Relations entre représentation et complexité en analyse calculable.

Hugo Férée
Mathieu Hoyrup, Emmanuel Hainry et Romain Péchoux

LORIA

1 Introduction

De nombreux modèles ont été développés pour définir la calculabilité (et parfois la complexité) sur des ensembles généraux, notamment sur l'ensemble des nombres réels. On peut citer notamment BSS [BCSS98], le modèle du General Purpose Analog Computer [Sha41,BCGH07] ou l'analyse récursive (Ko [Ko91]).

Nous nous intéresserons ici à l'approche de Weihrauch [Wei00], qui développe une théorie générale de la calculabilité (Type-2 Theory of Effectivity) en se rapportant aux machines de Turing fonctionnant sur des mots infinis. Cela permet par exemple de considérer la calculabilité des fonctions réelles ou des parties de $\mathbb{R}^n$. Un ensemble peut être muni de plusieurs représentations et il existe alors différentes notions de calculabilité pour cet ensemble. Il s'attache alors à comparer ces représentations entre elles et à caractériser celles qui font sens en faisant un lien avec la topologie. En particulier, toute représentation engendre une topologie et pour toute topologie (munie d'une structure supplémentaire), il existe une représentation qui l'engendre.

Cependant, cette méthodologie n'est pas réellement adaptée à l'étude de la complexité même si elle peut être définie de façon *ad hoc* pour correspondre par exemple à celle de nombres réels de Ko. Kawamura et Cook [KC10] ont proposé une généralisation de l'approche de Weihrauch pour étudier la complexité de manière uniforme en se ramenant aux machines à oracles et aux différentes classes de complexité déjà définies sur les fonctions de type 2 (notamment les Basic Feasible Functionals [Cob65,KC96] qui sont l'extension naturelle des fonctions calculables en temps polynomial). De même, des représentations différentes sur un même ensemble engendrent des classes de complexité différentes. Si l'on peut mettre en relation la topologie avec la calculabilité, cette structure ne suffit pas à caractériser une représentation canonique qui a du sens pour la complexité. Une structure plus adaptée est celle des espaces métriques (bien que l'on puisse parler de complexité sur des espaces non métrisables [KS05]) ; c'est d'ailleurs un cas particulier d'espace topologique.

De même qu'un lien a été fait entre calculabilité et continuité, nous nous efforcerons tout particulièrement de comprendre les liens entre les classes de complexité, en particulier le temps polynomial, engendrées par une représentation donnée et certaines propriétés mathématiques. Cela fournit des arguments pour justifier l'utilisation d'une représentation. De façon analogue, en théorie classique de la complexité, on a choisi de représenter les entiers par des mots binaires plutôt que sur par des mots unaires pour rendre certaines fonctions calculables en temps polynomial.

Il est naturel de se demander quelles sont les procédures mathématiques usuelles qui sont calculables (calcul intégral, inversion de matrice, etc.) et quelle est leur complexité.

Dans la section 2 nous définissons la calculabilité et la complexité relatives à une représentation. Nous étudions ensuite, dans la section 3 le cas des espaces métriques effectifs, qui sont des espaces définissant implicitement une représentation et une notion de complexité. Nous montrerons également dans le paragraphe 3.1 que l'on peut représenter l'espace des fonctions continues sur des tels ensembles et nous généraliserons un résultat de Kawamura et Cook [KC10] qui montre que les fonctions de $[0,1]$ dans $\mathbb{R}$ calculables en temps polynomial en tant que fonction sont exactement les fonctions continues calculables en temps polynomial en tant qu'élément d'un ensemble muni de la représentation précédemment définie. Cela permet de justifier l'usage de cette représentation et de la notion de complexité qu'elle engendre. Nous démontrerons ensuite un résultat similaire sur l'espace des compacts de $[0,1]$ dans le paragraphe 3.3. Enfin, dans la section 4, nous fournirons quelques résultats permettant de mieux comprendre la « forme » des fonctions de $\mathcal{C}[0,1]$ dans $\mathbb{R}$ calculables en temps polynomial (et en particulier des normes), puisque cela ne rentre pas dans le cadre de la section précédente.

2 Calculabilité et complexité

2.1 Calculabilité d'ordre supérieur

La théorie classique de la calculabilité est définie sur les mots finis d'un alphabet (soit Σ^* et on pourra considérer par la suite que $\Sigma = \{0,1\}$), mais nous avons besoin d'espaces de cardinal supérieur pour représenter des objets qui n'ont pas de description finie (comme les nombres réels par exemple), on définit alors la calculabilité sur les mots infinis (Σ^ω) ou sur les fonctions des mots finis ($\Sigma^* \to \Sigma^*$).

La calculabilité sur les mots finis étant bien connue, on adapte le modèle des machines de Turing aux mots infinis : une machine calcule sur un mot infini (dans l'espace de Cantor Σ^ω) si son ruban d'entrée contient ce mot infini. Elle calcule un mot infini si sa tête de lecture ne peut se déplacer que de gauche à droite sur son ruban de sortie et qu'elle y écrit ce mot infini.

Pour calculer avec des fonctions sur les mots finis ($\Sigma^* \to \Sigma^*$) en entrée, on utilise des machines à oracle. Une telle machine prend son argument f en tant qu'oracle et peut y faire appel après avoir écrit un mot w sur un ruban de requête. Elle a alors accès au mot $f(w)$ sur un second ruban. Pour retourner une telle fonction, une machine prend un argument supplémentaire (dans Σ^*) et calcule (au sens classique) la valeur de la sortie sur cet argument (en d'autres termes, elle calcule une fonction de type $((\Sigma^* \to \Sigma^*) \times \Sigma^*) \to \Sigma^*$).

2.2 Topologie des espaces de représentations

Nous allons montrer par la suite qu'une notion de calculabilité sur un ensemble est liée à une topologie[1] sur ce même ensemble et qu'en particulier toute fonction calculable est continue pour cette topologie. Considérons d'abord les ensembles Σ^ω et $\Sigma^* \to \Sigma^*$. La topologie usuelle sur Σ^ω est la topologie produit, dont les ouverts de base sont les ensembles (appelés cylindres) de la forme $w\Sigma^\omega$ (aussi noté $[w]$), où w est un mot fini. Or la définition de la calculabilité sur Σ^ω implique que pour écrire les n premiers caractères

1. C'est-à-dire un ensemble de sous-ensembles stable par union et intersection finie et complémentaire.

de la sortie, il suffit de connaître un nombre fini de caractères de l'entrée (puisque pour les écrire, une machine n'a qu'un temps fini et ne peut donc lire qu'un nombre fini de caractères de l'entrée). Cela revient alors à dire que la pré-image d'un ouvert par une fonction calculable est un ouvert pour cette topologie, ce qui signifie exactement que toute fonction calculable est continue pour cette topologie.

De même, on peut définir les ouverts de base de $\Sigma^* \to \Sigma^*$ comme les ensembles de fonctions qui coïncident sur un ensemble fini de mots (que l'on pourra noter $[w_1, \dots w_n]$). Une machine calculant une fonction n'a besoin que d'un nombre fini d'appels à l'oracle pour écrire un élément de la sortie et donc toute fonction calculable est continue pour cette topologie.

Remarque 1
Dans le cas des fonctions calculables au sens usuel (sur Σ^*), la topologie correspondante est la topologie discrète (pour laquelle tout ensemble est ouvert). Toute fonction étant continue pour cette topologie, toute fonction calculable est évidemment continue.

2.3 Représentations

Pour définir la calculabilité sur un ensemble, il est nécessaire d'encoder ses éléments dans l'ensemble manipulé par les machines, c'est-à-dire Σ^*, Σ^ω ou $(\Sigma^* \to \Sigma^*)$.

Remarque 2
On utilise déjà implicitement des représentations lorque l'on travaille sur des objets finis, tels que les graphes, les polynômes ou les matrices, et pour chacun de ces ensembles il existe différentes représentations qui peuvent être utilisées suivant le contexte.

En ce qui concerne les entiers naturels, il existe plusieurs manières d'encoder les entiers dans Σ^*, par exemple en utilisant la représentation binaire ou la représentation unaire ($w \in \Sigma^*$ encode $n \in \mathbb{N}$ si $|w| = n$). Même si l'on peut calculer une représentation à partir de l'autre, le choix de telle ou telle représentation n'est pas anodin puisqu'elles n'engendrent pas les mêmes classes de complexité.

