dans le cas des espaces compacts, la question est nettement plus délicate dans le cas général, car elle renvoie à la complexité des fonctionnelles de type 2 arbitraires.

Une autre question est celle de la complexité d'objets liés de manière naturelle à l'espace métrique qu'on étudie. Par exemple dans le cas des réels, et en ne considérant que la structure algébrique de $\mathbb{R}$ on est intéressé par le fait que la complexité de l'addition, celle de la multiplication, ou celle de la recherche des racines complexes d'un polynôme à coefficients réels soient toutes "de bas niveau". Ce genre de résultats légitime a posteriori le choix qui est fait usuellement pour présenter $\mathbb{R}$, et les résultats de nature inverse disqualifient d'autres présentations (cf. [20]), moins efficaces que la présentation via les suites de Cauchy de rationnels écrits en binaire[1]. De même, un espace métrique usuel est en général muni d'une structure plus riche que la seule structure métrique, et il s'agit alors d'étudier, pour chaque présentation, la complexité de ces "éléments naturels de structure".

Dans la section 3, nous introduisons l'espace $\mathbf{C}[0,1]$ des fonctions réelles uniformément continues sur l'intervalle $[0,1]$ du point de vue de ses présentations rationnelles.
La fonction d'évaluation $(f,x) \mapsto f(x)$ n'est pas localement uniformément continue. Vue son importance, nous discutons ce que signifie la complexité de cette fonction lorsqu'on a choisi une présentation rationnelle de l'espace $\mathbf{C}[0,1]$.
Nous donnons ensuite deux exemples significatifs de telles présentations rationnelles :

- Une présentation par circuits semilinéaires binaires notée $\mathcal{C}_{\mathrm{csl}}$, où les points rationnels sont exactement les fonctions semilinéaires binaires. Une telle fonction peut être définie par un circuit semilinéaire binaire (cf. définition 3.2.1) et codée par un programme d'évaluation correspondant au circuit.
- une présentation, notée $\mathcal{C}_{\mathrm{frac}}$, via des fractions rationnelles convenablement contrôlées et données en présentation par formule (cf. définition 3.2.5).

Enfin nous établissons des résultats de complexité liés au théorème d'approximation de Newman. En bref, le théorème de Newman a une complexité polynomiale et en conséquence les

[1] Néanmoins, le test de signe est indécidable pour les réels présentés à la Cauchy. On se contente d'avoir en temps polynomial le test constructif : $x + y \geq 1/2^n \Rightarrow (x \geq 1/2^{n+2}$ ou $y \geq 1/2^{n+2})$.

fonctions linéaires par morceaux sont, chacune individuellement, des points de complexité $\mathcal{P}$ dans l'espace $\mathcal{C}_{\text{frac}}$.

Dans la section 4 nous définissons et étudions des présentations rationnelles "naturelles" de $\mathbf{C}[0,1]$, équivalentes du point de vue de la complexité en temps polynomial :

- La présentation dite "à la Ko-Friedman", et notée $\mathcal{C}_{\text{KF}}$, pour laquelle un point rationnel est donné par un quadruplet (Pr, n, m, T) où Pr est un programme de machine de Turing. Les entiers n, m, T sont des paramètres de contrôle. Nous faisons le lien avec la notion de complexité introduite par Ko et Friedman. Nous montrons une propriété universelle qui caractérise cette présentation rationnelle du point de vue de la complexité en temps polynomial.
- La présentation par circuits booléens qu'on note par $\mathcal{C}_{\text{cb}}$ et pour laquelle un point rationnel est donné par un quadruplet (C, n, m, k) où C code un circuit booléen et n, m, k sont des paramètres de contrôle.
- La présentation par circuits arithmétiques fractionnaires (avec magnitude) notée $\mathcal{C}_{\text{caf}}$. Un point rationnel de cette présentation est donné par un couple (C, M) où C est le code d'un circuit arithmétique, et M est un paramètre de contrôle.
- La présentation par circuits arithmétiques polynomiaux (avec magnitude) notée $\mathcal{C}_{\text{cap}}$ analogue à la précédente, mais ici le circuit est polynomial (c.- à-d. ne contient pas les portes "passage à l'inverse").

Nous montrons dans la section 4.2 que les présentations $\mathcal{C}_{\text{KF}}$, $\mathcal{C}_{\text{cb}}$, $\mathcal{C}_{\text{csl}}$, $\mathcal{C}_{\text{caf}}$ et $\mathcal{C}_{\text{cap}}$ sont équivalentes en temps polynomial. Ce résultat généralise et précise les résultats de Hoover. Non seulement les $\mathcal{P}$-points de $\mathcal{C}_{\text{KF}}$ sont "les mêmes" que les $\mathcal{P}$-points de $\mathcal{C}_{\text{cap}}$, mais bien mieux, les bijections

$$\mathcal{C}_{\text{KF}} \to \mathcal{C}_{\text{cap}} \quad \text{et} \quad \mathcal{C}_{\text{cap}} \to \mathcal{C}_{\text{KF}}$$

qui représentent l'identité de $\mathbf{C}[0,1]$ sont, globalement, calculables en temps polynomial. Ainsi nous obtenons une formulation complètement contrôlée du point de vue algorithmique pour le théorème d'approximation de Weierstrass.

Dans la section 4.3 , nous montrons que ces présentations ne sont pas de classe $\mathcal{P}$ en établissant la non faisabilité du calcul de la norme (si $\mathcal{P} \neq \mathcal{NP}$). Plus précisément, nous définissons convenablement "le problème de la norme" et nous démontrons qu'il s'agit d'un problème $\mathcal{NP}$-complet pour les présentations considérées.
Pour ce qui concerne le test d'appartenance à l'ensemble des (codes des) points rationnels, c'est un problème co-$\mathcal{NP}$-complet pour les présentations $\mathcal{C}_{\text{KF}}$ et $\mathcal{C}_{\text{cb}}$, tandis qu'il est en temps linéaire pour la présentation $\mathcal{C}_{\text{csl}}$. Cette dernière est donc légèrement plus satisfaisante.

Nous définissons dans la section 5 d'autres présentations de l'espace $\mathbf{C}[0,1]$ à savoir :

- La présentation notée $\mathcal{C}_{\text{W}}$ (comme Weierstrass) pour laquelle l'ensemble des points rationnels est l'ensemble des polynômes (à une variable) à coefficients rationnels donnés en présentation dense.
- La présentation notée $\mathcal{C}_{\text{sp}}$ pour laquelle l'ensemble des points rationnels est l'ensemble des fonctions polynomiales par morceaux, chaque polynôme étant donné comme pour $\mathcal{C}_{\text{W}}$.
- La présentation notée $\mathcal{C}_{\text{sfrac}}$ est obtenue à partir de $\mathcal{C}_{\text{frac}}$ de la même manière que $\mathcal{C}_{\text{sp}}$ est obtenue à partir de $\mathcal{C}_{\text{W}}$.

Nous essayons de voir jusqu'à quel point le caractère de classe $\mathcal{P}$ de ces présentations fournit un cadre de travail adéquat pour l'analyse numérique.
Nous caractérisons les $\mathcal{P}$-points de $\mathcal{C}_{\mathrm{W}}$ en établissant l'équivalence entre les propriétés suivantes : (cf. théorème 5.2.7) :

a) f est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{W}}$

b) la suite $A_n(f)$ (qui donne le développement de f en série de Chebyshev) est une $\mathcal{P}$-suite dans $\mathbb{R}$ et vérifie une majoration :

$$| A_n(f) | \leq Mr^{n^\gamma} \text{ avec } M > 0,\ \gamma > 0,\ 0 < r < 1.$$

c) f est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{KF}}$ et est dans la classe de Gevrey

Nous en déduisons une équivalence analogue entre (cf. theorem 5.2.8) :

a) f est une fonction analytique et est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{W}}$.

b) f est une fonction analytique et est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{KF}}$.

Un assez bon comportement de la dérivation vis à vis de la complexité est obtenu en montrant que pour tout $\mathcal{P}$-point (ou toute $\mathcal{P}$-suite) de $\mathcal{C}_{\mathrm{W}}$ la suite (ou la suite double) de ses dérivées est une $\mathcal{P}$-suite de $\mathcal{C}_{\mathrm{W}}$. Les calculs usuels sur les $\mathcal{P}$-points de $\mathcal{C}_{\mathrm{W}}$ (calcul de la norme, du maximum et de l'intégrale d'un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{W}}$ ou de ses dérivées) sont en temps polynomial (cf. proposition 5.2.6, théorème 5.2.10 et corollaire 5.2.11). Dans le théorème 5.2.13 et son corollaire 5.2.14, nous donnons une version plus uniforme des résultats précédents.
Tout ceci améliore sensiblement les résultats de [27] et [16]. En outre nos preuves sont plus conceptuelles.
Par ailleurs, ces résultats, combinés avec le théorème de Newman (dans sa version précisée à la section 3.3), montrent que le passage de la présentation par fraction rationnelles $\mathcal{C}_{\mathrm{frac}}$ à la présentation par polynômes (denses) $\mathcal{C}_{\mathrm{W}}$ n'est pas en temps polynomial. Le théorème de Newman montre également que les présentations $\mathcal{C}_{\mathrm{frac}}$ et $\mathcal{C}_{\mathrm{sfrac}}$ sont polynomialement équivalentes.

En résumant les résultats des sections 4 et 5, nous obtenons que l'identité de $\mathbf{C}[0,1]$ est uniformément de classe $\mathcal{P}$ dans les cas suivants :

$$\mathcal{C}_{\mathrm{W}} \to \mathcal{C}_{\mathrm{sp}} \to \mathcal{C}_{\mathrm{frac}} \equiv \mathcal{C}_{\mathrm{sfrac}} \to \mathcal{C}_{\mathrm{KF}} \equiv \mathcal{C}_{\mathrm{cb}} \equiv \mathcal{C}_{\mathrm{csl}} \equiv \mathcal{C}_{\mathrm{caf}} \equiv \mathcal{C}_{\mathrm{cap}}.$$

et aucune des flèches dans la ligne ci-dessus n'est une $\mathcal{P}$-équivalence sauf peut être $\mathcal{C}_{\mathrm{sp}} \to \mathcal{C}_{\mathrm{frac}}$ et très éventuellement $\mathcal{C}_{\mathrm{frac}} \to \mathcal{C}_{\mathrm{KF}}$ (mais cela impliquerait $\mathcal{P} = \mathcal{NP}$).

Nous terminons cette introduction par quelques remarques sur le constructivisme.
Le travail présenté ici est écrit dans le style des mathématiques constructives à la Bishop telles qu'elles ont été développées notamment dans les livres de Bishop [4], Bishop & Bridges [5], Mines, Richman & Ruitenburg [24]. Il s'agit d'un corps de mathématiques constructives en quelque sorte minimal. Tous les théorèmes démontrés de cette manière sont en effet également valables pour les mathématiciens classiques, le bénéfice étant qu'ici les théorèmes et les preuves ont toujours un contenu algorithmique. Le lecteur classique peut donc lire ce travail comme un prolongement des travaux en analyse récursive par Turing puis plus tard notamment par Goodstein [11], Ker-I. Ko & H. Friedman ([15], [18]), N. Th. Müller, Pour El & Richards [31], qui se situent eux dans un cadre de mathématiques classiques.
Par ailleurs les théorèmes et leurs preuves dans le style de Bishop sont également acceptables dans le cadre des autres variantes du constructivisme, comme l'intuitionnisme de Brouwer ou l'école constructive russe de A.A. Markov, G.S Cejtin, N.A Shanin, B.A. Kushner et leurs élèves.

On trouvera une discussion éclairante sur ces différentes variantes de constructivisme dans le livre de Bridges & Richman [9]. Le livre très complet de Beeson [3] donne également des discussions approfondies de ces points de vue et de leurs variantes, notamment en s'appuyant sur une étude remarquable des travaux des logiciens qui ont tenté de formaliser les mathématiques constructives. Les mathématiques constructives russes peuvent être découvertes à travers les livres de Kushner [19] et O. Aberth [1]. Un article historique très pertinent sur la question est écrit par M. Margenstern [23]. Le chapitre IV de [3] est également très instructif. Beeson déclare page 58 : "nous espérons montrer que [cet] univers [mathématique] est un endroit extrêmement divertissant, plein de surprises (comme n'importe quel pays étranger), mais en aucun cas trop chaotique ni invivable". Les mathématiques constructives russes restreignent leurs objets d'étude aux "êtres récursifs" et se rapprochent en cela de certains travaux d'analyse récursive classique développés notamment par Grzegorczyk, Kreisel, Lacombe, Schoenfield et Specker, avec lesquels elles partagent de nombreux résultats. Un des principes des mathématiques constructives russes est par exemple que seuls existent les réels récursifs donnés par des algorithmes (qui calculent des suites de rationnels à vitesse de convergence controlée). Et une fonction réelle définie sur les réels est un algorithme F qui prend en entrée un algorithme x et donne en sortie, sous la condition que x est un algorithme produisant un réel récursif, un algorithme y produisant un réel récursif. Ceci conduit par exemple au théorème de Cejtin, faux classiquement, selon lequel toute fonction réelle définie sur les réels est continue en tout point. L'analyse récursive classique énonce quant à elle : si un algorithme termine chaque fois que l'entrée est le code d'un réel récursif et donne alors en sortie le code d'un réel récursif, et s'il définit une fonction (c.-à-d. deux codes du même réel récursif en entrée conduisent à deux codes d'un même réel récursif en sortie) alors il définit une fonction continue en tout point réel récursif (théorème de Kreisel- Lacombe-Schoenfield). Beeson a analysé la preuve de Kreisel-Lacombe- Schoenfield pour en préciser les aspects non constructifs. La preuve de Cejtin, qui est plus constructive que celle de Kreisel-Lacombe-Schoenfield, est analysée dans [9].
Dans le style de Bishop, comme on considère que la notion d'effectivité est une notion primitive qui ne se réduit pas nécessairement à la récursivité, et que la récursivité, au contraire, ne peut être définie sans cette notion primitive d'effectivité, les nombres réels et les fonctions réelles sont des objets qui conservent une plus grande part de "liberté" et sont donc plus proches des réels et des fonctions réelles telles que les conçoivent intuitivement les mathématiciens classiques. Et le théorème "russe" précédent est donc indémontrable dans le style Bishop. De manière symétrique, les théorèmes de mathématiques classiques qui contredisent directement des résultats du constructivisme russe (comme par exemple la possibilité de définir sans aucune ambigüité des fonctions réelles discontinues) ne peuvent être démontrés dans les mathématiques du style Bishop.
En conclusion, les mathématiques constructives russes présentent un intérêt historique indéniable, développent une philosophie mathématique très cohérente et peuvent sans doute trouver un renouveau à partir de préoccupations d'informatique théorique. Il serait donc également intéressant de faire une étude de ces mathématiques du point de vue de la complexité algorithmique.

1 Préliminaires

1.1 Notations

$\mathbb{N}_1$ ensemble des entiers naturels en unaire

$\mathbb{N}$ 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.

$\mathbb{D}$ ensemble des nombres de la forme $k/2^n$ avec $(k,n) \in \mathbb{Z} \times \mathbb{N}_1$

$\mathbb{D}_{[0,1]}$ $\mathbb{D} \cap [0,1]$

$\mathbb{D}_n$ ensemble des nombres de la forme $k/2^n$ avec $k \in \mathbb{Z}$

$\mathbb{D}_{n,[0,1]}$ $\mathbb{D}_n \cap [0,1]$

$\mathbb{D}[X]$ ensemble des polynômes à coefficients dans $\mathbb{D}$ donnés en présentation dense

$\mathbb{D}[X]_f$ ensemble des polynômes à coefficients dans $\mathbb{D}$ donnés en présentation par formule

$\mathbb{R}$ ensemble des nombres réels présentés par les suites de Cauchy dans $\mathbb{Q}$.

MTO machine de Turing à oracle.

μ module de continuité uniforme (cf. section 2.2 définition 2.2.1)

$\lg(a)$ la longueur du codage binaire du dyadique $|a|$ (pour $a \in \mathbb{D}$).

$\mathrm{t}(C)$ taille du circuit C (le nombre de ses portes).

$\mathrm{prof}(C)$ profondeur du circuit C.

$\mathrm{mag}(C)$ magnitude du circuit arithmétique C (cf. définition 4.1.10)

$\widetilde{f}$ fonction continue codée par f.

$\mathcal{M}(n)$ complexité du calcul de la multiplication de deux entiers en représentation binaire (en multiplication rapide $\mathcal{M}(n) = \mathrm{O}(nlog(n)loglog(n))$.

$\perp d \perp$ la longueur (du codage discret) de l'objet d (le codage de d est un mot sur un alphabet fini fixé).

Présentations de l'espace $\mathbf{C}[0,1]$

$\mathcal{C}_{\mathrm{KF}}$ présentation par Machine de Turing, à la Ko-Friedman

$\mathcal{C}_{\mathrm{caf}}$ présentation par circuits arithmétiques (cf. définition 4.1.10)

$\mathcal{C}_{\mathrm{cap}}$ présentation par circuits arithmétiques polynomiaux

$\mathcal{C}_{\mathrm{cb}}$ présentation par circuits booléens (cf. définition 4.1.8)

$\mathcal{C}_{\mathrm{csl}}$ présentation par circuits semilinéaires binaires (cf. définition 3.2.1)

$\mathcal{C}_{\mathrm{frac}}$ présentation par fractions rationnelles dans un codage par formules (cf. définition 3.2.5)

$\mathcal{C}_{\mathrm{W}}$ présentation "à la Weierstrass" par polynômes dans un codage dense

$\mathcal{C}_{\mathrm{sp}}$ présentation par fonctions polynomiales par morceaux dans un codage dense

$\mathcal{C}_{\mathrm{sfrac}}$ présentation par fonctions fractions rationnelles par morceaux dans un codage par formules

1.2 Classes de fonctions discrètes intéressantes

Nous considérerons des classes de fonctions discrètes $\mathcal{C}$ (une fonction discrète est une fonction de $A^\star$ vers $B^\star$ où A et B sont deux alphabets finis[2]) jouissant des propriétés de stabilité élémentaires suivantes

- $\mathcal{C}$ contient les fonctions arithmétiques usuelles et le test de comparaison dans $\mathbb{Z}$ (pour $\mathbb{Z}$ codé en binaire).
- $\mathcal{C}$ contient les fonctions calculables en temps linéaire (c.-à-d. $\mathbf{LINTIME} \subset \mathcal{C}$)
- $\mathcal{C}$ est stable par composition.
- $\mathcal{C}$ est stable par listes : si $f : A^\star \to B^\star$ est dans $\mathcal{C}$ alors $\mathbf{lst}(f) : \mathbf{lst}(A^\star) \to \mathbf{lst}(B^\star)$ est également dans $\mathcal{C}$ ($\mathbf{lst}(f)[x_1, x_2, \ldots, x_n] = [f(x_1), f(x_2), \ldots, f(x_n)]$).

Une classe vérifiant les propriétés de stabilité précédentes sera dite *élémentairement stable*. En pratique, on sera particulièrement intéressé par les classes élémentairement stables suivantes :

- **Rec** : la classe des fonctions récursives.
- **Fnc** : la classe des fonctions constructivement définies (en mathématiques constructives, ce concept est un concept primitif qui ne coïncide pas avec le précédent, et il est nécessaire de l'avoir au préalable pour pouvoir définir le précédent, la récursivité étant interprétée comme une constructivité purement mécanique dans son déroulement comme processus de calcul)
- **Prim** : la classe des fonctions primitives récursives.
- $\mathcal{P}$: la classe des fonctions calculables en temps polynomial.
- $\mathcal{E}$: la classe des fonctions élémentairement récursives, c.-à-d. encore calculables en temps majoré par une composée d'exponentielles.
- **PSPACE** : la classe des fonctions calculables en espace polynomial (avec une sortie polynomialement majorée en taille).
- **LINSPACE** : la classe des fonctions calculables en espace linéaire (avec une sortie linéairement majorée en taille).
- $\mathbf{DSRT}(Lin, Lin, Poly)$: la classe des fonctions calculables en espace linéaire, en temps polynomial et avec une sortie linéairement majorée en taille.
- $\mathbf{DSRT}(Lin, Lin, \mathrm{O}(n^k))$: la classe des fonctions calculables en espace linéaire, en temps $\mathrm{O}(n^k)$ (avec $k > 1$) et avec une sortie linéairement majorée en taille.
- $\mathbf{DSRT}(Lin, Lin, Exp)$: la classe des fonctions calculables en espace linéaire, en temps $exp(\mathrm{O}(n))$ et avec une sortie linéairement majorée en taille.
- $\mathbf{DRT}(Lin, \mathrm{O}(n^k))$: la classe des fonctions calculables en temps $\mathrm{O}(n^k)$, (avec $k > 1$) et avec une sortie linéairement majorée en taille..
- $\mathbf{DSR}(Poly, Lin)$: la classe des fonctions calculables en espace polynomial avec une sortie linéairement majorée en taille.
- $\mathbf{DSR}(\mathrm{O}(n^k), Lin)$: la classe des fonctions calculables en espace $\mathrm{O}(n^k)$, (avec $k > 1$) avec une sortie linéairement majorée en taille.
- **QL** : la classe des fonctions calculables en temps quasilinéaire[3] ($\mathbf{QL} := \cup_b \mathbf{DTIME}(\mathrm{O}(n.lg^b(n))) = \mathbf{DTIME}(QLin)$).

[2] Si on veut donner une allure plus mathématique et moins informatique à la chose, on pourra remplacer $A^\star$ et $B^\star$ par des ensembles $\mathbb{N}^k$.

[3] Cf. Schnorr [33].

On remarquera que, hormis les classes **Rec** et **Fnc**, toutes les classes que nous avons considérées sont des classes de complexité (au sens de Blum). Il n'y a cependant aucune nécessité à cela, comme le montrent justement les exemples de **Rec** et **Fnc**. Lorsque nous considérons uniquement la classe **Fnc**, nous développons un chapitre de mathématiques constructives abstraites. Notez que $\mathbf{DTIME}(\mathrm{O}(n^k))$ pour $k > 1$ n'est pas stable par composition. Mais, le plus souvent, les calculs en temps $\mathrm{O}(n^k)$ que nous aurons à considérer sont dans la classe $\mathbf{DRT}(Lin, \mathrm{O}(n^k))$ ou même $\mathbf{DSRT}(Lin, Lin, \mathrm{O}(n^k))$ et ces classes ont les bonnes propriétés de stabilité.

1.3 Complexité d'une Machine de Turing Universelle

Nous aurons besoin dans la suite d'utiliser une Machine de Turing Universelle et d'estimer sa complexité algorithmique. Le résultat suivant, pour lequel nous n'avons pas trouvé de référence, semble faire partie du folklore, il nous a été signalé par M. Margenstern.

Lemme 1.3.1 *Il existe une machine de Turing universelle MU qui fait le travail suivant.*
Elle prend en entrée :
— le code (dont la taille est p) d'une machine de Turing M_0 (fonctionnant sur un alphabet fixé, avec une bande d'entrée, une bande de sortie, plusieurs bandes de travail) supposée être de complexité en temps T et en espace S (avec $S(n) \geq n$)
— une entrée x (de taille n) pour M_0.
Elle donne en sortie le résultat du calcul exécuté par M_0 pour l'entrée x.
Elle exécute cette tâche en un temps $\mathrm{O}(T(n)(S(n)+p))$ et en utilisant un espace $\mathrm{O}(S(n)+p)$.

Preuve. La machine MU utilise une bande de travail pour y écrire, à chaque étape élémentaire de la machine M_0, qu'elle simule, la liste des contenus de chacune des variables de M_0. Pour simuler une étape de M_0 la machine MU a besoin de $\mathrm{O}(S(n)+p)$ étapes élémentaires, en utilisant un espace du même ordre de grandeur. ∎

1.4 Circuits et programmes d'évaluation

Les familles de circuits constituent des modèles de calcul intéressants, notamment du point de vue du parallélisme. Les familles de circuits booléens constituent dans une certaine mesure une alternative au modèle standard des Machines de Turing. Des circuits arithmétiques de faible taille sont capables de calculer des polynômes de très grand degré. C'est par exemple le cas pour un circuit arithmétique qui simule une itération de Newton pour une fonction donnée par une fraction rationnelle.
Dans tous les cas se pose le problème de savoir quel codage on adopte pour un circuit. Nous choisirons de toujours coder un circuit par un des programmes d'évaluation (ou straight-line program) qui exécutent la même tâche que lui[4]).
Par ailleurs, concernant les circuits arithmétiques, qui représentent des polynômes ou des fractions rationnelles, nous les envisagerons non du point de vue du calcul exact (ce qui serait trop coûteux), mais du point de vue du calcul approché. Se pose alors la question d'évaluer leur temps d'exécution lorsqu'on veut garantir une précision donnée sur le résultat, pour des entrées dans $\mathbb{D}$ données elles-mêmes avec une certaine précision. Aucune majoration raisonnable du temps d'exécution ne peut être obtenue par des arguments d'ordre général si la profondeur du circuit n'est pas très faible, car les degrés obtenus sont trop grands et les nombres calculés risquent de voir leur taille exposer. Comme on n'arrive pas toujours à se limiter à des circuits

[4] A un même circuit peuvent correspondre différents programmes d'évaluation selon l'ordre dans lequel on écrit les instructions à exécuter.

de très faible profondeur, il s'avère indispensable de donner un paramètre de contrôle, appelé magnitude, qui assure que, malgré un éventuel très grand degré, la taille de tous les nombres calculés par le circuit (qui seront évalués avec une précision elle même limitée) n'est pas trop grande lorsque l'entrée représente un réel variant dans un intervalle compact.

2 Espaces métriques complets rationnellement présentés

2.1 Présentation rationnelle d'un espace métrique, complexité des points et des familles de points

Sauf mention expresse du contraire, les classes de fonctions discrètes que nous considérons seront des classes élémentairement stables.

Définition 2.1.1 *(présentation rationnelle de classe $\mathcal{C}$ pour un espace métrique complet)*
Un espace métrique complet (X, d_X) est *donné dans une présentation rationnelle de classe $\mathcal{C}$* de la manière suivante. On donne un triplet (Y, δ, η) où

- Y est une $\mathcal{C}$-partie d'un langage $A^\star$
- η est une application de Y dans X
- $\delta : Y \times Y \times \mathbb{N}_1 \to \mathbb{D}$ est une fonction dans la classe $\mathcal{C}$ et vérifiant (pour $n \in \mathbb{N}_1$ et $x, y, z \in Y$) :
  — $\mid d_X(x,y) - \delta(\eta(x), \eta(y)) \mid \leq 1/2^n$
  — $\delta(x, y, n) \in \mathbb{D}_n$
  — $\delta(x, y, n) = \delta(y, x, n)$
  — $\delta(x, x, n) = 0$
  — $\mid \delta(x, y, n+1) - \delta(x, y, n) \mid \leq 1/2^{n+1}$
  — $\delta(x, z, n) \leq \delta(x, y, n) + \delta(y, z, n) + 2/2^n$

Si on définit l'écart $d_Y(x, y)$ comme la limite de $\delta(x, y, n)$ lorsque n tend vers l'infini, l'application η de Y dans X identifie (X, d_X) au séparé complété de (Y, d_Y). L'ensemble $\eta(Y)$ est appelé l'ensemble des *points rationnels* de X pour la présentation considérée. Si $y \in Y$ on notera souvent $\widetilde{y}$ pour $\eta(y)$, et y est appelé le code de $\widetilde{y}$.

Nous abrégerons parfois "(Y, δ, η) est une présentation rationnelle de classe $\mathcal{C}$ pour (X, d_X)" en "(Y, δ) est une $\mathcal{C}$-présentation de (X, d_X)".

Remarques 2.1.2 1) On peut remplacer $\mathbb{D}$ par $\mathbb{Q}$ dans la définition ci-dessus sans modifier la notion qui est définie. Le fait de choisir $\mathbb{Q}$ est plus joli mathématiquement, tandis que le fait de choisir $\mathbb{D}$ est plus naturel d'un point de vue informatique. En outre la contrainte $\delta(x, y, n) \in \mathbb{D}_n$ répond à la requête naturelle de ne pas utiliser plus de place que nécessaire pour représenter une approximation à $1/2^n$ près d'un nombre réel.
2) Lorsqu'on a donné une présentation rationnelle pour un espace métrique abstrait (X, d_X), on dira qu'*on l'a muni d'une structure de calculabilité*. Cela revient essentiellement à définir un langage $Y \subset A^\star$ puis une application η de Y vers X dont l'image soit une partie dense de X. La présentation est complètement définie uniquement lorsqu'on a aussi donné une application $\delta : Y \times Y \times \mathbb{N}_1 \to \mathbb{D}$ vérifiant les requêtes de la définition 2.1.1. *Dans la suite, on se permettra néanmoins de dire qu'un codage d'une partie dense Y de X définit une présentation de classe $\mathcal{C}$ de X lorsqu'on montre que les requêtes de la définition 2.1.1 peuvent être satisfaites.*
3) Comprise au sens constructif, la phrase incluse dans la définition "on donne une application η de Y vers X" réclame qu'on ait "un certificat que $\eta(y)$ soit bien un élément de X pour tout y de

Y". Il se peut que ce certificat d'appartenance implique lui-même une notion naturelle de complexité. Lorsque ce sera le cas, par exemple pour l'espace $\mathbf{C}[0,1]$, il sera inévitable de prendre en compte cette complexité. *Ainsi, la définition 2.1.1 doit en l'état actuel être considérée comme incomplète et à préciser au cas par cas.* C'est sans doute dommage si on se place du point de vue l'élégance formelle des définitions générales. Mais c'est une situation de fait qui semble très difficile à contourner.

