

Informatique, vérité, théorème de Gödel

Edmond BIANCO¹

Résumé. – Si, comme pourraient le prétendre les médias, nous pénétrons dans l'ère de l'intelligence artificielle, il est bon, loin de vouloir briser les élans d'imagination, d'observer quelque peu les limites du domaine dans lequel on patauge. Il est prudent de voir clairement ce qu'on ne peut pas faire. A l'imagination l'initiative de trouver ce qu'on peut faire. En évitant l'écueil qui consiste à ramener la pensée informatique à une liste ouverte de recettes, il devient plus que nécessaire de montrer que l'informatique a sa méthodologie propre, et de mettre en évidence tout ce qui est commun dans les théories de Turing, Post, Von Neumann, Gödel et autres. Or, si abstraite que soit la démonstration de Gödel, elle utilise simplement une technique de base de l'informatique. Cela, les contemporains de Gödel ne pouvaient le voir.

1. Informatique, vérité, théorème de Gödel

En écrivant ces mots, je n'ai nulle prétention à redécouvrir le Théorème de Gödel, je préfère renvoyer à l'excellent ouvrage de J.- Y. Girard [GNNG89] cité en référence. Mon souci est autre. J'ai eu la chance de voir naître ce phénomène qu'on a nommé sur le tard "Informatique", qui a, je pense avec juste raison, englobé de nombreux phénomènes qui se sont petit à petit distingués les uns des autres tout en conservant, cependant, comme point commun, l'objet qu'on a rebaptisé toujours sur le tard : ordinateur. Mais par un étrange métaphénomène c'est l'une de ces branches du savoir, certes économiquement la plus visible, la programmation, qui masque pratiquement toutes les autres. Un peu comme si l'on prétendait que la "comptabilité" c'est les mathématiques.

Dans le théorème de Gödel, plusieurs domaines importants de la réflexion peuvent être dégagés, ou même engagés. Il me semble qu'il en est un autre pour lequel il est intéressant d'insister.

Quand on a commencé à se poser des questions sur la signification des choses et des moyens d'expression, c'est devenu un jeu amusant que de construire des paradoxes. Le paradoxe du menteur en est un exemple célèbre : Epiménide le Crétois dit de lui-même qu'il est un menteur. Le mot "menteur" possède de toute évidence plusieurs sens distincts dont un autre exemple apparaît dans le problème du voyageur. Les pérégrinations de ce dernier l'amènent à une fourche, et là il ne sait plus où aller. Heureusement se trouvent au carrefour un couple d'individus capables de le renseigner, mais l'un d'eux, on ne sait pas lequel, est un menteur, quelle est alors la question à poser. La solution brutale, implique que le menteur, fieffé menteur, dit systématiquement des contre-vérités. Peut-on alors continuer à le qualifier de menteur, à partir du moment où il est démasqué, un simple décodage le rend autant vecteur de vérité que son comparse. Le véritable mensonge est plus subtil, il consiste en fait, à utiliser essentiellement la vérité, et n'en travestir que juste ce qu'il faut pour atteindre un but hypothétique, tout en restant vraisemblable.

1. Note de la rédaction : article paru dans le numéro 30 du bulletin de décembre 1991.

L'antinomie de Russel met en évidence une sorte de manœuvre linguistique un peu voisine. Je définis un ensemble normal comme ne se contenant pas lui-même. Il est facile de trouver des exemples : l'ensemble de tous les clous n'est pas un clou. Cela implique immédiatement que je me mette à imaginer des ensembles, alors non normaux, qui se contiennent eux-mêmes. Cette notion est moins évidente, il devient nécessaire d'illustrer la propriété. Et force est bien de chercher une définition assez vague pour que ça marche. Exemple. L'ensemble des choses pensables, est une chose pensable. Donc l'ensemble des choses pensables est un élément de lui-même. Devant le vague de ce que représente une chose pensable, on ressent le besoin de trouver une idée plus précise. L'ensemble des objets rouges est un objet rouge. L'ensemble des masses de sable est une masse de sable. On perçoit qu'on frôle à chaque instant le jeu de mots. "Masse" passe beaucoup mieux que "objet", tout simplement parce que le mot objet sous-entend presque nettement une unicité dans la constitution. Il est alors réjouissant de se préoccuper de savoir, si l'ensemble de tous les ensembles normaux est lui aussi normal. S'il l'est, il tombe sous le sens qu'étant normal, nouvelle définition vague, il est aussi un élément de l'ensemble. Mais ceci est précisément la définition d'un ensemble non normal. Donc s'il est normal alors, conclusion, il est non normal.