Définition 1
Soit $Y \in \{\Sigma^*, \Sigma^\omega, \Sigma^* \to \Sigma^*\}$ un ***espace de représentation*** *(espace où l'on a précédemment défini la calculabilité). Une* ***représentation*** *de M est une fonction surjective $\delta : Y \hookrightarrow M$ (où $\hookrightarrow$ désigne une fonction partielle). Dans le cas d'une représentation sur les mots finis ($Y = \Sigma^*$), on dit que δ est une* ***notation****.*

Exemple 1
Il existe plusieurs notations des rationnels, par exemple $\delta(\langle\langle p, q\rangle, r\rangle) = \frac{p-q}{r}$, où $\langle,\rangle$ désigne une injection des couples de mots finis dans les mots finis.

Les ensembles Σ^ω et donc $(\Sigma^* \to \Sigma^*)$ permettent notamment d'encoder les suites de mots finis, et donc les suites d'éléments d'un ensemble muni d'une notation (en particulier les suites d'entiers). L'encodage dans Σ^ω n'est pas immédiat, mais on en trouvera une description dans [Wei00]. Dans $\Sigma^* \to \Sigma^*$, on encode simplement la suite $(u_n)_{n\in\mathbb{N}}$ par la fonction ϕ, avec $\forall n \in \mathbb{N}, \phi(0^n) = u_n$.

Il est alors facile de décrire différentes représentations des nombres réels (de $[0, 1]$, mais ces représentations s'étendent aussi à $\mathbb{R}$ tout entier) :

- *La représentation binaire $\delta_{0/1}$ décrit un réel par une de ses écritures binaires ($\delta_{0/1}(\varepsilon_0\varepsilon_1 \dots) = \Sigma_{n=1}^{\infty}\varepsilon_n 2^{-n}$ où $\varepsilon_n \in \Sigma = \{0, 1\}$).*

- *La représentation binaire signée $\delta_\pm$ décrit un réel par une de ses écritures binaires signées ($\Sigma_{n=0}^{\infty}\varepsilon_n 2^{-n}$ où $\varepsilon_n \in \Sigma = \{-1, 0, 1\}$)*
- *La représentation de Cauchy naïve consiste à remarquer que tout réel est limite de rationnels. Un réel x est alors représenté par une suite de Cauchy de rationnels convergeant vers x. Cette représentation est faible car elle n'indique aucune vitesse de convergence.*
- *La représentation de Cauchy δ_c représente les réels comme des suites de Cauchy de rationnels convergeant à vitesse connue (on la fixe usuellement à 2^{-n}).*
- *On peut aussi considérer le cas particulier où la suite de rationnels converge en croissant ($\delta_<$) ou en décroissant ($\delta_>$).*
- *Un réel est aussi représentable par une suite de dyadiques (les nombres de la forme $k2^{-n}, (k, n) \in \mathbb{N}^2$) convergeant à vitesse 2^{-n}*

Définition 2
Un élément de M est calculable pour une représentation δ de M s'il admet un représentant calculable.

On peut, de manière analogue, définir les fonctions calculables relativement à des représentations.

Définition 3 (Réalisation)
Une fonction $f : M \hookrightarrow M'$ est réalisée (relativement à deux représentations δ et δ' de M et M' respectivement) par une fonction $g : Y \hookrightarrow Y'$ (où Y, Y' sont les ensembles représentant M et M') si $f \circ \delta = \delta' \circ g$ sur le domaine de δ (noté par la suite $dom(\delta)$).

$$\begin{tikzcd}
Y \arrow[r, "\delta"] \arrow[d, "g"'] & M \arrow[d, "f"] \\
Y' \arrow[r, "\delta'"'] & M'
\end{tikzcd}$$

Figure 1. g réalise f.

On supposera implicitement par la suite que $Y \in \{\Sigma^*, \Sigma^\omega, (\Sigma^* \to \Sigma^*)\}$.

On dit alors que f est calculable (relativement à ces représentations) si elle est réalisable par une fonction calculable.

On remarque que la notion de calculabilité sur des ensembles dépend de leur représentation. Il est alors intéressant de se demander quelles représentations fournissent la même notion de calculabilité et s'il existe une représentation plus légitime que les autres.

Définition 4 (Réductibilité et équivalence)
Soient $\delta, \delta' : Y \hookrightarrow M$ des représentations.

δ est continûment réductible à δ' ($\delta \leq_t \delta'$) : *il existe une fonction continue f telle que $\delta = \delta' \circ f$ sur $dom(\delta)$.*

δ est réductible à δ' ($\delta \leq \delta'$) : *il existe une fonction calculable f telle que $\delta = \delta' \circ f$ sur $dom(\delta)$.*

δ est continûment équivalente à δ' ($\delta \equiv_t \delta'$) : $\delta \leq_t \delta'$ *et* $\delta' \leq_t \delta$

δ est équivalente à δ' ($\delta \equiv \delta'$) : $\delta \leq \delta'$ *et* $\delta' \leq \delta$

Informellement, $\delta \leq \delta'$ signifie que la représentation δ contient plus d'information que δ'.

Remarque 3
Étant donné qu'une fonction calculable (entre deux espaces de représentation) est continue, être réductible implique être continûment réductible.

Ces notions de réductibilité permettent notamment d'obtenir des inclusions entre les ensembles de fonctions calculables relatives à des représentations.

Propriété 1
Si $\delta_1 \leq \delta_2$ sont des représentations de M et $\delta'_1 \leq \delta'_2$ des représentations de M', telles que $f : M \to M'$ est calculable relativement à δ_2 et δ'_1, alors f est aussi calculable relativement à δ_1 et δ'_2.

Exemple 2
Il est facile de remarquer qu'à partir d'une expansion binaire d'un réel, on peut en calculer une suite d'approximations rationnelles rapidement convergente, autrement dit : $\delta_{0/1} \leq \delta_c$. De même, on peut aisément remarquer que les représentations binaire signée, de Cauchy et dyadique sont équivalentes. Cependant, la représentation binaire est strictement plus faible que les précédentes (entre autres, $\delta_{0/1} \leq_t \delta_\pm$ et $\delta_\pm \not\leq_t \delta_{0/1}$). Par exemple, la fonction qui multiplie un réel par 3 est calculable pour les représentations précédentes, excepté $\delta_{0/1}$. En effet, pour obtenir le premier bit de la représentation de $3x$, il peut être nécessaire de connaître toute l'écriture binaire de x : une machine lisant un encodage de x commençant par $01010101\ldots$ (soit le début de l'écriture binaire de $\frac{1}{6}$) ne peut décider en temps fini si elle doit écrire 0 (si $x \leq \frac{1}{6}$) ou 1 (si $x \geq \frac{1}{6}$).

Pour faire le lien entre représentation et topologie, on peut se demander quels ensembles de l'espace représenté correspondent (via une représentation donnée) à des ouverts de l'espace de représentation (cf. section 2.2).

Définition 5 (Topologie finale)
La topologie finale τ_δ d'une représentation δ est l'ensemble des parties X de M telles que $\delta^{-1}(X)$ est un ouvert de l'espace des représentations.

À chaque représentation correspond alors une topologie. Inversement, il est naturel de chercher à définir une représentation pour une topologie donnée. Pour cela, il faut que la topologie soit suffisante pour caractériser l'espace :

Définition 6 (Espace T_0, dit de Kolmogorov)
Un espace topologique (M, τ) est T_0 si tout élément de M est caractérisé par l'ensemble de ses voisinages (pour la topologie τ). Autrement dit, si deux éléments sont distincts, alors il existe un ouvert qui contient exactement l'un d'entre eux. (M, τ) est de plus à base dénombrable si la topologie τ est engendrée par une famille dénombrable d'ouverts.

On peut alors en définir une version effective :

Définition 7 (Espace topologique effectif)
$S = (M, \sigma, \nu)$ est un espace topologique effectif si σ est un ensemble dénombrable de sous-ensembles de M et ν est une notation pour σ. De plus, tout élément de M est caractérisé par l'ensemble des éléments de σ auxquels il appartient. La topologie associée à S (notée τ_S) est la topologie induite par σ. En particulier, (M, τ_S) est un espace T_0 à base dénombrable.

Remarque 4
Pour tout espace de Kolmogorov à base dénombrable, il existe un espace topologique effectif qui engendre la même topologie (en effet, pour obtenir un espace topologique effectif, il suffit d'une énumération de la base, et d'une notation des entiers).

