Diagonales de fractions rationnelles bivariées

Les algorithmes du chapitre précédent s'appliquent presque directement pour calculer un polynôme annulant une diagonale de fraction rationnelle bivariée. Le point clé est le fait qu'elles ont une représentation sous forme d'intégrale de fraction rationnelle. Nous avons déjà évoqué cela sommairement dans l'introduction et dans le premier chapitre. Dans la première section de ce chapitre, nous allons revenir sur la définition et les propriétés de base des diagonales. La deuxième section présente une solution algorithmique au calcul d'un polynôme annulateur. La méthode est très similaire à l'algorithme PolIntFRat à cela près que l'on peut apporter une optimisation supplémentaire en utilisant la forme particulière que prennent les représentations intégrales des diagonales. Enfin, on étudiera en fin de chapitre le polynôme minimal de la diagonale d'une fraction rationnelle F dans le cas générique et montrerons en particulier que son degré est génériquement exponentiel en le bidegré de F.

4.1 Généralités

Définition 81. Soit $F \in \mathbf{k}(x, y)$ une fraction rationnelle régulière en $(0,0)$. On peut alors développer F dans $\mathbf{k}[[x, y]]$:

$$F(x, y) = \sum_{i,j \geqslant 0} a_{i,j} x^i y^j,$$

avec $a_{i,j} \in \mathbf{k}$ pour tous i et j. On définit alors la *diagonale* de F, notée ΔF, comme étant la série univariée

$$\Delta F(t) = \sum_{i \geqslant 0} a_{i,i} t^i \in \mathbf{k}[[t]].$$

Commençons par une première remarque très simple mais fondamentale dans les calculs de diagonales.

Lemme 82. *Soit* $\mathrm{F} \in \mathbf{k}(x,y)$ *une fraction rationnelle régulière en* $(0,0)$. *Alors*

$$\Delta\mathrm{F}(t) = [y^{-1}]\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right).$$

Démonstration. Écrivons le développement de F en série entière :

$$\mathrm{F}(x,y) = \sum_{i,j\geqslant 0} a_{i,j}x^i y^j,$$

avec $a_{i,j} \in \mathbf{k}$ pour tous i et j. Alors le changement de variable $x \to t/y$ donne

$$\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right) = \sum_{i,j\geqslant 0} a_{i,j}t^i y^{j-i-1}.$$

Ceci est une égalité entre éléments de $\mathbf{k}((y))((t))$, on peut donc en extraire le coefficient de $[y^{-1}]$ au sens de la définition 7 :

$$[y^{-1}]\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right) = \sum_{i\geqslant 0} a_{i,i}t^i = \Delta\mathrm{F}(t).$$

□

Remarque 83. *Cette formule peut aussi être lue dans l'autre sens. En effet, supposons que l'on a écrit une série* $f \in \mathbf{k}[[t]]$

$$f(t) = [y^{-1}]\mathrm{F}(t,y),$$

pour une certaine fraction rationnelle $\mathrm{F} \in \mathbf{k}(t,y)$. *Alors, le lemme 82 montre que*

$$f(t) = \Delta\left\{y\mathrm{F}(xy,y)\right\},$$

pour peu que la fraction rationnelle $y\mathrm{F}(xy,y)$ *soit régulière en* $(0,0)$.

Proposition 84. *Soit* $\mathrm{F} \in \mathbf{k}(x,y)$ *une fraction rationnelle. Notons* $y_1, y_2, \ldots, y_c$ *les petits pôles de la fraction*

$$\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right)$$

en y.

Alors

$$\Delta\mathrm{F}(t) = \sum_{i=1}^{c} \mathrm{Res}\left(\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right), y_i\right).$$

Ce résultat est une généralisation à un corps de caractéristique 0 quelconque d'un résultat de Furstenberg [1].

1. FURSTENBERG, "Algebraic Functions over Finite Fields".

Démonstration. On part de l'expression de ΔF comme résidu (lemme 82) :

$$\Delta F(t) = [y^{-1}]\frac{1}{y}F\left(\frac{t}{y}, y\right).$$

On calcule alors le membre droit à l'aide de la formule des résidus (proposition 8 p. 29), ce qui donne le résultat escompté.

□

Corollaire 85. *Soit* $F \in \mathbf{k}(x,y)$ *une fraction rationnelle bivariée. Alors la diagonale de* F *est une série univariée algébrique.*

Démonstration. C'est un cas particulier du corollaire 9 p. 30. □

Il est naturel de se demander si la réciproque est vraie : une série algébrique étant donnée, peut-on toujours trouver une fraction rationnelle bivariée dont elle est la diagonale ? La proposition suivante, due à Furstenberg [2], montre que c'est en effet le cas si l'on considère une série algébrique qui satisfait une bonne condition de séparation par rapport à ses conjuguées.

Proposition 86. *Soit* $P \in \mathbf{k}[t][y]$ *un polynôme tel que*

$$P(0,0) = 0, \quad \textit{et} \quad \partial_y P(0,0) \neq 0.$$

Soit f *l'unique racine de* P *dans* $\mathbf{k}[[t]]$ *telle que* $f(0) = 0$. *Alors la fraction rationnelle*

$$F(x,y) = y^2 \partial_y P(xy, y)/P(xy, y)$$

est régulière en $(0,0)$ *et*

$$f = \Delta F.$$

Démonstration. Si l'on note $d = \deg_y P$ et $f_1 = f, f_2, \ldots, f_d$ les d racines de P dans $\overline{\mathbf{k}(x)}$, on a

$$\frac{\partial_y P(x,y)}{P(x,y)} = \sum_{i=1}^{d} \frac{1}{y - f_i}.$$

On déduit que

$$y\frac{\partial_y P(x,y)}{P(x,y)} = \sum_{i=1}^{d} \frac{y}{y - f_i} = d + \sum_{i=1}^{d} \frac{f_i}{y - f_i}.$$

