Coefficient Growth Bounds for Algorithms on Polynomials Over Algebraic Extension Fields

Trevor J. Smedley
Department of Computer Science

Research Report CS-86-46
October 1986

Coefficient Growth Bounds for Algorithms on Polynomials Over Algebraic Extension Fields

Trevor J. Smedley

Department of Computer Science
University of Waterloo
Waterloo, Ontario
CANADA N2L 3B9

ABSTRACT

This paper gives bounds on the coefficient growth in the standard algorithms on univariate polynomials over algebraic extension fields. The algorithms analysed are addition, multiplication, quotient, remainder, and gcd. All algorithms have been implemented in the Maple algebra system.

Introduction

Computer algebra systems have, from the very beginning, been able to perform exact arithmetic with integers and rationals. Many have also attempted to handle algebraic numbers in various fashions. One consistent method is to construct an algebraic extension of the rational numbers which contains all the desired algebraic numbers, and perform the calculations in this field. Any algebraic extension of the rationals can be represented by polynomials in one variable modulo an irreducible polynomial which is called the minimal polynomial for the extension. See Loos[2] for a complete explanation of algebraic numbers and computation in algebraic extension fields.

This paper presents coefficient growth analyses of some standard algorithms for computation with algebraic numbers, and univariate polynomials over algebraic extension fields.

Definition

2.1. Norms

The norm of a polynomial over the integers is defined as the maximum of the absolute values of the coefficients. The norm of a polynomial over the rationals is defined to be the maximum of the absolute value of the least common multiple of the denominators of the coefficients, and the norm of the polynomial over the integers which results from multiplying the polynomial by the least common multiple of the denominators of the coefficients. The norm of an algebraic number is given by its norm when taken as a univariate polynomial over the rationals. The norm of a univariate polynomial over an algebraic extension field is the norm of its representation as a bivariate rational polynomial.

Algorithms on Polynomials Over the Integers and Rational Numbers

The following are coefficient growth bounds for algorithms on polynomials over **Z** and **Q** . The analyses are straightforward, and the results are used extensively in the sequel.

3.1. Addition

The following are bounds for the norm of the result of adding i polynomials whose norms are bounded by l ;

$$\begin{aligned} \textit{over } \mathbf{Z} &= il \\ \textit{over } \mathbf{Q} &= il^i \end{aligned}$$

3.2. Multiplication

The following are bounds for the norm of the result of multiplying i polynomials whose norms are bounded by l , and degrees are bounded by n ;

$$\begin{aligned} \textit{over } \mathbf{Z} &= (n+1)^{i-1} l^i \\ \textit{over } \mathbf{Q} &= (n+1)^{i-1} l^i \end{aligned}$$

3.3. Quotient/Remainder

The following are bounds for the results of a quotient/remainder operation with univariate polynomials over **Z** or **Q** . They are also bounds for the results of a bivariate pseudo-division where the leading coefficient of the divisor, with respect to the variable of division, is a constant (whereas the other coefficients will be polynomials in the second variable).† A bound is also given for the degree of the coefficients in the result of the bivariate pseudo-division.

---

† This fact is used in the analysis of algebraic polynomial quotient/remainder.

The bounds are for division of a degree m by a degree n, where the norms of both polynomials are bounded by l. For the degree bound, p is a bound on the degrees of the coefficients.

3.3.1. Remainder or Pseudo-Remainder

The following is a bound for the norm of the remainder.

$$\begin{aligned} over\ \mathbf{Z} &= 2^{m-n+1} l^{m-n+2} \\ over\ \mathbf{Q} &= 2^{m-n+1} l^{m-n+2} \\ degree &\leq p\,(m-n+2) \end{aligned}$$

3.3.2. Quotient or Pseudo-Quotient

The following is a bound for the norm of the quotient.

$$\begin{aligned} over\ \mathbf{Z} &= 2^{m-n} l^{m-n+1} \\ over\ \mathbf{Q} &= 2^{m-n} l^{m-n+2} \\ degree &\leq p\,(m-n+1) \end{aligned}$$

3.4. Greatest Common Divisor

The following bound is from Knuth[1]. It is a bound for the gcd of two polynomials, one of degree n, and the other of degree m. A bound on the norms is l. The bound for the gcd over the rationals is the same as for over the integers, as it is the same gcd but made monic.