Exemples 2.1.3
— L'espace $\mathbb{R}$ est défini usuellement dans la présentation où l'ensemble des points rationnels est $\mathbb{Q}$. De manière équivalente, et c'est ce que nous ferons dans la suite, on peut considérer comme ensemble des points rationnels de $\mathbb{R}$ l'ensemble $\mathbb{D}$ des nombres dyadiques[5].
— On définira sans difficulté la présentation produit de deux présentations pour deux espaces métriques.
— Tout *ensemble discret* Z (Z est donné comme une partie d'un langage $A^\star$ avec une relation d'équivalence qui définit l'égalité dans Z et qui est testable dans la classe $\mathcal{C}$) donne lieu à un *espace métrique discret*, c.-à-d. dans lequel la distance de deux points distincts est égale à 1.
— Les espaces métriques complets des mathématiques constructives dans le style Bishop [5] admettent en général une présentation rationnelle de classe **Fnc**. Dans chaque cas concret la présentation s'avère être une présentation de classe **Prim** ou même $\mathcal{P}$.

Définition 2.1.4 *(Complexité d'un point dans un espace métrique rationnellement présenté)* On considère un espace métrique complet X donné dans une présentation (Y,δ,η) de classe $\mathcal{C}'$. Un point x de X est dit *de classe* $\mathcal{C}$ lorsqu'on connaît une suite $(n\mapsto y_n)$ de classe $\mathcal{C}$ (en tant que fonction $\mathbb{N}_1\to Y$) avec $d_X(x,\eta(y_n))\leq 1/2^n$. On dit encore que x est *un $\mathcal{C}$-point dans X*.

Exemple 2.1.5 Lorsque $X=\mathbb{R}$, la définition ci-dessus correspond à la notion usuelle de "nombre réel de classe $\mathcal{C}$" (au sens de Cauchy).

Remarque 2.1.6 Il semblerait naturel de demander que la classe $\mathcal{C}'$ contienne la classe $\mathcal{C}$, mais ce n'est pas complètement indispensable. Cette remarque vaut pour à peu près toutes les définitions qui suivent.

Définition 2.1.4bis *(Complexité d'un point dans un espace métrique rationnellement présenté, version plus explicite)* On considère un espace métrique complet X donné dans une présentation de classe $\mathcal{C}'$: (Y,δ,η).
Un point x de classe $\mathcal{C}$ dans X est donné par une suite $(n\mapsto y_n)$ de classe $\mathcal{C}$ (en tant que fonction $\mathbb{N}_1\to Y$) vérifiant la condition suivante

$$\delta(y_n,y_{n+1},n+1)\leq 1/2^n$$

avec $x=\lim_{n\to\infty}\eta(y_n)$.

Nous laissons au lecteur ou à la lectrice le soin de vérifier que les deux définition 2.1.4 et 2.1.4bis sont équivalentes. Nous passons maintenant à la définition de la complexité pour une famille de points (avec un ensemble d'indices discret)

Définition 2.1.7 *(Complexité d'une famille de points dans un espace métrique rationnellement présenté)*
On considère un préensemble discret Z (c'est l'ensemble des indices de la famille, il est donné comme une partie d'un langage $A^\star$ sur un alphabet fini A) et un espace métrique complet X donné dans une présentation de classe $\mathcal{C}'$: (Y,δ,η). Une fonction (ou famille) $f:Z\to X$ est

[5] Cela correspond à la notation $\mathbb{R}_{conv}$ dans [20] et $\mathbb{R}_{con}$ dans [17].

dite de classe $\mathcal{C}$ lorsqu'on connaît une fonction $\varphi : Z \times \mathbb{N}_1 \to Y$ qui est de classe $\mathcal{C}$ et qui vérifie :

$$d_X(f(z), \eta(\varphi(z,n))) \leq 1/2^n \text{ pour tout } z \in Z.$$

On dit alors que φ est *une présentation de classe $\mathcal{C}$ de la famille $f(z)_{z\in Z}$ de points de X.*

Exemples 2.1.8
— Lorsque $Z = \mathbb{N}_1$ et $X = \mathbb{R}$ la définition ci-dessus correspond à la notion usuelle de "suite de réels de classe $\mathcal{C}$" (on dit encore : *une $\mathcal{C}$-suite dans* $\mathbb{R}$).
— La définition d'un espace rationnellement présenté dans la classe $\mathcal{C}$ peut être relue de la manière suivante. On donne :
– une $\mathcal{C}$-partie Y d'un langage $A^\star$.
– une fonction $\varphi : Y \to X$ telle que $\varphi(Y)$ soit dense dans X et telle que la famille de nombres réels $Y \times Y \to \mathbb{R}, \quad (y_1, y_2) \mapsto d_X(\varphi(y_1), \varphi(y_2))$ soit de classe $\mathcal{C}$.

Proposition 2.1.9 *Soit (x_n) une suite de classe $\mathcal{C}$ (l'ensemble d'indices est $\mathbb{N}_1$) dans un espace métrique rationnellement présenté (X, d). Si la suite est explicitement de Cauchy avec la majoration $d(x_n, x_{n+1}) \leq 1/2^n$ alors la limite de la suite est un point de classe $\mathcal{C}$ dans X.*

Preuve. Soient (Y, δ, η) une représentation rationnelle de (X, d) et x la limite de la suite (x_n). La suite (x_n) est de classe $\mathcal{C}$ dans X, donc il existe une fonction $\psi : \mathbb{N}_1 \times \mathbb{N}_1 \to Y$ de classe $\mathcal{C}$ telle que :

$$d(x_n, \psi(n,m) \leq 1/2^m \text{ pour tout } n, m \in \mathbb{N}_1.$$

On pose $z_n = \psi(n+1, n+1)$, c'est une suite de classe $\mathcal{C}$ et

$$d(x, z_n) \leq d(x, x_{n+1}) + d(x_{n+1}, \psi(n+1, n+1)) \leq 1/2^{n+1} + 1/2^{n+1} = 1/2^n.$$

Donc x est un $\mathcal{C}$-point dans X. ∎

Remarque 2.1.10 Si on ralentit suffisamment la vitesse de convergence de la suite de Cauchy, on peut obtenir comme point limite d'une suite de classe $\mathbf{DTIME}(n^2)$ un point récursif arbitraire de X (cf. [15] pour l'espace $[0, 1]$).

Définition 2.1.7bis *(Complexité d'une famille de points dans un espace métrique rationnellement présenté, version plus explicite)* On considère un préensemble discret Z (une partie d'un langage $A^\star$) et un espace métrique complet X donné dans une présentation de classe $\mathcal{C}' : (Y, \delta, \eta)$. Une famille $f : Z \to X$ est dite de classe $\mathcal{C}$ si on a une fonction $\varphi : Z \times \mathbb{N}_1 \to Y$ de classe $\mathcal{C}$ qui vérifie :

$$\delta(\varphi(z,n), \varphi(z,n+1), n+1) \leq 1/2^n \text{ pour tout } z \in Z.$$

avec $f(z) = \lim_{n\to\infty} \eta(\varphi(z,n))$.

2.2 Complexité des fonctions uniformément continues

Nous commençons par donner une définition "raisonnable" qui sera justifiée par les exemples et propositions qui suivent.

Définition 2.2.1 *(complexité des fonctions uniformément continues entre espaces métriques rationnellement présentés)* On considère deux espaces métriques complets X_1 et X_2 donnés dans des présentations de classe $\mathcal{C}' : (Y_1, \delta_1, \eta_1)$ et (Y_2, δ_2, η_2). Soient $f : X_1 \to X_2$ une fonction

uniformément continue et $\mu : \mathbb{N}_1 \to \mathbb{N}_1$ une suite d'entiers.
On dira que μ est *un module de continuité uniforme pour la fonction* f si on a :

$$d_{X_1}(x,y) \leq 1/2^{\mu(n)} \Rightarrow d_{X_2}(f(x),f(y)) \leq 1/2^n \text{ pour tous } x,y \in X_1 \text{ et } n \in \mathbb{N}_1$$

On dira que la fonction f est *uniformément de classe* $\mathcal{C}$ (pour les présentations considérées) lorsque
— elle possède un module de continuité uniforme $\mu : \mathbb{N}_1 \to \mathbb{N}_1$ dans la classe $\mathcal{C}$
— la restriction de f à Y_1 est dans la classe $\mathcal{C}$ au sens de la définition 2.1.7, c.-à-d. qu'elle est présentée par une fonction $\varphi : \mathbb{N}_1 \times Y_1 \to Y_2$ qui est de classe $\mathcal{C}$ et qui vérifie :

$$d_{X_2}(f(y),\eta_2(\varphi(y,n))) \leq 1/2^n \text{ pour tout y} \in \mathrm{Y}_1.$$

Lorsque $X_1 = X_2 = X$ la fonction Id_X admet $\mathrm{Id}_{\mathbb{N}_1}$ pour module de continuité uniforme. Si les deux fonctions Id_X (de X_1 vers X_2 et de X_2 vers X_1) sont dans la classe $\mathcal{C}$ on dira que *les deux présentations sont (uniformément)* $\mathcal{C}$*-équivalentes.*

Remarques 2.2.2
1) On ne demande pas que, pour n fixé, la fonction $y \mapsto \varphi(y,n)$ soit uniformément continue sur Y_1 ni même qu'elle soit continue en chaque point de Y_1.
2) Notez que la définition ici donne un module de continuité uniforme correspondant (à très peu près) à la définition donnée en analyse constructive. En théorie classique de l'approximation on appelle en général module de continuité uniforme une suite croissante d'entiers $n \mapsto \nu(n)$ qui tend vers l'infini et qui vérifie :

$$d_{X_1}(x,y) \leq 1/2^n \Rightarrow d_{X_2}(f(x),f(y)) \leq 1/2^{\nu(u)}$$

La fonction ν est en quelques sorte "duale" de la fonction μ.

Exemples 2.2.3
— Lorsque $X_1 = [0,1]$ et $X_2 = \mathbb{R}$ et lorsque $\mathcal{C}$ est une classe de complexité en temps ou en espace *élémentairement stable*, la définition ci-dessus est équivalente à la notion usuelle de fonction réelle calculable dans la classe $\mathcal{C}$ (cf. [15], [18]), comme nous le prouverons en détail à la proposition 4.1.5.
— Lorsque X_1 est un espace métrique discret la définition 2.2.1 redonne la définition 2.1.7.

La définition 2.2.1 rend accessible la notion de complexité pour les fonctions uniformément continues. Cela traite donc toutes les fonctions continues dans le cas où l'espace de départ est compact. Rappelons à ce sujet qu'en analyse constructive on définit, dans le cas d'un espace compact, la continuité comme signifiant la continuité uniforme (cf. [5]) et non pas la continuité en tout point.

Remarque 2.2.4 Le contrôle de la continuité donné par le module de continuité uniforme est essentiel dans la définition 2.2.1. On peut par exemple définir une fonction $\varphi : [0,1] \to \mathbb{R}$ qui est continue au sens classique, dont la restriction à $\mathbb{D}_{[0,1]} = \mathbb{D} \cap [0,1]$ est **LINTIME** mais qui ne possède pas de module de continuité uniforme récursif. Pour cela on considère une fonction $\theta : \mathbb{N} \to \mathbb{N}$ de classe **LINTIME** injective et d'image non récursive. Pour chaque $m \in \mathbb{N}_1$ on considère $n = \theta(m)$, $a_n = 1/(3.2^n)$ et on définit $\psi_m : [0,1] \to \mathbb{R}$ partout nulle sauf sur un intervalle centré en a_n sur lequel le graphe de ψ_m fait une pointe de hauteur $1/2^n$ avec une pente égale à $1/2^m$. Enfin, on définit φ comme la somme de la série $\sum_m \psi_m$. Bien que la suite $\varphi(a_n)$ ne soit pas une suite récursive de nombres réels (ce qui implique d'ailleurs que φ ne puisse avoir de module de continuité uniforme récursif), la restriction de φ aux nombres dyadiques

est très facile à calculer (les nombres réels litigieux a_n ne sont pas des dyadiques). Cet exemple met bien en évidence que *la définition classique de la continuité (la continuité en tout point) ne permet pas d'avoir accès au calcul des valeurs de la fonction à partir de sa restriction à une partie dense de l'espace de départ.*

Remarque 2.2.5 Dans [15] il est "démontré" que si une fonctionnelle définie via une machine de Turing à oracle (MTO) calcule une fonction de $[0,1]$ vers $\mathbb{R}$, alors la fonction possède un module de continuité uniforme récursif. Si on évite tout recours aux principes non constructifs (caché dans le théorème de Heine-Borel), la preuve de [15] peut être facilement transformée en une preuve constructive du théorème suivant : si une fonction $f : [0,1] \to \mathbb{R}$ est uniformément continue et calculable par une MTO, alors son module de continuité uniforme est récursif.
A contrario, si on fait l'hypothèse (nullement invraisemblable) selon laquelle tout oracle d'une machine de Turing serait fourni par un procédé mécanique (mais inconnu), il est possible de définir des fonctions "pathologiques" de $[0,1]$ dans $\mathbb{R}$ au moyen de machines de Turing à oracles : ce sont des fonctions continues en tout point réel récursif mais non uniformément continues. Ceci est basé sur l'"arbre singulier de Kleene" : un arbre binaire récursif infini qui ne possède aucune branche infinie récursive. Cf. [3], théorème de la section 7 du chapitre 4, page 70 où est donnée une fonction $t(x)$ continue en tout point réel récursif sur $[0,1]$, mais qui n'est pas bornée (donc pas uniformément continue) sur cet intervalle.
Il semble étrange que dans une preuve concernant les questions de calculabilité, on puisse utiliser sans même la mentionner l'hypothèse que les oracles d'une MTO se comportent de manière antagonique avec la Thèse de Church (du moins sous la forme où elle est admise dans le constructivisme russe).

On vérifie sans peine que la définition 2.2.1 peut être traduite sous la forme plus explicite suivante :

Définition 2.2.1bis *(complexité des fonctions uniformément continues entre espaces métriques rationnellement présentés, forme plus explicite)* On considère deux espaces métriques complets X_1 et X_2 donnés dans des présentations de classe $\mathcal{C}'$: (Y_1, δ_1, η_1) et (Y_2, δ_2, η_2). Une fonction uniformément continue $f : X_1 \to X_2$ est dite *uniformément de classe* $\mathcal{C}$ (pour les présentations considérées) lorsqu'elle est présentée au moyen de deux données :
— la restriction de f à Y_1 est présentée par une fonction $\varphi : Y_1 \times \mathbb{N}_1 \to Y_2$ qui est de classe $\mathcal{C}$ et qui vérifie :

$$\delta_2(\varphi(y,n), \varphi(y,n+1), n+1) \leq 1/2^n \text{ pour tout y} \in \mathrm{Y}_1.$$

avec $f(y) = \lim_{n\to\infty} \eta_2(\varphi(y,n))$.
— une suite $\mu : \mathbb{N}_1 \to \mathbb{N}_1$ dans la classe $\mathcal{C}$ vérifiant : pour tous x et y dans Y_1

$$\delta_1(x,y,\mu(n)) \leq 1/2^{\mu(n)} \;\Rightarrow\; \delta_2(\varphi(x,n+2), \varphi(y,n+2), n+2) \leq 1/2^n.$$

Les résultats qui suivent sont faciles à établir.

Proposition 2.2.6 *La composée de deux fonctions uniformément de classe $\mathcal{C}$ est une fonction uniformément de classe $\mathcal{C}$.*

Proposition 2.2.7 *L'image d'un point (respectivement d'une famille de points) de classe $\mathcal{C}$ par une fonction uniformément de classe $\mathcal{C}$ est un point (respectivement d'une famille de points) de classe $\mathcal{C}$.*

Remarque 2.2.8 Considérons deux présentations rationnelles d'un même espace métrique complet X données par les deux familles de points rationnels respectifs $(\widetilde{y})_{y\in Y}$ et $(\widetilde{z})_{z\in Z}$. La

première famille est **LINTIME** pour la première présentation, et elle peut naturellement être de plus grande complexité pour la deuxième. *Dire que l'identité de X est uniformément de classe $\mathcal{C}$ lorsqu'on passe de la première à la deuxième présentation revient exactement à dire que la famille $(\widetilde{y})_{y\in Y}$ est une $\mathcal{C}$- famille de points pour la deuxième présentation.* Ainsi les deux présentations sont $\mathcal{C}$-équivalentes si et seulement si la famille $(\widetilde{y})_{y\in Y}$ est une famille de classe $\mathcal{C}$ dans la seconde présentation et $(\widetilde{z})_{z\in Z}$ est une famille de classe $\mathcal{C}$ dans la première. La proposition 2.2.7 nous permet de formuler un résultat analogue et plus intrinsèque : *deux présentations rationnelles d'un même espace métrique complet sont $\mathcal{C}$-équivalentes si et seulement si elles définissent les mêmes familles de points de classe $\mathcal{C}$.*

Nous passons maintenant à la définition de la complexité pour une famille de fonctions uniformément continues (avec un ensemble d'indices discret).

Définition 2.2.9 *(complexité d'une famille de fonctions uniformément continues entre espaces métriques rationnellement présentés)*
On considère un préensemble discret Z (c'est l'ensemble des indices de la famille, il est donné comme une partie d'un langage $A^\star$ sur un alphabet fini A) et deux espaces métriques complets X_1 et X_2 donnés dans des présentations de classe $\mathcal{C}'$: (Y_1, δ_1, η_1) et (Y_2, δ_2, η_2).
Nous notons $\mathbf{U}(X_1, X_2)$ l'ensemble des fonctions uniformément continues de X_1 dans X_2. Une famille de fonctions uniformément continues $\widetilde{f} : Z \to \mathbf{U}(X_1, X_2)$ est dite *uniformément de classe $\mathcal{C}$* (pour les présentations considérées) lorsque
— la famille possède un module de continuité uniforme $\mu : Z \times \mathbb{N}_1 \to \mathbb{N}_1$ dans la classe $\mathcal{C}$: la fonction μ doit vérifier

$$\forall n \in \mathbb{N}_1 \; \forall x, y \in X_1 \quad (d_{X_1}(x, y) \leq 1/2^{\mu(f,n)} \Rightarrow d_{X_2}(\widetilde{f}(x), \widetilde{f}(y)) \leq 1/2^n)$$

— la famille $(f, x) \mapsto \widetilde{f}(x) : Z \times X_2 \to X_2$ est une famille de points dans X_2 de classe $\mathcal{C}$ au sens de la définition 2.1.7, c.-à-d. qu'elle est présentée par une fonction $\varphi : Z \times Y_1 \times \mathbb{N}_1 \to Y_2$ qui est de classe $\mathcal{C}$ et qui vérifie :

$$d_{X_2}(\widetilde{f}(x), \varphi(f, x, n)) \leq 1/2^n \text{ pour tout } (f, x, n) \in Z \times Y_1 \times \mathbb{N}.$$

Remarque 2.2.10 La notion définie en 2.2.9 est naturelle car elle est la relativisation à la classe $\mathcal{C}$ de la notion constructive de famille de fonctions uniformément continues. Mais cette notion naturelle ne semble pas pouvoir se déduire de la définition 2.2.1 en munissant $Z \times X_1$ d'une structure convenable d'espace métrique rationnellement présenté et en demandant que la fonction $(f, x) \mapsto \widetilde{f}(x) : Z \times X_2 \to X_2$ soit uniformément de classe $\mathcal{C}$. Si par exemple, on prend sur $Z \times X_1$ la métrique déduite de la métrique discrète de Z et de la métrique de X_1 on obtiendra la deuxième des conditions de la définition 2.2.9 mais la première sera remplacée par la demande que toutes les fonctions de la famille aient un même module de continuité uniforme de classe $\mathcal{C}$. C'est-à-dire que la famille devrait être uniformément équicontinue. Cette condition est intuivement trop forte. Les propositions 2.2.11 et 2.2.12 qui suivent sont une confirmation que la définition 2.2.9 est convenable.

Les propositions 2.2.6 et 2.2.7 se généralisent au cas des familles de fonctions. Les preuves ne présentent aucune difficulté.

Proposition 2.2.11 *Soient deux espaces métriques complets X_1 et X_2 rationnellement présentés. Soit $(\widetilde{f})_{f\in Z}$ une famille dans $\mathbf{U}(X_1, X_2)$ uniformément de classe $\mathcal{C}$ et $(x_n)_{n\in\mathbf{N}_1}$ une famille de classe $\mathcal{C}$ dans X_1.*
Alors la famille $(\widetilde{f}(x_n))_{(f,n)\in Z\times\mathbf{N}_1}$ est une famille de classe $\mathcal{C}$ dans X_2.

Proposition 2.2.12 *Soient trois espaces métriques complets X_1, X_2 et X_3 rationnellement présentés. Soit $(\widetilde{f})_{f\in Z}$ une famille dans $\mathbf{U}(X_1, X_2)$ uniformément de classe $\mathcal{C}$ et $(\widetilde{g})_{g\in Z'}$ une famille dans $\mathbf{U}(X_2, X_3)$ uniformément de classe $\mathcal{C}$.*
Alors la famille $(\widetilde{f}\circ\widetilde{g})_{(f,g)\in Z\times Z'}$ dans $\mathbf{U}(X_1, X_3)$ est uniformément de classe $\mathcal{C}$.

2.3 Complexité des fonctions "localement uniformément continues"

La notion de complexité définie au paragraphe précédent pour les fonctions uniformément continues est entièrement légitime lorsque l'espace de définition est compact. Dans le cas d'un espace localement compact au sens de Bishop[6] les fonctions continues sont les fonctions uniformément continues sur tout borné (du point de vue classique c'est un théorème, du point de vue constructif, c'est une définition). Ceci conduit à la notion de complexité naturelle suivante.

Définition 2.3.1 On considère deux espaces métriques complets X_1 et X_2 donnés dans des présentations de classe $\mathcal{C}'$: (Y_1, δ_1, η_1) et (Y_2, δ_2, η_2). On suppose avoir spécifié un point x_0 de X_1 et un point y_0 de X_2. Une fonction $f : X_1 \to X_2$ est dite *localement uniformément continue* si elle est uniformément continue et bornée sur toute partie bornée.
Elle est dite *localement uniformément de classe $\mathcal{C}$* (pour les présentations considérées) lorsque
— elle possède dans la classe $\mathcal{C}$ une borne sur tout borné, c.-à-d. une suite $\beta : \mathbb{N}_1 \to \mathbb{N}_1$ vérifiant, pour tout x dans X_1 et tout m dans $\mathbb{N}_1$:

$$d_{X_1}(x_0, x) \leq 1/2^n \Rightarrow d_{X_2}(y_0, f(x)) \leq 1/2^{\beta(n)}$$

— elle possède dans la classe $\mathcal{C}$ un module de continuité uniforme sur tout borné, c.-à-d. une suite $\mu : \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{N}_1$ vérifiant, pour x, z dans X_1 et n, m dans $\mathbb{N}_1$:

$$\left(d_{X_1}(x_0, x) \leq 1/2^m,\ d_{X_1}(x, z) \leq 1/2^{\mu(m,n)}\right) \ \Rightarrow\ d_{X_2}(f(x), f(z)) \leq 1/2^n$$

— la restriction de f à Y_1 est dans la classe $\mathcal{C}$ au sens de la définition 2.1.7, c.-à-d. qu'elle est présentée par une fonction $\varphi : \mathbb{N}_1 \times Y_1 \to Y_2$ qui est de classe $\mathcal{C}$ et qui vérifie :

$$d_{X_2}(f(y), \varphi(y, n)) \leq 1/2^n \text{ pour tout } y \in Y_1.$$

Notez que la notion définie ci-dessus ne dépend pas du choix des points x_0 et y_0.

Exemples 2.3.2
— Lorsque $X_1 = \mathbb{R}$ et $X_2 = \mathbb{R}$ la définition ci-dessus est équivalente à la notion naturelle de fonction réelle calculable dans la classe $\mathcal{C}$ telle qu'on la trouve dans [13] et [18].
— La fonction $x \mapsto x^2$ est localement uniformément continue de classe **QL** mais elle n'est pas uniformément continue sur $\mathbb{R}$.

Remarques 2.3.3
1) Lorsque f est une fonction uniformément continue, la définition 2.3.1 et la définition 2.2.1 se ressemblent beaucoup. Cependant la définition 2.2.1 est a priori plus contraignante. En effet, si $\mu(n)$ est un module de continuité dans la définition 2.2.1, alors on peut prendre dans la définition 2.3.1 $\mu'(m, n) = \mu(n)$. Mais réciproquement, supposons qu'on ait un module de continuité uniforme près de tout borné vérifiant $\mu'(m, n) = \inf(m, 2^n)$ alors, la fonction est uniformément continue mais le meilleur module de continuité uniforme qu'on puisse en déduire est

$$\mu(n) = \sup\{\mu'(m, n) : m \in \mathbb{N}\} = 2^n$$

[6] Cf. [5] : tout borné est contenu dans un compact.

et il a un taux de croissance exponentiel alors que $\mu'(m,n)$ est linéaire. Ainsi la fonction f peut être de complexité linéaire en tant que fonction localement uniformément continue, et exponentielle en tant que fonction uniformément continue. Les deux définitions sont équivalentes si l'espace X_1 a un diamètre fini.
2) En analyse constructive un espace compact est un espace précompact et complet. Il n'est pas possible de démontrer constructivement que toute partie fermée d'un espace compact est compacte. Un espace (uniformément) localement compact est un espace métrique complet dans lequel tout borné est contenu dans un compact K_n, où la suite (K_n) est une suite croissante donnée une fois pour toutes (par exemple le compact K_n contient la boule $B(x_0, 2^n)$). Une fonction définie sur un tel espace est alors dite continue si elle est uniformément continue sur toutes les parties bornées. En particulier elle est bornée sur toute partie bornée. La définition 2.3.1 permet donc de donner dans ce cas une version "complexité" de la définition constructive de la continuité.
3) La proposition 2.2.6 sur la composition des fonctions uniformément de classe $\mathcal{C}$ reste valable pour les fonctions localement uniformément de classe $\mathcal{C}$. La proposition 2.2.7 également.

2.4 Une approche générale de la complexité des fonctions continues

La question de la complexité des fonctions continues n'est manifestement pas épuisée. Comme nous l'avons déjà signalé, s'il est bien vrai qu'une fonction continue $f(x)$ est classiquement bien connue à partir d'une présentation $(y,n) \mapsto \varphi(y,n)$ qui permet de la calculer avec une précision arbitraire sur une partie dense Y de X, la complexité de φ ne peut être tenue que pour un pâle reflet de la complexité de f (cf. les remarques 2.2.4 et 2.3.3(1)). Une question cruciale, et peu étudiée jusqu'à présent, est de savoir jusqu'à quel point on peut certifier qu'une telle donnée φ correspond bien à une fonction continue f. Dans le cas d'une réponse positive, il faut expliquer par quelle procédure on peut calculer des valeurs approchées de $f(x)$ lorsque x est un point arbitraire de X (donné par exemple par une suite de Cauchy de points rationnels de la présentation dans le cas d'un espace métrique rationnellement présenté).
Nous proposons une approche un peu informelle de cette question. Soit $\phi : X_1 \to X_2$ une fonction entre espaces métriques et $(F_\alpha)_{\alpha\in M}$ une famille de parties de X_1. *Un module de continuité uniforme pour ϕ près de chaque partie F_α* est par définition une fonction $\mu : M \times \mathbb{N}_1 \to \mathbb{N}_1$ vérifiant :

$$\forall \alpha \in M\ \forall x \in F_\alpha \quad \big(d_{X_1}(x,x') \le 1/2^{\mu(\alpha,n)} \Rightarrow d_{X_2}(\phi(x),\phi(x')) \le 1/2^n\big)$$

Définition 2.4.1 *(définition générale mais un peu informelle pour ce qu'est une fonction continue et ce qu'est sa complexité)* On considère deux espaces métriques complets X_1 et X_2 donnés dans des présentations rationnelles de classe $\mathcal{C}'$: (Y_1, δ_1, η_1) et (Y_2, δ_2, η_2). On suppose avoir spécifié un point y_0 de X_2.
Supposons que nous ayons défini une famille $F_{X_1} = (F_\alpha)_{\alpha\in M}$ de parties de X_1 avec la propriété suivante :
— (2.4.1.1) tout compact de X_1 est contenu dans un des F_α.
On dira qu'une fonction $\phi : X_1 \to X_2$ est F_{X_1}- *uniformément continue* si elle est bornée sur chaque partie F_α et si elle possède un module de continuité uniforme près de chaque partie F_α.
Supposons maintenant en plus que la famille $(F_\alpha)_{\alpha\in M}$ ait la propriété suivante :
— (2.4.1.2) l'ensemble d'indices M a une certaine "structure de calculabilité"
On dira qu'une fonction $\phi : X_1 \to X_2$ est F_{X_1}-*uniformément continue de classe $\mathcal{C}$* si elle vérifie

les propriétés suivantes :
— une borne sur chaque partie F_α peut être calculée en fonction de α dans la classe $\mathcal{C}$, c.-à-d. qu'on a une fonction de classe $\mathcal{C}$, $\beta : M \to \mathbb{N}_1$ vérifiant :

$$\forall \alpha \in M \; \forall x \in F_\alpha \;\; d_{X_2}(y_0, \phi(x)) \leq 2^{\beta(\alpha)}$$

— un module de continuité uniforme près de F_α peut être calculé dans la classe $\mathcal{C}$: une fonction $\mu : M \times \mathbb{N}_1 \to \mathbb{N}_1$ dans la classe $\mathcal{C}$ vérifiant :

$$\forall \alpha \in M \; \forall x \in F_\alpha \quad \big(d_{X_1}(x, x') \leq 1/2^{\mu(\alpha,n)} \Rightarrow d_{X_2}(\phi(x), \phi(x')) \leq 1/2^n\big)$$

— la restriction de ϕ à Y_1 est calculable dans la classe $\mathcal{C}$.