Mais par la proposition 122 de l'annexe A.3, l'hypothèse de séparation des racines de P implique que f est l'unique petit pôle de $y\partial_y P/P$, et le résidu de cette fraction en f vaut f. La proposition 8 donne alors

$$[y^{-1}]\left\{\frac{y\partial_y P(x,y)}{P(x,y)}\right\} = f.$$

Le résultat attendu découle ensuite de la remarque 83. Il faut simplement s'assurer que la fraction F est régulière en $(0,0)$. Mais ceci découle des hypothèses faites sur P. En effet, comme $P(0,0) = 0$, $P(xy,y)/y$ est un polynôme dont on vérifie facilement que la valeur en $(0,0)$ n'est autre que $\partial_y P(0,0)$. □

2. Ibid., Prop. 2.

Bien évidemment, ce lemme ne s'applique pas pour une série algébrique f générale. Mais Mechik[3] a montré qu'il est toujours possible de se ramener à la situation du lemme en développant f assez loin pour qu'elle se sépare de ses conjuguées. Plus précisément, il a prouvé que la queue du développement de f à l'ordre α est solution d'un polynôme satisfaisant les hypothèses du lemme, pour peu que l'on choisisse α assez grand. Cependant, sa méthode ne donne aucune information sur une valeur suffisante de α. Adamczewski et Bell[4] ont établi une version quantitative de ce résultat dans un cadre bien plus général, qui donne accès à une estimation d'un ordre de développement α suffisant. Le lemme suivant est une spécialisation de leur théorème au cas qui nous intéresse. J'en redonne la preuve en détail, d'une part parce qu'elle peut s'exprimer en des termes plus simples dans ce cas particulier, et également pour rectifier une légère imprécision dans la preuve d'Adamczewski et Bell.

Lemme 87. *Soit* $\mathrm{P} \in \mathbf{k}(x)[y]$ *un polynôme sans carré tel que* $\mathrm{P}(0,0) = 0$, $\partial_y \mathrm{P}(0,0) = 0$ *et admettant une racine* $f \in \mathbf{k}[[x]]$ *telle que* $f(0) = 0$. *On note*

$$\alpha = \mathrm{val}_x \, \text{Résultant}_y(\mathrm{P}, \partial_y \mathrm{P}),$$

et on écrit

$$f(x) = r(x) + x^\alpha g(x),$$

où $r(x) = f \bmod x^{\alpha+1}$.

Alors $g(x)$ *est annulée par un polynôme* $\mathrm{Q} \in \mathbf{k}[x,y]$ *tel que*

$$\mathrm{Q}(0,0) = 0, \quad \textit{et} \quad \partial_y \mathrm{Q}(0,0) \neq 0.$$

Démonstration. On pose $\mathrm{R} = \text{Résultant}_y(\mathrm{P}, \partial_y \mathrm{P})$. De par sa définition, la série g est annulée par le polynôme $\mathrm{P}(x, r(x) + x^\alpha y)$. Par la formule de Taylor, on peut récrire ce polynôme :

$$\mathrm{P}(x, r + x^\alpha y) = \mathrm{P}(x,r) + x^\alpha y \partial_y \mathrm{P}(x,r) + x^{2\alpha} y^2 \mathrm{H}(x,y), \tag{4.1}$$

pour un certain polynôme $\mathrm{H} \in \mathbf{k}[x,y]$. En évaluant cette égalité en g, on obtient

$$\mathrm{P}(x,r) = -x^\alpha g \partial_y \mathrm{P}(x,r) - x^{2\alpha} g^2 \mathrm{H}(x,r). \tag{4.2}$$

Comme $g(0) = 0$, ceci implique en particulier que

$$\mathrm{val}_x \, \mathrm{P}(x,r) > \alpha.$$

Maintenant, les propriétés élémentaires du résultant font qu'il existe des polynômes $\mathrm{U}, \mathrm{V} \in \mathbf{k}[x,y]$ tels que

$$\mathrm{R}(x) = \mathrm{U}(x,y)\mathrm{P}(x,y) + \mathrm{V}(x,y)\partial_y \mathrm{P}(x,y)$$

3. MECHIK, "Sur la constante d'Eisenstein".
4. ADAMCZEWSKI et BELL, "Diagonalization and rationalization of algebraic Laurent series".

(voir la proposition 129 de l'annexe A.5). Comme $\mathrm{val}_x \mathrm{R} = \alpha$ et $\mathrm{val}_x \mathrm{P} > \alpha$, cette égalité implique que $\mathrm{val}_x(\mathrm{V}(x,r)\partial_y \mathrm{P}(x,r)) = \alpha$, et donc

$$\mathrm{val}_x \partial_y \mathrm{P}(x,r) \leqslant \alpha.$$

(À noter que cette inégalité peut être stricte, c'est là l'imprécision dans la preuve originelle.) Posons $\beta = \mathrm{val}_x \partial_y \mathrm{P}(x,r)$. Alors en réinspectant l'égalité (4.2), on constate que

$$\mathrm{val}_x \mathrm{P}(x,r) \geqslant \min(\alpha+\beta+1, 2\alpha+2) = \alpha+\beta+1.$$

Ceci et l'égalité (4.1) montrent que le polynôme $\mathrm{P}(x, r+x^\alpha y)$ est divisible par $x^{\alpha+\beta}$. On pose donc

$$\mathrm{Q}(x,y) = \frac{\mathrm{P}(x, r+x^\alpha y)}{x^{\alpha+\beta}} \in \mathbf{k}[x,y].$$

Par construction, on a $\mathrm{Q}(x, g(x)) = 0$. De plus, l'égalité (4.1) se récrit

$$\mathrm{Q}(x,y) = \frac{\mathrm{P}(x,r)}{x^{\alpha+\beta}} + y\frac{\partial_y \mathrm{P}(x,r)}{x^\beta} + x^{\alpha-\beta}y^2 \mathrm{H}(x,y).$$

En évaluant cette égalité en $(0,0)$, on obtient $\mathrm{Q}(0,0) = 0$ puisque $\mathrm{val}_x(\mathrm{P}(x,r)/x^{\alpha+\beta}) \geqslant 1$. En la dérivant et en évaluant en $(0,0)$, on obtient

$$\partial_y \mathrm{Q}(0,0) = \frac{\partial_y \mathrm{P}(x,r)}{x^\beta}(0,0) \neq 0$$

par définition de β. □

Remarque 88. *Si l'on note (d_x, d_y) le bidgré de* P*, la proposition 130 donne une majoration de l'entier α du lemme :*

$$\alpha = \mathrm{val}_x \mathrm{Résultant}_y(\mathrm{P}, \partial_y \mathrm{P}) \leqslant \deg_x \mathrm{Résultant}_y(\mathrm{P}, \partial_y \mathrm{P}) \leqslant 2d_x d_y.$$

Grâce aux deux lemmes précédents, on obtient la réciproque du théorème de Furstenberg.

