Calcul des relations linéaires et multiplicatives entre les racines d'un polynôme

Thierry COMBOT

Université de Bourgogne, Dijon

November 21, 2024

Soit $P \in \mathbb{Q}[x]$ un polynôme de degré n, sans facteurs carrés.

On notera $\alpha_1, \ldots, \alpha_n$ ses n racines distinctes.

On s'intéresse à calculer les relations de la forme

$$r_1\alpha_1 + \cdots + r_n\alpha_n = q, \quad r_i, q \in \mathbb{Q} \quad \text{(relation linéaire)},$$

$$\alpha_1^{r_1} \cdots \alpha_n^{r_n} = q, \quad r_i \in \mathbb{Z},\ q \in \mathbb{Q} \quad \text{(relation multiplicative)}.$$

Trouver ces relations est décidable:

- Les relations linéaires peuvent être trouvées en considérant un idéal galoisien $\mathcal{I}$ définissant les relations polynomiales entre les racines de P. Les relations linéaires sont les éléments de $\mathcal{I}$ de degré ≤ 1, obtenables par une base de Groebner en degré total.
- Il existe une borne b telle que toutes les relations multiplicatives avec les $r_i \leq b$ génèrent toutes les relations multiplicatives. Des candidats peuvent être cherchés par approximation numérique, puis vérifiés en réduisant l'expression modulo $\mathcal{I}$.

Problème: ces approches sont très très lentes.

Elles sont en fait polynomiales en la taille du groupe de Galois de P:

Definition

On note $Gal_{\mathbb{K}}(P)$ *le groupe des automorphismes de* $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ *qui préserve* $\mathbb{K}$.

Ce groupe permute les racines α_i, et c'est donc un sous groupe de S_n, de cardinal $n!$.

Definition

Soit $P \in \mathbb{K}[x]$ un polynôme où $\mathbb{K}$ est une extension finie de $\mathbb{Q}$. On note $\mathbb{L}$ son corps de décomposition. La trace et la norme de $\beta \in \mathbb{L}$ sont

$$tr_{\mathbb{K}}(\beta) = \frac{1}{[\mathbb{L} : \mathbb{K}]} \sum_{\sigma \in Gal_{\mathbb{K}}(P)} \sigma(\beta), \qquad N_{\mathbb{K}}(\beta) = \prod_{\sigma \in Gal_{\mathbb{K}}(P)} \sigma(\beta).$$

Proposition

On a les égalités suivantes

$$tr_{\mathbb{K}}(\beta) = -\frac{coeff_{Z^{\deg T - 1}}(T)}{\deg T}, \qquad N_{\mathbb{K}}(\beta) = (-1)^{[\mathbb{L}:\mathbb{K}]} T(0)^{[\mathbb{L}:\mathbb{K}]/\deg T},$$

où $T \in \mathbb{K}[z]$ est le polynôme minimal unitaire de β.

Proposition

Une relation non homogène existe si et seulement si au moins un des facteurs de $P \in \mathbb{Q}[x]$ a un second coefficient no nul.

On applique la trace sur une relation

$$r_1\alpha_1 + \cdots + r_n\alpha_n = q$$

$$r_1 \mathrm{tr}_{\mathbb{Q}}(\alpha_1) + \cdots + r_n \mathrm{tr}_{\mathbb{Q}}(\alpha_n) = q.$$

Or la trace égale aussi

$$\mathrm{tr}_{\mathbb{Q}}(\alpha_i) = -\frac{\mathrm{coeff}_{z^{\deg T_i - 1}}(T_i)}{\deg T_i} = 0$$

où T_i est le polynôme minimal de α_i.
Inversement, si $\alpha_1, \ldots, \alpha_m$ sont les racines d'un facteur T de P, on a la relation

$$\alpha_1 + \cdots + \alpha_m = -\mathrm{coeff}_{z^{\deg T - 1}}(T)$$

Proposition

Soit G le groupe multiplicatif généré par les coefficients constant des facteurs unitaires de $P \in \mathbb{Q}[x]$. Alors pour toute relation multiplicative

$$\alpha_1^{r_1} \cdots \alpha_n^{r_n} = q \in \mathbb{Q}^*$$

il existe $\kappa \in \mathbb{N}^*$ tel que $q^\kappa \in G$

Inversement, pour tout facteur unitaire T de P, et $\alpha_1, \ldots, \alpha_m$ ses racines, on a la relation

$$\alpha_1 \cdots \alpha_m = (-1)^m T(0)$$

On peut réduire toute relation multiplicative à une relation homogène

- En en prenant une puissance pour que $q \in G$
- En la divisant par un produit de relations venant de facteurs de P.

