Université de Liège

# Extension d'un théorème de Cobham pour l'anneau des polynômes à coefficients dans un corps fini

Adeline Massuir

25 janvier 2017

# Changement de base

2049

Base 10 : $2 \times 10^3 + 4 \times 10^1 + 9 \times 10^0$

$$\rightsquigarrow (2, 0, 4, 9)$$

Base 2 : $1 \times 2^{11} + 1 \times 2^0$

$$\rightsquigarrow (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$$

Base 3 : $2 \times 3^6 + 2 \times 3^5 + 1 \times 3^4 + 2 \times 3^2 + 2 \times 3^1$

$$\rightsquigarrow (2, 2, 1, 0, 2, 2, 0)$$

# Reconnaissabilité

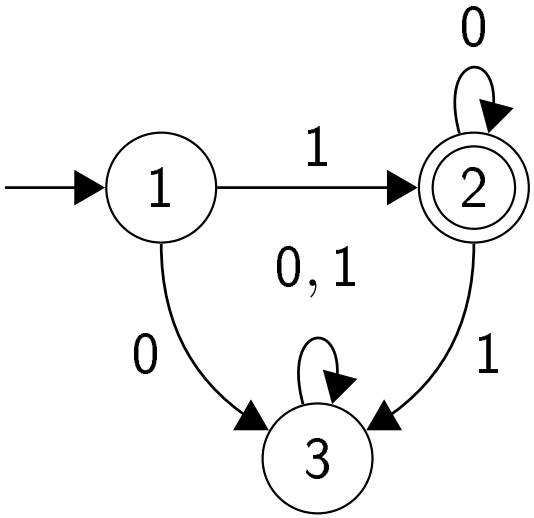
**Définition**

Soit $p \in \mathbb{N}\backslash\{0,1\}$. Une partie $\mathscr{N}$ de $\mathbb{N}$ est *p-reconnaissable* s'il existe un automate fini déterministe $\mathscr{A} = (Q, q_0, F, \{0,1,\ldots,p-1\}, \delta)$ qui accepte le langage $\rho_p(\mathscr{N})$.

**Définition**

Soit $p \in \mathbb{N}\backslash\{0,1\}$. Une partie $\mathscr{N}$ de $\mathbb{N}$ est *p-reconnaissable* s'il existe un automate fini déterministe $\mathscr{A} = (Q, q_0, F, \{0,1,\ldots,p-1\}, \delta)$ qui accepte le langage $\rho_p(\mathscr{N})$.

Base 2 :

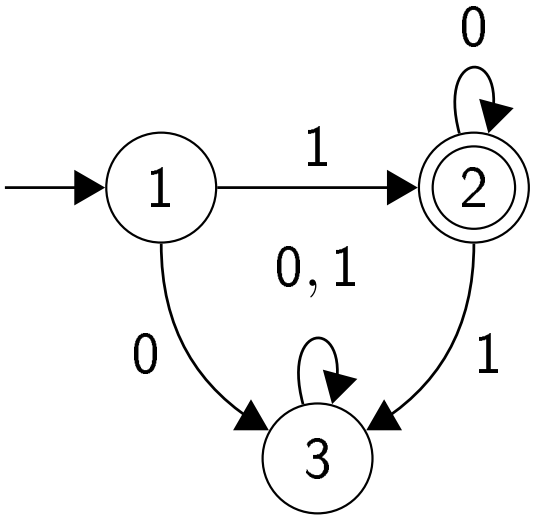


# Reconnaissabilité

**Définition**

Soit $p \in \mathbb{N}\backslash\{0,1\}$. Une partie $\mathscr{N}$ de $\mathbb{N}$ est *p-reconnaissable* s'il existe un automate fini déterministe $\mathscr{A} = (Q, q_0, F, \{0,1,\ldots,p-1\}, \delta)$ qui accepte le langage $\rho_p(\mathscr{N})$.

Base 2 :




Base 10 :

$2^{63} = 9223372036854775808$

# Théorème de Cobham

**Thérorème de Cobham (1969)**

Soient $p, q \in \mathbb{N}\backslash\{0,1\}$ multiplicativement indépendants. Si $\mathscr{N} \subseteq \mathbb{N}$ est $p$-reconnaissable et $q$-reconnaissable alors c'est une union finie de progressions arithmétiques.

**Corollaire**

Un ensemble de naturels est reconnaissable si, et seulement si, c'est une union finie de progressions arithmétiques.

