# The computational complexity of polynomial factorization

organized by
Shuhong Gao, Mark van Hoeij, Erich Kaltofen, and Victor Shoup

Workshop Summary

## *Introduction*

*The Mathematics.*

It is a classical theorem of mathematics that polynomials admit unique factorization. In particular, one has:

If $D$ is a unique factorization domain (UFD), then $D[x_1, \ldots, x_n]$ is a UFD.

The above theorem is applied to many coefficient domains. Examples are: $D = \mathbb{Z}$ (the integers), $\mathbb{Q}$ (the rational numbers), $\mathbb{R}$ (the real numbers), $\mathbb{C}$ (the complex numbers), $\mathbb{Z}_p$ (integer residues modulo $p$), $\mathbb{F}_q$ (finite fields of $q$ elements), $\mathbb{Q}[\alpha]/(g(\alpha))$ (algebraic numbers), $\mathbb{Q}_p$ (p-adic numbers), $K[[t]]$ (power series), $K((t))$ (extended power series), $\mathbb{C}^*(t)$ (Puiseux series), $\mathbb{F}_q(t)[\alpha]/(g(t, \alpha))$ (a global field).

Already Isaac Newton in his Arithmetica Universalis gives an algorithm for computing irreducible factors in $\mathbb{Z}[x]$. Well-known mathematicians, among them Legendre, Gauss, and Kronecker, have made contributions. With the rise of computers, the question arose how feasible and practical the algorithms for factoring polynomials are.

*Computer Science Theory.*

It turns out that for most coefficient domains, polynomial factorization can be carried out in polynomial-time. The very first results are summarized in the following theorem.

Factorization in $\mathbb{Z}_p[x]$ and $\mathbb{F}_q[x]$ [**?**, **?**] and $\mathbb{Q}[x]$ [**?**] is polynomial-time.
If factorization in $K[x]$ is polynomial-time, then factorization in $K[x_1, \ldots, x_n]$ is polynomial-time [**?**].
Factorization in $\mathbb{Q}[\alpha]/(g(\alpha))$ is polynomial-time [**?**, **?**].
Factorization in $\mathbb{C}[x_1, \ldots, x_n]$ is polynomial-time given a suitable representation of the algebraic number coefficients [**?**, **?**].

Since then, many researchers have contributed more efficient algorithms, both in the asymptotic complexity sense (sequential and parallel) and in the sense of practical implementations.

## *Subject of Workshop*

Many of the participants have contributed recent theoretical and practical progress for the polynomial factoring problem. The following categorization of the different aspects of the factorization problem was given by the author in his introduction on May 15.

**Types of algorithm:** Both deterministic and probabilistic algorithms are investigated. A classical open problem is that of factoring in $\mathbb{Z}_p[x]$ in deterministic polynomial-time in $\log p$. The two talks on May 16 by Ming-Deh Huang and Shuhong Gao disussed the state-of-the art and possible approaches to its resolution.

In addition, parallel algorithms were discussed by Jan Verschelde's on May 17. Numerical algorithms are discussed below (see "coefficient representation").

**Data structures representing polynomials:** Polynomials can be represented by a list of coefficients (dense representation), or by a list of terms (sparse; lacunary; "super"sparse; "fewnomials") or by straight-line programs and black-box evaluation programs. The workshop discussions addressed hardness results for sparse polynomials (see "complexity analysis" below).

**Complexity analyses:** The complexities of the asymptotically fastest known algorithms for factoring in $\mathbb{F}_q[x]$ [**?**, **?**] and $\mathbb{K}[x, y]$ [**?**, **?**, **?**] were discussed, the latter in Gregoire Lecerf's talk on May 15. A proof for polynomial-time complexity of the practical algorithm for factoring in $\mathbb{Z}[x]$ [**?**, **?**] was presented by Mark van Hoeij in May 15.

Some problems for polynomial factorization are NP-hard. Jintai Ding mentioned at the workshop a result in [**?**], which shows that computing a root in $\mathbb{F}_q$, i.e., a linear factor, of a sparse polynomial

$$\sum_{i,j=0}^{n-1} a_{i,j} x^{p^i+p^j} + \sum_{k=0}^{n-1} b_k x^{p^k} + c \in \mathbb{F}_q[x], q = p^n \tag{1}$$

is NP-hard. This result sheds light on the open problems stated at the end of [**?**]. Note that over $\mathbb{Q}$, there are polynomial-time algorithms [**?**].

**Coefficient representations:** Multivariate polynomials with complex coefficients factor only if the input coefficients satisfy certain algebraic constraints, the Noether irreducibility forms. Errors in the coefficients due to floating point round-off or through physical measurement thus render the input polynomials irreducible. By symbolic-numeric methods one computes minimal deformations of the coefficients that yield non-trivial results. Kosaku Nagasaka's talk on May 17 discussed the computation of lower bounds on the minimal deformation required to yield reducibility. Four authors (Shuhong Gao, John May, Erich Kaltofen and Lihong Zhi) of the state-of-the-art approximate factoring algorithm [**?**] met at the conference.