Par la suite, nous nous intéresserons uniquement à ces espaces. Une telle structure suffit alors à définir une représentation :

Définition 8 (Représentation standard)
Si $S = (M, \sigma, \nu)$ est un espace topologique effectif, alors sa représentation standard $\delta_S : Y \hookrightarrow M$ est définie ainsi : $\delta_S(u) = x$ si u encode la suite des éléments de σ contenant x. Plus précisément, u encode une suite de mots, chacun représentant (via la notation ν) un élément de σ qui contient x et ils sont tous énumérés.

Propriété 2 (Propriétés de la représentation standard)
1. *δ_S est continue pour la topologie τ_S.*
2. *δ_S est ouverte (l'image d'un ouvert est un ouvert).*
3. *τ_S est la topologie finale de δ_S.*
4. *Si $\delta : Y \hookrightarrow M$ est continue (pour la topologie τ_S), alors $\delta \leq_t \delta_S$.*
5. *Si $f : M \hookrightarrow M'$ (pour un espace topologique (M', τ')), alors $f \circ \delta_S$ est continue $\iff$ f est continue.*
6. *Si deux espaces topologiques effectifs engendrent la même topologie, alors leurs représentations standard sont continûment équivalentes.*

Preuve

1. Si X est un ouvert, $\delta_S^{-1}[X]$ est l'ensemble des suites de $dom(\delta_S)$ qui contiennent un mot w tel que $\nu(w) \subseteq X$: c'est une union de cylindres, donc un ouvert.
2. L'image par δ_S d'un ouvert de la forme $[\{w_1, \ldots w_n\}]$ est $\cap_i = \nu(w_i)$. C'est une intersection finie d'ouverts, et donc un ouvert.
3. Les deux points précédents fournissent chacun une preuve des inclusions entre la topologie τ_S et la topologie finale τ_{δ_S}.
4. Soit $(w_i)_{i \in \mathbb{N}}$ une énumération de $dom(\nu)$. On définit alors $f(p)$ comme la suite qui à l'indice $\langle i, n \rangle$ vaut w_i si $\delta([p_1, \ldots p_n]) \subseteq \nu(w_i)$ et w_0 sinon (on suppose que $\nu(w_0) = M$). $f(p)$ encode alors l'ensemble des éléments de σ qui contiennent l'image par δ d'un voisinage ($[p_1 \ldots p_n]$) de p. $\delta(p) \in \nu(w_i) \iff p \in \delta^{-1}(\nu(w_i))$, donc comme δ est continue et $\nu(w_i)$ est ouvert, cet ensemble est ouvert et donc $\delta(p) \in \nu(w_i) \iff \exists n \in \mathbb{N}, [p_1 \ldots p_n] \subseteq \delta^{-1}(\nu(w_i)) \iff \exists n \in \mathbb{N}, \delta([p_1 \ldots p_n]) \subseteq \nu(w_i)$.
   Donc pour tout p dans $dom(\delta)$, $\delta(p) = \delta_S(f(p))$. De plus, un préfixe fini de p suffit à connaître un préfixe fini de $f(p)$, ce qui veut dire que f est continue, et donc $\delta \leq_t \delta_S$.

5. Par définition de la continuité : f est continue $\iff \forall U \in \tau_{S'}, f^{-1}(U) \in \tau_S \iff \forall U \in \tau_{S'}, \delta_S^{-1}(f^{-1}(U)) \in \tau_Y$ puisque τ_S est la topologie finale de δ_S d'après le point 3. Cela est équivalent à : $\forall U \in \tau', (f \circ \delta_S)^{-1}(U) \in \tau$, ce qui est la définition de la continuité de $f \circ \delta_S$.
6. Si $\tau_S = \tau_{S'}$, alors comme δ_S est continue pour la topologie τ_S elle l'est pour $\tau_{S'}$ et vérifie donc $\delta_S \leq_t \delta_{S'}$ d'après le point 4. De même, $\delta_{S'} \leq_t \delta_S$, d'où $\delta_S \equiv_t \delta_{S'}$.

$\square$

Ces résultats expriment le fait que la représentation standard est la représentation la plus générale (c'est-à-dire maximale pour $\leq_t$) compatible avec la topologie qu'elle engendre, et pour une topologie donnée, toutes ses représentations standard sont continûment équivalentes.

Cependant, il est restrictif de ne considérer que des représentations standard. D'ailleurs, aucune des représentations de l'exemple 1 ne l'est.

Définition 9 (Représentation admissible)
Une représentation admissible d'un espace T_0 à base dénombrable est une représentation continûment équivalente aux représentations standard de cet espace.

Les propriétés suivantes illustrent le fait que les représentations admissibles sont celles qui font sens pour la topologie :

Proposition 1
$f : M \hookrightarrow M'$ est continue (relativement aux topologies sur M et M') si et seulement si elle est continûment réalisable pour des représentations admissibles de M et M'.

Preuve

Par définition des représentations admissibles, il suffit de prouver le résultat dans le cas de deux représentations standard δ et δ' respectivement de M et M'. Si f est continue, alors $f \circ \delta$ l'est aussi puisque δ est continue. Cependant, le point 4 de la propriété 2 montre que $f \circ \delta \leq_t \delta'$, ce qui implique l'existence d'une fonction continue g telle que $f \circ \delta = \delta' \circ g$, ce qui veut dire que f est continûment réalisable. Inversement, si f est continûment réalisable, on a de même $f \circ \delta = \delta' \circ g$, et donc $f \circ \delta$ est continue et le point 5 implique que f est continue. $\square$

Exemple 3
La fonction partie entière n'est continûment réalisable pour aucune représentation admissible de $\mathbb{R}$ (muni de sa topologie usuelle) puisqu'elle n'est pas continue (elle n'es a fortiori pas calculable non plus).

Proposition 2 (Caractérisation des représentations admissibles)
Une représentation δ est admissible pour (M, τ) si et seulement si elle est continue (pour la topologie τ) et $\delta' \leq_t \delta$ pour toute représentation continue δ' de M.

Preuve

D'après la propriété 2, si δ est continue, alors pour une représentation standard δ_S, $\delta \leq_t \delta_S$. De plus, l'hypothèse appliquée à δ_S donne $\delta_S \leq_t \delta$. L'autre implication est un résultat direct de cette même propriété. $\square$

Remarque 5
Cette propriété implique qu'une représentation admissible est continue et donc que si son domaine est compact, alors son image (l'ensemble qu'elle représente) est compacte. Par exemple, il n'y a pas de représentation admissible totale de $\mathbb{R}$ dans Σ^ω, car Σ^ω est compacte, contrairement à $\mathbb{R}$).

2.4 Complexité d'ordre 2

Pour étudier la complexité, nous nous intéresserons seulement aux représentations sur $\Sigma^* \to \Sigma^*$. En effet, l'espace de Cantor est mal adapté à la complexité.

Pour pouvoir exprimer le temps de calcul d'une machine à oracle de manière similaire à la complexité de type 1, et donc la complexité de la fonction qu'elle calcule, il faut pouvoir exprimer la taille de l'entrée, qui n'est plus un mot mais une fonction.

Pour cela, on se restreindra aux fonctions régulières (définies par Kawamura et Cook [KC10]) :

Définition 10
*Les **fonctions régulières** $\varphi \in$ **Reg** sont les fonctions $\varphi : \Sigma^* \hookrightarrow \Sigma^*$ compatibles avec la taille : $\forall w, w' \in dom(\varphi), |w| \leq |w'| \Rightarrow |\varphi(w)| \leq |\varphi(w')|$.*

On définit alors la taille $|\phi|$ d'une fonction régulière ϕ comme une fonction de type $\mathbb{N} \to \mathbb{N}$:

$$\forall n \in \mathbb{N}, |\phi|(n) = \max_{|w| \leq n} |\phi(w)|$$

$|\phi|(n)$ borne la taille des valeurs de ϕ sur les entrées de taille inférieure à n.

