Tight and rigourous error bounds for basic building blocks of double-word arithmetic

Mioara Joldes Jean-Michel Muller Valentina Popescu

Most of today's numerical computations are done using floating-point (FP) formats for representing real numbers. The two most widely implemented formats defined by the IEEE 754-2008 standard [1] for FP arithmetic are *single*-precision (*binary32*) and *double*-precision (*binary64*). For some critical problems, such precisions do not suffice. Since higher precisions, such as *quad*-precision (*binary128*) is not hardware implemented on widely distributed processors, the only solution is to use software emulation for extended precision.

There are mainly two ways of representing numbers in higher precision. The first one, the *multiple-digit* method, uses integers for representing numbers as a sequence of possibly high-radix digits coupled with an exponent. The second one, the *multiple-term* method, represents real numbers as unevaluated sums of several FP numbers, allowing for computations to be carried out naturally using the underlying FP hardware level. The later one is called a *floating-point expansion* when made up with an arbitrary number of terms and it makes use of well known *error-free-transforms* algorithms such as *2Sum, Fast2Sum* and *Fast2Mult* (see [2]).

In this work we focus on the "double-double" (DD) precision, i.e., the number x is represented as the sum of two *double*-precision FP numbers, x_h+x_ℓ, the high and the low part, that satisfy $|x_\ell| \leq \frac{1}{2}ulp|x_h|$. As a matter of fact, we should better talk about "double-word" precision, since the algorithms and proofs we discuss can be used with any precision-p underlying FP format ($p = 53$ for *double*-precision). More precisely we talk about two algorithms that were first presented by Kahan et. al. in [3]. The first one (Alg. 1) computes the sum of two DD numbers and returns also a DD number. In the initial paper they claim to have a relative error bound of $2 \cdot 2^{-2p}$, but no rigorous proof is given. During our tests we observed that this bound is too optimistic, so we present here a slightly larger bound, $2^{-2p} \cdot (5 + 9 \cdot 2^{-p} + 7 \cdot 2^{-2p} + 6 \cdot 2^{-3p})$, for which we can provide a rigorous proof.

Alg. 2 computes the product of a DD number with a standard *double*-precision one and returns also a DD number. In this case we proved a tighter error bound that the one given in [3]. The initial error bound was $4 \cdot 2^{-2p}$ and we provide a proof for $2^{-2p}|xy|\left(3 + 4 \cdot 2^{-p} + 2 \cdot 2^{-2p}\right)$.

Algorithm 1 $(z_h, z_\ell) = (x_h, x_\ell) + (y_h, y_\ell)$.

1: $(s_h, s_\ell) \leftarrow \text{2Sum}(x_h, y_h)$
2: $(t_h, t_\ell) \leftarrow \text{2Sum}(x_\ell, y_\ell)$
3: $c \leftarrow \text{RN}(s_\ell + t_h)$
4: $(v_h, v_\ell) \leftarrow \text{Fast2Sum}(s_h, c)$
5: $w \leftarrow \text{RN}(t_\ell + v_\ell)$
6: $(z_h, z_\ell) \leftarrow \text{Fast2Sum}(v_h, w)$
7: **return** (z_h, z_ℓ)

Algorithm 2 $(z_h, z_\ell) = (x_h, x_\ell) * y$.

1: $(c_h, c_{\ell 1}) \leftarrow \text{Fast2Mult}(x_h, y)$
2: $c_{\ell 2} \leftarrow \text{RN}(x_\ell \cdot y)$
3: $(t_h, t_{\ell 1}) \leftarrow \text{Fast2Sum}(c_h, c_{\ell 2})$
4: $t_{\ell 2} \leftarrow \text{RN}(t_{\ell 1} + c_{\ell 1})$
5: $(z_h, z_\ell) \leftarrow \text{Fast2Sum}(t_h, t_{\ell 2})$
6: **return** (z_h, z_ℓ)

References

[1] IEEE Computer Society, *IEEE Standard for Floating-Point Arithmetic*, IEEE Standard 754-2008, Aug. 2008.

[2] J.-M. Muller, N. Brisebarre, F. de Dinechin, C.-P. Jeannerod, V. Lefevre, G. Melquiond, N. Revol, D. Stehle, and S. Torres, *Handbook of Floating-Point Arithmetic*, Birkhauser Boston, 2010.

[3] X.S.Li, J.W.Demmel, D.H.Bailey, G.Henry, Y.Hida, J.Iskandar, W.Kahan, A.Kapur, M.C.Martin, T.Tung, D.J.Yoo, *Design, Implementation and Testing of Extended and Mixed Precision BLAS*, ACM TOMS, vol. 28, no. 2, 2002.

[4] M. Joldes, J.-M. Muller, and V.Popescu, *Tight and rigourous error bounds for basic building blocks of double-word arithmetic*, https://hal.archives-ouvertes.fr/hal-01351529.

Approximations de Tchebychev rigoureuses de solutions d'équations différentielles linéaires en temps linéaire

Florent Bréhard[*•] Nicolas Brisebarre[*] Mioara Joldeș[•]

[•]LAAS-CNRS, 7 Avenue du Colonel Roche, 31077 Toulouse, France
[*]CNRS, LIP, ENS Lyon, 46 Allée d'Italie, 69364 Lyon, France
florent.brehard@ens-lyon.fr, nicolas.brisebarre@ens-lyon.fr, joldes@laas.fr

À première vue, la résolution des équations différentielles ordinaires linéaires est chose aisée : la théorie garantit l'existence et l'unicité de la solution sur tout l'intervalle de définition de l'équation et bien que l'on n'ait pas d'expression explicite de la solution générale, il existe un grand nombre d'algorithmes de résolution numérique (telles les méthodes de Runge-Kutta, de collocation, spectrales, etc.) assortis de résultats de convergence asymptotique. Néanmoins, ces résultats ne fournissent pas en général de bornes effectives de l'erreur d'approximation, qui dans certains domaines critiques tout comme dans le monde des preuves mathématiques assistées par ordinateur, sont souvent nécessaires.

Dans cette optique, une des possibilités est de recourir à des méthodes de validation *a priori*, qui construisent l'approximation et la borne d'erreur certifiée parallèlement (voir par exemple [3] pour des approximations de Taylor certifiées). Par opposition, les méthodes *a posteriori* prennent en argument une approximation de la solution et calculent *a posteriori* une borne de l'erreur. Notre contribution s'inscrit dans le cadre de cette deuxième classe et repose sur des arguments de point fixe d'opérateurs contractants [5].

Les deux outils fondamentaux que nous utilisons sont les suivants :

1. L'approximation numérique par des séries de Tchebychev tronquées pour des fonctions suffisamment régulières sur un intervalle compact donné. Guère plus compliquées à manipuler que les séries de Taylor, les séries de Tchebychev offrent de bien meilleurs résultats d'approximation que ces dernières et requièrent de surcroît des hypothèses de régularité plus faibles sur la fonction à approximer [2].
2. La reformulation des équations différentielles linéaires en équations intégrales de Volterra de seconde espèce met en évidence un opérateur intégral (défini par des multiplications et des intégrations) qui se trouve être compact et présente une structure creuse dite « quasi-bande » dans la base de Tchebychev. Cette structure de l'opérateur rend possible la résolution numérique de l'équation en temps proportionnel au degré de troncature, que ce soit par des méthodes directes d'algèbre linéaire (factorisation QR par algorithme d'Olver et Townsend [4]) ou issues de la théorie des récurrences linéaires à coefficients polynomiaux [1].