Note that these bounds also apply to the s and t found when solving $sa+tb=gcd\,(a\,,b\,)$ using the extended euclidean algorithm.

$$\begin{aligned} over\ \mathbf{Z} &= l^{m+n}(m+1)^{\frac{n}{2}}(n+1)^{\frac{m}{2}} \\ over\ \mathbf{Q} &= l^{m+n}(m+1)^{\frac{n}{2}}(n+1)^{\frac{m}{2}} \end{aligned}$$

Algorithms for Algebraic Numbers

The following are coefficient growth bounds for algorithms with algebraic numbers. Throughout, p is the degree of the minimal polynomial, and l is a bound on the norms of the algebraic numbers.

4.1. Addition

Adding algebraic numbers is the same as adding univariate polynomials over the rationals, and thus the bounds are the same. We get the following bound for adding i algebraic numbers.

$$norm \leq il^i$$

4.2. Multiplication

Multiplying algebraic numbers is performed by multiplying their representations as univariate polynomials over the rationals, and taking the remainder modulo the minimal polynomial. This gives the following bounds for the multiplication of i algebraic numbers.

The norm of the result of the polynomial multiplication is bounded by,

$$(p+1)^{i-1} l^i$$

and its degree is bounded by ip. So the following is a bound on the result of the algebraic multiplication;

$$norm \leq 2^{ip-p+1} k^{ip-p+2}$$

$$where\ k = max\ ((p+1)^{i-1} l^i\ ,norm\ \ of\ \ minimal\ \ polynomial\ )$$

4.3. Inverse

The inverse of an algebraic number is found by solving $as + mt = 1$ using the extended gcd algorithm where m is the minimal polynomial, and the s found is a^{-1}.† Thus we have the following bound for the inverse operation, where l is also a bound for the norm of the minimal polynomial.

$$norm \leq (p+1)^p\ l^{2p}$$

---

† Since a minimal polynomial is, by definition, irreducible over the rationals, we know that the gcd is one.

Algorithms for Polynomials Over an Algebraic Extension Field

The following are norm bounds for algorithms with polynomials over an algebraic extension field. Throughout, p is the degree of the minimal polynomial, and l is a bound on the norms of the algebraic polynomials.

5.1. Addition

Addition of polynomials over an algebraic extension is performed as a bivariate polynomial addition. This gives the following bound on the norm for addition of i degree n algebraic polynomials.

$$norm \leq il^i$$

5.2. Multiplication

Multiplying algebraic polynomials involves multiplying the bivariate polynomial representations, and then taking the remainder, modulo the minimal polynomial, of each coefficient with respect to the indeterminate. This gives the following bounds for multiplication of i degree n algebraic polynomials;

$$norm \leq 2^{ip-p+1} k^{ip-p+2}$$

$$where\ k = max\ ((np+1)^{i-1} l^i \dagger, norm\ \ of\ \ minimal\ \ polynomial\ )$$

5.3. Quotient/Remainder

The algorithm used for quotient/remainder for polynomials over an algebraic extension will first make the divisor monic by multiplying by the inverse of its leading coefficient‡, and then perform a bivariate pseudo-remainder operation. The coefficients in the results of this operation are reduced modulo the minimal polynomial, and this gives the required results. This algorithm leads to the following analysis.

Step one involves taking the inverse of the leading coefficient of the divisor, and then multiplying the divisor by this. This gives the following bounds where l is a bound on the norms of the divisor and the minimal polynomial.

$$norm \leq (p+1)^p\ l^{2p}$$

$$norm\ of\ product\ \leq\ (p+1)^{2p+1} l^{4p}$$

---

† This quantity is a bound on the norm of the result of the bivariate polynomial multiplication. Thus it is a bound on the norms of the dividends in the remainder operations.

‡ This multiplication is done as a polynomial multiplication, rather than an algebraic number multiplication for efficiency reasons. Since we know that the result will be monic we can replace the leading coefficient by 1. The result is reduced modulo the minimal polynomial at the end of all of the calculations.

The degree of the coefficients in the product will be bounded by;

$$degree \leq 2p$$

Step 2 is a bivariate pseudo-division.

If j is a bound on the norm of the dividend, and a bound on the norm of the product given above, then the following are the bounds on the norms of the results of the pseudo-division;

$$norm\ of\ remainder \leq 2^{m-n+1} j^{m-n+2}$$

$$norm\ of\ quotient \leq 2^{m-n} j^{m-n+2}$$

and the degrees of the coefficients are bounded by;

$$degree\ of\ coefficients\ in\ remainder \leq 2p\ (m-n+2)$$

$$degree\ of\ coefficients\ in\ quotient \leq 2p\ (m-n+1)$$

Finally the coefficients are reduced modulo the minimal polynomial.

