Suites récurrentes linéaires

Le point de vue informatique

Emmanuel Jeandel

ENS Lyon

Le problème

Problème

u_n est une suite récurrente linéaire d'ordre k si

$$u_n = \sum_{i \leq k} \alpha_i u_{n-i}$$

➧ Est-ce qu'il existe n tel que $u_n = 0$?

Propriétés algébriques

Dans l'algèbre des suites à valeurs dans $\mathbb{K}$:

$(u_n)_{n\in\mathbb{N}}$ est une suite récurrente $\iff$ l'espace vectoriel engendré par les suites $(u_{n+k})_{n\in\mathbb{N}}$ est de dimension finie

- Si u et v sont des suites linéaires récurrentes et $\lambda \in \mathbb{K}$
  - $u+v, -v, \lambda u$ est une SLR
  - $u \cdot v$ est une SLR

L'ensemble des SLR est donc une sous-algèbre de l'ensemble des suites, et les diviseurs de zéro sont les suites u tel qu'il existe n avec $u_n = 0$.

Contenu

Dans $\mathbb{C}$, les suites linéaires récurrentes sont engendrées (en tant qu'algèbre) par

$$\begin{array}{lll} u_n & = & \lambda^n \qquad u_n = \lambda u_{n-1}, u_0 = 1 \\ u_n & = & n \qquad u_n = 2u_{n-1} - u_{n-2}, u_0 = 0, u_1 = 1 \\ u_n & = & \chi_p(n) \end{array}$$

Dans $\mathbb{R}$, il faut ajouter $u_n = cos(n\theta)$ $(u_n = 2cos(\theta)u_{n-1} - u_{n-2})$ et $u_n = sin(n\theta)$.

Forme matricielle

$u_n = \sum_{k=1}^{p} \alpha_k u_{n-k}$ s'écrit aussi

$$u_n = \begin{pmatrix} 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_{p-1} & \alpha_p \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}^n \begin{pmatrix} u_p \\ u_{p-1} \\ \vdots \\ u_1 \\ u_0 \end{pmatrix}$$

Le problème est donc équivalent au problème $\mathbf{u}^T \mathcal{M}^n \mathbf{v} = 0$
C'est le problème d'atteignabilité point-hyperplan qu'on peut aussi écrire

$$\mathbf{u}^T \mathcal{X} \mathbf{v} = 0, \mathcal{X} \in \{\mathcal{M}\}^\star$$

Généralisations indécidables

- Equations diophantiennes exponentielles
  $\alpha^n + \beta^m + \gamma^p \cdots = 0$
  ⇝ indécidable (Davis-Putnam-Robinson 1961)

Généralisations indécidables

- Equations diophantiennes exponentielles
  $\alpha^n + \beta^m + \gamma^p \cdots = 0$
  ⇝ indécidable (Davis-Putnam-Robinson 1961)
- Equations diophantiennes $n^\alpha + m^\beta\, p^\gamma \cdots = 0$
  ⇝ indécidable (Matiyasevich 1970)

Généralisations indécidables

- Equations diophantiennes exponentielles
  $\alpha^n + \beta^m + \gamma^p \cdots = 0$
  ⇒ indécidable (Davis-Putnam-Robinson 1961)
- Equations diophantiennes $n^\alpha + m^\beta\, p^\gamma \cdots = 0$
  ⇒ indécidable (Matiyasevich 1970)
- On change $\mathbf{u}^T \mathcal{X} \mathbf{v} = 0$ avec $\mathcal{X} \in \{\mathcal{M}\}^\star$ en
  $\mathbf{u}^T \mathcal{X} \mathbf{v} = 0, \mathcal{X} \in \{\mathcal{A}, \mathcal{B}\}^\star$
  Également indécidable

Reformulation

Dans la formule

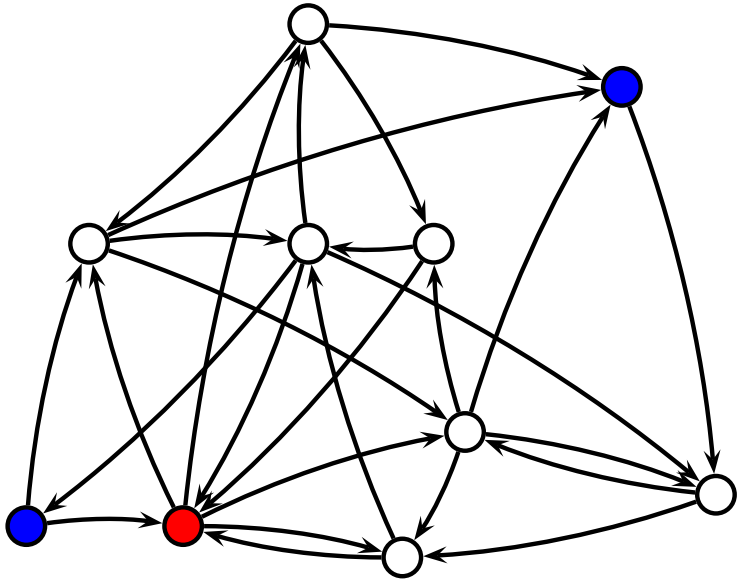
$$\mathbf{u}^T \mathcal{M}^n \mathbf{v} = 0$$

on peut supposer

- Les coefficients de $\mathcal{M}$ sont 0 ou 1.
- $\mathbf{u}$ contient au maximum deux coefficients non nuls, -1 et 1.
- $\mathbf{v}$ ne contient au maximum qu'un coefficient non nul, qui vaut 1.

