

Automates finis et séries de Laurent algébriques

Alina FIRICEL

Institut Camille Jordan, Université Lyon 1

INRIA, 21 mars 2011

Problème

Soit \mathbb{K} un corps fini.

- ▶ **But** : « **Approcher** » une série de Laurent $f \in \mathbb{K}((T))$, algébrique, par des fractions rationnelles $P_n/Q_n \in \mathbb{K}(T)$:

$$|Q_n|^\rho \ll \left| f - \frac{P_n}{Q_n} \right| \ll |Q_n|^\delta.$$

- ▶ **Idée** : **Troncation** du développement en série de Laurent de f à certains endroits « bien choisis » en utilisant une approche qui combine la théorie des nombres, la théorie des automates finis et la combinatoire des mots.
- ▶ **Motivation** : Absence du théorème de Roth \rightsquigarrow difficile d'obtenir des informations sur les **mesures d'irrationalité** des séries de Laurent algébriques.

Séries de Laurent à coefficients dans un corps fini

- ▶ Dans cet exposé, p désigne un nombre premier et q une puissance de p .
- ▶ Rappelons l'analogie entre les deux séries d'inclusions suivantes :

$$\begin{array}{ccc} \mathbb{Z} & & \mathbb{F}_q[T] \\ \cap & & \cap \\ \mathbb{Q} & \approx & \mathbb{F}_q(T) \\ \cap & & \cap \\ \mathbb{R} & & \mathbb{F}_q((T^{-1})). \end{array}$$

- ▶ On définit une **valeur absolue ultramétrique** par

$$|f| = q^{-n_0} \quad \text{si } f = \sum_{n \geq -n_0} a_n T^{-n} \neq 0, \quad a_{-n_0} \neq 0, \quad \text{et } |0| = 0.$$

Le corps $\mathbb{F}_q((T^{-1}))$ est le complété de $\mathbb{F}_q(T)$ pour cette valeur absolue.

Séries de Laurent algébriques

Définition. Une série de Laurent $f \in \mathbb{F}_q((T^{-1}))$ est **algébrique** sur $\mathbb{F}_q(T)$ s'il existe $P \in \mathbb{F}_q(T)[X]$, non nul, tel que $P(f) = 0$. Sinon, elle est dite **transcendante** sur $\mathbb{F}_q(T)$.

Exemple de Mahler. La série

$$f_M(T) = \sum_{n \geq 0} T^{-p^n} \in \mathbb{F}_p[[T^{-1}]]$$

est racine du polynôme

$$TX^p - TX + 1 = 0.$$

En effet, si

$$f_M(T) = \frac{1}{T} + \frac{1}{T^p} + \frac{1}{T^{p^2}} + \cdots,$$

alors

$$f_M^p(T) = \frac{1}{T^p} + \frac{1}{T^{p^2}} + \frac{1}{T^{p^3}} + \cdots = f_M(T) - \frac{1}{T},$$

ce qui implique

$$Tf_M^p(T) - Tf_M(T) + 1 = 0.$$

Remarque. Les p racines de l'équation sont $a + f_M(T)$, pour $a \in \mathbb{F}_p$.

Séries de Laurent algébriques

Exemple de Thue–Morse. Soit $f_{\mathbf{t}}(T) := \sum t_n T^{-n} \in \mathbb{F}_2((T^{-1}))$, où $\mathbf{t} := (t_n)_{n \geq 0}$ est la suite :

$$t_n = \begin{cases} 1 & \text{si } (n)_2 \text{ contient un nombre impair de } 1 \\ 0 & \text{sinon.} \end{cases}$$

Remarque. $t_{2n} = t_n \pmod{2}$ et $t_{2n+1} = (t_n + 1) \pmod{2}$

Ainsi

$$f_{\mathbf{t}}(T) = \sum t_{2n} T^{-2n} + \sum t_{2n+1} T^{-2n-1} = \sum t_n T^{-2n} + T^{-1} \sum (t_n + 1) T^{-2n}$$

et alors

$$f_{\mathbf{t}}(T) = f_{\mathbf{t}}(T^2) + \frac{1}{T} f_{\mathbf{t}}(T^2) + \frac{T}{T^2 - 1}.$$