Il s'agit manifestement d'une extension des deux définitions précédentes. Le caractère informel de la définition tient évidemment à "la structure de calculabilité" de M.
A priori on voudrait prendre pour $(F_\alpha)_{\alpha \in M}$ une famille de parties suffisamment simple pour vérifier la condition (2.4.1.2) et suffisamment grande pour vérifier la condition (2.4.1.1).
Mais ces deux conditions tirent dans deux sens opposés.
Notez que la définition 2.4.1 est inspirée de la notion de fonction continue définie par D. Bridges en analyse constructive ([8]).

2.5 Ouverts et fermés

Nous passons à la définition d'une structure de calculabilité pour un sous-espace ouvert U d'un espace métrique X muni d'une structure de calculabilité. La métrique induite par X sur U ne saurait en général nous satisfaire car l'espace obtenu n'est généralement pas complet. On a néanmoins une construction qui fonctionne dans un cas particulier important.
Soient X un espace métrique complet et $f : X \to \mathbb{R}$ une fonction localement uniformément continue. L'ouvert $U_f = \{x \in X : f(x) > 0\}$ est un espace métrique complet pour la distance d_f définie par :

$$d_f(x, y) = d_X(x, y) + \mid 1/f(x) - 1/f(y) \mid$$

Proposition et définition 2.5.1 *Soient X un espace métrique complet donné avec une $\mathcal{C}$-présentation (Y, δ, η), et $f : X \to \mathbb{R}$ une fonction localement uniformément de classe $\mathcal{C}$ représentée par un module de continuité uniforme et une fonction discrète de classe $\mathcal{C}$, $\varphi : Y \times \mathbb{N}_1 \to \mathbb{D}$. Alors l'espace métrique complet (U_f, d_f) peut être muni d'une $\mathcal{C}$-présentation où l'ensemble des points rationnels est (codé par) l'ensemble Y_U des couples (y, n) de $Y \times \mathbb{N}_1$ vérifiant :*

$$n \geq 10 \;\text{ et }\; \varphi(y, n) \geq 1/2^{n/8}$$

Preuve. Une preuve détaillée est donnée dans [25]. ∎

Nous attaquons maintenant la définition d'une structure de calculabilité pour un sous-espace fermé F d'un espace métrique X muni d'une structure de calculabilité. En analyse constructive, un sous-ensemble fermé n'est vraiment utile que lorsqu'il est situé, c.-à-d. lorsque la fonction D_F "distance au fermé" est calculable. Au moment de traduire cette notion en termes de calculabilité récursive ou de complexité, nous devons prendre garde que dans la définition constructive, le fait que la fonction D_F est la fonction "distance au fermé" doit être aussi rendu explicite.

Définition 2.5.2 On considère un espace métrique complet X donné par une $\mathcal{C}$-présentation (Y, δ, η). Une partie F de X est appelée *un fermé $\mathcal{C}$-situé de X* si :

i) La fonction $DF : x \mapsto d_X(x, F)$ de X vers $\mathbb{R}^{\geq 0}$ est calculable dans la classe $\mathcal{C}$.
ii) Il existe une fonction calculable dans la classe $\mathcal{C}$: $P_F : Y \times \mathbb{N}_1 \to X$ qui certifie la fonction D_F au sens suivant : pour tout $(y, n) \in Y \times \mathbb{N}_1$,

$$D_F(P_F(y, n)) = 0, \quad d_X(y, P_F(y, n)) \leq D_F(y) + 1/2^n$$

Remarques 2.5.3
1) La fonction $P_F(y, n)$ calcule un élément de F dont la distance à y est suffisamment proche de $D_F(y)$. Cependant, la fonction $P_F(y, n)$ ne définit pas en général, par prolongement par continuité à X et par passage à la limite lorsque n tend vers ∞, un projecteur sur le fermé F.
2) On peut montrer que les points $P_F(y, n)$ (codés par les couples $(y, n) \in Y \times \mathbb{N}_1$) forment une partie dénombrable dense de F qui est l'ensemble des points rationnels d'une $\mathcal{C}$-présentation de F (cf. [25]).

2.6 Espaces de Banach rationnellement présentés

Nous donnons une définition minimale. Il va de soi que pour chaque espace de Banach particulier, des notions de complexité naturellement attachées à l'espace considéré peuvent éventuellement être prises en compte en plus pour obtenir une notion vraiment raisonnable.

Définition 2.6.1 *(présentation rationnelle d'un espace de Banach)* Une présentation rationnelle d'un espace de Banach séparable X sur le corps $\mathbb{K}$ ($\mathbb{R}$ ou $\mathbb{C}$) sera dite de classe $\mathcal{C}$ si, d'une part elle est de classe $\mathcal{C}$ en tant que présentation de l'espace métrique et, d'autre part les opérations d'espace vectoriel suivantes sont dans la classe $\mathcal{C}$
— le produit par un scalaire,
— la somme d'une liste de vecteurs choisis parmi les points rationnels.

Dans le contexte du corps des complexes $\mathbb{C}$ nous désignerons par $\mathbb{D}_{\mathbb{K}}$ l'ensemble des complexes dont les parties réelle et imaginaire sont dans $\mathbb{D}$. Dans le contexte réel $\mathbb{D}_{\mathbb{K}}$ sera seulement une autre dénomination de $\mathbb{D}$.
La proposition suivante n'est pas difficile à établir.

Proposition 2.6.2 *Donner une présentation rationnelle de classe $\mathcal{C}$ d'un espace de Banach X au sens de la définition ci-dessus revient à donner :*
— un codage de complexité $\mathcal{C}$ pour une partie dénombrable G de X qui engendre X en tant qu'espace de Banach[7]
— une application ν : $\mathbf{lst}(\mathbb{D}_{\mathbb{K}} \times G) \times \mathbb{N}_1 \to \mathbb{D}$ qui est dans la classe $\mathcal{C}$ (pour le codage de G considéré) et qui "calcule la norme d'une combinaison linéaire d'éléments de G" au sens suivant :
pour tout $([(x_1, g_1), (x_2, g_2), \ldots, (x_n, g_n)], m)$ dans $\mathbf{lst}(\mathbb{D}_{\mathbb{K}} \times G) \times \mathbb{N}_1$, on a la majoration

$$| \nu([(x_1, g_1), (x_2, g_2), \ldots, (x_n, g_n)], m) - \| x_1.g_1 + x_2.g_2 + \cdots + x_n.g_n \|_X | \leq 1/2^n$$

Remarques 2.6.3
1) Comme pour la définition 2.1.1 (cf. remarque 2.1.2 (3)), il se peut que le certificat d'inclusion de G dans X implique une notion de complexité, qu'il sera inévitable de prendre en compte dans une définition plus précise, au cas par cas.
2) Les espaces $L^p(\mathbb{R})$ de l'analyse fonctionnelle, avec $1 \leq p < \infty$ peuvent être rationnellement présentés de différentes manières, selon différents choix possibles pour l'ensemble des "points

[7] On peut supposer que tous les éléments de G sont des vecteurs de norme comprise entre $1/2$ et 1.

rationnels" et un codage de cet ensemble. Tous les choix raisonnables s'avèrent donner des présentations **Prim**-équivalentes.
3) Il serait intéressant de savoir si le cadre de travail proposé par M. Pour El et I. Richards [31] concernant la calculabilité dans les espaces de Banach peut avoir des conséquences concrètes qui iraient au delà de ce qui peut être traité par les présentations rationnelles (lesquelles offrent un cadre naturel non seulement pour les problèmes de récursivité mais aussi pour les problèmes de complexité). Le "contre-exemple" concernant L^∞ donné dans [31] incite à penser le contraire.

3 Espace des fonctions réelles continues sur un intervalle compact : premières propriétés

Dans cette section, nous introduisons le problème des présentations rationnelles pour l'espace $\mathbf{C}[0,1]$: l'espace des fonctions réelles uniformément continues sur l'intervalle [0,1], muni de la norme usuelle :

$$\| f \|_\infty = \mathbf{Sup}\{| f(x) | ; 0 \leq x \leq 1\}.$$

Considérons une présentation rationnelle de l'espace $\mathbf{C}[0,1]$ donnée par une famille $(\widetilde{f})_{f\in Y}$ de fonctions uniformément continues indexée par une partie Y d'un langage $A^\star$. Nous sommes intéressés par les problèmes de complexité suivants :
— la complexité de l'ensemble des (codes des) points rationnels de la présentation, c.-à-d. plus précisément la complexité de Y en tant que partie du langage $A^\star$ (c.-à-d. la complexité du test d'appartenance).
— la complexité des opérations d'espace vectoriel (le produit par un scalaire d'une part, la somme d'une liste de vecteurs d'autre part).
— la complexité du calcul de la norme (ou de la fonction distance).
— la complexité de l'ensemble $(\widetilde{f})_{f\in Y}$ des points rationnels de la présentation, en tant que famille de fonctions uniformément continues sur $[0,1]$.
— la complexité de la fonction d'évaluation $\mathbf{E} : \mathbf{C}[0,1] \times [0,1] \to \mathbb{R} : (g,x) \mapsto g(x)$.
Il va de soi que l'on peut remplacer l'intervalle $[0,1]$ par un autre intervalle $[a,b]$ avec a et b dans $\mathbb{D}$ ou de faible complexité dans $\mathbb{R}$.

3.1 La définition d'une présentation rationnelle de l'espace des fonctions continues

La complexité de l'ensemble $(\widetilde{f})_{f\in Y}$ des points rationnels de la présentation, en tant que famille de fonctions uniformément continues sur $[0,1]$ n'est rien d'autre que la complexité de l'application $f \mapsto \widetilde{f}$ de l'ensemble des codes de points rationnels Y vers l'espace $\mathbf{C}[0,1]$. Nous devons donc, conformément à ce que nous disions dans la remarque 2.1.2(3), inclure dans la définition de ce qu'est une présentation rationnelle de classe $\mathcal{C}$ de $\mathbf{C}[0,1]$, le fait que $(\widetilde{f})_{f\in Y}$ est une famille uniformément de classe $\mathcal{C}$ au sens de la définition 2.2.9. Le problème de la complexité de la fonction d'évaluation est également un problème important car il serait "immoral" que la fonction d'évaluation ne soit pas une fonction de classe $\mathcal{C}$ lorsqu'on a une présentation rationnelle de classe $\mathcal{C}$. Cependant, la fonction d'évaluation n'est pas uniformément continue, ni même localement uniformément continue.
Pour traiter en général la question des fonctions continues mais non localement uniformément continues sur l'espace $\mathbf{C}[0,1]$ nous faisons appel à la définition informelle 2.4.1 avec la famille suivante de parties de $\mathbf{C}[0,1]$:

Notation 3.1.1 Si α est une fonction croissante de $\mathbb{N}_1$ vers $\mathbb{N}_1$ et $r \in \mathbb{N}_1$, on note $F_{\alpha,r}$ la partie de $\mathbf{C}[0,1]$ formée par toutes les fonctions qui, d'une part acceptent α comme module de continuité uniforme, et d'autre part ont leur norme majorée par 2^r.

La "structure de calculabilité" sur l'ensemble d'indices

$$M := \{(\alpha, r); \alpha \text{ est une fonction croissante de } \mathbb{N}_1 \text{ vers } \mathbb{N}_1 \text{ et r} \in \mathbb{N}_1\}$$

n'est pas une chose bien définie dans la littérature, mais nous n'aurons besoin de faire appel qu'à des opérations parfaitement élémentaires comme "évaluer α en un entier n"[8]. Le module de continuité de la fonction d'évaluation est alors "très simple" (uniformément linéaire pour toute définition raisonnable de cette notion).
En effet, près de la partie $F_{\alpha,r} \times [0,1]$ de $\mathbf{C}[0,1] \times [0,1]$ un module de continuité de la fonction $\mathbf{E}$ est donné par :

$$\mu(n, \alpha, r) = \max(\alpha(n+1), n+1) \text{ pour n} \in \mathbb{N}_1 \text{ et } (\alpha, \text{r}) \in \text{M}$$

comme il est très facile de le vérifier. Et la borne sur $F_{\alpha,r}$ est évidemment donnée par $\beta(\alpha, r) = r$.
Toute la question de la complexité de la fonction d'évaluation dans une présentation donnée est donc concentrée sur la question de la complexité de la fonction d'évaluation restreinte à l'ensemble des points rationnels

$$(f, x) \mapsto \widetilde{f}(x) : Y \times \mathbb{D}_{[0,1]} \to \mathbb{R}.$$

Or cette complexité est subordonnée à celle de $(\widetilde{f})_{f \in Y}$ en tant que famille de fonctions uniformément continues : c'est ce que nous précisons dans la proposition suivante (dont la preuve est immédiate).

Proposition 3.1.2 *Considérons sur l'espace* $\mathbf{C}[0,1]$ *la famille de parties* $(F_{\alpha,r})_{(\alpha,r)\in M}$ *pour contrôler les questions de continuité sur* $\mathbf{C}[0,1]$ *(cf. notation 3.1.1 et définition 2.4.1).*
Alors si $(\widetilde{f})_{f \in Y}$ *est une famille uniformément de classe* $\mathcal{C}$ *et si on considère la présentation rationnelle de l'espace métrique* $\mathbf{C}[0,1]$ *attachée à cette famille considérée comme ensemble des points rationnels de la présentation, la fonction d'évaluation*

$$\mathbf{E} : \mathbf{C}[0,1] \times [0,1] \to \mathbb{R} : (g, x) \mapsto g(x)$$

est elle même de classe $\mathcal{C}$.

Comme en outre nous demandons que la structure d'espace de Banach soit elle même de classe $\mathcal{C}$, cela nous donne finalement la définition suivante.

Définition 3.1.3 Une présentation rationnelle de classe $\mathcal{C}$ de l'espace $\mathbf{C}[0,1]$ est donnée par une famille de fonctions $(\widetilde{f})_{f \in Y}$ qui est une famille uniformément de classe $\mathcal{C}$, dense dans $\mathbf{C}[0,1]$ et telle que soient également dans la classe $\mathcal{C}$ les calculs suivants :
— le produit par un scalaire,
— la somme d'une liste de fonctions choisies parmi les points rationnels,
— le calcul de la norme.

Dans toute la suite, nous nous intéresserons à une étude précise des complexités impliquées dans la définition 3.1.3. Notre conclusion est qu'il n'existe pas de paradis en temps polynomial des fonctions continues, du moins si $\mathcal{P} \neq \mathcal{NP}$.

[8] Notez que le théorème d'Ascoli classique affirme que toute partie compacte de $\mathbf{C}[0,1]$ est contenue dans une partie $F_{\alpha,r}$, et que les parties $F_{\alpha,r}$ sont compactes. En mathématiques constructives la partie directe est encore valable, mais la deuxième partie de l'énoncé doit être raffinée, cf [5] chap 4 théorème 4.8, pages 96 à 98.

3.2 Deux exemples significatifs de présentations rationnelles de l'espace $\mathbf{C}[0,1]$

Nous donnons maintenant deux exemples significatifs de présentations de $\mathbf{C}[0,1]$ (d'autres exemples seront donnés plus loin)

3.2.1 Présentation par circuits semilinéaires binaires

Cette présentation et l'ensemble des (codes des) "points rationnels" seront notés respectivement $\mathcal{C}_{\text{csl}}$ et $\mathbf{Y}_{csl}$. Nous appellerons *fonction semilinéaire à coefficients dans* $\mathbb{D}$ une fonction linéaire par morceaux qui est égale à une combinaison par max et min de fonctions $x \mapsto ax+b$ avec a et b dans $\mathbb{D}$.

Définition 3.2.1 Un *circuit semilinéaire binaire* est un circuit qui a pour portes d'entrée des variables "réelles" x_i (ici, une seule suffira parce que le circuit calcule une fonction d'une seule variable) et les deux constantes 0 et 1. Il y a une seule porte de sortie.
Les portes qui ne sont pas des portes d'entrée sont de l'un des types suivants :
— des portes à une entrée, des types suivants : $x \mapsto 2x$,$x \mapsto x/2$, $x \mapsto -x$
— des portes à deux entrées, des types suivants : $(x,y) \mapsto x+y$, $(x,y) \mapsto \max(x,y)$, $(x,y) \mapsto \min(x,y)$.
Un circuit semilinéaire binaire avec une seule variable d'entrée définit une fonction semilinéaire à coefficients dans $\mathbb{D}$. Un tel circuit peut être codé par un programme d'évaluation. L'ensemble $\mathbf{Y}_{csl}$ est l'ensemble des (codes de ces) circuits semilinéaires, c'est l'ensemble des points rationnels de la présentation $\mathcal{C}_{\text{csl}}$.

Nous verrons plus loin que cette présentation est en quelque sorte la plus naturelle, mais qu'elle manque d'être une présentation de classe $\mathcal{P}$ à cause du calcul de la norme.
On a une majoration facile d'un module de Lipschitz de la fonction définie par le circuit :

$$| \widetilde{f}(x) - \widetilde{f}(y) | \leq 2^p \mid x-y \mid \text{ où } p \text{ est la profondeur du circuit}$$

Ceci donne pour module de continuité uniforme $\mu(k) = k+n$. Ceci implique en particulier qu'on n'a pas besoin de se limiter à un intervalle fermé borné de $\mathbb{D}$ dans la proposition suivante.

Proposition 3.2.2 (Complexité de la famille de fonctions $(\widetilde{f})_{f\in\mathbf{Y}_{csl}}$)
La famille de fonctions $(\widetilde{f})_{f\in\mathbf{Y}_{csl}}$ *est uniformément de classe* $\mathcal{P}$. *Précisément, cette famille admet* $\mu(f,k) = k + \text{prof}(f)$ *pour module de continuité uniforme et on peut expliciter une fonction* $\varphi : \mathbf{Y}_{csl} \times \mathbb{D} \times \mathbb{N}_1 \to \mathbb{D}$ *de classe* $\mathbf{DRT}(Lin, \mathrm{O}(N^2))$ *(où* N *est la taille de l'entrée* (f,x,k)*) avec,*

$$\forall (f,x,k) \in \mathbf{Y}_{csl} \times \mathbb{D} \times \mathbb{N}_1 \mid \widetilde{f}(x) - \varphi(f,x,k) \mid \leq 1/2^k$$

Plus précisément encore, comme il n'est pas nécessaire de lire x *en entier, la taille de* x *n'intervient pas, et la fonction* φ *est dans les classes* $\mathbf{DRT}(Lin, \mathrm{O}(\mathrm{t}(f)(\text{prof}(f)+k)))$ *et* $\mathbf{DSPACE}(\mathrm{O}(\text{prof}(f)(\text{prof}(f)+k)))$ *où* $\mathrm{t}(f)$ *et* $\text{prof}(f)$ *sont respectivement la taille et la profondeur de* f.

Preuve. Pour calculer $\varphi(f,x,k)$ on évalue le circuit f sur l'entrée x dont on ne considère que les $k+2\text{prof}(f)$ premiers bits, en tronquant le résultat intermédiaire calculé à la porte π à la précision $k+2\text{prof}(f)-\text{prof}(\pi)$. Enfin, pour le résultat final on ne garde que la précision k.
Une telle méthode appliquée naïvement nécessite de garder stockés tous les résultats obtenus à une profondeur fixée p pendant qu'on calcule des résultats à la profondeur $p+1$. Nous faisons alors $\mathrm{t}(f)$ calculs élémentaires $(\bullet+\bullet, \bullet-\bullet, \bullet\times 2, \bullet/2, \max(\bullet,\bullet), \min(\bullet,\bullet))$ sur des objets de

taille $\leq k + 2\text{prof}(f)$. Chaque calcul élémentaire prend un temps $O(k + \text{prof}(f))$, et donc le calcul global se fait en temps $O(t(f)(\text{prof}(f)+k))$. Et cela prend aussi un $O(t(f)(\text{prof}(f)+k))$ comme espace de calcul.
Il existe une autre méthode d'évaluation d'un circuit, un peu moins économe en temps mais nettement plus économe en espace, suivant l'idée de Borodin [6]. Avec une telle méthode on économise l'espace de calcul qui devient un $O(\text{prof}(f)(\text{prof}(f)+k))$. ∎

Remarque 3.2.3 Nous n'avons pas pris en compte dans notre calcul le problème posé par la gestion de $t = t(f)$ objets (ici des nombres dyadiques) de tailles majorées par $s = \text{prof}(f) + k$. Dans le modèle RAM cette gestion serait a priori en temps $O(t\lg(t)s)$ ce qui n'augmente pas sensiblement le $O(ts)$ que nous avons trouvé, et ce qui reste en $O(N^2)$ si on se rappelle que le codage du circuit semilinéaire par un programme d'évaluation lui donne une taille de $O(t\lg(t))$. Dans le modèle des machines de Turing par contre, cette gestion réclame a priori un temps $O(t^2 s)$ car il faut parcourir t fois la bande où sont stockés les objets sur une longueur totale $\leq ts$. Nous avons donc commis une certaine sous estimation en nous concentrant sur le problème que nous considérons comme central : estimer le coût total des opérations arithmétiques proprement dites. Nous omettrons dans la suite systématiquement le calcul du *temps de gestion* des valeurs intermédiaires (très sensible au modèle de calcul choisi) chaque fois qu'il s'agira d'évaluer des circuits.

3.2.2 Présentation $\mathcal{C}_{\text{frac}}$ (via des fractions rationnelles contrôlées et données en présentation par formule)

La présentation précédente de l'espace $\mathbf{C}[0,1]$ n'est pas de classe $\mathcal{P}$ (sauf si $\mathcal{P} = \mathcal{NP}$ comme nous le verrons à la section 4.3) parce que la norme n'est pas calculable en temps polynomial. Pour obtenir une présentation de classe $\mathcal{P}$ il est nécessaire de restreindre assez considérablement l'ensemble des "points rationnels" de la présentation, de manière à ce que la norme devienne une fonction calculable en temps polynomial. Un exemple significatif est celui où les points rationnels sont des fractions rationnelles bien contrôlées et données dans une présentation du type dense. On a le choix entre plusieurs variantes et nous avons choisi de donner le dénominateur et le numérateur dans une présentation dite "par formules". Une formule est un arbre dont les feuilles sont étiquetées par la variable X ou par un élément de $\mathbb{D}$ et dont chaque noeud est étiqueté par un opérateur arithmétique. Dans les formules que nous considérons, les seuls opérateurs utilisés sont $\bullet + \bullet, \bullet - \bullet$ et $\bullet \times \bullet$, de sorte que l'arbre est un arbre binaire (chaque noeud de l'arbre est une sous formule et représente un polynôme de $\mathbb{D}[X]$.)

Lemme 3.2.4 *Désignons par $\mathbb{D}[X]_f$ l'ensemble des polynômes à coefficients dans $\mathbb{D}$, donnés en présentation par formule. Pour un polynôme à une variable et à coefficients dans $\mathbb{D}$ le passage de la représentation dense à la représentation par formule est* **LINTIME** *et le passage de la représentation par formule à la représentation dense est polynomial. Plus précisément si on procède de manière naïve on est en* $\mathbf{DTIME}(O(N^2\mathcal{M}(N)))$.

Preuve. Tout d'abord, la représentation dense peut être considérée comme un cas particulier de représentation par formule, selon le schéma de Horner.
Ensuite, passer de la représentation par formule à la représentation dense revient à évaluer la formule dans $\mathbb{D}[X]$. Introduisons les paramètres de controle suivants. Un polynome $P \in \mathbb{D}[X]$ a un degré noté d_P et la taille de ses coefficients est controlée par l'entier $\sigma(P) := log(\sum_i \mid a_i \mid)$ où les a_i sont les coefficients de P. Une formule $F \in \mathbb{D}[X]_f$ contient un nombre d'opérateurs arithmétiques noté t_F et la taille de ses coefficients est controlée par l'entier $\lambda(F) = \sum_i(\lg(b_i))$

où les b_i sont les dyadiques apparaissant dans la formule.
La taille $\perp F \perp$ de la formule F est évidemment un majorant de t_F et $\lambda(F)$.
Pour deux dyadiques a et b on a toujours $\lg(a \pm b) \leq \lg(a) + \lg(b)$ et $\lg(ab) \leq \lg(a) + \lg(b)$.
On vérifie alors facilement que $\sigma(P \pm Q) \leq \sigma(P) + \sigma(Q)$ et $\sigma(PQ) \leq \sigma(P) + \sigma(Q)$. Le temps de calcul (naïf) de PQ est un $\mathrm{O}(d_P d_Q \mathcal{M}(\sigma(P) + \sigma(Q)))$.
On montre ensuite par récurrence sur la taille de la formule F que le polynome correspondant $P \in \mathbb{D}[X]$ vérifie $d_P \leq t_F$ et $\sigma(P) \leq \lambda(F)$. On montre également par récurrence que le temps pour calculer P à partir de F est majoré par $t_F^2 \mathcal{M}(\lambda(F))$. ∎

Définition 3.2.5 L'ensemble $\mathbf{Y}_{frac} \subset \mathbb{D}[X]_f \times \mathbb{D}[X]_f$ est l'ensemble des fractions rationnelles (à une variable) à coefficients dans $\mathbb{D}$, dont le dénominateur est minoré par 1 sur l'intervalle $[0,1]$. L'espace $\mathbf{C}[0,1]$ muni de l'ensemble $\mathbf{Y}_{frac}$ comme famille des (codes des) points rationnels est noté $\mathcal{C}_{\mathrm{frac}}$

Proposition 3.2.6 (Complexité de la famille de fonctions $(\widetilde{f})_{f \in \mathbf{Y}_{frac}}$)
La famille de fonctions $(\widetilde{f})_{f \in \mathbf{Y}_{frac}}$ est uniformément de classe $\mathcal{P}$, plus précisément de classe $\mathbf{DRT}(Lin, \mathrm{O}(\mathcal{M}(N)N))$, où $\mathcal{M}(N)$ est la complexité de la multiplication de deux entiers de taille N.

Preuve. Nous devons calculer un module de continuité uniforme pour la famille $(\widetilde{f})_{f \in \mathbf{Y}_{frac}}$. Nous devons aussi expliciter une fonction φ de classe $\mathbf{DRT}(Lin, \mathrm{O}(\mathcal{M}(N)N))$

$$\varphi : \mathbf{Y}_{frac} \times \mathbb{D}_{[0,1]} \times \mathbb{N}_1 \to \mathbb{D} \ , \ (f, x, n) \mapsto \varphi(f, x, n)$$

vérifiant
$\mid \widetilde{f}(x) - \varphi(f, x, n) \mid \leq 1/2^n$. En fait, le module de continuité uniforme va se déduire du calcul de φ.
Puisque le dénominateur de la fraction est minoré par 1, il nous suffit de donner un module de continuité uniforme et une procédure de calcul en temps $\mathrm{O}(\mathcal{M}(N)N)$ pour évaluer une formule $F \in \mathbb{D}[X]_f$ avec une précision $1/2^n$ sur l'intervalle $[0,1]$ ($N = n + \perp F \perp$). Nous supposons sans perte de généralité que la taille $m = \perp F \perp$ de la formule $F = F_1 * F_2$ est égale à $m_1 + m_2 + 2$ si $m_1 = \perp F_1 \perp$ et $m_2 = \perp F_2 \perp$ ($*$ désigne un des opérateurs $+$, $-$ $ou \times$). On établit alors (par récurrence sur la profondeur de la formule) les deux faits suivants :
— lorsqu'on évalue de manière exacte la formule $F \in \mathbb{D}[X]_f$ en un $x \in [0,1]$ le résultat est toujours majoré en valeur absolue par 2^m.
— lorsqu'on évalue la formule F en un $x \in [0,1]$ de manière approchée, en prenant x et tous les résultats intermédiares avec une précision (absolue) $1/2^{n+m}$ le résultat final est garanti avec la précision $1/2^n$.
On conclut ensuite sans difficulté. ∎

Proposition 3.2.7 *a) La famille de nombres réels $(\| \widetilde{f} \|)_{f \in \mathbf{Y}_{frac}}$ est de complexité $\mathcal{P}$.*
b) Le test d'appartenance $f \in \mathbf{Y}_{frac}$? est de complexité $\mathcal{P}$.