Proposition 89. *Soit $\mathrm{P} \in \mathbf{k}[t,y]$ un polynôme admettant une série $f \in \mathbf{k}[[t]]$ comme solution.*

Alors il existe une fraction rationnelle $\mathrm{F} \in \mathbf{k}(x,y)$ régulière en $(0,0)$ telle que

$$f = \Delta \mathrm{F}.$$

Démonstration. On peut sans perte de généralité supposer que P est sans carré, quitte à le remplacer par un facteur sans carré annulant f. De plus, on peut supposer que $\mathrm{P}(0,0) = 0$ (il suffit pour cela que $f(0) = 0$). En effet, si l'on écrit $f(x) = f(0) + x\tilde{f}(x)$, on remarque que si $\tilde{f} = \Delta\tilde{\mathrm{F}}$, alors $f = \Delta\{f(0) + \tilde{\mathrm{F}}\}$. Il suffit donc de montrer la proposition pour $\tilde{f}$ qui vérifie $\tilde{f}(0) = 0$.

Maintenant, si de plus $\partial_y \mathrm{P}(0,0) \neq 0$, on peut conclure directement par le lemme 86. Si au contraire $\partial_y \mathrm{P}(0,0) = 0$, on utilise le lemme 87 pour écrire

$$f(x) = r(x) + x^\alpha g(x),$$

de telle sorte que g est annulée par un polynôme Q satisfaisant les hypothèses du lemme 86. g est alors la diagonale de la fraction

$$\mathrm{G}(x,y) = y^2 \frac{\partial_y \mathrm{Q}(xy,y)}{\mathrm{Q}(xy,y)}.$$

On en déduit que f est la diagonale de la fraction rationnelle

$$\mathrm{F}(x,y) = r(xy) + (xy)^{\alpha}\mathrm{G}(x,y).$$

□

4.2 Polynôme annulateur pour une diagonale de fraction rationnelle bivariée

Jusqu'à la fin du chapitre, on se donne une fraction rationnelle $\mathrm{F} \in \mathbf{k}(x,y)$ régulière en $(0,0)$. On a vu que la diagonale de F est une série algébrique (corollaire 85). Il est alors naturel de chercher à calculer un polynôme annulateur de $\Delta\mathrm{F}$. Le point de départ est la formule

$$\Delta\mathrm{F}(t) = [y^{-1}]\frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right).$$

On peut donc appliquer directement l'algorithme PolIntFRat à la fraction rationnelle $\mathrm{G}(t,y) = \mathrm{F}(t/y,y)/y$ pour obtenir un polynôme annulateur. Cependant, on peut faire mieux, en prenant en compte la structure particulière de la fraction G qui et obtenue à partir du changement de variables $x \mapsto t/y$ dans F. Dans le paragraphe suivant, on va prédire la forme de G, ce qui permet dans certains cas de prédire une factorisation du polynôme qui serait calculé par l'algorithme PolIntFRat. Ceci conduit à une variante de cet algorithme qui calcule directement le facteur qui nous intéresse.

4.2.1 Effet du changement de variables

Pour suivre l'impact du changement de variables $x \mapsto t/y$ sur un polynôme, on introduit la notion de degré diagonal.

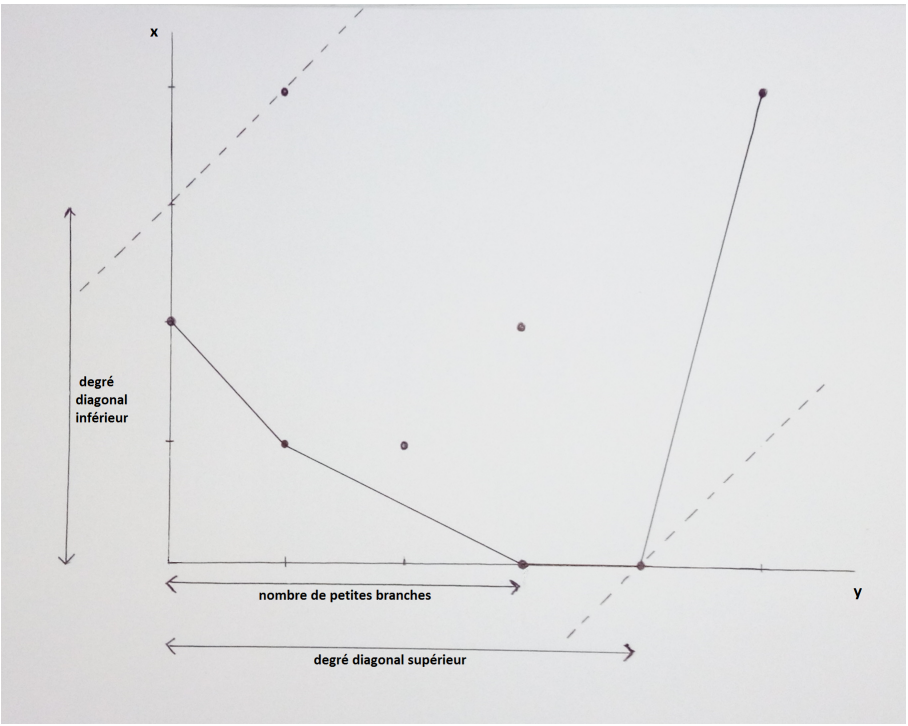
Définition 90. Soit $\mathrm{P} \in \mathbf{k}[x,y]$ un polynôme, que l'on écrit

$$\mathrm{P}(x,y) = \sum_{i,j} a_{i,j} x^i y^j.$$

On définit le *degré diagonal inférieur* et le *degré diagonal supérieur* de P, respectivement notés $\mathrm{ddeg}^-(\mathrm{P})$ et $\mathrm{ddeg}^+(\mathrm{P})$ par

$$\begin{aligned} \mathrm{ddeg}^-(\mathrm{P}) &= \sup\{i-j \mid a_{i,j} \neq 0\} \\ \mathrm{ddeg}^+(\mathrm{P}) &= \sup\{j-i \mid a_{i,j} \neq 0\} \end{aligned} \tag{4.3}$$

Plus concrètement, comme illustré dans le dessin ci-dessous, le degré diagonal inférieur d'un polynôme peut se lire sur son polygone de Newton de la façon suivante : on fait descendre une droite de pente 1 depuis l'infini jusqu'à rencontrer un point du support des coefficients du polynôme. Le degré diagonal inférieur est l'ordonnée à l'origine de cette droite. Le degré diagonal supérieur est obtenu en faisant monter une droite de pente 1 depuis l'infini jusqu'à rencontrer le support du polynôme, et en lisant l'abscisse du point d'intersection de cette droite avec l'axe horizontal.