Ainsi la série $f_{\mathbf{t}}$ satisfait l'équation algébrique suivante :

$$(T + 1)^3 X^2 + T(T + 1)^2 X + T^2 = 0.$$

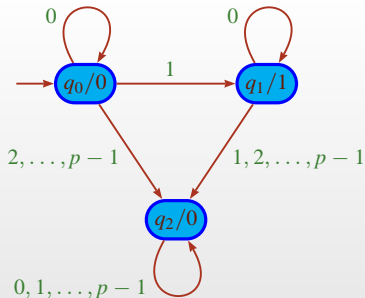
Suites automatiques

Définition. Une suite $\mathbf{a} = (a_n)_n$ est **k -automatique** s'il existe un automate fini qui produit a_n comme sortie quand l'entrée est le développement en base k de n .

Exemple de Mahler. La suite $\mathbf{a} := (a_n)_{n \geq 0}$ définie par

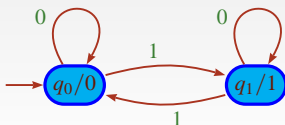
$$a_n = \begin{cases} 1 & \text{si } n \text{ est une puissance de } p ; \\ 0 & \text{sinon} \end{cases}$$

est p -automatique car elle peut être engendrée par l'automate suivant



Suites automatiques et k -noyaux

Exemple de Thue–Morse. Cette suite est 2-automatique car elle peut être engendrée par l'automate suivant



Si l'entrée est $W := 11001$, on obtient 1 et donc $t_{25} = 1$.

Rappel. Pour tout $n \geq 0$ on a : $t_{2n} = t_n \pmod 2$ et $t_{2n+1} = (t_n + 1) \pmod 2$.

Définition. Pour tout entier $k \geq 1$, le k -noyau de $\mathbf{a} := (a_n)_{n \geq 0}$ est l'ensemble défini par :

$$\mathcal{N}_k(\mathbf{a}) = \left\{ (a_{k^i n + j})_{n \geq 0} \mid i \geq 0 \text{ et } 0 \leq j < k^i \right\}.$$

Théorème (Eilenberg, 1974). Une suite est k -automatique si et seulement si son k -noyau est un ensemble fini.

Exemple. On a $\mathcal{N}_2(\mathbf{t}) = \{(t_n)_{n \geq 0}, (t_{2n+1})_{n \geq 0}\}$.

Suites automatiques et morphismes de monoïdes libres

Morphisme. Soient \mathcal{A}, \mathcal{B} deux alphabets finis. Un **morphisme** est une application $\sigma : \mathcal{A}^* \mapsto \mathcal{B}^*$ telle que $\sigma(UV) = \sigma(U)\sigma(V)$ pour tous les mots $U, V \in \mathcal{A}^*$.

Un morphisme est dit **k -uniforme** si chaque lettre a pour l'image un mot de longueur k . Si l'image d'une lettre est une lettre, alors le morphisme est appelé **codage**.

Théorème (Cobham, 1972). Une suite \mathbf{a} est k -automatique si et seulement si il existe une lettre a , un **morphisme k -uniforme** σ et un **codage** φ tels que $\mathbf{a} = \varphi(\sigma^\infty(a))$.

Exemple. La suite de Thue–Morse peut être caractérisée comme suit :

$$\mathbf{t} := (t_n)_{n \geq 0} = 0110100110010110100101 \dots = \sigma^\infty(0),$$

où σ est défini par $\sigma(0) = 01, \sigma(1) = 10$.

Séries algébriques et suites automatiques

Théorème (Christol, 1979). Soit f une série de Laurent à coefficients dans \mathbb{F}_q . Alors f est algébrique sur $\mathbb{F}_q(T)$ si et seulement si la suite de ses coefficients est p -automatique.

Remarque. Pour tout $m \geq 1$, une suite $\mathbf{a} = (a_n)_{n \geq 0}$ est k -automatique si et seulement si elle est k^m -automatique.

Théorème (Cobham, 1969). Soit $\mathbf{a} = (a_n)_{n \geq 0}$ une suite à valeurs dans un alphabet fini. Soient k et l deux entiers multiplicativement indépendants (c'est-à-dire $\log k / \log l$ est irrationnel). Alors \mathbf{a} est k et l -automatique si et seulement si \mathbf{a} est ultimement périodique.