Preuve. a) Soit $f = P/Q \in \mathbf{Y}_{frac}$. Pour calculer une valeur approchée à $1/2^n$ de la norme de $\widetilde{f}$, on procède comme suit :
— calculer $(P'Q - Q'P)$ en tant qu'élément de $\mathbb{D}[X]$ (lemme 3.2.4)
— calculer m : la précision requise sur x pour pouvoir évaluer $\widetilde{f}(x)$ avec la précision $1/2^n$ (proposition 3.2.6)
— calculer les racines $(\alpha_i)_{1 \leq i \leq n})$ de $(P'Q - Q'P)$ sur $[0,1]$ avec la précision 2^{-m}
— calculer $\max\{\widetilde{f}(0); \widetilde{f}(1); \widetilde{f}(\alpha_i)\ 1 \leq i \leq s\}$ avec la précision $1/2^n$ (proposition 3.2.6)
b) Le code f contient les codes de P et Q. Il s'agit de voir qu'on peut tester en temps polynomial

que le dénominateur Q est minoré par 1 sur l'intervalle $[0,1]$. Ceci est un résultat classique concernant les calculs avec les nombres réels algébriques : il s'agit de comparer à 1 le inf des $Q(\alpha_i)$ avec $\alpha_i = 0, 1$ ou un zéro de Q' sur l'intervalle. ∎

Remarques 3.2.8
1) Il est bien connu que le calcul des racines réelles d'un polynome de $\mathbb{Z}[X]$ situées dans un intervalle rationnel donné est un calcul de classe $\mathcal{P}$. Peut-être la méthode la plus performante n'est pas celle que nous avons indiquée, mais une légère variante. En effet la recherche des racines complexes d'un polynome (pour une précision donnée) est aujourd'hui extrêmement rapide (cf. [29]). Plutôt que de chercher spécifiquement les zéros réels sur l'intervalle $[0,1]$ on pourrait donc chercher avec la précision 2^{-m} les zéros réels ou complexes $(\beta_j)_{1\leq j\leq t}$ suffisamment proches de l'intervalle $[0,1]$ (i.e. leur partie imaginaire est en valeur absolue $\leq 2^{-m}$ et leur partie réelle est sur $[0,1]$ à 2^{-m} près) et évaluer $\widetilde{f}$ en les $Re(\beta_j)$.
2) Comme cela résulte de la proposition 3.3.5 ci-dessous, toute fonction semilinéaire à coefficients dans $\mathbb{D}$ est un point de complexité $\mathcal{P}$ dans $\mathcal{C}_{\text{frac}}$. Le fait que la présentation $\mathcal{C}_{\text{csl}}$ ne soit pas de classe $\mathcal{P}$ (si $\mathcal{P} \neq \mathcal{NP}$, cf. section 4.3) implique par contre que la famille de fonctions $(\widetilde{f})_{f\in\mathbf{Y}_{csl}}$ n'est pas une famille de classe $\mathcal{P}$ dans $\mathcal{C}_{\text{frac}}$.
3) On montre facilement que les opérations d'espace vectoriel sont aussi en temps polynomial.

Les résultats précédents se résument en :

Théorème 3.2.9 *La présentation $\mathcal{C}_{\text{frac}}$ de $\mathbf{C}[0,1]$ est de classe $\mathcal{P}$.*

3.3 Le théorème d'approximation de Newman et sa complexité algorithmique

Le théorème de Newman est un théorème fondamental en théorie de l'approximation. L'énoncé ci-après est un cas particulier[9].

Théorème 3.3.1 (Théorème de Newman, [28], voir par exemple [30] p. 73–75)
Soit n entier ≥ 6, définissons

$$H_n(x) = \prod_{1\leq k<n^2} (x + e^{-k/n}).$$

et considérons les deux polynômes $P_n(x)$ et $Q_n(x)$, de degrés majorés par $n^2/2$, donnés par

$$P_n(x^2) = x(H_n(x) - H_n(-x)) \text{ et } Q_n(x^2) = H_n(x) + H_n(-x)$$

Alors on a pour tout $x \in [-1,1]$

$$|\,|\,x\,| - (P_n/Q_n)(x^2)\,| \leq 3e^{-n} \leq 2^{-(n+1)}$$

et

$$|\,Q_n(x^2)\,| \geq 2H_n(0) = 2/e^{(n^3-n)/2} \geq 1/2^{3(n^3-n)/4}$$

Du théorème de Newman découle que les fonctions semilinéaires se laissent individuellement bien approcher par des fractions rationnelles "faciles à écrire et bien contrôlées". C'est ce que précisent le lemme 3.3.3 ci-après et ses corollaires, les propositions et théorèmes qui suivent. Nous rappelons d'abord le résultat suivant. (cf. [7])

[9] Nous avons pris le théorème "à l'ordre n^2" de manière à obtenir une majoration en e^{-n}.

Lemme 3.3.2 (théorème de Brent) *Soit $a \in [-1,1] \cap \mathbb{D}_m$. Le calcul de $\exp(a)$ avec la précision 2^{-m} peut être fait en temps $O(\mathcal{M}(m)\log(m))$.*
En d'autres termes, la fonction exponentielle sur l'intervalle $[-1,1]$ est de complexité $\mathbf{DTIME}(O(\mathcal{M}(m)\log(m)))$

On en déduit facilement, en notant $\mathbb{D}[X]_f$ la présentation de $\mathbb{D}[X]$ par formules.

Lemme 3.3.3 *Il existe une suite $\mathbb{N}_1 \to \mathbb{D}[X]_f \times \mathbb{D}[X]_f \ ; \ n \mapsto (u_n, v_n)$, de classe $\mathbf{DRT}(O(n^5), O(\mathcal{M}(n^3)n^2lg^3(n)))$, telle que pour tout $x \in [0,1]$*

$$| \, | \, x \, | - p_n(x^2)/q_n(x^2) \, | \leq 2^{-n}$$

Les degrés des polynômes p_n et q_n sont majorés par $n^2/2$, leurs tailles, en présentation par formule sont majorées par un $O(n^5)$, et $q_n(x^2)$ est minoré par $1/e^{(n^3-n)}$.

Preuve. On définit p_n et q_n comme P_n et Q_n en remplaçant dans la définition le réel $e^{-k/n}$ par une approximation dyadique $c_{n,k}$ suffisante calculée au moyen du lemme 3.3.2.
Si $| \, e^{-k/n} - c_{n,k} \, | \leq \varepsilon$ on vérifie que pour tout $x \in [0,1]$

$$| \, P_n(x) - p_n(x) \, | \leq (n^2-1)2^{n^2}\varepsilon \quad \text{et} \quad | \, Q_n(x) - q_n(x) \, | \leq (n^2-1)2^{n^2}\varepsilon = \varepsilon_1$$

Pour l'écart entre les fractions rationnelles on utilise

$$| \, A/B - a/b \, | \leq | \, A/B \, | \, | \, b - B \, | \, /b + \, | \, A - a \, | \, /b \leq 3\varepsilon_1/b$$

Comme $B \geq 1/2^{3(n^3-n)/4}$ on a $1/b \leq 2.2^{3(n^3-n)/4}$si $| \, b - B \, | \leq B/2$, en particulier si

$$(n^2-1)2^{n^2}\varepsilon \leq (1/2) \cdot 1/2^{3(n^3-n)/4}$$

On est alors conduit à prendre un ε tel que

$$3\varepsilon_1/b \leq 6(n^2-1)2^{n^2}2^{3(n^3-n)/4}\varepsilon \leq 1/2^{n+1}$$

Il suffit donc de prendre $\varepsilon \leq 2^{-n^3}$ (pour n assez grand).
On va donc être amené à décrire p_n et q_n par des formules de taille algébrique $O(n^2)$ portant sur des termes de base $(x + c_{n,k})$ où $c_{n,k}$ est un dyadique de taille $O(n^3)$. La taille (booléenne) de la formule est donc un $O(n^5)$. L'essentiel du temps de calcul est absorbé par le calcul des $c_{n,k}$ en utilisant le lemme 3.3.2. ∎

Notez que la majoration du temps de calcul est à peine moins bonne que la taille du résultat.
On en déduit immédiatement les résultats suivants.

Théorème 3.3.4 *La fonction $x \mapsto | \, x - 1/2 \, |$ est un point de complexité $\mathcal{P}$ (plus précisément $\mathbf{DRT}(O(n^5), O(\mathcal{M}(n^3)n^2lg^3(n)))$ dans l'espace $\mathcal{C}_{\text{frac}}$. En d'autres termes, il existe une suite $\mathbb{N}_1 \to \mathbf{Y}_{frac} \ , \ n \mapsto (u_n, v_n)$, de classe $\mathbf{DRT}(O(n^5), O(\mathcal{M}(n^3)n^2lg^3(n)))$, telle que*

$$\| \, | \, x - 1/2 \, | - u_n(x)/v_n(x) \, \| \leq 2^{-n}$$

Les degrés des polynômes u_n et v_n sont majorés par n^2.

Proposition 3.3.5 *La fonction $x \mapsto | \, x \, |$ sur l'intervalle $[-2^m, 2^m]$ peut être approchée à $1/2^n$ près par une fraction rationnelle $p_{n,m}/q_{n,m}$ dont le dénominateur est minoré par 1 (sur le même intervalle), et le calcul*

$$(n,m) \mapsto (p_{n,m}, q_{n,m}) \ \ \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{D}[X]_f \times \mathbb{D}[X]_f$$

est de complexité $\mathbf{DRT}(O(N^5), O(\mathcal{M}(N^3)N^2lg^3(N)))$ où $N = n+m$. Les degrés des polynômes $p_{n,m}$ et $q_{n,m}$ sont majorés par N^2. De même la fonction $(x,y) \mapsto \max(x,y)$ (resp. $(x,y) \mapsto \min(x,y)$) sur le carré $[-2^m, 2^m] \times [-2^m, 2^m]$ peut être approchée à $1/2^n$ près par une fraction rationnelle du même type et de même complexité que les précédentes.

Preuve. Pour la fonction valeur absolue :
Si $x \in [-2^m, 2^m]$ on écrit

$$\mid x \mid = 2^m \mid x/2^m \mid$$

avec $x/2^m \in [-1, 1]$. Donc, avec les notations de la preuve du lemme 3.3.3, il suffit de prendre $p_{n,m}(x) = 2^m p_{n+m}(x/2^m)$ et $q_{n,m}(x) = 2^m q_{n+m}(x/2^m)$.
Pour les fonctions max et min, il suffit d'utiliser les formules :

$$\max(x, y) = \frac{x + y + \mid x - y \mid}{2} \quad \text{et} \quad \min(x, y) = \frac{x + y - \mid x - y \mid}{2}$$

∎

Dans la suite, on aura besoin d'"approcher" la fonction discontinue

$$C_a(x) = \begin{cases} 1, & \text{si } x \geq a \\ 0, & \text{sinon} \end{cases}$$

Une telle "approximation" est donnée par la fonction semilinéaire continue $C_{p,a}$:

$$C_{p,a} = \min(1, \max(0, 2^p(x - a))) \text{ où p} \in \mathbb{N}_1 \text{ et a} \in \mathbb{D}_{[0,1]}$$

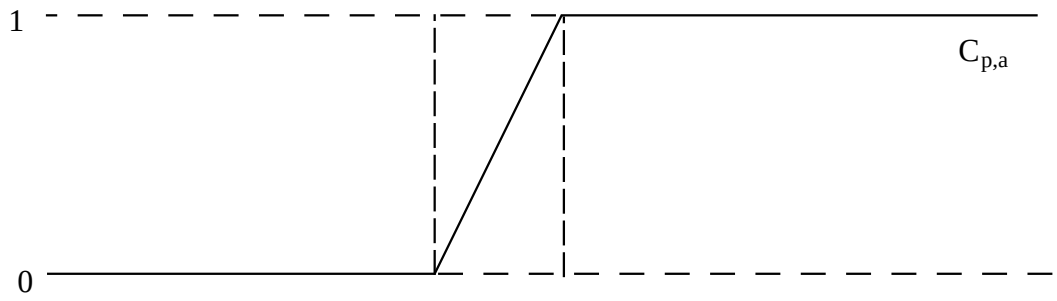

FIG. 1: courbe représentative de la fonction $C_{p,a}$

La complexité de la famille de fonctions $(p, a) \mapsto C_{p,a}$ est donnée dans la proposition suivante.

Proposition 3.3.6 *La famille de fonctions*

$$\mathbb{N}_1 \times \mathbb{D}_{[0,1]} \quad (p, a) \mapsto C_{p,a}$$

définie par :

$$C_{p,a} = min(1, max(0, 2^p(x - a)))$$

est une famille de classe $\mathcal{P}$. Plus précisément, elle est de complexité $\mathbf{DRT}(\mathrm{O}(N^5), \mathrm{O}(\mathcal{M}(N^3)N^2 lg^3(N)))$ *où* $N = max(\lg(a), n + p)$.

La proposition suivante concerne la fonction racine carrée.

Proposition 3.3.7 *La fonction $x \mapsto \sqrt{\mid x - 1/2 \mid}$ sur $[0, 1]$ est un $\mathcal{P}$-point de $\mathcal{C}_{\text{frac}}$.*

Preuve. (esquisse) Dans les polynômes $P_n(x^2)$ et $Q_n(x^2)$ du théorème de Newman, si on remplace x^2 par une bonne approximation de $\mid x \mid$ sur $[0, 1]$ obtenue elle même par le théorème de Newman, on obtiendra une fraction rationnelle $R_n(x)/S_n(x)$ telle que,

$$\forall x \in [0, 1] \mid \sqrt{\mid x \mid} - (R_n/S_n)(x) \mid \leq 2^{-n}$$

Les degrés de $R_n(x)$ et $S_n(x)$ seront en $\mathrm{O}(n^4)$.
Notez que la fraction $(P_n/Q_n)(x)$ n'est pas impaire, elle fournit donc une bonne approximation de la fonction $\sqrt{\mid x \mid}$ uniquement sur l'intervalle $[0, 1]$. ∎

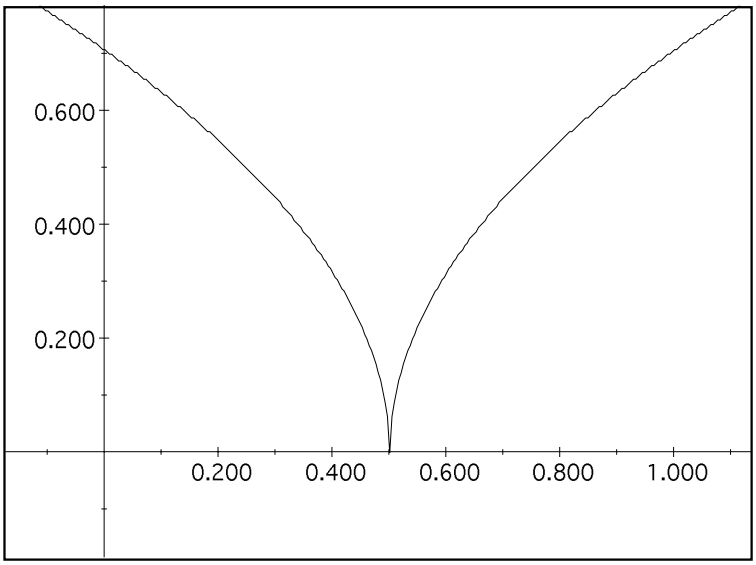

FIG. 2: courbe de la fonction $x \mapsto \sqrt{|\, x - 1/2 \,|}$

4 Une présentation naturelle de l'espace $\mathbf{C}[0,1]$ et quelques présentations équivalentes

Une notion naturelle de complexité pour les "points" et pour les "suites de points" de l'espace $\mathbf{C}[0,1]$ est donnée par K. I Ko et H. Friedman dans [15]. Nous étudions dans cette section une présentation rationnelle de l'espace $\mathbf{C}[0,1]$ qui donne (à très peu près) les mêmes notions de complexité. Nous étudions également d'autres présentations utilisant des circuits, qui s'avèrent équivalentes du point de vue de la complexité $\mathcal{P}$. La preuve de ces équivalences est basée sur la preuve d'un résultat analogue mais moins général donnée par [12, 13].

4.1 Définitions de quelques présentations de l'espace $\mathbf{C}[0,1]$

4.1.1 Presentation KF (KF comme Ko-Friedman)

Rappelons qu'on note $\mathbb{D}_n = \{k/2^n; k \in \mathbb{Z}\}$ et $\mathbb{D}_{n,[0,1]} = \mathbb{D}_n \cap [0,1]$.
Dans la définition donnée par Ko et Friedman, on considère, pour $f \in \mathbf{C}[0,1]$, une machine de Turing à Oracle (MTO) qui "calcule" la fonction f au sens suivant. L'oracle délivre, pour la question "m ? " une approximation $\xi \in \mathbb{D}_{m,[0,1]}$ de x avec la précision 2^{-m}. Pour l'entrée $n \in \mathbb{N}_1$, la machine calcule, en utilisant l'oracle, une approximation $\zeta \in \mathbb{D}_n$ de $f(x)$ à $1/2^n$ près.
La seule lecture du programme de la MTO ne permet évidemment pas de savoir si la MTO calcule bien une fonction de $\mathbf{C}[0,1]$. En conséquence, puisque nous souhaitons avoir des objets clairement identifiés comme "points rationnels" de la présentation que nous voulons définir, nous prenons le parti d'introduire des paramètres de contrôle. Mais pour que de tels paramètres soient vraiment efficaces, il est nécessaire de limiter l'exécution de la machine à une précision de sortie donnée a priori. En conséquence la précision nécessaire en entrée est également limitée a priori. Ainsi, la MTO est approximée par une suite de machines de Turing ordinaires (sans oracle) n'exécutant chacune qu'un nombre fini de calculs. Nous sommes donc conduits à définir une présentation rationnelle de $\mathbf{C}[0,1]$ qui sera notée $\mathcal{C}_{\mathrm{KF}}$ (l'ensemble des "points rationnels" sera noté $\mathbf{Y}_{KF}$) de la manière suivante.

Définition 4.1.1 On considère un langage, choisi une fois pour toutes, pour décrire les programmes de machines de Turing avec une seule entrée, dans $\mathbb{D}_{[0,1]}$ (notée x), et avec une seule sortie, dans $\mathbb{D}$ (notée y). Soit **Prog** la partie de ce langage formée par les programmes bien écrits (conformément à une syntaxe précisée une fois pour toutes). Soit $f = (Pr, n, m, T) \in \mathbf{Prog} \times \mathbb{N}_1 \times \mathbb{N}_1 \times \mathbb{N}_1$ où on a :
— n est la précision réclamée pour y
— m est la précision avec laquelle est donnée x
Le quadruplet (Pr, n, m, T) est dit *correct* lorsque sont vérifiées les conditions suivantes :
— le programme Pr calcule une fonction de $\mathbb{D}_{m,[0,1]}$ vers $\mathbb{D}_n$, c.-à-d. pour une entrée dans $\mathbb{D}_{m,[0,1]}$ on obtient en sortie un élément de $\mathbb{D}_n$.
— T majore le temps d'exécution maximum pour tous les x de $\mathbb{D}_{m,[0,1]}$
— pour deux éléments consécutifs (distants de $1/2^m$) de $\mathbb{D}_{m,[0,1]}$ en entrée, le programme donne en sortie deux éléments de $\mathbb{D}_n$ distants d'au plus $1/2^n$.
L'ensemble des quadruplets (Pr, n, m, T) corrects est noté $\mathbf{Y}_{KF}$. Lorsque la donnée f est correcte, elle définit le "point rationnel" $\widetilde{f}$ suivant : c'est la fonction linéaire par morceaux qui joint les points du graphe donnés sur la grille $\mathbb{D}_{m,[0,1]} \times \mathbb{D}_n$ par l'exécution du programme Pr pour toutes les entrées possibles dans $\mathbb{D}_{m,[0,1]}$.

Remarque 4.1.2 On notera que les deux premières conditions pourraient être réalisées de manière automatique par des contraintes de type syntaxique faciles à mettre en oeuvre. Par contre, comme on le verra dans la proposition 4.4.1, la troisième est incontrôlable en temps polynomial (sauf si $\mathcal{P} = \mathcal{NP}$) (cette condition de correction définit un problème $\mathcal{CO}$–$\mathcal{NP}$-complet). Notez aussi que si on n'avait pas imposé la condition de correction pour les points de $\mathbf{Y}_{KF}$ on n'aurait eu aucun contrôle a priori du module de continuité uniforme pour la fonction linéaire par morceaux définie par une donnée, et la famille $(\widetilde{f})_{f \in \mathbf{Y}_{KF}}$ n'aurait pas été uniformément de classe $\mathcal{P}$.

Proposition 4.1.3 *(Complexité de la famille de fonctions attachées à* $\mathbf{Y}_{KF}$*) La famille de fonctions continues* $(\widetilde{f})_{f \in \mathbf{Y}_{KF}}$ *est uniformément de classe* $DRST(Lin, Lin, \mathrm{O}(N^2))$.

Preuve. Tout d'abord, on remarque que la fonction $\widetilde{f}$ correspondant à $f = (Pr, n, m, T)$ est linéaire par morceaux et que, puisque la donnée est correcte, la pente de chaque morceau est majorée en valeur absolue par 2^{m-n} ce qui donne le module de continuité uniforme $\mu(f, k) = k + m - n$ pour la famille $(\widetilde{f})_{f \in \mathbf{Y}_{KF}}$.
Nous devons exhiber une fonction $\varphi : \mathbf{Y}_{KF} \times \mathbb{D}_{[0,1]} \times \mathbb{N}_1 \to \mathbb{D}$ de complexité $\mathbf{DSRT}(Lin, Lin, N^2)$ telle que :

$$\forall (f, x, k) \in \mathbf{Y}_{KF} \times \mathbb{D}_{[0,1]} \times \mathbb{N}_1 \quad | \varphi(f, x, k) - \widetilde{f}(x) | \leq 2^{-k}$$

Soit $z = (f, x, k) = ((Pr, n, m, T), x, k) \in \mathbf{Y}_{KF} \times \mathbb{D}_{[0,1]} \times \mathbb{N}_1$. Nous supposerons sans perte de généralité que $k \geq n$ et que x est donné avec au moins m bits.
Par simple lecture de x on repère deux éléments consécutifs a et b de $\mathbb{D}_{m,[0,1]}$ tels que $a \leq x \leq b$ et on trouve le dyadique $r \in \mathbb{D}_{[0,1]}$ tel que $x = a + r/2^n$.
Notons $\varepsilon \in \{-1, 0, 1\}$ l'entier vérifiant $\widetilde{f}(a) = \widetilde{f}(b) + \varepsilon/2^n$.
Alors $\widetilde{f}(x) = \widetilde{f}(a) + \varepsilon r/2^n$. En outre $\widetilde{f}(a) = \mathbf{Exec}(Pr, a)$ est le résultat de l'exécution du programme Pr pour l'entrée a. Le calcul complet consiste donc essentiellement à :
— lire x (et en déduire a, b et r)
— calculer $\mathbf{Exec}(Pr, a)$ et $\mathbf{Exec}(Pr, b)$.
La complexité est donc majorée par la complexité de la Machine de Turing Universelle que nous utilisons pour exécuter le programme Pr. D'après le lemme 1.3.1 cela se fait en temps $\mathrm{O}(T(T + \perp Pr \perp))$ et en espace $\mathrm{O}(T + \perp Pr \perp)$. Et la taille de la sortie est majorée par T. ∎

Le fait que la présentation $\mathcal{C}_{\mathrm{KF}}$ qui résulte de la définition 4.1.1 soit appelée " présentation à la Ko-Friedman " est justifié par la proposition suivante.

Proposition 4.1.4 *Une fonction $f : [0,1] \to \mathbb{R}$ est calculable en temps polynomial au sens de Ko- Friedman si et seulement si elle est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{KF}}$. Plus précisément*
a) Si la fonction f est de complexité en temps $T(n)$ au sens de Ko-Friedman alors elle est un $\mathbf{DTIME}(T)$*-point de $\mathcal{C}_{\mathrm{KF}}$*
b) Si la fonction f est un $\mathbf{DTIME}(T)$*-point de $\mathcal{C}_{\mathrm{KF}}$ alors elle est de complexité en temps $T^2(n)$ au sens de Ko-Friedman.*

Nous prouverons d'abord une caractérisation de la complexité d'une fonction au sens de Ko-Friedman, pour une classe $\mathcal{C}$ de complexité en temps ou en espace élémentairement stable. Nous l'avons déjà affirmée sans preuve dans le premier exemple 2.2.3. Nous en donnons un énoncé plus précis ici.

Proposition 4.1.5 *Soit $\mathcal{C}$ une classe élémentairement stable de type* $\mathbf{DTIME}(\bullet)$ *ou* $\mathbf{DSPACE}(\bullet)$ *ou* $\mathbf{DSRT}(\bullet,\bullet,\bullet)$ *ou* $\mathbf{DRT}(\bullet,\bullet)$ *ou* $\mathbf{DSR}(\bullet,\bullet)$ *et soit une fonction continue $f : [0,1] \to \mathbb{R}$. Les propriétés suivantes sont équivalentes :*
1) la fonction f est calculable au sens de Ko-Friedman dans la classe $\mathcal{C}$
2) la fonction f est uniformément de classe $\mathcal{C}$.
NB *: Pour ce qui concerne la complexité d'une MTO, nous entendons ici que les questions posées à l'oracle doivent être comptées parmi les sorties de la machine. Autremant dit la taille des entiers m qui sont les questions à l'oracle doivent avoir la majoration requise pour la sortie dans les classes du type* $\mathbf{DSRT}(\bullet,\bullet,\bullet)$ *ou* $\mathbf{DRT}(\bullet,\bullet,\bullet)$ *ou* $\mathbf{DSR}(\bullet,\bullet,\bullet)$.

Preuve. (de la proposition 4.1.5) Rappelons qu'une fonction est uniformément de classe $\mathcal{C}$ (cf. définition 2.1.1) lorsque :
a) la fonction f possède un module de continuité uniforme dans la classe $\mathcal{C}$.
b) la famille $(f(a))_{a\in\mathbb{D}}$ est une $\mathcal{C}$-famille de nombres réels.
Soit tout d'abord $f \in \mathbf{C}[0,1]$ et M une MTO qui, pour toute entrée $n \in \mathbb{N}_1$ et tout $x \in [0,1]$ (donné comme oracle) calcule $f(x)$ à 2^{-n} près dans la classe $\mathcal{C}$. Si on remplace l'oracle, qui donne à la demande une approximation de x à 2^{-m} près dans $\mathbb{D}_m$, par la lecture d'un nombre dyadique a arbitraire, on obtient une machine de Turing usuelle qui calcule $(f(a))_{a\in\mathbb{D}}$ en tant que famille de nombres réels, ceci dans la classe $\mathcal{C}$.
Voyons la question du module de continuité uniforme. Sur l'entrée n (précision requise pour la sortie) et pour n'importe quel oracle pour n'importe quel $x \in [0,1]$, la MTO va calculer $y = f(x)$ à 2^{-n} près en interrogeant l'oracle pour certaines précisions m. Puisque $\mathcal{C}$ est une classe de complexité du type prévu, le plus grand des entiers m utilisés sur l'entrée n peut être majoré par $\mu(n)$ où $\mu : \mathbb{N}_1 \to \mathbb{N}_1$ est une fonction dans la classe $\mathcal{C}$[10] . C'est le module de continuité uniforme que nous cherchons.
Supposons maintenant que la fonction f soit uniformément de classe $\mathcal{C}$. Soit M la machine de Turing (sans oracle) qui calcule $(f(x))_{x\in\mathbb{D}}$ en tant que famille de nombres réels dans la classe $\mathcal{C}$. Soit M' une machine de Turing qui calcule un module de continuité uniforme $\mu : \mathbb{N}_1 \to \mathbb{N}_1$ dans la classe $\mathcal{C}$. La MTO à la Ko-Friedman est alors la suivante. Sur l'entrée n elle calcule $m = \mu(n+1)$ (en utilisant M'), elle interroge l'oracle avec la précision m, l'oracle donne un élément $a \in \mathbb{D}_m$. La MTO utilise alors M pour calculer $f(a)$ avec une approximation de $1/2^{n+1}$, qui, privée de son dernier bit, constitue la sortie de la MTO. ∎

[10] Par exemple pour une classe de complexité où on spécifie que les sorties sont de taille linéaire, la taille de m dépend linéairement de n (indépendamment de l'oracle) puisque m, en tant que question posée à l'oracle, est une des sorties.

