Le système formel $\mathbf{RCA}_0$ et l'analyse calculable

David Waszek
Dans le cadre du séminaire de M2 de Marco Panza

28 juin 2013

Introduction

Le projet de « mathématiques à l'envers » de Friedman et Simpson (voir [Simpson, 1999] pour une présentation détaillée) consiste à isoler les postulats minimaux d'existence nécessaires à la démonstration de tel ou tel théorème des mathématiques classiques. Le cadre choisi par ces auteurs est celui de l'arithmétique du second ordre $\mathbf{Z}_2$, dans laquelle une grande part des mathématiques peut être formalisée. La question posée est alors la suivante : si l'on remplace le schème de compréhension habituel suivant :

$$\exists X \, \forall n \, (n \in X \leftrightarrow \phi(n)), \tag{1}$$

qui postule l'existence de tout ensemble définissable par une formule du second ordre ϕ, par des postulats d'existence plus faibles, quels sont les théorèmes que l'on peut encore démontrer ? Un exemple simple de sous-système de l'arithmétique est le système $\mathbf{ACA}_0$: on l'obtient en ne postulant (1) que pour des formules *arithmétiques*, c'est-à-dire pour des formules ϕ sans quantification sur des ensembles. Ce système suffit pour démontrer la complétude des nombres réels, mais pas, par exemple, pour prouver qu'une fonction continue sur un compact est uniformément continue (théorème de Heine).

Mais les « mathématiques à l'envers » ont une autre dimension, que l'on pourrait appeler sémantique. On travaille ici dans le cadre de la *sémantique de Henkin*, dans laquelle on s'autorise à faire varier non seulement l'ensemble dans lequel les variables du premier ordre prennent leurs valeurs, mais également l'ensemble des valeurs possibles des variables du deuxième ordre (voir ci-dessous, conventions générales). Les sous-systèmes de $\mathbf{Z}_2$ admettent alors des modèles qui ont les entiers standard pour ensemble d'individus, mais

dans lesquels seulement certains sous-ensembles des entiers existent ; par exemple, le sous-système $\mathbf{ACA}_0$ évoqué plus haut admet un modèle dans lequel n'existent que les ensembles qui peuvent être définis par des formules arithmétiques. Ces modèles peuvent être d'autant plus pauvres existentiellement que les postulats du sous-système correspondant sont plus faibles. Ils reflètent les limitations que l'on s'est imposées dans le sous-système concerné, mais peuvent être étudiés avec tous les outils des mathématiques classiques. En bref, si le premier point de vue considérait les théorèmes démontrés dans un sous-système de $\mathbf{Z}_2$ comme les mêmes théorèmes qu'en mathématiques classiques, mais démontrés sur la base de postulats d'existence minimaux, le second point de vue y voit des théorèmes valables dans des univers mathématiques moins riches que l'univers habituel.

Le but de ce travail est d'illustrer cette seconde dimension dans un cas particulier, celui des mathématiques constructives — correspondant approximativement au système $\mathbf{RCA}_0$ — sur l'exemple de l'analyse élémentaire (définition des réels, suites de réels, fonctions réelles continues, et leurs propriétés élémentaires). L'idée de départ est la suivante : au lieu de ne s'autoriser que des opérations « effectives » dans un sens vague, et de travailler avec une logique intuitionniste, comme l'exige le programme constructiviste (dans le cas de l'analyse, cette approche est représentée par [Bishop et Bridges, 1985]), on peut travailler de manière classique sur des objets *calculables* au sens formel que procure la théorie de la calculabilité. Cette traduction n'est pas directement fidèle, mais rien ne semble véritablement y être perdu (nous reviendrons sur ce point au cours de notre travail). Une fois cette traduction effectuée, il est possible d'isoler un sous-système $\mathbf{RCA}_0$ de $\mathbf{Z}_2$ dont les postulats sont juste assez forts pour n'exiger l'existence dans ses modèles que des objets calculables ; les résultats que ce système formel permet de démontrer sont essentiellement ceux dont la reformulation dans un cadre calculable est valable.

Conventions générales, rappels

À la manière de Simpson [Simpson, 1999], nous travaillons dans le cadre d'une logique du deuxième ordre. Plus précisément, nous utilisons un langage à *deux sortes*, qui contient, en plus des symboles logiques usuels (connecteurs propositionnels et quantificateurs),

- des variables d'individus ou variables *numériques*, que nous noterons par des minuscules (a, b, m, n, x, y, *etc.*) ;
- des variables d'ensembles, que nous noterons par des majuscules (A, B, X, Y, *etc.*).

De surcroît, le langage de base est équipé de symboles de relation $\in$ et $=$ qui permettent la formation des formules atomiques $t \in T$ et $t_1 = t_2$, pour t, t_1, t_2 des termes d'individu et T un terme d'ensemble.

Une *théorie* $\mathbb{T}$ est alors un ensemble d'axiomes écrits dans ce langage de base potentiellement enrichi de symboles supplémentaires. Un *modèle* $M = (|M|, \mathcal{S}_M, \ldots)$ de $\mathbb{T}$ consiste en la donnée

- d'un ensemble $|M| \neq \emptyset$ qui sert à l'interprétation des variables d'individus,
- d'une partie $\emptyset \neq \mathcal{S}_M \subseteq \mathcal{P}(|M|)$ qui sert à l'interprétation des variables d'ensembles,
- d'une interprétation appropriée des éventuels symboles supplémentaires du langage

tels que tous les axiomes de $\mathbb{T}$ soient vrais (la relation $\in$ étant interprétée comme l'appartenance entre éléments de $|M|$ et parties de $|M|$, et la relation $=$ comme l'égalité entre éléments de $|M|$). Remarquons que les valeurs des variables d'ensembles sont ici limitées à un sous-ensemble de $\mathcal{P}(|M|)$: on parle parfois de *sémantique de Henkin* pour distinguer cette sémantique de la sémantique habituelle en logique du second ordre.

Le langage de l'*arithmétique du second ordre* comporte cinq symboles supplémentaires : deux symboles d'opérations (entre individus) $+$ et $\cdot$, un symbole de relation (entre individus) $<$ et deux symboles de constantes d'individu 0 et 1. L'arithmétique du second ordre comporte, outre huit axiomes du premier ordre portant sur $+$, $\cdot$ et $<$ que nous ne reproduisons pas (voir [Simpson, 1999, p. 4]) un axiome de récurrence :

$$\forall X \left[\big(0 \in X \wedge \forall n (n \in X \to n+1 \in X)\big) \to \forall n (n \in X) \right]$$

et un schème de compréhension : pour toute formule $\phi(n)$ dans laquelle X n'apparaît pas de manière libre, on a la clôture universelle de

$$\exists X \, \forall n \, (n \in X \leftrightarrow \phi(n)).$$

Un *sous-système* de l'arithmétique du second ordre est une variante de cette théorie dans laquelle le schème de compréhension et éventuellement l'axiome d'induction ci-dessus ont été remplacés par des variantes plus faibles. On appelle $\boldsymbol{\omega}$-modèle d'un tel sous-système de l'arithmétique tout modèle de la forme

$$(\boldsymbol{\omega}, \mathcal{S} \subseteq \mathcal{P}(\boldsymbol{\omega}), +_{\boldsymbol{\omega}}, \cdot_{\boldsymbol{\omega}}, <_{\boldsymbol{\omega}}, 0_{\boldsymbol{\omega}}, 1_{\boldsymbol{\omega}})$$

où $+_{\boldsymbol{\omega}}$, $\cdot_{\boldsymbol{\omega}}$, *etc.* désignent les opérations usuelles $+$, $\cdot$, *etc.* dans $\boldsymbol{\omega}$. Un tel modèle est donc entièrement déterminé par la donnée de $\mathcal{S}$.

