Résultants et sous-résultants de polynômes p-adiques

X. Caruso
IRMAR
Université Rennes 1
Campus de Beaulieu
35042 Rennes Cedex
xavier.caruso@normalesup.org

Soient p un nombre premier et $\mathbb{Z}_p$ l'anneau des entiers p-adiques. À l'origine de ce travail est la volonté d'obtenir des algorithmes à la fois efficaces et stables numériquement pour le calcul du PGCD — ainsi que des coefficients de Bézout — de polynômes à coefficients dans $\mathbb{Z}_p$.

Un premier candidat est, bien entendu, l'algorithme d'Euclide usuel. Malheureusement, s'il est plutôt efficace, on s'aperçoit rapidement qu'il ne fait pas le poids au niveau de la stabilité numérique. En effet, on observe expérimentalement que sur des entrées aléatoires A et B piochées parmi les polynômes unitaires de degré d à coefficients dans $\mathbb{Z}_p$, l'algorithme d'Euclide étendu calcule les coefficients de Bézout correspondants U et V avec une perte moyenne d'un nombre de chiffres significatifs sur chaque coefficient qui croît proportionnellement à d. De surcroît, on obtient fréquemment des exemples pour lesquels on observe une chute importante de la précision alors que le résultant $\text{Rés}(A, B)$ est inversible dans $\mathbb{Z}_p$. Or, avec un algorithme stable, ceci ne devrait pas se produire car la théorie des résultants affirme que les coefficients de U et V s'écrivent comme le quotient d'une expression polynômiale en les coefficient de A et B par $\text{Rés}(A, B)$; ainsi, si $\text{Rés}(A, B)$ est inversible dans $\mathbb{Z}_p$, on s'attend à connaître les coefficients de Bézout avec la même précision que les entrées.

La première partie de mon exposé sera consacrée à l'explication des phénomènes qui viennent d'être décrits. Plus précisément, je montrerai que les pertes de précision qui s'accumulent au cours de l'exécution de l'algorithme

d'Euclide valent approximativement :

$$2 \cdot \sum_{j=0}^{d-1} V_j(A,B) \tag{1}$$

où $V_j(A,B)$ désigne la valuation de coefficient dominant du j-ième sous-résultant de (A,B). Cette quantité est à mettre en comparaison avec la valeur $2 \cdot V_0(A,B)$ qui est la perte « théorique » donnée par l'argument des résultants. J'étudierai ensuite les fonctions V_j considérées comme des variables aléatoires : j'énoncerai un théorème qui décrit leur loi et, comme corollaire, en déduirai les résultats descriptifs que voici.

Théorème 1. *Pour tout $j \in \{0, \dots, d-1\}$, on a :*

i) $\frac{1}{p-1} \leq \mathbb{E}[V_j] \leq \frac{p}{(p-1)^2}$ *;*

ii) $\sigma(V_j) = O\big(\frac{1}{\sqrt{p}}\big)$ *;*

iii) $\mathbb{P}[V_j \leq m] = O\big(p^{-m+O(\sqrt{m})}\big)$

où les constantes dans tous les $O(\cdot)$ sont absolues (et, en particulier, ne dépendent ni de j, ni de d).

Il résulte du théorème que l'expression (1) vaut en moyenne $\simeq \frac{2d}{p-1}$, en accord avec ce qui avait été observé initialement. En comparaison, la perte « théorique » $2 \cdot V_0(A,B)$ ne vaut en moyenne que $\simeq \frac{2}{p-1}$. En d'autres termes, l'algorithme d'Euclide surestime les pertes de précision d'un facteur d.

Enfin, dans une deuxième partie de mon exposé, je présenterai une variante « stabilisée » de l'algorithme d'Euclide qui conserve sa complexité mais atteint également la perte de précision donnée par la théorie des résultants. Cette variante repose de façon essentielle sur la théorie de la précision p-adique développée dans [1].

Bibliographie

[1] X. Caruso, D. Roe, T. Vaccon, *Tracking p-adic precision*, LMS J. Comput. Math. **17** (Special issue A), 2014, 274–294