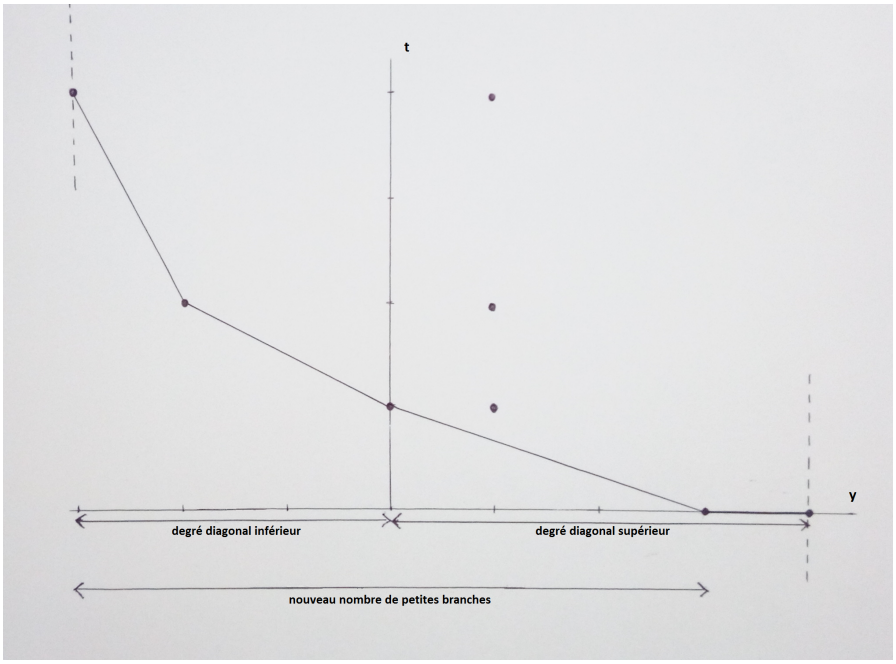
Lecture du degré diagonal d'un polynôme sur son polygone de Newton

La proposition suivante rassemble les propriétés importantes du degré diagonal dans notre contexte. (On rappelle que la notation $(\cdot)^\star$ désigne la prise de partie sans carré.)

Lemme 91. *Pour tous polynômes* $P, Q \in \mathbb{K}[x,y]$,

1. $\mathrm{ddeg}^-(P) \leqslant \deg_x P$ *et* $\mathrm{ddeg}^+(P) \leqslant \deg_y P$;
2. $\mathrm{ddeg}^\pm(PQ) = \mathrm{ddeg}^\pm(P) + \mathrm{ddeg}^\pm(Q)$;
3. *il existe un polynôme* $\tilde{P} \in \mathbb{K}[t,y]$ *tel que* $P(t/y, y) = y^{-\mathrm{ddeg}^-(P)}\tilde{P}(t,y)$, *avec* $\tilde{P}(t,0) \neq 0$ *et*
$$\mathrm{bideg}_{t,y}(\tilde{P}) = (\deg_x P, \mathrm{ddeg}^-(P) + \mathrm{ddeg}^+(P)) ;$$
4. $\mathrm{bideg}_{t,y}((\tilde{P})^\star) = (\deg_x P^\star, \mathrm{ddeg}^-(P^\star) + \mathrm{ddeg}^+(P^\star))$.

Avant de démontrer ce lemme, illustrons ce résultat en appliquant le changement de variable $x \mapsto t/y$ au polynôme dont le polygone de Newton était dessiné dans l'illustration précédente. Sur l'image ci-dessous, on constate notamment que le point de coordonnées (i, j) est envoyé sur le point $(i, j-i)$. En particulier, le degré diagonal inférieur et supérieur donnent la valuation et le degré en y du polynôme de Laurent obtenu par ce changement de variable.



Polygone de Newton après le changement de variable $x \mapsto t/y$

Démonstration. Le *(1)* est immédiat. Les quantités $\mathrm{ddeg}^-(\mathrm{P})$ et $\mathrm{ddeg}^+(\mathrm{P})$ ne sont autres que $-\mathrm{val}_y \mathrm{P}(t/y, y)$ et $\deg_y \mathrm{P}(t/y, y)$, ce qui rend limpides le *(2)* et le *(3)*. De là, on obtient l'égalité $\widetilde{\mathrm{PQ}} = \tilde{\mathrm{P}}\tilde{\mathrm{Q}}$ pour P et Q quelconques, d'où $(\tilde{\mathrm{P}})^\star = \widetilde{\mathrm{P}^\star}$. Le *(4)* est alors une conséquence de *(1)* et *(3)*. □

Par ailleurs, pour utiliser l'algorithme SommeCompPure de la section 3.2, on a également besoin de connaître le nombre de petites branches du dénominateur après le changement de variables. Comme on l'a déjà rappelé, le nombre de petites branches d'un polynôme est exactement la largeur totale des pentes strictement négatives dans son polygone de Newton. Dans le lemme suivant, on note Nsmall(P) le nombre de petites branches d'un polynôme P.

