International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 21 No. 1 Aug. 2017, pp. 96-102

http://www.ijias.issr-journals.org/

L'arithmétique formelle et l'incomplétude

A.-Roger LULA BABOLE[1-2] and Yves MANGONGO TINDA[3]

[1]Département des Mathématiques et Informatique, Université de Kinshasa, RD Congo

[2]Faculté de Philosophie, Université Catholique du Congo, RD Congo

[3]Département des Mathématiques et Informatique, Université de Kinshasa, RD Congo

ABSTRACT: By applying the formal arithmetic model, the mathematic and logic theories have created the self-references and have chosen a specific model for accomplish the logic-mathematics proves. A formal arithmetic (ROBINSON et PEANO) constitute in this fact the basic hypothesis for the two incompleteness theorems.

KEYWORDS: formal arithmetic, incompleteness, decidability, axiomatic, coherence.

RÉSUMÉ: En appliquant le modèle de l'arithmétique formelle, les théories mathématiques et logiques ont créé les autoréférences et ont choisi un modèle spécifique pour faire assoir les preuves logico-mathématiques. L'arithmétique formelle (ROBINSON et PEANO) constitue, à cet effet, les hypothèses de base de deux théorèmes d'incomplétude.

MOTS-CLEFS: Arithmétique formelle, incomplétude, décision, axiomatique, cohérence.

INTRODUCTION

Nous indiquons les rapports existant entre l'arithmétique formelle et les deux théorèmes d'incomplétude. En effet, l'arithmétique de ROBINSON (PA^{-}) et

L'arithmétique de PEANO (PA) sert de base formelle pour la démonstration de ces théorèmes. En somme, l'arithmétique de ROBINSON, petit fragment de l'arithmétique de PEANO, permet d'établir le théorème de représentation faisant assoir le premier théorème d'incomplétude par sa moindre expressivité. Sa preuve formelle se présente par des inductions structurelles et utilise les récurrences externes. Alors que, quand la preuve est internalisée dans l'arithmétique, on a recours aux récurrences internes. Donc, on se sert de l'arithmétique PEANO. Ainsi, le second théorème d'incomplétude ne vaut que pour les théories récursives comprenant l'arithmétique de PEANO.

1 LES HYPOTHÈSES DES DEUX THÉORÈMES D'INCOMPLÉTUDE [1]

La démonstration du premier théorème d'incomplétude n'utilise en effet qu'un tout petit fragment de l'arithmétique de PEANO qui permet juste d'établir le théorème de représentation. Le fragment essentiel à l'établissement de ce théorème, est appelé arithmétique de ROBINSON (PA^{-}). Il exprime donc toutes les propriétés récursives des entiers standards.

Du point de vue formel, l'arithmétique de ROBINSON se définit par suppression de toutes les instances du schéma de récurrence, l'exception d'une instance permettant de prouver que tout entier est soit nul, soit le successeur d'un autre entier.

Dans cette perspective, l'arithmétique de ROBINSON permet de prouver que toutes les additions commutent (4+3=3+4, 71+13=13+71, etc.), mais ce n'est pas que l'addition est commutative en ($\forall x \forall y(x+y=y+x)$).

L'hypothèse selon laquelle la théorie T est récursive est fondamentale au regard de cette remarque. La raison essentielle est qu'elle permet d'appliquer le théorème de représentation à la fonction qui teste si un entier est le code d'une preuve correcte dans T.

On notera en effet par ailleurs que la démonstration du théorème d'incomplétude de la logique du premier ordre, autre fameux résultat dû à GÖDEL, indique que l'arithmétique formelle, qu'elle soit de PEANO ou de ROBINSON, a des extensions non récursives qui sont complètes.

La démonstration du premier théorème d'incomplétude utilise les récurrences externes qui sont les inductions structurelles sur les termes, les formules et les preuves aux fins de définir le codage et montrer ses propriétés logiques. Quand cette démonstration est internalisée dans l'arithmétique, on voit alors que ces récurrences se retrouvent sur le plan interne ; raison pour laquelle le second théorème d'incomplétude n'est valable que pour les théories récursives qui comprennent l'arithmétique de PEANO(PA)[1].

