Automates, Langages et Logique

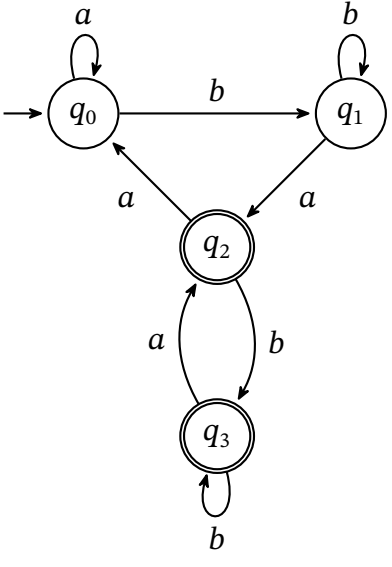
6. Logique, arithmétique et langages

L2, Université d'Orléans — S1 2024/2025

Nicolas Ollinger

Plan du cours

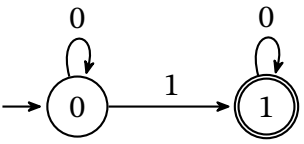
1. Alphabets – Mots – Langages
2. Automates finis déterministes
3. Automates finis non déterministes
4. Théorème de Kleene
5. Minimisation
6. **Logique, arithmétique et langages**

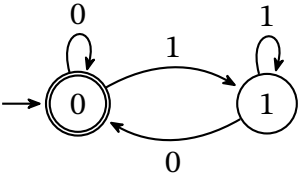


Des nombres et des mots

Si on **représente les nombres** par leur écriture **binaire**, on peut **coder** des ensembles d'entiers sous forme de langages.

Certains de ces langages sont **reconnaissables** !

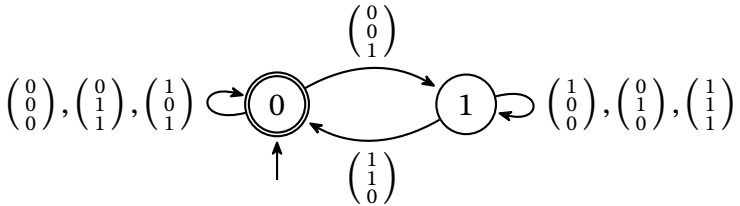




Question Quels ensembles intéressants peut-on **reconnaître** ainsi ?

Des mots et des tuples

En utilisant l'**isomorphisme** canonique $\langle ., . \rangle : A^n \times B^n \to \cup_{n \geqslant 0}(A \times B)^n$ on peut reconnaître des **relations** sur les entiers.



la relation d'addition : $\{\langle x, y, z \rangle | \nu(x) + \nu(y) = \nu(z)\}$

Question Quelles relations intéressantes peut-on **reconnaître** ainsi ?

Question Quels problèmes arithmétiques peut-on **résoudre** ainsi ?

Comment **formaliser**
une propriété arithmétique ?

Retour au cours de logique

Définition Une **signature** d'un langage du premier ordre, c'est la donnée d'une collection (potentiellement infinie) :

- de **symboles de constantes** ;
- de **symboles de fonctions** $f(x_1, \dots, x_n)$ (ici d'**arité** n) ;
- de **symboles de relations** $R(x_1, \dots, x_m)$ (ici d'**arité** m).

Par exemple, pour faire de l'**arithmétique** sur les entiers, on pourrait prendre comme signature $(\{0, 1\}, \{+\}, \{<\})$ ou encore $(\{0, 1\}, \{+, \times\}, \{=\})$.

Des termes aux formules

Les **termes** calculent des valeurs du domaine d'interprétation :

$$
\begin{aligned}
T \coloneqq\ & x \mid y \mid \ldots && \textit{variables} \\
& \mid c_0 \mid c_1 \mid \ldots && \textit{constantes} \\
& \mid f(T_1, \ldots, T_n) \mid g(T_1, \ldots, T_m) \mid \ldots && \textit{fonctions}
\end{aligned}
$$

Des termes aux formules

Les **termes** calculent des valeurs du domaine d'interprétation :

$$
\begin{aligned}
T &:= x \mid y \mid \ldots && \textit{variables} \\
&\mid c_0 \mid c_1 \mid \ldots && \textit{constantes} \\
&\mid f(T_1, \ldots, T_n) \mid g(T_1, \ldots, T_m) \mid \ldots && \textit{fonctions}
\end{aligned}
$$

