Recherche

Géométrie et Algorithmique des polynômes

Mes recherches portent sur la géométrie et l'algorithmique des polynômes. Je me suis en particulier intéressé à la factorisation bivariée (sur les corps de nombres et les corps finis), aux singularités des courbes planes, à la gonalité des courbes algébriques et aux discriminants minimaux. Actuellement, je poursuis mes recherches sur les liens factorisation/singularités (k-nômes, séries de Puiseux, adjoints) et je m'intéresse à de nouvelles thématiques, comme les problèmes d'incidences droites-hypersurfaces. Un fil conducteur majeur de mes travaux est de tenir compte d'indicateurs de complexité plus fins que le degré ou le multi-degré dans les problèmes d'algorithmique des polynômes, en particulier pour la factorisation. Les variétés toriques y jouent un rôle important, offrant le cadre géométrique naturel pour tenir compte du polytope de Newton lorsque les singularités à l'infini sont non dégénérées. De manière générale, les algorithmes que je développe utilisent des outils théoriques à l'interface entre le calcul formel, la géométrie algébrique, l'analyse complexe et la théorie des nombres : géométrie torique, fibrés vectoriels, cohomologie, courants, syzygies, résidus, résultants, discriminants, extensions de corps, etc. Je détaille dans ces quelques pages mes travaux effectués et en cours les plus significatifs (entre parenthèse les articles se rapportant à la thématique en question qui seront détaillés ci-après) :

I. Travaux effectués.

- A. Problèmes type Abel-inverse dans le cadre torique (**1,2,3,5**).
- B. Factorisation des polynômes bivariés :
  - a. Factorisation et géométrie torique (**4,5,6**).
  - b. Factorisation et singularités (**7,8**).
- C. Discriminants minimaux (**9**).
- D. Gonalité des courbes algébriques (**10**).

II. Travaux en cours.

- E. Factorisation et singularités à l'infini.
- F. Réductibilité des k-nômes.
- G. Calcul des séries de Puiseux.
- H. Calcul des polynômes adjoints.
- K. Problèmes de contact droites-hypersurfaces.

I. Travaux effectués.

A. Problèmes type Abel-inverse dans le cadre torique.

Cette partie regroupe les travaux issus de ma thèse *La trace en Géométrie projective et torique*. Je revisite les travaux de Griffiths [15] et Henkin-Passare [19] autour de la transformée d'Abel-Radon et du théorème d'Abel-inverse *via* une utilisation systématique du calcul résiduel. Afin de prendre en compte le polytope de Newton dans les problèmes d'algébricité des courants localement résiduels, je généralise les théorèmes d'Abel et d'Abel-inverse du cadre projectif au cadre torique.

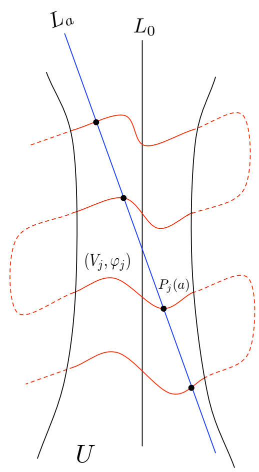


Figure 1 – Le théorème d'Abel-inverse, le cas projectif

1. M. Weimann, *Trace et calcul résiduel : nouvelle version du théorème d'Abel-inverse et formes abéliennes*, Ann. Fac. Sci. Toulouse, Sér.6, Vol.16, no.2 (2007), 397-424. J'étudie dans cet article les relations entre résidus multidimensionels et la transformée d'Abel-Radon des courants localement résiduels dans les domaines linéairement concave de l'espace projectif complexe $\mathbb{P}^n$. En étudiant des propriétés de rigidité de systèmes non linéaires d'équations aux dérivées partielles, je prouve une version plus forte du théorème d'Abel-inverse de Henkin-Passare [19] donnant des conditions de rationnalité d'un courant localement résiduel. Cette approche permet entre autres d'établir le lien entre le théorème d'Abel-inverse et le théorème de Wood [38] donnant des critères pour l'algébricité d'une famille de germes d'hypersurfaces analytiques en des points alignés de $\mathbb{C}^n$. Enfin, je dérive une nouvelle méthode pour calculer la dimension de l'espace des n-formes abéliennes sur une hypersurface de $\mathbb{P}^{n+1}$.