Proposition

Si P avec un groupe de Galois 2-transitif, alors il n'admet pas d'autres relations que les relations triviales

$$\sum_{i=1}^{n} \alpha_i \in \mathbb{Q}, \prod_{i=1}^{n} \alpha_i \in \mathbb{Q}$$

Quitte à faire une translation, on peut supposer que P est à trace nulle
Quite à remplacer P par le polynome dont les racines sont $\alpha_i^n/P(0)$, on peut supposer $P(0) = (-1)^n$.

On considère la trace et la norme sur le corps $\mathbb{Q}(\alpha_i)$.

Le polynome P se factorise dans $\mathbb{Q}(\alpha_i)[x]$ en

$$P = (x - \alpha_i)(x^{n-1} + (-\mathrm{tr} + \alpha_i)x^{n-2} + \cdots - P(0)\alpha_i^{-1})$$

On peut supposer que

- Pour les relations linéaires, P est à trace nulle.
- Pour les relations multiplicatives, que $P(0) = (-1)^n$.

Ainsi, on a

$$\mathrm{tr}_{\mathbb{Q}(\alpha_i)}(\alpha_j) = -\frac{1}{n-1}\alpha_i, \quad \forall j \neq i, \qquad \mathrm{tr}_{\mathbb{Q}(\alpha_i)}(\alpha_i) = \alpha_i$$

$$\frac{\ln \mathrm{N}_{\mathbb{Q}(\alpha_i)}(\alpha_j)}{[\mathbb{L} : \mathbb{K}]} = -\frac{1}{n-1}\ln \alpha_i, \quad \forall j \neq i, \qquad \frac{\ln \mathrm{N}_{\mathbb{Q}(\alpha_i)}(\alpha_i)}{[\mathbb{L} : \mathbb{K}]} = \ln \alpha_i$$

Or si une relation linéaire existe, elle existe aussi sur la trace.

Si une relation multiplicative existe, alors elle existe aussi sur la norme.

Donc si une relation existe, elle doit être dans le noyau d'une matrice de la forme

$$\begin{pmatrix} 1 & -\frac{1}{n-1} & \cdots & -\frac{1}{n-1} \\ -\frac{1}{n-1} & 1 & \cdots & -\frac{1}{n-1} \\ & \cdots & & \\ -\frac{1}{n-1} & \cdots & -\frac{1}{n-1} & 1 \end{pmatrix}$$

La dimension du noyau de cette matrice est toujours 1 $\Rightarrow$ Seules les relations triviales existent.

Lemma

Soit $\mathcal{V} = \bigoplus_{i=1}^{n} \mathbb{Q}.\alpha_i$. *Alors*

$$\varphi : \mathcal{V} \to \mathcal{V}^n, \quad \varphi(\beta) = \left(tr_{\mathbb{Q}(\alpha_1)}(\beta), \ldots, tr_{\mathbb{Q}(\alpha_n)}(\beta)\right)$$

est linéaire, bien définie et injective.
Soit $\tilde{\mathcal{V}} = \left\{\prod_{i=1}^{n} \alpha_i^{n_i},\ n_i \in \mathbb{Z}\right\}$. *Alors*

$$\Phi : \tilde{\mathcal{V}} \to \tilde{\mathcal{V}}^n, \quad \Phi(\beta) = \left(N_{\mathbb{Q}(\alpha_1)}(\beta), \ldots, N_{\mathbb{Q}(\alpha_n)}(\beta)\right)$$

est multiplicative, bien définie et injective.