Nous disons qu'une formule est *arithmétique* dès lors qu'elle ne comporte pas de quantificateurs d'ensembles.

Nous notons $\boldsymbol{\omega} = \{0, 1, 2, \ldots\}$ l'ensemble usuel des entiers.

1 Préliminaires

1.1 Calculabilité

Notre objectif ici est double. Nous souhaitons d'une part effectuer un bref survol des quelques résultats élémentaires de théorie de la calculabilité que nous utiliserons. Pour ce faire, nous nous satisferons d'une approche informelle fondée sur l'idée intuitive de calculabilité algorithmique. D'autre part, nous voulons donner une définition précise des notions de fonction récursive, d'ensemble récursif et d'ensemble récursivement énumérable, de manière à pouvoir en formuler précisément une petite généralisation, légèrement moins classique, qui nous sera nécessaire ; et surtout de manière à pouvoir donner une preuve à peu près rigoureuse des lemmes 1.18 et 1.22 (section suivante), indispensables pour faire le lien entre le système $\mathbf{RCA}_0$ et la théorie de la calculabilité.

En l'absence de précision supplémentaire, *fonction* signifie dans cette section fonction $\boldsymbol{\omega}^k \to \boldsymbol{\omega}$ pour un entier k, et *ensemble* signifie sous-ensemble de $\boldsymbol{\omega}^k$ pour un entier k.

1.1.1 Fonctions récursives

Nous donnons ici une définition formelle de la notion de *fonction récursive*, avant d'en donner une caractérisation intuitive. Tout d'abord, une définition préliminaire.

Définition 1.1. Soit $g : \boldsymbol{\omega}^{k+1} \to \boldsymbol{\omega}$ une fonction telle que

$$\forall x_1, \ldots, x_k \exists y \, (g(x_1, \ldots, x_k, y) = 0).$$

On dit que $f : \boldsymbol{\omega}^k \to \boldsymbol{\omega}$ est définie à partir de g par *schéma* μ si

$$f(x_1, \ldots, x_k) = \min\{y \mid g(x_1, \ldots, x_k, y) = 0\}.$$

On note $f(x_1, \ldots, x_k) = \mu y(g(x_1, \ldots, x_k, y) = 0)$.

Définition 1.2. L'ensemble des *fonctions récursives* (totales) est le plus petit ensemble de fonctions contenant :

- les projections $(x_1, \ldots, x_k) \mapsto x_i$;
- la somme $(x_1, x_2) \mapsto x_1 + x_2$ et le produit $(x_1, x_2) \mapsto x_1 \cdot x_2$;

– la fonction caractéristique de l'égalité

$$(x_1, x_2) \mapsto \begin{cases} 1 & \text{si } x_1 = x_2 \\ 0 & \text{sinon,} \end{cases}$$

et clos par composition et schéma μ.

Remarque 1.3. Notons $\mathcal{C}_0$ l'ensemble des fonctions initiales, et pour $i \geq 1$, notons $\mathcal{C}_i$ l'ensemble des fonctions que l'on peut obtenir à partir de fonctions de $\mathcal{C}_{i-1}$ par une opération de composition ou une application du schéma μ. Alors

$$\mathcal{C} = \bigcup_{i \geq 0} \mathcal{C}_i$$

est le plus petit ensemble contenant $\mathcal{C}_0$ et clos par composition et schéma μ. On voit ainsi que toute fonction récursive peut être obtenue par une suite finie de compositions et d'applications du schéma μ à partir des fonctions initiales ; l'ensemble des fonctions récursives est donc dénombrable.

Nous avons l'équivalence fondamentale suivante. Pour la rendre précise, il faudrait formaliser une notion particulière de calculabilité, par exemple à la manière de Turing (cf. [Odifreddi, 1989, chap. I]).

Affirmation informelle 1.4. *Une fonction est récursive si et seulement si elle est « algorithmiquement calculable ».*

Nous donnons à présent une généralisation des définitions précédentes, qui capture la notion de calculabilité relative.

Définition 1.5. Pour $g_1, \ldots, g_k$ données, l'ensemble des *fonctions récursives relativement à* $g_1, \ldots, g_k$ est le plus petit ensemble de fonctions contenant $g_1, \ldots, g_k$ ainsi que les mêmes fonctions initiales que précédemment, et clos par les mêmes opérations. On dit souvent qu'une fonction f de cet ensemble est *Turing-réductible* à $g_1, \ldots, g_k$.

Comme précédemment, on a la caractérisation suivante.

Affirmation informelle 1.6. *Une fonction est récursive relativement à $g_1, \ldots, g_k$ si et seulement si elle est « algorithmiquement calculable » étant donné des « oracles » capables de fournir toute valeur demandée de $g_1, \ldots, g_k$.*

1.1.2 Ensembles récursifs, récursivement énumérables

Nous définissons ici les notions d'ensemble récursif et récursivement énumérable et en donnons quelques propriétés fondamentales, que nous justifions informellement. Nous en donnons ensuite une généralisation au cas relatif, comme ci-dessus.

Définition 1.7. Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est *récursif* si sa fonction caractéristique χ_A est récursive.

Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est donc récursif s'il existe une procédure algorithmique de *décision* capable de répondre, pour tout k-uplet d'entiers, s'il appartient ou non à A.

Remarque 1.8. Tout ensemble fini est récursif, et le complémentaire d'un ensemble récursif est encore récursif.

Informellement, un ensemble $A \subseteq \boldsymbol{\omega}^k$ est récursivement énumérable s'il existe un programme à k entrées qui termine et renvoie 1 si le k-uplet fourni est dans A, et ne termine pas ou renvoie 0 sinon ; en d'autres termes, s'il existe une procédure algorithmique capable de *confirmer* qu'un k-uplet donné appartient à A. Cette notion est plus faible que celle d'ensemble récursif : il peut exister une telle procédure de confirmation mais pas de procédure de décision pour A (voir ci-dessous).

Une formalisation correcte de la définition que nous venons de donner requiert la notion de *fonction partielle récursive*, que nous ne développerons pas ici (voir par exemple [Odifreddi, 1989, p. 126 *sq.*]). Nous donnons ici une définition sans doute plus obscure, dont nous justifions informellement l'équivalence avec la précédente.

Définition 1.9. Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est *récursivement énumérable* si et seulement si A est projection d'un ensemble récursif, i.e. s'il existe un ensemble récursif $B \subseteq \boldsymbol{\omega}^{k+1}$ tel que

$$A = \{(x_1, \ldots, x_k) \mid \exists y,\, (x_1, \ldots, x_k, y) \in B\}.$$

Justification informelle. Supposons qu'il existe une procédure de confirmation pour A au sens ci-dessus. L'ensemble

$$B = \left\{ (x_1, \ldots, x_k, t) \;\middle|\; \begin{array}{l} \text{La procédure de confirmation sur l'entrée} \\ x_1, \ldots, x_k \text{ a terminé au bout de } t \text{ étapes élé-} \\ \text{mentaires de calcul} \end{array} \right\}$$

convient. Réciproquement, s'il existe un B convenable, on obtient une procédure de confirmation comme suit. Soient $(x_1, \ldots, x_k)$ donnés. On applique

successivement, pour chaque $y \in \boldsymbol{\omega}$, la procédure de décision de B à l'entrée $(x_1, \ldots, x_k, y)$; on s'arrête dès qu'on rencontre un y tel que $(x_1, \ldots, x_k, y) \in B$. Ce programme terminera pour l'entrée $(x_1, \ldots, x_k)$ si et seulement ce k-uplet est dans A. □

Remarque 1.10. Dans le cas d'un ensemble $A \subseteq \boldsymbol{\omega}$, on rencontre souvent la caractérisation suivante, qui justifie l'expression employée : A est récursivement énumérable si et seulement s'il existe un algorithme qui énumère A sans répétitions, i.e. une fonction récursive injective $f : \boldsymbol{\omega} \to \boldsymbol{\omega}$ telle que $A = \operatorname{Im} f = \{f(0), f(1), \ldots\}$. Or s'il existe une telle fonction f, le graphe

$$\Gamma_f = \{(n, f(n)) \mid n \in \boldsymbol{\omega}\}$$

de f est récursif puisque f est récursive, et $A = \operatorname{Im} f$ est la projection de Γ_f sur la seconde variable : donc A est récursivement énumérable. Réciproquement, s'il existe une procédure de confirmation pour A, on parcourt les couples (n, t) (par exemple dans un ordre « zig-zag »), et pour chacun de ces couples, on exécute t étapes de la procédure de confirmation pour n ; on énumère n si cette procédure a terminé en exactement t étapes.