Le paradoxe marche d'autant mieux que le mot pivot possède un sens très large, il est visiblement d'ordre sémantique, des termes comme volume, surface font très bien l'affaire.

En toute généralité, un raisonnement sera d'autant plus rigoureux qu'il portera sur des notions plus précisément définies, et surtout très soigneusement délimitées. C'est précisément, à la limite, le cas des mathématiques, dont l'efficacité consiste à vider les mots de toute substance afin de n'en conserver que le squelette. Le théorème de Gödel intervient alors pour montrer l'importance du hiatus qui existe entre ce dont on parle, et ce qui permet d'en parler. Le langage et le méta-langage.

Le même hiatus existe dans la société, mais dans un domaine d'application légèrement différent. Prenons le cas de l'enseignement des mathématiques. Nombre d'élèves ont du mal à se faire à l'idée d'utiliser des mots vides de sens, pour eux le mot conserve toujours un peu de sa richesse, et l'application du raisonnement mathématique devient alors difficile voire impossible. L'enseignant, oubliant un peu les difficultés qu'il a vécues dans son passé, oublie en même temps d'insister lourdement sur l'importance du côté conventionnel. De telle sorte que bien trop souvent des élèves doués d'une intelligence fine se trouvent rejetés par l'aridité de la manipulation de concepts vides. Tout le monde ne peut être passionné par l'emballage, juste pour l'intérêt de l'emballage. Et cela explique également qu'on puisse revenir sur le tard aux mathématiques, quand on a pu surmonter l'écœurement d'un enseignement exsangue. Prenons un exemple. Les mots "vrai" et "faux". Ils sont définis sans ambiguïté en logique. Quelque chose qui est vrai est définitivement vrai. Point. Quand j'apprends les mathématiques, je me rends compte qu'il y a deux univers, l'univers mathématique, où tout est rigoureusement "vrai", bref un univers pur, cristallin. Et surtout ceux qui peuvent y accéder sont considérés comme les plus intelligents. Et puis l'autre univers où rien ne peut jamais être aussi systématique, toutes les vérités sont non seulement fluctuantes, mais encore jamais nettement

établies. Telles théories politiques semblent permettre de résoudre de graves conflits et on s'aperçoit à l'usage qu'elles ont tendance à les aggraver. L'élève qui, pour diverses raisons commence dans la vie avec une étiquette de cancre, se trouve dans la situation difficile suivante : s'il admet ce fait, c'est visiblement définitif, puisque toute vérité est éternelle, alors pourquoi essayer de sortir du puits ? S'il ne l'admet pas, il va se heurter à une sorte de barrière de potentiel, à son premier petit succès il va recevoir des quolibets indirects du style : comment avez-vous pu rater cet exercice alors que même lui a pu le comprendre. La vérité essentielle demeure : crétin je suis, crétin je reste. Devenir fort en math implique de rendre fausse une vérité définitive, ce qui revient à remettre en question la mathématique elle-même. Essayons alors d'imaginer la frustration du cancre qui perçoit nettement qu'il ne pourra jamais participer à l'élaboration des bombes à billes, à la dispersion de la dioxine ou à la conception d'un surrégénérateur.

Le raisonnement formel implique deux idées de base, d'abord que les vérités établies se conservent pour tous les systèmes d'objets qui sont munis des propriétés exigées au départ. Ensuite, il faut être sûr que le raisonnement, dans le domaine choisi, n'aboutira jamais à une contradiction. Par exemple que sur tel type de figure on réussisse à montrer que deux droites à la fois se coupent et ne se coupent pas.

Il y a ainsi de nombreux chapitres des mathématiques pour lesquels l'expérience des mathématiciens, et la qualité des résultats obtenus permettent seuls, jusqu'à présent, d'en affirmer la cohérence.