Approximation rationnelle des séries de Laurent algébriques

Approximation rationnelle des séries de Laurent algébriques

Question. Dans quelle mesure peut-on approcher les nombres irrationnels par des nombres rationnels ?

- ▶ Pour $\xi \in \mathbb{R} \setminus \mathbb{Q}$ on définit l'**exposant d'irrationalité** (ou **mesure d'irrationalité**) $\mu(\xi)$ comme le supremum des nombres réels τ pour lesquels l'inégalité

$$\left| \xi - \frac{p}{q} \right| \leq \frac{1}{|q|^\tau}$$

possède une infinité de solutions rationnelles p/q .

- ▶ On a une définition analogue pour les séries de Laurent à coefficients dans un corps fini : on remplace les nombres rationnels par les fractions rationnelles.

Résultats généraux

- ▶ **Inégalité de Liouville (1849)**. Si $\xi \in \mathbb{R}$ algébrique irrationnel de degré d , alors $\mu(\xi) \in [2, d]$.

Dans le corps $\mathbb{F}_q((T^{-1})) \rightsquigarrow$ **Mahler (1949)**.

- ▶ **Théorème de Thue (1909)**. Si $\xi \in \mathbb{R}$ algébrique irrationnel de degré d , alors $\mu(\xi) \in [2, \frac{d}{2} + 1]$.

Dans le corps $\mathbb{F}_q((T^{-1})) \rightsquigarrow$ **Voloch (1988), de Mathan–Lasjaunias (1996)** (seulement pour certaines séries algébriques).

- ▶ **Théorème de Roth (1955)**. Soient ξ un nombre algébrique irrationnel et $\varepsilon > 0$. Alors l'inégalité

$$\left| \xi - \frac{p}{q} \right| < \frac{1}{q^{2+\varepsilon}}$$

ne possède qu'un nombre fini de solutions rationnelles p/q et donc $\mu(\xi) = 2$.

- ▶ **Schmidt (1999), Thakur (1999)**. Pour tout $s \in [2, \infty[\cap \mathbb{Q}$, il existe $f(T)$ algébrique sur $\mathbb{F}_q(T)$ telle que $\mu(f) = s$.

Une mesure d'irrationalité générale

Théorème (F., 2010). Soit $f = \sum_{n \geq 0} a_n T^{-n} \in \mathbb{F}_q((T^{-1}))$ algébrique sur $\mathbb{F}_q(T)$. Alors on a

$$\mu(f) \leq p^{s+1} e,$$

où s est le cardinal du p -noyau de la suite $\mathbf{a} = (a_n)_{n \geq 0}$ et e le nombre d'états de l'automate minimal engendrant \mathbf{a} (dans le sens direct).

Remarque. En pratique, on peut améliorer cette borne et on peut éliminer la dépendance en p -noyau. Dans les meilleurs cas, on peut obtenir la valeur exacte de l'exposant.

Un lemme d'approximation

Lemme. Soit f une série de Laurent à coefficients dans \mathbb{F}_q . Soient δ, ρ et θ des nombres réels tels que $0 < \delta \leq \rho$ et $\theta \geq 1$. On suppose qu'il existe une suite $(P_n/Q_n)_{n \geq 1}$ de fractions rationnelles à coefficients dans \mathbb{F}_q telles que :

$$(i) \quad \frac{1}{|Q_n|^{1+\rho}} \ll \left| f - \frac{P_n}{Q_n} \right| \ll \frac{1}{|Q_n|^{1+\delta}},$$

$$(ii) \quad |Q_n| < |Q_{n+1}| \ll |Q_n|^\theta.$$

Alors l'exposant d'irrationalité de f , $\mu(f)$, vérifie :

$$1 + \delta \leq \mu(f) \leq \frac{\theta(1 + \rho)}{\delta}.$$

Remarque. De plus, si on suppose pour tout n assez grand que $(P_n, Q_n) = 1$, alors

$$1 + \delta \leq \mu(f) \leq \max\left(1 + \rho, 1 + \frac{\theta}{\delta}\right).$$

Dans ce dernier cas, si $\delta = \rho \geq \sqrt{\theta}$, on obtient **la valeur exacte de l'exposant**.