On a l'équivalence essentielle suivante.

Proposition 1.11. *Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est récursif si et seulement si A et son complémentaire $\boldsymbol{\omega}^k \setminus A$ sont récursivement énumérables.*

Preuve informelle. La procédure de décision de A donne immédiatement une procédure de confirmation pour A et une pour son complémentaire. Réciproquement, si l'on possède deux telles procédures de confirmation, il suffit de les faire fonctionner en parallèle (i.e. faire alternativement une étape de calcul de l'une et de l'autre) jusqu'à ce que l'une d'elles termine. □

Comme nous l'avons annoncé ci-dessus, *récursivement énumérable* est plus faible que *récursif*. Le résultat suivant fonde toutes les différences que nous étudierons entre l'analyse calculable et l'analyse usuelle.

Théorème 1.12. *Il existe un ensemble $A \subseteq \boldsymbol{\omega}$ récursivement énumérable, mais non récursif.*

Preuve informelle. Supposons que nous ayons choisi une formalisation précise de la notion de programme prenant un entier en entrée et (s'il termine) retournant un entier, i.e. grossièrement parlant que nous ayons fixé un « langage de programmation » ; tous les programmes possibles sont alors représentables par des suites finies de caractères d'un certain alphabet fini, donc

par des entiers. On appelle l'entier associé à un programme *indice* de ce programme.

On peut alors concevoir un programme à deux entrées, dit *universel*, qui, pour un couple (i, n) :

– ne termine pas si i n'est pas l'indice d'un programme à une entrée ;

– simule le fonctionnement du programme d'indice i sur l'entrée n sinon.

Notons U un tel programme.

Considérons l'ensemble A des indices de programmes qui terminent sur leur propre indice, i.e.

$$A = \{i \in \boldsymbol{\omega} \mid U \text{ termine sur l'entrée } (i, i)\}.$$

Il est récursivement énumérable, car $n \in A$ si et seulement si le programme universel s'arrête sur l'entrée (n, n).

Il n'est pas récursif car son complémentaire n'est pas récursivement énumérable (proposition 1.11) : il s'agit en effet de l'ensemble des indices de programmes qui ne s'arrêtent pas sur leur propre indice. Supposons qu'il existe un programme à une entrée i s'arrêtant ssi $i \in \boldsymbol{\omega} \setminus A$: il s'arrêterait ssi $i \notin A$, donc ssi le programme d'indice i ne s'arrête pas sur l'entrée i. Considérons maintenant l'indice d de ce programme : sur l'entrée d, s'il s'arrête, il devrait ne pas s'arrêter ; et s'il ne s'arrête pas, il devrait s'arrêter. Un tel programme ne peut donc exister et A n'est pas récursif. □

Nous donnons pour finir la généralisation annoncée des définitions précédentes.

Définition 1.13. Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est *récursif relativement à des ensembles* $X_1, \ldots, X_k$ si sa fonction caractéristique χ_A est récursive relativement aux fonctions caractéristiques $\chi_{X_1}, \ldots, \chi_{X_k}$. Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est *récursivement énumérable relativement à des ensembles* $X_1, \ldots, X_k$ s'il est projection d'un ensemble récursif relativement à $X_1, \ldots, X_k$.

La proposition 1.11 s'étend immédiatement à ce contexte.

1.2 Hiérarchie arithmétique

Avant de pouvoir faire le lien entre les réels calculables, que l'on construit à partir des sous-ensembles récursifs de $\mathbf{N}$, et les théorèmes du système formel $\mathbf{RCA}_0$, il nous faut donner les bases d'une classification des sous-ensembles de $\boldsymbol{\omega}$ du point de vue de la complexité logique des formules nécessaires à leur définition.

Définition 1.14. On dit qu'une formule ϕ est Σ_0^0 (ou Π_0^0) si tous les quantificateurs qui apparaissent dans ϕ sont numériques et bornés. Pour $n > 0$, on dit qu'une formule ϕ est Σ_n^0 (resp. Π_n^0) si elle est de la forme

$$\exists x_1 \exists x_2 \cdots \exists x_k \, \psi \text{ (resp. } \forall x_1 \forall x_2 \cdots \forall x_k \, \psi)$$

où ψ est une formule Π_{n-1}^0 (resp. Σ_{n-1}^0).

Une formule arithmétique est donc dans l'une de ces catégories dès lors que tous ses quantificateurs non bornés sont regroupés en tête de formule ; l'indice n correspond au nombre d'alternances entre $\exists$ et $\forall$ dans ce préfixe, et la formule est Σ ou Π suivant la nature de son premier quantificateur.

Remarquons qu'une formule Σ_n^0 ou Π_n^0 peut contenir des variables libres (mais pas liées) d'ensembles.

Définition 1.15.

1. Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est Σ_n^0 (resp. Π_n^0) s'il existe une formule Σ_n^0 (resp. Π_n^0) à k variables numériques libres et sans variable d'ensemble $\phi(n_1, \ldots, n_k)$ telle que

   $$A = \{(n_1, \ldots, n_k) \in \boldsymbol{\omega}^k \mid \phi(n_1, \ldots, n_k)\}.$$

   On dit alors que A est *défini* par la formule ϕ.
2. Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est Δ_n^0 s'il est à la fois Σ_n^0 et Π_n^0, c'est-à-dire s'il peut être défini à la fois par une formule Σ_n^0 et par une formule Π_n^0.
3. Un ensemble est *arithmétique* s'il est Σ_n^0 ou Π_n^0 pour un $n \in \boldsymbol{\omega}$.

Remarque 1.16. Toute formule arithmétique est logiquement équivalente à une formule Σ_n^0 ou Π_n^0 (des manipulations élémentaires permettent en effet de déplacer tous les quantificateurs en tête de formule ; voir par exemple [Odifreddi, 1989, p. 366]). Un ensemble est donc arithmétique si et seulement s'il peut être défini par une formule arithmétique.

Remarque 1.17. La négation d'une formule Σ_n^0 est logiquement équivalente à une formule Π_n^0 et réciproquement (à équivalence logique près, on a en effet $\neg\exists = \forall\neg$ et $\neg\forall = \exists\neg$). Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est donc Σ_n^0 si et seulement si son complémentaire $\boldsymbol{\omega}^k \setminus A$ est Π_n^0.

On peut alors faire le lien entre le premier niveau de cette hiérarchie et les notions de base de la théorie de la calculabilité. Nous utiliserons de manière essentielle le lemme suivant.

Lemme 1.18. *Tout ensemble récursif $A \subseteq \boldsymbol{\omega}^k$ est Σ_1^0.*

Preuve. Nous allons montrer que pour toute fonction récursive $f : \boldsymbol{\omega}^k \to \boldsymbol{\omega}$, il existe une formule Σ_1^0 à $k+1$ variables libres $\phi_f(x_1, \ldots, x_k, y)$ qui *définit* f au sens où

$$f(x_1, \ldots, x_k) = y \quad \text{ssi} \quad \phi_f(x_1, \ldots, x_k, y).$$

La conclusion en découle en prenant $f = \chi_A$ et en remplaçant y par la constante 1 dans la formule correspondante.