Mais à partir de là, l'idée a germé selon laquelle le processus du raisonnement mathématique est un processus mécanique, en foi de quoi il devient judicieux d'en concevoir le mécanisme. Première étape l'axiomatisation. On se donne un ensemble fini de propriétés de base, et un jeu de règles de déduction. De quelle nature est alors le mécanisme ? Eh bien il suffit de se donner les moyens de représenter les axiomes et de se donner les moyens d'en déduire tous les théorèmes possibles et imaginables, par application mécanique des règles de déduction, elles-mêmes dûment représentées pour qu'une machine puisse faire tout le travail.

Comment se présente alors le problème ? Nous nous donnons de la sorte des signes et des jeux de signes auxquels nous attribuons une signification arbitraire, mais telle qu'on puisse montrer que toutes les "bonnes constructions", ainsi définies par notre système mécanique comportent un sens cohérent. Hélas Gödel a montré que cette "méta-assertion" est fausse. Tant pis pour la mécanique, tant mieux pour l'esprit humain.

Le principe de la démonstration passe par la définition d'un "codage" dont on est certain qu'il permet de représenter de manière bien distincte des objets formellement distincts. Ensuite on se place par exemple dans le cadre de l'arithmétique de Péano, et on montre qu'on peut construire une formule, parfaitement concevable, mais dont il est visible qu'elle déclare d'elle-même qu'elle est fausse.

On se donne le moyen mécanique de construire et de reconnaître toutes les formules rigoureusement vraies du système. Ce sont des considérations méta-linguistiques qui permettent alors de les interpréter. Il doit être parfaitement clair que seules les vérités telles qu'elles apparaissent dans le méta-langage sont importantes puisque c'est comme

ça que le système est utile. Il doit être un support écrit non ambigu dans lequel il suffit de lire une formule construite, déclarée vraie, pour lire une vérité utilisable.

Ainsi se plaçant dans un système connu et cohérent on prouve qu'on peut, en respectant les règles de ce système, construire au moins une formule reconnue vraie, qui, si on l'en croit en l'interprétant, signifie qu'elle-même est fausse.

Cela ne prouve qu'une seule chose, c'est que dès lors qu'on a construit un système formel, donc constructible mécaniquement, on sépare l'univers de la réflexion en deux parties : celle qui est contenue dans le système et qui est capable de distinguer ce qui est intérieurement vrai de ce qui ne l'est pas, et celle qui permet d'observer le système de l'extérieur et d'en déduire certaines propriétés que le mécanisme ne peut pas mettre en évidence, ce sont les méta-propriétés. Ce que montre Gödel, c'est que, vouloir inclure les méta-propriétés dans le système lui-même, le rend inconsistant. Il suffit de montrer qu'il est possible, en respectant les règles du système, d'y inclure une propriété contradictoire.

Rappelons les axiomes de Péano :

- 1) Zéro est un nombre.
- 2) Le successeur immédiat d'un nombre est un nombre.
- 3) Zéro n'est pas le successeur immédiat d'un nombre.
- 4) Il n'existe pas deux nombres distincts qui possèdent le même successeur.
- 5) Toute propriété qui appartient à Zéro et à tout successeur d'un nombre qui a cette propriété, appartient à tous les nombres.

On va choisir un ensemble suffisant de signes et de variables et un codage biunivoque : d'abord dix signes :

0 s = $\exists \cup \supset \neg ()$, ceci n'est pas limitatif mais doit suffire, puis des variables à substitution numérique :

x y z ...

des variables à substitution propositionnelle :

p q r ...

des variables prédicatives :

P Q R ...

Toutes ces variables en quantité suffisante et dénombrable. On code les dix signes avec les entiers 1, 2, 3, ... 10.

0 s = $\exists \cup \supset \neg ()$,
1 2 3 4 5 6 7 8 9 10

pour les variables numériques on choisit les nombres premiers plus grands que 10 :

x y z ...
11 13 17 19 ...

pour les variables de proposition, les carrés de ces nombres premiers :

p q r ...
11² 13² 17² 19² ...

pour les variables prédicatives, les cubes de ces mêmes nombres :

P Q R ...
11³ 13³ 17³ 19³ ...