La proposition 4.1.5 montre, par contraste, que la non parfaite adéquation obtenue dans la proposition 4.1.4 est seulement due à la difficulté de faire entrer exactement et à tout coup la notion de complexité d'une fonction uniformément continue (en tant que fonction) dans le moule de la notion de "complexité d'un point dans un espace métrique". Cette adéquation parfaite a lieu pour des classes comme $\mathcal{P}$, **Prim** ou **Rec** mais pas pour $\mathbf{DRT}(Lin, \mathrm{O}(n^k))$.
Enfin on pourra noter la grande similitude entre les preuves des propositions 4.1.5 et 4.1.4, avec une complication un peu plus grande pour cette dernière. **Preuve.** (de la proposition 4.1.4)
Soit tout d'abord $f \in \mathbf{C}[0,1]$ et M une MTO qui, pour toute entrée $n \in \mathbb{N}_1$ et tout $x \in [0,1]$ (donné comme oracle) calcule $f(x)$ à 2^{-n} près, en temps majoré par $T(n)$.
Considérons la suite $f_n = (Pr_n, n, T(n), T(n))_{n\in\mathbf{N}_1}$ où on a :
Pr_n est obtenu à partir du programme Pr de la machine M en remplaçant la réponse (x_m) de l'oracle à la question "m ?" par l'instruction "lire x avec la précision m"
La correction de la donnée f_n est claire. Soit $\widetilde{f_n}$ la fonction linéaire par morceaux correspondant à la donnée f_n. On a pour $\xi \in [0,1]$ et d une approximation de ξ à $1/2^{T(n)}$ près

$$\mathbf{Exec}(Pr_n, d) = \mathbf{Exec}(Pr, n, \text{Oracle pour } \xi) = \mathrm{M}^{\xi}(\mathrm{n})$$

et donc

$$\mid \widetilde{f_n}(\xi) - f(\xi) \mid \leq \mid f(d) - \mathbf{Exec}(Pr_n, \xi) \mid + \mid \widetilde{f_n}(d) - \mathbf{Exec}(Pr_n, \xi) \mid \leq 2^{-n} + 2^{-n} \leq 2^{-(n-1)}$$

Enfin la suite $n \mapsto f_{n+1}$ est de complexité $\mathbf{DTIME}(\mathrm{O}(n))$.
Réciproquement, supposons que $\parallel f_n - f \parallel \leq 2^{-n}$ avec $n \mapsto f_n$ de classe $\mathbf{DTIME}(T(n))$.
On a $f_n = (Pr_n, q(n), m(n), t(n))$. Considérons la MTO M qui, pour tout entier $n \in \mathbb{N}_1$ et tout $\xi \in [0,1]$, effectue les tâches suivantes :
— prendre l'élément $f_{n+1} = (Pr_{n+1}, q(n+1), m(n+1), t(n+1))$, de la suite, correspondant à $n+1$.
— poser à l'oracle la question $Q(n) = m(n+1) + n + 1 - q(n)$ (on obtient une approximation d de ξ à $2^{-Q(n)}$ prs).
— calculer $\widetilde{f_{n+}}(d)$ par interpolation linéaire (cf. proposition 4.1.3) : ceci est la sortie de la machine M.
On a alors

$$\mid \widetilde{f_n}(\xi) - M^{\xi}(n) \mid \leq \mid \widetilde{f_n}(\xi) - \widetilde{f}_{n+1}(\xi) \mid + \widetilde{f}_{n+1}(\xi) - \widetilde{f}_{n+1}(d) \mid \leq 2^{-(n+1)} + 2^{-(n+1)} = 2^{-n} \; \forall \, \xi \in [0,1]$$

donc

$$\parallel f - M^{\xi}(n) \parallel \leq \parallel f - \widetilde{f_n} \parallel + \parallel \widetilde{f_n} - M^{\xi}(n) \parallel \leq \; 2^{-n} + 2^{-n}$$

De plus la machine M est de complexité $\mathrm{O}(T^2(n))$ (cf. proposition 4.1.3). ∎

Dans le même style que la proposition 4.1.5, on obtient deux caractérisations naturelles, à $\mathcal{P}$-équivalence près, de la présentation rationnelle $\mathcal{C}_{\mathrm{KF}}$ de $\mathbf{C}[0,1]$

Proposition 4.1.6 *Soit $\mathcal{C}^\star$ une présentation rationnelle de l'espace $\mathbf{C}[0,1]$. Alors on a l'équivalence des deux assertions suivantes :*
1) la présentation $\mathcal{C}^\star$ est $\mathcal{P}$-équivalente à $\mathcal{C}_{\mathrm{KF}}$
2) une famille $(\widetilde{f})_{f\in Z}$ dans $\mathbf{C}[0,1]$ est uniformément de classe $\mathcal{P}$ si et seulement si elle est une $\mathcal{P}$-famille de points de $\mathcal{C}^\star$.

Preuve. Pour n'importe quelle classe élémentairement stable $\mathcal{C}$, deux présentations rationnelles d'un espace métrique arbitraire sont $\mathcal{C}$-équivalentes si et seulement si elles définissent les mêmes $\mathcal{C}$-familles de points (cf. remarque 2.2.8). Il suffit donc de vérifier que la présentation rationnelle $\mathcal{C}_{\mathrm{KF}}$ vérifie la condition (2). La preuve est identique à celle de la proposition 4.1.4.
∎

Théorème 4.1.7 *La présentation $\mathcal{C}_{\mathrm{KF}}$ est universelle pour l'évaluation au sens suivant. Si (Y,δ,η) est une présentation de $\mathbf{C}[0,1]$ pour laquelle la famille $(\widetilde{f})_{f\in Y}$ est uniformément de classe $\mathcal{P}$, et si on note $\mathcal{C}^\star$ l'espace $\mathbf{C}[0,1]$ muni de cette structure de calculabilité, alors la fonction $\mathrm{Id}_{\mathbf{C}}[0,1]$ de $\mathcal{C}^\star$ vers $\mathcal{C}_{\mathrm{KF}}$ est uniformément de classe $\mathcal{P}$. Le résultat se généralise à toute classe de complexité $\mathcal{C}$ élémentairement stable vérifiant la propriété suivante :*
si $F\in\mathcal{C}$ alors le temps de calcul de $F:\mathbb{N}_1\to\mathbb{N}_1$, $N\mapsto F(N)$, est majoré par une fonction de classe $\mathcal{C}$.

Preuve. Cela résulte de 4.1.6. Donnons néanmoins la preuve. Nous devons montrer que la famille $(\widetilde{f})_{f\in Y}$ est une famille de points de classe $\mathcal{P}$ pour la présentation $\mathcal{C}_{\mathrm{KF}}$. Puisque la famille $(\widetilde{f})_{f\in Y}$ est uniformément de classe $\mathcal{P}$, on a deux fonctions y et μ de classe $\mathcal{P}$:

$$\psi : Y\times\mathbb{D}_{[0,1]}\times\mathbb{N}_1\to\mathbb{D}\quad (f,d,n)\mapsto\psi(f,d,n)=\widetilde{f}(d)\text{ avec la précision }1/2^n$$

et

$$\mu : Y\times\mathbb{N}_1\to\mathbb{D},\qquad (f,n)\mapsto\mu(f,d,n)=m$$

où μ est un module de continuité uniforme pour la famille. Soit $S:\mathbb{N}_1\to\mathbb{N}_1$ une fonction de classe $\mathcal{P}$ qui donne une majoration du temps de calcul de ψ.
Considérons alors la fonction $\varphi : Y\times\mathbb{N}_1\to\mathbf{Y}_{KF}$ définie par :

$$\varphi(f,n)=(Pr(f,n),n,\mu(f,n),S(\perp f\perp+\mu(f,n)+n))$$

où $\perp f\perp$ est la taille de f et Pr est le programme calculant ψ à peine modifié : il prend en entrée seulement les $d\in\mathbb{D}_{m,[0,1]}$ et ne garde pour la sortie que les chiffres significatifs dans $\mathbb{D}_n$.
La fonction φ est aussi dans la classe $\mathcal{P}$.
De plus il est clair que le point rationnel $(Pr,n,m,S(\perp f\perp+m+n))$ ainsi construit approxime f à $1/2^n$ prés. ∎

Notez que cette propriété universelle de la présentation $\mathcal{C}_{\mathrm{KF}}$ est évidemment partagée par toute autre présentation $\mathcal{P}$-équivalente à $\mathcal{C}_{\mathrm{KF}}$.

4.1.2 Présentation par circuits booléens

La présentation par circuits booléens est essentiellement la même chose que la présentation à la Ko-Friedman. Elle est un peu plus naturelle dans le cadre que nous nous sommes fixés (présentation rationnelle de l'espace métrique $\mathbf{C}[0,1]$).
Notons **CB** l'ensemble des (codes des) circuits booléens. Codé informatiquement, un circuit booléen C est simplement donné par un programme d'évaluation booléen (boolean straight-line program) qui représente l'exécution du circuit C. Un point rationnel de la présentation par circuits booléens est une fonction linéaire par morceaux $\widetilde{f}$ codée par un quadruplet $f=(C,n,m,k)$ où C est (le code d')un circuit booléen, n est la précision réclamée pour $f(x)$, m la précision nécessaire en entrée, 2^{k+1} majore la norme de $\widetilde{f}$.

Définition 4.1.8 Un point rationnel de la présentation par circuits booléens $\mathcal{C}_{\mathrm{cb}}$ est codé par un quadruplet $f=(C,n,m,k)\in\mathbf{CB}\times\mathbb{N}_1\times\mathbb{N}_1\times\mathbb{N}_1$ où C est (le code d')un circuit booléen ayant m portes d'entrée et $k+n+1$ portes de sortie : les m portes d'entrée permettent de coder un élément de $\mathbb{D}_{m,[0,1]}$ et les $k+n+1$ portes de sortie permettent de coder les éléments de $\mathbb{D}$ de la forme $\pm 2^k\left(\sum_{i=1,\dots,n+k} b_i 2^{-i}\right)$ (où les b_i sont égaux à 0 ou 1).
La donnée $f=(C,n,m,k)$ est dite *correcte* lorsque deux entrées codant des éléments de $\mathbb{D}_{m,[0,1]}$ distants de $1/2^m$ donnent en sortie des codages de nombres distants de au plus $1/2^n$. L'ensemble

des données correctes est $\mathbf{Y}_{cb}$.
Lorsqu'une donnée f est correcte, elle définit une fonction linéaire par morceau $\widetilde{f}$ qui est bien contrôlée (c'est le "point rationnel" défini par la donnée).

On notera que les paramètres de contrôle n, m et k sont surtout indiqués pour le confort de l'utilisateur. En fait $n+k$ et m sont directement lisibles sur le circuit C.
De ce point de vue, la situation est un peu améliorée par rapport à la présentation $\mathcal{C}_{\mathrm{KF}}$ pour laquelle les paramètres de contrôle sont absolument indispensables. La taille de C contrôle à elle seule le temps d'exécution du circuit (c.-à-d. la fonction qui calcule, à partir du code d'un circuit booléen et de la liste de ses entrées, la liste de ses sorties est une fonction de très faible complexité).

Proposition 4.1.9 (Complexité de la famille de fonctions attachées à $\mathbf{Y}_{cb}$). *La famille de fonctions continues $(\widetilde{f})_{f\in\mathbf{Y}_{cb}}$ est uniformément de classe* $\mathbf{DSRT}(lin, Lin, QLin)$.

Preuve. On recopie presque à l'identique la preuve de la proposition 4.1.3 concernant la famille $(\widetilde{f})_{f\in\mathbf{Y}_{KF}}$. La seule différence est le remplacement de la fonction $\mathbf{Exec}(Pr, a)$ par l'évaluation d'un circuit booléen. La fonction qui calcule, à partir du code d'un circuit booléen et de la liste de ses entrées, la liste de ses sorties est une fonction de complexité en temps $\mathrm{O}(tlog(t))$ (avec $t = \mathrm{t}(C)$), donc de classe $\mathbf{DSRT}(Lin, Lin, QLin)$. ∎

NB : Si on avait pris en compte "le temps de gestion" (cf. remarque 3.2.3) on aurait trouvé une complexité $\mathbf{DSRT}(Lin, Lin, \mathrm{O}(N^2))$, c.-à-d. le même résultat que pour la famille $(\widetilde{f})_{f\in\mathbf{Y}_{KF}}$ (la complexité de $\mathbf{Exec}(Pr, a)$ prend justement en compte "le temps de gestion").

4.1.3 Présentation par circuits arithmétiques fractionnaires (avec magnitude)

Rappelons qu'un circuit *arithmétique (fractionnaire)* est par définition un circuit qui a pour portes d'entrées des variables "réelles" x_i et des constantes dans $\mathbb{Q}$. (on pourrait évidemment ne tolérer que les deux constantes 0 et 1 sans changement significatif).
Les autres portes sont :
— des portes à une entrée, des types suivants : $x \mapsto x^{-1},\ x \mapsto -x$
— des portes à deux entrées, des deux types suivants : $x + y,\ x \times y$.
Un circuit arithmétique calcule une fraction rationnelle, (ou éventuellement "error" si on demande d'inverser la fonction identiquement nulle). Nous considérerons des circuits arithmétiques avec une seule variable en entrée et une seule porte de sortie et nous noterons **CA** l'ensemble des (codes de) circuits arithmétiques à une seule entrée. Le code d'un circuit est le texte d'un programme d'évaluation (dans un langage et avec une syntaxe fixés une fois pour toutes) correspondant au circuit arithmétique considéré.

Définition 4.1.10 Un entier M est appelé *un coefficient de magnitude* pour un circuit arithmétique α à une seule entrée lorsque 2^M majore en valeur absolue toutes les fractions rationnelles du circuit (c.-à-d. celles calculées à toutes les portes du circuit) en tout point de l'intervalle $[0, 1]$.
Un couple $f = (\alpha, M) \in \mathbf{CA} \times \mathbb{N}_1$ est une donnée '*correcte* lorsque M est un coefficient de magnitude pour le circuit α. Cela définit les éléments de $\mathbf{Y}_{caf}$. Un élément f de $\mathbf{Y}_{caf}$ définit la fraction rationnelle notée $\widetilde{f}$ lorsqu'elle est vue comme un élément de $\mathbf{C}[0, 1]$. La famille $(\widetilde{f})_{f\in\mathbf{Y}_{caf}}$ est la famille des points rationnels d'une présentation de $\mathbf{C}[0, 1]$ qui sera notée $\mathcal{C}_{\mathrm{caf}}$

Notez que, à cause de la présence des multiplications et du passage à l'inverse, la taille de M peut être exponentielle par rapport à celle de α, même lorsqu'aucune fraction rationnelle de α n'a de pole sur $[0, 1]$. Ce genre de mésaventure n'avait pas lieu avec les circuits semilinéaires

binaires. Il semble même improbable que la correction d'un couple $(\alpha, M) \in CA \times \mathbb{N}_1$ puisse être testée en temps polynomial (par rapport à la taille de la donnée (α, M)).

Proposition 4.1.11 (Complexité de la famille de fonctions attachées à $\mathbf{Y}_{caf}$) *La famille de fonctions continues $(\widetilde{f})_{f\in\mathbf{Y}_{caf}}$ est uniformément de classe $\mathcal{P}$, et plus précisément de classe* $\mathbf{DSRT}(\mathrm{O}(N^3), Lin, \mathrm{O}(N\mathcal{M}(N^2)))$.

Preuve. Soit $f = (\alpha, M)$ un élément de $\mathbf{Y}_{caf}$. Soit p la profondeur du cirduit α. On montre par récurrence sur π que, pour une porte de profondeur π la fonction rationnelle correspondante a une dérivée majorée par $2^{2M\pi}$ sur l'intervalle $[0,1]$. Ceci fournit le module de continuité uniforme $\mu(f,k) = k + 2Mp$ (qui est en $\mathrm{O}(N^2)$) pour la famille $(\widetilde{f})_{f\in\mathbf{Y}_{caf}}$.
Nous devons maintenant exhiber une fonction $\psi : \mathbf{Y}_{caf} \times \mathbb{D}_{[0,1]} \times \mathbb{N}_1 \to \mathbb{D}$ de complexité $\mathbf{DRT}(Lin, \mathrm{O}(N\mathcal{M}(N^2)))$ telle que :

$$\forall (f,x,k) \in \mathbf{Y}_{caf} \times \mathbb{D}_{[0,1]} \times \mathbb{N}_1 \quad | \, \psi(f,x,k) - \widetilde{f}(x) \, | \leq 2^{-k}$$

Soit $(f,x,k) \in \mathbf{Y}_{caf} \times \mathbb{D}_{[0,1]} \times \mathbb{N}_1$ où $f = (\alpha, M)$. Soit $t = \mathrm{t}(\alpha)$ le nombre des portes du circuit α. La taille des entrées est $N = t + M + k$.
Pour calculer $\psi((\alpha, M), x, k)$ on procède comme suit. On lit $m = k + 2Mp + p$ bits de x ce qui donne les deux points consécutifs a et b de $\mathbb{D}_{m,[0,1]}$ tels que $a \leq x \leq b$. On exécute le circuit α au point a en tronquant le calcul effectué sur chaque porte aux m premiers bits significatifs. La valeur obtenue à la sortie, tronquée aux k premiers bits significatifs, est l'élément $\psi((\alpha, M), x, k)$. Comme une multiplication (ou une division) se fait en temps $\mathcal{M}(m)$, le temps des opérations arithmétiques proprement dites est un $\mathrm{O}(t\mathcal{M}(k + 2Mp + p)) = \mathrm{O}(N\mathcal{M}(N^2))$ et l'espace occupé est en $\mathrm{O}(N^3)$. ∎

NB : Si on avait pris en compte "le temps de gestion" (cf. remarque 3.2.3) on aurait dit :
Le temps des opérations arithmétiques proprement dites est $\mathrm{O}(N\mathcal{M}(N^2))$, et la gestion des objets est en $\mathrm{O}(N^4)$. Ainsi si on considère la multiplication rapide (respectivement naïve), la fonction d'évaluation est dans $\mathbf{DRT}(Lin, \mathrm{O}(N^4))$ (respectivement $\mathbf{DRT}(Lin, \mathrm{O}(N^5))$) où N est la taille des données.

4.1.4 Présentation par circuits arithmétiques polynomiaux (avec magnitude)

La présentation suivante de $\mathbf{C}[0,1]$ sera notée $\mathcal{C}_{\mathrm{cap}}$. L'ensemble des "points rationnels" sera noté $\mathbf{Y}_{cap}$.
C'est la même chose que les circuits arithmétiques fractionnaires, sauf qu'on supprime les portes "passage à l'inverse". Il n'est donc pas nécessaire d'écrire la définition en détail.
On retrouve les mêmes difficultés concernant la magnitude, en un peu moins grave. Il ne semble pas que l'on puisse obtenir pour les circuits polynomiaux de majorations senseiblement meilleures que celles obtenues à la proposition 4.1.11 pour les circuits avec divisions.

4.2 Comparaisons des présentations précédentes

Nous montrons dans cette section un résultat important, l'équivalence entre la présentation à la Ko-Friedman et les quatre présentations "par circuits" de $\mathbf{C}[0,1]$ citées dans la section précédente, ceci du point de vue de la complexité en temps polynomial. En particulier nous obtenons une formulation complètement contrôlée du point de vue algorithmique pour le théorème d'approximation de Weierstrass.
Pour montrer l'équivalence entre ces cinq présentations du point de vue de la complexité en temps polynomial, nous suivrons le plan ci-dessous :

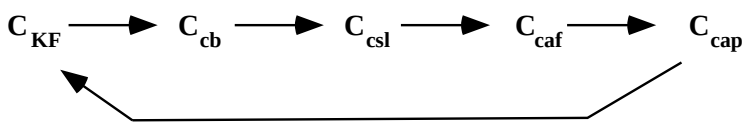

FIG. 3: schéma de la preuve

Pour donner l'équivalence entre ces différentes présentations, nous devons construire des fonctions qui permettent de transformer un point rationnel d'une présentation donnée en un point rationnel d'une autre présentation, qui approche convenablement le premier.

Proposition 4.2.1 *L'identité de* $\mathbf{C}[0,1]$ *de* $\mathcal{C}_{\mathrm{KF}}$ *vers* $\mathcal{C}_{\mathrm{cb}}$ *est uniformément de classe* $\mathcal{P}$*, en fait de classe* $\mathbf{DTIME}(N^{14})$.

La preuve de cette proposition est basée sur le Lemme 1.3.1 qui décrit la complexité d'une Machine de Turing Universelle et sur le lemme suivant :

Lemme 4.2.2 (cf. [34] et [25])
Soient M *une machine de Turing fixée,* T *et* m *des éléments de* $\mathbb{N}_1$*. Alors on a une fonction calculable en temps* $\mathrm{O}((T+m)^7)$ *qui calcule* $\gamma_{T,m}$ *: un circuit booléen simulant les* T *premières configurations de* M *pour n'importe quelle entrée dans* $\{0,1\}^m$.

Remarque 4.2.3 J. Stern a donné dans [34], pour tout entier $T \in \mathbb{N}_1$, une construction assez simple d'un circuit γ_T qui calcule la configuration de M obtenue après T pas de calcul à partir d'une configuration initiale de taille $\leq T$ (on peut supposer que $T \geq m$ ou prendre $\max(T,m)$). La taille du circuit γ_T est un $\mathrm{O}(T^2)$. L'auteur a mentionné aussi que cette construction se fait en temps polynomial. Une complexité plus précise (de l'ordre de $\mathrm{O}(T^7)$) est donnée dans [25].

Preuve. (de la proposition 4.2.1) On considère la Machine de Turing Universelle MU du lemme 1.3.1. Soit $f = (Pr, n, m, T)$ un élément de $\mathbf{Y}_{KF}$. Notons p la taille du programme Pr. La taille de f est $N = p + n + m + T$. La machine MU prend en entrée le programme Pr ainsi qu'une entrée $x \in \mathbb{D}_{m,[0,1]}$ et le nombre d'étapes T. Elle exécute en $\mathrm{O}(T(max(T,m)+p)) = \mathrm{O}(N^2)$ étapes (cf. lemme 1.3.1) la tâche de calculer la sortie pour le programme Pr sur la même entrée x après T étapes de calcul. En appliquant le lemme 4.2.2 on obtient un temps $\mathrm{O}(N^{14})$ pour calculer à partir de l'entrée f un élément g de $\mathbf{Y}_{cb}$ (un circuit booléen ainsi que ses paramètres de contrôle) pour lequel on a $\widetilde{g} = \widetilde{f}$. ∎

Proposition 4.2.4 *L'identité de* $\mathbf{C}[0,1]$ *de* $\mathcal{C}_{\mathrm{cb}}$ *vers* $\mathcal{C}_{\mathrm{csl}}$ *est uniformément de classe* $\mathbf{LINTIME}$*. Plus précisément, on a une fonction discrète qui, à partir d'un élément* $f = (\gamma, n, m, k)$ *de* $\mathbf{Y}_{cb}$ *et d'un entier* $q \in \mathbb{N}_1$*, calcule en temps* $\mathrm{O}(N)$ *(où* N *est la taille de l'entrée* $((\gamma, n, m, k), q)$*, un circuit semilinéaire binaire* g *tel que :*

$$| \widetilde{f}(x) - \widetilde{g}(x) | \leq 2^{-q} \quad \forall x \in [0,1] \quad (F4.2.1)$$

La preuve de cette proposition utilise le lemme suivant :

Lemme 4.2.5 *Il existe une fonction calculable en temps* $\mathrm{O}(N)$ *qui transforme tout élément* $f = ((\gamma, n, m, k), h)$ *de* $\mathbf{Y}_{cb} \times \mathbb{N}_1$ *en un élément* $f' = (\gamma', n+h, m+h, k)$ *de* $\mathbf{Y}_{cb}$ *correspondant à la même fonction semilinéaire.*

Preuve. (lemme 4.2.5) Supposons que le circuit γ calcule, pour l'entrée $x = u/2^m$ où $0 \leq u \leq 2^m - 1$, la valeur $y = \ell/2^n$, et pour $x' = (u+1)/2^m$, la valeur $y' = \ell'/2^n$ avec $\ell, \ell' \in \mathbb{Z}$

et $\mid \ell - \ell' \mid \leq 1$. Alors le circuit γ' calcule, pour l'entrée $x + r2^{-h}2^{-m}$, $0 \leq r \leq 2^h$, la valeur $y + (y' - y)r2^{-h}$.
Noter de plus que $\mathrm{t}(\gamma') = \mathrm{O}(\mathrm{t}(\gamma) + h)$ et $\mathrm{prof}(\gamma') = \mathrm{O}(\mathrm{prof}(\gamma) + h)$. ∎

Preuve. (proposition 4.2.4) D'après le lemme 4.2.5, la condition (F4.2.1) de la proposition peut être remplacée par la condition :

$$\mid \widetilde{f}(x) - \widetilde{g}(x) \mid \leq 2^{-(n-1)} \quad \forall x \in [0,1] \quad (F4.2.2)$$

En effet : si $q < n$ alors (F4.2.1) découle de (F4.2.2), sinon, on utilise l'interpolation linéaire donnée dans la preuve du lemme 4.2.5.
Nous cherchons donc maintenant à simuler le circuit booléen $f = (\gamma, n, m, k)$ par un circuit semilinéaire binaire g avec la précision $1/2^n$.
Tout d'abord remarquons qu'il est facile de simuler de manière exacte toutes les portes, "sauf l'entrée", par un circuit semilinéaire simple λ qui consiste en :
1) remplacer les constantes booléennes 0 et 1 de γ par les constantes rationnelles 0 et 1.
2) remplacer chaque sommet de γ calculant $\neg u$ par un sommet de λ calculant $1 - u$.
3) remplacer chaque sommet de γ calculant $u \wedge v$ par un sommet de λ calculant $\min(u, v)$.
4) remplacer chaque sommet de γ calculant $u \vee v$ par un sommet de λ calculant $\max(u, v)$.
5) calculer, à partir des sorties $c_0, c_1, \ldots, c_{n+k}$ du circuit γ, le point rationnel :

$$\pm 2^k \sum_{i=1,\ldots,n+k} c_i 2^{-i} \ (c_0 \text{ code le signe})$$

Il est clair que le circuit λ se construit en temps linéaire et admet une taille $\mathrm{t}(\lambda) = \mathrm{O}(\mathrm{t}(\gamma))$ et une profondeur $\mathrm{prof}(\lambda) = \mathrm{O}(\mathrm{prof}(\gamma))$.
Maintenant nous cherchons à "simuler l'entrée" du circuit γ, c.-à-d. les bits codant x, par un circuit semilinéaire binaire.
Usuellement, pour déterminer le développement binaire d'un nombre réel x, on utilise le pseudo-algorithme suivant qui utilise la fonction discontinue C définie par :

$$C(x) = \begin{cases} 1, & \text{si x} \geq 1/2 \\ 0, & \text{sinon} \end{cases}$$

Algorithme 1 ("calcul" des m premiers bits d'un nombre réel x)

Entrées : $x \in [0,1]$, $m \in \mathbb{N}$
Sortie : la liste$(b_1, b_2, \ldots, b_m) \in \{0,1\}^m$

Pour $j := 1$ à m Faire

$b_j \leftarrow C(x)$
$x \leftarrow 2x - b_j$

Fait
Fin.

La fonction C est discontinue, donc l'algorithme 1 *n'est pas vraiment un algorithme*; et il ne peut pas être simulé par un circuit semilinéaire binaire. On considère alors la fonction continue

$$C_p(x) := C_{p,1/2} = \min(1, \max(0, 2^p(x - 1/2))) \quad \text{(cf. fig. 1)}$$

qui "approche" la fonction C. Et on considère l'algorithme suivant :

Algorithme 2 (calcul "approximatif" des m premiers bits qui codent un nombre réel x)

Entrées : $x \in [0,1],\ m \in \mathbb{N}_1$
Sortie : une liste $(b_1, b_2, \ldots, b_m) \in [0,1]^m$

$p \leftarrow m+2$
Pour $j := 1$ à m Faire
$b_j \leftarrow C(x)$
$x \leftarrow 2x - b_j$
$p \leftarrow p-1$
Fait
Fin.