2 L'ARITHMÉTIQUE DE PEANO (PA)

L'arithmétique de PEANO, notée PA, est la théorie qui s'obtient en ajoutant à la théorie de l'égalité ε les six axiomes suivant :

- $(PA1)$ $\forall y(0+y=y)$
- $(PA2)$ $\forall x(s(x)+y=s(x+y))$
- $(PA3)$ $\forall y(0\times y=y)$
- $(PA4)$ $\forall x\forall y(s(x)+y=(x+y)+y)$
- $(PA5)$ $\forall x\forall y(s(x)=s(y)\Longrightarrow x=y)$
- $(PA6)$ $\forall x(s(x)\neq 0)$

Ainsi que les axiomes de récurrence

$(PA7)$ $\forall z_1 \dots z_n(A=\{x:=0\}\wedge \forall x(A\Longrightarrow A\{x:=\ s(x)\})\forall xA)$. Cet axiome est en effet la clé de voute de l'arithmétique. C'est donc le seul à faire appel à la notion de classe.

Pour chaque formule A de variables libres $x, z_1, .., z_n$

D'une manière concrète, PEANO a étendu l'axiomatique de ROBINSON à partir de la possibilité offerte par la logique du premier ordre consistant à formaliser le principe de récurrence. L'axiome 7 est remplacé par le schéma d'axiomes suivant :

Ax7' ! (p[0]$\wedge\forall$a : (p[a]$\rightarrow$p[Sa]))$\rightarrow\forall$b : p[b],

ou

Ax7'' $\forall$p : (p[0]$\wedge\forall$a (p[a]$\rightarrow$p[Sa]))$\rightarrow\forall$b :p[b],

qui aurait l'avantage de pouvoir condenser le schéma de récurrence en un axiome unique.

L'arithmétique de PEANO, PA_1 du premier ordre, sert de cadre de référence consensuel pour la théorie des nombres naturels. Quand bien même elle adopte l'axiome d'induction lui permettant de lever l'indécidabilité des énoncés élémentaires tels que : a+a=a, a=(b+c)= (a+b)+c,…, cette arithmétique est au fond syntaxiquement incomplète et indécidable.

[1] *La démonstration du premier théorème d'incomplétude n'utilise pas le schéma de récurrence interne qui est du domaine de l'arithmétique formelle, numérisée.*

Expressivité de l'arithmétique de PEANO, PA

L'arithmétique de PEANO est une théorie très expressive permettant de prouver les propriétés simples de l'addition et de la multiplication (associativité, commutative, éléments neutres, distributivité, etc.), de l'ordre (réflexivité, transitivité, antisymétrie et totale) et de l'ordre strict. Particulièrement le schéma de récurrence forte s'écrit de la manière suivante :

$$PA \longmapsto \forall x \left(\forall y\big(y < x \longrightarrow A(y)\big) \longrightarrow A(x)\right) \longrightarrow xA(x)$$

et la propriété de bon ordre

$PA \longmapsto \exists x A(x) \longrightarrow \exists x(\forall y(x) \wedge \forall y(A(x) \longrightarrow x \leq y))$ sont prouvables dans PA

Les théorèmes de PA concernent aussi bien les propriétés élémentaires, les propriétés de la divisibilité et de l'arithmétique modulaire que des propriétés de nombres premiers. On utilise à cet effet :

$Prim\ (x) \equiv x \neq 1 \wedge \forall y \forall z(x = y \times z \longrightarrow 1 \vee z = 1).$

Le travail d'adaptation au niveau de l'énoncé et de la preuve conduit à énoncer le théorème d'EUCLIDE sous sa forme originelle comme suit :

$$\forall x\ \exists y\ (y > x \wedge Prim\ (y))$$

Pour la preuve de ce théorème, on vérifie si les formules suivantes sont prouvables dans PA.