On peut de la sorte coder toutes les formules dont on a besoin, par exemple :

$$(\exists x)(x = s 0)$$

qui se lit : il existe un x tel que ce x soit le successeur immédiat de zéro, formule tirée des axiomes 1 et 2 de Péano. Je peux également construire la formule :

$$(\exists x)(x = s y)$$

qui est l'expression de l'axiome 2. On peut coder ces formules puisque chacun de leurs signes porte un code :

$$\begin{array}{cccccccc} (& \exists & x &) & (& x & = & s & 0 &) \\ 8 & 4 & 11 & 9 & 8 & 11 & 3 & 2 & 1 & 9 \end{array}$$

On cherche alors à coder une telle formule de manière unique et telle que toute autre formule qui en différerait si peu que ce soit porte un code distinct. On peut procéder ainsi : ces entiers servent d'exposant aux premiers successifs et on fait le produit de l'ensemble :

$$2^8 \times 3^4 \times 5^{11} \times 7^9 \times 11^8 \times 13^{11} \times 17^3 \times 19^2 \times 23^1 \times 29^9 = n1$$

Il est parfaitement clair que si je transforme si peu que ce soit ma formule, son code devient très différent. Imaginons qu'on permute = et s. Alors dans le nombre précédent le facteur :

$$17^3 \times 19^2$$

devient :

$$17^2 \times 19^3$$

Si on se réfère au théorème de l'arithmétique qui dit que tout nombre entier se décompose en une suite unique de facteurs premiers, on constate que l'on obtient pour ces deux formules deux codes distincts. Réciproquement partant d'un tel code, la décomposition en facteurs premiers permet de retrouver facilement la formule. Tout nombre qui est l'image d'une formule du système est désigné par "nombre de Gödel" de la formule. Je dirai indistinctement "code de" ou "nombre de Gödel de". De la même manière, la deuxième formule portera le nombre de Gödel :

$$\begin{array}{l} (\exists x)(x = s y) \\ 2^8 \times 3^4 \times 5^{11} \times 7^9 \times 11^8 \times 13^{11} \times 17^3 \times 19^2 \times \mathbf{23^{13}} \times 29^9 = n2 \end{array}$$

Ce code diffère du précédent par le facteur marqué en gras. Désignons par n1 et n2 ces deux codes. On peut être amenés à se donner un code pour la suite des deux formules, ou, plus généralement, pour toute suite quelconque de formules. Cela permettrait d'obtenir également un nombre de Gödel unique pour chacune des suites possibles, qu'on appelle plutôt des démonstrations. Ainsi si je considère que la suite des deux règles précédentes constitue une démonstration, j'en construis le code de la manière unique, en prenant le nombre de Gödel de chaque formule et en le portant en exposant de la suite des nombres premiers à partir de 2. De sorte que la démonstration :

$$(\exists x)(x = s y)$$

$$(\exists x)(x = s 0)$$

va porter le nombre de Gödel :

$$2^{n1} \times 3^{n2} = k$$

visiblement, le raisonnement déjà appliqué marche encore, avec ce procédé deux démonstrations différentes porteront obligatoirement des codes différents. C'est ce qu'on peut constater en intervertissant simplement l'ordre des deux formules.

2. Démonstration de Gödel

On se donne alors deux moyens pour la démonstration. D'abord je constate que je peux coder les deux formules suivantes :

$$F1(x) (\text{dém}(k, n1))$$

$$F2(x) (\neg \text{dém}(k, n1))$$

qui se lisent, la première : « pour tout x, la suite de formules de code k est une démonstration de la formule de code n1. »

La seconde : « pour tout x, la suite de formules de code k n'est pas une démonstration de la formule de code n1. »

J'ai là deux énoncés méta-linguistique que je peux parfaitement coder dans le système mécanique, ce sont des formules qui peuvent être construites automatiquement pour tout n1 possible et pour tout k correspondant.

Il est à ce moment-là évident que si je prends au hasard une suite quelconque de formules valables cette suite ne sera généralement pas la démonstration de la dernière formule, et dans ce cas F2 est une formule "vraie".