Ceci est réalisé par un circuit de taille et profondeur $\mathrm{O}(m)$ sous la forme suivante :

Algorithme 2bis (forme circuit semilinéaire de l'algorithme 2)

Entrées : $x \in [0,1],\ m \in \mathbb{N}_1$
Sortie : une liste $(b_1, b_2, \ldots, b_m) \in [0,1]^m$

$p \leftarrow m+2,\ q \leftarrow 2^p$
Pour $j := 1$ à m Faire
$y \leftarrow q(x - 1/2)$
$b_j \leftarrow \min(1, \max(0, y))$
$x \leftarrow 2x - b_j$
$q \leftarrow q/2$
Fait
Fin.

Mais un problème crucial se pose quand le réel x en entrée est dans un intervalle de type $]k/2^m, k/2^m + 1/2^p[$ où $0 \leq k \leq 2^m - 1$. Dans ce cas au moins un bit calculé dans l'algorithme 2 est dans $]0,1[$. Par conséquent le résultat final de la simulation du circuit booléen peut être incohérent. Pour contourner cette difficulté, on utilise une technique introduite par Hoover [12, 13]. On fait les remarques suivantes :
— Pour tout $x \in [0,1]$ au plus une des valeurs $x_\sigma = x + \sigma/2^{m+2}$ (où $\sigma \in \{-1,0,1\}$), est dans un intervalle de type précédent
— Notons $z_\sigma = \sum_{j=1,\ldots,m} b_j 2^{-j}$ où les b_j sont fournis par l'agorithme 2bis sur l'entrée x_σ. D'après la remarque précédente, au moins deux valeurs $\phi(\widetilde{\lambda}(z_\sigma)$ $(\sigma \in \{-1,0,1\})$, correspondent exactement à la sortie du circuit arithmétique γ lorsqu'on met en entrée les m premiers bits de x_σ. C.-à-d., pour au moins deux valeurs de σ, on a $z_\sigma \in \mathbb{D}_m$ et $\widetilde{\lambda}(z_\sigma) = \widetilde{f}(z_\sigma)$ avec en outre $\mid z_\sigma - x \mid \leq 1/2^m + 1/2^{m+2} \leq 1/2^{m-1}$ (d'où $\mid \widetilde{f}(z_\sigma) - \widetilde{f}(x) \mid \leq 1/2^{n-1}$))
— Donc, une éventuelle mauvaise valeur calculée par le circuit semilinéaire ne peut être que la première ou la troisième des valeurs si on les ordonne par ordre croissant. Ainsi, si y_{-1}, y_0 et y_1, sont les trois valeurs respectivement calculées par le circuit aux points x_σ $(\sigma \in \{-1,0,1\})$, alors la deuxième des 3 valeurs approche correctement $\widetilde{f}(x)$. Etant donnés trois nombres réels y_{-1}, y_0 et y_1, le 2ème par ordre croissant, $\theta(y_{-1}, y_0, y_1)$, est calculé par exemple par l'un des deux circuits semilinéaires binaires représentés par le deuxième membre dans les équations :

$$\theta(y_{-1}, y_0, y_1) = y_{-1} + y_0 + y_1 - \min(y_{-1}, y_0, y_1) - \max(y_{-1}, y_0, y_1)$$

$$\theta(y_{-1}, y_0, y_1) = \min(\max(y_0, y_1), \max(y_1, y_{-1}), \max(y_0, y_{-1}))$$

Résumons : à partir de l'entrée x nous calculons les $x_\sigma = x + \sigma/2^{m+2}$ (où $\sigma \in \{-1,0,1\}$), et nous appliquons successivement :

— le circuit ε (de taille $O(m) = O(N)$) qui décode correctement les m premiers digits de x_σ pour au moins deux des trois x_σ
— le circuit λ qui simule le circuit booléen proprement dit et recode les digits de sortie sous forme d'un dyadique, ce circuit est de taille $O(N)$
— puis le circuit θ qui choisit la 2ème valeur calculée par ordre croissant.
Nous obtenons donc un circuit qui calcule la fonction :

$$\widetilde{g}(x) = \theta(\lambda(\varepsilon(x - 1/2^p)), \lambda(\varepsilon(x)), \lambda(\varepsilon(x + 1/2^p))) \text{ avec } p = m + 2$$

de taille et de profondeur O(N) :

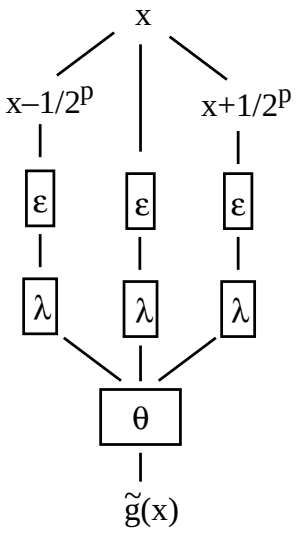

FIG. 4: vue globale du calcul

et tel que :

$$| \widetilde{f}(x) - \widetilde{g}(x) | \leq 2^{-n} \; \forall x \in [0,1]$$

En outre, le temps mis pour calculer (le code de) g à partir de l'entrée f est également en $O(N)$. ∎

Nous passons à la simultation d'un circuit semilinéaire binaire par un circuit arithmétique (avec divisions). Nous donnons tout d'abord une version "circuit" de la proposition 3.3.5.

Proposition 4.2.6 *Les fonctions* $(x,y) \mapsto \max(x,y)$ *et* $(x,y) \mapsto \min(x,y)$ *sur le carré* $[-2^m, 2^m] \times [-2^m, 2^m]$ *peuvent être approchées à* $1/2^n$ *près par des circuits arithmétiques de taille* $O((n+m)^3)$, *de magnitude* $O((n+m)^3)$ *et qui peuvent être calculés dans la classe* $\mathbf{DTIME}(O(N^3))$ $(N = n + m)$.

Preuve. On reprend la preuve du lemme 3.3.3. La représentation de polynomes approchant convenablement P_n et Q_n au moyen de circuits est plus économique en espace. Tout d'abord il faut construire un circuit qui calcule une approximation de $e^{-1/n}$ avec la précision $1/2^{n^3}$. On considère le développement de Taylor

$$F_m(z) = \sum_{0 \leq i \leq m} (-1)^i / i! z^i$$

qui approche e^z $1/2^{m+2}$ près si $m \geq 5$ et $0 \leq z \leq 1$. Ici, on peut se contenter de donner un circuit qui calcule $d_n = F_{n^3}(1/n)$ dont la taille et le temps de calcul sont a priori en $O(n^3)$ (alors

qu'on était obligé de donner explicitement une approximation dyadique $c_{n,1}$ de d_n). Ensuite on construit un circuit qui calcule une bonne approximation de $H_n(x) = \prod_{1\leq k<n^2}(x + e^{-k/n})$ sous la forme $h_n(x) = (x + d_n)(x + d_n^2)\cdots(x + d_n^{n^2-1})$. Ce qui réclame un temps de calcul (et une taille de circuit) en $\mathrm{O}(n^2)$. Ceci fait que le circuit arithmétique qui calcule une approximation à $1/2^n$ près de $\mid x \mid$ sur $[0, 1]$ est calculé en temps $\mathrm{O}(n^3)$.
On voit aussi facilement que le coefficient de magnitude est majoré par la taille de $1/h_n(0)$ c.-à-d. également un $\mathrm{O}(n^3)$. ∎

On remarquera que le coefficient de magnitude peut difficilement être amélioré. Par contre, il ne semble pas impossible que d_n puisse être calculé par un circuit de taille plus petite que la taille naïve en $\mathrm{O}(n^3)$.

Proposition 4.2.7 *L'identité de* $\mathbf{C}[0, 1]$ *de* $\mathcal{C}_{\mathrm{csl}}$ *vers* $\mathcal{C}_{\mathrm{caf}}$ *est uniformément de classe* $\mathcal{P}$*, en fait de classe* $\mathbf{DTIME}(N^4)$*. Plus précisément, on a une fonction discrète qui, à partir d'un élément* g *de* $\mathbf{Y}_{csl}$ *de taille* $\mathrm{t}(g) = t$ *et de profondeur* $\mathrm{prof}(g) = p$*, et d'un entier* $n \in \mathbb{N}_1$*, calcule en temps* $\mathrm{O}(t(n + p)^3)$ *un élément* $f = (\alpha, M) \in \mathbf{Y}_{caf}$
de taille $\mathrm{t}(\alpha) = \mathrm{t}(g)\mathrm{O}((n + p)^3)$,
de profondeur $\mathrm{prof}(\alpha) = \mathrm{O}(p(n + p)^3)$
avec coefficient de magnitude $M = \mathrm{mag}(\alpha) = \mathrm{O}((n + p)^3)$,
et tel que : $\mid \widetilde{f}(x) - \widetilde{g}(x) \mid \leq 2^{-n}\ \ \forall x \in [0, 1]$

Preuve. Notons $p = \mathrm{prof}(g)$. Les portes de g pour une entrée $x \in [0, 1]$ prennent des valeurs dans l'intervalle $[-2^p, 2^p]$. On veut simuler à 2^{-n} près le circuit g par un circuit arithmétique. Il suffit de simuler les portes max et min du circuit semilinéaire à $2^{-(n+p)}$ près sur l'intervalle $[-2^p, 2^p]$. Chaque simulation réclame, d'après la proposition 4.2.6, un circuit arithmétique (avec division) dont toutes les caractéristiques sont majorées par un $\mathrm{O}(n + p)^3$. ∎

Nous passons à la simultation d'un circuit arithmétique avec divisions par un circuit arithmétique polynomial.

Proposition 4.2.8 *L'identité de* $\mathbf{C}[0, 1]$ *de* $\mathcal{C}_{\mathrm{caf}}$ *vers* $\mathcal{C}_{\mathrm{cap}}$ *est uniformément de classe* $\mathcal{P}$*, en fait de classe* $\mathbf{DTIME}(N^2)$*. Plus précisément, on a une fonction discrète qui, à partir d'un élément* $f = (\alpha, M)$ *de* $\mathbf{Y}_{caf}$*, et d'un entier* $n \in \mathbb{N}_1$*, calcule en temps* $\mathrm{O}(N^2)$ *un circuit arithmétique polynomial* $(\Gamma, M') \in \mathbf{Y}_{cap}$ *(*N *est la taille de l'entrée* $((\alpha, M), n)$
de taille $\mathrm{t}(G) = \mathrm{O}(\mathrm{t}(\alpha)(n + M))$,
de profondeur $\mathrm{prof}(G) = \mathrm{O}(\mathrm{prof}(\alpha)(n + M))$
de magnitude $\mathrm{mag}(G) = M' = \mathrm{O}(n + M)$,
et tel que : $\mid \widetilde{f}(x) - \widetilde{g}(x) \mid \leq 2^{-n}$ *pour tout* $x \in [0, 1]$.

Le problème se pose seulement au niveau des portes "passage à l'inverse". Nous cherchons donc à les simuler par des circuits polynomiaux tout en gardant la magnitude bien majorée.

Lemme 4.2.9 *La fonction* $x \mapsto 1/x$ *sur l'intervalle* $[-2^m, 2^m]$ *peut être réalisée avec la précision* $1/2^n$ *par un circuit polynomial de magnitude* $\mathrm{O}(m)$*, de taille* $\mathrm{O}(m + n)$ *et qui est construit en temps linéaire.*

Preuve. Nous utilisons comme Hoover la méthode de Newton qui permet de calculer l'inverse d'un réel z à 2^{-n} prés en un nombre raisonnable d'additions et multiplications en fonction de n :
Méthode de Newton (pour le calcul de l'inverse de z)
Pour $-2^{-m} < z < 2^m$ on pose

$$C(x) = \begin{cases} y_0 = 2^{-m} \\ y_{i+1} = y_i(2 - zy_i) \end{cases}$$

On vérifie facilement que, pour $i \geq 3m + log(m+n)$, on a :

$$| z^{-1} - y_i | \leq 2^{-n}$$

Ainsi pour l'entrée $(n,m) \in \mathbb{N}_1 \times \mathbb{N}_1$, l'application de la méthode de Newton jusqu'à l'itération $i = 3m+log(m+n)$ est représentée par un circuit polynomial de taille O(m+n) et de magnitude $O(m+n)$. De plus, il est facile de vérifier que la construction de ce circuit se fait en temps linéaire. ∎

Proposition 4.2.10 *L'identité de* $\mathbf{C}[0,1]$ *de* $\mathcal{C}_{\text{cap}}$ *vers* $\mathcal{C}_{\text{KF}}$ *est uniformément de classe* $\mathcal{P}$*, en fait de classe* $\mathbf{DRT}(Lin, O(N^4))$.

Preuve. Le fait d'être de classe $\mathcal{P}$ résulte du théorème 4.1.7 et de la proposition 4.1.11. La lecture précise des preuves du théorème 4.1.7 et de la proposition 4.1.11 donne le résultat $\mathbf{DRT}(Lin, O(N^4))$ (en tenant compte du Nota bene après 4.1.11). ∎

En résumant les résultats qui précèdent nous obtenons le théorème suivant.

Théorème 4.2.11 *Les cinq présentations* $\mathcal{C}_{\text{KF}}$, $\mathcal{C}_{\text{cb}}$, $\mathcal{C}_{\text{csl}}$, $\mathcal{C}_{\text{caf}}$ *et* $\mathcal{C}_{\text{cap}}$ *de* $\mathbf{C}[0,1]$ *sont* $\mathcal{P}$*-équivalentes.*

Notation 4.2.12 *Pour autant qu'on se situe à un niveau de complexité suffisamment élevé pour rendre le théorème de comparaison valable (en particulier la classe* $\mathcal{P}$ *suffit) il n'y a pas de raison de faire de différence entre les cinq présentations* $\mathcal{C}_{\text{KF}}$, $\mathcal{C}_{\text{cb}}$, $\mathcal{C}_{\text{csl}}$, $\mathcal{C}_{\text{caf}}$ *et* $\mathcal{C}_{\text{cap}}$ *de* $\mathbf{C}[0,1]$. *En conséquence, désormais la notation* $\mathbf{C}[0,1]$ *signifiera qu'on considère l'espace* $\mathbf{C}[0,1]$ *avec la structure de calculabilité* $\mathcal{C}_{\text{csl}}$.

4.3 Complexité du problème de la norme

On sait que la détermination du maximum, sur un intervalle $[0,1]$ d'une fonction calculable en temps polynomial $f : \mathbb{N} \to \{0,1\}$ est à très peu près la même chose que le problème $\mathcal{NP}$-complet le plus classique : SAT.
Il n'est donc pas étonnant de trouver comme problème $\mathcal{NP}$-complet un problème relié au calcul de la norme pour une fonction continue. Il nous faut tout d'abord formuler le problème de la norme attaché à une présentation rationnelle donnée de l'espace $\mathbf{C}[0,1]$ d'une manière suffisamment précise et invariante.

Définition 4.3.1 Nous appelons "problème de la norme", relativement à une présentation $\mathcal{C}_1 = (Y_1, \delta_1, \eta_1)$ de $\mathbf{C}[0,1]$) le problème :
Résoudre *approximativement* la question $a \leq \| f \|_\infty$? dans la présentation $\mathcal{C}_1$ de $\mathbf{C}[0,1]$.
La formulation précise de ce problème est la suivante :
Entrées : $(f, a, n) \in Y_1 \times \mathbb{D} \times \mathbb{N}_1$
Sortie : fournir correctement une des deux réponses :
— voici un $x \in \mathbb{D}$ tel que $| f(x) | \geq a - 1/2^n$
— il n'existe pas de $x \in \mathbb{D}$ vérifiant $| f(x) | \geq a$.

Cette définition est justifiée par le lemme suivant.

Lemme 4.3.2 *Pour deux présentations rationnelles* $\mathcal{C}_1$ *et* $\mathcal{C}_2$ *de* $\mathbf{C}[0,1]$ *polynomialement équivalentes, les problèmes de la norme correspondants sont aussi polynomialement équivalents.*

Preuve. La transformation du problème correspondant à une présentation $\mathcal{C}_1$ au problème correspondant à une autre présentation $\mathcal{C}_2$ se fait par un algorithme ayant la même complexité que l'algorithme qui permet de présenter la fonction identité entre $\mathcal{C}_1$ et $\mathcal{C}_2$. En effet, pour les

données $(f, a, n) \in Y_1 \times \mathbb{D} \times \mathbb{N}_1$, on cherche $g \in Y_2$ telle que $\| f - g \|_\infty \leq 2^{-(n+2)}$, puis on résout le problème avec les entrées $(g, a - 1/2^{n+1}, n + 2)$.
Si on trouve $x \in \mathbb{D}$ tel que $| g(x) | \geq a - 2^{-(n+1)} - 2^{-(n+2)}$, alors $| f(x) | \geq a - 2^{-n}$.
Si on déclare forfait, c'est qu'il n'existe pas de $x \in \mathbb{D}$ tel que $| g(x) | \geq a - 2^{-(n+1)}$. A fortiori, il n'existe pas de $x \in \mathbb{D}$ tel que $| f(x) | \geq a$. ∎

Théorème 4.3.3 *Le problème de la norme est $\mathcal{NP}$-complet pour les présentations $\mathcal{C}_{\mathrm{KF}}$, $\mathcal{C}_{\mathrm{cb}}$, $\mathcal{C}_{\mathrm{csl}}$, $\mathcal{C}_{\mathrm{caf}}$ et $\mathcal{C}_{\mathrm{cap}}$.*

Preuve. D'après le lemme 4.3.2 il suffit de faire la preuve pour la présentation $\mathcal{C}_{\mathrm{cb}}$. Le caractère $\mathcal{NP}$ du problème est immédiat. Pour voir la $\mathcal{NP}$-dureté, nous considérons le problème de la norme limité aux entrées $((\gamma, 1, m, 1), 3/4, 2)$ où γ est un circuit booléen arbitraire à m entrées et une sortie (le quadruplet est alors évidement correct), et la réponse oui correspond à la satisfiabilité du circuit γ. ∎

On a également le résultat suivant, essentiellement négatif[11], et donc moins intéressant.

Proposition 4.3.4 *Pour les présentations considérées, la fonction norme $f \mapsto \| f \|_\infty$ de $\mathbf{C}[0,1]$ vers $\mathbb{R}^+$ est uniformément de classe $\mathcal{P}$ si et seulement si $\mathcal{P} = \mathcal{NP}$.*

Preuve. Il suffit de raisonner avec la présentation $\mathcal{C}_{\mathrm{cb}}$. Si la fonction norme est $\mathcal{P}$- calculable[12], le problème de la norme se résout en temps polynomial, et donc $\mathcal{P} = \mathcal{NP}$.
Si $\mathcal{P} = \mathcal{NP}$, le problème de la norme se résout en temps polynomial, ce qui permet de calculer la norme par dichotomie en initialisant avec la majoration 2^k, jusqu'à obtenir la précision $1/2^q$. Ceci réclame $k + q$ étapes de dichotomie. L'ensemble du calcul est en temps polynomial sur l'entrée $(g, q) \in \mathbf{Y}_{cb} \times \mathbb{N}_1$. ∎

Corollaire 4.3.5 *L'identité de $\mathbf{C}[0,1]$ de $\mathcal{C}_{\mathrm{KF}}$ vers $\mathcal{C}_{\mathrm{frac}}$ n'est pas calculable en temps polynomial, au moins si $\mathcal{P} \neq \mathcal{NP}$.*

Preuve. La fonction norme est calculable en temps polynomial pour la présentation $\mathcal{C}_{\mathrm{frac}}$ d'après la proposition 3.2.7. On conclut par la proposition précédente. ∎

Proposition 4.3.6 *Pour les cinq présentations précédentes de $\mathbf{C}[0,1]$, si l'évaluation est dans $\mathbf{DSPACE}(S(N))$ avec $S(N) \geq N$, alors la fonction norme est aussi dans $\mathbf{DSPACE}(S(N))$.*

Preuve. Si $k \mapsto \mu(k)$ est un module de continuité d'un point rationnel $\widetilde{f}$ d'une présentation donnée de $\mathbf{C}[0,1]$, alors pour calculer la norme avec une précision n il suffit d'évaluer $\widetilde{f}$ sur les éléments de $\mathbb{D}_{m,[0,1]}$ (où $m = \mu(n)$) et prendre la valeur maximale. Puisque les résultats intermédiaires inutiles sont immédiatement effacés, et puisque $S(N) \geq N \geq m$ l'espace de calcul de la fonction norme est le même que celui de la fonction d'évaluation. ∎

4.4 Complexité des présentations rationnelles étudiées

Dans cette section, nous présentons rapidement la complexité du test d'appartenance et des opérations d'espace vectoriel, pour les cinq présentations considérées, et nous récapitulons l'ensemble des résultats obtenus.

Proposition 4.4.1 *Le test d'appartenance (à l'ensemble des points rationnels) est :*
— **LINSPACE** *et $\mathcal{CO}$–$\mathcal{NP}$-complet pour les présentations $\mathcal{C}_{\mathrm{KF}}$ et $\mathcal{C}_{\mathrm{cb}}$*
— **LINTIME** *pour la présentation $\mathcal{C}_{\mathrm{csl}}$.*

[11] Puisque $\mathcal{P} \neq \mathcal{NP}$!.
[12] Nous utiliserons quelquefois la terminologie $\mathcal{P}$- calculable comme abréviation pour calculable en temps polynomial.

Preuve. Pour la présentation $\mathcal{C}_{\rm csl}$, c'est évident. Les preuves sont essentiellement les mêmes pour les deux présentations $\mathcal{C}_{\rm KF}$ et $\mathcal{C}_{\rm cb}$. Nous n'en donnons qu'une chaque fois.
Voyons que le test d'appartenance est **LINSPACE** pour $\mathbf{Y}_{KF}$. Pour une entrée (Pr, n, m, T) on fait le calcul suivant :
pour $i = 1, \ldots, 2m$ vérifier que

$$Pr(i/2^m) \in \mathbb{D}_n \text{ et } \mid P((i-1)/2^m) - Pr(i/2^m) \mid \leq 1/2^n$$

Ce calcul est **LINSPACE**. Pour la $\mathcal{CO}-\mathcal{NP}$-complétude du test d'appartenance, nous donnons la preuve pour les circuits booléens. On peut se limiter aux entrées $(\gamma, 2, m, 0)$ où γ est un circuit qui ne calcule qu'une sortie correspondant au premier bit, les deux autres bits sont nuls. On demande la cohérence sur deux points consécutifs de la grille. Seules les fonctions constantes sont donc tolérées.
Le problème opposé du test d'appartenance revient à savoir si un circuit booléen est non constant, ce qui implique la résolution du problème de satisfiabilité. ∎

Proposition 4.4.2 *Les opérations d'espace vectoriel (sur l'ensemble des points rationnels) sont dans* **LINTIME** *pour les cinq présentations* $\mathcal{C}_{\rm KF}$, $\mathcal{C}_{\rm cb}$, $\mathcal{C}_{\rm csl}$, $\mathcal{C}_{\rm caf}$ *et* $\mathcal{C}_{\rm cap}$ *de* $\mathbf{C}[0,1]$.

Preuve. Les calculs sont évidents. Par exemple si $(f_1, \ldots, f_s) \in \mathbf{lst}(\mathbf{Y}_{KF})$ et $n \in \mathbb{N}_1$, on peut calculer facilement $f \in \mathbf{Y}_{KF}$ tel que :

$$\| \widetilde{f} - \sum_{i=1,\ldots,s} \widetilde{f_i} \| \leq 1/2^n$$

car il suffit de connaître chaque $\widetilde{f_i}$ avec la précision $1/2^{n+log(s)}$. ∎

Le seul "drame" est évidemment que les présentations $\mathcal{C}_{\rm KF}$ et $\mathcal{C}_{\rm cb}$ ne sont pas des $\mathcal{P}$-présentations de $\mathbf{C}[0,1]$ (sauf si $\mathcal{P} = \mathcal{NP}$ cf. la proposition 4.3.4.)
Pour terminer cette section nous donnons un tableau récapitulatif dans lequel nous regroupons presque tous les résultats de complexité établis pour les cinq présentations rationnelles $\mathcal{C}_{\rm KF}$, $\mathcal{C}_{\rm cb}$, $\mathcal{C}_{\rm csl}$, $\mathcal{C}_{\rm caf}$ et $\mathcal{C}_{\rm cap}$ de l'espace $\mathbf{C}[0,1]$.

	Evaluation	Fonction Norme	Test d'appartenance	Opérations d'espace vectoriel
$\mathcal{C}_{\rm KF}$ et $\mathcal{C}_{\rm cb}$	**DSRT**$(Lin, Lin, \mathrm{O}(N^2))$	**LINSPACE** et $\mathcal{NP}$-complet	**LINSPACE** et $\mathcal{CO}-\mathcal{NP}$-complet	**LINTIME**
$\mathcal{C}_{\rm csl}$	**DSRT**$(\mathrm{O}(N^2), Lin, \mathrm{O}(N^2))$	**DSPACE**$(\mathrm{O}(N^2))$ et $\mathcal{NP}$-complet	**LINTIME**	**LINTIME**
$\mathcal{C}_{\rm caf}$ et $\mathcal{C}_{\rm cap}$	**DSRT**$(\mathrm{O}(N^3), Lin, \mathrm{O}(N^4))$	**DSPACE**$(\mathrm{O}(N^3))$ et $\mathcal{NP}$-complet	**PSPACE**	**LINTIME**

Pour le test d'appartenance **PSPACE** il est probable que sa complexité soit bien moindre.

Remarque 4.4.3 Malgré la facilité de calcul de la fonction d'évaluation pour les présentations $\mathcal{C}_{\rm KF}$ et $\mathcal{C}_{\rm cb}$, c'est encore la présentation par circuits semilinéaires binaires qui semble au fond la plus simple. Sa considération a permis en outre d'éclairer le théorème de comparaison 4.2.11, qui est une version renforcée, uniforme, des résultats établis par Hoover.

Le défaut inévitable (si $\mathcal{P} \neq \mathcal{NP}$) des présentations définies jusqu'à maintenant est la non faisabilité du calcul de la norme. Ceci empêche d'avoir une procédure de contrôle faisable pour les suites de Cauchy de points rationnels. Ceci diminue d'autant l'intérêt des $\mathcal{P}$-points de $\mathcal{C}_{\text{csl}}$. Cela souligne bien le fait qu'il est un peu artificiel d'étudier les $\mathcal{P}$-points d'un espace qui est donné dans une présentation de complexité non polynomiale.
En outre des problèmes a priori au moins aussi difficiles que la calcul de la norme, comme par exemple le calcul d'une primitive ou la solution d'une équation différentielle, sont également sans espoir de solution raisonnable dans le cadre des présentations que nous venons d'étudier.
Il est donc légitime de se tourner vers d'autres présentations rationnelles de l'espace $\mathbf{C}[0,1]$ pour voir dans quelle mesure elles sont mieux adaptées aux objectifs de l'analyse numérique.

5 Quelques présentations de classe $\mathcal{P}$ pour l'espace $\mathbf{C}[0,1]$

Dans cette section on aborde la question de savoir jusqu'à quel point des présentations rationnelles dans la classe $\mathcal{P}$ de l'espace $\mathbf{C}[0,1]$ fournissent un cadre de travail adéquat pour l'analyse numérique. Il ne s'agit que d'une première étude, qui devrait être sérieusement développée.

5.1 Définitions de quelques présentations de classe $\mathcal{P}$

5.1.1 Présentation $\mathcal{C}_{\text{W}}$ (à la Weierstrass)

L'ensemble des points rationnels $\mathbf{Y}_W$ de la présentation $\mathcal{C}_{\text{W}}$ est simplement l'ensemble $\mathbb{D}[X]$ des polynômes (à une variable) à coefficients dans $\mathbb{D}$ donnés en présentation dense.
Un $\mathcal{P}$-point f de $\mathcal{C}_{\text{W}}$ est donc donné par une suite $\mathcal{P}$-calculable :

$$m \mapsto P_m \ : \ \mathbb{N}_1 \to \mathbb{D}[X], \text{ avec } : \forall m : \parallel P_m - f \parallel_\infty \leq 1/2^m$$

Et une $\mathcal{P}$-suite f_n de $\mathcal{C}_{\text{W}}$ est donnée par une suite double $\mathcal{P}$- calculable :

$$(n,m) \mapsto P_{n,m} \ : \ \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{D}[X], \text{ avec } : \forall n,m : \parallel P_{n,m} - f_n \parallel_\infty \leq 1/2^m$$

Remarque 5.1.1 Une définition équivalente pour un $\mathcal{P}$-point f de $\mathcal{C}_{\text{W}}$ est obtenue en demandant que f s'écrive comme somme d'une série $\sum Q_m$, où (Q_m) est une suite $\mathcal{P}$-calculable dans $\mathbb{D}[X]$ vérifiant : $\parallel Q_m \parallel_\infty \leq 1/2^m$. Ceci donne une manière agréable de présenter les $\mathcal{P}$-points de $\mathcal{C}_{\text{W}}$. En effet on peut contrôler en temps polynomial (par rapport à m) le fait que la suite est correcte pour les termes de 1 à m. En outre, dans l'optique d'un calcul "paresseux", on peut contrôler la série (Q_m) au fur et à mesure que le besoin de précision augmente. Cette remarque est valable pour toute autre présentation rationnelle de classe $\mathcal{P}$ alors qu'elle ne le serait pas pour les présentations étudiées à la section 4.