Construction de bonnes approximations rationnelles

Soit $f(T) = \sum_{n \geq 0} a_n T^{-n} \in \mathbb{F}_q((T^{-1}))$ algébrique sur $\mathbb{F}_q(T)$.

Christol + Cobham \rightsquigarrow Il existe un morphisme p -uniforme $\sigma : \mathcal{A} \mapsto \mathcal{A}$ et un codage $\varphi : \mathcal{A} \mapsto \mathbb{F}_q$ tels que

$$\mathbf{a} := a_0 a_1 a_2 \cdots = \varphi(\sigma^\infty(a_0)).$$

- ▶ **Principe des tiroirs** \rightsquigarrow Il existe $w \in \mathbb{Q}$, $w > 1$, et deux mots finis U et V tels que UV^w soit préfixe de $\mathbf{a} := a_0 a_1 a_2 \cdots$.
- ▶ Pour tout $n \in \mathbb{N}$, on pose $U_n := \varphi(\sigma^n(U))$ et $V_n := \varphi(\sigma^n(V))$.

Construction de bonnes approximations rationnelles

Pour tout $n \in \mathbb{N}$, la suite des coefficients de f commence par $U_n \underbrace{V_n V_n \cdots V_n}_{w \text{ fois}}$.

Pour tout $n \in \mathbb{N}$, on note P_n/Q_n la fraction rationnelle dont le développement en série de Laurent est la suite (ultimement périodique) $U_n \underbrace{V_n V_n V_n \cdots}_{\text{une infinité de fois}}$.

- ▶ On obtient alors :

$$\left| f - \frac{P_n}{Q_n} \right| \leq \frac{1}{|Q_n|^{1+\delta}}, \text{ où } \delta = \frac{|U_n V_n^w|}{|U_n V_n|}.$$

- ▶ Si les deux suites ont en commun que les premiers $U_n V_n^w$ chiffres \rightsquigarrow égalité.
- ▶ Le **lemme d'approximation** \rightsquigarrow encadrement de l'exposant d'irrationalité.

Remarque. Cette approche a été déjà utilisée, dans le contexte des nombres réels automatiques, par Adamczewski et Cassaigne (2006), Adamczewski et Rivoal (2009), Adamczewski et Bugeaud (2010).

L'étude de coprimauté

Soient $k := |U|$ et $\ell := |V|$. On peut montrer que les dénominateurs

$$Q_n(T) = T^{kp^n-1}(T^{\ell p^n} - 1) = T^{kp^n-1}(T^\ell - 1)^{p^n}.$$

Remarque. Soit $n \in \mathbb{N}^*$. On a $(P_n, Q_n) = 1$ (sur $\mathbb{F}_q(T)$) si et seulement si

- (i) $P_n(0) \neq 0$ (condition qui peut être vérifiée facilement),
- (ii) pour tout $a \in \overline{\mathbb{F}}_p$, tel que $a^\ell = 1$, $P_n(a) \neq 0$.

On peut aussi montrer que $P_n(T) = P_{U_n}(T)(T^{\ell p^n} - 1) + P_{V_n}(T)$.

Notation. Si $U = a_0 a_1 \cdots a_{s-1}$ alors $P_U(T) := a_0 T^{s-1} + a_1 T^{s-2} + \cdots + a_{s-1}$.

Remarque. Pour $a \in \overline{\mathbb{F}}_p$, tel que $a^\ell = 1$,

$$P_n(a) = P_{V_n}(a) = P_{\varphi(\sigma^n(V))}(a).$$

Le calcul des numérateurs

Soit $\sigma : \mathcal{A}_3 \mapsto \mathcal{A}_3^*$ le morphisme 3-uniforme défini par :

$$\begin{cases} \sigma(0) & = & 010 \\ \sigma(1) & = & 210 \\ \sigma(2) & = & 001. \end{cases}$$

Les polynômes associés :

$$\begin{cases} P_{\sigma(0)}(T) & = & T \\ P_{\sigma(1)}(T) & = & 2T^2 + T \\ P_{\sigma(2)}(T) & = & 1. \end{cases}$$

