数理解析研究所講究録
986巻 1997年 66-72

The Average Number of Modular Factors in Trager's Polynomial Factorization Algorithm [1)]

Mark J. Encarnación

Abstract. Trager's algorithm for factoring a univariate polynomial over an algebraic number field computes the norm of the polynomial and then factors the norm over the integers. It has been observed by the author as well as others that the norm tends to factor modulo a prime into more irreducible factors than one would expect from a typical random polynomial over the integers, but no explanation has previously been given. In this paper, an exact formula is derived for the average number of irreducible factors of the norm modulo a prime. For large primes, the asymptotic average is larger than corresponding average for random polynomials with integer coefficients.

1. Introduction

Let $M(t) \in \mathbf{Z}[t]$ be an irreducible polynomial of degree $n \geq 2$ and let α be a root of M. Let $F(\alpha, x)$ be a univariate polynomial of degree $d \geq 2$ over the algebraic number field $\mathbf{Q}(\alpha)$. By clearing denominators, we may assume that F has coefficients in the set $\mathbf{Z}[\alpha]$. Trager's algorithm [8] factors F by first computing the norm

$$N(x) = \mathrm{res}_t(M(t), F(t, x - st)), \tag{1}$$

for $s = 0, 1, 2, \ldots,$ until $N(x)$ is squarefree. If $C(x)$ is an irreducible factor of $N(x)$, then $G(\alpha, x + s\alpha)$, where $G(\alpha, x) = \gcd(C(x), F(\alpha, x - s\alpha))$, is an irreducible factor of F; each of the irreducible factors of F can be computed in this way. Thus, the problem of factoring F has been reduced to the problem of factoring N, a polynomial with rational integer coefficients.

Good implementations of Trager's algorithm factor the norm N using some variant of the Berlekamp-Zassenhaus algorithm [3, 2]. The first step of that algorithm factors N modulo a prime $p \in \mathbf{Z}$ that divides neither the leading coefficient nor the discriminant of N; this

[1)] Parts of this paper were written while the author was visiting the Computer Centre of the University of Tokyo. The author would like to thank the Japan Society for the Promotion of Science for sponsoring the visit, and Dr. Hirokazu Murao for being such a gracious host. The author is currently supported by grants from the U.P. Engineering Research and Development Foundation and the U.P. Office of Research Coordination.

choice of $p$ ensures that $N \bmod p$ will have degree $nd = \deg N$ and will be squarefree. It has been observed previously by the author as well as others that the norm $N$ tends to factor modulo $p$ into more irreducible factors than one would expect from a typical random polynomial of degree $nd$ over $\mathbf{Z}$. Abbott *et al.* [1] give a heuristic explanation for this observation for the case when the input polynomials have a certain special form. In this paper we derive an exact formula for the average number of irreducible factors of the norm modulo a prime $p$, assuming the polynomials $M$ and $F$ are chosen at random. It will follow from the exact formula that the average tends to $H_n H_d$, as $p \to \infty$, where $H_k = 1 + 1/2 + \cdots + 1/k$ is the kth harmonic number. In comparison, a polynomial of degree $nd$ with random integer coefficients factors into an average of $H_{nd}$ irreducible factors modulo $p$, as $p \to \infty$. Notice that $H_n H_d > H_{nd}$, for all $n \geq 2$ and $d \geq 2$.

2. Squarefree polynomials over finite fields

In this section we will derive an exact formula for the average number of irreducible factors of a random squarefree polynomial over a finite field. The formula will be used in the next section, where we present the main result of this paper. Knopfmacher and Knopfmacher [5] present formulas for the mean and variance of the number of irreducible factors of arbitrary polynomials, that is, not necessarily squarefree, but the case of squarefree polynomials has apparently not been discussed in the literature.

Let $\mathrm{GF}(q)$ be the finite field with $q$ elements, where $q$ is a prime power. Let $\pi(q,r)$ be the number of irreducible polynomials over $\mathrm{GF}(q)$ of degree $r$. One has

$$\pi(q,r) = \frac{1}{r} \sum_{d|r} \mu(d) q^{r/d},$$

where $\mu$ is the Möbius function (see [5] or [7, p. 624]). Denote by $\sigma(q,n)$ the number of monic squarefree polynomials over $\mathrm{GF}(q)$ of degree $n$. Then

$$\sigma(q,n) = \begin{cases} 1 & : \ n = 0, \\ q & : \ n = 1, \\ q^n - q^{n-1} & : \ n > 1. \end{cases}$$