Nous énonçons tout de suite un résultat comparant les présentations rationnelles $\mathcal{C}_{\text{frac}}$ et $\mathcal{C}_{\text{W}}$.

Proposition 5.1.2
— *L'identité de* $\mathbf{C}[0,1]$ *de* $\mathcal{C}_{\text{W}}$ *vers* $\mathcal{C}_{\text{frac}}$ *est* **LINTIME**.
— *L'identité de* $\mathbf{C}[0,1]$ *de* $\mathcal{C}_{\text{frac}}$ *vers* $\mathcal{C}_{\text{W}}$ *n'est pas de classe* $\mathcal{P}$.

Preuve. La première affirmation est triviale. La seconde résulte du fait que la fonction $x \mapsto| x - 1/2 |$ est un $\mathcal{P}$-point de $\mathcal{C}_{\text{frac}}$ (théorème 3.3.4) tandis que tous les $\mathcal{P}$-points de $\mathcal{C}_{\text{W}}$ sont des fonctions infiniment dérivables (cf. ci-dessous le théorème 5.2.7). ∎

Puisque la présentation $\mathcal{C}_{\text{frac}}$ de $\mathbf{C}[0,1]$ est de classe $\mathcal{P}$, on a immédiatement.

Proposition 5.1.3 *La présentation $\mathcal{C}_{\text{W}}$ de $\mathbf{C}[0,1]$ est de classe $\mathcal{P}$.*

L'intérêt de la présentation $\mathcal{C}_{\text{W}}$ est notamment souligné par les théorèmes de caractérisation (cf. section 5.2) qui précisent des phénomènes "bien connus" en analyse numérique, avec les polynômes de Chebyshev comme méthode d'attaque des problèmes.

5.1.2 Présentation $\mathcal{C}_{\text{sp}}$ (via des semi-polynômes en présentation dense)

Il s'agit d'une présentation qui augmente notablement l'ensemble des $\mathcal{P}$-points (par rapport à $\mathcal{C}_{\text{W}}$). Un élément de $\mathbf{Y}_{sp}$ représente une fonction polynomiale par morceaux (ou encore un semi-polynôme) donné "en présentation dense".
Plus précisément $\mathbf{Y}_{sp} \subset \mathbf{lst}(\mathbb{D}) \times \mathbf{lst}(\mathbb{D}[X])$, et les deux listes dans $\mathbf{lst}(\mathbb{D})$ et $\mathbf{lst}(\mathbb{D}[X])$ sont assujetties aux conditions suivantes :
— la liste $(x_i)_{0\leq i\leq t}$ de points rationnels dyadiques est ordonnée par ordre croissant :

$$0 = x_0 < x_1 < x_2 < \cdots < x_{t-1} < x_t = 1$$

— la liste $(P_i)_{1\leq i\leq t}$ dans $\mathbf{lst}(\mathbb{D}[X])$ vérifie $P_i(x_i) = P_{i+1}(x_i)$ pour $1 \leq i \leq t-1$.
Le point rationnel $f = ((x_i)_{0\leq i\leq t}, (P_i)_{1\leq i\leq t})$ définit la fonction continue $\widetilde{f}$ qui coïncide avec P_i sur l'intervalle $[x_{i-1}, x_i]$.
La présentation $\mathcal{C}_{\text{sp}}$ de $\mathbf{C}[0,1]$ est clairement de classe $\mathcal{P}$. La proposition suivante se démontre comme la proposition 5.1.2.

Proposition 5.1.4
— *L'identité de $\mathbf{C}[0,1]$ de $\mathcal{C}_{\text{W}}$ vers $\mathcal{C}_{\text{sp}}$ est* **LINTIME**.
— *L'identité de $\mathbf{C}[0,1]$ de $\mathcal{C}_{\text{sp}}$ vers $\mathcal{C}_{\text{W}}$ n'est pas de classe $\mathcal{P}$.*

5.1.3 Présentation $\mathcal{C}_{\text{sfrac}}$ (via des semi-fractions rationnelles contrôlées et données en présentation par formule)

L'ensemble des points rationnels $\mathbf{Y}_{sfrac}$ est maintenant l'ensemble (codant) des fonctions rationnelles par morceaux (ou semi-fractions rationnelles) à coefficients dyadiques et convenablement contrôlées. Plus précisément, $\mathbf{Y}_{sfrac} \subset \mathbf{lst}(\mathbb{D}) \times \mathbf{lst}(\mathbb{D}[X]_f \times \mathbb{D}[X]_f)$, et les deux listes dans $\mathbf{lst}(\mathbb{D})$ et $\mathbf{lst}(\mathbb{D}[X] \times \mathbb{D}[X]_f))$ sont assujetties aux conditions suivantes :
— la liste $(x_i)_{0\leq i\leq t}$ de points rationnels dyadiques est ordonnée par ordre croissant :

$$0 = x_0 < x_1 < x_2 < \cdots < x_{t-1} < x_t = 1$$

— chaque couple (P_i, Q_i) $(1 \leq i \leq t$ de la 2ème liste représente une fraction rationnelle $R_i = P_i/Q_i$ avec son dénominateur minoré par 1 sur l'intervalle $[x_{i-1}, x_i]$.
— la liste $(R_i)_{1\leq i\leq t}$ vérifie $R_i(x_i) = R_{i+1}(x_i)$ pour $1 \leq i < t$. Le point rationnel $f = ((x_i)_{0\leq i\leq t}, (R_i)_{1\leq i\leq t})$ définit la fonction continue $\widetilde{f}$ qui coïncide avec R_i sur l'intervalle $[x_{i-1}, x_i]$.
La présentation $\mathcal{C}_{\text{sfrac}}$ de $\mathbf{C}[0,1]$ est clairement de classe $\mathcal{P}$.

5.2 Résultats concernant la présentation à la Weierstrass

Les résultats de cette section sont essentiellement dans [21] et [22].
Avant de caractériser les $\mathcal{P}$-points de $\mathcal{C}_{\text{W}}$, il nous faut rappeler quelques résultats classiques de la théorie de l'approximation uniforme par des polynômes.

Attention ! Vu la manière usuelle dont est formulée la théorie de l'approximation, on utilisera l'intervalle $[-1, 1]$ pour donner les résultats et les preuves concernant $\mathcal{C}_{\text{W}}$.

5.2.1 Quelques définitions et résultats de la théorie de l'approximation uniforme par des polynômes

Voir par exemple [32] et [10].

Notation 5.2.1 $\mathbf{C}[a,b]$ est l'espace des fonctions réelles continues sur le segment $[a,b]$.

$\mathbf{C}$ est l'espace $\mathbf{C}[-1,1]$, la norme uniforme sur cet intervalle est notée $\| f \|_\infty$ et la distance correspondante d_∞.

$\mathbf{C}^{(k)}$ est l'espace des fonctions k fois continûment dérivables sur $[-1,1]$.

$\mathbf{C}^{(\infty)}$ est l'espace des fonctions indéfiniment dérivables sur $[-1,1]$.

$\mathbf{P}_n$ est l'espace des polynômes de degré $\leq n$.

T_n est le polynôme de Chebyshev de degré n :

$$\mathrm{T}_n(\varphi(z) = \varphi(z^n) \text{ avec } \varphi(z) = \frac{1}{2}(z + 1/z)$$

on peut également les définir par $\mathrm{T}_n(\cos(x)) = \cos(nx)$ ou par

$$F(u,x) = \frac{1 - u.x}{1 - u^2 - 2u.x} = \sum_{n=0}^{\infty} \mathrm{T}_n(x)u^n$$

On note : $E_n(f) = d_\infty(f, \mathbf{P}_n)$ pour $f \in \mathbf{C}$.

On considère sur $\mathbf{C}$ le produit scalaire

$$\langle g, h\rangle := \int_{-1}^{1} \frac{g(x).h(x)}{\sqrt{1-x^2}}dx = \int_0 \pi g(\cos(x))h(\cos(x))dx$$

On notera $\| f \|_2$ la norme au sens de ce produit scalaire. Les polynômes $(\mathrm{T}_i)_{0\leq i\leq n}$ forment une base orthogonale de $\mathbf{P}_n$ pour ce produit scalaire, avec

$$\langle \mathrm{T}_0, \mathrm{T}_0\rangle = \pi \text{ et } \langle \mathrm{T}_i, \mathrm{T}_i\rangle = \pi/2 \text{ pour } i > 0.$$

On note

$$A_k = A_k(f) := \frac{2}{\pi}\int_{-1}^{1} f(x).\mathrm{T}_k(x)\frac{dx}{\sqrt{(1-x^2)}} = \frac{2}{\pi}\int_0^{\pi} \cos(kx)f(\cos(x))dx$$

Les A_k sont appelés les *coefficients de Chebyshev* de f.

La fonction

$$S_n(f) := A_0/2 + \sum_{i=1}^{n} A_i\mathrm{T}_i = {\sum_{i=1..n}}' A_i\mathrm{T}_i$$

est la projection orthogonale de f sur $\mathbf{P}_n$ au sens du produit scalaire considéré.

La série correspondante est appelée *la série de Chebyshev* de f [13].

On note : $S_n(f) = \| f - s_n(f) \|_\infty$, on a immédiatement $| A_{n+1} | \leq S_n(f) + S_{n+1}(f)$.

[13] Elle converge au sens de L^2 pour le produit scalaire considéré. La série de Chebyshev est aux fonctions continues sur $[-1,1]$ ce que la série de Fourier est aux fonctions continues périodiques, ce qui se comprend bien en considérant le "changement de variable" $z \mapsto 1/2(z + 1/z)$ qui transforme le cercle unité du plan complexe en le segment $[-1,1]$ et la fonction $z \mapsto z^n$ en le polynme T_n.

Les zéros de T_n sont les

$$\xi_i^{[n]} = \cos(\frac{2i-1}{n} \cdot \frac{\pi}{2}) \quad i = 1, 2, \ldots, n$$

et on a

$$\mathrm{T}_n(x) = 2^{n-1} \prod_{i=1}^{n} (x - \xi_i^{[n]}) \ \text{(pour } n \geq 1)$$

Les extrema de T_n sur $[-1,1]$ sont égaux à ± 1 et obtenus aux points

$$\eta_i^{[n]} = \cos(\frac{i}{n} \cdot \pi) \quad i = 0, 1, \ldots, n$$

Des valeurs approchées de $s_n(f)$ peuvent être calculées au moyen de formules d'interpolation : on pose

$$\alpha_k^{[m]} = \frac{2}{m} {\sum_{i=1..m}}' f(\xi_i^{[m]}) \mathrm{T}_k(\xi_i^{[m]}), \quad u_n^{[m]} = \sum_{k=1}^{n} \alpha_k^{[m]} \mathrm{T}_k(x)$$

et on a : $u_n^{[n+1]}$ est le polynôme qui interpole f aux zéros de T_n

La théorie de l'approximation uniforme par des polynômes établit des liens étroits entre "être suffisamment bien approchable par des polynômes" et "être suffisamment régulière".

5.2.2 Quelques résultats classiques

Évaluation d'un polynome $\sum_{k=0}^{n} A_k \mathrm{T}_k$
Les formules récurrentes $\mathrm{T}_{m+1}(x) = 2x\mathrm{T}_m(x) - \mathrm{T}_{m-1}(x)$ conduisent à un algorithme à la Horner :

$$B_{n+1} = B_{n+2} = 0, \ B_k = 2xB_{k+1} - B_{k+2} + A_k, \ p(x) = \frac{B_0 - B_2}{2}$$

Théorème de Markov
Si $g \in \mathbf{P}_n$ alors

$$\| g' \|_\infty \leq n^2 \| g \|_\infty \tag{1}$$

et pour $k \geq 2$

$$\| g^{(k)} \|_\infty \leq \mathrm{T}_n^{(k)}(1) \| g \|_\infty = \frac{n^2(n^2-1)\cdots(n^2-(k-1)^2)}{1.3.5\cdots(2k-1)} \| g \|_\infty \tag{2}$$

Comparaison de $E_n(f)$ et $S_n(f)$

$$E_n(f) \leq S_n(f) \leq (4 + \frac{4}{\pi^2} \log(n)) E_n(f) \tag{3}$$

Comparaison de $E_n(f)$ et $A_{n+1}(f)$
Pour $n \geq 1$ on a

$$\int_{-1}^{1} \frac{| \mathrm{T}_n(x) |}{\sqrt{1-x^2}} dx = 2$$

d'où on déduit

$$(\pi/4) \mid A_{n+1}(f) \mid \leq E_n(f) \tag{4}$$

Théorèmes de Jackson
Soit $f \in \mathbf{C}$. Pour tout entier $n \geq 1$ on a

$$E_n(f) \leq \pi\lambda/(2n+2) \quad \text{si} \quad \mid f(x) - f(y) \mid \leq \lambda \mid x - y \mid \tag{5}$$

$$E_n(f) \leq (\pi/2)^k \parallel f^{(k)} \parallel_\infty /[(n+1)(n)(n-1)\cdots(n-k+2)] \quad \text{si } f \in \mathbf{C}^{(k)} \text{ et } n \geq k \tag{6}$$

Convergence de la série de Chebyshev d'une fonction
La série de Chebyshev d'une fonction $f \in \mathbf{C}^{(k)}$ converge uniformément vers f si $k \geq 1$, et elle est absolument convergente (pour la norme $\parallel f \parallel_\infty$) si $k \geq 2$.

$$S_n(f) = \parallel s_n(f) - f \parallel_\infty \leq \sum_{j=n+1}^{\infty} \mid A_j \mid \tag{7}$$

et (cf. [32] théorème 3.12 p.182)

$$\parallel s_n(f) - u_n^{[n+1]} \parallel_\infty \leq \sum_{j=n+2}^{\infty} \mid A_j \mid \tag{8}$$

Approximation uniforme des fonctions dans $\mathbf{C}^{(\infty)}$ par des polynômes
Les propriétés suivantes sont équivalentes.

(i) $\forall k \;\; \exists M > 0 \;\; \forall n > 0 \;\; E_n(f) \leq M/n^k$

(ii) $\forall k \;\; \exists M > 0 \;\; \forall n > 0 \;\; S_n(f) \leq M/n^k$

(iii) $\forall k \;\; \exists M > 0 \;\; \forall n > 0 \;\; \mid A_n(f) \mid \leq M/n^k$

(iv) $\forall k \;\; \exists M > 0 \;\; \forall n > 0 \;\; \parallel u_n^{[n+1]} - f \parallel_\infty \leq M/n^k$

(v) La fonction f est de classe $\mathcal{C}^\infty$ (i.e., $f \in \mathbf{C}^{(\infty)}$)

Preuve. (i) et (ii) sont équivalents d'après (3).
(iv)⇒ (i) trivialement.
(ii) ⇒ (iii) parce que $\mid A_n(f) \mid \leq S_n(f) + S_{n-1}(f)$
(iii) ⇒ (iv) d'après (7) et (8).
(iii) ⇒ (v) : la série $\sum' A_i \mathrm{T}_i^{(h)}$ est absolument convergente d'après (2) et les majorations (iii) ; donc on peut dériver h fois terme à terme la série de Chebyshev
(v) ⇒ (i) d'après (6). ∎

Analyticité et approximation uniforme par des polynômes
Les propriétés suivantes sont équivalentes

(i) $\exists M > 0, \;\; r < 1 \;\; \forall n > 0 \;\; E_n(f) \leq Mr^n$

(ii) $\exists M > 0, \;\; r < 1 \;\; \forall n > 0 \;\; S_n(f) \leq Mr^n$

(iii) $\exists M > 0, \;\; r < 1 \; \forall n > 0 \;\; \mid A_n(f) \mid \leq Mr^n$

(iv) $\exists M > 0, \;\; r < 1 \;\; \forall n > 0 \;\; \parallel u_n^{[n+1]} - f \parallel_\infty \leq Mr^n$

(v) $\exists r < 1$ telle que f est analytique dans le plan complexe à l'intérieur de l'ellipse $\mathcal{E}_\rho$ de foyers 1, −1 et dont le demi-somme des diamètres principaux est égale à $\rho = 1/r$

(vi) $\exists M > 0, \;\; R > 1 \;\; \forall n \;\; \parallel f^{(n)} \parallel_\infty \leq MR^n n!$

(vii) f est analytique sur l'intervalle $[-1, 1]$.

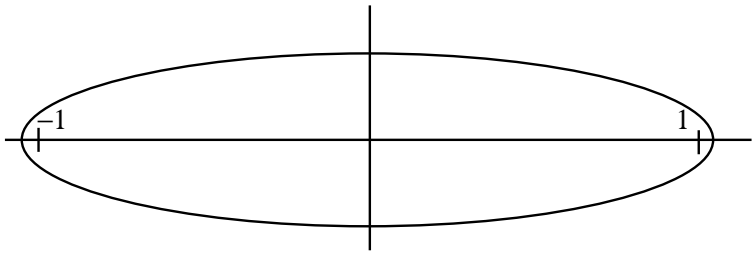

FIG. 5: L'ellipse $\mathcal{E}_\rho$

En outre la limite inférieure des valeurs de r possibles est la même dans les 5 premiers cas[14].

Remarques 5.2.2
1) L'espace des fonctions analytiques sur un intervalle compact possède donc une bonne description constructive, en termes de série de Chebyshev par exemple. Il apparaît comme une réunion dénombrable emboîtée d'espaces métriques complets (ceux obtenus en utilisant la définition (iii) et en fixant M et r rationnels par exemple). L'espace des fonctions $\mathbf{C}^{(\infty)}$ est beaucoup plus difficile à décrire constructivement, essentiellement parce qu'il n'existe pas de manière agréable d'engendrer les suites de rationnels à décroissance rapide[15].
2) La condition (i) peut être également lue comme suit : la fonction f peut être approchée à $1/2^n$ (pour la norme uniforme) par un polynôme de degré $\leq c.n$, où c est une constante fixée, c.-à-d. encore : il existe un entier h tel que $E_{hn}(f) \leq 1/2^n$.
Même remarque pour les conditions (ii), (iii) et (iv). Cela implique que la fonction f peut être approchée à $1/2^n$ par un polynôme à coefficients dyadiques dont la taille (en présentation dense sur la base des X^n ou sur la base des T_n) est en $\mathrm{O}(n^2)$. La taille de la somme des valeurs absolues des coefficients est, elle, en $\mathrm{O}(n)$. Bakhvalov (cf [2] chap IV 8 Th. p. 233) donne une condition suffisante du même genre pour qu'une fonction f soit analytique dans une lentille d'extrémités -1 et 1 du plan complexe (et non plus dans un voisinage du segment) : il suffit que la somme des valeurs absolues des coefficients d'un polynôme donnant f à $1/2^n$ près soit majorée par $M2^{qn}$ (où M et q sont des constantes fixées). C.-à-d. encore : la taille de la somme des valeurs absolues des coefficients d'un polynôme approchant f à $1/2^n$ est en $\mathrm{O}(n)$.

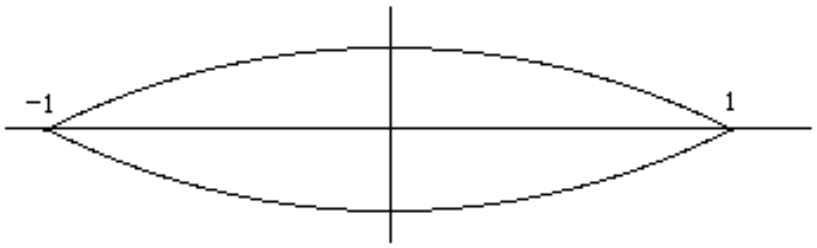

FIG. 6: La lentille de Bakhvalov

[14] Les équivalences (i) ... (iv) se montrent comme pour la proposition précédente. Pour l'équivalence avec (v) voir par exemple [32]. La condition (vi) représente à très peu près l'analyticité dans l'ouvert U_R formé des points dont la distance à l'intervalle est inférieure à $1/R$.

[15] Cela tient au $\forall k\ \exists M$ dans la définition de la décroissance rapide. Cette alternance de quantificateurs prend une forme explicite lorsqu'on donne M en fonction de k explicitement. Mais, en vertu de l'argument diagonal de Cantor, il n'y a pas de manière effective d'engendrer les fonctions effectives de $\mathbb{N}$ vers $\mathbb{N}$.

Classe de Gevrey et approximation uniforme par des polynômes
Si f est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{W}}$ donné par une suite $m \mapsto P_m$ $\mathcal{P}$-calculable (avec $\| f - P_m \|_\infty \leq 2^m$), alors le degré de P_m est majoré par un polynôme en m, donc il existe un entier k et une constante B telles que le degré de P_m soit majoré par $(Bm)^k$. Soit alors n arbitraire, et considérons le plus grand entier m tel que $(Bm)^k \leq n$, c.-à-d. $m := Ent(\sqrt[k]{n}/B)$. On a donc $m+1 \geq \sqrt[k]{n}/B$. En posant $r := 1/2^{1/B}$ et $\gamma := 1/k$, on obtient :

$$E_n(f) \leq 1/2^m \leq 2.r^{n^\gamma}, \text{ avec } r \in]0,1[,\ \gamma > 0.$$

En particulier, la suite $E_n(f)$ est à décroissance rapide et $f \in \mathbf{C}^{(\infty)}$. Ceci nous amène à étudier les fonctions f pour lesquelles ce genre de majoration est obtenu.

Définition 5.2.3 *(classe de Gevrey[16])* Une fonction $f \in \mathbf{C}^{(\infty)}$ est dite dans la classe de Gevrey d'ordre $\alpha > 0$ si ses dérivées vérifient une majoration :

$$\| f^{(n)} \|_\infty \ MR^n n^{\alpha n}$$

La classe de Gevrey est obtenue lorsqu'on ne précise pas l'ordre α.

Théorème 5.2.4 *Soit $f \in \mathbf{C}$. Les propriétés suivantes sont équivalentes.*

(i) $\exists M > 0,\ r < 1,\ \gamma > 0\ \forall n > 0\ E_n(f) \leq Mr^{n^\gamma}$
(ii) $\exists M > 0,\ r < 1,\ \gamma > 0\ \forall n > 0\ S_n(f) \leq Mr^{n^\gamma}$
(iii) $\exists M > 0,\ r < 1,\ \gamma > 0\ \forall n > 0\ \ | A_n(f) | \leq Mr^{n^\gamma}$
(iv) $\exists M > 0,\ r < 1\ \forall n > 0\ \| u_n^{[n+1]} - f \|_\infty \leq Mr^{n^\gamma}$
(j) $\exists c, \beta > 0\ \forall n > 0\ \forall m \geq cn^\beta\ E_m(f) \leq 1/2^n$
(jj) $\exists c, \beta > 0\ \forall n > 0\ \forall m \geq cn^\beta\ S_m(f) \leq 1/2^n$
(jjj) $\exists c, \beta > 0\ \forall n > 0\ \forall m \geq cn^\beta\ \ | A_m(f) | \leq 1/2^n$
(jw) $\exists c, \beta > 0\ \forall n > 0\ \forall m \geq cn^\beta\ \ \| u_m^{[m+1]} - f \|_\infty \leq 1/2^n$
(k) *f est dans la classe de Gevrey.*

Preuve. (i) ⇔ (ii) à partir de l'équation (3).
(i) ⇒ (iii) à partir de l'équation (4).
(iv) ⇒ (i) est triviale.
Les 4 équivalences du type (i) ⇔ (j) résultent du même genre de calcul que celui qui a été fait avant le théorème.
L'implication (jjj) ⇒ (jw) résulte d'un calcul de majoration simple utilisant les équations (7) et (8).
Supposons (k), c.-à-d. que f soit Gevrey d'ordre α, et montrons (i). Le problème de majoration n'est délicat que pour $\alpha \geq 1$, ce qu'on supposera maintenant. En appliquant le théorème de Jackson, on obtient une majoration $E_n(f) \leq \pi^k \| f^{(k)} \|_\infty / n^k$ dès que $n \geq 2k$, ce qui donne avec la majoration de Gevrey $E_n(f) \leq A(Ck^\alpha/n)^k$. On peut supposer $C^{1/\alpha} \geq 2$ et on prend pour k un entier proche de $(n/2C)^{1/\alpha}$ $(\leq n/2)$, d'où à très peu près :

$$E_n(f) \leq A(1/2)^{(n/2C)^{1/\alpha}} = Ar^{n^\gamma}, \text{ avec } \gamma = 1/\alpha.$$

Supposons maintenant que f vérifie (j) et montrons que f est Gevrey.
Le problème de majoration n'est délicat que pour $\beta \geq 1$, ce qu'on supposera maintenant. On

[16] Cf. par exemple Hörmander [14] : The Analysis of Linear Partial Differential Operators I p 281 (Springer 1983). Une fonction est Gevrey d'ordre 1 si et seulement si elle est analytique.

écrit $f^{(k)} = \sum' A_m \mathrm{T}_m^{(k)}$. D'où $\| f^{(k)} \|_\infty \leq \sum' | A_m | m^{2k}$ d'après le théorème de Markov. On utilise maintenant la majoration (jjj). On prend c et β entiers pour simplifier (ce n'est pas une restriction). Dans la somme ci-dessus, on regroupe les termes pour m compris entre cn^β et $c(n+1)^\beta$. Dans le paquet obtenu, on majore chaque terme par $(1/2^n)m^2k$, et on majore le nombre de termes par $c(n+1)b$, d'où :

$$\| f^{(k)} \|_\infty \leq \sum_n (c(n+1)^\beta/2^n)(c(n+1)^\beta)^{2k} \leq 2c^{2k+1} \sum_n (n+1)^{\beta(2k+1)}/2^n$$

$$\leq 4c^{2k+1} \sum_n n^h/2^n \text{ où } h = \beta(2k+1)$$

On majore cette série par la série obtenue en dérivant h fois la série $\sum_n x^n$ (puis en faisant $x = 1/2$) et on obtient que f est Gevrey d'ordre 2β. ∎

Remarques 5.2.5
1) L'espace des fonctions Gevrey possède donc une présentation constructive agréable.
2) Pour $\gamma = 1$ on obtient les fonctions analytiques. Pour $\gamma > 1$, on obtient des fonctions entières.
3) Pour $\gamma \leq 1$, la limite supérieure des γ possibles est la même dans (i), (ii), (iii) et (iv), la limite inférieure des β possibles est la même dans (j), (jj), (jjj) et (jw), avec $\gamma = 1/\beta$.
4) Si on se base sur le cas des fonctions analytiques ($\alpha = \beta = \gamma = 1$), on peut espérer, pour l'implication (j) $\Rightarrow$ (k), obtenir que f soit Gevrey d'ordre β au moyen d'un calcul de majoration plus sophistiqué.
5) Dans (j), (jj), (jw) on peut supprimer le quantificateur $\forall m$ si on prend c et β entiers et $m = cn^\beta$.

5.2.3 Retour aux questions de complexité dans l'espace $\mathcal{C}_\mathrm{W}$

Nous commençons par une
Remarque importante : en ce qui concerne $\mathbb{D}[X]$, la présentation dense ordinaire (sur la base des X^n) et la présentation dense sur la base des polynômes de Chebyshev T_n, sont équivalentes en temps polynomial. Nous utiliserons indifféremment l'une ou l'autre des deux bases, selon la commodité du moment.

Rappelons également que la norme $P \to \| P \|_\infty$ est une fonction $\mathcal{P}$-calculable de $\mathbb{D}[X]$ vers $\mathbb{R}$.

La preuve de la proposition suivante est immédiate. En fait toute fonctionnelle définie sur $\mathcal{C}_\mathrm{W}$ qui a un module de continuité uniforme polynomial et dont la restriction à $\mathbb{D}[X]$ est "facile à calculer" est elle même "facile à calculer". Cette proposition prend toute sa valeur au vu du théorème de caractérisation 5.2.7.

Proposition 5.2.6 (bon comportement des fonctionnelles usuelles)
Les fonctionnelles :

$$\mathcal{C}_\mathrm{W} \to \mathbb{R} \quad f \mapsto \| f \|_\infty,\ \| f \|_2,\ \| f \|_1$$

sont des fonctions uniformément de classe $\mathcal{P}$. Les fonctionnelles :

$$\mathcal{C}_\mathrm{W} \times [0,1] \times [0,1] \to \mathbb{R} \quad (f,a,b) \mapsto \sup_{x \in [a,b]} (f(x)),\ \int_a^b f(x)dx$$

sont des fonctions uniformément de classe $\mathcal{P}$.

