Quatre preuves du premier théorème d'incomplétude de Gödel, dont une utilisant la complexité de Kolmogorov (sans auto-réf.), et la dernière meilleure que les autres

1. Système formel et théorèmes de Gödel
2. Complexité de Kolmogorov
3. Preuves du premier théorème d'incomplétude

Kévin Perrot

Séminaire d'été CANA – 11.07.2023

1. Système formel

Question : qu'est-ce qu'un théorème ?
Réponse :

1. Système formel

Question : qu'est-ce qu'un théorème ?
Réponse : un énoncé qui admet une démonstration.

1. Système formel

Question : qu'est-ce qu'un théorème ?
Réponse : un énoncé qui admet une démonstration.

Question : qu'est-ce qu'une démonstration ?
Réponse :

1. Système formel

Question : qu'est-ce qu'un théorème ?
Réponse : un énoncé qui admet une démonstration.

Question : qu'est-ce qu'une démonstration ?
Réponse : un *raisonnement logique* dans un système formel.

1. Système formel

Question : qu'est-ce qu'un théorème ?
Réponse : un énoncé qui admet une démonstration.

Question : qu'est-ce qu'une démonstration ?
Réponse : un *raisonnement logique* dans un système formel.

Système formel = formules + axiomes + règles de déduction.

1. Système formel

Question : qu'est-ce qu'un théorème ?
Réponse : un énoncé qui admet une démonstration.

Question : qu'est-ce qu'une démonstration ?
Réponse : un *raisonnement logique* dans un système formel.

Système formel = formules + axiomes + règles de déduction.

Example : **Calcul des séquents** :

Formules propositionnelles $(\vee, \wedge, \neg, \Rightarrow)$ avec variables booléennes.

ou Formules du premier ordre $(\forall, \exists, \vee, \wedge, \neg, \Rightarrow)$ avec variables booléennes.

https://fr.wikipedia.org/wiki/Calcul_des_séquents

1. Système formel

Question : qu'est-ce qu'un théorème ?
Réponse : un énoncé qui admet une démonstration.

Question : qu'est-ce qu'une démonstration ?
Réponse : un *raisonnement logique* dans un système formel.

Système formel = formules + axiomes + règles de déduction.

Example : **Calcul des séquents** :

Formules propositionnelles $(\vee, \wedge, \neg, \Rightarrow)$ avec variables booléennes.
ou
Formules du premier ordre $(\forall, \exists, \vee, \wedge, \neg, \Rightarrow)$ avec variables booléennes.

https://fr.wikipedia.org/wiki/Calcul_des_séquents

- **Démonstration = arbre/séquence** de formules.
- **Démonstration vérifiable algorithmiquement**.
- **Ensemble des preuves/théorèmes récursivement énumérable**.

1. Système formel (opt.)

Exemple : **Arithmétique de Presburger** $FO(\mathbb{N}, +)$:
Formules du premier ordre $(\forall, \exists, \vee, \wedge, \neg, \Rightarrow)$ sur la signature $\{=, 0, s, +\}$ avec variables entières (dans $\mathbb{N}$).

1. $\forall x : \neg(0 = sx)$.
2. $\forall x, y : sx = sy \Rightarrow x = y$.
3. $\forall x : x + 0 = x$.
4. $\forall x, y : s(x + y) = x + sy$.
5. $(P(0) \wedge \forall x : [P(x) \Rightarrow P(sx)]) \Rightarrow (\forall x : P(x))$ pour toute formule P.

Question : que veulent dire $\exists y : x = y + y$ et $\exists z : x + z = y$?

Question : satisfiabilité de $sx + ssy = 4$?

Question : validité de $(sx + ssy = 3) \Rightarrow (x = 0 \wedge y = 0)$?

1. Système formel (opt.)

Exemple : **Arithmétique de Peano** $FO(\mathbb{N}, +, \cdot)$:
Formules du premier ordre $(\forall, \exists, \vee, \wedge, \neg, \Rightarrow)$ sur la signature $\{=, 0, s, +, \cdot\}$ avec variables entières (dans $\mathbb{N}$).

1. $\forall x : \neg(0 = sx)$.
2. $\forall x : (x = 0 \vee \exists y : x = sy)$.
3. $\forall x, y : sx = sy \Rightarrow x = y$.
4. $\forall x : x + 0 = x$.
5. $\forall x, y : s(x + y) = x + sy$.
6. $\forall x : x \cdot 0 = 0$.
7. $\forall x, y : (x \cdot sy = x \cdot y) + x)$.
8. $\forall \vec{X} : (P(0, \vec{X}) \wedge \forall x : [P(x, \vec{X}) \Rightarrow P(sx, \vec{X})]) \Rightarrow (\forall x : P(x, \vec{X}))$
   pour toute formule P.