2. M. Weimann, *An interpolation theorem in toric varieties*, Ann. Inst. Fourier, Vol. 58, no.4 (2008), 1371-1381. Dans cet article, je considère un problème d'interpolation en géométrie torique. Je prouve un théorème donnant des critères d'interpolabilité d'une famille de germes d'hypersurfaces analytiques dans une variété torique projective lisse X par une hypersurface algébrique de classe de Picard fixée, généralisant un théorème de Wood [38] dans le cadre projectif. Ce théorème d'interpolation torique a eu entre autres des applications en calcul symbolique-numérique, pour la factorisation des polynômes creux (cf B.4. et [11]).

3. M. Weimann, *Concavity, Abel-transform and the Abel-inverse Theorem in smooth complete toric varieties*, Collectanea Mathematica, Vol. 64, no.1 (2013), 111-133. Motivé par des problèmes d'effectivité, je généralise dans cet article la transformée d'Abel-Radon au cadre plus large des variétés toriques, mieux adaptées à la géométrie des polynômes creux. Je définis et j'étudie une notion de concavité torique attachée à une somme directe de fibrés en droites. Je caractérise les fibrés donnant lieu á une transformée d'Abel-Radon torique non triviale. Je généralise ensuite le théorème d'Abel-inverse de Henkin-Passare [19] au cadre des variétés toriques complètes lisses *via* une représentation résiduelle des formes traces, *via* le théoréme de dualité et *via* une étude de système d'équations aux dérivées partielles type "onde de choc".

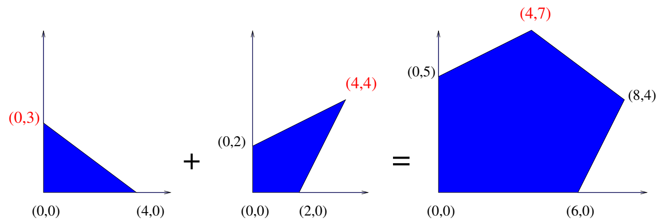
B. Factorisation des polynômes bivariés.

La factorisation bivariée est un thème central de l'algèbre computationnelle pour lequel de nombreux algorithmes ont été développés, avec maintenant de très bonnes complexités en le degré total. Le fil conducteur de mes travaux sur cette thématique est de tenir compte d'indicateurs de complexité plus fins que le degré ou le multi-degré. Je me suis intéressé dans un premier temps au polytope de Newton, puis plus généralement à la géométrie des singularités.

B. a) Factorisation bivariée et géométrie torique.

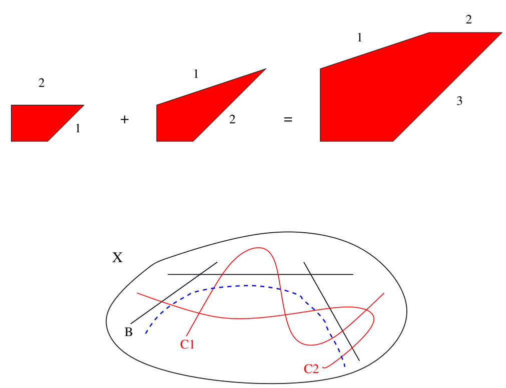
Je présente ici mes travaux sur les liens entre la factorisation des polynômes bivariés, le polytope de Newton, et la géométrie torique. Rappelons que le polytope de Newton N_f d'un polynôme multivarié f est l'enveloppe convexe des exposants qui apparaissent dans le développement monomial de f. Le théorème d'Ostrowski assure la fonctorialité $N_{f_1 f_2} = N_{f_1} + N_{f_2}$, faisant du polytope de Newton un objet naturel à prendre en compte dans les problèmes de factorisation multivariée. Géométriquement, cela demande de remplacer la compactification projective classique de l'espace affine par une compactification torique dont la théorie de l'intersection est cette fois intimement liée à la combinatoire du polytope.