LinearRelations

1. Factoriser $P = P_1 \cdots P_m \in \mathbb{Q}[x]$.
2. Isoler numériquement les racies $\alpha_1, \ldots, \alpha_n$ de P à précision ϵ. A chaque α_i associer son facteur P_k de P.
3. Soit $M \in M_{n,n}(\mathbb{L})$ Pour chaque α_i
   1. Factoriser $P \in \mathbb{Q}[y]/(P_k(y))[x]$.
   2. Pour chaque facteur T, substituer $y = \alpha_i$ dans T, et chercher les j tes que $T(\alpha_j) = 0$ (à la précision numérique).
   3. S'il y en a plus que le degré de T, augmenter la précision et recommencer.
   4. Pour chaque j, poser $M_{i,j} = -\text{coeff}_{x^{\deg T - 1}}(T)/\deg T$.
4. Remplacer les lignes de M par ses coefficients en y, donnant une matrice $\tilde{M}$.
5. Retourner une base de $\text{Ker}\tilde{M}$.

Exemple 1:
Soit $P = x^3 + x + 1$ et sa factorisation dans $\mathbb{Q}[y]/(P(y))[x]$

$$P = (x - y)(x^2 + yx + y^2 + 1).$$

La matrice M est

$$M = \begin{pmatrix} y & -y/2 & -y/2 \\ -y/2 & y & -y/2 \\ -y/2 & -y/2 & y \end{pmatrix}.$$

L'extraction des coefficients en y donne $\tilde{M}$

$$\tilde{M} = \begin{pmatrix} 1 & -1/2 & -1/2 \\ -1/2 & 1 & -1/2 \\ -1/2 & -1/2 & 1 \end{pmatrix}.$$

Le noyau est Span$(1, 1, 1)$, la relation triviale.

Exemple 2:
Soit $P = x^4 + x^2 + 2$ et sa factorisation dans $\mathbb{Q}[y]/(P(y))[x]$

$$P = (x - y)(x + y)(x^2 + y^2 + 1).$$

a matrice M est

$$M = \begin{pmatrix} y & -y & 0 & 0 \\ -y & y & 0 & 0 \\ 0 & 0 & y & -y \\ 0 & 0 & -y & y \end{pmatrix}.$$

L'extraction des coefficients en y donne $\tilde{M}$

$$\tilde{M} = \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}.$$

Le noyau est $\mathrm{Span}((1,1,0,0),(0,0,1,1))$, soit deux relations.

Exemple 3:
Soit $P = x^3 - 3x - 1$ et sa factorisation dans $\mathbb{Q}[y]/(P(y))[x]$

$$P = (x - y)(x + y^2 - 2)(x - y^2 + y + 2),$$

On note $\alpha_1, \alpha_2, \alpha_3$ les racines de P dans cet ordre. La matrice M est

$$M = \begin{pmatrix} y & -y^2+2 & y^2-y-2 \\ y^2-y-2 & y & -y^2+2 \\ -y^2+2 & y^2-y-2 & y \end{pmatrix}.$$

L'extraction des coefficients en y donne $\tilde{M}$

$$\tilde{M}^\intercal = \begin{pmatrix} 0 & 1 & 0 & -2 & -1 & 1 & 2 & 0 & -1 \\ 2 & 0 & -1 & 0 & 1 & 0 & -2 & -1 & 1 \\ -2 & -1 & 1 & 2 & 0 & -1 & 0 & 1 & 0 \end{pmatrix}.$$

Son noyau est $\mathrm{Span}(1, 1, 1)$, la relation triviale.

MultiplicativeRelations

1. Factoriser $P = P_1 \cdots P_m \in \mathbb{Q}[x]$.
2. Isoler numériquement les racines $\alpha_1, \ldots, \alpha_n$ à précision ϵ. A chaque racine α_i associer son facteur P_k de P.
3. Soit $M \in M_{n,n}(\mathbb{L})$ Pour chaque α_i
   1. Factoriser $P \in \mathbb{Q}[y]/(P_k(y))[x]$.
   2. Pour chaque facteur T, substituer $y = \alpha_i$ dans T, et chercher les j tes que $T(\alpha_j) = 0$ (à la précision numérique).
   3. S'il y en a plus que le degré de T, augmenter la précision et recommencer.
   4. Pour chaque j, poser $M_{i,j} = \ln T(0)/\deg T$.
4. Pour chaque ligne M, calculer les relations linéaires sur $\mathbb{Q}$ entre les log des éléments et $2i\pi$, dans le corps $\mathbb{Q}[y]/(P_k(y))$ par l'algorithme de Ge.