Théorème 5.2.7 (caractérisation des $\mathcal{P}$-points de $\mathcal{C}_{\mathrm{W}}$)
Soit $f \in \mathbf{C}$. Les propriétés suivantes sont équivalentes.
a) la fonction f est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{KF}}$ et est dans la classe de Gevrey
b) la suite $A_n(f)$ est une $\mathcal{P}$-suite dans $\mathbb{R}$ et vérifie une majoration $\mid A_n(f) \mid \leq Mr^{n^\gamma}$ avec $M > 0, \gamma > 0, 0 < r < 1$.
c) la fonction f est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{W}}$.

Preuve. Les implications (c) ⇒ (a) et (c) ⇒ (b) sont faciles à partir du théorème 5.2.4.
(b) ⇒ (c) : Un polynôme (en présentation dense sur la base des T_n) approchant f avec la précision $1/2^{n+1}$ est obtenu avec la somme partielle extraite de la série de Chebyshev de f en s'arrêtant à l'indice $(Bn)^h$ (où B et h se calculent à partir de M et γ). Il reste à remplacer chaque coefficient de Chebyshev par un dyadique l'approchant avec la précision :

$$1/[(Bn)^h 2^{n+1}] = 1/2^{n+1+h\log_2(Bn)}.$$

(a) ⇒ (c) : Un polynôme approchant f avec la précision $1/2^{n+1}$ est obtenu avec $u_m^{[m+1]}$, (où $m = (Cn)^k$, C et k se calculent à partir de M et γ, en tenant compte des équations (7) et (8). La formule définissant $u_m^{[m+1]}$ fournit ses coefficients sur la base des T_n et on peut calculer (en temps polynomial) une approximation à $1/2^{n+1+k\log_2(Cn)}$ près de ces coefficients en profitant du fait que la suite double $\xi_i^{[n]}$ est une $\mathcal{P}$-suite de réels et que la fonction f est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{KF}}$. ∎

Une conséquence immédiate du théorème précédent est obtenue dans le cas des fonctions analytiques.

Théorème 5.2.8 *Soit $f \in \mathbf{C}$. Les propriétés suivantes sont équivalentes.*

(a) la fonction f est une fonction analytique et c'est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{KF}}$

(b) la suite $A_n(f)$ est une $\mathcal{P}$-suite dans $\mathbb{R}$ et vérifie une majoration

$$\mid A_n(f) \mid \leq Mr^n \ (M > 0,\ r < 1)$$

(c) la fonction f est une fonction analytique et est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{W}}$

Définition 5.2.9 *(fonctions $\mathcal{P}$-analytiques)*
Lorsque ces propriétés sont vérifiées, on dira que la fonction f est $\mathcal{P}$-analytique sur l'intervalle $[-1, 1]$.

Théorème 5.2.10 (assez bon comportement de la dérivation vis à vis de la complexité)
Soit f un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{W}}$. Alors la suite $k \mapsto f^{(k)}$ est une $\mathcal{P}$-suite de $\mathcal{C}_{\mathrm{W}}$. Plus généralement, si (f_p) est une $\mathcal{P}$-suite de $\mathcal{C}_{\mathrm{W}}$ alors la suite double $(f_p^{(k)})$ est une $\mathcal{P}$-suite de $\mathcal{C}_{\mathrm{W}}$.

Preuve. Nous donnons la preuve pour la première partie de la proposition. Elle s'appliquerait sans changement pour le cas d'une $\mathcal{P}$-suite de $\mathcal{C}_{\mathrm{W}}$.
La fonction f est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{W}}$ donné comme limite d'une suite $n \mapsto P_n$, $\mathcal{P}$-calculable. La suite double $P_n(k)$ est $\mathcal{P}$- calculable (entrées en unaire). Il existe deux entiers a et b tels que le degré de $\mathbf{P}_n$ soit majoré par $2^a n^b$. Donc, d'après le théorème de Markov (equation (1)) on a la majoration :

$$\| P_n^{(k)} - P_{n-1}^{(k)} \|_\infty \leq (2^a n^{2b})^k \| P_n - P_{n-1} \|_\infty \leq (2^a n^{2b})^k / 2^{n-2} = 1/2^{n-(k.(a+2b\log_2(n))+2)}$$

On détermine alors aisément une constante n_0 telle que, pour $n \geq 2n_0 k$, on ait :

$$n \geq 2(k.(a + 2b\log_2(n)) + 2)$$

et donc

$$\| P_n^{(k)} - P_{n-1}^{(k)} \|_\infty \leq 1/2^{n/2}$$

de sorte qu'en posant $\nu(n) := 2\sup(n_0 k, n)$, on a, pour $q \geq \nu(n)$,

$$\| P_q^{(k)} - P_{q+1}^{(k)} \|_\infty \leq 1/2^n$$

et donc, puisque $\nu(n+1) = \nu(n)$ ou $\nu(n)+2$,

$$\| P_{\nu(n)}^{(k)} - P_{\nu(n+1)}^{(k)} \|_\infty \leq 1/2^{n-1}$$

d'où enfin :

$$\| P_{\nu(n)}^{(k)} - f^{(k)} \|_\infty \leq 1/2^{n-2}$$

On termine en notant que la suite double $(n,k) \mapsto P_{\nu(n+2)}^{(k)}$ est $\mathcal{P}$-calculable. ∎

Corollaire 5.2.11 *Si f est un $\mathcal{P}$-point de $\mathcal{C}_{\mathrm{W}}$ et a, b deux $\mathcal{P}$-points de $[-1,1]$, alors les suites*

$$\| f^{(n)} \|_\infty,\ \| f^{(n)} \|_2,\ \| f^{(n)} \|_1,\ f^{(n)}(a) \text{et } \sup_{x\in[a,b]} (f^{(n)}(x))$$

sont des $\mathcal{P}$-suites dans $\mathbb{R}$.
Plus généralement, si (f_p) est une $\mathcal{P}$-suite de $\mathcal{C}_{\mathrm{W}}$ alors les suites doubles

$$\| f_p^{(n)} \|_\infty,\ \| f_p^{(n)} \|_2,\ \| f_p^{(n)} \|_1,\ f_p^{(n)}(a) \text{ et } \sup_{x\in[a,b]} (f_p^{(n)}(x))$$

sont des $\mathcal{P}$-suites dans $\mathbb{R}$.

La preuve du théorème 5.2.10 (et donc du corollaire 5.2.11) est en quelque sorte uniforme et a une signification plus générale. Nous allons maintenant définir le cadre naturel dans lequel s'applique ce théorème et donner le nouvel énoncé, plus général et plus satisfaisant.

Définition 5.2.12 Pour c et $\beta > 0$ on note $\mathbf{Gev}_{c,\beta}$ la classe des fonctions Gevrey vérifiant la majoration (du type (jjj) dans 5.2.4)

$$\forall m > cn^\beta \quad | A_m(f) | \leq 1/2^n$$

C'est une partie convexe fermée de $\mathbf{C}$. Pour c et β entiers, on note $\mathbf{Y}_{\mathbf{Gev}_{c,\beta}}$ les éléments de $\mathbb{D}[X]$ qui sont dans la classe $\mathbf{Gev}_{c,\beta}$. Cet ensemble $\mathbf{Y}_{\mathbf{Gev}_{c,\beta}}$ peut être pris pour ensemble des points rationnels d'une présentation $\mathbf{C}_{\mathbf{Gev},c,\beta}$ rationnelle de $\mathbf{Gev}_{c,\beta}$.

On notera que le test d'appartenance à la partie $\mathbf{Y}_{\mathbf{Gev}_{c,\beta}}$ de $\mathbb{D}[X]$ est en temps polynomial, puisque les $A_m(f)$ pour un polynôme f sont ses coefficients sur la base de Chebyshev. Dans ce nouveau cadre, le théorème 5.2.10 admet une formulation plus uniforme et plus efficace.

Théorème 5.2.13 *Chaque fonctionnelle $f \mapsto f^{(n)}$ est une fonction uniformément de classe $\mathcal{P}$ de $\mathbf{C}_{\mathbf{Gev}_{c,\beta}}$ vers $\mathcal{C}_{\mathrm{W}}$. Plus précisément la suite de fonctionnelles*

$$(k,f) \mapsto f^{(k)} \ :\ \mathbb{N}_1 \times \mathbf{C}_{\mathbf{Gev}_{c,\beta}} \to \mathcal{C}_{\mathrm{W}}$$

est uniformément de classe $\mathcal{P}$ (au sens de la définition 2.2.9).

Preuve. La suite double $(k,f) \mapsto f^{(k)}$ est de faible complexité en tant que fonction de $\mathbb{N}_1 \times \mathbb{D}[X]$ vers $\mathbb{D}[X]$ donc aussi en tant que fonction de $\mathbb{N}_1 \times \mathbf{Y}_{\mathbf{Gev},\beta}$ vers $\mathbb{D}[X]$.
Tout le problème est donc de montrer que l'on a un module de continuité uniforme polynomial (au sens de 2.2.9). Nous devons calculer une fonction $\mu(k,h)$ telle que l'on ait pour tous f et g dans $\mathbf{Y}_{\mathbf{Gev},\beta}$:

$$\| f-g \|_\infty \leq 1/2^{\mu(k,h)} \Rightarrow \| f^{(k)} - g^{(k)} \|_\infty \leq 1/2^h$$

Ce calcul de majoration est assez proche de celui qui a été fait dans la preuve du théorème 5.2.10. On écrit

$$\| f^{(k)} - g^{(k)} \|_\infty \leq \| f^{(k)} - s_n(f)^{(k)} \|_\infty + \| g^{(k)} - s_n(g)^{(k)} \|_\infty + \| s_n(f-g)^{(k)} \|_\infty$$

Dans la somme du second membre les deux premiers termes sont majorés comme suit

$$\| f^{(k)} - s_n(f)^{(k)} \|_\infty \leq \sum_{q>n} | A_q(f) | \| T_q^{(k)} \|_\infty \leq \sum_{q>n} | A_q(f) | q^{2k}$$

Comme on a : $\forall q > cn^\beta \ \ | A_q(f) | \leq 1/2^n$, $\sum_{q>n} | A_q(f) | q^{2k}$ est "bien" convergente et on peut expliciter un $\alpha(k,h)$ polynomial en k,h tel que (voir l'explicitation en fin de preuve),

$$\text{avec } n = \alpha(k,h) \ \ \forall f \in \mathbf{Y}_{\mathbf{Gev},c,\beta} \ : \ \sum_{q>n} | A_q(f) | q^{2k} \leq 1/2^{h+2}$$

Une fois fixé $n = \alpha(k,h)$ il nous reste à rendre petit le terme $\| s_n(f-g)^{(k)} \|_\infty$. Le théorème de Markov (formule (2)) implique que

$$\| s_n(f-g)^{(k)} \|_\infty \leq \| s_n(f-g) \|_\infty \, n^{2k}$$

Il ne reste plus qu'à obtenir une majoration convenable de $\| s_n(f-g) \|_\infty$ à partir de $\| f-g \|_\infty$. Par exemple, on peut utiliser la majoration $S_n(f) \leq (4+\log(n))E_n(f)$ (d'après la formule (3)) d'où

$$\| f^{(k)} \|_\infty \leq \| f \|_\infty + S_n(f) \leq \| f \|_\infty + (4+\log(n))E_n(f) \leq (5+\log(n)) \| f \|_\infty$$

Donnons pour terminer l'explicitation de $\alpha(k,h)$. On a les inégalités

$$\sum_{q \geq cn_0^\beta} | A_q(f) | q^{2k} \leq \sum_{n \geq n_0} \sum_{q \leq c(n+1)^\beta} q^{2k}/2^n \leq \sum_{n \geq n_0} c(n+1)^\beta (c(n+1)^\beta)^{(}2k)/2^n$$

donc

$$\sum_{q \geq cn_0^\beta} | A_q(f) | q^{2k} \leq \sum_{n \geq n_0} (c(n+1)^\beta)^{2k+1}/2^n \leq \sum_{n \geq n_0} 1/2^{\varphi(n,\beta,c,k)}$$

avec, si $2^a \geq c$

$$\varphi(n,\beta,c,k) \geq n - (2k+1)a - (2k+1)\beta \log_2(n+1)$$

Si on a

$$\text{pour } n \geq n_0 \quad \varphi(n,\beta,c,k) \geq h + n/2 + 4 \ (\star)$$

on obtient

$$\sum_{q \geq cn_0^\beta} | A_q(f) | q^{2k} \leq \sum_{n \geq n_0} 1/2^{\varphi(n,\beta,c,k)} \leq (1/2^{h+2}(1/4) \sum_{n \geq n_0} 1/2^{n/2} \leq 1/2^{h+2}$$

Et on peut prendre $\alpha(k,h) = cn_0^\beta$.
Il reste à voir comment on peut réaliser la condition $(\star)$.
Pour tout entier b on a un entier $\nu(b) \leq \max(8, b^2)$ pour lequel

$$n > \nu(b) \;\Rightarrow\; n \geq b \log_2(n+1).$$

Si donc $n \geq \nu(4(2k+1)\beta)$ on obtient

$$\varphi(n,\beta,c,k) \geq n - (2k+1)a - (2k+1)\beta \log_2(n+1) \geq (3n/4) - (2k+1)a$$

et la condition $\varphi(n,\beta,c,k) \geq h + n/2 + 4$ est réalisée si $n/4 \geq (2k+1)a + h + 4$. D'où finalement $\alpha(h,k) = c \max(\nu(4(2k+1)\beta), 4((2k+1)a + h + 4))^\beta$. ∎

En appliquant la proposition 5.2.6, on obtient :

Corollaire 5.2.14 *i) Les trois suites de fonctionnelles*

$$(n,f) \mapsto \| f^{(n)} \|_\infty,\ \| f^{(n)} \|_2,\ \| f^{(n)} \|_1 \quad \mathbb{N}_1 \times \mathbf{C}_{\mathbf{Gev},c,\beta} \to \mathbb{R}$$

sont uniformément de classe $\mathcal{P}$ (au sens de la définition 2.2.9).
ii) La suite de fonctionnelles :

$$\mathbb{N}_1 \times (\mathbf{C}_{\mathbf{Gev},c,\beta} \times [-1,1]) \to \mathbb{R} \quad (f,x) \mapsto f^{(n)}(x)$$

est uniformément de classe $\mathcal{P}$.
iii) La suite de fonctionnelles :

$$\mathbb{N}_1 \times (\mathbf{C}_{\mathbf{Gev},c,\beta} \times [-1,1] \times [-1,1]) \to \mathbb{R} \quad (f,a,b)) \mapsto \sup_{x \in [a,b]} (f^{(n)}(x))$$

est uniformément de classe $\mathcal{P}$.

Remarque 5.2.15 Les théorèmes 5.2.7, 5.2.8, 5.2.10, 5.2.13, la proposition 5.2.6 et les corollaires 5.2.11 et 5.2.14 améliorent sensiblement les résultats de [15], [16] et [27] sur les fonctions analytiques calculables en temps polynomial (au sens de Ko-Friedman).

5.3 Comparaisons de différentes présentations de classe $\mathcal{P}$

Dans cette section, nous obtenons la chaîne suivante de fonctions uniformément de classe $\mathcal{P}$ pour l'identité de $\mathbf{C}[0,1]$.

$$\mathcal{C}_{\mathrm{W}} \to \mathcal{C}_{\mathrm{sp}} \to \mathcal{C}_{\mathrm{frac}} \equiv \mathcal{C}_{\mathrm{sfrac}} \to \mathcal{C}_{\mathrm{KF}}$$

et aucune des flèches $\to$ dans la ligne ci-dessus n'est une $\mathcal{P}$- équivalence sauf peut-être $\mathcal{C}_{\mathrm{sp}} \to \mathcal{C}_{\mathrm{frac}}$ et très éventuellement $\mathcal{C}_{\mathrm{frac}} \to \mathcal{C}_{\mathrm{KF}}$ (mais cela impliquerait $\mathcal{P} = \mathcal{NP}$). Tout d'abord, il est clair que l'identité de $\mathbf{C}[0,1]$ est de classe **LINTIME** pour les cas suivants :

$$\mathcal{C}_{\mathrm{W}} \to \mathcal{C}_{\mathrm{sp}};\ \mathcal{C}_{\mathrm{sp}} \to \mathcal{C}_{\mathrm{frac}};\ \mathcal{C}_{\mathrm{frac}} \to \mathcal{C}_{\mathrm{sfrac}}$$

Par ailleurs l'identité de $\mathbf{C}[0,1]$ est de classe $\mathcal{P}$ dans le cas suivant

$$\mathcal{C}_{\mathrm{frac}} \to \mathcal{C}_{\mathrm{caf}}$$

(en fait, seule le calcul de la magnitude n'est pas complètement trivial, et il est sûrement dans $\mathbf{DTIME}(\mathrm{O}(N^2))$). Il nous reste à montrer que l'identité de $\mathbf{C}[0,1]$ de $\mathcal{C}_{\mathrm{sfrac}}$ vers $\mathcal{C}_{\mathrm{frac}}$ est de classe $\mathcal{P}$.

Proposition 5.3.1 *L'identité de* $\mathbf{C}[0,1]$ *de* $\mathcal{C}_{\rm sp}$ *vers* $\mathcal{C}_{\rm frac}$ *est uniformément de classe* $\mathcal{P}$.

Preuve. Soit $n \in \mathbb{N}_1$ et $f \in \mathbf{Y}_{sp}$. On doit calculer un élément $g \in \mathbf{Y}_{frac}$ tel que

$$\| \widetilde{f} - \widetilde{g} \|_\infty \leq 1/2^n.$$

On a $f = ((x_0, x_1, \ldots, x_t), (P_1, P_2, \ldots, P_t))$ avec $P_i(x_i) = P_{i+1}(x_i)$ pour $i = 1, \ldots, t-1$.
On calcule $m \in \mathbb{N}_1$ tel que 2^m majore les $\| P_i \|_\infty$ et les $\| P_i' \|_\infty$.
On pose $p = m + n + 1$. Pour $i = 1, \ldots, t-2$ on considère la fonction $h_i := C_{p,z_i} - C_{p,z_{i+1}}$ avec $z_i = x_i - 1/2^{p+1}$:

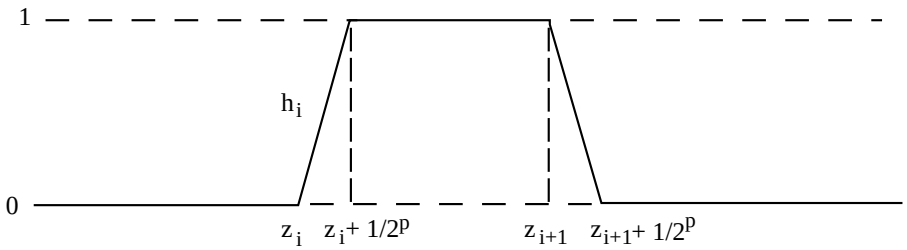

FIG. 7: La fonction h_i

Pour $i = 0$ $h_0 := -C_{p,z_1}$ et pour $i = t-1$ on a $h_{t-1} := -C_{p,z_{t-1}}$.
La fonction $\widetilde{f}$ est à très peu près égale à $h = \sum_i h_i P_{i+1}$: sur les intervalles $[z_i + 1/2^p, z_{i+1}]$ on a $h = \widetilde{f}$, tandis que sur un intervalle

$$[z_i, z_i + 1/2^p] = [x_i - 1/2^{p+1}, x_i + 1/2^{p+1}]$$

on obtient $h = h_{i-1}P_i + h_i P_{i+1}$ qui est une moyenne pondérée de P_i et P_{i+1}, au lieu de P_i ou P_{i+1}. En un point x de cet intervalle, on a $| x - x_i | \leq 1/2^{p+1}$, on applique le théorème des accroissements finis et en utilisant $P_i(x_i) = P_{i+1}(x_i)$ on obtient

$$| P_i(x) - P_{i+1}(x) | \leq | P_i(x) - P_i(x_i) | + | P_{i+1}(x) - P_{i+1}(x_i) | \leq 2^{m+1}/2^{p+1} \leq 1/2^{n+1}$$

et donc :

$$\| \widetilde{f} - h \|_\infty \leq 1/2^{n+1}$$

Il reste à remplacer chaque h_i par un élément g_i de $\mathbf{Y}_{frac}$ vérifiant $\| \widetilde{g_i} - h_i \|_\infty \leq 1/(t2^p)$ de sorte que $\| \widetilde{g_i} P_{i+1} - h_i P_{i+1} \|_\infty \leq 1/(t2^{n+1})$ et donc

$$\| h - \sum_i \widetilde{g_i} P_{i+1} \|_{infty} \leq 1/2^{n+1}$$

Vue la proposition 3.3.6 concernant l'approximation des fonctions $C_{p,a}$ par des fractions rationnelles, le calcul des g_i se fait en temps polynomial à partir de la donnée (f, n). Il reste à exprimer $\sum_i \widetilde{g_i} P_{i+1}$ sous forme $\widetilde{g}$ avec $g \in \mathbf{Y}_{frac}$, ce qui n'offre pas de difficulté, pour obtenir $\| \widetilde{f} - \widetilde{g} \|_\infty \leq 1/2^n$. ∎

Théorème 5.3.2 *Les représentations* $\mathcal{C}_{\text{frac}}$ *et* $\mathcal{C}_{\text{sfrac}}$ *de* $\mathbf{C}[0,1]$ *sont* $\mathcal{P}$*- équivalentes.*

Preuve. A partir d'un élément $f = ((x_0, x_1, \ldots, x_t), ((P_1, Q_1), \ldots, (P_t, Q_t)))$ arbitraire de $\mathbf{Y}_{sfrac}$ on peut calculer en temps polynomial des nombres dyadiques $d_1, d_2, \ldots, d_t \geq 1$ et vérifiant $d_i Q_i(x_i) = d_{i+1} Q_{i+1}(x_i)$ (et donc aussi $d_i P_i(x_i) = d_{i+1} P_{i+1}(x_i)$ pour $i = 1, \ldots, t-1$) Alors $\widetilde{f} = \widetilde{g}/\widetilde{h}$ où $g, h \in \mathbf{Y}_{Sp}$ sont donnés par :

$$g = ((x_0, x_1, \ldots, x_t), (d_1 P_1, \ldots, d_t P_t)) \text{ et } h = ((x_0, x_1, \ldots, x_t), (d_1 Q_1, \ldots, d_t Q_t))$$

On conclut en utilisant la proposition 5.3.1 qui permet d'approcher convenablement g et h par des fractions rationnelles. ∎

Conclusion

Hoover a relié de manière intéressante la notion naturelle de complexité des fonctions réelles continues donnée par Ko et Friedman à une autre notion, basée sur les circuits arithmétiques. Il a donné de cette manière une certaine version "en temps polynomial" du théorème d'approximation de Weierstrass. Dans cet article nous avons généralisé l'approche de Hoover, en introduisant un point de vue uniforme grâce à la notion de présentation rationnelle d'un espace métrique. Ceci fournit un cadre de travail général satisfaisant pour l'étude de très nombreux problèmes de complexité algorithmique en analyse. Nous avons également généralisé grâce à cette approche les résultats de Ko, Friedman et Müller concernant les fonctions analytiques calculables en temps polynomial. La présentation rationnelle $\mathcal{C}_{\text{csl}}$ $\mathcal{P}$-équivalente à $\mathcal{C}_{\text{KF}}$ est la plus naturelle du point de vue de l'informatique théorique. Cependant ce n'est pas une $\mathcal{P}$-présentation et elle est mal adaptée à l'analyse numérique dés qu'on se pose des problèmes plus compliqués que l'évaluation (le calcul de la norme, ou d'une primitive par exemple). Parmi les représentations que nous avons étudiées, la présentation $\mathcal{C}_{\text{W}}$ semble être la plus facile à utiliser pour de nombreux problèmes de l'analyse numérique. Quant à la présentation par les fractions rationnelles, elle mérite une étude renforcée. On aimerait obtenir un analogue du théorème (valable pour la présentation $\mathcal{C}_{\text{W}}$) concernant la caractérisation des $\mathcal{P}$-points. Il serait également intéressant d'obtenir pour $\mathcal{C}_{\text{frac}}$ la $\mathcal{P}$-calculabilité de certaines opérations usuelles de l'analyse numérique, comme le calcul d'une primitive ou plus généralement le calcul de la solution d'une équation différentielle ordinaire.

Remerciements Nous remercions Maurice Margenstern et le referee pour leurs remarques pertinentes.

Références

[1] Aberth O. : *Computable analysis.* McGraw-Hill (1980). 6

[2] Bakhvalov : *Méthodes Numériques.* Editions MIR. Moscou (1973). 48

[3] Beeson M. : *Foundations of Constructive Mathematics.* Springer- Verlag (1985). 6, 14

[4] Bishop E. : *Foundations of Constructive Analysis* McGraw-Hill, New York, (1967). 5

[5] Bishop E., Bridges D. : *Constructive Analysis.* Springer-Verlag (1985). 2, 5, 11, 13, 16, 21

[6] Borodin A. : *On relating time et space to size et depth.* SIAM J. Comput. **6** (4) 733–744 (1977). 23

[7] Brent R. : *Fast multiple-precision evaluation of elementary functions.* Journal of the ACM **23** (2) 242–251 (1976). 25

[8] Bridges D. : *Constructive Functional Analysis.* Pitman, London (1979). 18

[9] Bridges D., Richman F. : *Varieties of Constructive Mathematics.* London Math. Soc. LNS 97. Cambridge University Press (1987) 6

[10] Cheney E. W. : *Introduction to Approximation Theory.* Mc Graw Hill Book Company (1966). 45

[11] Goodstein R. : *Recursive Analysis.* Amsterdam, North-Holland, (1961). 5

[12] Hoover J. : *Feasibly constructive analysis.* PhD (1987). 28, 37

[13] Hoover J. : *Feasible real functions et arithmetic circuits.* Siam J. Comput. **19** (1) 182–204 (1990). 2, 16, 28, 37

[14] Hörmander : *The Analysis of Linear Partial I Differential Operators.* Springer (1983). 49

[15] Ker-I. KO, Friedman H. : *Computational complexity of real functions.* Theoretical Computer Science **20** 323–352 (1982). 2, 5, 12, 13, 14, 28, 54

[16] Ker-I. KO, Friedman H. : *Computing power series in polynomial time.* Adv. Appl. Math. **9** 40–50 (1988). 5, 54

[17] Ker I. KO : *On the definitions of some complexity classes of real numbers.* Math System Theory **16** 95–109 (1983). 11

[18] Ker I. Ko : *Complexity theory of real functions.* Birhaüser (1991). 5, 13, 16

[19] Kushner B. A. : *Lectures on constructive mathematical analysis.* AMS Translations of Mathematical monographs n°60 (1984) (la version russe est de 1973) 6

[20] Labhalla S., Lombardi H. : *Real numbers, continued fractions, et complexity classes.* Annals of Pure et Applied Logic **50** 1–28 (1990). 3, 11

[21] Lombardi H. : *Nombres algébriques et approximations.* Publications Mathématiques de l'Université (Besançon) Théorie des Nombres. Fascicule 2 (1989). 44

[22] Lombardi H. : *Complexité des nombres réels et des fonctions réelles.* CALSYF 90, journées du GRECO de Calcul Formel (1990). 44

[23] Margenstern M. : *L'école constructive de Markov. Revue d'Histoire des Mathématiques*, **1** (2), 271–305 (1995) 6

[24] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Springer-Verlag. Universitext. (1988). 5

[25] Moutai E.M. : *Complexité des fonctions réelles, comparaison de différentes présentations.* Thèse de Troisième Cycle, Marrakech.(1995). 18, 19, 35

[26] N. Th. Müller : *Subpolynomial complexity classes of real functions et real numbers.* Proc 13th ICALP LNCS n°226 284–293 (1986).

[27] N. Th. Müller : *Uniform computational complexity classes of Taylor series.* Lecture Notes in Computer Science 267 (1987). 5, 54

[28] Newman D.J. : *Rational approximation to* $|x|$. Michigan Math. Journal (1964). 25

[29] Pan V. : *Solving a polynomial equation : some history et recent progress.* à paraître dans Siam Review (1996). 25

[30] Petrushev P.P., Popov V.A. : *Rational approximation of real functions.* Encyclopedia of Mathematics et its applications. Cambridge University Press (1987). 25

[31] Pour El M., Richards I. : *Computability in Analysis et Physics.* Perspectives in Mathematical logic. Springer Verlag (1989). 5, 20

[32] Th. J. Rivlin : *The Chebyshev Polynomials.* A Wiley Interscience Publication. Wiley & Sons. New York (1974). 45, 47, 48

[33] Schnorr C.P. : *Satisfiability is quasilinear complete in NQL.* J. Ass. Comput. Machinery **25** (1) 136–145 (1978). 8

[34] Stern J. : *Fondements mathématiques de l'informatique.* Mc Graw-Hill, Paris, (1990). 35

Table des matières