Les **formules atomiques** transforment les termes en prédicats :

$$
\textit{Atom} := R_1(T_1, \ldots, T_n) \mid R_2(T_1, \ldots, T_m) \mid \ldots \qquad \textit{relations}
$$

Des termes aux formules

Les **termes** calculent des valeurs du domaine d'interprétation :

$$
\begin{aligned}
T &:= x \mid y \mid \dots && \textit{variables} \\
&\mid c_0 \mid c_1 \mid \dots && \textit{constantes} \\
&\mid f(T_1, \dots, T_n) \mid g(T_1, \dots, T_m) \mid \dots && \textit{fonctions}
\end{aligned}
$$

Les **formules atomiques** transforment les termes en prédicats :

$$
Atom := R_1(T_1, \dots, T_n) \mid R_2(T_1, \dots, T_m) \mid \dots \qquad \textit{relations}
$$

Les **formules** construisent des prédicats à partir de connecteurs :

$$
\begin{aligned}
\varphi, \psi &:= Atom && \textit{formules atomiques} \\
&\mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \varphi \to \psi && \textit{connecteurs logiques} \\
&\mid \exists x \varphi \mid \forall x \varphi && \textit{quantificateurs}
\end{aligned}
$$

Exemples de formules

Avec la signature $(\{0,1\},\{+\},\{=,<\})$:

$$\varphi_1(x) \doteq \exists n\ x = n + n$$
$$\varphi_2(x) \doteq \forall y\ \ (y < x \to y = 0)$$
$$\varphi_3 \doteq \exists x \exists y\ \ (x + y = 1 + 1 + 1 \wedge x = y + 1)$$
$$\varphi_4(x,y) \doteq \exists z\ \ (x = z + z + z + y \vee z + z + z + x = y)$$
$$\varphi_5(x,y) \doteq \neg(x < y) \wedge \neg(y < x)$$
$$\varphi_6(x,y) \doteq \exists z\ x + z = y$$
$$\varphi_7(x) \doteq \neg\exists y\ y < x$$
$$\varphi_8(x) \doteq \forall y\ \ (y < x \to y = 0)$$

Exemples de formules étendues

Avec la signature $(\{0,1\},\{+\},\{=,<\})$:

$$
\begin{aligned}
\varphi_1(x) &\doteq \exists n\ x = 2n \\
\varphi_2(x) &\doteq \forall y\ (y < x \to y = 0) \\
\varphi_3 &\doteq \exists x \exists y\ (x + y = 3 \wedge x = y + 1) \\
\varphi_4(x,y) &\doteq \exists z\ (x = 3z + y \vee 3z + x = y) \\
\varphi_5(x,y) &\doteq x \geqslant y \wedge y \geqslant x \\
\varphi_6(x,y) &\doteq \exists z\ x + z = y \\
\varphi_7(x) &\doteq \neg \exists y\ y < x \\
\varphi_8(x) &\doteq \forall y\ (y < x \to y = 0)
\end{aligned}
$$

Prédicats et formules closes

Une variable x est **libre** dans une formule φ si elle n'apparaît pas dans une sous-formule de la forme $\exists x\psi$ ou $\forall x\psi$. Une variable qui n'est pas libre est une variable **liée**.

Une **formule close** est une formule dont toutes les variables sont liées.

Une formule φ dont les variables libres sont $x_1, \dots, x_n$ sera notée $\varphi(x_1, \dots, x_n)$. On dit qu'elle code un **prédicat** d'arité n.

Comment **donner du sens**
aux formules ?

Approche syntaxique

L'approche **syntaxique** repose sur la notion de **théorie** et de **démonstration**. Elle manipule des formules et des séquents.

Une **théorie** $\mathcal{T} = \{\varphi_i\}$ sur une **signature** est une collection (pas nécessairement finie) de **formules closes** appelées **axiomes** de la théorie.

Un **système de règles** (par exemple le **calcul des séquents**) permet de construire des **démonstrations formelles** pour établir la notion de **formule prouvable** à partir d'hypothèses.

$$\Gamma \vdash \varphi$$

Démonstrations, consistance, complétude

Définition Une **formule close** φ est **prouvable** dans une théorie $\mathcal{T}$, noté $\mathcal{T} \vdash \varphi$ s'il existe un sous-ensemble fini $\Gamma \subseteq T$ tel que $\Gamma \vdash \varphi$.

Une théorie $\mathcal{T}$ est **consistante** si $\mathcal{T} \nvdash \bot$.