Plusieurs approches sont envisageables pour certifier des solutions numériques approchées (voir par exemple [1] pour une méthode basée sur les itérés de l'opérateur intégral). Notre algorithme est une variation autour de la méthode de Newton et consiste à faire apparaître un opérateur contractant en multipliant l'opérateur intégral par un inverse approché. Le résultat est alors proche de l'opérateur identité de sorte que la différence des deux est un opérateur contractant, ce qui nous permet de déduire un encadrement fin et rigoureux de l'erreur d'approximation. Le travail technique consiste alors à borner précisément, de manière systématique et en temps raisonnable (proportionnel au degré de troncature choisi) cette différence.

En application de cette nouvelle méthode, nous nous proposons de certifier les trajectoires de vaisseaux spatiaux dans le cadre du problème de rendez-vous en mécanique linéarisée tel que détaillé dans [6].

Références

[1] A. Benoit, M. Joldes, and M. Mezzarobba. Rigorous uniform approximation of D-finite functions using chebyshev expansions. *Mathematics of Computation*, (To appear), 2016.

[2] N. Brisebarre and M. Joldes. Chebyshev interpolation polynomial-based tools for rigorous computing. In *ISSAC '10 : Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, page 147–154, 2010.

[3] M. Neher, K. R. Jackson, and N. S. Nedialkov. On Taylor model based integration of ODEs. *SIAM J. Numer. Anal.*, 45 :236–262, 2007.

[4] S. Olver and A. Townsend. A fast and well-conditioned spectral method. *SIAM Review*, 55(3) :462–489, 2013.

[5] N. Yamamoto. A numerical verification method for solutions of boundary value problems with local uniqueness by banach's fixed-point theorem. *SIAM Journal on Numerical Analysis*, 35(5) :2004–2013, 1998.

[6] D. Arzelier, A. Théron and M. Kara-Zaitri. Étude bibliographique sur la modélisation du mouvement relatif pour le problème du rendez-vous. Note technique N.T. 2.1 Rapport LAAS 08258, CNRS, 30 Juin 2008.

On the nature of the generating series of random walks in the quarter plane

T. Dreyfus C. Hardouin J. Roques M. F. Singer

In the recent years, the nature of the generating series of the walks in the quarter plane $\mathbb{Z}^2_{\geq 0}$ has attracted the attention of many authors, see [1, 2, 5, 7, 9] and the references therein. The main questions are : are they algebraic, holonomic (solutions of linear differential equations) or at least hyperalgebraic (solutions of algebraic differential equations) ?

This problem was first considered in the seminal paper [2], where Bousquet-Mélou and Mishna attach a group to any walk in the quarter plane and make the conjecture that a walk has an holonomic generating series if and only if the associated group is finite. They proved that, if the group of the walk is finite, then the generating series is holonomic, except, maybe, in one case, which was solved positively by Bostan, van Hoeij and Kauers in [1]. In the infinite group case, Kurkova and Raschel proved in [7] that if the walk is in addition non singular, then the corresponding generating series is not holonomic. This work is very delicate, and relies on the explicit uniformization of a certain elliptic curve. Recently, it has been proved in [3], that 9 over the 51 such walks have a generating series which is hyperalgebraic. In this talk, we will prove, using the difference Galois theory, [8], see also [4, 6], that the remaining 42 walks, have a generating series which is not hyperalgebraic. In particular, we will reprove the results of [7].

Bibliography

[1] Bostan A., van Hoeij M., and Kauers M. The complete generating series function for Gessel walks is algebraic. Proceedings of the American Mathematical Society. 2010.

[2] Bousquet-Mélou M., and Mishna M. Walks with small steps in the quarter plane. Contemp. Math. 2010.

[3] Bernardi O., Bousquet-Mélou M., and Raschel K. Counting quadrant walks via Tutte's invariant method. Extended abstract of a talk at the conference FPSAC 2016.

[4] Dreyfus T., Hardouin C., and Roques J. Hypertranscendance of solutions of Mahler equations. To appear in J. Eur. Math. Soc. (JEMS). 2015.

[5] Fayolle G., Iasnogorodski, R., and Malyshev, V. Algebraic methods, boundary value problems and applications. 1999.

[6] Hardouin C., and Singer M. F. Differential Galois theory of linear difference equations. Math. Ann. 2008.

[7] Kurkova I., and Raschel K. On the functions counting walks with small steps in the quarter plane. Publications Mathématiques. Institut de Hautes Études Scientifiques. 2012.

[8] van der Put M., and Singer M. F. Galois theory of difference equations. 1997.

[9] Raschel K. Counting walks in a quadrant : a unified approach via boundary value problems. Journal of the European Mathematical Society (JEMS). 2012.

Calcul du rang de grandes matrices creuses modulo p par des méthodes d'élimination.

Charles Bouillaguet* **Claire Delaplace***†

* Université de Lille, CRIStAL
† Université de Rennes 1, Irisa

Soit p un nombre premier et $M \in \mathbb{F}_p^{n \times m}$ une matrice creuse dont on cherche à calculer le rang r. Il existe essentiellement deux grandes familles d'algorithmes pour calculer les opérations usuelles (rang, déterminant, solution d'un système linéaire) sur M : les méthodes itératives et les méthodes directes.

Les méthodes itératives, telles que l'algorithme de Wiedemann [6], fonctionnent en calculant une succession de produits matrice-vecteur, où la matrice de départ M n'est jamais modifiée. Retrouver le rang r de M nécessite généralement $\mathcal{O}(r)$ produits matrice-vecteur, dont la complexité est proportionnelle au nombre d'entrées dans la matrice. Le temps d'exécution de ces méthodes est donc prévisible, et leur avantage principal est que leur complexité en mémoire est faible.

Les méthodes directes, telles que la méthode du pivot de Gauss, sont très répandues dans le monde du calcul numérique. Leur principe est d'éliminer certaines entrées de la matrice de départ pour la mettre sous forme triangulaire. Le problème est que ce processus d'élimination produit souvent du « remplissage » ; c'est à dire que des entrées non-nulles apparaissent là où il n'y en avait initialement pas. Cela peut ralentir considérablement le processus et, dans certains cas, cela peut même conduire à un crash de mémoire. La complexité de ces algorithmes est donc assez difficile à prédire et la mémoire est souvent le facteur limitant.

En combinant des heuristiques de sélection de pivots utilisées pour le traitement de matrices issues de calcul de bases de Gröbner [4] et l'algorithme d'élimination GPLU [5] développé par Gilbert et Peierls, nous avons mis au point un nouvel algorithme [1] qui effectue une variante de la méthode du pivot de Gauss en réduisant le remplissage. Nous avons implémenté cet algorithme et nous l'avons comparé à l'algorithme d'élimination présent dans Linbox [3], ainsi qu'à une implémentation de GPLU adaptée aux corps finis. Les résultats obtenus montrent que notre nouvel algorithme est plus rapide que ces algorithmes sur les matrices de la collection SIMC de Jean-Guillaume Dumas [2], et dans certains cas, il est également plus rapide que la méthode itérative de Wiedemann. Les récentes modifications que nous avons apportées - notamment une heuristique de sélection de pivots plus élaborée - nous ont permis d'obtenir des résultats encore meilleurs.

Dans cet exposé, je présenterai cet algorithme et les améliorations qui y ont été apporté. J'illustrerai son fonctionnement sur quelques exemples.

Références

[1] C. Bouillaguet, C. Delaplace : Sparse Gaussian Elimination modulo p : An update. Proceeding of the 18th International Workshop of Computer Algebra in Scientific Computing, Bucharest, Romania, pp. 101-116, (2016).