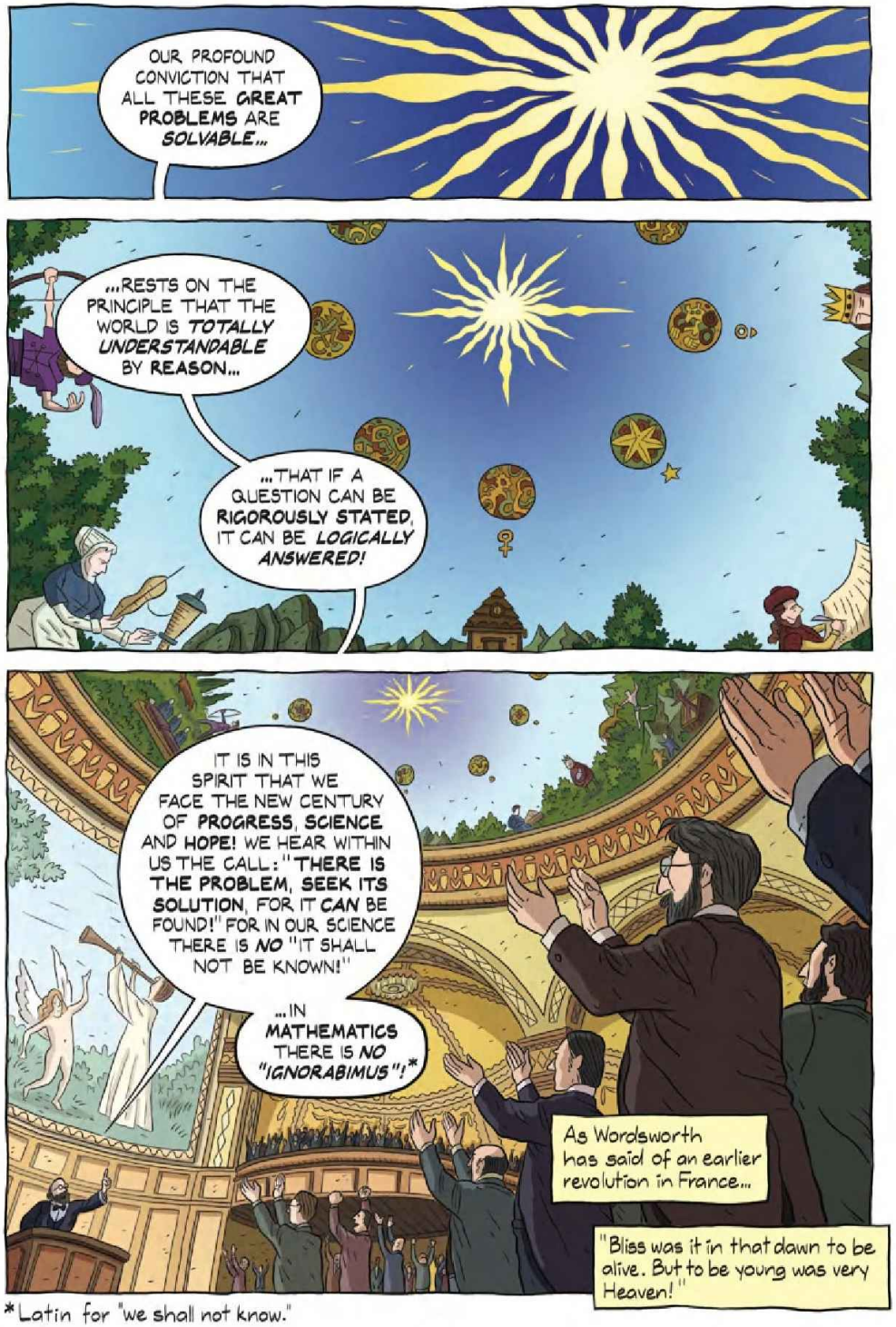
On a *seulement* ajouté la multiplication...

1. Système formel

Le système formel qui correspond à « toutes les mathématiques » est la **théorie des ensembles de Zermelo-Fraenkel (ZF)**.

https://en.wikipedia.org/wiki/Zermelo-Fraenkel_set_theory

...et l'**axiome du choix (ZFC)** ?



Vrai $\stackrel{?}{=}$ Prouvable

Procédure mécanique ?

1. Théorèmes d'incomplétude de Gödel

Défintions. Soit F un système formel.

F **Cohérent** $=$ on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** $=$ pour toute φ on peut démontrer φ ou $\neg\varphi$.