Suivons la définition 1.2.

- Les fonctions initiales sont visiblement définissables par des formules sans quantificateurs.
- Si
$$f(x_1, \ldots, x_k) = g(h_1(x_1, \ldots, x_k), \ldots, h_m(x_1, \ldots, x_k))$$
et que g, h_1, … , h_m sont représentées par ϕ_g, ϕ_{h_1}, … , ϕ_{h_m} respectivement, toutes Σ_1^0, alors f est représentée par
$$\exists z_1, \ldots, z_m \left[\left(\bigwedge_{i=1}^{m} \phi_{h_i}(x_1, \ldots, x_k, z_i) \right) \wedge \phi_g(z_1, \ldots, z_m, y) \right].$$
Tous les quantificateurs existentiels apparaissant en tête des ϕ_{h_i} et de ϕ_g peuvent être ramenés en début de formule : on obtient ainsi une formule Σ_1^0 représentant f. Remarquons pour la suite que, les x_j étant fixés, la valeur des z_i dans cette formule est déterminée de manière unique par les conditions $\phi_{h_i}(x_1, \ldots, x_k, z_i)$. Cela nous permet d'écrire $\neg\phi_f$ comme
$$\exists z_1, \ldots, z_m \left[\left(\bigwedge_{i=1}^{m} \phi_{h_i}(x_1, \ldots, x_k, z_i) \right) \wedge \neg\phi_g(z_1, \ldots, z_m, y) \right],$$
et nous autorise si besoin à permuter librement les $\exists z_i$ avec tout quantificateur portant sur une variable autre que les x_j.
- Pour finir, soit
$$f(x_1, \ldots, x_k) = \mu y(g(x_1, \ldots, x_k, y) = 0)$$
et supposons que g est définie par une formule ϕ_g qui est Σ_1^0. Considérons alors
$$\phi_g(x_1, \ldots, x_k, y, 0) \wedge (\forall z < y,\ \neg\phi_g(x_1, \ldots, x_k, z, 0)).$$
Tous les quantificateurs existentiels qui peuvent se trouver dans ϕ_g y ont été introduits par composition ; d'après les remarques ci-dessus, on peut donc écrire $\neg\phi_g$ avec des quantificateurs existentiels exclusivement (et éventuellement des quantificateurs bornés), puis permuter ceux-ci avec $\forall z < y$. Cette formule est donc logiquement équivalente à une formule Σ_1^0.

Toute fonction récursive pouvant être obtenue à partir des fonctions initiales par un nombre fini de compositions et d'applications du schéma μ (remarque 1.3), cela achève la preuve. □

Nous pouvons alors démontrer :

Proposition 1.19. *Soit $A \subseteq \boldsymbol{\omega}$.*

(i) A est Σ_1^0 si et seulement si A est récursivement énumérable.

(ii) A est Δ_1^0 si et seulement si A est récursif.

Preuve. (i) Tout ensemble défini par une formule Σ_0^0 est récursif (tous les quantificateurs d'une telle formule étant bornés, on a une procédure de décision évidente). Un ensemble Σ_1^0 est par définition projection d'un ensemble Σ_0^0, donc récursivement énumérable. Réciproquement, le lemme précédent nous garantit que tout ensemble récursif peut être défini par une formule Σ_1^0 ; toute projection d'un ensemble récursif peut donc toujours être défini par une formule Σ_1^0.

(ii) A est $\Delta_1^0 \Leftrightarrow A$ est Σ_1^0 et $\Pi_1^0 \Leftrightarrow A$ est Σ_1^0 et $\boldsymbol{\omega} \setminus A$ est Σ_1^0 (remarque 1.17) $\Leftrightarrow A$ et son complémentaire sont récursivement énumérables $\Leftrightarrow A$ est récursif (proposition 1.11).

□

Remarque 1.20. Il est plus usuel de définir la hiérarchie arithmétique en partant, au niveau 0, de la classe des ensembles récursifs : on dit qu'un ensemble est Σ_n^0, par exemple, s'il est définissable par (pour R un prédicat définissant un ensemble récursif)

$$Q_1 x_1 \dots Q_k x_k \; R(x_1, \dots, x_m)$$

avec $Q_i \in \{\forall, \exists\}$ pour tout i, $Q_1 = \exists$ et avec n alternances entre $\exists$ et $\forall$ dans le préfixe. Dans la mesure où chaque quantificateur $\exists$ correspond à une projection, et où chaque quantificateur $\forall$ (logiquement équivalent à $\neg\exists\neg$) correspond à un passage au complémentaire suivi d'une projection et d'un second passage au complémentaire, on obtient immédiatement la caractérisation suivante des ensembles arithmétiques : ce sont exactement ceux que l'on peut obtenir à partir d'un ensemble récursif par une suite finie de projections et de complémentations.

Les ensembles Σ_1^0 sont alors exactement les projections d'ensembles récursifs, soit les ensembles récursivement énumérables. Les deux définitions sont donc équivalentes à partir du niveau 1.

Nous généralisons maintenant ce développement au cas relatif. Reprenons tout d'abord la définition de la hiérarchie arithmétique.

Définition 1.21. Soient $A_1 \subseteq \boldsymbol{\omega}^{k_1}$, ..., $A_m \subseteq \boldsymbol{\omega}^{k_m}$.

1. Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est $\Sigma_n^{0,A_1,\ldots,A_m}$ (resp. $\Pi_n^{0,A_1,\ldots,A_m}$) s'il existe une formule Σ_n^0 (resp. Π_n^0) à m variables libres d'ensembles et k variables numériques libres $\phi(X_1, \ldots, X_m, n_1, \ldots, n_k)$ telle que
$$A = \{(n_1, \ldots, n_k) \in \boldsymbol{\omega}^k \mid \phi(A_1, \ldots, A_m, n_1, \ldots, n_k)\}.$$
2. Un ensemble $A \subseteq \boldsymbol{\omega}^k$ est $\Delta_n^{0,A_1,\ldots,A_m}$ s'il est à la fois $\Sigma_n^{0,A_1,\ldots,A_m}$ et $\Pi_n^{0,A_1,\ldots,A_m}$.

On a alors les analogues suivants du lemme 1.18 et de la proposition 1.19. Les preuves sont essentiellement identiques et nous les omettons.

Lemme 1.22. *Tout ensemble $A \subseteq \boldsymbol{\omega}^k$ récursif en $A_1, \ldots, A_m$ est $\Sigma_1^{0,A_1,\ldots,A_m}$.*

Proposition 1.23. *Soit $A \subseteq \boldsymbol{\omega}$, et soient $A_1 \subseteq \boldsymbol{\omega}^{k_1}$, ..., $A_m \subseteq \boldsymbol{\omega}^{k_m}$.*

(i) A est $\Sigma_1^{0,A_1,\ldots,A_m}$ si et seulement si A est récursivement énumérable relativement à $A_1, \ldots, A_m$.

(ii) A est $\Delta_1^{0,A_1,\ldots,A_m}$ si et seulement si A est récursif relativement à A_1, ..., A_m.

2 L'analyse calculable

Le principe de l'analyse calculable est de se limiter aux réels, suites de réels, fonctions d'une variable réelle, *etc.* pour lesquels il existe une procédure algorithmique d'approximation à une précision arbitraire. Nous donnons ici les définitions fondamentales de cette théorie et montrons que l'analogue calculable du théorème de Bolzano-Weierstrass est faux, mais que l'analogue du théorème des valeurs intermédiaires est vrai. Une référence commode en la matière est [Pour-El et Richards, 1989].