[2] J.-G. Dumas : Sparse Integer Matrix Collection, `http://hpac.imag.fr`

[3] J.-G. Dumas, G. Villard : Computing the Rank of Sparse Matrices over Finite Fields. Proceeding of the 5th International Workshop of Computer Algebra in Scientific Computing, Yalta, Ukraine, pp. 47-62, (2002).

[4] J.-C. Faugère, S. Lachartre : Parallel Gaussian Elimination for Gröbner Bases Computations in Finite Fields. In PASCO. pp. 89-97, ACM, (2010).

[5] J. R. Gilbert, T. Peierls : Sparse Partial Pivoting in Time Proportional to Arithmetic Operations. SIAM Journal on Scientific and Statistical Computing 9 No. 5, 862-874, (1988).

[6] D.H. Wiedemann : Solving sparse linear equations over finite fields. IEE Trans. Information Theory 32 No. 1, 54-62, (1986).

Généralisation de la transformée de Fourier tronquée pour des ordres quelconques.

Robin Larrieu
Laboratoire d'informatique de l'École polytechnique (LIX)

La transformée de Fourier rapide, ou FFT [1], est un algorithme fondamental pour la multiplication de polynômes et plus généralement pour les méthodes d'évaluation-interpolation. Dans sa version classique, elle permet d'évaluer très efficacement un polynôme en n points, où n est une puissance de 2. Pour pallier au phénomène de saut que cela engendre, il existe une variante dite « transformée de Fourier tronquée (TFT) » [2].

La TFT permet d'évaluer un polynôme en $l \leq n$ points, tout en évitant de calculer certaines valeurs intermédiaires inutilisées. Ainsi, si $\mathsf{F}(n)$ désigne la complexité d'une FFT classique, une TFT de longueur $l \leq n$ peut être réalisée en $(l/n)\mathsf{F}(n) + O(n)$ opérations élémentaires dans le corps de base. La TFT permet donc de gagner jusqu'à un facteur 2 (lorsque l est de l'ordre de $n/2$), mais la formulation initiale impose à n d'être une puissance de 2. Cependant, certaines applications, en particulier dans des corps finis, nécessitent des valeurs de n plus générales. Il est donc intéressant d'étendre la TFT à des valeurs de n quelconques.

Après avoir rapidement rappelé le principe de la FFT, et celui de la TFT quand n est une puissance de 2, nous verrons un algorithme calculant la TFT et son inverse dans le cas général.

Références

[1] James W. Cooley et John W. Tukey. *An algorithm for the machine calculation of complex Fourier series*, Avril 1965.

[2] J. van der Hoeven. *The truncated Fourier transform and applications* in Proc. ISSAC 2004 (pages 290-296).

Exhaustive search of optimal formulae for bilinear maps

Svyatoslav Covanov

Finding optimal formulae for computing bilinear maps is a problem of algebraic complexity theory [3, 2, 16, 8], initiated by the discoveries of Strassen [16] and Karatsuba [9]. It consists to determine almost optimal algorithms for important problems of complexity theory, among which the well studied complexity of matrix multiplication [16, 5, 10] and the complexity of polynomial multiplication [9, 17, 15, 6].

In the field of complexity of polynomial multiplication, the first improvement over the schoolbook method came from Karatsuba [9] in 1962, who proposed a decomposition of the bilinear map corresponding to the product of two polynomials of degree 2

$$P = p_0 + p_1 X \text{ and } Q = q_0 + q_1 X.$$

The product $P \cdot Q$ requires, to be computed, 4 multiplications using the schoolbook algorithm: p_0q_0, p_1q_0, p_0q_1, p_1q_1. With the Karatsuba algorithm, the coefficients of the product $P \cdot Q$ can be retrieved from the computation of the 3 following multiplications: p_0q_0, $(p_0 + p_1)(q_0 + q_1)$, p_1q_1. In particular, Karatsuba's algorithm can be used to improve the binary complexity of the multiplication of two n-bit integers: instead of $O(n^2)$ with the naive schoolbook algorithm, we obtain $O(n^{\log_2 3})$. Then, given a degree $d > 1$, computing the minimal amount of multiplications required for the product of polynomials of degree d leads to even better complexities and produces optimal formulae for a particular product.

The main obstacle to finding optimal formulae is the fact that the decomposition of bilinear maps is known to be NP-hard [7]. Montgomery proposed in [11] an algorithm to compute such a decomposition for the particular case of polynomials of small degree over a finite field. The author takes advantage of the fact that the number of all optimal formulae is limited on a finite field. He gets new formulae for the multiplication of polynomials of degree 5, 6 and 7 over $\mathbb{F}_2$. In [12], Oseledets proposes a heuristic approach and uses the formalism of vector spaces to solve the bilinear rank problem for the polynomial product over $\mathbb{F}_2$. Later, Barbulescu et al. proposed in [1] a unified framework, developping the idea proposed by Oseledets using the vector spaces formalism, permitting the authors to compute the bilinear rank of different applications, such as the short product or the middle product over a finite field. Their algorithm allows one to generate all the possible rank decomposition of any bilinear map over a finite field. This work is the main inspiration of the current presentation.

Our work is an improvement to the algorithm introduced in [1], allowing one to increase the family of bilinear maps over a finite field for which we are able to compute all the optimal formulae. Our algorithm relies on the automorphism group stabilizing a bilinear map, seen as a vector space, and on a topological invariant of such a vector space. It can be used for proving lower bounds on the rank of a bilinear map and it has applications for improving upper bounds on the Chudnovsky-Chudnovsky algorithms [4, 14, 13]. Especially, we compute all the decompositions for the short product of polynomials P and Q modulo X^5 and the product of 3×2 by 2×3 matrices. The latter problem was out of reach with the method used in [1]: we prove, in particular, that the set of possible decompositions for this matrix product is essentially unique, up to the automorphism group.

References

[1] R. Barbulescu, J. Detrey, N. Estibals, and P. Zimmermann. *Arithmetic of finite fields: 4th International Workshop, WAIFI 2012, Bochum, Germany, July 16-19, 2012. Proceedings*, chapter Finding Optimal Formulae for Bilinear Maps, pages 168–186. Springer, 2012. doi:10.1007/978-3-642-31662-3_12.

[2] R. W. Brockett and D. Dobkin. On the optimal evaluation of a set of bilinear forms. *Linear Algebra and its Applications*, 19(3):207 – 235, 1978. doi:10.1016/0024-3795(78)90012-5.

[3] P. Bürgisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory*. Springer, 1st edition, 2010.

[4] D. Chudnovsky and G. Chudnovsky. Algebraic complexities and algebraic curves over finite fields. *Journal of Complexity*, 4(4):285 – 316, 1988. doi:10.1016/0885-064X(88)90012-X.

[5] D. Coppersmith and S. Winograd. Computational algebraic complexity editorial matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9(3):251 – 280, 1990. doi:10.1016/S0747-7171(08)80013-2.

[6] D. Harvey, J. van der Hoeven, and G. Lecerf. Even faster integer multiplication. Technical report, ArXiv, 2014. arXiv:1407.3360.

[7] J. Håstad. Tensor rank is np-complete. *Journal of Algorithms*, 11(4):644 – 654, 1990. doi:10.1016/0196-6774(90)90014-6.

[8] J. JáJá. Optimal evaluation of pairs of bilinear forms. *SIAM Journal on Computing*, 8(3):443–462, 1979. doi:10.1137/0208037.

[9] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics-Doklady*, 7:595–596, 1963. (English translation).

[10] F. Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, ISSAC '14, pages 296–303. ACM, 2014. doi:10.1145/2608628.2608664.

[11] P. Montgomery. Five, six, and seven-term Karatsuba-like formulae. *Computers, IEEE Transactions on*, 54(3):362–369, 2005. doi:10.1109/TC.2005.49.