1. Théorèmes d'incomplétude de Gödel

Défintions. Soit F un système formel.

F **Cohérent** $=$ on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** $=$ pour toute φ on peut démontrer φ ou $\neg\varphi$.

- Incohérent $\Rightarrow$ 
- Incomplet $\Rightarrow$ 
- Complet $\Rightarrow$ procédure mécanique, car théorèmes r.e.

1. Théorèmes d'incomplétude de Gödel

Défintions. Soit F un système formel.

F **Cohérent** = on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** = pour toute φ on peut démontrer φ ou $\neg\varphi$.

- Incohérent ⇒ 
- Incomplet ⇒ 
- Complet ⇒ procédure mécanique, car théorèmes r.e.

Théorème d'incomplétude de Gödel (1^{er}).
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

1. Théorèmes d'incomplétude de Gödel

Défintions. Soit F un système formel.

F **Cohérent** = on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** = pour toute φ on peut démontrer φ ou $\neg\varphi$.

- Incohérent ⇒ 
- Incomplet ⇒ 
- Complet ⇒ procédure mécanique, car théorèmes r.e.

Théorème d'incomplétude de Gödel (1^{er}).
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Théorème d'incomplétude de Gödel (2^{nd}).
Tout système formel contenant l'arithmétique de Peano ne peut **pas démontrer sa propre cohérence** (sauf s'il est incohérent).

1. Théorèmes d'incomplétude de Gödel

Défintions. Soit F un système formel.

F **Cohérent** $=$ on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** $=$ pour toute φ on peut démontrer φ ou $\neg\varphi$.

- Incohérent $\Rightarrow$ 
- Incomplet $\Rightarrow$ 
- Complet $\Rightarrow$ procédure mécanique, car théorèmes r.e.

Théorème d'incomplétude de Gödel (1^{er}).
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Théorème d'incomplétude de Gödel (2^{nd}).
Tout système formel contenant l'arithmétique de Peano ne peut **pas démontrer sa propre cohérence** (sauf s'il est incohérent).

- Impossible à patcher... ZFC est incomplet 🤞🤞🤞.

https://fr.wikipedia.org/wiki/Liste_d'énoncés_indécidables_dans_ZFC

1. Théorèmes d'incomplétude de Gödel

F **Cohérent** = on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** = pour toute φ on peut démontrer φ ou $\neg\varphi$.

Théorème d'incomplétude de Gödel (1^{er}) .
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Preuve 1.

1. Théorèmes d'incomplétude de Gödel

F **Cohérent** = on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** = pour toute φ on peut démontrer φ ou $\neg\varphi$.

Théorème d'incomplétude de Gödel (1^{er}) .
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Preuve 1. Arithmétisation des métamathématiques g : formules $\to \mathbb{N}$.

$$g(\ll(\exists x)(x = sy)\gg) = 2^8 \cdot 3^4 \cdot 5^{11} \cdot 7^9 \cdot 11^8 \cdot 13^{11} \cdot 17^5 \cdot 19^7 \cdot 23^{13} \cdot 29^9$$

1. Théorèmes d'incomplétude de Gödel

F **Cohérent** = on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** = pour toute φ on peut démontrer φ ou $\neg\varphi$.

Théorème d'incomplétude de Gödel (1^{er}) .
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Preuve 1. Arithmétisation des métamathématiques g : formules $\to \mathbb{N}$.

$$g(\text{«}(\exists x)(x = sy)\text{»}) = 2^8 \cdot 3^4 \cdot 5^{11} \cdot 7^9 \cdot 11^8 \cdot 13^{11} \cdot 17^5 \cdot 19^7 \cdot 23^{13} \cdot 29^9$$

«$(\forall x)(\neg \mathtt{demo}(x, z))$» ≡ il n'existe pas de démonstration de $g^{-1}(z)$.

«$\mathtt{sub}(y, 13, y)$» ≡ g de $g^{-1}(y)$ où «y» est remplacé par $g^{-1}(y)$.

1. Théorèmes d'incomplétude de Gödel

F **Cohérent** = on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** = pour toute φ on peut démontrer φ ou $\neg\varphi$.