1. En oubliant le coefficient pour $2i\pi$, intersecter ces espaces pour obtenir un $\mathbb{Q}$-espace vectoriel $\mathcal{W}$.
2. Considérer une base du réseau $\mathcal{W} \cap \mathbb{Z}^n$, et pour chaque élément $(r_1, \ldots, r_n)$ de la base, calculer

$$\frac{1}{2i\pi} \sum r_i \ln \alpha_i$$

et reconnaitre un rational ℓ avec dénominateur $\leq 2n!^2$. Augmenter la précision si nécéssaire et recommencer. Etendre l'élement $(r_1, \ldots, r_n, \ell)$.
3. Rendre le sous réseau généré par ces éléments tels que le dernier coefficient soit dans $\mathbb{Z}$.

Proposition

Les polynomes irréductibles primitifs de degré ≤ 15 *admettant au moins une relation non triviale ont pour groupe de Galois*

- $G \simeq C_3^2 \propto C_4 \subset S_9$, $\dim(\mathcal{L}) \leq 5$
- $G \simeq A_5 \subset S_{10}$, $\dim(\mathcal{L}) \leq 6$
- $G \simeq S_5 \subset S_{10}$, $\dim(\mathcal{L}) \leq 6$
- $G \simeq A_6 \subset S_{15}$, $\dim(\mathcal{L}) \leq 10$
- $G \simeq S_6 \subset S_{15}$, $\dim(\mathcal{L}) \leq 10$

- $P = x^9 - 63x^7 + 63x^6 + 1026x^5 - 864x^4 - 6453x^3 + 2835x^2 + 14094x + 351$, 5 relations en $1.45s$
- $P = x^{10} - x^7 + 6x^6 + 33x^5 - x^4 - 8x^3 + 5x^2 + 25x - 7$, 6 relations en $4s$
- $P = x^{10} - 3x^6 - 33x^5 - 4x^2 + 12x - 9$, 6 relations en $2.9s$
- $P = x^{15} - 96x^{13} - 152x^{12} + 3330x^{11} + 8304x^{10} - 37166x^9 - 157896x^8 + 102105x^7 + 3373784x^6 + 2746494x^5 - 23345328x^4 - 62147359x^3 + 23529600x^2 + 233036112x + 267704384$, 10 relations en $35s$
- For $P = x^{15} - 10x^{10} - 26x^9 - 12x^5 + 18x^4 - 27x^3 - 1$, 10 relations en $39s$

- $P = x^9 - 9x^8 - 225x^7 - 597x^6 + 801x^5 + 1719x^4 - 807x^3 - 387x^2 + 45x - 1$, 5 relations en $2.1s$
- $P = x^{10} - \frac{80}{9}x^9 + \frac{3362}{81}x^8 - \frac{28517}{243}x^7 + \frac{1361204}{6561}x^6 - \frac{14137493}{59049}x^5 + \frac{100662985}{531441}x^4 - \frac{687872}{6561}x^3 + \frac{28595}{729}x^2 - \frac{251}{27}x + 1$, 6 relations en $12.3s$
- $P = x^{10} - x^7 + x^6 - 2x^5 - x + 1$, 6 relations en $5s$
- $P = x^{15} - 5x^{14} + 30x^{13} - 169x^{12} + 682x^{11} - 1270x^{10} + 726x^9 + 20x^8 - 103x^7 + 5x^6 + 132x^5 - 79x^4 + 33x^3 - 19x^2 + 6x - 1$, 10 relations en $460s$
- $P = x^{15} - x^{12} - 2x^{10} - 2x^9 + x^7 + 2x^6 + x^5 + x^4 + x^3 - 1$, 10 relations en $116s$

Soit l'intégrale hyperelliptique

$$I = \int \frac{P(x)}{Q(x)\sqrt{S(x)}}dx$$

où $P, Q, S \in \mathbb{Q}[x]$, avec S sans facteurs carrés, et de degré impair.