If l_q is a bound on the norm of the quotient and on the norm of the minimal polynomial, and l_r is a bound on the norm of the remainder and the norm of the minimal polynomial, then we get the following norm bounds;

$$norm\ of\ reduced\ remainder \leq 2^{2pm-2pn+3p+1} l_r^{2pm-2pn+3p+2}$$

$$norm\ of\ reduced\ quotient \leq 2^{2pm-2pn+p+1} l_q^{2pm-2pn+p+2}$$

If we assume that the maximum possible coefficient growth happens at every step, and let k be a bound on the norms of the input polynomials, the norm of the minimal polynomial, and the norm of the inverse of the leading coefficient of the divisor, then we get the following best and worst case bounds with respect to n .

Worst case ($n=0$);

$$remainder \quad 2^{7pm+3+6p+2pm^2+2m}(p+1)^{2pm^2+4+7pm+2m+6p} k^{4pm^2+8+14pm+4m+12p}$$

$$quotient \quad 2^{3pm+1+p+2pm^2+2m}(p+1)^{2pm^2+4+5pm+2m+2p} k^{4pm^2+8+10pm+4m+4p}$$

Best case ($n=m$);

$$remainder \quad 2^{6p+3}(p+1)^{6p+4} k^{12p+8}$$

$$quotient \quad 2^{p+1}(p+1)^{2p+4} k^{4p+8}$$

We can conclude that as long as the degrees of the two polynomials do not differ by too much, and the norm of the inverse of the leading coefficient is not too large, then the coefficient growth will not be unacceptably large. Unfortunately the norm of the inverse can be as large as $(p+1)^p\ l^{2p}$, and in fact is this large often.

5.4. Greatest Common Divisor

From Knuth[1] we know that the coefficients of the gcd of two polynomials can be expressed as determinants of $n \times n$ matrices of the coefficients of the original polynomials. So, using a bound on the norm of a determinant of a matrix of univariate, rational polynomials, and then taking the norm of the remainder of this result modulo the minimal polynomial, we can get a bound on the norm of the gcd of polynomials over an algebraic extension field.

First we give norm and degree bounds for the determinant of a matrix whose entries are univariate rational polynomials. The matrix is $n \times n$, p is a bound on the degree of the matrix elements, and l is a bound on the norms of the entries.†

$$norm \leq l^{3n} n! (p+1)^{n-1}$$

$$degree \leq np$$

Using the above bound, we get the following result for the norm of the gcd, where k is the maximum of the above quantity and the norm of the minimal polynomial, p is the degree of the minimal polynomial, and n is a bound on the degrees of the two polynomials.

$$norm\ of\ gcd \leq 2^{np-p+1} l^{3n(np-p+2)} n!^{np-p+2} (p+1)^{(n-1)(np-p+2)}$$

Empirical tests show this quantity to be pessimistic. A better bound could probably be obtained through finding a better bound for the determinant of a matrix of algebraic numbers.

---

† Also, in our case l^2 is a bound on the integer multiplier required to transform any row of the matrix to polynomials over the integers. This is because the entries in our case are coefficients of polynomials over an algebraic extension field, and the norms of the polynomials are both bounded by l .

Comments and Conclusions

Most of the bounds given are quite satisfactory, and can be verified to be fairly tight. Exceptions to this are algebraic number inverse, and algebraic polynomial quotient/remainder and gcd. In the case of the gcd, the bound is bad, but empirical results do not verify the bound to be accurate. One expects that a better bound can be found. In the case of the quotient/remainder the bound is bad, and in many cases accurate. One notices that as long as the inverse of the leading coefficient of the divisor has small norm, then the result of the operation does not grow too extremely. However, it is quite often the case that the inverse operation causes extremely large coefficient growth.

In general one can conclude that, as long as inverses do not have to be computed, or if they are computed they are small, then computing with algebraic numbers should be quite efficient.

References

1. D E Knuth, *The Art of Computer Programming, Vol II, Semi-Numerical Algorithms,* Addison-Wesley (1981).

2. R Loos, Computing in Algebraic Extensions, *Computing Suppl. 4,* pp. 173-187 Springer-Verlag, (1982).