De plus, il faut prendre en compte le temps de calcul induit par un appel à l'oracle. On considère alors qu'appeler l'oracle ϕ sur l'entrée w requiert un temps de calcul de $|\phi(w)|$ (soit la taille du résultat fourni par l'oracle). [2] On dit alors qu'une machine calcule en temps T (où T est une fonction de type 2, soit de la forme $(\mathbb{N} \to \mathbb{N})^k \to \mathbb{N}^l \to \mathbb{N}, k, l \in \mathbb{N}$) si étant donnés des entrées et des oracles, elle s'arrête après un temps borné par T appliqué aux tailles des entrées et des oracles. En particulier, on peut définir les fonctions calculables en temps polynomial comme les fonctions calculées par une machine dont le temps de calcul est borné par un polynôme de type 2 (une fonction de l'algèbre $P ::= X \mid P + P \mid P * P \mid Y(P)$ où X désigne une variable de type 1, et Y une variable de type 2).

Remarque 6
*Il est possible de calculer la taille d'une fonction régulière en temps polynomial en unaire ($\varphi, 0^n \mapsto 0^{|\varphi|(n)}$), de même que l'on peut calculer la taille d'un mot en unaire en temps polynomial. En effet, pour avoir $|\phi|(n)$, il suffit de calculer la taille de $\phi(w)$ pour un mot quelconque de taille n. Cela n'est pas vrai pour des fonctions quelconques (puisqu'il faut calculer la taille de ϕ sur un nombre exponentiel de valeurs) et c'est pour cela entre autres que l'on se restreint aux fonctions de **Reg**.*

2.5 Complexité relative à une représentation

Remarque 7
On peut déjà noter que, de façon analogue aux entiers, si un élément est calculable en temps polynomial alors il admet un représentant de taille polynomiale.

2. Pour une discussion sur la justification de ce modèle, on pourra se référer à [KC96].

Deux représentations équivalentes (en terme de calculabilité) peuvent engendrer différentes notions de complexité.

Exemple 4

- *Sur les entiers, la fonction* $n \mapsto n^{\log_2(n)}$ *est calculable en temps polynomial pour la représentation binaire, mais pas pour la représentation unaire.*
- *Il existe plusieurs représentations des polynômes, comme celle qui fournit la liste de tous les coefficients ou celle qui donne une liste de couples (degré, coefficient). Pour la première représentation, le polynôme* X^{2^n} *est de taille exponentielle en* n *(puisqu'il est de degré exponentiel), alors qu'il peut être représenté par le couple* $(2^n, 1)$ *qui est de taille polynomiale en* n.

Ces exemples concernent des objets à représentation finie, et on trouvera par la suite des exemples de différences de complexité selon la représentation pour des objets à représentation infinie (voir les remarques 11 et 12).

On peut alors raffiner l'ordre entre les représentations pour les comparer en termes de complexité. On note :

$\delta \leq_P \delta'$ lorsqu'il existe une fonction f calculable en temps polynomial telle que $\delta = \delta' \circ f$ sur $dom(\delta)$.

$\delta \equiv_P \delta'$ lorsque $\delta \leq_P \delta'$ et $\delta' \leq_P \delta$

De même qu'une fonction est calculable si elle est réalisée (pour des représentations données) par une fonction calculable, une fonction est calculable en temps polynomial si elle est réalisée par une fonction calculable en temps polynomial (et de façon similaire pour d'autres classes de complexité, dès lors qu'elles sont définies sur **Reg**). Les relations entre les représentations impliquent alors des inclusions entre les classes de complexité.

Propriété 3

Si $\delta_1 \leq_P \delta_2$ *sont des représentations de* M *et* $\delta'_1 \leq_P \delta'_2$ *des représentations de* M' *telles que* $f : M \to M'$ *est calculable en temps polynomial relativement à* δ_2 *et* δ'_1*, alors* f *est aussi calculable en temps polynomial relativement à* δ_1 *et* δ'_2.

Remarque 8

Dans le cas où f *est calculable en temps polynomial pour* δ_1 *et* δ'_1*, on ne peut rien dire en général pour sa complexité relativement à* δ_2 *et* δ'_2 *(voir entre autres l'exemple 6 page 14).*

Il est important de remarquer que la représentation standard n'est pas adaptée à la complexité : tout élément calculable admet une représentation calculable en temps polynomial (on peut en effet reporter l'écriture du $(n+1)^{\text{ième}}$ élément de la suite représentant x en répétant l'élément d'indice n autant de fois que nécessaire pour obtenir suffisamment de temps de calcul).

3 Espaces métriques effectifs

De la même manière que nous avons défini une représentation standard (et donc une notion de calculabilité) lorsque nous avions un structure d'espace T_0, nous allons définir une structure (qui est en fait un cas particulier d'espace T_0) sur laquelle il existe une représentation simple et qui a du sens en termes de complexité.

Définition 11 (Espace métrique effectif)
(M, d, Q, ν) est un espace métrique effectif si $Q = \{\nu(w) \mid w \in \Sigma^*\}$ est un sous-ensemble dense de M pour la topologie engendrée par la distance d.

Cette notion est un cas particulier des espaces que nous avons considérés pour la calculabilité :

Propriété 4
Tout espace métrique effectif est un espace de T_0 à base dénombrable pour la topologie engendrée par sa distance.

En effet, les ensembles de la forme $\mathcal{B}(\nu(w), 2^{-k})$ (où $w \in \Sigma^*$, $k \in \mathbb{N}$ et $\mathcal{B}(x, r)$ désigne la boule ouverte de rayon r et de centre x pour la distance d) forment une base de la topologie engendrée par d. On dénote alors $\mathcal{B}(\nu(w), 2^{-k})$ par un encodage de w et de k.

Exemple 5
Les ensembles suivants sont des espaces métriques effectifs :
- $[0, 1]$ *muni de la distance usuelle et au choix : des nombres dyadiques, des rationnels de $[0, 1]$, ou par exemple des nombres $a + q \in [0, 1]$, où $q \in \mathbb{Q}$ et a est un réel donné (par exemple irrationnel, ou même non calculable).*
- *l'ensemble des fonctions continues sur $[0, 1]$, muni de la distance induite par une norme usuelle ($\|.\|_\infty, \|.\|_1, \|.\|_2$) et d'un ensemble dense dénombrable comme les polynômes rationnels ou les fonctions linéaires par morceaux à extrémités rationnelles.*
- *l'ensemble des compacts de $[0, 1]^n$ muni de la distance de Hausdorff et ensembles finis de vecteurs rationnels (cf. section 3.3).*

Les espaces métriques effectifs sont en quelque sorte la structure minimale pour définir la représentation de Cauchy, de même que les espaces de Kolmogorov à base dénombrables le sont pour la représentation standard.

Définition 12
*La **représentation de Cauchy** δ_c sur un espace métrique effectif (M, d, Q, ν) est définie de manière similaire à l'exemple 1 : $\delta_c(\varphi) = x \in M$ lorsque φ encode une suite $(q_n)_{n \in \mathbb{N}}$ d'éléments de Q (via la notation ν) telle que $\forall n \in \mathbb{N}, d(x, q_n) \leq 2^{-n}$.*

De la même façon que la représentation standard caractérisait un élément par l'ensemble des ouverts de base (éléments de σ) le contenant, la représentation de Cauchy caractérise un élément par une suite d'ouverts de base (les boules centrées en Q) de taille décroissant à vitesse donnée (2^{-n}).

Remarque 9
Si l'on change la distance, alors les représentations ne sont plus nécessairement équivalentes, et l'on peut obtenir différentes classes de complexité.

De même, si l'on change le sous-ensemble dense, on peut changer la notion de complexité (voir par exemple la remarque 11 page 13) et même la notion de calculabilité si l'on utilise par exemple un sous-ensemble dense de réels contenant un réel non calculable (plutôt que les rationnels ou les dyadiques).

3.1 Représentation des fonctions continues sur un espace métrique effectif compact

Ce qui précède fournit des notions de calculabilité (en temps polynomial) sur des espaces métriques effectifs (via la représentation de Cauchy) et donc une notion de complexité sur les fonctions sur ces ensembles. On cherche maintenant à obtenir un résultat à l'ordre supérieur, en manipulant les fonctions continues d'un espace métrique dans un autre comme des éléments d'un espace muni lui aussi d'une représentation.