$\mathcal{M}$ peut alors être vu comme la matrice d'adjacence d'un graphe

Reformulation



Est-ce qu'il existe i tel qu'il y ait autant de chemins de longueur i entre le point rouge et chacun des deux points bleus ?

Langages rationnels

- Etant donnés deux automates, est-ce qu'il existe un entier n tels que ces automates reconnaissent autant de mots de longueur n ?

Langages rationnels

- Etant donnés deux automates, est-ce qu'il existe un entier n tels que ces automates reconnaissent autant de mots de longueur n ?
- Etant donnés deux automates non déterministes sur un lettre, est-ce qu'il existe un mot ω qu'ils reconnaissent par le même nombre de chemins ?

Langages rationnels

- Etant donnés deux automates, est-ce qu'il existe un entier n tels que ces automates reconnaissent autant de mots de longueur n ?
- Etant donnés deux automates non déterministes sur un lettre, est-ce qu'il existe un mot ω qu'ils reconnaissent par le même nombre de chemins ?
- Etant donnés un automate sur une lettre non déterministe, est-ce qu'il existe un mot ω non reconnu
  ⇒ Problème $\mathcal{NP}$-dur (Blondel-Portier, 99)

Résultats

Valeurs absolues dans $\mathbb{Q}$

Dans $\mathbb{Q}$, les seules valeurs absolues possibles sont

- La valeur absolue usuelle : $\|3/4\| = 0.75, \| -12\| = 12$
- Les valeurs absolues p-adiques $\|a\| = 1/p^n$, où p^n est la plus grande puissance de p présente dans a ($\|0\| = +\infty$)

$$\|3/4\|_2 = 4, \|3/4\|_3 = 1/3, \|3/4\|_5 = 1$$

$$\|-20\|_2 = 1/4, \|-20\|_3 = 1, \|-20\|_5 = 1/5$$

Ces valeurs absolues vérifient $\|a+b\| \leq \max(\|a\|, \|b\|)$

- Remarquons que $\|x\| \prod \|x\|_p = 1$

Valeurs absolues

Dans une extension finie de $\mathbb{Q}$, il y a plus de valeurs absolues, chacune extraite des valeurs absolues dans $\mathbb{Q}$. Prenons comme exemple l'extension générée par $\rho = -25 + \sqrt{665}$ vérifiant $\rho^2 + 50\rho - 40 = 0$ On a alors

- Deux valeurs absolues "normales" : $\|a + b\rho\| = |a + b\rho|$ et $\|a + b\rho\| = |a + b\overline{\rho}|$
- Les deux valeurs absolues 2-adiques : $\|\rho\|_a = 1/2$, $\|\rho\|_b = 1/4$
- La valeur absolue 5-adique : $\|\rho\|_c = 1/\sqrt{5}$
- La valeur absolue 7-adique : $\|\rho\|_d = 1$ et $\|\rho - 3\|_d = 1/\sqrt{7}$

Réductions

$u_n = \sum \alpha_i u_{n-i}$ peut s'écrire $u_n = \sum \rho_i^n f_i(n)$, où les ρ_i sont les racines du polynômes $X^n - \sum \alpha_i X^i$

- On peut supposer que 0 n'est pas racine (il suffit de s'intéresser à la suite u_{n+k} pour un k bien choisi)
- On peut supposer qu'il n'y a pas deux racines α et β tels que α/β soit une racine de l'unité différente de 1. (il suffit de s'intéresser aux suites u_{pn+l} pour p bien choisi et $0 \leq l \leq p-1$) On évite ainsi le cas :

$$u_n = \alpha^n + (i\alpha)^n$$

On dit alors que u_n est non dégénérée

Le théorème fondamental

(Skolem-Mahler-Lech)

L'ensemble des n tels que $u_n = 0$ est l'union de composantes périodiques et d'une partie finie.

De plus, si u_n est non dégénérée, l'ensemble des n tels que $u_n = 0$ est fini.

Plus précisément, si u_n et v_n sont non dégénérées, et que $u_n = v_n$ infiniment souvent, alors $u_n = v_n$.

Multiplicité

On peut définir $m(n)$ le plus petit entier m tel qu'une suite récurrente non dégénérée d'ordre n ait au plus m zéros. (Schmidt 1999)

$$m(n) \leq \exp\exp\exp(3n\log n)$$

Cas particuliers

(Vereschagin 1984)

Le problème est décidable pour les suites récurrentes à coefficients dans $\mathbb{R}$ d'ordre n, $n \leq 4$.

Atteignabilité point-espace

Le problème d'atteignabilité point-espace de dimension k est le problème

$$\mathcal{R}\mathcal{M}^i\mathbf{v} = \mathbf{s}$$

avec $\mathcal{R}$ de rang $n-k$. Les suites récurrentes correspondent au problème point-hyperplan (Kannan-Lipton) Le problème point-point est décidable et même polynomial.

Le problème point-espace k en toute dimension est décidable si et seulement si le problème point-hyperplan est décidable en dimension $k+1$