2.1 Les nombres réels

Un réel est calculable s'il existe un algorithme capable d'en fournir une approximation rationnelle à toute précision souhaitée. Nous donnons d'abord une définition préliminaire.

Définition 2.1. On dit qu'une suite de rationnels $(r_n)_{n\geq 0}$ est *calculable* s'il existe des fonctions récursives $p, q : \boldsymbol{\omega} \to \boldsymbol{\omega}$ (avec $q(n) \neq 0$ pour tout n) telles que
$$r_n = \frac{p(n)}{q(n)}.$$

Définition 2.2. On dit qu'un réel ξ est *calculable* s'il existe une suite de rationnels calculable $(r_n)_{n\geq 0}$ telle que

$$\forall n \in \boldsymbol{\omega},\ |\xi - r_n| \leq \frac{1}{2^n}. \tag{2}$$

Remarque 2.3. Tout rationnel r est calculable selon cette définition : il suffit de considérer la suite constante $r_n = r$.

Remarque 2.4. Notons qu'il ne suffit pas de demander que ξ soit limite d'une suite de rationnels calculable : si l'on ne sait pas jusqu'à quel terme aller pour obtenir une approximation à 2^{-k} près, une telle suite ne nous fournit pas véritablement de procédure d'approximation. Nous construirons dans la section suivante un réel non calculable qui est limite d'une telle suite (proposition 2.10). La simple existence de réels non calculable est claire : dans la mesure où l'ensemble des fonctions récursives est dénombrable (remarque 1.3), les réels calculables sont dénombrables, donc en un sens, presque tous les réels sont non calculables.

Il existe de nombreuses autres approches équivalentes : on peut demander la calculabilité d'un développement bicimal de ξ (c'est en fait l'approche originale de [Turing, 1936]), la décidabilité d'une coupure de Dedekind appropriée, *etc.* Toutes ces définitions sont équivalentes. Nous montrons par exemple le résultat suivant.

Proposition 2.5. *Un réel ξ est calculable si et seulement s'il existe une fonction récursive f calculant le développement bicimal propre de ξ, i.e. telle que (1) $f(0) \in \boldsymbol{\omega}$, (2) $f(i) \in \{0,1\}$ pour $i > 0$, (3) $\forall k \in \boldsymbol{\omega}\ \exists k' > k$, $f(k') \neq 0$ et (4) $\xi = \sum_{i\geq 0} f(i) \cdot 2^{-i}$.*

Preuve (esquisse). Le développement bicimal propre de ξ fournit immédiatement une approximation rationnelle de type (2), en posant pour tout $n \in \boldsymbol{\omega}$

$$r_n = \sum_{i=0}^{n} \frac{f(i)}{2^i}.$$

Réciproquement, supposons ξ calculable. Il faut distinguer deux cas. Si ξ est de la forme $a \cdot 2^{-i}$ pour un entier a, son développement bicimal propre est périodique (en fait de la forme $1111\ldots$) à partir d'un certain rang, donc calculable. Sinon, notons (r_n) une suite de rationnels calculable vérifiant (2). Soit à déterminer le i^{e} terme du développement bicimal de ξ. Cela revient à trouver l'entier a tel que

$$\frac{a}{2^i} < \xi < \frac{a+1}{2^i}.$$

Cela peut être fait si l'on trouve un entier n tel que, pour tout entier b,

$$\left|\frac{b}{2^i} - r_n\right| > \frac{1}{2^n}. \tag{3}$$

(Il est facile de tester cette propriété, pour un r_n donné, en le comparant aux deux $b \cdot 2^{-i}$ les plus proches de lui.) En effet, l'intervalle d'incertitude $[r_n - 2^{-n}, r_n + 2^{-n}]$ dans lequel doit se trouver ξ ne contient alors aucun $b \cdot 2^{-i}$ et ξ a le même développement bicimal que r_n jusqu'au i^{e} terme.

Or il existe nécessairement un n satisfaisant (3). En effet, puisque ξ n'est pas un nombre bicimal, il existe n_0 tel que

$$\left|\xi - \frac{a}{2^i}\right| > \frac{1}{2^{n_0}}$$

pour tout entier a, d'où

$$\begin{aligned}\left|\frac{a}{2^i} - r_{n_0+1}\right| &= \left|\frac{a}{2^i} - \xi + \xi - r_{n_0+1}\right| \\ &\geq \left|\frac{a}{2^i} - \xi\right| - |\xi - r_{n_0+1}| \\ &> \frac{1}{2^{n_0}} - \frac{1}{2^{n_0+1}} = \frac{1}{2^{n_0+1}}\end{aligned}$$

et donc $n = n_0 + 1$ convient. Il suffit par conséquent de calculer les r_n jusqu'à en trouver un qui satisfasse (3). □

Remarque 2.6. La distinction de cas qui apparaît dans cette preuve est importante : elle correspond au fait qu'il n'y a pas de procédure algorithmique générale permettant de passer d'une approximation rationnelle comme en (2) au développement bicimal correspondant.

Une telle procédure nécessiterait de pouvoir comparer un réel calculable quelconque avec des rationnels de la forme $a \cdot 2^{-i}$. Or il n'existe pas de procédure algorithmique générale permettant de déterminer si deux réels calculables décrits par des algorithmes d'approximation sont égaux ou non (aucune approximation finie ne peut permettre de décider l'égalité). En revanche, si les réels calculables α et α' décrits par les suites calculables de rationnels $(r_k)_k$ et $(r'_k)_k$ sont différents, il existe une procédure algorithmique permettant de déterminer si $\alpha > \alpha'$ ou $\alpha < \alpha'$ (puisque $\alpha \neq \alpha'$ il existe nécessairement un entier k tel que $|r_k - r'_k| > 2^{-k}$; alors $\alpha < \alpha'$ si et seulement si $r_k < r'_k$). D'un point de vue constructif, on refuserait donc le théorème

$$\alpha < \beta \vee \alpha = \beta \vee \alpha > \beta, \tag{4}$$

mais on accepterait une affirmation plus faible comme

$$\alpha \neq \beta \Rightarrow \alpha < \beta \vee \alpha > \beta$$

(voir par exemple [Bishop et Bridges, 1985, pp. 22–24]). D'un point de vue calculable, on accepte (4), mais on démontre l'inexistence d'une procédure générale de décision de l'égalité [Pour-El et Richards, 1989, fait 3 p. 23]. C'est cette approche que reflète $\mathbf{RCA}_0$, où (4) est démontrable [Simpson, 1999, p. 75].

2.2 Les suites de nombres réels

Nous suivons le modèle de la partie précédente et définissons la notion de suite calculable de réels, qui étend la définition 2.1 d'une suite calculable de rationnels.

Définition 2.7. On dira qu'une suite $(\xi_n)_{n\geq 0}$ de réels est *calculable* s'il existe une suite double calculable de rationnels $(r_{n,k})_{n,k\geq 0}$ telle que

$$\forall n, k \in \boldsymbol{\omega},\ |\xi_n - r_{n,k}| \leq \frac{1}{2^k}. \tag{5}$$

Remarque 2.8. *A fortiori*, tous les termes ξ_n d'une suite calculable sont des réels calculables.

Remarque 2.9. Comme ci-dessus, d'autres définitions sont possibles, si l'on part par exemple d'une représentation des réels par leurs développements bicimaux ou par leur coupure. Mais dans le cas des suites, ces définitions *ne sont plus équivalentes*. Le fait qu'il n'existe pas de procédure générale pour passer d'une représentation par approximations à une représentation bicimale (cf. remarque 2.6) permet l'existence d'une suite calculable au sens de notre définition qui ne l'est pas au sens bicimal. Il en est de même de la calculabilité au sens des coupures ; voir [Mostowski, 1957] pour des contre-exemples.