Si (M, d, Q, ν) est un espace métrique effectif compact et (M', d', Q', ν') un espace métrique effectif, alors on peut représenter les fonctions continues de M dans M' ainsi : une fonction continue $f : M \to M'$ peut être représentée par une fonction $f_Q : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ et une fonction $f_m : \mathbb{N} \to \mathbb{N}$ telles que :

- $\forall q \in \mathbb{N}, \forall n \in \mathbb{N}, d(\nu'(f_Q(q,n)), f(\nu(q))) \leq 2^{-n}$
- $\forall n \in \mathbb{N}, \forall x, y \in M, d(x,y) \leq 2^{-f_m(n)} \Rightarrow d'(f(x), f(y)) \leq 2^{-n}$

En d'autres termes, f_Q permet d'approcher l'image par f de tout élément de Q par un élément de Q', et f_m est un module de continuité pour f. Toute fonction continue sur un compact est uniformément continue et admet donc un module de continuité (et cette représentation est bien surjective). On remarque alors que pour calculer $f(x)$ à précision 2^{-n}, il suffit de calculer une approximation de x (par un élément de Q) à précision de l'ordre de $2^{-m(n)}$ et d'appliquer f_Q. On notera par la suite δ_0 la représentation qui encode à la fois f_Q et f_m ($\delta_0(\phi) = f$ si $\phi(0^n) = f_m(n)$ et $\phi(1\langle p, q\rangle) = f_Q(\nu(q), p)$).

Un exemple de tel espace de fonctions est $\mathcal{C}[0,1]$ des fonctions réelles continues sur $[0,1]$. Décrire une telle fonction revient alors à fournir un module de continuité et une approximation sur les rationnels.

Remarque 10
On se restreint à un espace compact pour obtenir l'existence d'un module de continuité. On peut cependant définir une représentation des fonctions sur une union dénombrable croissante de compacts (par exemple, $\mathbb{R} = \cup_{n\in\mathbb{N}}[-2^n, 2^n]$ *ou* $[-1,1] \setminus \{0\} = \cup_{n\in\mathbb{N}}[-1,1] \setminus (-2^{-n}, 2^{-n})$*) en fournissant à* f_m *un argument supplémentaire correspondant à l'indice du compact.*

Il est possible, dans certains cas, de caractériser une représentation (ou plutôt sa classe d'équivalence pour $\equiv_P$) par un ensemble de fonctions qu'elle rend calculables en temps polynomial.

3.2 Caractérisation de $\boldsymbol{\delta_0}$

Il a été montré par Kawamura que la représentation δ_0 sur $\mathcal{C}[0,1]$ est, en un sens, la meilleure en terme de complexité si l'on considère que la fonctionnelle Apply : $\mathcal{C}[0,1] \to [0,1] \to \mathbb{R}$ (qui applique une fonction à un réel) doit être calculable en temps polynomial. Ce résultat est en fait vrai pour notre définition de δ_0 (défini sur d'autres espaces métriques effectifs) lorsque l'on suppose qu'il existe un polynôme tel que tout élément de M a un représentant (pour la représentation de Cauchy) de cette taille. C'est le cas de $[0,1]$, mais pas de $\mathbb{R}$ tout entier (par exemple, le réel 2^n n'a pas de représentant de taille plus petite que $k \mapsto n$). De façon générale, si M n'est pas compact, il possède des éléments de taille arbitrairement grande. C'est aussi le cas s'il est compact mais qu'il ne peut être recouvert par $2^{P(n)}$ (où P est un polynôme) de boules de taille 2^{-n} (autrement dit, si pour tout P il possède $2^{P(n)}$ éléments à distance 2^{-n} les uns des autres).

Théorème 1

Soient δ et δ' les représentations de Cauchy de M et M' (comme définies au début de la section 3). Supposons qu'il existe un polynôme λ tel que tout élément de M a une représentation de taille inférieure à λ ($\forall x \in M, \exists \varphi \in \boldsymbol{Reg}, \delta(\varphi) = x$ et $\forall n \in \mathbb{N}, |\varphi|(n) \leq \lambda(n)$). Alors pour toute représentation ρ des fonctions continues de M dans M', $\rho \leq_P \delta_0$ si et seulement si Apply : $\mathcal{C}(M, M') \to M \to M'$ est calculable en temps polynomial relativement à ρ, δ et δ'.

Preuve

Pour le premier sens, d'après la propriété 3, il suffit de montrer que δ_0 rend Apply calculable en temps polynomial. Étant donné $f : M \to M'$ représenté par f_Q et f_m, une représentation de $x \in M$ et une précision p, on calcule $f_m(p+1)$ puis une approximation q de x à précision $f_m(n+1)$. Enfin, par définition de f_Q et f_m, $f_Q(q, p+1)$ est une approximation à 2^{-p} près de $f(x)$:

$$d(f(x), f_Q(q, p+1)) \leq d(f(q), f(x)) + d(f(q), f_Q(q, p+1)) \leq 2^{-(p+1)} + 2^{-(p+1)} \leq 2^{-p}$$

Tous les calculs ont bien été faits en temps polynomial par rapport aux tailles des représentations de x et f.

Pour l'autre sens, il s'agit de convertir une $\rho-$représentation en une δ_0-représentation. Comme Apply est calculable en temps polynomial pour ρ, il existe un polynôme P d'ordre 2 tel que $P(|\phi|, |\psi|, n)$ borne le temps de calcul de Apply à précision n sur f et x (représentés par ϕ et ψ). Soit λ un polynôme tel que tout élément de M a une représentation de taille λ. Alors $n \to P(|\phi|, \lambda, n)$ est un module de continuité de $f = \rho(\phi)$. En effet, tout élément de M a une représentation de taille λ et le temps calcul de Apply(f, x) à précision n est borné par $P(|\phi|, \lambda, n)$. La machine peut connaître x à précision au plus $2^{-P(|\phi|, \lambda, n)}$ et retournera donc le même résultat sur les éléments à cette distance de x (car ils ont une représentation avec le même préfixe de taille $P(|\phi|, \lambda, n)$). Pour calculer f_Q sur $q \in Q$ et n, il suffit d'appliquer Apply sur ϕ et la fonction θ de **Reg** constamment égale à q (et donc de taille constante : $\forall n \in \mathbb{N}, |\theta|(n) = |q|$), ce qui prend un temps $P(|\phi|, |\theta|, n)$, ce qui est polynomial en $|\phi|$, $|q|$ et n. $\square$

Cette preuve est une adaptation de celle de Kawamura, et pour obtenir le résultat original, il suffit de constater que tout réel de $[0, 1]$ admet un représentant (pour toutes les représentations décrites dans l'exemple 1) de taille linéaire (par exemple, tout réel de $[0, 1]$ peut être approximé à précision 2^{-n} par un dyadique de longueur n).

Corollaire 1

Si δ est une représentation de $\mathcal{C}[0, 1]$, alors Apply est calculable en temps polynomial (par rapport à δ et la représentation de Cauchy des réels) si et seulement si $\delta \leq_P \delta_0$.

Ce résultat permet de plus de faire le lien entre la complexité d'ordre 2 (des fonctions de M dans M' pour les représentations de Cauchy de ces deux espaces) et celle d'ordre 1 (des éléments de $\mathcal{C}(M, M')$ pour la représentation δ_0).

Proposition 3

*$f \in \mathcal{C}(M, M')$ est calculable en temps polynomial relativement à δ_0 (autrement dit, représentée via δ_0 par un élément de **Reg** calculable en temps polynomial) si et seulement si elle est calculable en temps polynomial pour les représentations δ_c et δ'_c (c'est-à-dire réalisable par une fonction polynomiale de **Reg** dans **Reg** pour ces représentations).*

Preuve

Pour le sens direct, la composition de Apply (polynomiale d'après le théorème) et f (polynomiale par hypothèse) fournit f en tant que fonction de $M \to M'$.

Inversement, la seconde partie de la preuve du théorème fournit un moyen de calculer f_m et f_Q (et donc une δ_0-représentation de f) à partir d'une machine calculant f en temps polynomial, ce qui donne le résultat. $\square$

Ce résultat permet de justifier la définition de la représentation δ_0, puisque la notion de complexité induite par celle-ci prolonge celle induite par celle de M dans M'. En particulier cela implique, d'après la définition de δ_0, qu'une fonction est calculable en temps polynomial si et seulement si elle admet une approximation f_Q sur Q calculable en temps polynomial et si elle a un module de continuité borné par un polynôme. Ce résultat a déjà été démontré, notamment par Ko [Ko91], mais est aussi valable pour des espaces métriques plus généraux (vérifiant les hypothèses du théorème) munis de leur représentation de Cauchy.