1. $\forall x\ \big(x \geq 2 \longrightarrow \exists y\ Prim\ (y) sy(x)\big)$
2. $\forall x\ \exists y(y \neq 0 \wedge \forall x'(1 \leq x' s x' \leq x \longrightarrow x')y)$
3. $\forall x \forall y(y \neq 0 \wedge \forall x'(1 \leq x' s x' \leq x \longrightarrow x')y)$

$$\longrightarrow \forall z\big(Prim\ (z) \wedge z(s(y) \longrightarrow x < z)\big)$$

Dès le début, PEANO avait formulé son arithmétique au moyen des axiomes (ou une variable) et du schéma d'induction.

L'expression :

$A[0] \wedge \forall y(A[y] \Longrightarrow A[Sy]) \longrightarrow \forall x A[x]$ est formulée par une propriété arbitraire des nombres naturels. Par ailleurs, le paradoxe de RICHARD (1905) montre le contraire c'est-à-dire il doit faire partie d'un langage formel bien défini. Cela signifie que c'est l'arithmétique de PEANO qui est le système formel PA obtenu par ajoute aux axiomes de PA, du schéma d'induction restreint aux propriétés arithmétiques, $c'est - \text{à} - dire$ aux énoncés du langage.

Le second théorème d'incomplétude est au fond une formalisation du premier théorème. La preuve informelle du premier théorème se montre par des inductions. Donc, le second théorème est établi dans l'arithmétique de PEANO (ou sa variante intuitionniste).

En effet, il est à préciser naturellement que les inductions ont lieu sur des énoncés de prouvabilité, donc expansifs $\sum_1^0$. Le second théorème exploite ainsi l'induction restreinte pour les énoncés $\sum_1^0$. Ce n'est pas optimal, quand bien même il présente une bonne idée claire et précise.

En effet, le « bon système » prend en compte les primitives fonctionnelles. La fonction exponentielle est obtenue de manière à pouvoir remplacer dans certains cas des quantifications non bornées. Alors que l'induction est limitée aux énoncés sans quantificateurs non bornés.

Enfin, on peut aussi formuler l'induction avec deux ou trois variables emboitées etc. pour les inductions généralisées, on les voit apparaitre en des inductions transfinies.

On a par exemple, deux variables jusqu'à ω^2, à trois jusqu'$a\omega^3$. Donc, *a priori* on se retrouve avec deux paramètres pour une induction. D'une part, la longueur de l'induction et, d'autre part, la complexité (alternance de quantificateurs) de l'énoncé « induit ».

La seconde preuve de GENTZEN montre que l'induction initiale est de longueur courte (ω), mais de complexité arbitraire (n'importe quel$\sum_n^0$), tandis que sa preuve de cohérence utilise une induction longue(ε_0), mais de basse complexité. Ici, elle est sans quantificateurs.

L'arithmétique de PEANO exhibe un exemple de système non finement axiomatisé et d'ailleurs non finement axiomatisable. Il est vrai qu'on doit imposer des limitations à l'utilisation de listes infinies d'axiomes. Autrement, on tombe dans le travers des logiques non monotones c'est-à-dire, plus de notion de preuve. Naturellement, on définit une famille décidable avec les axiomes.

Une fausse généralisation, dans ce cas, est une axiomatisation expansive, c'est-à-dire récursivement énumérable qui ne produit rien de plus. De manière concrète, si on remplace l'axiome An fourni à l'étape n par une variante qui lui est équivalente au moins de taille $\underline{n}$, par exemple, la conjonction ou la disjonction de $\underline{n}$ copies de $A\underline{n}$. Ce qui veut dire qu'on remplace une axiomatique $r.e.$ par une axiomatique dite récursive.