Lemme 92. *Soit* $\mathrm{P} \in \mathbf{k}[x, y]$ *un polynôme tel que* $\mathrm{P}(0, y) \neq 0$. *Alors*

$$\mathrm{Nsmall}\left(y^{\mathrm{ddeg}^-(\mathrm{P})}\mathrm{P}(t/y, y)\right) = \mathrm{Nsmall}(\mathrm{P}^\star) + \mathrm{ddeg}^-(\mathrm{P}^\star).$$

Démonstration. Écrivons $\mathrm{P}(x, y) = \sum_{i,j} a_{i,j} x^i y^j$. On a déjà vu que le changement de variables $x \mapsto t/y$ change les coordonnées du point correspondant à $a_{i,j}$ en

$(i, j-i)$. Cette transformation envoie les sommets du polygone de Newton de P sur les sommets du polygone de Newton du polynôme de Laurent $\mathrm{P}(t/y, y)$. De plus, l'hypothèse $\mathrm{P}(0, y) \neq 0$ fait que le point le plus à droite de la partie de pente strictement négative du polygone de Newton est invariant par la transformation (puisque sur l'axe des abscisses). Ainsi, la largeur des pentes négatives est augmentée exactement de $\mathrm{ddeg}^-(\mathrm{P})$ (voir le dessin ci-dessus). La multiplication par $y^{\mathrm{ddeg}^-(\mathrm{P})}$, ne fait qu'une translation du polygone, le résultat est donc démontré. □

On peut maintenant utiliser les deux lemmes précédents pour prévoir la forme de la fraction rationnelle $\mathrm{G}(t, y)$.

Proposition 93. *Soient* $\mathrm{A}, \mathrm{B} \in \mathbf{k}[x, y]_{d_x, d_y}$ *deux polynômes premiers entre eux et tels que* $\mathrm{B}(0,0) \neq 0$. *Soit* $(d_x^\star, d_y^\star)$ *une borne sur le bidegré de la partie sans carré de* B. *Notons* $\mathrm{F} = \mathrm{A}/\mathrm{B}$ *et*

$$\mathrm{G}(t, y) = \frac{1}{y}\mathrm{F}\left(\frac{t}{y}, y\right).$$

Alors il existe des polynômes $\mathrm{P}, \mathrm{Q} \in \mathbf{k}[t, y]$ *tels que*

$$\mathrm{G}(t, y) = y^\alpha \frac{\mathrm{P}(t, y)}{\mathrm{Q}(t, y)},$$

où

$$\begin{gathered} \alpha = \mathrm{ddeg}^-(\mathrm{B}) - \mathrm{ddeg}^-(\mathrm{A}) - 1, \qquad (4.4) \\ \mathrm{bideg}\,\mathrm{P} \leqslant (d_x, \mathrm{ddeg}^-(\mathrm{A}) + \mathrm{ddeg}^+(\mathrm{A})), \quad \mathrm{bideg}\,\mathrm{Q} \leqslant (d_x, \mathrm{ddeg}^-(\mathrm{B}) + \mathrm{ddeg}^+(\mathrm{B})), \\ \mathrm{bideg}\,\mathrm{Q}^\star = (d_x^\star, \mathrm{ddeg}^-(\mathrm{B}^\star) + \mathrm{ddeg}^+(\mathrm{B}^\star)), \\ \mathrm{Nsmall}(\mathrm{Q}) = \mathrm{ddeg}^-(\mathrm{B}^\star). \end{gathered}$$

Démonstration. C'est une application directe des lemmes 91 et 92, en prenant pour P et Q les polynômes $\tilde{\mathrm{A}}$ et $\tilde{\mathrm{B}}$. Pour le nombre de petites branches, on utilise en plus le fait que comme $\mathrm{B}(0,0) \neq 0$, $\mathrm{Nsmall}(\mathrm{B}^\star) = 0$ (son polygone de Newton n'a que des pentes positives). □

4.2.2 Algorithme

On garde les mêmes notations que dans la proposition précédente, et on revient au calcul d'un polynôme annulateur pour $\Delta\mathrm{F}$. Il y a une légère différence entre les cas $\alpha \geqslant 0$ et $\alpha < 0$: dans le second cas le dénominateur admet 0 comme petite branche supplémentaire. Notons $r \in \mathbf{k}(t)$ le résidu de G en 0 si $\alpha < 0$, et $r = 0$ si $\alpha \geqslant 0$. Alors la formule de la proposition 84 se récrit

$$\Delta\mathrm{F}(t) = r(t) + \tilde{f}(t),$$

où, en notant $c = \mathrm{Nsmall}(\mathrm{Q})$ et $y_1, y_2, \ldots, y_c$ les petites branches de Q,

$$\tilde{f}(t) = \sum_{i=1}^{c} \mathrm{Res}\left(\mathrm{G}, y_i\right).$$

Algorithme **PolynômeDiagonale**(A/B)

Entrée Deux polynômes $A, B \in \mathbf{k}[x, y]$, avec $B(0,0) \neq 0$

Sortie Un polynôme $\Phi \in \mathbf{k}[t, y]$ tel que $\Phi(t, \Delta\{A/B\}) = 0$

$P, Q, \alpha \leftarrow y^{\mathrm{ddeg}^-(A)} A(\frac{t}{y}, y),\ y^{\mathrm{ddeg}^-(B)} B(\frac{t}{y}, y),\ \mathrm{ddeg}^-(B) - \mathrm{ddeg}^-(A) - 1$;
si $\alpha < 0$ **alors**
  $r \leftarrow$ **PolynômeRésidus**$(P / y^{-\alpha} Q, y)$;
  $R \leftarrow$ **PolynômeRésidus**$(P / y^{-\alpha} Q, Q)$;
sinon
  $R \leftarrow$ **PolynômeRésidus**$(y^{\alpha} P / Q, Q)$;
$c \leftarrow$ nombre de petites branches de Q ;
$\Phi(t, y) \leftarrow \mathrm{numer}($**SommeCompPure**$(R, c))$;
si $\alpha < 0$ **alors**
  $\Phi(t, y) \leftarrow \mathrm{numer}(\Phi(t, y - r))$;
renvoyer $\Phi(t, y)$

Algorithme 9: Polynôme annulant la diagonale d'une fraction rationnelle. La notation ddeg est définie dans l'équation (4.3) p. 84

Ainsi, pour obtenir un polynôme Φ annulant ΔF, on commence par calculer un polynôme R annulant les $\mathrm{Res}(G, y_i)$ en appliquant l'algorithme PolynômeRésidus p. 67 à $((y^{\alpha} P)/Q, Q)$ si $\alpha \geqslant 0$, et à $(P/y^{-\alpha} Q), Q)$ dans le cas contraire. On obtient ensuite un polynôme $\tilde{\Phi}$ annulant $\tilde{f}$ en appliquant l'algorithme SommeCompPure à (R, c). On en déduit que le polynôme $\Phi(t, y) = \tilde{\Phi}(t, y - r(t))$ annule ΔF.