Théorème d'incomplétude de Gödel (1^{er}) .
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Preuve 1. Arithmétisation des métamathématiques $g : \text{formules} \to \mathbb{N}$.

$$g(\text{«}(\exists x)(x = sy)\text{»}) = 2^8 \cdot 3^4 \cdot 5^{11} \cdot 7^9 \cdot 11^8 \cdot 13^{11} \cdot 17^5 \cdot 19^7 \cdot 23^{13} \cdot 29^9$$

«$(\forall x)(\neg \mathtt{demo}(x,z))$» ≡ il n'existe pas de démonstration de $g^{-1}(z)$.
«$\mathtt{sub}(y,13,y)$» ≡ g de $g^{-1}(y)$ où «y» est remplacé par $g^{-1}(y)$.

$$g(\text{«}(\forall x)(\neg \mathtt{demo}(x, \mathtt{sub}(y,13,y)))\text{»}) = n$$
$$G = \text{«}(\forall x)(\neg \mathtt{demo}(x, \mathtt{sub}(n,13,n)))\text{»}$$
$$g(G) = \mathtt{sub}(n,13,n)$$

1. Théorèmes d'incomplétude de Gödel

F **Cohérent** = on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** = pour toute φ on peut démontrer φ ou $\neg\varphi$.

Théorème d'incomplétude de Gödel (1^{er}) .
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Preuve 1. Arithmétisation des métamathématiques $g : \text{formules} \to \mathbb{N}$.

$$g(\text{«}(\exists x)(x = sy)\text{»}) = 2^8 \cdot 3^4 \cdot 5^{11} \cdot 7^9 \cdot 11^8 \cdot 13^{11} \cdot 17^5 \cdot 19^7 \cdot 23^{13} \cdot 29^9$$

«$(\forall x)(\neg \mathtt{demo}(x,z))$» ≡ il n'existe pas de démonstration de $g^{-1}(z)$.
«$\mathtt{sub}(y,13,y)$» ≡ g de $g^{-1}(y)$ où «y» est remplacé par $g^{-1}(y)$.

$$g(\text{«}(\forall x)(\neg \mathtt{demo}(x, \mathtt{sub}(y,13,y)))\text{»}) = n$$
$$G = \text{«}(\forall x)(\neg \mathtt{demo}(x, \mathtt{sub}(n,13,n)))\text{»}$$
$$g(G) = \mathtt{sub}(n,13,n)$$

$G \equiv$ il n'existe pas de démonstration de G.

1. Théorèmes d'incomplétude de Gödel

F **Cohérent** = on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** = pour toute φ on peut démontrer φ ou $\neg\varphi$.

Théorème d'incomplétude de Gödel (1^{er}) .
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Preuve 1. Arithmétisation des métamathématiques g : formules $\to \mathbb{N}$.

$$g(\text{«}(\exists x)(x = sy)\text{»}) = 2^8 \cdot 3^4 \cdot 5^{11} \cdot 7^9 \cdot 11^8 \cdot 13^{11} \cdot 17^5 \cdot 19^7 \cdot 23^{13} \cdot 29^9$$

«$(\forall x)(\neg \mathtt{demo}(x,z))$» ≡ il n'existe pas de démonstration de $g^{-1}(z)$.

«$\mathtt{sub}(y,13,y)$» ≡ g de $g^{-1}(y)$ où «y» est remplacé par $g^{-1}(y)$.

$$g(\text{«}(\forall x)(\neg \mathtt{demo}(x, \mathtt{sub}(y,13,y)))\text{»}) = n$$
$$G = \text{«}(\forall x)(\neg \mathtt{demo}(x, \mathtt{sub}(n,13,n)))\text{»}$$
$$g(G) = \mathtt{sub}(n,13,n)$$

$G \equiv$ il n'existe pas de démonstration de G.

Si F complet alors...

1. Théorèmes d'incomplétude de Gödel

F **Cohérent** = on ne peut jamais démontrer φ et $\neg\varphi$.

F **Complet** = pour toute φ on peut démontrer φ ou $\neg\varphi$.

F **Correct** = φ démontrable implique φ *vraie*.

- Correct $\Rightarrow$ cohérent. ⚠ démontrer un énoncé faux $\not\Rightarrow$ incohérent

Théorème d'incomplétude de Gödel (1^{er}) faible.
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **correct et complet**.

Preuve 1. Arithmétisation des métamathématiques g : formules $\to \mathbb{N}$.

$$g(\text{«}(\exists x)(x = sy)\text{»}) = 2^8 \cdot 3^4 \cdot 5^{11} \cdot 7^9 \cdot 11^8 \cdot 13^{11} \cdot 17^5 \cdot 19^7 \cdot 23^{13} \cdot 29^9$$

«$(\forall x)(\neg \mathtt{demo}(x,z))$» $\equiv$ il n'existe pas de démonstration de $g^{-1}(z)$.
«$\mathtt{sub}(y,13,y)$» $\equiv$ g de $g^{-1}(y)$ où «y» est remplacé par $g^{-1}(y)$.

$$g(\text{«}(\forall x)(\neg \mathtt{demo}(x, \mathtt{sub}(y,13,y)))\text{»}) = n$$
$$G = \text{«}(\forall x)(\neg \mathtt{demo}(x, \mathtt{sub}(n,13,n)))\text{»}$$
$$g(G) = \mathtt{sub}(n,13,n)$$

$G \equiv$ il n'existe pas de démonstration de G.