[12] I. Oseledets. Optimal Karatsuba-like formulae for certain bilinear forms in gf(2). *Linear Algebra and its Applications*, 429(8–9):2052 – 2066, 2008. doi:10.1016/j.laa.2008.06.004.

[13] M. Rambaud. *Arithmetic of Finite Fields: 5th International Workshop, WAIFI 2014, Gebze, Turkey, September 27-28, 2014. Revised Selected Papers*, chapter Finding optimal Chudnovsky-Chudnovsky multiplication algorithms, pages 45–60. Springer, 2015. doi:10.1007/978-3-319-16277-5_3.

[14] H. Randriambololona. Bilinear complexity of algebras and the Chudnovsky–Chudnovsky interpolation method. *Journal of Complexity*, 28(4):489 – 517, 2012. doi:10.1016/j.jco.2012.02.005.

[15] A. Schönhage and V. Strassen. Schnelle multiplikation großer zahlen. *Computing*, 7(3-4):281–292, 1971. doi:10.1007/BF02242355.

[16] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356. doi:10.1007/BF02165411.

[17] A. L. Toom. The complexity of a scheme of functional elements realizing the multiplication of integers. *Soviet Mathematics Doklady*, 3:714–716, 1963. (English translation).

Nichtnegativstellensätze for Univariate Polynomials

Victor Magron[1] Mohab Safey El Din[2,3]
Markus Schweighofer[4]

Every nonnegative univariate real polynomial can be written as the sum of two polynomial squares with real coefficients. A natural question arising from this fact is the following:

Question: *Given an ordered real field K and a nonnegative univariate polynomial $f \in K[X]$, can we always write f as a (weighted) sum of squares with coefficients in K?*

A positive answer to this question was given in [Sch99, Chapter 2], together with an algorithm providing weighted sums of squares (SOS) decompositions. We first present this algorithm, denoted by `univsos1`, which relies on root isolation, quadratic approximations of positive polynomials and square-free decomposition. When $K = \mathbb{Q}$, we show that the total bitsize length of the coefficients involved in the SOS decomposition of f obtained with Algorithm `univsos1` is exponential w.r.t. the degree of f. Our complexity analysis is obtained by using of quantifier elimination and root isolation bounds.

Next, we analyze a second algorithm, denoted by `univsos2`, initially provided in [CHJL11, Section 5.2]. This algorithm provides SOS decompositions of nonnegative univariate polynomials with rational coefficients. Algorithm `univsos2` relies on root isolation of perturbed positive polynomials and square-free decomposition. We show that the total bitsize length of the coefficients involved in the SOS decomposition of f obtained with Algorithm `univsos2` is polynomial w.r.t. the degree of f. Our complexity analysis is obtained by using Vieta's formulas and root isolation bounds.

Finally, we provide comparison results for the performance of Algorithm `univsos1` and Algorithm `univsos2` on several application benchmarks.

References

[CHJL11] Sylvain Chevillard, John Harrison, Mioara Joldeş, and Christoph Lauter. Efficient and accurate computation of upper bounds of approximation errors. *Theoretical Computer Science*, 412(16):1523 – 1543, 2011.

[Sch99] Markus Schweighofer. Algorithmische Beweise für Nichtnegativ- und Positivstellensätze. Master's thesis, Diplomarbeit an der Universität Passau, 1999.

[1]CNRS Verimag; 700 av Centrale 38401 Saint-Martin d'Hères, France
[2]Sorbonne Universités, Universite Pierre et Marie Curie (Paris 6), France
[3]Joint INRIA/UPMC/LIP6 Project-Team PolSys
[4]Fachbereich Mathematik und Statistik, Universität Konstanz, 78457 Deutschland

Computer algebra for polynomial optimization: from semidefinite to hyperbolic programming

Simone Naldi*

January 5, 2017

Understanding the theoretical complexity and designing efficient exact algorithms for polynomial optimization problems is a central (and in its whole generality open) question. In the last years it has attracted lot of attention from the symbolic computation community.

Universal for polynomial optimization is the role of semidefinite programming (SDP): this class of problems consists in minimizing a linear function over the affine section of the cone of $m \times m$ positive semidefinite matrices defined by the LMI (linear matrix inequality)

$$A(X) = A_0 + X_1 A_1 + \cdots + X_n A_n \succeq 0.$$

where $\succeq 0$ means positive semidefinite, A_i are symmetric matrices and $X = (X_1, \ldots, X_n)$ is a vector of unknowns. Recent results [**?**, **?**] have shown that exploiting the geometry of the spectrahedral semialgebraic set $\mathscr{S} = \{x \in \mathbb{R}^n : A(x) \succeq 0\}$, one can compute an exact representation of a solution of the SDP in time which is essentially quadratic in the algebraic degree of SDP [**?**]. The size of the output representation (in terms of the degree of a rational parametrization) equals the algebraic degree of the given semidefinite program.

These algorithms are now implemented in a Maple library called Spectra [**?**]. The goal of the first (very short) part of the talk will be to discuss interesting examples of LMI from the literature, where the exact representation computed by Spectra gives important information about the computed solution.

The second part of the talk will focus on hyperbolic programming. A homogeneous polynomial $f \in \mathbb{R}[X]_d$, $X = (X_0, \ldots, X_n)$, is hyperbolic with respect to $e \in \mathbb{R}^{n+1}$ when $f(e) > 0$, and the polynomial $f(Te - x) \in \mathbb{R}[T]$ has only real roots (in number of d, counted multiplicities) for all $x \in \mathbb{R}^{n+1}$. This is a strong condition but holding on interesting classes of homogeneous polynomials: for example, if f admits a definite symmetric determinantal representation $f = \det(X_0 A_0 + \cdots + X_n A_n)$, A_i real symmetric, with $A(e) \succ 0$ for some e, then f is hyperbolic.

To f one can associate two convex cones. The first is the hyperbolicity cone:

$$\Lambda(f, e) = \left\{x \in \mathbb{R}^{n+1} : f(Te - x) = 0 \text{ implies } T \geq 0\right\}.$$

Computing the infimum of a linear function over $\Lambda(f, e)$ is called a hyperbolicity program HP. When $\Lambda(f, e)$ is a spectrahedral cone (*e.g.*, when $f = \det(X_0 A_0 +$

*Technische Universität Dortmund, Fakultät für Mathematik, Vogelpothsweg 87, 44227 Dortmund

$\cdots + X_n A_n)$), then the corresponding HP is a SDP. I will show that in the general case (that is, in absence of a determinantal representation for f) one can design exact algorithms to solve two different questions: (1) compute the maximum multiplicity[1] of x for $x \in \Lambda(f, e)$, and (2) represent exactly one solution of a HP. The strategy is to reduce these problems to that of computing witness points on real algebraic sets.

Finally, I will focus on a second convex set associated to f, the cone of interlacers. An interlacer for f w.r.t. e is a polynomial $g \in \mathbb{R}[X]_{d-1}$ such that $g(e) > 0$ and for all $x \in \mathbb{R}^{n+1}$, the roots of $g(Te - x)$ interlaces those of $f(Te - x)$ (that is, $\alpha_1 \leq \beta_1 \leq \alpha_2 \leq \cdots \leq \beta_{d-1} \leq \alpha_d$, with α_j, β_j roots respectively of $f(Te - x)$ and $g(Te - x)$). The set of interlacers, denoted $I(f, e)$, turns out to be a convex cone in $\mathbb{R}[X]_{d-1}$.