Nous avons ici un nouvel exemple de la divergence entre les interprétations constructive et calculable (ou classique) d'un même fait. Puisqu'il n'existe pas d'algorithme de conversion entre représentation par approximation et représentation par développement bicimal ou coupure, on ne peut pas prouver constructivement l'équivalence de ces définitions de *nombre réel*. Mais comme on peut prouver de manière non constructive, en distinguant cas rationnel et cas irrationnel, que dès lors qu'il existe un algorithme d'approximation, il existe aussi un algorithme calculant le développement bicimal ou décidant la coupure, du point de vue classique les différentes définitions des

réels calculables sont bien équivalentes ; l'inexistence d'une procédure générale de conversion réapparaît néanmoins dès lors qu'on ne considère plus un réel isolé mais une infinité de réels à la fois : les définitions correspondantes des *suites calculables* ne sont plus équivalentes, et cela peut faire l'objet d'une démonstration.

Le système $\mathbf{RCA}_0$ reflète le point de vue calculable : la différence n'apparaît qu'au niveau des suites. C'est d'ailleurs cette différence au niveau des suites (dans le cas des coupures) qui a forcé Simpson à changer sa définition initiale de réel dans $\mathbf{RCA}_0$ (voir [Simpson, 1999, note p. 78] et [Brown et Simpson, 1986, p. 129]).

En quel sens les réels calculables pourraient-ils être complets ? Il est clair que la limite d'une suite arbitraire de réels calculables n'est pas nécessairement calculable : tout réel peut en effet s'écrire comme limite d'une suite de rationnels. Nous montrons à présent que la limite d'une *suite calculable* convergente non plus n'est pas nécessairement calculable. Cet exemple a été introduit par [Specker, 1949].

Proposition 2.10. *Soit A un ensemble récursivement énumérable non récursif (théorème 1.12), et soit $a : \boldsymbol{\omega} \to \boldsymbol{\omega}$ une fonction récursive injective telle que $A = Ima$ (remarque 1.10). La suite calculable de rationnels*

$$u_n = \sum_{k=0}^{n} \frac{1}{2^{a(k)}}$$

converge vers un réel non calculable.

Preuve. La suite u est croissante et majorée par $\sum_{k=0}^{\infty} 2^{-n} = 2$ (puisque a est injective) donc converge. Si ξ était calculable, alors son développement bicimal propre serait calculable (proposition 2.5) ; or ce développement bicimal est précisément donné par la fonction caractéristique de A (le développement en question ne peut être impropre, sinon A serait le complémentaire d'un ensemble fini donc récursif). Donc si ξ était calculable, cette fonction caractéristique serait récursive et A serait récursif, une contradiction. □

En particulier, la transposition directe du théorème de Bolzano-Weierstrass en analyse calculable est fausse : il existe des suites calculables sans valeur d'adhérence calculable.

2.3 Les fonctions

L'idée de départ est que pour qu'une fonction $\phi : \mathbf{R} \to \mathbf{R}$ soit calculable, il faut que l'on dispose d'un algorithme permettant de calculer une approxima-

tion à une précision arbitraire de $\phi(x)$ à partir de l'algorithme d'approximation de x. Pour formaliser cette idée, il faut développer la notion de *fonction récursive d'ordre supérieur* (voir [Kleene, 1952, Grzegorczyk, 1955]). Nous admettrons (cf. [Grzegorczyk, 1957]) que cette définition est équivalente à la suivante.

Définition 2.11. Soient $\alpha < \beta$ des réels calculables. On dira que $f : I = [\alpha, \beta] \to \mathbf{R}$ est calculable si :

(i) L'image par f de toute suite calculable de I est une suite calculable (en particulier, l'image de tout réel calculable est calculable) ;

(ii) f est *calculablement uniformément continue* : il existe une fonction récursive $d : \boldsymbol{\omega} \to \boldsymbol{\omega}$ telle que

$$\forall x, y \in I,\ \forall n \in \boldsymbol{\omega}, \left[|x - y| \leq \frac{1}{d(n)} \Rightarrow |f(x) - f(y)| \leq \frac{1}{2^n} \right].$$

Remarque 2.12. La propriété (i) seule est moins forte : il existe une fonction continue vérifiant (i) et pas (ii) [Pour-El et Richards, 1989, pp. 67–68]. De fait, même si les réels calculables sont dénombrables, il n'existe pas de suite *calculable* les parcourant tous (voir par exemple [Weihrauch, 2000, pp. 104–105], ou [Simpson, 1999, p. 77], sa preuve étant aisément transposable) ; on ne peut donc pas conclure de l'existence, pour chaque suite calculable particulière, d'une procédure de calcul de f valable pour tous les termes de la suite, à l'existence d'une procédure de calcul de f valable pour tous les réels calculables.

Il est aisé de vérifier que les fonctions usuelles (addition, multiplication, inverse, exponentielle, fonctions trigonométriques...) satisfont cette définition [Pour-El et Richards, 1989, p. 27]. En particulier, les réels calculables forment un sous-corps (dénombrable) de $\mathbf{R}$.

On a une version calculable du théorème des valeurs intermédiaires.

Théorème 2.13. *Soit $f : I = [0, 1] \to \boldsymbol{R}$ une fonction calculable. Supposons que $f(0) < 0$ et $f(1) > 0$. Alors il existe un réel calculable $0 < \xi < 1$ tel que $f(\xi) = 0$.*

Preuve. Il nous faut distinguer deux cas.

- S'il existe un rationnel $r \in I$ tel que $f(r) = 0$, alors $\xi = r$ est calculable et convient.
- Si pour tout rationnel $r \in I$, $f(r) \neq 0$, on construit deux suites calculables de rationnels (u_n) et (v_n) telles que $\forall n \in \boldsymbol{\omega}$, $f(u_n) < 0$, $f(v_n) > 0$ et $v_n - u_n = 2^{-n}$. Ces conditions garantissent qu'elles convergent vers un

réel ξ et que pour tout n, $|u_n - \xi| \leq 2^{-n}$, de telle sorte que ξ est calculable. De plus, par continuité de f, on a alors $f(\xi) = \lim_{n\to\infty} f(u_n) \leq 0$ et de même $f(\xi) = \lim_{n\to\infty} f(v_n) \geq 0$, donc ξ est un zéro de f.
On fixe $u_0 = 0$, $v_0 = 1$. Supposons u et v définies jusqu'au rang n, avec $v_n - u_n = 2^{-n}$. Pour $m = \frac{1}{2}(u_n + v_n)$, $f(m) \neq 0$ puisque m est rationnel ; on peut alors comparer algorithmiquement $f(m)$ à 0 (remarque 2.6). Si $f(m) < 0$, on pose $u_{n+1} = m$, $v_{n+1} = v_n$; si $f(m) > 0$, on pose $u_{n+1} = u_n$ et $v_{n+1} = m$. Dans les deux cas, $v_{n+1} - u_{n+1} = 2^{-n-1}$. Ces suites sont donc calculables et vérifient les propriétés voulues.

□

Remarque 2.14. Là encore, la preuve repose sur une distinction de cas entre rationnels et irrationnels et n'est donc pas constructive.

Remarque 2.15. La condition (ii) de la définition de fonction calculable est en fait inutile à la preuve de ce théorème. En fait, seule une version affaiblie de la propriété (i) est véritablement nécessaire, à savoir

(i)′ L'image par f de tout réel calculable de I est un réel calculable.