Une théorie $\mathcal{T}$ est **complète** si elle est **consistante** et si pour toute formule close φ, on a $\mathcal{T} \vdash \varphi$ ou $\mathcal{T} \vdash \neg\varphi$.

Approche sémantique

L'approche **sémantique** repose sur la notion de **modèle** et d'**interprétation**. Elle interprète des formules dans des domaines.

Une **interprétation** $\mathcal{M}$ est un **modèle** d'une **théorie** $\mathcal{T}$, noté $\mathcal{M} \models \mathcal{T}$, si $\mathcal{M}$ **satisfait** toutes les formules de $\mathcal{T}$.

Une **théorie** est **contradictoire** si elle n'admet aucun modèle.

Définition Une **formule close** φ est **valide** dans $\mathcal{T}$, noté $\mathcal{T} \models \varphi$, si $\mathcal{M} \models \varphi$ pour tout modèle $\mathcal{M}$ de $\mathcal{T}$.

Théorème de complétude

Les notions syntaxique de prouvabilité et sémantique de vérité coïncident !

Théorème de complétude (Gödel 1929) Soit $\mathcal{T}$ une théorie et φ une formule close. La formule est **prouvable** si et seulement si elle est **valide**, *i.e.*

$$\mathcal{T} \vdash \varphi \iff \mathcal{T} \models \varphi \quad .$$

Théorème de complétude

Les notions syntaxique de prouvabilité et sémantique de vérité coïncident !

Théorème de complétude (Gödel 1929) Soit $\mathcal{T}$ une théorie et φ une formule close. La formule est **prouvable** si et seulement si elle est **valide**, *i.e.*

$$\mathcal{T} \vdash \varphi \iff \mathcal{T} \models \varphi \quad .$$

Remarque Ce théorème permet de **définir** une **théorie** à partir d'un **modèle** : on prend sa signature avec l'ensemble des formules valides comme axiomes.

$$\mathrm{Th}(\mathcal{M}) = \{\varphi | \mathcal{M} \models \varphi\}$$

$$\mathrm{Th}(\mathbb{N}, +, <)$$

Arithmétique de Presburger

Une théorie étudiée par Presburger, un élève de Tarski, c'est le fragment limité de l'arithmétique $\mathrm{Th}(\mathbb{Z}, +, 0, 1, =)$. Ces travaux s'inscrivaient dans l'étude de l'**Entscheidungsproblem** d'Hilbert et Ackermann.

Arithmétique de Presburger

Une théorie étudiée par Presburger, un élève de Tarski, c'est le fragment limité de l'arithmétique $\mathrm{Th}(\mathbb{Z}, +, 0, 1, =)$. Ces travaux s'inscrivaient dans l'étude de l'**Entscheidungsproblem** d'Hilbert et Ackermann.

Presburger a montré que cette théorie est **consistante**, **complète**, **récursivement axiomatisable** et **décidable**. Pour cela il utilise une technique d'**élimination des quantificateurs**.

Théorème (Presburger 1929) La théorie au premier ordre des entiers munis de l'addition est **décidable**.

Arithmétique de Presburger

Une théorie étudiée par Presburger, un élève de Tarski, c'est le fragment limité de l'arithmétique $\mathrm{Th}(\mathbb{Z}, +, 0, 1, =)$. Ces travaux s'inscrivaient dans l'étude de l'**Entscheidungsproblem** d'Hilbert et Ackermann.

Presburger a montré que cette théorie est **consistante**, **complète**, **récursivement axiomatisable** et **décidable**. Pour cela il utilise une technique d'**élimination des quantificateurs**.

Théorème (Presburger 1929) La théorie au premier ordre des entiers munis de l'addition est **décidable**.

En 1960, Büchi propose un algorithme utilisant les **automates finis** pour décider la validité des formules.

Axiomatisation de $\mathrm{Th}(\mathbb{N}, 0, 1, +, =)$

En plus des axiomes usuels pour $=$, on ajoute :

1. $\forall x \neg(x + 1 = 0)$
2. $\forall x, y \ (x + 1 = y + 1 \to x = y)$
3. $\forall x \ (x + 0 = x)$
4. $\forall x, y \ (x + (y + 1) = (x + y) + 1)$
5. Schéma d'induction pour toute formule $\varphi(x, y_1, \dots, y_n)$:
   $\forall y_1 \forall y_2 \dots \forall y_n \big((\varphi(0, y_1, , y_n) \wedge \forall x(\varphi(x, y_1, , y_n) \to \varphi(x + 1, y_1, , y_n))) \to \forall x \varphi(x, y_1, , y_n)\big)$

Interlude

Les théories **complètes** et **décidables** sont rares !