Au cas où on abandonnait les restrictions récursives sur la prouvabilité, on perdrait l'expansivité et le lien avec le calcul, alors que toute la machinerie reste intacte. On doit, pour ce faire, prendre en compte la complexité logique de la « déduction » : ne pas se priver de n cohérences… pour atteindre donc une généralisation de tout genre.

Le système d'axiomes de PEANO est un ensemble de conventions qui permettent de représenter les formules et d'établir les preuves mathématiques au sujet des nombres entiers. L'utilisation de cette axiomatique permet d'écrire et de prouver une formule signifiant que « 30 = 2x3x5 » ou que « 40 est la somme des deux carrés » (36 et 4).

Pour ce système formel les raisonnements sur les entiers se ramènent à des manipulations formelles. Cela veut dire qu'on a des manipulations de symboles qui respectent rigoureusement les règles intangibles [2].

3 L'ARITHMÉTIQUE DE ROBINSON (PA^-)

L'arithmétique de ROBINSON, notée PA^-, est la théorie du premier ordre qui s'obtient à partir de l'arithmétique de PEANO et cela par suppression de tous les axiomes de récurrence $(PA7)$ et par substitution en un unique axiome de « filtrage ».

$$(PA\overline{7}) \qquad \forall x(x = 0 \wedge \exists y(x = s(y)))$$

C'est-à-dire tout entier naturel est soit nul, soit le successeur d'un autre entier. En effet, le « ou » exclusif découle de $(PA6)$.

A l'opposé de PA, la théorie PA^-se définit à partir d'un ensemble fini d'axiomes.

Il est pertinemment à remarquer bien que l'axiome de filtrage $(PA\overline{7})$ est logiquement équivalent à l'axiome de récurrence.

$A(0) \wedge \forall x(A(s(x)) \Longrightarrow \forall x A(x))$pour la formule $A(x) \equiv x = 0 \vee \exists y(x = s(y))$. En clair, l'axiome $(PA\overline{7})$ est de manière implicite contenu dans les axiomes de récurrence $(PA7)$ de l'arithmétique de PEANO. D'où, il n'est pas inclus dans la liste d'axiomes présentée.

Il va de soi que toute formule prouvable dans PA^- est également prouvable dans PA. Ce qui laisse entendre que l'arithmétique de ROBINSON est un système de l'arithmétique de (PA).

L'arithmétique de ROBINSON PA^- formalise plus simplement l'arithmétique universelle dans le cadre d'un langage du premier ordre. Elle va poser l'existence de ''0'' et de la fonction unaire. Elle va aussi définir les opérations binaires, ''addition'' et ''multiplication''.

Il sied de reconnaître que l'axiomatique de ROBINSON sur le plan syntaxique, est incomplète puisqu'un grand nombre de propositions y sont indécidables, tel l'énoncé, a+b=b+a ; cette axiomatique ne permet ni de prouver ni de réfuter en toute généralité, alors qu'elle prouve ainsi séparément chaque instance du schéma, par exemple :

SS0+S0= S (SS0+0)=SSS0=SS (S0+0)=S (S0+S0)= S0+SS0

Ax_4 $\quad$ Ax_3 $\quad$ Ax_3 $\quad$ Ax_4Ax_4

Cela signifie donc que l'arithmétique de ROBINSON $P\bar{A}$ peut prouver la commutativité de l'addition et ce, instance après instance, mais elle est incapable de les condenser entièrement en une seule formule.

D'autres énoncés indécidables de l'arithmétique de ROBINSON $P\bar{A}$ sont :

a+a=a ou a+(b+c)=(a+b)+c,..

Evidemment, cette axiomatique est ω-*incomplétude*. Ce qui veut dire qu'il existe des chaînes de théorèmes entièrement indexés par un entier i, tel qu'on se permet de dire que la formule quantifiée, les condensant toutes, n'est pas un théorème.