Je me donne alors un autre moyen de calculer. Si j'observe la formule :

$$(\exists x)(x = s y)$$

je constate que ce qu'elle exprime, c'est qu'il existe toujours un entier successeur immédiat d'un entier quelconque, donc je peux en déduire autant de formules parfaitement vraies dans notre système, au moyen du remplacement de y par n'importe quel entier. Ainsi si je veux dire que 4 est successeur de 3², j'ai la formule vraie :

$$(\exists x)(x = sss 0)$$

avec les notations choisies 3 s'écrit évidemment sss 0. Mais tout autre moyen de faire apparaître un entier quelconque conserve à la formule sa valeur de vérité. En particulier si je remplace le code de y par le code de l'entier code de n2. Auquel cas je donne un nom à cette opération qui consiste à remplacer le code de y par le code du nombre de Gödel de la formule. La nouvelle formule porte à ce moment là un autre nombre de Gödel qu'on peut facilement calculer.

$$2^8 \times 3^4 \times 5^{11} \times 7^9 \times 11^8 \times 13^{11} \times 17^3 \times 19^2 \times \mathbf{23^{13}} \times 29^9 = n2$$

C'est le terme $\mathbf{23^{13}}$ qu'il faut remplacer par une suite :

$$23^2 \times 29^2 \times \dots \times p^2$$

si p est le n1ème premier à partir de 23. La nouvelle formule portera donc un code qu'on désignera par N2. Cette opération qui n'est en fait qu'une simple substitution, sera désignée par la notation :

$$\text{subst}(n2, \mathbf{23^{13}}, n2)$$

qui se lit : « Substitution dans la formule de nombre de Gödel n2, du code de l'entier n2 au terme $\mathbf{23^{13}}$. »

Cette opération donne une formule de code N2. Je reprends alors la formule :

$$F2(k) (\neg \text{dém}(k, n2))$$

Cette formule est en fait une démonstration dans laquelle je remplace la dernière formule de code n2, par la même formule sur laquelle j'ai appliqué la substitution. Cela donne :

2. Note de la rédaction : correction introduite en gras souligné

$$F2'(k) (\neg \text{dém}(k, \text{subst}(k, 23^{13}, k)))$$

La formule F2 porte par définition le code k, j'applique la substitution sur la formule complète F2, et cela aura pour effet de remplacer l'élément 23^{13} par le code, obtenu comme on l'a vu, de l'entier k. L'application de ce calcul donne comme code un nombre de Gödel facile à calculer qu'on désignera par K.

On se demande alors quel est le code ou nombre de Gödel de F2'. La nature de l'opération

$$\text{subst}(k, 23^{13}, k)$$

montre de toute évidence que K est le nombre de Gödel de F2'.

3. Raisonnement

Par construction on a vu qu'à chaque formule correspond un seul nombre de Gödel, de plus chaque fois qu'on rencontre un nombre de Gödel, on peut reconstituer la formule dont il est le code. Il est alors clair que si je sais qu'une déduction provenant d'une suite de formules vraies amène à une formule également vraie, si un code qui correspond à la déduction entraîne un code qui correspond à la conclusion, on peut méta-déduire que ce code exprime une vérité dans le système.

Or, si j'interprète la formule F2' voici ce qu'elle dit :

Hypothèse : « Quel que soit k la formule F2' n'est pas une démonstration de la dernière formule. »

Conclusion : « Or, cette dernière formule porte comme nombre de Gödel précisément le nombre de Gödel de F2'. Qui affirme donc qu'elle n'est pas une démonstration d'elle-même, et ceci quel que soit k. Il n'existe donc pas de démonstration de F2'.

Et c'est F2' qui le dit. »

4. Quelques réflexions

Pour construire un mécanisme, quel qu'il puisse être, il faut avoir à l'avance un ensemble d'idées. Pour fixer ces idées il devient nécessaire de trouver un moyen graphique de les exprimer. D'où l'invention du symbole. Mais le symbole n'est pas la pensée, car cela voudrait dire que les peuples qui n'ont pas d'écriture ne pensent pas. Mais il existe toutefois de bonnes raisons d'être inquiet quand on voit ce que pensent les peuples qui en ont une.

Quels que soient les signes employés, ou leurs combinaisons, ce n'est que par ce qu'on leur accole de signification arbitraire, qu'ils peuvent être intéressants. Le symbole en lui-même n'a aucun pouvoir, aucune valeur. Il n'en est pas de même de son pouvoir évocateur, qui implique l'existence d'une imagination observante. Quand on se livre à la construction d'un système formel, que fait-on en réalité ? On essaye désespérément de supprimer toutes les ambiguïtés que l'on considère comme gênantes. Il paraît ainsi naturel de se priver d'une source riche, sinon importante d'expression.