Si F complet alors... incorrect. Gödel ω-cohérence

2. Complexité de Kolmogorov

- 0101010101010101010101010101010101010101010101010101010101010101
- 0010110011101100111010110001011000101101111001100010101011010101

Questions : quelle est la plus aléatoire ? quelle est la plus probable ?

2. Complexité de Kolmogorov

- 0101010101010101010101010101010101010101010101010101010101010101
- 0010110011101100111010110001011000101101111001100010101011010101

Questions : quelle est la plus aléatoire ? quelle est la plus probable ?

Idée : la plus petite description algorithmique.

Définition. La complexité de Kolmogorov-Chaitin de $x \in \{0,1\}^*$ est la taille du plus court programme $\downarrow$ donnant x en sortie, notée $K(x)$.

⚠ self-delimiting (prefix-free)

2. Complexité de Kolmogorov

- 0101010101010101010101010101010101010101010101010101010101010101
- 0010110011101100111010110001011000101101111001100010101011010101

Questions : quelle est la plus aléatoire ? quelle est la plus probable ?

Idée : la plus petite description algorithmique.

Définition. La complexité de Kolmogorov-Chaitin de $x \in \{0,1\}^*$ est la taille du plus court programme $\downarrow$ donnant x en sortie, notée $K(x)$.

⚠ self-delimiting (prefix-free)

- $\exists c : \forall x : K(x) \leq |x| + c$.
- Indépendante du langage de programmation L choisi : $\forall L, L' : \exists c : \forall x : K_L(x) \leq K_{L'}(x) + c$.
- $K : \{0,1\}^* \to \mathbb{N}$ n'est pas calculable, mais sur-approximable.
- Mots incompressibles : $\forall n \in \mathbb{N} : \exists x \in \{0,1\}^n : K(x) \geq |x| = n$. Aucun sous-ensemble infini n'est semi-décidable.

2. Complexité de Kolmogorov (opt.)

Application à la densité des nombres premiers.

2. Complexité de Kolmogorov (opt.)

Application à la densité des nombres premiers.

Idée : la décomposition en facteurs premiers représente succinctement les entiers (mots binaires), mais des incompressibles existent.

2. Complexité de Kolmogorov (opt.)

Application à la densité des nombres premiers.

Idée : la décomposition en facteurs premiers représente succinctement les entiers (mots binaires), mais des incompressibles existent.

Définition. Soit $\pi(n)$ le nombre d'entiers premiers $\leq n$. $\pi(11) = 5$

Théorème [Hadamard et de la Vallée Poussin 1896]. $\pi(n) \sim \frac{n}{\ln n}$

Théorème. $\pi(n) \geq \frac{\log n}{\log \log n} - o(1)$.

2. Complexité de Kolmogorov (opt.)

Application à la densité des nombres premiers.

Idée : la décomposition en facteurs premiers représente succinctement les entiers (mots binaires), mais des incompressibles existent.

Définition. Soit $\pi(n)$ le nombre d'entiers premiers $\leq n$. $\pi(11) = 5$

Théorème [Hadamard et de la Vallée Poussin 1896]. $\pi(n) \sim \frac{n}{\ln n}$

Théorème. $\pi(n) \geq \frac{\log n}{\log \log n} - o(1)$.

Preuve. $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_m^{e_m}$ avec $e_i \leq \log n$ donc $\log \log n$ bits chacun.

2. Complexité de Kolmogorov (opt.)

Application à la densité des nombres premiers.

Idée : la décomposition en facteurs premiers représente succinctement les entiers (mots binaires), mais des incompressibles existent.

Définition. Soit $\pi(n)$ le nombre d'entiers premiers $\leq n$. $\pi(11) = 5$

Théorème [Hadamard et de la Vallée Poussin 1896]. $\pi(n) \sim \frac{n}{\ln n}$

Théorème. $\pi(n) \geq \frac{\log n}{\log \log n} - o(1)$.

Preuve. $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_m^{e_m}$ avec $e_i \leq \log n$ donc $\log \log n$ bits chacun.

On peut écrire un programme avec $(e_1, e_2, \ldots, e_m)$ codé en dur, qui calcule les m premiers entiers premiers $p_1, p_2, \ldots, p_m$, puis calcule n.

