An Inequality About Factors of Multivariate Polynomials

M. Jason Hinek and Douglas R. Stinson*

David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada

June 13, 2006

Abstract

We give a bound on the Euclidean norm of factors of multivariate polynomials. The result is a simple extension of the bivariate case given by Coron, which is an extension of the univariate case given by Mignotte. We use the result to correct a proof by Ernst et al., regarding computing small integer solutions of certain trivariate polynomials.

1 Introduction

In 1974, Mignotte [7] presented some results concerning norms of factors of univariate polynomials. In particular, we are interested in part of one result [7, Theorem 2], which we restate as the following theorem.

Theorem 1 (Mignotte) *Let $f(x)$ and $g(x)$ be two non-zero polynomials over $\mathbb{Z}$ such that* $\deg f \leq d$ *and g is a multiple of f in $\mathbb{Z}[x]$. Then*

$$\|g\|_2 \geq 2^{-d} \cdot \|f\|_\infty.$$

*research supported by NSERC discovery grant 203114-06.

Here $\|\cdot\|_2$ denotes the normal Euclidean norm and $\|\cdot\|_\infty$ denotes the infinity norm, or the height of the polynomial. That is, for any polynomial $h(x_1,\ldots,x_n) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x_1^{i_1}\cdots x_n^{i_n}$, the Euclidean and infinity norms of $h(x_1,\ldots,x_n)$ are defined by

$$\begin{aligned} \|h(x_1,\ldots,x_n)\|_2 &= \sqrt{\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n}^2}, \quad \text{and} \\ \|h(x_1,\ldots,x_n)\|_\infty &= \max_{i_1,\ldots,i_n} \left(|a_{i_1,\ldots,i_n}|\right), \end{aligned}$$

respectively.

In 2004, Coron [3] extended Mignotte's result to bivariate polynomials. The main result is given in the following theorem.

Theorem 2 (Coron) *Let $a(x,y)$ and $b(x,y)$ be two non-zero polynomials over $\mathbb{Z}$ of maximum degree d separately in x and y, such that $b(x,y)$ is a multiple of $a(x,y)$ in $\mathbb{Z}[x,y]$. Then*

$$\|b\|_2 \geq 2^{-(d+1)^2} \cdot \|a\|_\infty.$$

In addition to extending Mignotte's result to bivariate polynomials, Coron also considers the special case when a multiple of a bivariate polynomial has content that is relatively prime to the constant term of the original polynomial. We state this result in the following corollary.

Corollary 3 (Coron) *Let $a(x,y)$ and $b(x,y)$ be as in Theorem 2. Assume that $a(0,0) \neq 0$ and $b(x,y)$ is divisible by a non-zero integer r such that $\gcd(r, a(0,0)) = 1$. Then $b(x,y)$ is a multiple of $r \cdot a(x,y)$ and*

$$\|b\|_2 \geq 2^{-(d+1)^2} \cdot |r| \cdot \|a\|_\infty.$$

2 Factors of Multivariate Polynomials

Coron's results are easily extended to multivariate polynomials in general. We present the extended results below along with their proofs.

Theorem 4 *Let $a(x_1,x_2,\ldots,x_n)$ and $b(x_1,x_2,\ldots,x_n)$ be two non-zero polynomials over $\mathbb{Z}$ of maximum degree d in each variable separately such that $b(x_1,x_2,\ldots,x_n)$ is a multiple of $a(x_1,x_2,\ldots,x_n)$ in $\mathbb{Z}[x_1,x_2,\ldots,x_n]$. Then*

$$\|b\|_2 \geq 2^{-(d+1)^n+1} \cdot \|a\|_\infty.$$

The proof we give follows Coron's bivariate proof very closely. Essentially, one applies Mignotte's result to univariate polynomials that are constructed from the multivariate polynomials in such a way that the norms are preserved.