The choice of g interlacing f is crucial in the algorithm [**?**] to compute definite determinantal representations of f, while in [**?**], the cone of interlacers is characterized as a section of the cone of nonnegative polynomials as follows:

$$I(f, e) = \{g \in \mathbb{R}[X]_{d-1} : g\, D_e f - f\, D_e g \geq 0\}$$

where $D_e h$ is the directional derivative of h in direction e. Relaxing the relation "$g\, D_e f - f\, D_e g \geq 0$" to "$g\, D_e f - f\, D_e g$ is a sum of squares", then interlacers with prescribed properties can be computed using exact arithmetic as above. The topics of the second part of the talk are work in progress, jointly with D. Plaumann.

[1] The multiplicity of $T = 0$ as a root of $f(Te - x)$ is called the multiplicity of x

Intersections réelles entre une courbe de petit degré et une hypersurface creuse

Mohab Safey El Din Sébastien Tavenas

La règle des signes de Descartes assure qu'un polynôme réel univarié avec seulement t monôme a au plus (t-1) racines réelles positives. Il a été montré dans une série de travaux (Khovanskiĭ [4], Bihan-Sottile [3]) que le nombre de solutions réelles d'un système peut être majoré par une borne qui ne dépend pas du degré des polynômes, mais seulement du nombre de monômes qui apparaissent dans le système.

Cependant toutes ces bornes sont exponentielles en ce nombre de monômes, et on ne sait pas aujourd'hui si cette croissance exponentielle est nécessaire ou s'il pourrait être possible de trouver des bornes (par exemple polynomiales) en le nombre de monômes.

Dans l'autre direction, de nombreux petits systèmes particuliers ont été étudiés. Une succession de résultats (Li-Rojas-Wang [6], Avedaño [1], Bihan-El Hilany [2]) borne le nombre de solutions réelles pour des systèmes en deux dimensions : intersection d'une courbe creuse planaire avec une ligne ou courbe définie par un trinôme. Ainsi pour le cas planaire, Koiran, Portier et Tavenas [5], ont prouvé une une borne (polynomiale en d et t) qui majeure le nombre d'intersections entre une courbe planaire creuse (définie par un polynôme à t monômes) et une courbe de degré d. Nous voulons généraliser ce résultat à des systèmes à n dimensions. Nous proposons de montrer comment borner (par une borne polynomiale en d et t) le nombre d'intersections réelles entre une courbe de degré d et une hypersurface définie par un polynôme avec au plus t monômes.

Références

[1] Martin Avedaño. *The number of real roots of a bivariate polynomial on a line.* arXiv preprint math/0702891, 2007.

[2] Frédéric Bihan et Boulos El Hilany *A sharp bound on the number of real intersection points of a sparse plane curve with a line.* arXiv preprint arXiv :1506.03309, 2015.

[3] Frédéric Bihan et Frank Sottile. *New fewnomial upper bounds from Gale dual polynomial systems.* Moscow mathematical journal 7(3), 387–407, 2007.

[4] AG. Khovanskiĭ, *Fewnomials.* American Mathematical Society, vol. 88, 1991.

[5] Pascal Koiran, Natacha Portier et Sébastien Tavenas. *On the intersection of a sparse curve and a low-degree curve : A polynomial version of the lost theorem.* Discrete & Computational Geometry 53(1), 48–63, 2015.

[6] Tien-Yien Li, J. Maurice Rojas et Xiaoshen Wang. *Counting real connected components of trinomial curve intersections and m-nomial hypersurfaces.* Discrete & Computational Geometry 30(3), 379–414, 2003.

Dérivation de solutions d'équations différentielles par rapport aux paramètres. Une implantation en Maple

John Masse (Appedge) François Ollivier (CNRS)

La dérivation automatique de programme est une technique bien connue et dont les avantages par rapport aux méthodes de différences finies sont clairement établis. Cependant, dans certaines situations, un calcul satisfaisant nécessite de remonter à la source du problème. C'est en particulier le cas pour les solutions d'équations différentielles paramétrées. La présence de discontinuités est une circonstance agravante.

Le package Diffedge, développé par Appedge, permet de dériver des modèles décrits par des schémas-blocs en Matlab/Simulink[5]. Afin d'illustrer un article sur cette problématique un petit package Maple a été écrit, permettant de traiter des problèmes d'optimisation ou de tester l'identifiabilité des paramètres d'un modèle (*cf. e.g.* [2]).

On décrira la stratégie d'implémentation, à partir d'un résultat mathématique classique qui exprime les dérivées comme solutions d'un nouveau système[4, 1, 3, 6], les difficultés rencontrées et des situations *a priori* déroutantes, quand `evalb(N=N)` retourne `false`.

Références

[1] Bliss (Gilbert Ames), "Solutions of differential equations as functions of the constants of integration", *Bull. Amer. Math. Soc.* vol.25 , 15–26, 1918.

[2] Dubois (François), textescLe Meur (Hervé V.J.) et Reiss (Claude), « Mathematical modeling of antigenicity for HIV dynamics », *MathematicS In Action*, **3**, (1), 1–35, 2010.

[3] Grönwall (Thomas Hakon), "Note on the Derivatives with Respect to a Parameter of the Solutions of a System of Differential Equations", *Annals of Mathematics*, Second Series, Vol.20, No. 4, pp. 292–296, 1919.

[4] Jacobi (Carl Gustav Jacob), "De investigando ordine systematis aequationum differentialum vulgarium cujuscunque", Gesammelte Werke V, 193-216. "The order of a system of ordinary differential equations", *AAECC*, **20**, (1), 7–32, 2009.

[5] Masse (John) and Cambois (Thierry), "Differentiation, sensitivity analysis and identification of hybrid Models under Simulink", *Symposium Techniques Avancéeés et Stratégies Innovantes en Modélisation et Commandes Robustes des Processus Industriels*, Martigues, 21 & 22 septembre 2004.

[6] Ritt (Joseph Fels), "On the differentiability of the solution of a differential equation with respect to a parameter", *Ann. of Math.* vol. 20, 289–291, 1919.

OpenDreamKit – The EU is actually paying to develop open source CAS's!

Luca De Feo

OpenDreamKit is a H2020 European project entering its 2nd year. Behind the acronym (Digital Research Environment Toolkit for the Advancement of Mathematics) thrives a consortium of 16 universities and industrial partners, working together for the advancement of some of the most popular open source software for pure mathematics (LinBox, MPIR, SageMath, GAP, PARI/GP, LMFDB, Singular, MathHub, IPython/Jupyter, ...)

In this presentation I will briefly present the structure of the consortium, then I will demo some of the newest tools developed by OpenDreamKit in collaboration with the open source community.

`http://opendreamkit.org`

Formules de Thomae généralisées aux courbes résolubles sur $\mathbb{P}^1$

A. Fiorentino, A. Le Meur et D. Lubicz

16 Janvier 2017

À une courbe projective lisse sur $\mathbb{C}$, on peut lui associer sa jacobienne J. C'est une variété algébrique mais possédant également une structure de groupe. On dit que c'est une variété abélienne. Une bonne manière de décrire ces variétés abéliennes est d'utiliser des fonctions θ comme coordonnées projectives. Les coordonnées du point neutre de A sont appelés θ *constantes*. D'un point de vue modulaire, ces θ constantes caractérisent la variété abélienne A. Des relations algébriques existent entre ces θ constantes et fournissent des équations de A. On connaît une caractérisation des jacobiennes de courbes hyperelliptiques au moyen des équations de Frobenius. Plus généralement, ces relations peuvent être utilisées en vue de résoudre le problème de Schottky, c'est-à-dire de caractériser les variétés jacobiennes parmi les variétés abéliennes. Pour les courbes hyperelliptiques, on connaît des formules permettant de relier les points de ramification de la courbe aux θ constantes. Il s'agit des *formules de Thomae*. Ces formules ont connu un regain d'intérêt, particulièrement dans la communauté des physiciens, vers la fin des années 80. Ainsi, Bershadsky et Radul [1] ont généralisé ce type de formules pour les courbes cycliques sur $\mathbb{P}^1$ ayant un modèle affine non singulier. En 1997, Nakayashiki [2] propose une réécriture plus mathématique de leurs travaux. Plus récemment, Farkas et Zemel ont proposé [3] une méthode plus géométrique pour calculer des formules de Thomae pour ces courbes cycliques. En 2013, Zemel écrit dans un article non publié [4] une généralisation de ces méthodes pour traiter le cas des courbes cycliques totalement ramifiées sur $\mathbb{P}^1$. Notre travail généralise cette construction au cas des courbes résolubles sur $\mathbb{P}^1$. Pour cela, nous écrivons notamment une version « galoisienne »d'un théorème de Riemann permettant de relier les zéros d'un translaté de θ avec le point par lequel on a translaté.