2. Complexité de Kolmogorov (opt.)

Application à la densité des nombres premiers.

Idée : la décomposition en facteurs premiers représente succinctement les entiers (mots binaires), mais des incompressibles existent.

Définition. Soit $\pi(n)$ le nombre d'entiers premiers $\leq n$. $\pi(11) = 5$

Théorème [Hadamard et de la Vallée Poussin 1896]. $\pi(n) \sim \frac{n}{\ln n}$

Théorème. $\pi(n) \geq \frac{\log n}{\log\log n} - o(1)$.

Preuve. $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_m^{e_m}$ avec $e_i \leq \log n$ donc $\log\log n$ bits chacun.

On peut écrire un programme avec $(e_1, e_2, \ldots, e_m)$ codé en dur, qui calcule les m premiers entiers premiers $p_1, p_2, \ldots, p_m$, puis calcule n.

Donc $c + m \cdot \log\log n \geq K(n)$, or pour n incompressible $K(n) \geq \log n$ d'où

2. Complexité de Kolmogorov (opt.)

Application à la densité des nombres premiers.

Idée : la décomposition en facteurs premiers représente succinctement les entiers (mots binaires), mais des incompressibles existent.

Définition. Soit $\pi(n)$ le nombre d'entiers premiers $\leq n$. $\quad \pi(11) = 5$

Théorème [Hadamard et de la Vallée Poussin 1896]. $\pi(n) \sim \frac{n}{\ln n}$

Théorème. $\pi(n) \geq \frac{\log n}{\log\log n} - o(1)$.

Preuve. $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_m^{e_m}$ avec $e_i \leq \log n$ donc $\log\log n$ bits chacun.

On peut écrire un programme avec $(e_1, e_2, \ldots, e_m)$ codé en dur, qui calcule les m premiers entiers premiers $p_1, p_2, \ldots, p_m$, puis calcule n.

Donc $c + m \cdot \log\log n \geq K(n)$, or pour n incompressible $K(n) \geq \log n$
d'où $c + m \cdot \log\log n \geq \log n \quad \Rightarrow \quad \pi(n) \geq m \geq \frac{\log n}{\log\log n} - \frac{c}{\log\log n}$ $\square$

3. Preuves 1er théorème

Théorème d'incomplétude de Gödel (1er) faible.
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **correct et complet**.

Gödel's Theorem and Information, Gregory J. Chaitin.
International Journal of Theoretical Physics 21(12), 1982. doi-link

- Requiert l'arithmétique pour parler des programmes.

3. Preuves 1er théorème

Théorème d'incomplétude de Gödel (1er) faible.
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **correct et complet**.

Gödel's Theorem and Information, Gregory J. Chaitin.
International Journal of Theoretical Physics 21(12), 1982. doi-link

- Requiert l'arithmétique pour parler des programmes.

Preuve 2. Correct et complet $\Rightarrow$ Arrêt décidable $\lightning$. □

3. Preuves 1er théorème

Théorème d'incomplétude de Gödel (1er) faible.
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **correct et complet**.

Gödel's Theorem and Information, Gregory J. Chaitin.
International Journal of Theoretical Physics 21(12), 1982. doi-link

- Requiert l'arithmétique pour parler des programmes.

Preuve 2. Correct et complet ⇒ Arrêt décidable ↯. □

Preuve 3.
Paradoxe de Berry. « Le plus petit entier positif qui n'est pas définissable en moins de seize mots ».

3. Preuves 1er théorème

Théorème d'incomplétude de Gödel (1er) faible.
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **correct et complet**.

Gödel's Theorem and Information, Gregory J. Chaitin.
International Journal of Theoretical Physics 21(12), 1982. doi-link

- Requiert l'arithmétique pour parler des programmes.

Preuve 2. Correct et complet $\Rightarrow$ Arrêt décidable $\lightning$. $\square$

Preuve 3.
Paradoxe de Berry. « Le plus petit entier positif qui n'est pas définissable en moins de seize mots ».

Lemme. Si F est cohérent alors, pour tout $\alpha \in \mathbb{N}$ suffisamment grand et tout $x \in \{0,1\}^*$, l'énoncé « $K(x) > \alpha$ » n'est pas démontrable.

3. Preuves 1er théorème

Théorème d'incomplétude de Gödel (1er) faible.
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **correct et complet**.

Gödel's Theorem and Information, Gregory J. Chaitin.
International Journal of Theoretical Physics 21(12), 1982. doi-link

- Requiert l'arithmétique pour parler des programmes.

Preuve 2. Correct et complet $\Rightarrow$ Arrêt décidable $\lightning$. $\square$

Preuve 3.
Paradoxe de Berry. « Le plus petit entier positif qui n'est pas définissable en moins de seize mots ».