Proof: Let $f(x) = a(x, x^{d+1}, x^{(d+1)^2}, \ldots, x^{(d+1)^{n-1}})$. By construction, $f(x)$ and $a(x_1, x_2, \ldots, x_n)$ have the same list of non-zero coefficients and so they have the same height (i.e., $\|f\|_\infty = \|a\|_\infty$). Also, notice that the degree of f satisfies $\deg f \leq (d+1)^n - 1$, because

$$d + d(d+1) + d(d+1)^2 + \cdots + d(d+1)^{n-1} = d\frac{(d+1)^n - 1}{(d+1) - 1} = (d+1)^n - 1.$$

Similarly, let $g(x) = b(x, x^{d+1}, x^{(d+1)^2}, \ldots, x^{(d+1)^{n-1}})$. Since $b(x_1, x_2, \ldots, x_n)$ and $g(x)$ have the same list of non-zero coefficients they have the same Euclidean norm (i.e., $\|g\|_2 = \|b\|_2$). Now, given that $b(x_1, x_2, \ldots, x_n)$ is a multiple of $a(x_1, x_2, \ldots, x_n)$ in $\mathbb{Z}[x_1, x_2, \ldots, x_n]$, we know that $g(x)$ is a multiple of $f(x)$ in $\mathbb{Z}[x]$. Therefore, applying Theorem 1, Mignotte's result, on $f(x)$ and $g(x)$ yields

$$\|b\|_2 = \underbrace{\|g\|_2 \geq 2^{-(d+1)^n+1} \cdot \|f\|_\infty}_{\text{Mignotte's result}} = 2^{-(d+1)^n+1} \cdot \|a\|_\infty,$$

which completes the proof. ❑

Notice that the bound obtained in Theorem 4 for bivariate polynomials improves the bound in Coron's result (Theorem 2) by a factor of two.

Corollary 5 *Let $a(x_1, x_2, \ldots, x_n)$ and $b(x_1, x_2, \ldots, x_n)$ be as in Theorem 4. Assume that $a(0, 0, \ldots, 0) \neq 0$ and $b(x_1, x_2, \ldots, x_n)$ is divisible by a non-zero integer r such that $\gcd(r, a(0, 0, \ldots, 0)) = 1$. Then $b(x_1, x_2, \ldots, x_n)$ is divisible by $r\,a(x_1, x_2, \ldots, x_n)$ and:*

$$\|b\|_2 \geq 2^{-(d+1)^n+1} \cdot |r| \cdot \|a\|_\infty.$$

Let $p_{\ell_1,\ell_2,\ldots,\ell_n}$ denote the coefficient of $x_1^{\ell_1} x_2^{\ell_2} \cdots x_n^{\ell_n}$ for a given polynomial $p(x_1, x_2, \ldots, x_n)$.

Proof: Let $q(x_1, x_2, \ldots, x_n)$ be the polynomial such that $b(x_1, x_2, \ldots, x_n)$ is equal to $q(x_1, x_2, \ldots, x_n) \cdot a(x_1, x_2, \ldots, x_n)$. First we show that r divides

$q(x_1, x_2, \ldots, x_n)$. Assume that this is not the case and let $q_{\ell_1,\ell_2,\ldots,\ell_n}$ be the smallest coefficient of $q(x_1, x_2, \ldots, x_n)$, in the lexicographical ordering, that is not divisible by r. We then have that $b_{\ell_1,\ell_2,\ldots,\ell_n} \equiv q_{\ell_1,\ell_2,\ldots,\ell_n} \cdot a(0, \ldots, 0) \pmod{r}$. Since $a(0, \ldots, 0)$ is invertible modulo r and $b_{\ell_1,\ell_2,\ldots,\ell_n} \equiv 0 \pmod{r}$, this gives a contradiction. Thus, we have that $b(x_1, x_2, \ldots, x_n)$ is a multiple of $r \cdot a(x_1, x_2, \ldots, x_n)$ and the result follows from Theorem 4. ❑

3 An Application

In practice, the contrapositive of the main result (Theorem 4) can be used as a tool to show that certain polynomials are not a multiple of a given polynomial. Indeed, Coron's results for bivariate polynomials was originally used for just that purpose. Below, we briefly outline Coron's application of the result and discuss Ernst et al.'s extension of it.