Cette méthode est implémentée par l'algorithme PolynômeDiagonale (algorithme 9).

Exemple 94. Soit d un entier positif, et soit $F_d \in \mathbb{Q}(x, y)$ la fraction rationnelle définie par

$$F_d(x, y) = \frac{1}{(1 - x - y)^{d+1}}.$$

Sur cet exemple simple, on peut calculer explicitement la diagonale par un développement direct :

$$\Delta F_d(t) = \sum_{n \geqslant 0} \binom{2n + d}{n} \binom{n + d}{d} t^n.$$

D'après le lemme 82 et le corollaire 85, c'est une série algébrique qui est égale à la somme des résidus de la fraction rationnelle G_d de l'exemple 65 à ses petites branches (avec x remplacé par t). Ici, comme le dénominateur est $y - t - y^2$, il n'a qu'une seule petite branche. La diagonale ΔF_d est donc annulée par le polynôme

$$(1 - 4t)^{2d+1} y^2 - \left(\sum_{k=0}^{\lfloor d/2 \rfloor} \binom{d}{2k} \binom{2k}{k} x^k \right)^2.$$

Exemple 95. Soit d un entier strictement positif, et soit $\mathrm{F}_d \in \mathbb{Q}(x,y)$ la fraction rationnelle définie par

$$\mathrm{F}_d(x,y) = \frac{x^{d-1}}{1-x^d-y^{d+1}}$$

C'est une fraction de bidegré $(d,d+1)$. La première étape de l'algorithme 9 produit

$$\mathrm{G}_d(t,y) = y^\alpha \frac{\mathrm{P}}{\mathrm{Q}} = \frac{t^{d-1}}{y^d - t^d - y^{2d+1}},$$

qui est de bidegré $(d,2d+1)$, et dont le dénominateur est irréductible et possède d petites branches. De là, l'algorithme calcule des polynômes Φ_d annulant $\Delta\mathrm{F}_d$. Expérimentalement, ces polynômes sont irréductibles et leurs bidegrés pour $d = 1,2,3,4$ sont $(2,3)$, $(18,10)$, $(120,35)$, $(700,126)$.

À partir de ces valeurs, il est facile de conjecturer que le bidegré est donné par

$$\left(d(d+1)\binom{2d-1}{d-1}, \binom{2d+1}{d}\right),$$

ce qui met en évidence une croissance exponentielle en d. Nous allons voir avec le théorème 97 que, dans le cas général, la croissance du bidegré est au plus du même ordre de grandeur que dans cet exemple.

Exemple 96. Cet exemple est tiré d'une solution trouvée avec Bostan et Lairez à un exercice proposé dans l'American Mathematical Monthly par Gessel[5]. La question est de prouver l'égalité :

$$[x^n y^n] \frac{1}{(1-3y)(1-x-3y+3y^2)} = 9^n. \tag{4.5}$$

On remarque immédiatement que le membre de gauche est le n-ième coefficient de la diagonale de la fraction

$$\mathrm{F}(x,y) = \frac{1}{(1-3y)(1-x-3y+3y^2)}.$$

On peut donc appliquer l'algorithme PolynômeDiagonale à F, ce qui produit un polynôme annulateur pour $\Delta\mathrm{F}(t)$:

$$(9t-1)^3((1-9t)y+3)((1-9t)y-1)^3.$$

On en déduit que

$$\Delta\mathrm{F}(t) = -\frac{3}{1-9t}, \text{ ou bien } \Delta\mathrm{F}(t) = \frac{1}{1-9t}.$$

Mais comme il est évident que $\Delta\mathrm{F}(0) = 1$, la seule possibilité est

$$\Delta\mathrm{F}(t) = \frac{1}{1-9t},$$

5. "Problems and Solutions". Dans : *The American Mathematical Monthly* 123 (4) (avr. 2016), p. 399–406.

ce qui est équivalent à l'équation (4.5).

Il se trouve que pour cet exemple, on peut retrouver le résultat à la main. En effet, le changement de variable $x \mapsto t/y$ donne ici :

$$\Delta \mathrm{F}(t) = [y^{-1}] \frac{1}{(1-3y)(y-3y^2+3y^3-t)}$$

(c'est le lemme 82). Le dénominateur de cette fraction a une forme très particulière : le polynôme

$$\mathrm{P}(t,y) = y - 3y^2 + 3y^3 - t$$

admet une unique racine f telle que $f(0) = 0$, qui n'est autre que l'inverse du polynôme $y - 3y^2 + 3y^3$ pour la composition des séries. Ceci se voit également sur le polygone de Newton de P. Maintenant, on sait par la proposition 84 que

$$\Delta \mathrm{F} = \mathrm{Res}\left(\frac{1}{(1-3y)\mathrm{P}(t,y)}, f\right).$$

Comme f est un pôle simple, un calcul classique (voir aussi la remarque sous le corollaire 64) donne :

$$\mathrm{Res}\left(\frac{1}{(1-3y)\mathrm{P}(t,y)}, f\right) = \frac{1}{\partial_y\left\{(1-3y)\mathrm{P}\right\}(t,f)} = \frac{1}{(1-3f)\partial_y \mathrm{P}(t,f)} = \frac{1}{1-9f+27f^2-27f^3},$$

et comme $f - 3f^2 + 3f^3 = t$, on en déduit à nouveau que

$$\Delta \mathrm{F}(t) = \frac{1}{1-9t}.$$

4.2.3 Bornes

On dispose déjà de tous les outils nécessaires pour analyser l'algorithme PolynômeDiagonale. L'étape du changement de variables a été analysée dans le paragraphe 4.2.1, et les algorithmes PolynômeRésidus et SommeCompPure ont été analysés dans le chapitre précédent.