Lemme. Si F est cohérent alors, pour tout $\alpha \in \mathbb{N}$ suffisamment grand et tout $x \in \{0,1\}^*$, l'énoncé « $K(x) > \alpha$ » n'est pas démontrable.

Fin. Pourtant il est parfois vrai.

3. Preuves 1er théorème

Théorème d'incomplétude de Gödel (1er) faible.
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **correct et complet**.

Gödel's Theorem and Information, Gregory J. Chaitin.
International Journal of Theoretical Physics 21(12), 1982. doi-link

- Requiert l'arithmétique pour parler des programmes.

Preuve 2. Correct et complet $\Rightarrow$ Arrêt décidable $\lightning$. $\square$

Preuve 3.
Paradoxe de Berry. « Le plus petit entier positif qui n'est pas définissable en moins de seize mots ».

Lemme. Si F est cohérent alors, pour tout $\alpha \in \mathbb{N}$ suffisamment grand et tout $x \in \{0,1\}^*$, l'énoncé « $K(x) > \alpha$ » n'est pas démontrable.

Fin. Pourtant il est parfois vrai. Si F complet alors incorrect. $\square$

3. Preuves 1er théorème (diapo la plus intéressante de l'exposé)

Lemme. Si F est cohérent alors, pour tout $\alpha \in \mathbb{N}$ suffisamment grand et tout $x \in \{0,1\}^*$, l'énoncé « $K(x) > \alpha$ » n'est pas démontrable.

3. Preuves 1er théorème (diapo la plus intéressante de l'exposé)

Lemme. Si F est cohérent alors, pour tout $\alpha \in \mathbb{N}$ suffisamment grand et tout $x \in \{0,1\}^*$, l'énoncé « $K(x) > \alpha$ » n'est pas démontrable.

Fixons α arbitrairement, et supposons qu'il existe une preuve de « $K(x) > \alpha$ ». Soit w la plus courte de ces preuves, pour $z \in \{0,1\}^*$.

3. Preuves 1er théorème (diapo la plus intéressante de l'exposé)

Lemme. Si F est cohérent alors, pour tout $\alpha \in \mathbb{N}$ suffisamment grand et tout $x \in \{0,1\}^*$, l'énoncé « $K(x) > \alpha$ » n'est pas démontrable.

Fixons α arbitrairement, et supposons qu'il existe une preuve de « $K(x) > \alpha$ ». Soit w la plus courte de ces preuves, pour $z \in \{0,1\}^*$.

Alors l'algo suivant donne z en sortie: énumérer toutes les preuves de F jusqu'à rencontrer une preuve de « $K(x) > \alpha$ », et donner ce x en sortie.

3. Preuves 1er théorème (diapo la plus intéressante de l'exposé)

Lemme. Si F est cohérent alors, pour tout $\alpha \in \mathbb{N}$ suffisamment grand et tout $x \in \{0,1\}^*$, l'énoncé « $K(x) > \alpha$ » n'est pas démontrable.

Fixons α arbitrairement, et supposons qu'il existe une preuve de « $K(x) > \alpha$ ». Soit w la plus courte de ces preuves, pour $z \in \{0,1\}^*$.

Alors l'algo suivant donne z en sortie: énumérer toutes les preuves de F jusqu'à rencontrer une preuve de « $K(x) > \alpha$ », et donner ce x en sortie.

La longueur de ce programme est $c + \log \alpha$, donc on a :
1. « $K(z) > \alpha$ » est démontrable.
2. « $K(z) \leq c + \log \alpha$ » est vrai... ⚠ et donc démontrable.

Quand $\alpha \geq c + \log \alpha$, on conclut que F est incohérent. □

3. Preuves 1er théorème (diapo la plus intéressante de l'exposé)

Lemme. Si F est cohérent alors, pour tout $\alpha \in \mathbb{N}$ suffisamment grand et tout $x \in \{0,1\}^*$, l'énoncé « $K(x) > \alpha$ » n'est pas démontrable.

Fixons α arbitrairement, et supposons qu'il existe une preuve de « $K(x) > \alpha$ ». Soit w la plus courte de ces preuves, pour $z \in \{0,1\}^*$.

Alors l'algo suivant donne z en sortie: énumérer toutes les preuves de F jusqu'à rencontrer une preuve de « $K(x) > \alpha$ », et donner ce x en sortie.

La longueur de ce programme est $c + \log \alpha$, donc on a :
1. « $K(z) > \alpha$ » est démontrable.
2. « $K(z) \leq c + \log \alpha$ » est vrai... ⚠ et donc démontrable.