# $P$-représentation d'un polynôme

$$X^3 + X^2 + 2X + 1$$

Base $X$ : $1 \times X^3 + 1 \times X^2 + 2 \times X^1 + 1 \times X^0$

$$\rightsquigarrow (1, 1, 2, 1)$$

Base $X^2 + 2$ : $(X + 1) \times (X^2 + 2)^1 + 2 \times (X^2 + 2)^0$

$$\rightsquigarrow (X + 1, 2)$$

# Reconnaissabilité

**Définition**

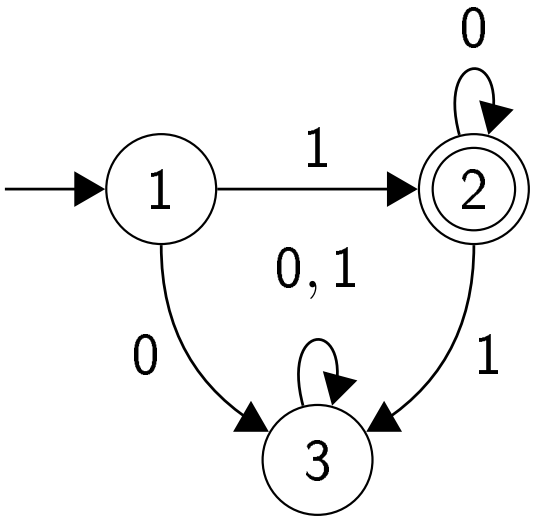
Soit $P \in \mathbb{F}[X]_{>0}$. Une partie $\mathscr{F}$ de $\mathbb{F}[X]$ est *P-reconnaissable* s'il existe un automate fini déterministe $\mathscr{A} = \left(Q, q_0, F, \mathbb{F}[X]_{<\deg P}, \delta\right)$ qui accepte le langage $\rho_P(\mathscr{F})$.

# Reconnaissabilité

**Définition**

Soit $P \in \mathbb{F}[X]_{>0}$. Une partie $\mathscr{F}$ de $\mathbb{F}[X]$ est *$P$-reconnaissable* s'il existe un automate fini déterministe $\mathscr{A} = \left(Q, q_0, F, \mathbb{F}[X]_{<\deg P}, \delta\right)$ qui accepte le langage $\rho_P(\mathscr{F})$.

Base $X+1$ :

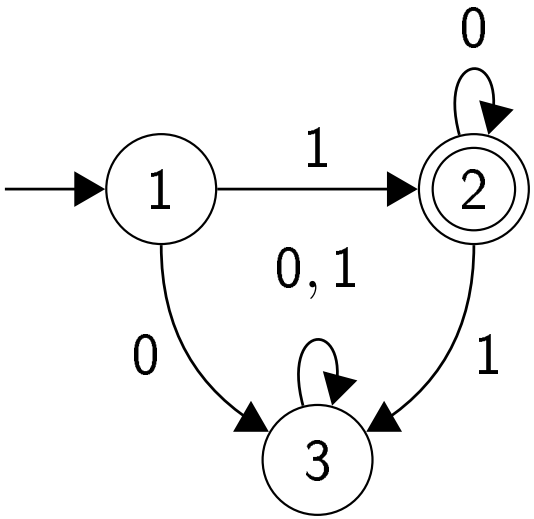


# Reconnaissabilité

**Définition**

Soit $P \in \mathbb{F}[X]_{>0}$. Une partie $\mathscr{F}$ de $\mathbb{F}[X]$ est *P-reconnaissable* s'il existe un automate fini déterministe $\mathscr{A} = \left(Q, q_0, F, \mathbb{F}[X]_{<\deg P}, \delta\right)$ qui accepte le langage $\rho_P(\mathscr{F})$.

Base $X+1$ :




Base $X$ :