L'**arithmétique de Peano** correspond à $\mathrm{Th}(\mathbb{N}, 0, 1, +, \times, =)$.

Interlude

Les théories **complètes** et **décidables** sont rares !

L'**arithmétique de Peano** correspond à $\mathrm{Th}(\mathbb{N}, 0, 1, +, \times, =)$.

Théorème d'incomplétude (Gödel 1931) Dans n'importe quelle théorie **récursivement axiomatisable** consistante au moins aussi expressive que l'**arithmétique de Peano**, on peut construire une formule close qui n'est ni prouvable ni réfutable.

Interlude

Les théories **complètes** et **décidables** sont rares !

L'**arithmétique de Peano** correspond à $\mathrm{Th}(\mathbb{N}, 0, 1, +, \times, =)$.

Théorème d'incomplétude (Gödel 1931) Dans n'importe quelle théorie **récursivement axiomatisable** consistante au moins aussi expressive que l'**arithmétique de Peano**, on peut construire une formule close qui n'est ni prouvable ni réfutable.

Théorème (Tarski 1936) La théorie au premier ordre des entiers munis de l'addition et de la multiplication est **indécidable**.

Arithmétique de Presburger

Reprenons **calmement** !

Arithmétique de Presburger

Reprenons **calmement**!

L'**arithmétique de Presburger** est la théorie du premier ordre des entiers naturels sur la signature $(0, 1, +, =)$.

Arithmétique de Presburger

Reprenons **calmement** !

L'**arithmétique de Presburger** est la théorie du premier ordre des entiers naturels sur la signature $(0, 1, +, =)$. Ses formules sont définies inductivement par la grammaire suivante :

$$\varphi, \psi \coloneqq s = t \mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \varphi \to \psi \mid \exists\varphi \mid \forall\varphi$$
$$s, t \coloneqq 0 \mid 1 \mid x \mid s + t \qquad \text{où } x \text{ est une variable}$$

Arithmétique de Presburger

Reprenons **calmement**!

L'**arithmétique de Presburger** est la théorie du premier ordre des entiers naturels sur la signature $(0, 1, +, =)$. Ses formules sont définies inductivement par la grammaire suivante :

$$\varphi, \psi \coloneqq s = t \mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \varphi \to \psi \mid \exists\varphi \mid \forall\varphi$$
$$s, t \coloneqq 0 \mid 1 \mid x \mid s + t \qquad \text{où } x \text{ est une variable}$$

Une **interprétation** I d'un prédicat $\varphi(x_1, \dots, x_n)$ associe un **entier** $I(x)$ à chaque **variable libre** x.

Arithmétique de Presburger

Reprenons **calmement** !

L'**arithmétique de Presburger** est la théorie du premier ordre des entiers naturels sur la signature $(0, 1, +, =)$. Ses formules sont définies inductivement par la grammaire suivante :

$$\varphi, \psi \coloneqq s = t \mid \neg\varphi \mid \varphi \wedge \psi \mid \varphi \vee \psi \mid \varphi \to \psi \mid \exists\varphi \mid \forall\varphi$$
$$s, t \coloneqq 0 \mid 1 \mid x \mid s + t \qquad \text{où } x \text{ est une variable}$$

Une **interprétation** I d'un prédicat $\varphi(x_1, \dots, x_n)$ associe un **entier** $I(x)$ à chaque **variable libre** x.

L'interprétation I **satisfait** le prédicat $\varphi(x_1, \dots, x_n)$, noté $I \models \varphi$, si la formule instanciée par I est **valide** dans $\mathbb{N}$.

Codage des interprétations

On **code** les tuples de n entiers comme des mots sur l'alphabet $\{0,1\}^n$.

Codage des interprétations

On **code** les tuples de n entiers comme des mots sur l'alphabet $\{0,1\}^n$.

On les voit comme n pistes qui codent chacune une **représentation binaire** d'un entier, complétée si besoin avec des 0 non significatifs.

$$\text{repr}(3,7,54) = \binom{0}{0}\binom{0}{0}\binom{0}{0}\binom{0}{1}\binom{1}{1}\binom{1}{1}\binom{1}{0}$$

Codage des interprétations

On **code** les tuples de n entiers comme des mots sur l'alphabet $\{0,1\}^n$.