Quand $\alpha \geq c + \log \alpha$, on conclut que F est incohérent. □

Chaitin: «If a theorem contains more information than a given set of axoims, then it is impossible for the theorem to be derived from the axioms.»

3. Preuves 1er théorème

Théorème d'incomplétude de Gödel (1er).
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Preuve 4. *Rosser's Theorem via Turing machines*, Scott Aaronson. Blog, 2011.

3. Preuves 1er théorème

Théorème d'incomplétude de Gödel (1er).
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Preuve 4. *Rosser's Theorem via Turing machines*, Scott Aaronson. Blog, 2011.

$$g(\text{«}(\forall x)[\texttt{demo}(x, \texttt{sub}(y, 13, y)) \Rightarrow (\exists z < x)(\texttt{demo}(z, \neg\texttt{sub}(y, 13, y)))]\text{»}) = n$$

$$R = \text{«}(\forall x)[\texttt{demo}(x, \texttt{sub}(n, 13, n)) \Rightarrow (\exists z < x)(\texttt{demo}(z, \neg\texttt{sub}(n, 13, n)))]\text{»}$$

$$g(R) = \texttt{sub}(n, 13, n)$$

$R \equiv$ pour toute démonstration de R, il existe une réfutation plus courte.

3. Preuves 1^{er} théorème

Théorème d'incomplétude de Gödel (1^{er}).
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Preuve 4. *Rosser's Theorem via Turing machines*, Scott Aaronson. Blog, 2011.

$$g(\ll(\forall x)[\mathtt{demo}(x,\mathtt{sub}(y,13,y)) \Rightarrow (\exists z < x)(\mathtt{demo}(z,\neg\mathtt{sub}(y,13,y)))]\gg) = n$$

$$R = \ll(\forall x)[\mathtt{demo}(x,\mathtt{sub}(n,13,n)) \Rightarrow (\exists z < x)(\mathtt{demo}(z,\neg\mathtt{sub}(n,13,n)))]\gg$$

$$g(R) = \mathtt{sub}(n,13,n)$$

$R \equiv$ pour toute démonstration de R, il existe une réfutation plus courte.

Si F complet alors...

3. Preuves 1^{er} théorème

Théorème d'incomplétude de Gödel (1^{er}).
Tout système formel contenant l'arithématique de Peano ne peut **pas** être à la fois **cohérent et complet**.

Preuve 4. *Rosser's Theorem via Turing machines*, Scott Aaronson. Blog, 2011.

$$g(\ll(\forall x)[\mathtt{demo}(x,\mathtt{sub}(y,13,y)) \Rightarrow (\exists z < x)(\mathtt{demo}(z,\neg\mathtt{sub}(y,13,y)))]\gg) = n$$

$$R = \ll(\forall x)[\mathtt{demo}(x,\mathtt{sub}(n,13,n)) \Rightarrow (\exists z < x)(\mathtt{demo}(z,\neg\mathtt{sub}(n,13,n)))]\gg$$

$$g(R) = \mathtt{sub}(n,13,n)$$

$R \equiv$ pour toute démonstration de R, il existe une réfutation plus courte.

Si F complet alors... incohérent. 😎 □

3. Preuve 2nd théorème

Théorème d'incomplétude de Gödel (2nd).
Tout système formel contenant l'arithmétique de Peano ne peut **pas démontrer sa propre cohérence** (sauf s'il est incohérent).

The Surprise Examination Paradox and the Second Incompleteness Theorem, Shira Kritchman and Ran Raz. Notices of the AMS 57(11), 2010. arXiv:1011.4974

Paradoxe de l'interrogation surprise.
L'enseignant annonce à la classe : « la semaine prochaine vous aurez une interrogation, mais il vous sera impossible de savoir quel jour l'interrogation aura lieu, jusqu'au jour où elle aura lieu ».

3. Preuve 2nd théorème

Théorème d'incomplétude de Gödel ($2^{\mathbf{nd}}$).
Tout système formel contenant l'arithmétique de Peano ne peut **pas démontrer sa propre cohérence** (sauf s'il est incohérent).

The Surprise Examination Paradox and the Second Incompleteness Theorem, Shira Kritchman and Ran Raz. Notices of the AMS 57(11), 2010. arXiv:1011.4974

Paradoxe de l'interrogation surprise.
L'enseignant annonce à la classe : « la semaine prochaine vous aurez une interrogation, mais il vous sera impossible de savoir quel jour l'interrogation aura lieu, jusqu'au jour où elle aura lieu ».

Une prochaine fois 😰
Merci pour votre attention !