Theorem 1 *Let $A(q,n,r)$ denote the average number of monic irreducible factors of degree $r$ of a random squarefree polynomial over $\mathrm{GF}(q)$ of degree $n$. Then*

$$A(q,n,r) = \frac{\pi(q,r)}{\sigma(q,n)} \sum_{i=1}^{\lfloor n/r \rfloor} (-1)^{i+1} \sigma(q, n - ir).$$

Proof. Let $g$ be a monic irreducible polynomial over $\mathrm{GF}(q)$ of degree $r$. Let $\delta_g(q,n)$ be the total number of monic squarefree polynomials over $\mathrm{GF}(q)$ of degree $n$ that are divisible by $g$. Since a squarefree polynomial $f$ of degree $n$ is divisible by $g$ if, and only if, $f = gh$

for some squarefree polynomial h of degree $n-r$ that is not divisible by g, we have the recursion

$$\delta_g(q,n) = \begin{cases} 0 & : \; n < r, \\ 1 & : \; n = r, \\ \sigma(q,n-r) - \delta_g(q,n-r) & : \; n > r, \end{cases}$$

whose solution is

$$\delta(q,n) := \delta_g(q,n) = \sum_{i=1}^{\lfloor n/r \rfloor} (-1)^{i+1} \sigma(q, n-ir).$$

Now $A(q,n,r)$ can be written as

$$\begin{aligned} A(q,n,r) &= \frac{1}{\sigma(q,n)} \sum_g \delta_g(q,n) \\ &= \frac{\pi(q,r)}{\sigma(q,n)} \delta(q,n), \end{aligned}$$

the sum being over all irreducible polynomials g over $\mathrm{GF}(q)$ of degree r. □

The average number of monic irreducible factors of a random squarefree polynomial over $\mathrm{GF}(q)$ of degree n will be the sum of the averages for each degree, namely

$$\sum_{r=1}^{n} A(q,n,r).$$

Note that $A(q,n,r) \to 1/r$ as $q \to \infty$, so that $\sum_{r=1}^{n} A(q,n,r) \to H_n$. As expected, the asymptotic average is the same as that for arbitrary polynomials.

3. The average number of modular factors

In this section, we derive an exact formula for the average number of modular factors that appear in Trager's algorithm applied to random input.

We first define our model of randomness. Let $p \in \mathbf{Z}$ be a prime. An integer a is *random with respect to* p if the residue $a \bmod p$ is equally likely to be any of the values 0, 1, $\ldots$, $p-1$. If $P \subset \mathbf{Z}$ is a finite set of distinct primes, then we say that an integer a is *random with respect to* P if the integer a is random with respect to p, for each $p \in P$. Let m be the product of the primes in P, and let $b = \lfloor (m-1)/2 \rfloor$. By the Chinese remainder theorem, an integer a that is chosen uniformly at random from the set $S = \{-b, -b+1, \ldots, -1, 0, 1, \ldots, b-1, b\}$ will be a random integer with respect to P. For the rest of the paper, we will assume that we are given the set P, and we will denote an arbitrary element of P by p. By a *random integer* we will mean an integer chosen uniformly at random from the set S.

Let $M(t) \in \mathbf{Z}[t]$ be a polynomial of degree $n \geq 2$, whose coefficients are independently chosen random integers. We will assume that M is irreducible over the integers; with high probability this assumption will be true, and the probability will approach 1 as the product of the primes in P approaches infinity (see [7, exercise 4.6.2-27]). By our assumption that M is irreducible, if α is a root of M, then the algebraic number field $\mathbf{Q}(\alpha)$ is well defined. Let $\bar{F}(\alpha, x) \in \mathbf{Q}(\alpha)[x]$. Then $\bar{F}$ can be written as $\bar{F} = (1/c)F$, where $c \in \mathbf{Z}$ and $F(\alpha, x) \in \mathbf{Z}[\alpha][x]$. Let F have degree $d \geq 2$ with coefficients, viewing F as a bivariate polynomial in α and x, that are independently chosen random integers.

With these definitions, we can now state our main result.

Theorem 2 *Let $M(t)$ and $F(\alpha, x)$ be defined as above. If $N(x)$ is the norm of F, and p is a prime dividing neither the leading coefficient nor the discriminant of N, then N will have an average of*

$$\sum_{k=1}^{n} \sum_{r=1}^{d} A(p, n, k) A(p^k, d, r)$$

factors modulo p.

One has the following immediate corollary.