L'expressivité de l'arithmétique de ROBINSON est beaucoup moins expressive que l'arithmétique de PEANO puisqu'on ne peut pas y prouver que l'addition est associative ou commutative :

$$PA^{-} \vdash (x+y)+z = x+(y+z), \quad PA^{-} \vdash x+y = y+x$$

Le premier théorème d'incomplétude est d'ordinaire formulé pour des systèmes fondés sur un langage simpliste dû à PEANO. Il opère avec quatre symboles fonctionnels, à savoir :

La constante 0, le successeur S (unaire) et les symboles binaires $+, \times$. Ainsi va – t – on coder l'entier 5 par le terme $\overline{5} := sssss0$. En général, on note n par n, n symboles s suivi d'un zéro. Retenons que la régression accompagnant le progrès, c'est-à-dire le formalisme, nous amène à la numération pré-babylonienne. Deux symboles binaires de prédicats sont considérés $=, <$. Les axiomes du système PA^{-} se subdivisent en trois groupes, à savoir :

Egalité : ces axiomes expriment que l'égalité est une congruence :

$$x = x\,; x = y \rightarrow y \rightarrow x; x = y \wedge y = z \rightarrow x = z\,;$$

$$x = y \wedge z = t \wedge x < z \rightarrow y < t; x = y \rightarrow Sx = Sy\,;$$

$$x = y \wedge z = t \rightarrow x + z = y + t; x = y \wedge z \rightarrow t \rightarrow x \times z = y \times t\,;$$

Ces axiomes suffisent pour prouver $x = y \wedge A[x] \longrightarrow [y]$.

Définitions : Quant à leurs définitions, ces axiomes aident à prouver les équations et inéquations de base. Le groupe $x + 0 = x; x + Sy = S(x+y): x \times 0 = 0; x \times Sy = (x \times y) + x$, pour tout terme clos t dont la valeur est n, l'égalité $t = \overline{n}$. Evidemment, toutes égalités $t = \mu$ entre termes clos sont vraies. Le groupe $Sx \neq 0; Sx = Sy \rightarrow x = y$ (troisième et quatrième axiomes de PEANO) prouve toutes les inéquations $t \neq \mu$ entre termes clos. Elles sont donc vraies. Retenons que ces deux axiomes laissent penser à un domaine infini (sans eux on s'attendrait à avoir $\overline{10} = \overline{0}$).

Finalement, le groupe $\neg(x < 0); x < Sy \Leftrightarrow x < y \vee x = y$ prouve toutes les inégalités ou non inégalités $t < \mu, \neg(t < \mu)$ entre termes clos. Elles sont donc vraies. Ainsi il prouve l'équivalence $x < n \Leftrightarrow x = \overline{0} \vee x = \overline{1} \vee \ldots \vee x = \overline{n-1}$. Il permet aussi de passer à l'étape cruciale des quantificateurs bornés.

Notons qu'un dernier axiome laisse penser que l'axiome $x < y \vee x = y \vee y < x$ est intrinsèquement différent des autres. Il n'est donc pas nécessaire à l'incomplétude. En effet, la représentation des propriétés expansives est assurée par les axiomes de définition. Il sert à la représentation des fonctions récursives. Cela signifie qu'il sert à l'indécidabilité algorithmique de PA et de toutes ses extensions cohérentes. Il est utilisé également dans la variante de ROSSER.

L'incomplétude utilise d'habitude la logique classique. Elle peut aussi utiliser la logique intuitionniste, voir aussi la logique linéaire[2].

En termes clairs, tout système cohérent qui contient ces quelques axiomes sera incomplet et, donc indécidable. L'indécidabilité signifie ici que le système ne décide pas toutes les propriétés, mais surtout on n'est pas en mesure au niveau d'algorithme de savoir si un énoncé est prouvable ou non. Par contre, la décidabilité dit plus que cela, par exemple, on peut :

(i) Remplacer le troisième axiome de PEANO par, disons $\overline{10} = \overline{0}$. Dans ce cas, on est dans le fini (les entiers *modulo* 10) et le système est dit décidable ; au cas contraire, on reste dans l'indécidable.

