

Rappel Le langage de la Théorie de Presburger est L constitué de

0 = symbole de zéro ; s = symbole de fonction unaire ; $+$ = symbole de fonction binaire ;
 $=$ = symbole de prédicat binaire.

th PRES : $\left\{ \begin{array}{l} \text{entier} = \varphi \text{ une } L\text{-formule close} \\ \text{stabi} = \text{oui si } \mathbb{N} \models \varphi \text{ (N est 1 modèle pour } \varphi), \text{ non sinon} \end{array} \right.$
 est un problème décidable.

démo • plan démo : ① expliquer comment on code les k -uplets d'entiers
 ② ramener le pb à la vacuité/universalité d'un langage
 sur l'alphabet de codage
 ③ montrer que ledit langage est régulier en construisant
 pour lui 1 automate

Comme on sait décider la vacuité et l'universalité d'un langage reg, ça conclura.

① Codage de $(m_i)_{i \in [1, k]} \in \mathbb{N}^k$:

- on écrit chaque m_i en binaire : $m_i = \overset{\text{bit faible}}{c_i^1} \dots c_i^{\overset{\text{bit fort}}{n}} \quad (\text{bits faibles en } 1^{er})$
 - quitte à rajouter des zéros au bout, on peut écrire tous les m_i sur le même nb

$$\begin{array}{l} \text{de bits } n : \\ m_1 = \begin{pmatrix} c_1^1 \\ \vdots \\ c_1^n \end{pmatrix} \\ \vdots \\ m_k = \begin{pmatrix} c_k^1 \\ \vdots \\ c_k^n \end{pmatrix} \end{array}$$

- Le codage de $(m_i)_i$ est alors $\underbrace{\begin{pmatrix} c_1^1 \\ \vdots \\ c_k^1 \end{pmatrix}}_{\in \Sigma_k} \underbrace{\begin{pmatrix} c_1^2 \\ \vdots \\ c_k^2 \end{pmatrix}}_{\in \Sigma_k} \dots \underbrace{\begin{pmatrix} c_1^n \\ \vdots \\ c_k^n \end{pmatrix}}_{\in \Sigma_k} \in \Sigma_k^*$
 $\in \Sigma_k = \{ \text{vecteurs colonnes à } k \text{ colonnes avec des } 0 \text{ et } 1 \}$

- Si $w \in \Sigma_k^*$, on note $\llbracket w \rrbracket_k$ le décodage de w = le k -uplet correspondant.

- ex (2, 3, 6) devient en binaire avec poids faibles en 1^{er}

$$(010, 110, 011) \text{ et son codage est donc } \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Réciproquement le décodage $\llbracket \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \rrbracket_k$ est (6, 5)

- us : on oublie ds la suite les parenthèses

$$\llbracket \varepsilon \rrbracket_k = () \text{ et } \llbracket \varepsilon \rrbracket_k = (0, 0, 0)$$

② Def On nomme "formule atomique simple en L " toute formule de la forme
 $x_i = 0$; $x_i = x_j$; $s(x_i) = x_j$ ou $x_i + x_j = x_k$ où i, j, k 2 à 2 $\neq$

• Soit φ une formule close. on peut la mettre sous forme préfixe et, quitte à ajouter des variables, on peut se ramener à une formule préfixe dont les formules atomiques sont simples

$$\begin{aligned} \text{Par ex, si } \varphi &= (\exists x_1 \quad s(x_1) = 0) \wedge (\exists x_2 \quad \exists x_3 \quad x_2 = x_3) \\ &= \exists x_1 \exists x_2 \exists x_3 \underbrace{(s(x_1) = 0) \wedge (x_2 = x_3)}_{\text{non simple}} \quad [\text{préfixe}] \\ &= \exists x_1 \exists x_2 \exists x_3 \exists x_4 \quad (x_4 = 0) \wedge (s(x_1) = x_4) \wedge (x_2 = x_3) \quad [\text{ok}] \end{aligned}$$

On peut donc supposer que $\varphi = Q_1 x_1 \dots Q_m x_m \psi$

avec les Q_i des quantificateurs, les x_i des variables et ψ une [comb. booléenne ($\wedge, \vee, \neg$)] de formules atomiques simples sans quantificateurs.