On associe au morphisme σ la matrice :

$$M_\sigma(T) = \begin{pmatrix} T^2 + 1 & T & 0 \\ 1 & T & T^2 \\ T^2 + T & 1 & 0 \end{pmatrix}.$$

On a alors

$$\begin{pmatrix} P_{\sigma(0)}(T) \\ P_{\sigma(1)}(T) \\ P_{\sigma(2)}(T) \end{pmatrix} = \begin{pmatrix} T^2 + 1 & T & 0 \\ 1 & T & T^2 \\ T^2 + T & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}.$$

Matrices associées aux morphismes

En général, on a :

$$\begin{pmatrix} P_{\varphi(\sigma(0))}(T) \\ P_{\varphi(\sigma(1))}(T) \\ \vdots \\ P_{\varphi(\sigma(m-1))}(T) \end{pmatrix} = M_{\sigma}(T) \begin{pmatrix} \varphi(0) \\ \varphi(1) \\ \vdots \\ \varphi(m-1) \end{pmatrix}.$$

Remarque. Pour déterminer $P_{V_n}(T) = P_{\varphi(\sigma^n(V))}(T)$, on va s'intéresser à $M_{\sigma^n}(T)$.

Matrices associées aux morphismes

Proposition. Soit σ un p -morphisme défini sur \mathcal{A}_m . Alors pour tout $n \in \mathbb{N}^*$ on a

$$M_{\sigma^n}(T) = M_{\sigma}(T^{p^{n-1}})M_{\sigma}(T^{p^{n-2}}) \cdots M_{\sigma}(T)$$

où $M_{\sigma}(T)$ est la matrice associée à σ .

Remarque. Si $a \in \mathbb{F}_p$, alors pour tout $n \in \mathbb{N}$, on a :

$$M_{\sigma^n}(a) = M_{\sigma}(a)^n.$$

Proposition. Si V est un mot fini sur l'alphabet \mathcal{A}_m et $a \in \overline{\mathbb{F}_p}$, alors la suite $(P_{\varphi(\sigma^n(V))}(a))_{n \geq 0}$ est **ultimement périodique**.

Résumé

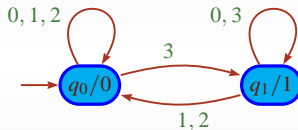
- On a une **formule explicite** pour les numérateurs $P_n(a)$, à l'aide de la matrice associée au morphisme.
- La suite $(P_n(a))_{n \geq 0}$ est ultimement périodique. De plus, la période et la pré-période de la suite $(P_n(a))_{n \geq 0}$ peuvent être **bornées de manière explicite**.
- Pour tester si P_n et Q_n sont premiers entre eux pour tout n assez grand, il suffit de tester, pour les a (racines ℓ -ièmes de l'unité), si $P_n(a)$ est différent de 0 **pour un nombre fini d'entiers n** .

Exemple

- ▶ Soit P le polynôme irréductible, à coefficients dans $\mathbb{F}_2(T)$, défini par :

$$P(X) = X^4 + X + \frac{T}{T^4 + 1}.$$

- ▶ Soit $f = \sum_{n \geq 0} a_n T^{-n}$ l'unique racine dans le corps $\mathbb{F}_2((T^{-1}))$. La suite des coefficients $\mathbf{a} = (a_n)_{n \geq 0}$ est engendrée par le 4-automate suivant :



- ▶ De plus, on peut montrer que $\mathbf{a} = \sigma^\infty(0)$, où σ est le morphisme défini par :

$$\sigma(0) = 0001$$

$$\sigma(1) = 1001.$$

Proposition. On a $\mu(f) = 3$.

Le théorème de **Liouville-Mahler** implique seulement que $\mu(f) \leq 4$.