When factorization of polynomials with coefficients from a power series domain $K[[t]]$ is performed, the results again are approximations, namely initial jets of the series. Maki Iwami's talk on May 18 covered her recent Ph.D. thesis on this subject.

The last talk by Michael Mossinghoff on May 18 covered questions in enumerative mathematics (Barker sequences) in their relations to polynomial factorization problems. He also reminded us of Lehmer's problem on the Mahler measure of a non-cyclotomic polynomial.

## *Progress Achieved at Workshop*

The ARCC workshop format required a large percentage of discussion time. Interaction has led to a substantial list of problems that are still unresolved. Werner Krandick offered a problem on addition chains for integer vectors and made a conjecture that Horner's scheme was optimal, which was disproved by an example given by the graduate student Andrew

Novocin. As stated above (see "complexity analysis") the results by [**?**] were brought to light. In addition, Dan Bernstein informally presented his essentially linear algorithm for computing GCD-free (co-prime) bases. Numerous other subjects were discussed and intitial investigation initiated. In fact, the ARCC workshop format with a limited time for talks turned out more successful than I had expected.

## *A Selection of Open Problems*

Many problems were raised, and I give a selection of well-formed problems.

*Dense polynomials over $\mathbb{F}_q$.*

Several open problems concerning deterministic polynomial-time complexity were posed in an earlier ARCC workshop, see "Problems" at http://www.aimath.org/WWN/primesinp/.

The fastest randomized algorithm for factoring a degree $d$ polynomial in $\mathbb{F}_q[x]$, where $q = d^{O(1)}$, requires $O(d^{1.81})$ bit operations [**?**]. The problem is to lower the exponent by a non-negligible amount, say to 1.75.

The fastest randomized algorithm for factoring a polynomial in $\mathbb{F}_q[x, y]$ of total degree $d$, where $q = d^{O(1)}$, requires $d^{3+o(1)}$ bit operations [**?**]. The problem is to lower the exponent below 3.

*Dense polynomials over $\mathbb{Q}$ and algebraic extensions of $\mathbb{Q}$.*

The analysis in [**?**] is worst case, but Mark van Hoeij suggests that the "gradual feeding" technique completes much faster. The problem is to derive a better worst case exponent.

A related question is on the complexity for factoring an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ over $\mathbb{Q}(\alpha)/(f(\alpha))$. The state-of-the-art seems the algorithm [**?**].

Dan Bernstein reminded us that the worst case complexity of integer lattice basis reduction is not know to be $l^{1+o(1)}$, where $l$ is the number of digits in the input.

*Dense polynomials over algebraically closed fields.*

The analysis in [**?**] does not cover fields of small characteristic. The problem is to apply Gao's techniques also to that case.

*Sparse polynomials.*

Jingtai Ding asked the question if there are sufficiently large subclasses of polynomials of the type (1) on page 2 whose roots (or a proof that they have none) can be computed in $(\log q)^{O(1)}$. In [**?**] we have posed the more concrete problem of finding roots in $\mathbb{F}_q$ of trinomials.

Victor Miller asked if there are irreducibility certificates for sparse polynomials in $\mathbb{F}_q[x]$ that can be verified faster than running the best factoring algorithm.

We add that the generalization of the algorithm in [**?**] to supersparse polynomials in $n$ variables has recently been accomplished [**?**].

*Approximate factorization.*

A polynomial-time solution to Problem 1 in [**?**] remains open. However, good numerical algorithms are available (see [**?**] and the literature cited there).

Design a hybrid symbolic-numeric algorithm that computes the nearest polynomial $\tilde{f}$ to $f \in \mathbb{C}[x, y]$ with $\deg(\tilde{f}) \leq \deg(f)$ and so that $\tilde{f}$ has all linear factors.

**Bibliography**

[Be04] Belabas, Karim. A relative van Hoeij algorithm over number fields. *J. Symbolic Comput.*, 37(5):641–668, 2004.

[BvHKS04] Belabas, K., van Hoeij, M., Klueners, J., and Steel, A. Factoring polynomials over global fields. Available from `http://www.math.fsu.edu/~hoeij/papers.html`, 2004.

[Ber67] Berlekamp, E. R. Factoring polynomials over finite fields. *Bell Systems Tech. J.*, 46:1853–1859, 1967. Republished in revised form in: E. R. Berlekamp, *Algebraic Coding Theory*, Chapter 6, McGraw-Hill Publ., New York, 1968.

[Ber70] Berlekamp, E. R. Factoring polynomials over large finite fields. *Math. Comp.*, 24: 713–735, 1970.