Théorème 97. *Soient* $\mathrm{A}, \mathrm{B} \in \mathbf{k}[x,y]_{d_x,d_y}$ *des polynômes premiers entre eux tels que* $\mathrm{B}(0,0) \neq 0$. *Soit* $\mathrm{B}^\star$ *la partie sans carré de* B, *de bidegré majoré par* $(d_x^\star, d_y^\star)$. *Alors le polynôme* $\Phi(t,y)$ *calculé par l'appel* PolynômeDiagonale(A/B) *vérifie*

$$\deg_t \Phi \leqslant \mathrm{D}_x \binom{\mathrm{D}_y}{c}, \quad \deg_y \Phi = \binom{\mathrm{D}_y}{c},$$

où

$$c = \mathrm{ddeg}^-(\mathrm{B}^\star),$$
$$\mathrm{D}_x = 2d_x(d_x+d_y+1) + d_x - 2(d_x - d_x^\star)(d_x - d_x^\star + d_y - d_y^\star + 1),$$
$$\mathrm{D}_y := \mathrm{ddeg}^-(\mathrm{B}^\star) + \mathrm{ddeg}^+(\mathrm{B}^\star).$$

Démonstration. D'après le théorème 69, quel que soit le signe de α l'appel à PolynômeRésidus produit un polynôme de degré

$$\mathrm{D}_y := \mathrm{ddeg}^-(\mathrm{B}^\star) + \mathrm{ddeg}^+(\mathrm{B}^\star). \tag{4.6}$$

Puis, par le théorème 77, on en déduit que

$$\deg_y \Phi = \binom{\mathrm{D}_y}{c}.$$

Pour majorer le degré de Φ en t, on peut ignorer l'optimisation qui consiste à prendre en compte la petite branche en 0 et appliquer l'algorithme PolynômeRésidus à $(y^\alpha \mathrm{P}, \mathrm{Q}, \mathrm{Q})$ ou $(\mathrm{P}, y^{-\alpha}\mathrm{Q}, y^{-\alpha}\mathrm{Q})$ selon que $\alpha \geqslant 0$ ou $\alpha < 0$. En effet, le polynôme obtenu de cette façon est clairement un multiple de celui calculé par l'algorithme. Par le théorème 69, comme les bidegrés de P, y^αP, Q et $y^{-\alpha}$Q sont tous majorés par $(d_x, d_x + d_y + 1)$, on calcule un polynôme R de degré en x majoré par D_x. Ensuite, on fait appel au théorème 77 appliqué à (R, c) ou $(\mathrm{R}, c+1)$ selon le signe de α. Dans les deux cas, on obtient

$$\deg_y \Phi = \binom{\mathrm{D}_y}{c}.$$

□

4.2.4 Complexité

Théorème 98. *On reprend les notations du théorème 97. Alors l'appel* PolynômeDiagonale(A/B) *est effectué en*

$$\tilde{\mathrm{O}}\left(c\mathrm{D}_x\binom{\mathrm{D}_y}{c}^2 + (d_x + d_y)^6\right)$$

opérations dans **k**.

Démonstration. Le calcul de P et Q ne nécessite aucune opération. Ensuite, d'après la remarque 71, le calcul de R et r se fait en $\tilde{\mathrm{O}}((d_x + d_y)^6)$ opérations. Le nombre de petits pôles est obtenu gratuitement à partir de la décomposition sans carré calculée par l'algorithme PolynômeRésidus. De là, comme le degré en x de R est borné par D_x (voir la preuve du théorème 97), le théorème 78 montre que l'appel à l'algorithme SommeCompPure coûte $\tilde{\mathrm{O}}(c\mathrm{D}_x\binom{\mathrm{D}_y}{c}^2)$ opérations. Enfin, si une translation de la variable est requise, elle peut être effectuée par évaluation et interpolation en $\tilde{\mathrm{O}}(\mathrm{D}_x\binom{\mathrm{D}_y}{c}^2)$ opérations. (On pourrait également évaluer et interpoler par rapport à x et utiliser de meilleurs algorithmes pour la translation univariée[6].) □

6. BOSTAN, FLAJOLET et al., "Fast Computation of Special Resultants", §5.

4.3 Degré du polynôme minimal dans le cas générique

La borne du théorème 97 sur le bidegré de Φ est légèrement pessimiste en t, mais génériquement atteinte en y. Cette dernière affirmation fait l'objet de la proposition 100 ci-dessous. On commence tout d'abord par démontrer un lemme de théorie de Galois, dans lequel on utilise la notation $\mathfrak{S}_n$ pour désigner le groupe symétrique de degré n.

Lemme 99. *Soit $\mathbb{K}$ un corps de caractéristique 0, et $p \in \mathbb{K}[y]$ un polynôme de degré d, dont le groupe de Galois sur $\mathbb{K}$ est $\mathfrak{S}_d$. On suppose que les racines $\alpha_1, \ldots, \alpha_d$ de p dans $\overline{\mathbb{K}}$ sont algébriquement indépendantes sur $\mathbb{Q}$. Alors, pour tout $c \leqslant d$, le polynôme $\Sigma_c p$ de degré $\binom{d}{c}$ est irréductible sur $\mathbb{K}$.*

($\Sigma_c p$ a été défini dans le paragraphe 3.2.2.)