Construction des approximations rationnelles

- ▶ La suite \mathbf{a} commence par $\underbrace{0001\ 0001\ 0001}_{\text{motifs répétitifs}}\ 1001 \dots$, donc pour tout $n \in \mathbb{N}$, la suite des coefficients de f commence par

$$f := \sigma^n(0001) \sigma^n(0001) \sigma^n(0001) 1 \dots .$$

- ▶ La série f est « proche » de la série rationnelle dont le développement est

$$\frac{P_n}{Q_n} := \sigma^n(0001)\sigma^n(0001) \sigma^n(0001) \sigma^n(0001) \dots = (\sigma^n(0001))^\infty .$$

- ▶ Plus précisément,

$$\left| f - \frac{P_n}{Q_n} \right| = \frac{1}{|Q_n|^3} .$$

- ▶ Ainsi, le **lemme d'approximation** implique :

$$3 \leq \mu(f) \leq 6 .$$

Si de plus $(P_n, Q_n) = 1$ alors

$$\mu(f) = 3 .$$

Coprimauté des polynômes

- ▶ De plus, $Q_n(T) = T^{4^n} - 1 = (T - 1)^{4^n}$ et $P_n(T) = P_{\sigma^n(0)}(T)$.
- ▶ Ainsi $(P_n, Q_n) = 1$ si et seulement si $P_n(1) \neq 0$, pour tout n assez grand.
- ▶ La matrice associée à σ est $M_\sigma(T) = \begin{pmatrix} T^3 + T^2 + T & 1 \\ T^2 + T & T^3 + 1 \end{pmatrix}$.
- ▶ Si $T = 1$, on obtient :

$$M_\sigma(1) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

Coprimauté des polynômes

- ▶ Puisque $M_{\sigma^n}(1) = M_\sigma(1)^n$, on obtient alors :

$$M_{\sigma^n}(1) = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},$$

ce qui permet de montrer :

$$\begin{pmatrix} P_{\sigma^n(0)}(T) \\ P_{\sigma^n(1)}(T) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

- ▶ Par conséquent, $P_n(1) = P_{\sigma^n}(1) = 1 \neq 0$, pour tout n . Donc $(P_n, Q_n) = 1$ sur $\overline{\mathbb{F}_p}(T)$.

Perspectives

Utiliser cette approche afin d'obtenir des résultats plus précis pour des familles particulières de séries de Laurent algébriques.

- ▶ Quelles propriétés doivent satisfaire le morphisme ou l'automate afin d'obtenir des approximations rationnelles irréductibles ?
- ▶ Quelles propriétés doivent satisfaire le morphisme ou l'automate afin d'obtenir la valeur exacte de l'exposant ?

Perspectives

Étendre cette approche à certaines séries de Laurent transcendentes.

Exemple - l'analogie de π

Il existe une fonction ζ définie dans le module de Carlitz, pour tout $s > 0$:

$$\zeta(s) = \sum_{\substack{P \in \mathbb{F}_q[T] \\ P \text{ unitaire}}} \frac{1}{P^s}.$$

Si $q - 1 | s$ alors $\zeta(s) = \Pi_q^s r_s$ où $r_s \in \mathbb{F}_q(T)$ et Π_q est défini par

$$\Pi_q = \prod_{j=1}^{\infty} \left(1 - \frac{1}{T^{q^j - 1}} \right)^{-1}$$

Π_q est transcendant sur $\mathbb{F}_q(T)$

(plusieurs preuves, en particulier, preuve « automatique » (Allouche, Berthé)).

Perspectives

Soit $\mathbf{a} = (a_n)_{n \geq 0}$ une suite à valeurs dans \mathbb{F}_q et $f(T) = \sum_{n \geq 0} a_n T^{-n}$.

- ▶ La **fonction de complexité** de \mathbf{a} est définie par :

$$p(\mathbf{a}, m) = \text{Card} \{ (a_j, a_{j+1}, \dots, a_{j+m-1}) \mid j \geq 0 \} .$$

- ▶ On définit alors la fonction de complexité f par $p(f, m) = p(\mathbf{a}, m)$.

Théorème (F., 2009). Si $q = 2$, alors $p(\frac{1}{\Pi_2}, m) = \Theta(m^2)$. Si $q \geq 3$, alors $p(\frac{1}{\Pi_q}, m) = \Theta(m)$.

Remarques.

Cela donne, en particulier, une autre preuve de transcendance de Π_2 sur $\mathbb{F}_2(T)$.

Résultat plutôt **surprenant** ! On s'attend que $p(\pi, b, m) = b^m$ pour tout $b \geq 2$ et $m \geq 1$ (conjecture de normalité).

Basse **complexité** \rightsquigarrow Motifs répétitifs \rightsquigarrow Bornes pour l'**exposant d'irrationalité** de Π_q .