On les voit comme n pistes qui codent chacune une **représentation binaire** d'un entier, complétée si besoin avec des 0 non significatifs.

$$\mathrm{repr}(3,7,54) = \binom{0}{0}\binom{0}{0}\binom{0}{0}\binom{0}{1}\binom{1}{1}\binom{1}{0}$$

Pour **coder une interprétation** I, il faut se donner un **ordre** $\prec$ sur les variables. On note $\mathrm{repr}(I, \prec)$ le codage de I ordonné par $\prec$.

Théorème de Büchi

On associe à un **prédicat** le langage des interprétations qui le **satisfont**.

$$L(\varphi, \prec) = \{\text{repr}(I, \prec) | I \models \varphi\}$$

Théorème Pour tout prédicat $\varphi(x_1, \dots, x_n)$ et tout ordre $\prec$ sur $\{x_i\}$, le langage $L(\varphi, \prec)$ est **reconnaissable**.

Théorème de Büchi

On associe à un **prédicat** le langage des interprétations qui le **satisfont**.

$$L(\varphi, \prec) = \{\text{repr}(I, \prec) | I \models \varphi\}$$

Théorème Pour tout prédicat $\varphi(x_1, \ldots, x_n)$ et tout ordre $\prec$ sur $\{x_i\}$, le langage $L(\varphi, \prec)$ est **reconnaissable**.

Idée de la preuve On commence par canoniser la formule :

(1) en remplaçant les termes par des termes simples de la forme $x = y$ ou $z = x + y$, quitte à ajouter des variables supplémentaires.

(2) en mettant la formule en forme prénexe : on remonte les quantificateurs en tête pour obtenir $Q_1 x_1 Q_2 x_2 \ldots Q_m x_m \psi$ avec ψ sans quantificateur.

On construit ensuite un automate à partir des formules atomiques. On fait attention à la quantification et aux zéros en tête des pistes.

Théorème de Cobham

Dans tout ce qui précède, le choix de la base 2 pour la représentation des nombres est **arbitraire**.

Théorème de Cobham

Dans tout ce qui précède, le choix de la base 2 pour la représentation des nombres est **arbitraire**.

Notons $L_k(\varphi, \prec)$ le langage associé à φ en base k et $L_k(X)$ le langage associé à un ensemble de tuples $X \subseteq \mathbb{N}^m$ arbitraire.

Théorème de Cobham

Dans tout ce qui précède, le choix de la base 2 pour la représentation des nombres est **arbitraire**.

Notons $L_k(\varphi, \prec)$ le langage associé à φ en base k et $L_k(X)$ le langage associé à un ensemble de tuples $X \subseteq \mathbb{N}^m$ arbitraire.

Théorème (Cobham 1969) Soit $X \subseteq \mathbb{N}$ et $m, n \geqslant 2$ premiers entre eux. Si $L_m(X)$ et $L_n(X)$ sont **reconnaissables** alors X est **définissable** par une formule de l'**arithmétique de Presburger**.

Théorème de Cobham

Dans tout ce qui précède, le choix de la base 2 pour la représentation des nombres est **arbitraire**.

Notons $L_k(\varphi, \prec)$ le langage associé à φ en base k et $L_k(X)$ le langage associé à un ensemble de tuples $X \subseteq \mathbb{N}^m$ arbitraire.

Théorème (Cobham 1969) Soit $X \subseteq \mathbb{N}$ et $m, n \geqslant 2$ premiers entre eux. Si $L_m(X)$ et $L_n(X)$ sont **reconnaissables** alors X est **définissable** par une formule de l'**arithmétique de Presburger**.

Théorème (Semenov 1977) Soit $X \subseteq \mathbb{N}^k$ et $m, n \geqslant 2$ premiers entre eux. Si $L_m(X)$ et $L_n(X)$ sont **reconnaissables** alors X est **définissable** par une formule de l'**arithmétique de Presburger**.

Pour aller plus loin

Les ensembles définissables dans l'**arithmétique de Presburger** ont une jolie caractérisation en tant qu'**ensembles semi-linéaires**.

Les ensembles d'entiers définissables dans une base fixée ont une jolie caractérisation comme **arithmétiques de Büchi**.

En TP, vous expérimenterez ces arithmétiques avec l'outil **Walnut** :

> *Walnut is free software, written in Java, for deciding first-order statements phrased in an extension of Presburger arithmetic, called Buchi arithmetic. It can be used to prove hundreds of results in combinatorics on words, number theory, and other areas of discrete mathematics. It can handle a wide variety of problems.*