$$f_1 = 1 - 2x^4 + y^3 - xy, \qquad f_2 = 3 - x^2 + xy^2 - 2x^4y^4 + y^2, \qquad f_1 f_2 = 3 + 2x^6 + 4x^8y^4 - 2x^4y^7 + y^5 + \cdots$$



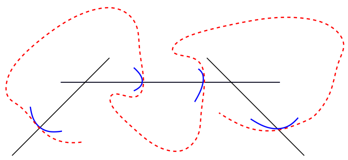
Polytopes de Newton et théorème d'Ostrowski : $N_{f_1 f_2} = N_{f_1} + N_{f_2}$

4. M. Elkadi, A. Galligo, M. Weimann, *Towards Toric Absolute Factorization*, J. of Symb. Comp., Vol. 44 (2009), 1194-2011. On développe ici un algorithme probabiliste semi-numérique de factorisation absolue des polynômes bivariés sur un corps de nombre, dont la complexité tient compte du polytope de Newton (enveloppe convexe des exposants). L'idée géométrique centrale est d'étudier la clôture de Zariski de la courbe définie par le polynôme d'entrée dans une compactification torique X adéquate du plan affine, le cas dense correspondant à la compactification projective usuelle $X = \mathbb{P}^2$. Notre méthode étend ainsi au cadre torique un algorithme de Chèze-Galligo-Rupprecht [13]. Elle est basée sur un théorème d'interpolation torique issus de ma thèse [33] qui permet de tenir compte du théorème d'Ostrowski dans les problèmes de recombinaisons. Nous testons l'algorithme sur quelques exemples avec Maple.



Compactification torique associée au polytope de Newton.

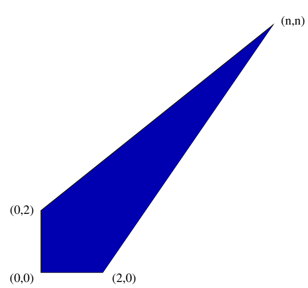
5. *Algebraic osculation and factorization of sparse polynomials*, J. of Found. of Comp. Math. 12 no.2 (2012), 173-201. Etant donnée une compactification projective lisse X de $\mathbb{C}^2$ de bord B, sous quelles conditions existe-t-il un diviseur de X ayant des jets prescrits le long de B ?



Osculation au bord de X

Ce problème se traduit par une caractérisation du conoyau du morphisme de restriction $Pic(X) \to Pic(D)$ pour D un diviseur de Cartier effectif supporté par B. Je résouds ce problème d'extension des fibrés en droites à l'aide de la dualité de Serre, de la cohomologie de Dolbeault et des courants résiduels. Ce résultat généralise un théorème de Griffiths-Harris [16] et Wood [39] qui considèrent le cas $X = \mathbb{P}^2$. En appliquant ce résultat au cas X torique, je dérive un algorithme de factorisation bivariée déterministe, version torique de la remontée de Hensel classique, permettant maintenant de profiter de la géométrie du polytope de Newton : la factorisation univariée de haut degré est remplacée par la factorisation de petit degré des polynômes de facettes, et le nombre (exponentiel) de recombinaisons possibles des facteurs modulaires est réduit par les contraintes combinatoires imposées par le théorème d'Ostrowski.

6. *A lifting and recombination algorithm for rational factorization of sparse polynomials*, Journal of Complexity 26 (2010), 608-628. J'obtiens ici un algorithme déterministe de factorisation bivariée dans $K[x, y]$ (K un corps de nombre) en temps polynomial en le volume du polytope. Ma méthode généralise l'algorithme dense de Lecerf [22] au cadre torique, le point clé étant le théorème d'osculation torique ((5),[35]). La preuve utilise formes logarithmiques et cohomologie des variétés toriques. J'ai implémenté une version de mon algorithme avec le logiciel Sage.