Corollary 1 *With the hypotheses of Theorem 2, the norm N will have an average of $H_n H_d$ factors modulo p, as $p \to \infty$.*

The rest of the paper is devoted to proving Theorem 2. We will need the following lemmas.

Lemma 1 *If u is a random integer with respect to p, then so is $au + b$, for integers a and b, with $a \not\equiv 0 \pmod{p}$.*

Proof. Since a is invertible modulo p, there is a one-to-one correspondence between the values of $(au + b) \bmod p$ and those of $u \bmod p$. □

Lemma 2 *Fix the minimal polynomial M and let p be a prime not dividing the leading coefficient ℓ of M. If $F(\alpha, x)$ is a polynomial over $\mathbf{Z}[\alpha]$ whose coefficients are random with respect to p, then so is $\ell^e F(\alpha, x - \alpha)$, where the integer $e \geq 0$ is such that $\ell^e F(\alpha, x - \alpha) \in \mathbf{Z}[\alpha][x]$.*

Proof. First note that if $d > n - 1$, then the coefficients of $F(\alpha, x - \alpha)$, after reduction modulo M, will be elements of $(1/\ell^{d-n+1})\mathbf{Z}[\alpha]$. Therefore we will have $\ell^{d-n+1} F(\alpha, x - \alpha) \in \mathbf{Z}[\alpha][x]$. If $d \leq n - 1$, then reduction modulo M is not necessary, and $F(\alpha, x - \alpha) \in \mathbf{Z}[\alpha][x]$.

Let $F(\alpha, x) = \sum_{i=0}^{d} a_i x^i$ and $F(\alpha, x - \alpha) = \sum_{i=0}^{d} b_i x^i$, with a_i, $b_i \in \mathbf{Q}(\alpha)$. Then $b_d = a_d$ and, for $i = 0, 1, \ldots, d - 1$, the coefficient b_i will be equal to a_i plus some function of the coefficients $a_{i+1}, \ldots, a_d$, but not of $a_0, \ldots, a_i$. The assertion now follows from Lemma 1. □

What the previous lemma is saying is that the even though we may need to apply a non-trivial preliminary transformation to F to obtain a squarefree norm—that is, we need $s > 0$ in equation (1)—the transformed polynomial will still behave like a random polynomial. This not obvious. For example, the polynomials described by Kaltofen *et* *al.* [4] are the norms of certain polynomials of the form $G(x-\alpha)$, for certain α. Those norms are irreducible over the integers yet they factor modulo every prime; they do not behave like random polynomials. In fact, the heuristic arguments given by Abbott *et al.* [1] are based on the assumption that a non-trivial preliminary transformation is applied to F. Abbott *et al.* then argue that the transformation will lead to norms that behave in a way similar to those described in [4]. We have just shown that the bad behavior of the norms is not caused by the transformation.

Lemma 3 *Let S and T be polynomials in* $\mathrm{GF}(p)[t]$. *If T is fixed and S has coefficients that are distributed uniformly and independently at random, then the remainder of S modulo T has coefficients that are distributed uniformly and independently at random.*

Proof. Let $m = \deg S$ and $n = \deg T$, and let Q and R, respectively, be the quotient and remainder of S modulo T, so that $S = QT + R$, with $\deg R < n$. If $m < n$, then $R = S$ and we are done, so assume that $m \geq n$. Let $S(t) = a_m t^m + \cdots + a_1 t + a_0$. From the equation $R = S - QT$ we see that the coefficient of t^i in R, for $i = 0, 1, \ldots, n-1$, is the difference of a_i and the coefficient of t^i in QT. Furthermore, the coefficients of Q, and therefore of QT, are independent of a_i, for $i = 0, 1, \ldots, n-1$. An application of Lemma 1 completes the proof. □

We now come to the proof of the main theorem.

Proof. [Proof of Theorem 2] By Lemma 2, we can restrict our attention to random polynomials whose norms are squarefree.