Démonstration. Comme $\Sigma = \alpha_1 + \cdots + \alpha_c$ est une racine de $\Sigma_c p$, il suffit de montrer que le degré de $\mathbb{K}(\Sigma)$ sur $\mathbb{K}$ vaut $\binom{d}{c}$. Les α_i étant algébriquement indépendants sur $\mathbb{Q}$, toute permutation $\sigma \in \mathfrak{S}_d$ des α_i par laquelle Σ est invariant doit également fixer les ensembles $\{\alpha_1, \ldots, \alpha_c\}$ et $\{\alpha_{c+1}, \ldots, \alpha_d\}$. Réciproquement, toute permutation ayant cette propriété induit un automorphisme de $\mathbb{K}(\alpha_1, \ldots, \alpha_d)$ par lequel Σ est invariant. En d'autres termes, le groupe de Galois de $\mathbb{K}(\alpha_1, \ldots, \alpha_d)$ sur $\mathbb{K}(\Sigma)$ est égal à $\mathfrak{S}_c \times \mathfrak{S}_{d-c}$. On en déduit que $\mathbb{K}(\alpha_1, \ldots, \alpha_d)$ a un degré $c!(d-c)!$ sur $\mathbb{K}(\Sigma)$ et $d!$ sur $\mathbb{K}$, de telle sorte que $\mathbb{K}(\Sigma)$ a un degré $\binom{d}{c}$ sur $\mathbb{K}$. □

Proposition 100. *Soit $A \in \mathbb{Q}[x, y]$ un polynôme. Soient d_x et d_y des entiers positifs, $s^- \leqslant d_x$, $s^+ \leqslant d_y$, et*

$$B(x, y) = \sum_{i=0}^{s^-} b_i^{(x)} x^i + \sum_{j=1}^{s^+} b_j^{(y)} y^j + \sum_{\substack{i \leqslant d_x, j \leqslant d_y \\ -s^- \leqslant j-i \leqslant s^+}} b_{i,j} x^i y^j \in \mathbb{Q}[(b_i^{(x)}), (b_j^{(y)}), x, y],$$

où les $b_i^{(x)}$ et $b_j^{(y)}$ sont des indéterminées et $b_{i,j} \in \mathbb{Q}$.

Alors le polynôme $\Phi(t, y)$ calculé par l'appel PolynômeDiagonale(A/B) *est irréductible de degré $\binom{s^- + s^+}{s^-}$ sur $\mathbb{K} = \mathbb{Q}[(b_i^{(x)}), (b_j^{(y)}), t, y]$.*

Démonstration. On reprend les notations de l'algorithme PolynômeDiagonale. D'après sa définition dans l'algorithme, le polynôme Q vaut

$$Q(t, y) = \sum_{i=0}^{s^-} b_i^{(x)} t^i y^{s^- - i} + \sum_{j=1}^{s^+} b_j^{(y)} y^{s^- + j} + \sum_{i,j} b_{i,j} t^i y^{s^- - i + j}.$$

Notons $d = s^- + s^+$. Alors le polynôme $Q(1, y)$ a la forme $\sum_{j \leqslant d} t_j y^j$ où chacun des t_j est la somme de l'une des indéterminées et de nombres rationnels. Ceci implique que les t_j sont algébriquement indépendants sur $\mathbb{Q}$. Donc $Q(1, y)$ admet $\mathfrak{S}_d$ pour groupe de Galois sur $\mathbb{Q}(t_0, \ldots, t_d)$ et ses racines sont algébriquement indépendantes

sur $\mathbb{Q}$ [7]. Cette propriété s'étend à $\mathrm{Q}(t,y)$ [8], qui a donc $\mathfrak{S}_d$ comme groupe de Galois et des racines algébriquement indépendantes, notées $y_1,\dots,y_d$.

Maintenant, on définit le polynôme $\mathrm{R}(t,y) = \prod_i (y - \tilde{\mathrm{P}}(t,y_i)/\partial_y \mathrm{Q}(t,y_i))$, où $\tilde{\mathrm{P}} = y^\alpha \mathrm{P}$ si $\alpha \geqslant 0$ et $\tilde{\mathrm{P}} = \mathrm{P}$ sinon. Comme toutes les racines de Q sont simples, R est exactement le polynôme calculé par l'algorithme PolynômeRésidus. Alors la famille $\{\mathrm{P}(t,y_i)/\partial_y \mathrm{Q}(t,y_i)\}$ est algébriquement indépendante sur $\mathbb{Q}$, puisque toute relation algébrique entre ses éléments en induirait également une pour les y_i en réduisant au même dénominateur. En particulier, le morphisme naturel $\mathrm{Gal}(\mathrm{Q}/\mathbb{K}) = \mathfrak{S}_d \to \mathrm{Gal}(\mathrm{R}/\mathbb{K})$ est injectif, et donc un isomorphisme. (Ici, on note $\mathrm{Gal}(\mathrm{P}/\mathbb{K})$ le groupe de Galois sur $\mathbb{K}$ de $\mathrm{P} \in \mathbb{K}[y]$.) Comme une simple inspection du polygone de Newton de Q montre qu'il a s^- petites branches, on peut conclure en utilisant le lemme 99 et le fait qu'une translation de la variable ne change en rien l'irréductibilité de Φ. □

La proposition 100 doit être comprise comme un résultat d'optimalité. En effet, pour une fraction rationnelle A/B générique, comme dans la proposition, on a $\mathrm{B} = \mathrm{B}^\star$, $\mathrm{ddeg}^-(\mathrm{B}) = s^-$, $\mathrm{ddeg}^+(\mathrm{B}) = s^+$ et B a s^- petites branches. Ceci montre que la borne du théorème 97 est optimale dans ce cas (générique).

Si l'on croit au fait que les exemples aléatoires devraient se comporter comme le cas générique, alors la proposition 100 met en évidence que le polynôme calculé par l'algorithme 9 sera irréductible la plupart du temps.

À titre d'exemple, on considère le cas particulier de la proposition 100 où $s^- = s^+ = d_x = d_y = d$. On a alors $\deg_y \Phi = \binom{2d}{d}$.

Exemple 101. Illustrons ce résultat davantage en observant le degré du polynôme minimal sur des diagonales de fractions rationnelles tirées au hasard. On considère une fraction rationnelle $\mathrm{F}(x,y) = 1/\mathrm{B}(x,y)$, où $\mathrm{B}(x,y)$ est un polynôme dense de bidegré (d,d) choisi au hasard. Pour $d = 1,2,3,4$, la sortie de l'algorithme 9 est irréductible de bidegré $(2,2)$, $(16,6)$, $(108,20)$, $(640,70)$. Ces valeurs correspondent à la formule

$$\left(2d^2\binom{2d-2}{d-1}, \binom{2d}{d}\right). \tag{4.7}$$

On constate donc que la borne sur $\deg_y \Phi$ est fine dans ce cas, et l'irréductibilité de la sortie indique que la proposition 100 ne peut être améliorée.

7. WAERDEN, *Modern Algebra*, §57.
8. Ibid., §61.