The main result of Coron's work [3] is a simplification of Coppersmith's method for finding small integer solutions to bivariate equations [2] (cf. Howgrave-Graham's simplification [5] of Coppersmith's univariate modular method [1]). Wanting to find small integer roots of a given bivariate polynomial $f(x, y)$, a lattice is constructed using certain polynomial multiples of $f(x, y)$ and certain monomials (see [3] for details). Using the LLL algorithm [6], a new polynomial $g(x, y)$ is found in the lattice that has the same small integer roots as $f(x, y)$ but with degree greater than $f(x, y)$. Using properties of the LLL algorithm, Coron shows that the Euclidean norm of $g(x, y)$ is small enough so that Corollary 3 implies that $g(x, y)$ cannot be a multiple of $f(x, y)$. Since the degree of $g(x, y)$ is greater than the degree of $f(x, y)$ and $g(x, y)$ is not a multiple of $f(x, y)$, the two polynomials are algebraically independent and the system of equations $\{f(x, y) = 0\ ,\ g(x, y) = 0\}$ can be solved.

Coron's result for bivariate integer root finding was extended to certain trivariate polynomials $f(x, y, z)$ by Ernst et al. in [4]. Here, instead of using one polynomial found in the lattice by the LLL algorithm, two polynomials, $g_1(x, y, z)$ and $g_2(x, y, z)$, are used. The polynomials $g_1(x, y, z)$ and $g_2(x, y, z)$ both have the same small integer roots as $f(x, y, z)$ but with higher total degree than $f(x, y, z)$. Using properties of the LLL algorithm in conjunction with Corollary 3, it is claimed that both $g_1(x, y, z)$ and $g_2(x, y, z)$ are not multiples of $f(x, y, z)$ and hence $g_1(x, y, z)$ and $f(x, y, z)$ are algebraically

independent, and furthermore, $g_2(x, y, z)$ and $f(x, y, z)$ are algebraically independent. Under the commonly used assumption that the polynomials obtained by the LLL algorithm are algebraically independent, it follows that all three polynomials are algebraically independent and hence the system $\{f(x, y, z) = 0, g_1(x, y, z) = 0, g_2(x, y, z) = 0\}$ can be solved. Because of the algebraic independence assumption, the method remains a heuristic, in contrast to Coron's provable method, however.

In justifying the correctness of their method, modulo the algebraic independence assumption, Ernst et al. apply Corollary 3 to trivariate polynomials. However, this is an invalid application of Corollary 3, which refers only to bivariate polynomials. Their informal proof is easily corrected by simply using Corollary 5 with $n = 3$. It should also be pointed out, however, that Ernst et al.'s result involves taking limits in which the factor $2^{-(d+1)^n+1}$ becomes insignificant for any finite n. Thus, the end results are unchanged when the incorrect factor, $2^{-(d+1)^2}$, is used instead of the correct factor, $2^{-(d+1)^3-1}$.

4 Conclusion

In conclusion, we have given a lower bound on the Euclidean norm of factors of multivariate polynomials. The result is a simple extension of Coron's result for bivariate polynomials, which is itself an extension of Mignotte's univariate result. While Mignotte's result gives the tightest known bound for univariate polynomials, it remains an open question if the bound given in Theorem 4 can be made tighter.

We have also made a correction to an informal proof of Ernst et al., regarding finding small integer solutions to some trivariate polynomials.

References

[1] D. Coppersmith. Finding a small root of a univariate modular equation. *Lecture Notes in Computer Science* **1070** (1996), 155–165 (EUROCRYPT 1996).

[2] D. Coppersmith. Finding a small root of a bivariate integer equation; factoring with high bits known. *Lecture Notes in Computer Science* **1070** (1996), 178–189 (EUROCRYPT 1996).

[3] J.-S. Coron. Finding small roots of bivariate integer polynomial equations revisited. *Lecture Notes in Computer Science* **3027** (2004), 492–505 (EUROCRYPT 2004).

[4] M. Ernst, E. Jochemsz, A. May and B. de Weger. Partial key exposure attacks on RSA up to full size exponents. *Lecture Notes in Computer Science* **3494** (2005), 371–387 (EUROCRYPT 2005).

[5] N. Howgrave-Graham. Finding small roots of univariate modular equations revisited. *Lecture Notes in Computer Science* **1355** (1997), 131–142 (Coding and Cryptography).

[6] A. K. Lenstra and H. W. Lenstra and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen* **261** (1982), 515–534.

[7] M. Mignotte. An inequality about factors of polynomials. *Mathematics of Computation*, **20**(128):1153–1157, October 1974.