Pour un tel polytope, l'algorithme de Lecerf utilise 1 factorisation univariée de degré $2n$ et $\mathcal{O}(n^{\omega+1})$ opérations arithmétiques sur le corps de base. L'approche torique réduit la complexité à 2 factorisations univariées de degré 2 et $\mathcal{O}(n^{\omega})$ opérations.

B. b) Factorisation et singularités.

Le cadre torique permet de factoriser plus rapidement les polynômes dont les singularités à l'infini sont non dégénérées relativement au polytope (au sens de Kushnirenko). Le cas dégénéré requiert une étude plus fine des relations locales/globales entre singularités et factorisation. L'idée est de considérer cette fois un morphisme birationnel

$$\pi : X \longrightarrow \mathbb{P}^2$$

tel que X soit une compactification du plan affine dont le bord $B := X \setminus \mathbb{A}^2$ rencontre transversalement la clôture de Zariski $C \subset X$ de la courbe affine $f = 0$. On peut choisir X torique précisément lorsque f est non dégénéré. Mon but est de prouver une "conjecture" du type :

Conjecture : *Il existe un algorithme déterministe qui, donné $f \in k[x, y]$ sans facteurs carrés sur k un corps fini ou un corps de nombre, factorise f avec $\widetilde{\mathcal{O}}(\Delta r^{\omega-1})$ opérations sur k, où Δ est le genre arithmétique de C et $r = C \cdot B$.*

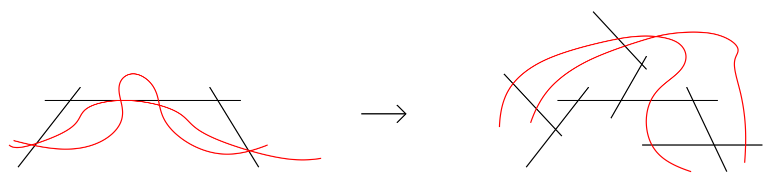


FIGURE 2 – De la compactification torique à la compactification non torique. Nouvelles composantes exceptionnelles à l'infini. Le nombre de facteurs analytiques à recombiner décroît

Ici, on note $2 < \omega < 2,35$ l'exposant de multiplication des matrices. Dans le cas régulier $X = \mathbb{P}^2$, on a $\Delta = (d-1)(d-2)/2$ et $r = d$ où d est le degré total de f et l'on retrouve La complexité actuelle $\widetilde{\mathcal{O}}(d^{\omega+1})$ plus une factorisation univariée de degré d [22]. Si le polynôme est singulier à l'infini, les invariants Δ et r décroissent. Autrement dit, je cherche à valider le principe général suivant :

"Plus un polynôme est singulier à l'infini, plus vite on le factorise".

Les articles (7) et (8) qui suivent offrent une résolution partielle de ce problème, mais il reste encore quelques zones d'ombres. Un problème théorique majeur est lié à l'annulation de la cohomologie de certains fibrés logarithmiques (résolu dans (6) dans le cas X torique). Un problème algorithmique majeur est la complexité du calcul des séries de Puiseux (calcul de $C \cap B$), problème en bonne voie de résolution (section F) et le calcul rapide des polynômes adjoints (section G).

7. *Factoring bivariate polynomials using adjoints*, J. of Symb. Comp. 58 (2013), 77-98. On établit le lien entre la factorisation et la désingularisation de la courbe projective $\mathcal{C} \subset \mathbb{P}^2_k$ définie par $f \in k[x, y]$ pour un corps de base k quelconque. On développe un algorithme déterministe qui, étant donnée une base de l'espace $\mathcal{A} \subset \mathbb{K}[x, y]$ engendré par les adjoints de f de degrés $d - 2$ (respectivement leur reste modulo (x)), factorise f sur k avec une factorisation univariée de degré d plus $\mathcal{O}(gd^{\omega-1})$ opérations sur k (respectivement $\mathcal{O}(d^{\omega})$ opérations), où g est le genre géométrique de $\mathcal{C}$. Ce résultat pose la question de savoir s'il est possible de calculer les polynômes adjoints (ou leur reste modulo (x)) en temps "raisonnable". Ce problème est fortement lié à la complexité du calcul des séries de Puiseux (cf Section F).