3 L'analyse dans $\mathbf{RCA}_0$

Dans le sous-système $\mathbf{RCA}_0$ de l'arithmétique du second ordre, l'axiome de récurrence est remplacé par le *schème de* Σ^0_1*-récurrence*, qui consiste en la clôture universelle de

$$\big(\phi(0) \wedge \forall n\,(\phi(n) \to \phi(n+1))\big) \to \forall n\,\phi(n)$$

pour chaque formule Σ^0_1 $\phi(n)$; et le schème de compréhension est remplacé par le *schème de* Δ^0_1*-compréhension*, qui consiste en la clôture universelle de

$$\forall n\,(\phi(n) \leftrightarrow \psi(n)) \to \exists X\,\forall n\,(n \in X \leftrightarrow \phi(n))$$

pour chaque formule Σ^0_1 $\phi(n)$ et chaque formule Π^0_n $\psi(n)$.

Nous commençons par étudier les $\boldsymbol{\omega}$-modèles de $\mathbf{RCA}_0$; nous montrons en particulier que $\mathbf{RCA}_0$ admet un $\boldsymbol{\omega}$-modèle REC dans lequel les seuls sous-ensembles de $\boldsymbol{\omega}$ sont les ensembles récursifs. Nous rappelons ensuite la définition des réels et suites de réels dans $\mathbf{RCA}_0$ et montrons que dans REC, les réels et suites de réels en ce sens sont exactement les réels et suites de réels calculables. Nous interprétons pour finir dans ce cadre les résultats que l'on peut prouver dans $\mathbf{RCA}_0$ ainsi que les limitations de ce sous-système de l'arithmétique.

3.1 Les $\boldsymbol{\omega}$-modèles de $\mathbf{RCA}_0$

Nous dirons ici que $\mathcal{S} \subseteq \mathcal{P}(\boldsymbol{\omega})$ *définit* un $\boldsymbol{\omega}$-modèle de $\mathbf{RCA}_0$ si

$$(\boldsymbol{\omega}, \mathcal{S}, +_{\boldsymbol{\omega}}, \cdot_{\boldsymbol{\omega}}, <_{\boldsymbol{\omega}}, 0_{\boldsymbol{\omega}}, 1_{\boldsymbol{\omega}}) \models \mathbf{RCA}_0.$$

Proposition 3.1. *Un sous-ensemble $\mathcal{S} \subseteq \mathcal{P}(\boldsymbol{\omega})$ définit un $\boldsymbol{\omega}$-modèle de $\boldsymbol{RCA}_0$ si et seulement si, pour tout $m \in \boldsymbol{\omega}$ et tous $A_1, \ldots, A_m \in \mathcal{S}$ donnés, tout ensemble récursif relativement aux A_i est dans $\mathcal{S}$.*

Preuve. Dans tout $\boldsymbol{\omega}$-modèle, les axiomes de base ainsi que le schème de Σ^0_1-récurrence sont bien sûr satisfaits. Le sous-ensemble $\mathcal{S} \subseteq \mathcal{P}(\boldsymbol{\omega})$ définit donc un $\boldsymbol{\omega}$-modèle si et seulement si le schème de Δ^0_1-compréhension est satisfait. En d'autres termes, il faut et il suffit que tout ensemble définissable à la fois par une formule Σ^0_1 et par une formule Π^0_n, pour une certaine attribution de valeurs dans $\mathcal{S}$ aux éventuelles variables libres d'ensembles de ces formules, existe dans le modèle, i.e. soit encore dans $\mathcal{S}$. Or les ensembles ainsi définissables sont par définition les ensembles qui sont $\Delta_1^{0,A_1,\ldots,A_m}$ pour certains $A_1, \ldots, A_m \in \mathcal{S}$, soit d'après la proposition 1.23, les ensembles récursifs relativement à certains $A_1, \ldots, A_m \in \mathcal{S}$. □

Remarque 3.2. Un tel $\mathcal{S} \subseteq \mathcal{P}(\boldsymbol{\omega})$ est souvent appelé *idéal de Turing* ou *degré d'insolubilité* dans la littérature.

On en déduit immédiatement :

Corollaire 3.3. *L'ensemble des sous-ensembles récursifs de $\boldsymbol{\omega}$ définit un $\boldsymbol{\omega}$-modèle REC de $\boldsymbol{RCA}_0$.*

Preuve. Si $A_1, \ldots, A_n$ sont des ensembles récursifs, alors tout ensemble récursif relativement aux A_i est encore récursif. □

Remarque 3.4. On peut adapter les méthodes que nous avons employées ici au cas du sous-système $\mathbf{ACA}_0$: on peut démontrer que l'ensemble des sous-ensembles *arithmétiques* (définition 1.15) de $\boldsymbol{\omega}$ définit un $\boldsymbol{\omega}$-modèle de $\mathbf{ACA}_0$ [Simpson, 1999, chap. VIII].

3.2 Réels, suites de réels et fonctions dans $\mathbf{RCA}_0$

Dans $\mathbf{RCA}_0$, on peut définir $\mathbf{N}$ par la formule $x = x$, où x est une variable numérique. Dans tout $\boldsymbol{\omega}$-modèle, $\mathbf{N}$ désigne alors $\boldsymbol{\omega}$. On définit ensuite les ensembles $\mathbf{Z}$ et $\mathbf{Q}$ comme des sous-ensembles de $\mathbf{N}$ en utilisant la fonction de codage

$$\langle n, m \rangle = (n + m)^2 + n$$

qui définit un isomorphisme récursif $\mathbf{N}^2 \to \mathbf{N}$; nous omettons les détails (voir [Simpson, 1999, II.2, II.4]). Il est facile de montrer que les fonctions de décodage correspondantes sont également récursives.

De même, on peut représenter un couple $(m, q) \in \mathbf{N} \times \mathbf{Q}$ par l'entier $\langle m, q \rangle$, et on peut alors représenter une suite de rationnels $(q_n)_{n \geq 0}$ par le sous-ensemble

$$\{\langle n, q_n \rangle \mid n \geq 0\} \subseteq \mathbf{N}.$$

Formellement, on donne la définition suivante.

Définition 3.5. Dans $\mathbf{RCA}_0$, une *suite de rationnels* est un sous-ensemble $X \subseteq \mathbf{N}$ vérifiant les conditions

(i) $\forall n\ [n \in X \to \exists k\, \exists l,\ n = \langle k, l \rangle]$

(ii) $\forall n\, \exists q\ (q \in \mathbf{Q} \wedge \langle n, q \rangle \in X)$

(iii) $\forall n\, \forall m_1, m_2\ [(\langle n, m_1 \rangle \in X \wedge \langle n, m_2 \rangle \in X) \to m_1 = m_2]$.

On définit alors les réels de la manière suivante.

Définition 3.6. Dans $\mathbf{RCA}_0$, un *nombre réel* est une suite de rationnels $(q_n)_n$ telle que

$$\forall k\, \forall i,\ |q_k - q_{k+i}| \leq 2^{-k}. \tag{6}$$

On dit que deux réels $(q_n)_n$ et $(q'_n)_n$ sont *égaux*, et l'on note $(q_n) =_{\mathbf{R}} (q'_n)$, dès lors que

$$\forall k,\ |q_k - q'_k| \leq 2^{-k+1}.$$

On peut alors prouver le résultat suivant. Remarquons que pour ne pas compliquer inutilement notre langage, on identifie ici REC à une partie de l'univers mathématique habituel.

Proposition 3.7. *Les réels qui existent dans le modèle REC de* $\boldsymbol{RCA}_0$ *sont précisément les réels calculables.*

Preuve. Soit (q_n) un réel dans le modèle REC de $\mathbf{RCA}_0$. Notons ξ la limite de cette suite de Cauchy dans l'ensemble $\mathbf{R}$ habituel. La condition (6) implique

$$\forall k,\ |q_k - \xi| \leq 2^{-k},$$

qui est précisément la condition (2) de la définition 2.2 ; donc ξ est calculable si et seulement si la suite de rationnels (q_n) l'est. Toute suite de rationnels (q_n) correspond, par la méthode de codage précédent, à un sous-ensemble $X_{(q_n)} \subseteq \boldsymbol{\omega}$: il nous reste à montrer que $X_{(q_n)}$ est récursif si et seulement si la suite (q_n) est calculable.