Binôme de Newton

# Exemples de base dans $\mathbb{F}[X]$

1. $\{AQ + B \mid Q \in \mathbb{F}[X]\}$ avec $A, B \in \mathbb{F}[X]$

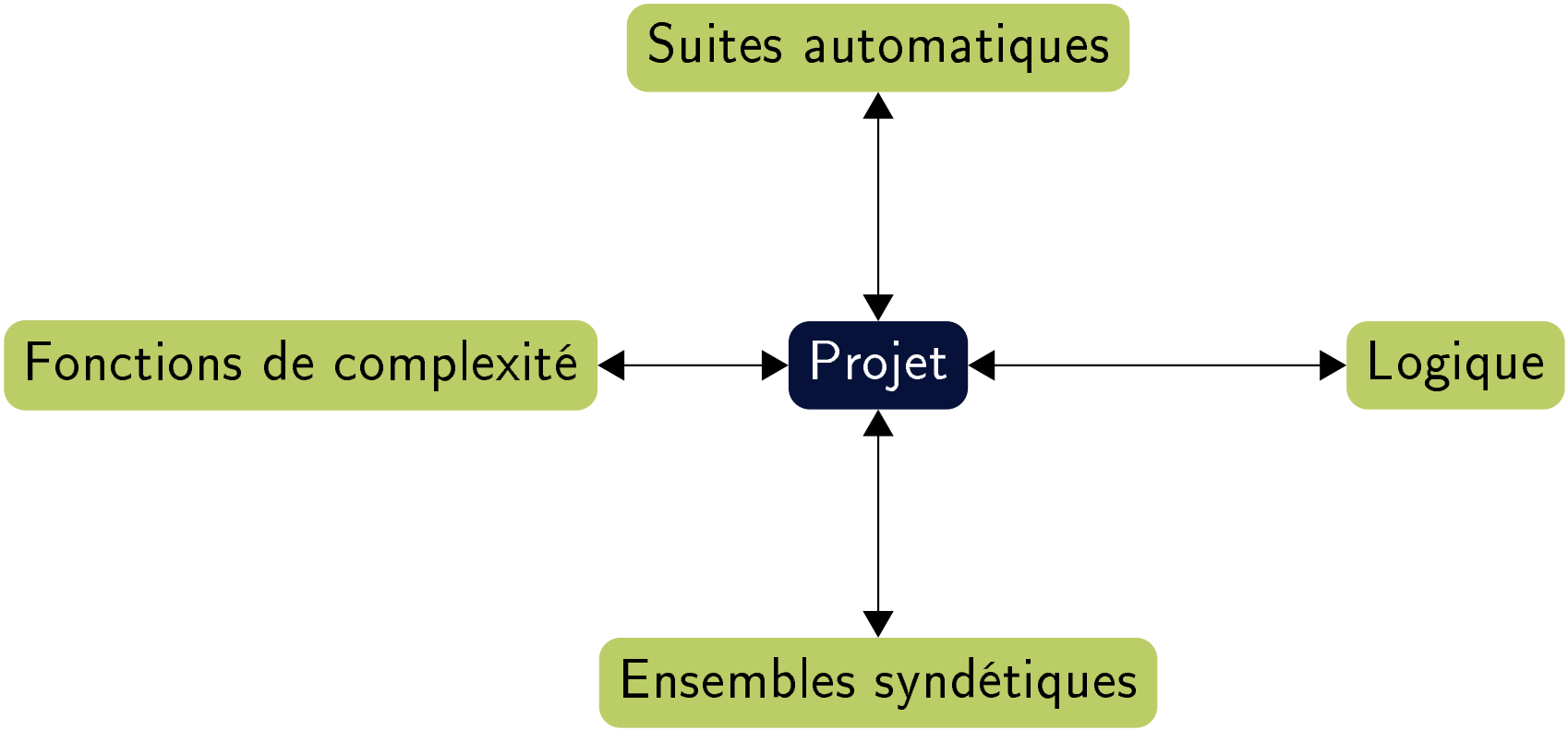
# Exemples de base dans $\mathbb{F}[X]$

1. $\{AQ + B \mid Q \in \mathbb{F}[X]\}$ avec $A, B \in \mathbb{F}[X]$
2. $\{Q \in \mathbb{F}[X] \mid \deg Q \equiv r \bmod d\}$ avec $d, r \in \mathbb{N}$, $d \neq 0$ et $r < d$

# Exemples de base dans $\mathbb{F}[X]$

1. $\{AQ + B \mid Q \in \mathbb{F}[X]\}$ avec $A, B \in \mathbb{F}[X]$
2. $\{Q \in \mathbb{F}[X] \mid \deg Q \equiv r \bmod d\}$ avec $d, r \in \mathbb{N}$, $d \neq 0$ et $r < d$
3. $\{X^n.Q + R \mid n \in \mathbb{N}, R \in \mathbb{F}[X]_{<n}\}$ avec $Q \in \mathbb{F}[X] \setminus \{0\}$

# Approches possibles/Applications



# Logique pour les naturels

Dans $\mathbb{N}$ :

$$(\mathbb{N}, \{=\}, \{+, V_p\}, \{\neg, \rightarrow\}, \{\forall\})$$

# Logique pour les naturels

Dans $\mathbb{N}$ :

$$(\mathbb{N}, \{=\}, \{+, V_p\}, \{\neg, \rightarrow\}, \{\forall\})$$

$$a \vee b = \neg a \rightarrow b$$

# Logique pour les naturels

Dans $\mathbb{N}$ :

$$(\mathbb{N}, \{=\}, \{+, V_p\}, \{\neg, \rightarrow\}, \{\forall\})$$

$$a \vee b = \neg a \rightarrow b$$

- $0$ : $a = 0 \Leftrightarrow a + a = a$

# Logique pour les naturels

Dans $\mathbb{N}$ :