Références

[1] Bershadsky, M. and Radul, A., Fermionic fields on $\mathbb{Z}_N$-curves, Communications in mathematical physics, vol.116, n 4, p.689-700, Springer, 1988

[2] Nakayashiki, A., On the Thomae formula for $\mathbb{Z}_N$ curves, Publications of the Research Institute for Mathematical Sciences, vol.33, n 6, p.987-1015, 1997

[3] Farkas, H.M. and Zemel, S., Generalizations of Thomae's Formula for $\mathbb{Z}_n$ Curves, Developments in Mathematics, Springer New York, 2010

[4] Zemel, S., Thomae Formulae for General Fully Ramified $\mathbb{Z}_n$ Curves, arXiv preprint arXiv :1311.4717, 2013

Solutions rationnelles d'équations de Mahler linéaires

Philippe Dumas, Inria Saclay

5 janvier 2017

De même que les équations différentielles utilisent comme opérateur de base une dérivation, de même les équations de Mahler emploient l'opérateur de substitution $f(x) \mapsto f(x^b)$. Elles ont été introduites par Kurt Mahler à la fin des années 1920 pour prouver des résultats de transcendance. Si la base de numération b est un nombre premier p qui est aussi la caractéristique du corps de base, elles se révèlent être des équations algébriques et sont liées à des automates qui se nourrissent de l'écriture en base p des entiers. Ces équations sont aussi liées à l'étude de la complexité des algorithmes de type diviser pour régner ou encore à certains problèmes de combinatoire des mots ou des partitions d'entiers.

La méthode de Mahler pour la transcendance est restée très vivante et a conduit récemment au besoin de résoudre des équations de Mahler. Nous nous concentrons dans cette présentation sur la recherche des solutions rationnelles à coefficients dans un corps de nombres, même si nous avons aussi étudié la recherche des solutions séries formelles, polynômes ou séries de Puiseux. Une des difficultés dans l'étude de ces équations est l'explosion en degré qui apparaît dès que l'on applique l'opérateur de Mahler à des polynômes. Les méthodes classiques pour les équations aux différences ne s'appliquent pas directement parce qu'il s'avère nécessaire de remplacer la structure linéaire des entiers par une structure arborescente. Nous montrons qu'il est possible de bâtir un algorithme de résolution rationnelle dont la complexité est polynomiale par rapport à la taille du résultat.

Ce travail est un travail commun avec Frédéric Chyzak (Inria Saclay), Thomas Dreyfus (Université Lyon 1) et Marc Mezzarobba (CNRS, Lip6).

On the Formal Reduction of Linear Singular Differential Systems

Joelle Saadé

16-20 Janvier 2017, JNCF

We present a new algorithm of formal reduction of first order systems of differential equations with singularities of pole type at the origine:

$$[A] : Y' = A(x)Y, \tag{1}$$

where A is an n-dimensional formal meromorphic power series matrix over a field $k \subset \mathbb{C}$.

The *formal reduction* refers here to the process of splitting the given system of dimension n into subsystems of smaller dimension using formal *gauge transformation* $Y = PZ$ where $P \in GL_n(\overline{k((x))})$.
We say that $[A]$ is decomposable over $k((x))$ if there exists $P \in GL_n(k((x)))$ such that :

$$P[A] := P^{-1}AP - P^{-1}P' = \begin{pmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_m \end{pmatrix} \tag{2}$$

where $m \geq 2$ and B_i is a square matrix of size $n_i < n$. We know from [3] that such a transformation P can be constructed using a suitable element in $\mathscr{E}_{k((x))}$, the local eigenring of $[A]$ defined as:

$$\mathscr{E}_{k((x))}([A]) = \{T \in \mathscr{M}_n(k((x))/T' = AT - TA\}.$$

Algorithms for computing $\mathscr{E}_{k((x))}([A])$ exist (see [2]).
Our approach consists in first computing a *maximal decomposition* of $[A]$ over $k((x))$, which means that each sub-system $[B_i]$ in (2) is indecomposable over $k((x))$; we then proceed by trying to decompose each sub-system $[B_i]$ over a suitable algebraic extension of $k((x))$, to be determined. It turns out that it is sufficient to look for solutions of the equation $T' = B_iT - TB_i$ of the form $T = x^\alpha \sum_{i\geq 0} x^i T_i$ with $\alpha = \frac{m}{s} \in \mathbb{Q}$. Once we find such a T, we consider the ramification $x = t^s$ in order to obtain a more refined decomposition. We note that this decomposition corresponds to the structure of the formal fundamental matrix solution of system $[A]$ (see [1]). Hence we will discuss how we can recover the exponential parts of the system.

References

[1] H. L. Turrittin, *Convergent solutions of ordinary linear homogeneous differential equations in the neighborhood of an irregular singular point.* Acta Math., vol. 93, 1995, pp.27-66.

[2] M. A. Barkatou and E. Pflügel, *An algorithm computing the regular singular formal solutions of a linear differential system*. In Journal of Symbolic Computation 28(4-5), 1999.

[3] M. A. Barkatou, *Factoring Systems of Linear Functional Systems Using Eigenrings*. Computer algebra 2006, 22–42, World Sci. Publ., Hackensack, NJ, 2007.

Problème du centre isochrone et correction de champs de vecteurs

Jordy Palafox

Dans cet exposé, je présenterai de nouveaux résultats obtenus avec Jacky Cresson (UPPA) sur les systèmes différentiels Hamiltoniens polynomiaux du plan réel dont la partie linéaire est un centre (voir [2]). En particulier, on s'intéressera aux centres isochrones.

Notre principal problème est la conjecture énoncée par Jarque et Villadelprat dans [5] :
Soit X un champ de vecteurs Hamiltonien polynomial réel de la forme :

$$X = -\partial_y(H)\partial_x + \partial_x(H)\partial_y,$$

où H est un polynôme réel en les variables réelles x et y. Le degré maximal des polynômes $\partial_x(H)$ et $\partial_y(H)$ est le degré du champ de vecteurs Hamiltonien.

Conjecture 1. *Il n'existe pas de système Hamiltonien polynomial de degré pair dans le plan réel qui soit isochrone.*

On sait que la conjecture est vraie pour les systèmes quadratiques grâce aux résultats de Loud (voir [7]). Jarque et Villadelprat ont montré que le cas quartique est aussi vérifié. Mais la conjecture est toujours ouverte en dépit des résultats partiels obtenus par B.Schuman dans [9]. La preuve de Jarque et Villadelprat est basée sur l'étude approfondie des ensembles de bifurcations et semble difficile à étendre en degré supérieur.