8. ***Factoring bivariate polynomials using a critical fiber*** **, J. of Found. of Comp. Math. 2016 (à paraître, 40 pages)** Pour factoriser un polynôme $f \in k[x, y]$ (k un corps), on peut considérer sa factorisation analytique dans $k[[x]][y]$ calculée à une certaine précision, puis recombiner ces "facteurs analytiques tronqués" pour découvrir les facteurs rationels. Cette approche marche bien dans le cas $f(0, y)$ séparable. J'étudie ici le problèmes des recombinaisons dans le cas $f(0, y)$ non séparable (fibre critique $x = 0$), généralisant en quelques sortes le cas non dégénéré traité dans [34]. Un avantage majeur est qu'il y a moins de facteurs analytiques à recombiner dû à la présence de ramification. Une des difficultés majeures est le calcul des facteurs analytiques, un travail sur ce sujet est en cours en collaboration avec Adrien Poteaux (Section F).

D. Discriminants minimaux.

Lorsque l'on veut factoriser un polynôme en le désingularisant, les polynômes dont la valuation du discriminant au-dessus de l'infini est "anormalement élévée" posent problème. Ainsi, on s'est intéressé avec Denis Simon à la "réduction" (type réduction de Gauss) des polynômes de "discriminants minimaux". Dans une certaine mesure, nos résultats valident dans le cas des corps de fonctions des conjectures ouvertes dans le cas des corps de nombres.

9. ***Plane curves with minimal discriminant (avec D. Simon)*****, Journal of Commutative Algebra (2016), 43 pages (à paraître), preprint arXiv :1507.01091.** On caractérise ici les polynômes univariés à coefficients dans $k[T]$ dont le discriminant est de degré minimal respectivement à certains invariants (bidegré, genre, nombre de facteurs). On montre que ces polynômes correspondent aux courbes lisses de $\mathbb{A}^1 \times \mathbb{P}^1$ ayant une seule place à l'infini. On étudie les processus de "réduction" de ces polynômes via l'action de $SL_2(k[T])$. Le théorème d'Abhyankar-Moh caractérisant les courbes rationnelles lisses affines ayant une seule place à l'infini de $\mathbb{P}^2$ permet entre autres de clarifier totalement la situation dans le cas rationel unitaire irréductible. Des résultats similaires partiels sont obtenus dans le cas non unitaire.

E. Gonalité des courbes algébriques.

La gonalité d'une courbe algébrique C est le plus petit entier n tel qu'il existe un morphisme $\pi : C \to \mathbb{P}^1$ de degré n (éventuellement définit sur une extension du corps de base). Comme le genre, cet invariant mesure la "non rationalité" d'une courbe algébrique. En particulier $gon(C) = 1$ si et seulement si $g = 0$ et $gon(C) = 2$ si et seulement si C est hyperelliptique. Outre son intérêt théorique évident, le calcul d'un morphisme gonal trouve des applications en particulier pour la paramétrisation par radicaux (i.e. en autorisant $\sqrt{}, \sqrt[3]{}, \ldots$) des courbes planes de petite gonalité.

10. *Computational aspects of gonal maps (avec F-O. Schreyer et J. Schicho)*, AAECC 24, Issue 5 (2013), 313-341.. On développe ici un algorithme déterministe permettant de calculer la gonalité et un morphisme gonal de n'importe quelle courbe algébrique irréductible définie sur un corps algébriquement clos de caractéristique nulle (ou positive suffisamment grande). L'idée centrale est d'utiliser la résolution projective minimale d'un modèle canonique de la courbe. On peut ainsi calculer en temps raisonnable la gonalités des courbes de genre $g \leq 9$. On étudie des variantes plus rapides sous certaines conditions sur les syzygies du modèle canonique, permettant de traiter en temps raisonnable certaines courbes de genre $g \leq 14$ sur un corps fini.