• On a donc $\varphi = Q_1 x_1 \dots Q_k x_k \underbrace{Q_{k+1} x_{k+1} \dots Q_m x_m \psi}_{:= \psi_k}$

Ainsi, $\psi_0 = \varphi$, $\psi_m = \psi$ et ψ_k est tg des variables libres sont $x_1, \dots, x_k$.

On note $\forall k \in [0, m]$, $\mathcal{V}_k = \{ (m_1, \dots, m_k) \mid N[x_1 = m_1, \dots, x_k = m_k] \models \psi_k \}$ N avec attribution $x_i = m_i$ pour $i \leq k$

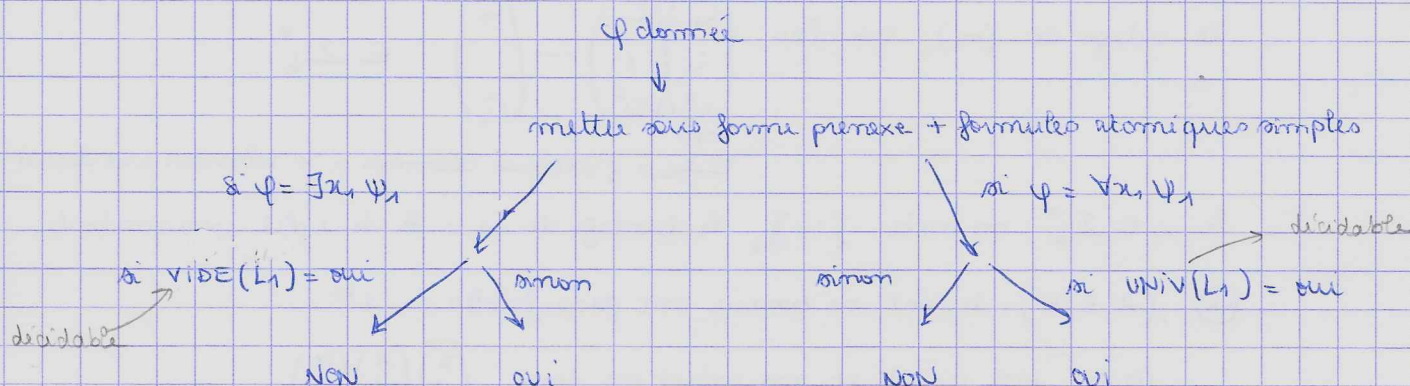
et $\mathcal{L}_k = \{ w \in \Sigma_k^* \mid \llbracket w \rrbracket_k \in \mathcal{V}_k \}$ (version "collage" de $\mathcal{V}_k$)

moment crucial $\triangle$

↳ Si $\varphi = \exists x_1 \psi_1$ alors $N \models \varphi \Leftrightarrow \mathcal{V}_1 \neq \emptyset \Leftrightarrow \mathcal{L}_1 \neq \emptyset$

Si $\varphi = \forall x_1 \psi_1$ alors $N \models \varphi \Leftrightarrow \mathcal{V}_1 = N \Leftrightarrow \mathcal{L}_1 = \Sigma_1^*$

Donc si on arrive à montrer que $\mathcal{L}_1$ est rat, voici la procédure pour décider PRES :



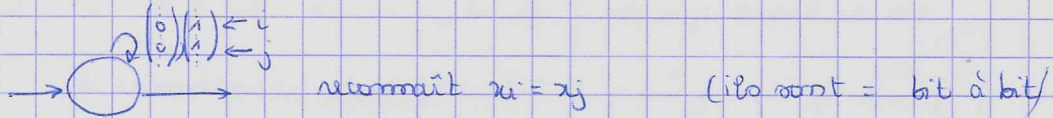
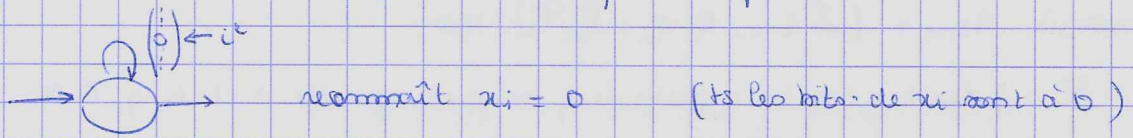
③ Montrons donc /rec que $\mathcal{L}_1$ est rationnel = reconnaissable.