En utilisant le formalisme des moules introduit par Jean Ecalle (voir [3]) et en particulier un objet attaché à un champ de vecteurs, la *correction*, qui est définie par Ecalle et Vallet dans [4] on obtient une réponse partielle à la conjecture en degré quelconque. Il est bien connu que l'isochronisme d'un centre réel est équivalent à la linéarisabilité (voir [1], Théorème 3.3 p.12). Une des principales propriétés de la correction est qu'elle donne un critère pratique de linéarisation. En effet, un champ de vecteurs est linéarisable si et seulement si sa correction est nulle. Comme la correction possède une forme algorithmique et explicite qui est facile à calculer en utilisant le calcul moulien, on est capable de donner plus d'informations sur l'ensemble des conditions d'isochronisme. En particulier, en utilisant la représentation complexe (voir [6]) d'un champ de vecteurs réel, on obtient :

Théorème 1. *Soit X un champ de vecteurs Hamilonien réel de degré $2n$ de la forme :*

$$X = i(x\partial_x - \bar{x}\partial_{\bar{x}}) + \sum_{j=1}^{2n}(P_j(x,\bar{x})\partial_x + \overline{P(x,\bar{x})}\partial_{\bar{x}}),$$

pour $x \in \mathbb{C}$, avec $P_j(x,\bar{x}) = \sum_{k=0}^{j} p_{j-k-1}x^{j-k}\bar{x}^k$. Si X satisfait une des conditions suivantes :
a) il existe un entier r, $1 \leq r < n-1$ tel que $p_{j,j} = 0$ pour $j = 1, ..., r$ et $p_{r,r} > 0$,
b) $p_{j,j} = 0$ pour $j = 1, ..., n-1$,
Alors le champ de vecteurs X n'est pas isochrone.

Le fait que les champs de vecteurs Hamiltonien homogênes sont non-isochrones (voir [8]) se déduit facilement de notre preuve.
Dans cet exposé, je donnerai en particulier les principales étapes de la preuve.

Références

[1] J.Chavarriga and M.Sabatini. A survey of isochronous centers. *Qualitative Theory Of Dynamical Systems*, 1 :1-70, 1999.

[2] J.Cresson and J.Palafox. Isochronous centers of polynomial Hamiltonian systems and a conjecture of Jarque and Villadelprat. Version Arxiv : `https://arxiv.org/pdf/1605.07775.pdf`. Soumis.

[3] J.Ecalle. Les fonctions résurgentes, Tome I, II et III. *Publications Mathématiques d'Orsay*, 81, Vol 5. Université de Paris-Sud, Dépatement de Mathématiques, Orsay, 1981-1985.

[4] J.Ecalle et B.Vallet. Correction and linearization of resonant vector fields and diffeomorphisms. *Math. Z.*, 229 :249-318, 1998.

[5] X.Jarque and J.Villadelprat. Nonexistence of isochronous centers in planar polynomial Hamiltonian systems of degree four. *Journal of Differential Equations*, 259 :1649-1662, 2015.

[6] J.Llibre and V.G.Romanoski. Isochronicity and lineariability of planar polynomial Hamiltonian systems. *Journal of Differential Equations*, 259 :1649-1662, 2015.

[7] W.S.Loud. Behaviour of the period of solutions of certain planar autonomous systems near centers. *Contibutions to Differential Equations*, 3 :21-36, 1964.

[8] B.Schuman. Sur la forme normale de Birkhoff et les centres isochrones. *C.R. Acad. Sci. Paris*, 322 :21-24, 1996.

[9] B Schuman. Une classe d'Hamiltoniens polynomiaux isochrones. *Canad. Math. Bull.*, Vol.44(3), 323-334, 2001.

An effective approach for the stabilization of a class of multidimensional systems

Yacine Bouzidi

A multidimensional system (also called n-D systems) is a system in which information propagates in more than one independent direction (usually the time axis for standard 1-D systems). Multidimensional systems naturally arise in the study of partial difference equations, differential time-delay systems, partial differential equations, images, filters ... Within the fractional representation approach, the study of these systems relies on computations with matrices having entries in the integral domain of rational fractions with no poles in the closed unit polydisc i.e. $\overline{\mathbb{U}}^n = \{z = (z_1, \ldots, z_n) \in \mathbb{C}^n \mid |z_1| \leq 1, \ldots, |z_n| \leq 1\}$ ..

A fundamental problem in the synthesis of n-D systems is the stabilization problem (i.e. construction of a stabilizing control). Within the above algebraic framework, this problem translates as follows :

Given an ideal $I := \langle p_1, \ldots, p_r \rangle \subset \mathbb{Q}[z_1, \ldots, z_n]$, check that

$$V_{\mathbb{C}}(I) = \{z \in \mathbb{C}^n \mid p_1(z) = \cdots = p_r(z) = 0\} \cap \overline{\mathbb{U}}^n = \emptyset,$$

and if so, compute a polynomial $s \in I$ such that

$$V(s) \cap \overline{\mathbb{U}}^n = \emptyset.$$

Provided that the variety $V_{\mathbb{C}}(I)$ is devoid from zeros in the closed unit polydisc, the existence as well as the computation of the polynomial s is known as the *Polydisk nullstelensatz problem* and no constructive proof is given so far in the literature. In the present talk, we are going to present an effective proof together with an algorithm for the computation of such a polynomial in the specific case of zero-dimensional ideal, i.e. $\sharp V_{\mathbb{C}}(I) < \infty$

Private Multi-party Matrix Multiplication and Trust Computation

Jean-Guillaume Dumas, Pascal Lafourcade, Jean-Baptiste Orfila
Maxime Puys

In this talk, we present new results on secure distributed matrix multiplication. Each player owns only one row of both matrices and wishes to learn about one distinct row of the product matrix, without revealing its input to the other players. We first improve on a weighted average protocol, in order to securely compute a dot-product with a quadratic volume of communications and linear number of rounds. We also propose a protocol with five communication rounds, using a Paillier-like underlying homomorphic public key cryptosystem, which is secure in the semi-honest model or secure with high probability in the malicious adversary model. Using ProVerif, a cryptographic protocol verification tool, we are able to check the security of the protocol and provide a countermeasure for each attack found by the tool. We also give a randomization method to avoid collusion attacks. As an application, we show that this protocol enables a distributed and secure evaluation of trust relationships in a network, for a large class of trust evaluation schemes.

References

[Amirbekyan and Estivill-Castro, 2007] Amirbekyan, A. and Estivill-Castro, V. (2007). A new efficient privacy-preserving scalar product protocol. In *AusDM 2007*, volume 70 of *CRPIT*, pages 209–214.

[Batir, 2011] Batir, N. (2011). Sharp bounds for the psi function and harmonic numbers. *Mathematical inequalities and applications*, 14(4).

[Ben-Or et al., 1988] Ben-Or, M., Goldwasser, S., and Wigderson, A. (1988). Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *STOC'88*. ACM.

[Benaloh, 1994] Benaloh, J. (1994). Dense probabilistic encryption. In *SAC'94*.

[Bendlin et al., 2011] Bendlin, R., Damgård, I., Orlandi, C., and Zakarias, S. (2011). Semi-homomorphic encryption and multiparty computation. In *EUROCRYPT'11*, LNCS.

[Blanchet, 2001] Blanchet, B. (2001). An efficient cryptographic protocol verifier based on prolog rules. In *IEEE CSFW'01*.

[Blanchet, 2004] Blanchet, B. (2004). *Cryptographic Protocol Verifier User Manual*.

[Chaum et al., 1986] Chaum, D., Evertse, J., van de Graaf, J., and Peralta, R. (1986). Demonstrating possession of a discrete logarithm without revealing it. In *CRYPTO'86*.