Si (q_n) est calculable, on écrit $q_n = p(n)/q(n)$ avec p et q récursives ; alors

$$X_{(q_n)} = \left\{ (n,q) \in \mathbf{N} \times \mathbf{Q} \;\middle|\; q = \frac{p(n)}{q(n)} \right\}$$

est récursif. Réciproquement, si $X_{(q_n)}$ est récursif, il existe une procédure algorithmique pour calculer les termes de (q_n) : pour n fixé, il suffit de parcourir les couples (n,q) et de leur appliquer la procédure de décision de $X_{(q_n)}$ jusqu'à rencontrer le couple $(n,q_n) \in X_{(q_n)}$. □

On peut également encoder les suites doubles de rationnels par des entiers, et donner une caractérisation explicite des sous-ensembles de $\mathbf{N}$ qui définissent ainsi une suite double, sur le modèle de la définition 3.5. On définit alors dans $\mathbf{RCA}_0$ les suites de nombres réels.

Définition 3.8. Dans $\mathbf{RCA}_0$, une suite de nombres réels est une suite double $(q_{n,k})_{n,k\geq 0}$ telle que

$$\forall n \, \forall k \, \forall i, \; |q_{n,k} - q_{n,k+i}| \leq 2^{-k} \tag{7}$$

On démontre alors comme précédemment le résultat suivant.

Proposition 3.9. *Les suites de réels qui existent dans le modèle REC de* $\boldsymbol{RCA}_0$ *sont précisément les suites calculables au sens de la définition 2.7.*

Preuve. En notant $\xi_n = \lim_{k\to\infty} q_{n,k}$ (dans l'ensemble $\mathbf{R}$ standard) la condition (7) se réécrit

$$\forall n \, \forall k, \; |q_{n,k} - \xi_n| \leq 2^{-k}$$

ce qui est la condition (5) de la définition 2.7. Il suffit donc de montrer que la suite double $(q_{n,k})$ est calculable si et seulement si le sous-ensemble de $\boldsymbol{\omega}$ correspondant est récursif, ce qui peut se faire sans difficulté particulière sur le modèle de la démonstration précédente. □

En ce qui concerne les fonctions, la situation est beaucoup plus complexe. La définition de fonction continue que donne Simpson dans $\mathbf{RCA}_0$ [Simpson, 1999, p. 85] est en fait beaucoup trop faible pour garantir la calculabilité (au sens de la définition 2.11) des « fonctions continues » (au sens de la définition de Simpson) qui existent dans REC. Il est cependant possible, pour ϕ une fonction continue au sens de Simpson, d'établir dans $\mathbf{RCA}_0$ que pour tout réel x de son domaine, $\phi(x)$ existe [Simpson, 1999, *id.*]. Par conséquent, la définition de Simpson suffit pour établir que toute fonction continue ϕ qui existe dans REC vérifie la propriété (i)′ de la remarque 2.15 : l'image par ϕ de tout réel calculable est un réel calculable.

3.3 Le système $\mathbf{RCA}_0$ et l'analyse calculable

Puisque REC $\models \mathbf{RCA}_0$, tout résultat démontrable dans $\mathbf{RCA}_0$ doit être vrai dans le modèle REC que nous venons d'étudier, c'est-à-dire doit être vrai en remplaçant « réel » par « réel calculable » et suite par « suite calculable ». On peut par exemple en déduire la proprosition suivante.

Proposition 3.10. *Le théorème de Bolzano-Weierstrass n'est pas démontrable dans* $\boldsymbol{RCA}_0$.

Preuve. Si le théorème de Bolzano-Weierstrass était démontrable dans le système $\mathbf{RCA}_0$, il serait vrai dans REC au sens où toute suite calculable admettrait une valeur d'adhérence calculable. Or nous avons vu en 2.2 qu'il existe des suites calculables convergentes dont la limite n'est pas calculable (proposition 2.10). □

Remarque 3.11. Simpson prouve en fait que l'on peut démontrer dans $\mathbf{RCA}_0$ l'équivalence entre le théorème de Bolzano-Weierstrass et l'axiome de compréhension arithmétique qui caractérise le système plus fort $\mathbf{ACA}_0$ [Simpson, 1999, chap. III.2].

Pour illustrer la tension qui peut exister entre le projet de « mathématiques à l'envers » de Simpson et l'interprétation de ses résultats dans des modèles différents du modèle standard de l'arithmétique du second ordre, nous mentionnons à présent le résultat suivant [Simpson, 1999, p. 77].

Proposition 3.12. *On peut démontrer dans* $\boldsymbol{RCA}_0$ *que pour toute suite de réels* $(\xi_n)_n$, *il existe un réel* ξ' *tel que* $\forall n,\ \xi_n \neq \xi'$.

Simpson présente ce résultat comme une preuve dans $\mathbf{RCA}_0$ de l'indénombrabilité de $\mathbf{R}$. C'est exact du point de vue des mathématiques à l'envers : ce résultat correspond, *dans le modèle standard de l'arithmétique du second ordre*, à l'indénombrabilité des réels. En revanche, dans REC, l'interprétation en est très différente : il s'agit du fait, déjà évoqué à la remarque 2.12, qu'il n'existe pas de suite *calculable* parcourant tous les réels calculables.

Quant au théorème des valeurs intermédiaires, il est démontrable dans $\mathbf{RCA}_0$. Ce résultat s'interprète dans le cadre de l'analyse calculable : on peut montrer que ce théorème est vrai de toutes les fonctions continues au sens de la définition de Simpson qui existent dans REC. En effet, comme nous l'avons vu à la fin de la section précédente, celles-ci vérifient toutes la condition affaiblie qui suffit à démontrer le théorème des valeurs intermédiaires calculable (remarque 2.15).

Références

[Bishop et Bridges, 1985] Bishop, E. et Bridges, D. (1985). *Constructive analysis*. Springer.

[Brown et Simpson, 1986] Brown, D. K. et Simpson, S. G. (1986). Which set existence axioms are needed to prove the separable Hahn-Banach theorem ? *Annals of Pure and Applied Logic*, 31:123–144.

[Grzegorczyk, 1955] Grzegorczyk, A. (1955). Computable functionals. *Fundamenta Mathematicae*, 42:168–202.

[Grzegorczyk, 1957] Grzegorczyk, A. (1957). On the definitions of computable real continuous functions. *Fundamenta Mathematicae*, 44:61–71.

[Kleene, 1952] Kleene, S. C. (1952). *Introduction to metamathematics*. North-Holland.

[Mostowski, 1957] Mostowski, A. (1957). On computable sequences. *Fundamenta Mathematic æ*, 44:37–51.

[Odifreddi, 1989] Odifreddi, P. (1989). *Classical recursion theory*. North-Holland.

[Pour-El et Richards, 1989] Pour-El, M. B. et Richards, J. I. (1989). *Computability in Analysis and Physics*. Springer-Verlag.

[Simpson, 1999] Simpson, S. G. (1999). *Subsystems of second-order arithmetic*. Springer.

[Specker, 1949] Specker, E. (1949). Nicht konstruktiv beweisbare Sätze der Analysis. *The Journal of Symbolic Logic*, 14(3).

[Turing, 1936] Turing, A. M. (1936). On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society, second series*, 42:230–265.

[Weihrauch, 2000] Weihrauch, K. (2000). *Computable analysis*. Springer-Verlag.