on montre /rec sur k allant de m à 1 H_k " $\exists$ 1 automate A_k tg $L(A_k) = \mathcal{L}_k$ "

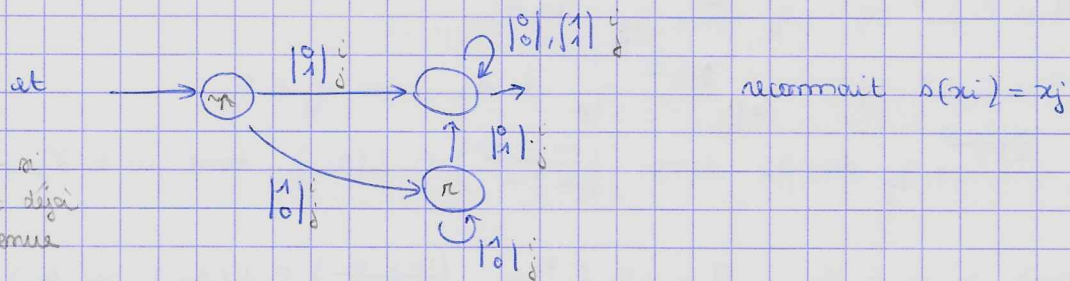
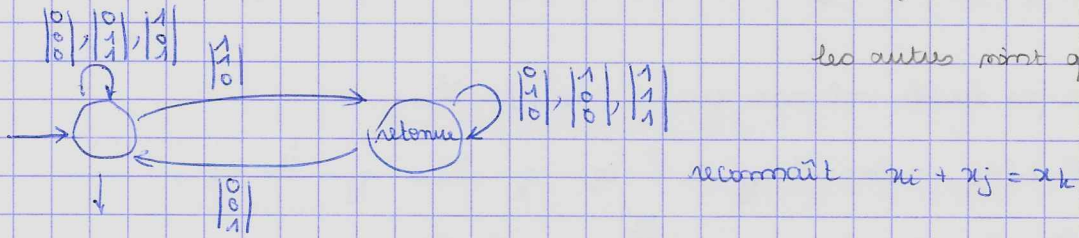
Pour $k = m$: ψ = combiné bool de formules atomiques simples. Concluons A_m / induit par ψ

→ on mg $\exists$ 1 automate qui reconnaît les codages des entiers satisfaisant

F pour F = chacune des 4 formules atomiques simples



Soit = on note juste les bits de x_i de x_j de x_k les autres sont quelconques



comme si
y avait déjà
1 retenue

→ Si $\psi = \neg \tilde{\psi}$, on construit 1 automate pour $\tilde{\psi}$ et son complémentaire convient pour ψ

Si $\psi = \psi_1 \vee \psi_2$, l'union des automates pour ψ_1 et ψ_2 convient pour ψ

Si $\psi = \psi_1 \wedge \psi_2$, l'intersection " " " " "

donc Mm.

Soit $k > 1$ tq H_k et notons $A_k = (\Sigma_k, Q, q_0, F, T)$. Montrons H_{k-1} .