[Damgård et al., 2012] Damgård, I., Pastro, V., Smart, N., and Zakarias, S. (2012). Multiparty computation from somewhat homomorphic encryption. In *CRYPTO'12*, LNCS. Springer.

[Delaune, 2006] Delaune, S. (2006). An undecidability result for agh. *Theor. Comput. Sci.*

[Dolev et al., 2010] Dolev, S., Gilboa, N., and Kopeetsky, M. (2010). Computing multi-party trust privately: in $O(n)$ time units sending one (possibly large) message at a time. In *SAC'10*. ACM.

[Du and Atallah, 2001] Du, W. and Atallah, M. J. (2001). Privacy-preserving cooperative statistical analysis. In *ACSAC '01*, pages 102–110.

[Du and Zhan, 2002] Du, W. and Zhan, Z. (2002). A practical approach to solve secure multi-party computation problems. In *NSPW'02*. ACM.

[Dumas and Hossayni, 2012] Dumas, J.-G. and Hossayni, H. (2012). Matrix powers algorithm for trust evaluation in PKI architectures. In *STM'12, ESORICS 2012*, LNCS.

[Foley et al., 2010] Foley, S. N., Adams, W. M., and O'Sullivan, B. (2010). Aggregating trust using triangular norms in the keynote trust management system. In *STM'2010*.

[Fousse et al., 2011] Fousse, L., Lafourcade, P., and Alnuaimi, M. (2011). Benaloh's dense probabilistic encryption revisited. In *AFRICACRYPT'11*.

[Goethals et al., 2005] Goethals, B., Laur, S., Lipmaa, H., and Mielikäinen, T. (2005). On private scalar product computation for privacy-preserving data mining. In *ICISC'04*, LNCS. Springer.

[Guha et al., 2004] Guha, R. V., Kumar, R., Raghavan, P., and Tomkins, A. (2004). Propagation of trust and distrust. In *WWW'2004*.

[Huang and Nicol, 2010] Huang, J. and Nicol, D. M. (2010). A formal-semantics-based calculus of trust. *IEEE Internet Computing*.

[Jøsang, 2007] Jøsang, A. (2007). Probabilistic logic under uncertainty. In *CATS'2007*.

[Lafourcade and Puys, 2015] Lafourcade, P. and Puys, M. (2015). Performance evaluations of cryptographic protocols verification tools dealing with algebraic properties. In *FPS'15*.

[Lindell, 2009] Lindell, Y. (2009). Secure computation for privacy preserving data mining. In *Encyclopedia of Data Warehousing and Mining, Second Edition 4 Volumes)*. IGI Global.

[Michalas et al., 2012] Michalas, A., Dimitriou, T., Giannetsos, T., Komninos, N., and Prasad, N. R. (2012). Vulnerabilities of decentralized additive reputation systems regarding the privacy of individual votes. *Wireless Personal Commnications*, 66(3):559–575.

[Mohassel, 2011] Mohassel, P. (2011). Efficient and secure delegation of linear algebra. *IACR Cryptology ePrint Archive*.

[Ozarow and Wyner, 1984] Ozarow, L. H. and Wyner, A. D. (1984). Wire-tap channel II. In *EUROCRYPT'84*.

[Paillier, 1999] Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT'99*.

[Yao, 1982] Yao, A. C. (1982). Protocols for secure computations. *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*.

Une mise en revue des couplages

Razvan Barbulescu

Les applications bilinéaires non-dégénérées sont des outils importants pour les protocoles cryptographiques récents comme l'échange de clé tripartite. Avec les applications bilinéaires associées aux réseaux euclidiens, les couplages de Weil sont les seules constructions qui peuvent être calculées en rapidement et dont l'inversion est difficile.

Pour une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$, un entier r et un point rationnel $P \in E$ d'ordre r on définie le couplage de Weil (restreint au sous-groupe engendré par P) par

$$\begin{array}{rccc} e_{E,r,P,\mu}: & \frac{\mathbb{Z}}{r\mathbb{Z}}P \times \frac{\mathbb{Z}}{r\mathbb{Z}}P & \to & \mu^{\mathbb{Z}/r\mathbb{Z}} \\ & ([a]P, [b]P) & \mapsto & \mu^{ab}, \end{array}$$

où μ est une racine $r$ème de l'unité dans la clôture algébrique de $\mathbb{F}_q$. Les couplage de Weil restreint à $\mathbb{Z}$P est aussi une forme bilinéaire symétrique non-dégénérée, donc offre une définition alternative pour le même objet, modulo un changement éventuel de μ. Le couplage de Weil se calcule en temps polynomial alors que les meilleurs attaques consiste à résoudre calculer a soit à partir de $[a]P$ (problème du logarithme discret(DLP) sur les courbes elliptiques) soit à partir de μ^a (problème des logarithmes discrets dans les corps finis).

On appelle degré de plongement d'un couplage associé à $E/\mathbb{F}_q$ et r le plus petit k tel que Φ_r a une racine dans $\mathbb{F}_{q^k}$. La proportion des paires $E/\mathbb{F}_q$ et r avec un petit degré de plongement étant très faible, elles ne peuvent pas être construite en choisissant des courbes au hasard et en calculant leur k. Mise à part une famille peu utilisée, les familles de couplages sont des solutions du système d'équations CM, et demande d'utiliser la méthode CM. On obtient ainsi cinq types : supersingulières, Cocks-Pinch, Dupond-Enge-Morain, creuse (ex. MNT) et complètes(ex. BN). Le seul type qui permet de produire un nombre considérable de couplages à la volée est le dernier.

La sécurité des couplages a été estimée sous une hypothèse : le logarithme discret dans les corps finis est aussi dur que la factorisation d'un module RSA. En effet, le meilleur algorithme pour calculer de tels logarithmes discrets est le crible algébrique (NFS), une version de l'algorithme utilisé également pour factoriser des modules RSA. Cet algorithme a une version plus rapide, appelée SNFS, pour factoriser des nombres de forme spéciale : $P(u)$ avec u entier et $P \in \mathbb{Z}[x]$ de degré donné et $\|P\|_\infty$ inférieur à une constante absolue.

SNFS n'a pas été adapté au cas du logarithme discret dans des corps $\mathbb{F}_{q^k}$ avec $k \neq 1$ avant 2013, quand Joux et Pierrot ont proposé un algorithme de même complexité asymptotique que la version SNFS pour la factorisation. Néanmoins cet algorithme a été considéré comme non-pratique et les recommandations des tailles n'ont pas été changées.

En collaboration avec Pierrick Gaudry et Thorsten Kleinjung [BGK15] nous avons réhabilité un algorithme d'Oliver Schirokauer, appelé le crible algébrique

des tours d'extensions. Cette version a été également considérée comme non-pratique. Par une deuxième collaboration avec Taechan Kim [KB16] nous avons combiné cette version avec celle de Joux-Pierrot et nous obtenons une méthode pratique, qui demande de changer les tailles des clés.

Références

[Bar16] Razvan Barbulescu. A brief history of pairings. In *International Workshop on the Arithmetic of Finite Fields WAIFI 2016*, volume 10064 of *Lecture Notes in Comput. Sci.*, Gand, Belgium, 2016. Université de Gand, Springer.

[BGK15] Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung. The Towed Number Field Sieve. In *Advances in Cryptology – ASIACRYPT 2015*, volume 9453 of *Lecture Notes in Comput. Sci.*, pages 31–55, 2015.

[KB16] T. Kim and R. Barbulescu. Extended tower number field sieve : A new complexity for medium prime case. In *Advances in Cryptology – CRYPTO 2016 (part 1)*, volume 9815 of *Lecture Notes in Comput. Sci.*, pages 543–571, 2016.