II. Travaux en cours.

F. Séries de Puiseux en temps rapide et applications (avec A. Poteaux).

En collaboration avec Adrien Poteaux, on s'intéresse à améliorer les bornes de complexité du calcul des parties singulières des séries de Puiseux d'un polynôme $f \in k[x,y]$ au-dessus de $x = 0$. L'idée est d'utiliser un schéma dichotomique "à la Hensel" combiné à une approche "à la D5" permettant d'éviter des factorisations univariées trop coûteuses. On a ainsi obtenu récemment une complexité totale $\tilde{\mathcal{O}}(d_y \mathcal{V})$ où $\mathcal{V}$ est la valuation en x du discriminant de f, améliorant la meilleure complexité $\tilde{\mathcal{O}}(d^4)$ connue actuellement [29]. Ce résultat admet pour conséquence le calcul du genre d'une courbe plane définie sur un corps de nombre ou un corps fini en $\tilde{\mathcal{O}}(hd^3)$ opérations binaires où h est la hauteur maximale des coefficients de f et d est le degré total. Ce résultat admet aussi comme corollaire une factorisation analytique rapide dans $k[[x]][y]$ avec des conséquences importantes en factorisation bivariée (cf [37] et Section B.b)).

G. Calcul rapide des polynômes adjoints.

Les fibrés du type $\Omega^2_X(D)$ où $X \to \mathbb{P}^2$ résoud (partiellement ou non) les singularités d'une courbe projective plane $\mathcal{C}$ jouent un rôle crucial dans plusieurs problèmes algorithmiques, par exemple le calcul de la jacobienne ou encore les relations factorisation-singularités ([34], [35], [36] et Problème 1 ci-dessus). Dans le cas où $D \in |C|$, où C est la transformée stricte de $\mathcal{C}$ par la résolution minimale plongée de $\mathcal{C}$, le calcul d'une base de $H^0(X, \Omega^2_X(D))$ se ramène au calcul d'une base des polynômes adjoints de certains degrés, *i.e* polynômes s'annulant à un certain ordre en les singularités. Il existe à notre connaissance deux algorithmes pour calculer une telle base : soit *via* l'algorithme de Newton-Puiseux et les courbes polaires [31], soit *via* le conducteur de la clôture intégrale dans l'anneau des fonctions rationnelles (théorème de Mnũk [9, 25]). Aucune étude de complexité ne nous est connue à ce jour. On cherche à développer un tel algorithme avec une complexité raisonnable pour espérer une application en factorisation. Là encore, un algorithme de Newton-Puiseux rapide est une composante essentielle de ce projet.

H. Réductibilité des k-nômes (avec F. Amoroso et M. Sombra)

Un résultat de Schintzel [30] assure qu'un trinôme $Ax^n + Bx^m + C \in \mathbb{C}(t)[x]$ non "dégénéré" admet soit un facteur de degré 1 ou 2, soit est irréductible sauf pour un nombre fini de valeurs de n et m. On cherche à généraliser ce résultat au cas des k-nômes (somme de k monômes) : on s'attend à ce qu'il existe deux constantes $n_0(k)$ et $n_1(k)$ *ne dépendant que de* k telles que tout k-nôme à coefficients dans $\mathbb{C}(t_1, \ldots, t_{k-2})$ non "dégénéré" (dans un sens précis) de degré $n \geq n_0(k)$ ne puisse avoir que des facteurs de degrés $\leq n_1(k)$. Une astuce directement inspirée des travaux de Schintzel permet de réduire ce problème au calcul explicite des invariants birationnels cohomologiques d'un corps de fonctions. Le cas des trinômes correspond au calcul du genre du corps de fonction d'une courbe. Le cas (ouvert) des k-nômes avec $k \geq 4$ requiert de calculer certains invariants (ramification, genre, irrégularités, etc) d'un corps de fonctions de degré de transcendance $k - 2 \geq 2$.