On souhaite essayer de l'écrire sous forme élémentaire

$$I(x) = G_0(x) + \sum \lambda_i \ln G_i(x), \quad G_i \in \mathbb{C}(x, \sqrt{S}).$$

Definition

On dit que I est

- *élémentaire si I peut s'écrire*

$$I(x) = G_0(x) + \sum_i \lambda_i \ln G_i(x), \ G_i \in \overline{\mathbb{Q}}(x, \sqrt{S}).$$

- *réduite si Q est sans facteur carrés, premier avec S et* $\deg P < \deg Q + \frac{1}{2}\deg S - 1$
- *de première espèce si I est réduit et Q constant.*
- *de torsion si I est la somme d'une intégrale élémentaire et d'une intégrale de première espèce.*

La partie algébrique G_0 s'obtient rapidement par réduction de Hermite.

Elle existe toujours si I est élémentaire.

Les résidus de I peuvent se calculer avec la formule

$$R(\lambda) = \text{squarefree}(\text{resultant}(P^2 - \lambda^2 Q'^2, Q))$$

Proposition (See [?])

We can build a set Soit α un nombre algébrique. On peut construire un ensemble $\mathcal{S}_\alpha$ d'intégrales $\int P_j/(Q_j\sqrt{S})dx$ telles que $Q_j \mid Q$ et $\forall p \in \mathcal{C}$

$$res_p \frac{P_j}{Q_j\sqrt{S}} = d_j coeff_{\alpha^j} tr_{\mathbb{Q}(\alpha)} \left(res_p \frac{P}{Q\sqrt{S}} \right)$$

avec $d_j \in \mathbb{N}^*$, tous les résidus sont dans $\mathbb{Z}$. De plus, si $\int P/(Q\sqrt{S})dx$ est réduit et de torsion, alors les intégrales $\mathcal{S}_\alpha$ sont de torsion.

Proposition

Une intégrale hyperelliptique réduite peut toujours s'écrire comme une combination linéaire des intégrales $\mathcal{S}_\alpha$, $\forall \alpha,\ R(\alpha) = 0$ et d'une intégrale de première espèce.

Proposition

Une intégrale hyperelliptique réduite peut toujours s'écrire comme une combination linéaire dans $\mathbb{Q}$ d'une intégrale de première espèce et des intégrales

$$Y_{i,j,k} = \sum_{R_i(\alpha)=0} \alpha^k T_{i,j}(\alpha), \quad k = 0 \dots \deg R_i - 1$$

où $R_i \mid R \in \mathbb{Q}[\lambda]$, et $T_{i,j}(\alpha)$ sont les intégrales $\mathcal{S}_\alpha$, $R_i(\alpha) = 0$

ElementaryIntegrate

1. Calculer la réduction de Hermite de I. S'il y en a une, noter $I = H + \int \tilde{P}/(\tilde{Q}\sqrt{S})$ et continuer avec l'expression réduite
2. Calculer et factoriser le polynome des résidues $R = R_1 \cdots R_\ell$, puis les intégrales $\mathcal{S}_\alpha$ avec $R_i(\alpha) = 0$.
3. Pour chaque intégrale, tester si elle est de torsion. Si toutes le sont, continuer.
4. Calculer la matrice $\tilde{M}$ pour R.
5. Enlever le maximum de lignes de $\tilde{M}$ sans réduire son rang, et chercher une combinaison linéaire de ses lignes donnant les racines de R.
6. Retourner H plus la même combinaison linéaire appliquée aux intégrales $\mathcal{S}_\alpha$ avec $R(\alpha) = 0$.

Theorem

Soit $I = \int P/(Q\sqrt{S})$ une intégrale hyperelliptique avec S sans facteurs carrés de degré impair. ElementaryIntegrate calcule I sous forme élémentaire si et seulement si c'est possible, et à genre fixé, en temps probabiliste polynomial en $n = \max(\deg P, \deg Q, \deg S)$ et h la hauteur des coefficients.

En ignorant le cout des factorisations la complexité de l'algorithme est $O(n^{\omega+2g+1} h^{g+1})$