$$(\mathbb{N}, \{=\}, \{+, V_p\}, \{\neg, \rightarrow\}, \{\forall\})$$

$$a \vee b = \neg a \rightarrow b$$

- $0 : a = 0 \Leftrightarrow a + a = a$
- $1 : a = 1 \Leftrightarrow V_p(0) = a$

# Logique pour les polynômes

Dans $\mathbb{F}[X]$ :

$$(\mathbb{F}[X], \{=, \prec\}, \{+, (.C : C \in \mathbb{F}[X]), V_P\}, \{\neg, \rightarrow\}, \{\forall\})$$

# Logique pour les polynômes

Dans $\mathbb{F}[X]$ :

$$(\mathbb{F}[X], \{=, \prec\}, \{+, (.C : C \in \mathbb{F}[X]), V_P\}, \{\neg, \rightarrow\}, \{\forall\})$$

- $0 : A = 0 \Leftrightarrow (\forall B)(A \prec B \vee A = B)$

# Logique pour les polynômes

Dans $\mathbb{F}[X]$ :

$$(\mathbb{F}[X], \{=, \prec\}, \{+, (.C : C \in \mathbb{F}[X]), V_P\}, \{\neg, \rightarrow\}, \{\forall\})$$

- $0 : A = 0 \Leftrightarrow (\forall B)(A \prec B \vee A = B)$
- $1 : A = 1 \Leftrightarrow V_P(0) = A$

# Retour à la définition du 0

Dans $\mathbb{N}$ :

$a = 0 \Leftrightarrow a + a = a$

Dans $\mathbb{F}[X]$ :

$A = 0 \Leftrightarrow (\forall B)\,(A \prec B \vee A = B)$

# Retour à la définition du 0

Dans $\mathbb{N}$ :
$a = 0 \Leftrightarrow a + a = a$

Dans $\mathbb{F}[X]$ :
$A = 0 \Leftrightarrow (\forall B)\,(A \prec B \vee A = B)$

**Exemple**

$$\begin{array}{rr} & 53 \\ + & 27 \\ \hline & 80 \end{array}$$

**Exemple**

Si $\mathbb{F} = \{0, 1, 2\}$, alors

$$\begin{array}{rrrrrr} & X^2 & + & 2X & + & 1 \\ + & & & 2X & + & 2 \\ \hline & X^2 & + & X & & \end{array}$$

# Retour aux structures

Dans $\mathbb{N}$ :

$$(\mathbb{N}, \{=\}, \{+, V_p\}, \{\neg, \rightarrow\}, \{\forall\})$$

Dans $\mathbb{F}[X]$ :

$$(\mathbb{F}[X], \{=, \prec\}, \{+, (.C : C \in \mathbb{F}[X]), V_P\}, \{\neg, \rightarrow\}, \{\forall\})$$

# Retour aux structures

Dans $\mathbb{N}$ :

$$(\mathbb{N}, \{=\}, \{+, V_p\}, \{\neg, \rightarrow\}, \{\forall\})$$

Dans $\mathbb{F}[X]$ :

$$(\mathbb{F}[X], \{=, \prec\}, \{+, (.C : C \in \mathbb{F}[X]), V_P\}, \{\neg, \rightarrow\}, \{\forall\})$$

- $\prec$ : $a < b \Leftrightarrow \exists m(a + m + 1 = b)$

# Retour aux structures

Dans $\mathbb{N}$ :

$$(\mathbb{N}, \{=\}, \{+, V_p\}, \{\neg, \rightarrow\}, \{\forall\})$$

Dans $\mathbb{F}[X]$ :

$$(\mathbb{F}[X], \{=, \prec\}, \{+, (.C : C \in \mathbb{F}[X]), V_P\}, \{\neg, \rightarrow\}, \{\forall\})$$

- $\prec$ : $a < b \Leftrightarrow \exists m(a + m + 1 = b)$
- $(.C : C \in \mathbb{F}[X])$ : $a.c = b \Leftrightarrow \underbrace{a + \ldots + a}_{c \text{ termes}} = b$

# Bibliographie


• Michel Rigo, *Théorie des automates et langages formels*, Université de Liège, 2009–2010.

• Michel Rigo et Laurent Waxweiler, *Logical characterization of recognizable sets of polynomials over a finite field*, International Journal of Foundations of Computer Science **22** (2011), 7, pp. 1549–1563.

• Laurent Waxweiler, *Caractère reconnaissable d'ensembles de polynômes à coefficients dans un corps fini*, Thèse de doctorat, Université de Liège, Liège, Décembre 2009.