Remarque 11
Il existe d'autres moyens de représenter les fonctions continues sur $[0, 1]$*, comme par exemple en les approchant par des suites de polynômes rationnels* (δ_P) *ou des suites de fonctions linéaires par morceaux (à extrémités rationnelles) convergeant (à vitesse* 2^{-n}*) en norme infini* ($\delta_\wedge$)*. Il est alors facile de remarquer que ces représentations permettent de calculer Apply en temps polynomial et le résultat précédent implique donc qu'elles sont réductibles (pour* $\leq_P$*) à* δ_0*. On peut aussi montrer que l'inverse est faux (on peut notamment calculer la norme infini d'une limite d'une suite de fonctions linéaires par morceaux en temps polynomial, alors que cette norme n'est pas calculable en temps polynomial pour* δ_0*). Ces deux représentations sont aussi partiellement incomparables, puisque* $\delta_P \not\leq_P \delta_\wedge$ *: une fonction telle que* $x \mapsto x^2$ *est trivialement représentable en temps polynomial par une suite de fonctions polynômes, mais ne l'est pas pour une suite de fonctions linéraires par morceaux (il faut un nombre exponentiel de segments pour l'approcher à précision* 2^{-n}*). La figure 2 résume les relations entre ces représentations. Notons que ces représentations*

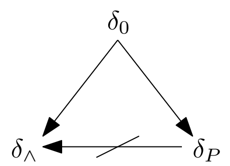

Figure 2. Comparaison de quelques représentations de $\mathcal{C}[0, 1]$ (où $\longleftarrow$ représente $<_P$).

sont des représentations de Cauchy pour différents espaces métriques effectifs sur $\mathcal{C}[0, 1]$*, alors que* δ_0 *n'est pas de cette forme.*

De façon analogue, la représentation binaire des entiers (et les représentations en base $b \geq 2$ en général) est la représentation la plus générale (c'est-à-dire maximale pour $\leq_P$) qui rende le calcul du $i^{\text{ème}}$ bit d'un nombre n calculable en temps polynomial en i et $|n|$. La représentation unaire étant strictement plus faible que les représentations en base $b \geq 2$, c'est un moyen de justifier l'utilisation de ces représentations plutôt que la représentation unaire.

De façon générale, on peut chercher la représentation maximale qui rende certains opérateurs calculables en temps polynomial.

Si δ est une représentation de M et $F : M \to M'$ (avec $M \neq M'$), alors on peut définir $\delta^F(\langle \alpha, \beta \rangle) = x$ lorsque $\delta(\alpha) = x$ et $\delta'(\beta) = F(x)$ (où $\langle , \rangle$ désigne une injection de **Reg** $\times$ **Reg** dans **Reg**). Alors δ^F est la représentation maximale qui rend F calculable en temps polynomial et qui vérifie $\delta^F \leq_P \delta$. Remarquons que l'on peut obtenir le même résultat pour n'importe quel nombre fini d'opérateurs.

Exemple 6
Par exemple, étant donné que δ_0 ne permet pas de calculer la norme infini, on peut considérer $\delta_0^{\|.\|_\infty}$ (la représentation d'une fonction contient alors explicitement une représentation de sa norme infini), qui est alors la représentation la plus générale qui rend Apply et $\|.\|_\infty$ calculables en temps polynomial. On remarque cependant que cette représentation est très faible, puisqu'elle ne permet plus de calculer la somme de deux fonctions en temps polynomial (en effet, la connaissance de $\|f\|_\infty$ et $\|g\|_\infty$ ne permet pas de déduire plus rapidement $\|f+g\|_\infty$). L'existence d'une représentation maximale rendant l'addition, la multiplication et la norme infini calculables en temps polynomiale n'est pas garantie.

3.3 Exemple : l'espace métrique des compacts de $[0, 1]$

Si X et Y sont deux compacts non vides, on définit la distance de Hausdorff de X à Y par : $d_H(X, Y) = \max(\max_{x\in X} d(x, Y), \max_{y\in Y} d(y, X))$. On vérifie que c'est effectivement une distance sur l'ensemble des compacts de $[0, 1]$.

De plus, l'ensemble des ensembles finis de rationnels de $[0, 1]$ est dense dans l'ensemble des compacts de $[0, 1]$. Cela forme un espace métrique effectif et l'on peut définir la représentation de Cauchy δ_H sur cet espace.

Remarquons tout d'abord que cette représentation permet de calculer la distance à un compact en temps polynomial.

Lemme 1
La fonction distance ($(K, x) \mapsto \min_{y\in K} |x - y|$) est calculable en temps polynomial pour la représentation δ_H.

Preuve
À partir d'une représentation de K et d'une précision n, on peut obtenir en temps polynomial une liste $x_1, \dots x_k$ (de taille polynomiale en taille de K et n) de rationnels qui approchent K en distance de Hausdorff à précision $2^{-(n+1)}$ et une approximation q à $2^{-(n+1)}$ de x. Par définition de la distance de Hausdorff, pour tout point de K, il existe un point x_i proche à $2^{-(n+1)}$. Inversement, pour tout i, il existe un point de K proche à $2^{-(n+1)}$. Donc $\min_i |q - x_i|$ est une approximation à 2^{-n} de la distance de x à K. $\square$

Remarque 12
On peut représenter un compact par sa fonction distance ($x \mapsto d(x, K)$) via la représentation δ_0 de $\mathcal{C}[0, 1]$. Notons δ_d cette représentation (voir [Bra05] pour plus d'exemples et de résultats sur cette représentation). Le lemme précédent prouve alors que $\delta_H \leq_P \delta_d$. On sait aussi que cette inégalité est stricte. En particulier, un compact calculable en temps polynomial pour δ_H est de mesure nulle, et donc ne peut contenir aucun intervalle non

vide, alors que la distance à un intervalle $[a,b]$ où a et b sont calculables en temps polynomial est calculable en temps polynomial. Les compacts de taille polynomiale pour δ_H sont en effet « petits » (de dimension nulle), au sens où des ensembles de mesure nulle comme l'ensemble triadique de Cantor peuvent être de taille exponentielle (voir figure 3 pour une illustration).

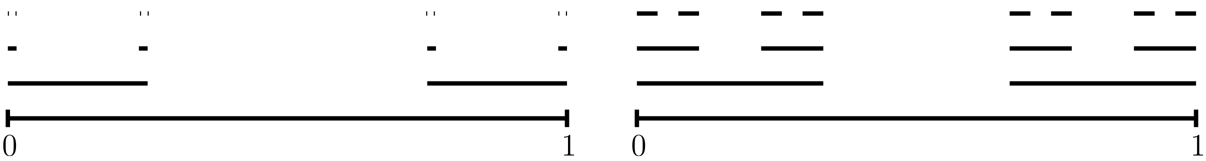

Figure 3. À gauche, un exemple de compact calculable en temps polynomial (représenté par les premières étapes de recouvrement). À droite, l'espace triadique de Cantor.

La proposition suivante permet de caractériser l'ensemble des compacts K sur lesquels on peut calculer la borne supérieure d'une fonction ($f \mapsto \sup_K f$) en temps polynomial (pour la représentation δ_0 des fonctions continues).

Théorème 2
Une représentation δ de l'ensemble des compacts de $[0,1]$ rend la fonctionnelle $K, f \mapsto \sup_K f$ calculable en temps polynomial si et seulement si $\delta \leq_P \delta_H$.

Preuve

Montrons d'abord que la fonctionnelle sup est calculable en temps polynomial relativement à δ_H. Si l'on a une δ_H-représentation de K, alors sur l'entrée f et à précision n, il suffit de demander à l'oracle le module $f_m(n+1)$, puis la liste des rationnels approchant K à cette précision. On calcule ensuite f à précision $2^{-(n+1)}$ en chacun de ces points (leur nombre est polynomial en la taille de la représentation de K, en f_m et en n) puis d'en calculer le maximum. À l'intérieur de chaque intervalle de rayon $2^{-(m(n+1)}$, f varie au plus de 2^{-n} (par définition de f_m). Le résultat obtenu est donc une approximation à 2^{-n} de $\sup_K f$. En effet, par définition de la distance de Hausdorff, tout point de K est à distance au plus $2^{-m(n+1)}$ l'un de ces points rationnels et chacun de ces points est au plus à la même distance d'un point de K.

Inversement, soit une représentation δ qui permet de calculer sup en temps polynomial via une machine $\mathcal{M}$. Soit K un compact de $[0,1]$ et notons $q_1^n, \dots q_{k_n}^n$ la liste des appels à l'oracle de $\mathcal{M}$ sur K et l'entrée représentant la fonction nulle telle que $f_Q = 0$ et $\forall n, f_m(n) = n$ (notons que k_n est borné par un polynôme en n).