K. Incidence droites-hypersurfaces (avec L. Busé, C. D'Andrea et M. Sombra)

Soit $V \subset \mathbb{P}^n$ une hypersurface projective. On dit que $p \in V$ est *un flex* s'il existe une droite L passant par p et d'ordre de contact au moins $n+1$ avec V en p. Il est connu que le lieu flex d'une courbe irréductible de degré d est une sous-variété de dimension 0 et de degré $d(3d-6)$, déterminé par l'intersection de la courbe et de son Hessien. Le théorème de Salmon-Cayley généralise ce résultat au cas des surfaces (montrant en particulier qu'une cubique lisse contient précisément 27 droites). On généralise ce résultat en dimension supérieure : le lieu flex $Flex(V) \subset V$ d'une hypersurface V de $\mathbb{P}^n$ est soit la variété V elle-même si V est réglée, soit une sous-variété de codimension 1 de V, intersection de V avec une hypersurface W dont nous avons calculé le degré. On obtient de plus diverses formules permettant de calculer l'équation de W à l'aide de la théorie des résultants multidimensionnels. La rédaction d'un papier sur ces résultats est en cours et on travaille maintenant sur deux questions ouvertes : trouver des équations explicites type "hessien" pour le lieu flex d'une hypersurface, puis étudier le lieu de contact maximal entre une variété V et des sous-variétés linéaires en toute dimension.

Références

[1] F. Abu Salem, S. Gao, A.G.B. Lauder, Factoring polynomials via polytopes, proc. of ISSAC (2004), pp. 4-11.

[2] M. Avendano, T. Krick, M. Sombra, Factoring bivariate sparse (lacunary) polynomials, J. of Complexity 23 (2007), pp. 193-216.

[3] K. Belabas, M. Van Hoeij, J. Kluners, A. Steel, *Factoring polynomials over global fields*, J. of Symb. Comp. Vol. 40, Issue 6, pp. 1325-1339 (2005).

[4] J. Berthomieu, G. Lecerf, Convex-dense bivariate polynomial factorization, à paraître dans Math. Comp.

[5] G. Chèze and G. Lecerf, Lifting and recombination techniques for absolute factorization, J. of Complexity 23, no. 3 (2007), pp. 380-420.

[6] D. Cox, Toric residues, Ark Mat. 34 (1996), pp. 73-96.

[7] D. Cox, J. Little, D. O'Shea, Using algebraic geometry, Graduate Texts in Mathematics, 185. Springer-Verlag, New York (1998).

[8] C. D'Andrea, M. Sombra, Rational parametrizations, intersection theory and Newton polytopes, IMA Vol. Math. Appl. 151 (2009) pp. 35-50.

[9] B. Deconinck, M. Van Hoeij, Computing Riemann matrices of algebraic curves, PhysicaD, 152 (2001), pp. 28-46.

[10] D. Duval, Absolute factorization of polynomials, a geometric approach, SIAM J. Comput. 20, No. 1 (1991), pp. 1-21.

[11] M. Elkadi, A. Galligo, M. Weimann, Towards Toric Absolute Factorization, J. Symb. Comp., Vol. 44, no 9 (2009), pp. 1194-1211.

[12] W. Fulton, Introduction to Toric Varieties, Annals of Math. Studies, Princeton University Press (1993).

[13] A. Galligo, D. Rupprecht, Irreducible Decomposition of Curves, J. of Symb. Comp. 33, (2002) pp 661-677.

[14] J. von zur Gathen, J. Gerhard, Modern computer algebra, Cambridge University Press, 1st edition (1999).

[15] P.A. Griffiths, *Variations on a therorem of Abel*, Inventiones math. 35 (1976), pp. 321-390.