→ Si $\psi_{k-1} = \exists x_k \psi_k$ alors (si $\psi_{k-1} = \neg \exists x_k \neg \psi_k = \neg (\exists x_k \neg \psi_k) \Rightarrow$ on utilise des complémentaires)

$$P_{k-1} = \{ (m_1, \dots, m_{k-1}) \mid \exists m_k, (m_1, \dots, m_k) \in P_k \}$$

$$\text{et } L_{k-1} = \{ w \in \Sigma_{k-1}^* \mid \exists m_k, (w \cdot \mathbb{I}_{k-1}, m_k) \in P_k \}$$

$$= \{ w \in \Sigma_{k-1}^* \mid \exists c \in \Sigma_1^* (w \cdot \mathbb{I}_{k-1}, \mathbb{I}_c \cdot \mathbb{I}_1) \in P_k \}$$

$$\stackrel{(*)}{=} \{ w \in \Sigma_{k-1}^* \mid \exists c \in \Sigma_1^*, \mathbb{I}_c \cdot w \cdot \mathbb{I}_1 \in P_k \}$$

$$= \{ w \in \Sigma_{k-1}^* \mid \exists u, v \in \Sigma_1^*, \left(\frac{w}{u} \cdot \frac{0 \dots 0}{v} \right) \in L_k \}$$

$$\stackrel{(*)}{=} L_{k-1} = \{ w \in \Sigma_{k-1}^* \mid \exists u, v \in \Sigma_1^*, \left(\frac{w}{u} \cdot \frac{0 \dots 0}{v} \right) \in L(A_k) \}$$

et au besoin on
ajoute des zéros au codage
c pour que celui-ci soit
plus long que w
 $\Rightarrow (*)$ est ok

par HR

On note alors p la projection $\left\{ \begin{array}{l} \Sigma_k \rightarrow \Sigma_{k-1} \\ \begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} \mapsto \begin{pmatrix} c_1 \\ \vdots \\ c_{k-1} \end{pmatrix} \end{array} \right.$ qui consiste à oublier la dernière composante et

on construit $A_{k-1} = (\Sigma_{k-1}, Q, q_0, \tilde{F}, \tilde{T})$ avec

$\tilde{F} = \{ \text{états } q \in Q \text{ tq à partir de } q \text{ on peut rejoindre 1 état } q_f \in F$

en notant que des $\frac{q}{v}$ de $A_k \} = \{ q \mid \exists q_f \in F, q \xrightarrow{\tilde{T} \begin{pmatrix} 0 \\ 0 \end{pmatrix}^*} q_f \text{ de } A_k \}$

et $\tilde{T} = \{ q \xrightarrow{p(a)} q' \mid q \xrightarrow{a} q' \in T \} = \{ \text{transitions de } A_k$

de lesquelles on a effacé la dernière ligne des étiquettes $\}$

On montre par double inclusion que $L(A_{k-1}) = L_k$

Si $w \in L(A_{k-1})$ alors $\exists q_{g'} \in \tilde{F}$ tq $q_0 \xrightarrow{w} q_{g'}$ de A_{k-1}

Par def $\tilde{T}$, $\exists u \in \Sigma_1^*$ tq $q_0 \xrightarrow{u} q_{g'}$ de A_k

Par def $\tilde{F}$, $\exists v \in \Sigma^*$ tq $q_{g'} \xrightarrow{\begin{pmatrix} 0 \\ 0 \end{pmatrix}^*} q_f$ de A_k avec $q_f \in F$

Alors $q_0 \xrightarrow{\frac{w|0}{u|v}} q_f$ de A_k donc $\left(\frac{w|0}{u|v} \right) \in L(A_k)$ donc $w \in L_{k-1}$ par (*)

Réciproquement, si $w \in L_{k-1}$, $\exists u, v \in \Sigma_1^*$ tq $\left(\frac{w|0}{u|v} \right) \in L(A_k)$ par (*)

De $\exists q_{g'} \in \tilde{F}$ et $q_f \in F$ tq $q_0 \xrightarrow{u} q_{g'} \xrightarrow{\begin{pmatrix} 0 \\ 0 \end{pmatrix}^*} q_f$ de A_k

Par def de $\tilde{T}$, $q_0 \xrightarrow{w} q_{g'}$ et par def $\tilde{F}$, $q_{g'} \in \tilde{F}$ donc $w \in L(A_{k-1})$

Ceci assure que M_{k-1} donc conclut la réc donc assure que L_1 est rationnel donc conclut la démo.