Montrons tout d'abord que pour tout n, K est recouvert par les intervalles centrés en q_i^{n+2} et de rayon 2^{-n} (autrement dit, tout point de K est à distance au plus 2^{-n} de l'un des q_i^{n+2}). En effet, si ce n'est pas le cas, alors le sup sur K de la fonction distance à l'ensemble $\{q_1^{n+2}, \dots q_{k_{n+2}}^{n+2}\}$ (noté d) est strictement supérieur à 2^{-n}. Or cette fonction admet une représentation qui vaut 0 sur chacun des q_i^{n+2} (puisque la distance vaut 0 en ces points) et admet la fonction identité comme module de continuité (une fonction distance est 1−lipschitzienne). $\mathcal{M}$ a donc le même comportement (à précision $2^{-(n+2)}$) que sur la fonction nulle et retourne donc au plus $2^{-(n+2)} + 2^{-(n+2)} = 2^{-(n+1)} < d - 2^{-(n+2)}$, ce qui fournit la contradiction.

L'ensemble de rationnels précédemment décrit est alors un bon candidat pour approcher K en distance de Hausdorff. Cependant, rien n'assure que certains appels à l'oracle q_i^{n+2} ne soient inutiles et soient éloignés de K : il faut les éliminer.

Pour cela, nous avons besoin de calculer la distance de ces points à K.

Lemme 2
$\delta \leq_P \delta_d$ (en particulier, la fonction distance est calculable en temps polynomial pour cette représentation).

Preuve
Sur une entrée $x \in [0,1]$ et un compact K, on peut calculer la fonction $y \mapsto -|x-y|$ en temps polynomial. Le sup sur K de cette fonction fournit alors l'opposé de la distance de x à K. □

Pour chaque q_i^{n+4}, on calcule sa distance à K à précision $2^{-(n+2)}$. Si le résultat est strictement supérieur à $2^{-(n+1)}$, alors q_i^{n+4} est à distance au moins $2^{-(n+2)}$ de K et on l'enlève alors de l'approximation de K. Dans le cas contraire, la distance à K est au plus $2^{-(n+1)} + 2^{-(n+2)} \leq 2^{-n}$ on conserve q_i^{n+4} dans l'approximation de K. L'ensemble des points qui ont été conservées forme alors une approximation à 2^{-n} près en distance de Hausdorff de K : tout point de K est à distance au plus $2^{-(n+2)}$ de l'ensemble de ces points (en effet, les points enlevés étaient au moins à cette distance) et chacun de ces points est à distance au plus 2^{-n} de K.

Notons que la construction est polynomiale puisque sup est calculable en temps polynomial. En particulier le calcul des appels à l'oracle se fait en temps polynomial, et le calcul de leur distance à K se fait aussi en temps polynomial, d'après le lemme 2. □

De manière similaire à la proposition 3, ce théorème et sa preuve permettent de fournir un résultat non uniforme supplémentaire.

Proposition 4
Un compact K est calculable en temps polynomial (pour δ_H) si et seulement si la fonction $\sup_K : \mathcal{C}[0,1] \to \mathbb{R}$ est calculable en temps polynomial (pour la représentation δ_0 des fonctions continues et l'une des représentations usuelles de réels).

Preuve
Si K est calculable en temps polynomial, le théorème implique alors directement que la fonction $\sup_K$ l'est aussi.

Inversement, la preuve du théorème fournit un moyen de construire en temps polynomial un représentant de K pour la représentation δ_H à partir de la machine calculant $\sup_K$. □

Il serait intéressant de caractériser, si c'est possible, d'autres représentations sur le même principe (par exemple les représentations des fonctions continues décrites dans la remarque 11) puisque cette approche permet notamment de comparer facilement deux représentations et de mieux comprendre les classes de complexité qu'elle induit. Par exemple, la représentation des fonctions comme limite de suites de fonctions linéaires par morceaux ($\delta_\wedge$) permet de calculer la norme infini en temps polynomial, mais n'est pas la représentation maximale (pour δ_P) permettant de calculer Apply et $\|.\|_\infty$ en temps polynomial, puisque c'est la représentation $\delta^{\|\cdot\|_\infty}$ de l'exemple 6 (qui ne permet pas de calculer l'addition en temps polynomial, contrairement à $\delta_\wedge$). On peut se demander s'il est possible d'ajouter certaines fonctions (comme l'intégrale, la somme, le produit de fonctions) pour caractériser cette représentation.

4 Cas particulier des normes sur $\mathcal{C}[0,1]$

Contrairement à $\mathcal{C}[0,1]$, nous ne possédons pas de représentation de $\mathcal{C}[0,1] \to \mathbb{R}$ qui prolonge la calculabilité et la complexité des fonctions de $\mathcal{C}[0,1]$ dans $\mathbb{R}$, comme il a été fait dans la section 3. Nous chechons donc à mieux comprendre les implications de la calculabilité en temps polynomial pour cet ensemblen et nous intéressons ici au cas particulier des normes des fonctions continues sur $[0,1]$. La norme infini n'étant pas calculable en temps polynomial (intuitivement parce qu'elle requiert d'évaluer son argument en un nombre exponentiel de points pour une précision donnée, mais cela sera prouvé formellement par la suite), on cherche à déterminer quelles normes font partie de cette classe de complexité.

Tout d'abord, les normes calculables sont toutes plus faibles (au sens large) que la norme infini (autrement dit, toute suite qui converge vers en norme infini converge pour toute norme calculable), simplement parce qu'elles sont continues.

De plus, lorsque l'on se restreint à des compacts de $\mathcal{C}[0,1]$ pour la norme infini (c'est-à-dire un ensemble de fonctions bornées et de module donné), alors toutes les normes sont équivalentes (au sens où elles induisent la même notion de convergence).

Propriété 5
Soit F une norme continue pour $\|.\|_\infty$. Si $(f_n)_{n\in\mathbb{N}}$ est une suite de fonctions de même module de continuité m, alors ces trois points sont équivalents :

- $\lim_{n\to\infty} F(f_n) = 0$
- $\lim_{n\to\infty} ||f_n||_\infty = 0$
- $\forall x \in [0,1], \lim_{n\to\infty} f_n(x) = 0$

Preuve

La convergence en norme infini implique la convergence simple et la convergence pour F (d'après le lemme précédent).

Supposons que $(f_n)_{n\in\mathbb{N}}$ converge simplement vers 0 en tout point. Pour tout $n \in \mathbb{N}$, on peut couvrir $[0,1]$ avec un nombre fini d'intervalles de rayon au plus $2^{-m(n)}$. Pour k assez grand, $|f_k|$ est plus petit que 2^{-n} au milieu de chacun de ces intervalles. Donc par définition du module de continuité, $||f_k||_\infty \le 2^{-n+1}$ et donc $(f_n)_{n\in\mathbb{N}}$ converge en norme infini. Enfin, supposons que (f_n) converge vers 0 pour F mais pas pour $||.||_\infty$. Alors il existe une sous-suite dont la norme infini est plus grande que $\varepsilon > 0$. Comme ces fonctions sont dans un compact pour $||.||_\infty$, on peut en extraire une sous-suite convergente et sa limite est non nulle. Or, par continuité, l'image par F de cette limite est 0, ce qui donne une contradiction. □

Cependant, on ne peut rien dire dans le cas où le module de continuité n'est pas borné.

Il existe des exemples simples de normes calculables en temps polynomial :

Exemple 7
Si $(q_n)_{n\in\mathbb{N}}$ *est une suite dans* $[0,1]$ *calculable en temps polynomial énumérant un sous-ensemble dense de* $[0,1]$ *(par exemple une énumération des rationnels ou des dyadiques), alors* $F_0(f) = \Sigma_{n\in\mathbb{N}} \frac{|f(q_n)|}{2^n}$ *est une norme sur* $\mathcal{C}[0,1]$ *calculable en temps polynomial (pour la représentation* δ_0 *des fonctions). On vérifie en effet que c'est une norme et pour calculer* $F_0(f)$*, on calcule une borne supérieure* 2^k *de* $|f|$ *à partir de* $f(0)$ *et du module de* f*, puis on calcule* f *à précision suffisante sur* $q_0, \dots q_{n+k+1}$ *(c'est un nombre polynomial d'évaluations).*

Il est facile de montrer que la norme infini est calculable en temps exponentiel : si m est un module pour f, on peut couvrir $[0,1]$ avec un nombre exponentiel en $m(n)$ intervalles sur lesquels f varie au plus de 2^{-n} et il suffit alors d'évaluer f en chacun de ces intervalles.