Suppose that the minimal polynomial M factors modulo p into irreducible factors M_1, M_2, ..., M_s. Let $k_i = \deg M_i$, for $i = 1, \ldots, s$. Reduce the coefficients of F modulo both p and M_i to get $F_i(\alpha_i, x) \in \mathrm{GF}(p^{k_i})[x]$, where α_i is a root of M_i. By Lemma 3, the coefficients of $F_i(\alpha_i, x)$ will be random elements of $\mathrm{GF}(p^{k_i})[x]$. Therefore, by Theorem 1, the polynomial F_i will have an average of

$$\sum_{r=1}^{d} A(p^{k_i}, d, r) \tag{2}$$

irreducible factors. Since resultants are multiplicative, the norm will have the (partial) factorization $N \equiv N_1 N_2 \cdots N_s \pmod{p}$, where $N_i \equiv \mathrm{res}_t(M_i(t), F(t,x)) \pmod{p}$, for $i = 1, \ldots, s$. The factor N_i, which in general will not be irreducible, is the norm of the polynomial $F_i(\alpha_i, x)$. From Theorem 2.2 of [8], which also holds for finite fields, there is a one-to-one correspondence between the factors of N_i over $\mathrm{GF}(p)$ and the factors of F_i over $\mathrm{GF}(p^{k_i})$. Therefore, the average number of factors of N_i will also be given by (2), and the average number of factors of $N \bmod p$ will be the average value of

$$\sum_{i=1}^{s} \sum_{r=1}^{d} A(p^{k_i}, d, r).$$

The theorem now follows from the fact that $M \bmod p$ will have an average of $A(p, n, k_i)$ irreducible factors of degree k_i. □

	$p=3$		$p=23$		$p\to\infty$	
n	norm	random	norm	random	norm	random
5	4.14	3.32	5.07	3.75	5.21	3.82
10	6.91	4.66	8.36	5.12	8.58	5.19
20	10.74	6.03	12.67	6.50	12.94	6.57
40	15.64	7.41	17.97	7.89	18.31	7.96

Table 1. Numeric values of the average number of factors.

4. Concluding remarks

We have shown that a norm has, on the average, more modular factors than a random polynomial having the same degree. This suggests that factoring norms is harder than factoring "ordinary" polynomials. Fortunately, since norms have a certain structure, there is a device that can be used to limit the number of modular-factor products that have to be examined during the trial-division step of the Berlekamp-Zassenhaus algorithm [3].

Theorems 2 can be used in the design and analysis of algorithms for factoring polynomials. For example, the lifting method presented in [2] has a running time that depends on the number of factors being lifted. Theorem 2 can thus be used to get a bound on the average lifting time.

To get some idea of the magnitudes of the numeric values of the formulas, we give in Table 1 the values for the special case where $d=n$, that is, the polynomial being factored has the same degree as the minimal polynomial. The first column gives the values of n. The second column gives the values of the formula of Theorem 2 evaluated at $d=n$ and $p=3$. The third column gives the value of the formula of Theorem 1 evaluated at $n \leftarrow n^2$ and $q=3$. Similarly for the fourth and fifth columns, except that we evaluate the formulas at p, $q=23$. The last two columns give the asymptotic values for $p\to\infty$. These are simply the values of $(H_n)^2$ and H_{n^2}, respectively. Every number in Table 1 is the exact value rounded to two decimal places.

Note that we have the approximation

$$H_n = \ln n + \gamma + o(1),$$

where $\ln\cdot$ is the natural logarithm function and $\gamma = 0.57721\ldots$ is Euler's constant. (See Knuth [6, p. 74].) Therefore, the numbers given in the last two columns of Table 1 have values $\Theta(\ln^2 n)$ and $\Theta(\ln n)$, respectively, for large n.

参 考 文 献

[1] John A. Abbott, Russell J. Bradford, and James H. Davenport, *A remark on factorization*, SIGSAM Bulletin **19** (1985), no. 2, 31–33 and 37.

[2] George E. Collins and Mark J. Encarnación, *Improved techniques for factoring univariate polynomials*, Journal of Symbolic Computation **21** (1996), 313–327.

[3] Mark J. Encarnación, *Faster algorithms for reconstructing rationals, computing polynomial gcds, and factoring polynomials*, Dissertation, Johannes Kepler University, 1995.

[4] Erich Kaltofen, David R. Musser, and B. David Saunders, *A generalized class of polynomials that are hard to factor*, SIAM Journal on Computing **12** (1983), no. 3, 473–483.

[5] Arnold Knopfmacher and John Knopfmacher, *Counting irreducible factors of polynomials over a finite field*, Discrete Mathematics **112** (1993), 103–118.

[6] Donald E. Knuth, *Fundamental algorithms: The art of computer programming 1*, second ed., Addison-Wesley, 1973.

[7] ———, *Seminumerical algorithms: The art of computer programming 2*, second ed., Addison-Wesley, 1981.

[8] Barry M. Trager, *Algebraic factoring and rational function integration*, Proceedings of the 1976 Symposium on Symbolic and Algebraic Computation, ACM Press, 1976, pp. 219–226.