(ii) Se priver du symbole propre au produit (arithmétique de PRESBURGER[3], décidable). Il est clair que cette privation est comprise, par la multiplication, dans la représentation des suites finies. Ces systèmes sont donc décidables.

---

[2] *La logique linéaire est une invention du logicien français Jean-Yves GIRARD.*

[3] ***L'arithmétique de PRESBURGER,***

L'arithmétique de PRESBURGER est une restriction de L'arithmétique de PEANO où est éliminée la multiplication. Elle opère avec l'addition et éventuellement l'ordre. Elle a la même syntaxe et sémantique que celle de PEANO, mais pas de multiplications. Précisons ici que la multiplication par une constante est permise. Dans ce cas la multiplication est une suite finie d'additions.

Illustrons cela par un exemple

$\forall x \exists y . y \geq 2 * x$

Pour LASCAR, il est possible de construire dans le langage de l'arithmétique un énoncé, noté Dem(n) qui dépend du paramètre n et qui veut dire que l'entier naturel n est le code répondant à une formule à prouver à partir des axiomes de PEANO. L'arithmétique est ici reflétée à l'intérieur d'elle-même. Il résulte dans le cas de l'incomplétude de prendre une formule, notamment fausse du genre, 1 = 2. Si son code est, par exemple, 337500 et φ , la négation de Dem (3307500). En termes clairs, la formule signifie que 1 = 2 n'est pas prouvable à partir des axiomes de PEANO .De toute évidence, il y a lieu de constater que ces axiomes ne sont pas contradictoires. Or, disons-le, GÖDEL a su parfaitement montrer que la formule φ en elle-même n'était pas prouvable, à partir des axiomes de PEANO. D'où, il faut affirmer que ce qui est vrai n'est pas nécessairement démontable [3].

4 Conclusion

En arithmétique formelle, il y a des énoncés vrais qu'on ne peut pas démontrer à partir des axiomes de ce système axiomatique. Donc, pour contourner les tribulations de l'incohérence logique, l'incomplétude est justement le prix à payer. L'arithmétique formelle sert de fondement logique pour prouver le théorème d'incomplétude. Par ses récurrences externes, l'arithmétique de ROBINSON permet d'établir le théorème de représentation qui sert à la preuve du premier théorème d'incomplétude et le second théorème n'est valable que pour, les théories récursives qui comprennent l'arithmétique de PEANO.

Notons en effet que l'arithmétique de PRESBURGER est beaucoup moins expressive mais décidable et complète pour le sous-ensemble qui correspond aux axiomes de PEANO. Elle est construite sur une complexité triple exponentielle déterministe $2^{2^{2^{cn}}}$*, mais elle est simple sans quantificateurs.*

L'arithmétique de PRESBURGER comporte les axiomes suivants :

1. $\neg(O=x+1)$
2. $x+1=y+1 \rightarrow x=y$
3. $x+O=x$
4. $(x+y)+1=x+(y+1)$
5. *Supposons que P(x) soit une formule logique du premier ordre opérant dans le langage de l'arithmétique de PRESBURGER, n'ayant pas d'autres symboles de fonction que le successeur et l'addition et possédant la variable libre x (et avec l'éventualité d'autres variables libres). Disons alors que la formule suivante est un axiome :*
   $(P(0) \wedge \forall x\ (P(x) \rightarrow P(x+1))) \rightarrow P(y)$.

REFERENCES

[1] Alexandre Miquel, *Les théorèmes d’incomplétude de GÖDEL*, 2013.
[Online] Available : http://perso.enslyon.fr/natacha.portier/enseign/logique/GoedelParAlex.pdf, (Août 2013).

[2] Jean-Paul Delahave, « L’incomplétude, le hasard et la physique », *Pour la science*, n°355, pp.90-94,2007.

[3] D. Lascar, « Formalisation de l’arithmétique », *Encyclopédie Philosophique Universelle. Les Notions Philosophiques*. T1, Paris : PUF, pp.1022-1024, 1990.