[BLSSW04] Bostan, A., Lecerf, G., Salvy, B., Schost, Éric, and Wiebelt, B. Complexity issues in bivariate polynomial factorization. In ISSAC04, pages 42–49.

[ChGr82] Chistov, A. L. and Grigoryev, D. Yu. Polynomial-time factoring of multivariable polynomials over a global field. LOMI Preprints E-5-82, USSR Acad. Sci., Steklov Math. Inst., Leningrad, 1982.

[Gao03] Gao, Shuhong. Factoring multivariate polynomials via partial differential equations. *Math. Comput.*, 72(242):801–822, 2003.

[GKMYZ04] Gao, Shuhong, Kaltofen, Erich, May, John P., Yang, Zhengfeng, and Zhi, Lihong. Approximate factorization of multivariate polynomials via differential equations. In ISSAC04, pages 167–174.

[ISSAC04] Gutierrez, Jaime, editor. *ISSAC 2004 Proc. 2004 Internat. Symp. Symbolic Algebraic Comput.*, 2004. ACM Press. ISBN 1-58113-827-X.

[Hoeij02] van Hoeij, Mark. Factoring polynomials and the knapsack problem. *J. Number Theory*, 95:167–189, 2002. Implementation available at `http://web.math.fsu.edu/~hoeij/`.

[Ka82:focs] Kaltofen, E. A polynomial-time reduction from bivariate to univariate integral polynomial factorization. In *Proc. 23rd Annual Symp. Foundations of Comp. Sci.*, pages 57–64. IEEE, 1982. Journal version in [Ka85:sicomp].

[Ka85:jsc] Kaltofen, E. Fast parallel absolute irreducibility testing. *J. Symbolic Comput.*, 1 (1):57–67, 1985a. Misprint corrections: *J. Symbolic Comput.* vol. 9, p. 320 (1989).

[Ka85:sicomp] Kaltofen, E. Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM J. Comput.*, 14(2):469–489, 1985b.

[Ka2K] Kaltofen, E. Challenges of symbolic computation my favorite open problems. *J. Symbolic Comput.*, 29(6):891–919, 2000. With an additional open problem by R. M. Corless and D. J. Jeffrey.

[KaKoi05] Kaltofen, Erich and Koiran, Pascal. On the complexity of factoring bivariate supersparse (lacunary) polynomials. In Kauers, Manuel, editor, *ISSAC'05 Proc. 2005 Internat. Symp. Symbolic Algebraic Comput.*, pages 208–215, New York, N. Y., 2005. ACM Press. ISBN 1-59593-095-7. ACM SIGSAM's ISSAC 2005 Distinguished Paper Award.

[KaKoi06] Kaltofen, Erich and Koiran, Pascal. Finding small degree factors of multivariate supersparse (lacunary) polynomials over algebraic number fields. In Dumas, Jean-Guillaume, editor, *ISSAC MMVI Proc. 2006 Internat. Symp. Symbolic Algebraic Comput.*, pages 162–168, New York, N. Y., 2006. ACM Press. ISBN 1-59593-276-3.

[KaSh97] Kaltofen, E. and Shoup, V. Fast polynomial factorization over high algebraic extensions of finite fields. In Küchlin, W., editor, *Proc. 1997 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'97)*, pages 184–188, New York, N. Y., 1997. ACM Press. ISBN 0-89791-875-4.

[KaSh98] Kaltofen, E. and Shoup, V. Subquadratic-time factoring of polynomials over finite fields. *Math. Comput.*, 67(223):1179–1197, July 1998.

[KipnisS99] Kipnis, Aviad and Shamir, Adi. Cryptanalysis of the HFE public key cryptosystem by relinearization. In Wiener, Michael J., editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.

[Lan85] Landau, S. Factoring polynomials over algebraic number fields. *SIAM J. Comp.*, 14: 184–195, 1985. Erratum: *SIAM J. Comput.* **20**/5, p. 998 (1991).

[Lec05] Lecerf, G. Improved dense multivariate polynomial factorization algorithms. Available from `http://www.math.uvsq.fr/~lecerf/publications/index.html`, 2005.

[LLL82] Lenstra, A. K., Lenstra, Jr., H. W., and Lovász, L. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[Len99a] Lenstra, Jr., H. W. Finding small degree factors of lacunary polynomials. In Győry, Kálmán, Iwaniec, Henryk, and Urbanowicz, Jerzy, editors, *Number Theory in Progress*, volume 1 Diophantine Problems and Polynomials, pages 267–276. Stefan Banach Internat. Center, Walter de Gruyter Berlin/New York, 1999. ISBN 3-11-015715-2.

[Tr76] Trager, B. M. Algebraic factoring and rational function integration. In *Proc. 1976 ACM Symp. Symbolic Algebraic Comp.*, pages 219–228, New York, 1976. ACM.