Le théorème suivant permet de montrer que toutes les normes calculables en temps polynomial sont strictement plus faibles que la norme infini (et donc que celle-ci n'est pas calculable en temps polynomial).

Théorème 3
Il n'existe pas de norme sur $\mathcal{C}[0,1]$ *calculable en temps polynomial équivalente à la norme infini. Autrement dit, si* F *est calculable en temps polynomial alors il existe une suite de fonctions convergeant vers* 0 *pour* F *mais pas en norme infini.*

Preuve
Soit F une norme calculée par une machine $\mathcal{M}$ fonctionnant en temps polynomial. On considère la fonction nulle représentée par 0 en tout rationnel et de module identité ($n \mapsto n$). Sur cette entrée et à précision n, $\mathcal{M}$ fait un nombre polynomial en n de requêtes à l'oracle, notées $q_1^n, \dots, q_{k_n}^n$. Soit g_n la fonction distance à l'ensemble $\{q_1^n, \dots, q_{k_n}^n\}$. L'identité est aussi un module de continuité pour cette fonction et elle admet une représentation qui vaut 0 en chacun des q_i^n, donc $\mathcal{M}$ ne peut la distinguer de la fonction nulle à précision 2^{-n} et alors $F(g_n) \leq 2^{-n}$. On a de plus $||g_n||_\infty = max_{0\leq i\leq k_n} \frac{(q_{i+1}^n - q_i^n)}{2}$ (avec $q_0 = 0$ et $q_{k_n+1} = 1$). Cela divise $[0,1]$ en $k_n + 1$ intervalles, donc il y en a au moins un de taille supérieure à $\frac{1}{k_n+1}$, d'où $||g_n||_\infty \geq \frac{1}{2(k_n+1)} \geq \frac{1}{2(P(n)+1)}$ (où P est un polynôme bornant le nombre d'appels). Alors $h_n = (k_n + 1)g_n$ converge vers 0 pour F mais pas en norme infini. $\square$

Corollaire 2
Ce résultat implique immédiatement que $\|.\|_\infty$ *n'est pas calculable en temps polynomial.*

La preuve de ce résultat peut être facilement adaptée pour prouver un résultat plus fort : la convergence pour une norme calculable en temps polynomial n'implique pas non plus la convergence en probabilité (f_n converge en probabilité vers 0 si pour tout $\varepsilon > 0$, la mesure de $f_n^{-1}\mathbb{R} \setminus [-\varepsilon, \varepsilon]$ tend vers 0).

Théorème 4
Si F *est calculable en temps polynomial, alors il existe une suite de fonctions convergeant vers* 0 *pour* F *mais pas en probabilité.*

Preuve

Soient h_n les fonctions définies dans la preuve du théorème 3. Pour montrer qu'elles ne convergent pas en probabilité, il suffit de montrer que la mesure de l'ensemble où elles sont plus grandes qu'une constante (on choisit ici $\frac{1}{4}$) ne converge pas vers 0. D'après la définition de h_n, la mesure de cet ensemble est la somme sur les intervalles de la forme $[q_i, q_{i+1}]$ plus grand que $\frac{1}{2(k_n+1)}$ de $q_i^n - q_{i+1}^n - \frac{1}{2(k_n+1)}$. Cette somme est minimale lorsque tous les intervalles ont la même taille et dans ce cas elle vaut $1 - \frac{k_n}{2(k_n+1)} \geq \frac{1}{2}$. $\square$

Remarque 13
Ce résultat permet de distinguer plus de normes non calculables en temps polynomial, par exemple la norme $\|.\|_1 : f \mapsto \int_0^1 |f|$*, dont la convergence implique la convergence en probabilité mais pas en norme infini.*

5 Conclusion

La théorie de la complexité sur des objets quelconques a été assez peu développée (contrairement à la calculabilité) ou seulement dans des cas bien particuliers (notamment celui des réels). Nous nous sommes donc attachés à poursuivre l'approche et les résultats de Kawamura et Cook [KC10] notamment via les théorèmes 1 et 2 qui décrivent les représentations rendant certaines fonctions (en l'occurence Apply et sup) calculables en temps polynomial. Cela permet d'en déduire les propositions 3 et 4 qui caractérisent respectivement les fonctions et les compacts calculables en temps polynomial pour les représentations considérées.

Ces résultats décrivent une méthode générale consistant à caractériser une représentation par un ensemble fini de fonctions qu'elle rend calculable « efficacement ». Cela permet entre autres de mieux comprendre les classes de complexité qu'elle induit et de justifier son utilisation. Cela soulève diverses questions. Étant donnée une algèbre de fonctions (par exemple les fonctions réelles munies des opérateurs usuels tels que l'addition, la multiplication, la norme infini ou l'intégration), existe-t-il une représentation rendant les opérateurs de l'algèbre calculables en temps polynomial et dans ce cas, en existe-t-il une maximale pour $\leq_P$?

Nous nous sommes aussi intéressés à l'espace des fonctions de $\mathcal{C}[0,1]$ dans $\mathbb{R}$ pour lequel nous ne connaissons pas de représentation prolongeant la notion de complexité relative à δ_0 et δ_c (de même que δ_0 induit la même notion de complexité que celle induite par δ_c, d'après la proposition 3). Cet exemple ne rentre pas dans le cadre des espaces métriques effectifs et on peut alors se demander quelle structure plus fine pourrait rendre compte de la complexité sur un tel espace.

Il serait aussi intéressant d'obtenir une caractérisation des fonctions de $\mathcal{C}[0,1]$ dans $\mathbb{R}$ calculables en temps polynomial, notion du second ordre, exprimée en termes de complexité au premier ordre, de même que la complexité des fonctions de $[0,1]$ dans $\mathbb{R}$ peut se ramener à la complexité des fonctions f_Q et f_m définies sur les entiers. Un tel résultat permettrait de mieux comprendre la « forme » des fonctions de $\mathcal{C}[0,1]$ dans $\mathbb{R}$ calculables en temps polynomial, de même que l'on sait qu'une fonction $f : \mathbb{N} \to \mathbb{N}$ calculable en temps P est bornée par $n \mapsto 2^{P(n)}$ pour la représentation binaire des entiers, ou qu'une fonction de $\mathbb{R} \to \mathbb{R}$ calculable en temps polynomial admet un module de continuité borné par un polynôme.

Références

BCGH07. O. Bournez, M. L. Campagnolo, D. S. Graça et E. Hainry – « Polynomial differential equations compute all real computable functions on computable compact intervals », *Journal of Complexity* **23** (2007), no. 3, p. 317 – 335.

BCSS98. L. Blum, F. Cucker, M. Shub et S. Smale – *Complexity and real computation*, Springer, 1998.

Bra05. M. Braverman – « On the complexity of real functions », *FOCS*, 2005, p. 155–164.

Cob65. A. Cobham – « The Intrinsic Computational Difficulty of Functions », *Logic, methodology and philosophy of science III : proceedings of the Third International Congress for Logic, Methodology and Philosophy of Science, Amsterdam 1967*, North-Holland Pub. Co., 1965, p. 24.

KC96. B. Kapron et S. Cook – « A new characterization of type-2 feasibility », *SIAM Journal on Computing* **25** (1996), no. 1, p. 117–132.

KC10. A. Kawamura et S. Cook – « Complexity theory for operators in analysis », *Proceedings of the 42nd ACM Symposium on Theory of Computing* (New York, NY, USA), STOC '10, ACM, 2010, p. 495–502.

Ko91. K.-I. Ko – *Complexity Theory of Real Functions*, Birkhauser Boston Inc. Cambridge, MA, USA, 1991.

KS05. D. Kunkle et M. Schröder – « Some examples of non-metrizable spaces allowing a simple type-2 complexity theory », *Electr. Notes Theor. Comput. Sci.* **120** (2005), p. 111–123.

Sha41. C. E. Shannon – « Mathematical theory of the differential analyzer », *J. Math. Phys. MIT* **20** (1941), p. 337–354.

Wei00. K. Weihrauch – *Computable Analysis : An Introduction*, Springer Verlag, 2000.