[16] P.A. Griffiths, J. Harris, *Principles of Algebraic Geometry*, Pure and applied mathematics, Wiley-Intersciences (1978).

[17] J. Guardia, J. Montes, E. Nart, Higher Newton polygons and integral basis, arXiv 0902.3428v2 (2011).

[18] P.A. Griffiths, J. Harris, Residues and zero-cycles on algebraic varieties, Annals of Math. 108 (1978), pp. 461-505.

[19] G. Henkin, M. Passare, *Abelian differentials on singular varieties and variation on a theorem of Lie-Griffiths*, Inventiones math. 135 (1999), pp. 297-328.

[20] M. van Hoeij, Factoring polynomials and the Knapsack problem, J. of Numb. Theory 95 (2002), pp. 167-189.

[21] E. Kaltofen, Polynomial factorization : a success story, ISSAC 03, Proceedings of the 2003 international symposium on Symbolic and algebraic computation, ACM Press, (2003), pp. 3-4.

[22] G. Lecerf, New recombination algorithms for bivariate polynomial factorization based on Hensel lifting, Applicable algebra in engineering, communication and computing 21 (2010), pp. 151-176.

[23] G. Lecerf, Sharp precision in Hensel lifting for bivariate polynomial factorization. Mathematics of Computation, 75 (2006), pp. 921-933.

[24] A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovasz, Factoring Polynomials with Rational Coefficients, Math. Ann. 261, no.2 (1982), pp. 515-534.

[25] M. Mnũk, An Algebraic Approach to Computing Adjoint Curves, J. Symbolic Computation 23 (1997), pp.229-240

[26] P. Philippon, M. Sombra, Quelques aspects diophantiens des variétés toriques projectives, Dioph. Approx. : Festschrift for Wolfgang Schmidt. Dev. Math. 16, Springer-Verlag (2008) pp. 295-338.

[27] P. Philippon, M. Sombra, A refinement of the Bernstein-Kushnirenko estimate, Adv. Math. 218 (2008), pp. 1370-1418.

[28] A. Poteaux, M. Rybowicz, Complexity Bounds for the rational Newton-Puiseux Algorithm over Finite Fields, Appl. Alg. in Eng., Comm. and Comp. 22, no 3 (2011), pp. 187-217.

[29] A. Poteaux, M. Rybowicz, Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields, ISSAC 2015, pp. 299-306.

[30] A. Schintzel, On reducible trinomials, Dissertations Mathematicae (1993), pp. 1-82.

[31] P. Stadelmeyer, F. Winkler, Computing the System of Adjoint Plane Curves by Puiseux Expansion, Tech. report 97-38 RISC Report Series, Univ. Linz, Austria (1997).

[32] M. Van Hoeij, An algorithm for computing an integral basis in an algebraic function field, J. Symb. Comput., 18 (1994), pp. 353-363.

[33] M. Weimann, An interpolation theorem in toric varieties , Annales de l'Institut Fourier 58 no.4 (2008), pp. 1371-1381.

[34] M. Weimann, A lifting and recombination algorithm for rational factorization of sparse polynomials, J. of Complexity 26 no.6 (2010), pp. 608-628.

[35] M. Weimann, Algebraic osculation and factorization of sparse polynomials, Journal of Foundation of Computational Mathematics 12 no.2 (2012), pp. 173-201.

[36] M. Weimann, Factoring bivariate polynomials using adjoints , J. of Symb. Comp. 58 (2013) pp. 77-98.

[37] M. Weimann, Bivariate factorization using a critical fiber , arXiv :1501.03011, to appear in J. of Foun. of Comp. Math (2016).

[38] J.A. Wood, *A simple criterion for an analytic hypersurface to be algebraic*, Duke Mathematical Journal 51, 1 (1984), pp. 235-237.

[39] J.A. Wood, *Osculation by Algebraic Hypersurfaces*, J. Differential Geometry 18 (1983), pp. 563-573.

[40] R. Zippel, Effective Polynomial Computation, Kluwer Academic Publishers (1993).