Le système tronqué de la sorte ne devra vraisemblablement plus pouvoir exprimer un certain nombre de vérités utiles mais d'un niveau qui dépasse les possibilités laissées au système. Or, c'est bien le phénomène que cette démonstration met en évidence. Les lois de construction des images de vérités permettent de construire des images que le système

est parfaitement incapable d'interpréter. La force de la pensée de Gödel réside dans le fait qu'il a créé un raisonnement de type informatique. D'abord il fabrique un code dont la propriété essentielle est la biunivocité. L'algorithme de construction de son code, basé sur un méta-théorème de l'arithmétique, fonctionne dans les deux sens. Partant du code il peut refabriquer la formule.

On ne fait rien d'autre quand on utilise un "langage machine" qui présente toujours deux formes, l'une plus commode pour le programmeur, comporte un maximum d'objets symboliques tels que des identificateurs. Mais c'est un code finalement de forme binaire, pour l'autre, donc enregistrable en mémoire et qui sera soumis à la machine universelle.

Une démonstration n'est en fait, qu'une construction de formules et une vérification qu'une formule obtenue est une bonne formule. Informatiquement on peut imaginer une sorte de machine universelle qui, à la donnée des axiomes de Péano dûment codés, et à la lecture d'un jeu adéquat de règles de déduction également codées construirait toutes les formules possibles.

C'est ainsi que partant des deux objets :

$$(\exists x)(x = s \ 0)$$

$$(\exists x)(x = s \ y)$$

par une construction combinatoire, il est clair que la machine en question tombera obligatoirement sur une formule du type F2'. Ce qu'il faut entendre par là c'est qu'elle va construire tous les nombres de Gödel possibles jusqu'à un certain ordre et on peut montrer facilement qu'il finira par tomber sur le code d'une version de F2'. Mais ce que l'automate ne possède pas c'est le moyen de relever ce que cette formule a de remarquable. Pour lui, c'est une formule vraie, donc un théorème. Il n'a aucun moyen d'en saisir le méta-sens. C'est le contre-exemple qui montre qu'il existe dans le système, des formules qu'il considère comme "vraies" mais dont l'interprétation "normale" n'a aucune signification. Il ne s'agit là, en fait que d'une "méta-propriété" supplémentaire, et pas tellement évidente.

Note de la rédaction : [GNNG89] est la seule référence explicitement citée par Edmond Bianco. Les autres références, qui se rapportent au sujet ont été insérées, font partie de sa bibliothèque : [Pea89], [Göd31],[Göd62], [CN04], [Wan90], [And15], [Del02], [Hof85], [Göd56], [You05], [Göd65].

RÉFÉRENCES

- [And15] D. Andler. *Kurt Gödel, 1906-1978*. Encyclopaedia Universalis [en ligne], 2015.
- [CN04] P. Cassou-Noguès. *Gödel*. Paris, Les Belles Lettres, 2004.
- [Del02] J.-P. Delahaye. *L'intelligence et le calcul, de Gödel aux ordinateurs quantiques*. Belin. Pour la Science, 2002.
- [GNNG89] K. Gödel, E. Nagel, J. Newman, and J.-Y. Girard. *Le Théorème de Gödel*. Seuil, 1989.
- [Göd31] K. Gödel. Über formal unentscheidbare Sätze der principia mathematica und verwandter Systeme I. *Monatshefte für Mathematik und Physik*, 38 :173–198, 1931.
- [Göd56] K. Gödel. *Gödel's Lost Letter and P=NP : a personal view of the theory of computation*. Richard J. Lipton, 1956.
- [Göd62] K. Gödel. *On Formally Undecidable Propositions*. New York, Basic Books, 1962.

- [Göd65] Kurt Gödel. On undecidable propositions of formal mathematical systems, (1934) lecture notes taken by Kleene and Rosser at the Institute for Advanced Study : reprinted in M. Davis (ed.), 1965.
- [Hof85] D. Hofstadter. *Gödel Escher Bach. Les brins d'une guirlande éternelle*. Interéditions, 1985.
- [Pea89] G. Peano. *Arithmetices principia, nova methodo exposita*. Turin, Bocca, 1889.
- [Wan90] H. Wang. *Gödel*. Armand Colin, 1990.
- [You05] P. Yourgrau. *Einstein/Gödel. Quand deux génies refont le monde*. Dunod, 2005.