# IRREDUCIBILITY OF POLYNOMIALS MODULO $p$ VIA NEWTON POLYTOPES

SHUHONG GAO AND VIRGÍNIA M. RODRIGUES

Abstract. Ostrowski established in 1919 that an absolutely irreducible integral polynomial remains absolutely irreducible modulo all sufficiently large prime numbers. We obtain a new lower bound for the size of such primes in terms of the number of integral points in the Newton polytope of the polynomial, significantly improving previous estimates for sparse polynomials.

## 1. Introduction

A polynomial $f \in \mathbb{Z}[x, y]$, absolutely irreducible over $\mathbb{Q}$, is said to have a *good reduction* at a prime $p$ (or $p$ is *good* for $f$) if it remains absolutely irreducible modulo $p$; otherwise $f$ is said to have a *bad reduction* at $p$ (or $p$ is *bad* for $f$). In 1919, Ostrowski [6] proved that a multivariate integral polynomial, absolutely irreducible over the rationals, has good reduction at all sufficiently large primes. This well-known result motivates the search for lower bounds for such primes.

In 1976, Schmidt [11] gave a triple exponential bound for good primes based on the total degree $d > 0$ of the polynomial $f$. He proved that $f$ has a good reduction at all primes $p$ with

$$p > (4\|f\|_1)^{k^{2^k}},$$

where $k = \binom{d+1}{2}$ and $\|f\|_1$ is the sum of the absolute values of its coefficients. A substantial improvement of this result was given by Kaltofen [4] in 1985 (see also [5]). For $f$ monic in $x$ he obtained

$$p \geq (2d \cdot H(f))^{10d^8},$$

where $H(f)$ is the *height* of $f$, i.e. the maximum of the absolute values of its coefficients. In 1986, Ruppert [8] presented a sharper estimate:

$$p > d^{3d^2-3} \cdot H(f)^{d^2-1}.$$

*Date*: Revised December 4, 2002.

*Key words and phrases.* Absolute irreducibility, Newton polytopes, PDE, good reduction.

This work was supported in part by NSF Grant DMS9970637, NSA Grant MDA904-02-1-0067, ONR Grant N00014-00-1-0565, and a Research Initiative Grant from South Carolina Commission on Higher Education. The second author also gratefully acknowledges the support of CAPES, Brazil.

In 1997, Zannier [12] derived a bound for good primes in terms of the degrees of $f$ with respect to $x$ and $y$:

$$p > e^{12n^2m^2}(4n^2m)^{8n^2m} \cdot H(f)^{2(2n-1)^2m},$$

where $\deg(f) = (m, n)$.[1] His result was improved by Ruppert [9], who in 1999 obtained the estimate

$$p > [m(n+1)n^2 + (m+1)(n-1)m^2]^{mn+(n-1)/2} \cdot H(f)^{2mn+n-1}. \tag{1}$$

In this paper we present a new lower bound that improves (1), specially when $f$ is sparse. Our estimate is given in terms of the bidegree of $f$ and *the number of integral points in its Newton polytope*, which gives a nice geometric visualization of the values involved in the computation and allows the *shape* of $f$ to be exploited.

The Newton polytope of a polynomial $f = \sum_{i,j} a_{ij}x^iy^j \in \mathbb{F}[x, y]$, where $\mathbb{F}$ is any field, is defined as the convex hull in the Euclidean plane $\mathbb{R}^2$ of the exponent vectors $(i, j)$ of all the nonzero terms of $f$. We denote it by $P(f)$ (see Figure 1 for an example). Newton polytopes carry a lot of information about irreducibility and factorization of polynomials. Indeed, Gao [1] presents several criteria for absolute irreducibility of polynomials based on the explicit construction of indecomposable polytopes, generalizing the well-known Eisenstein's irreducibility criterion. Also, Gao and Lauder [3] study computational problems about decomposition of polytopes and polynomials. Here we show how Newton polytopes can be used to estimate the size of the primes that preserve absolute irreducibility of polynomials. Our main contribution is the following result.

**Theorem 1.** *Let $f = \sum_{i,j} a_{ij}x^iy^j \in \mathbb{Z}[x, y]$ be absolutely irreducible over $\mathbb{Q}$ with bidegree $(m, n)$, where $m, n \geq 1$. Then $f$ is absolutely irreducible over $\mathbb{Z}_p$ for every prime $p$ such that*

$$p > \left(\sqrt{m^2 + n^2} \cdot \|f\|_2\right)^{2t-3}, \tag{2}$$

*where $t$ is the number of integral points in the Newton polytope of $f$, and $\|f\|_2 = (\sum_{i,j} a_{ij}^2)^{1/2}$, the Euclidean norm of $f$.*

For an example of bound (2), consider the polynomial $f = x^2 + y^3 + 3x^4y^5$. Its Newton polytope is the triangle with vertices $(2, 0)$, $(0, 3)$ and $(4, 5)$, shown in Figure 1. $P(f)$ contains 11 integral points, so Theorem 1 guarantees that $f$ has a good reduction at any prime $p$ greater than $1.64 \times 10^{25}$. For this polynomial, Ruppert's bound (1) is $1.573 \times 10^{86}$. The big difference between these estimates can be explained in terms of Newton polytopes: (1) essentially corresponds to considering the integral points in the rectangle with vertices $(0, 0)$, $(m, 0)$, $(0, n)$ and $(m, n)$, where $(m, n)$ is the bidegree of $f$, while our result implies that it suffices to count only those in $P(f)$.

The Euclidean norm of a polynomial depends only on its nonzero coefficients, while the number of integral points in the Newton polytope depends on its shape,

[1] We say that a bivariate polynomial $f$ has *bidegree* $(m, n)$ and write $\deg(f) = (m, n)$, when $\deg_x(f) = m$ and $\deg_y(f) = n$. We make the convention that if $\deg(f) \leq (m, n)$ and $m$ or $n$ is negative, then f is identically zero.

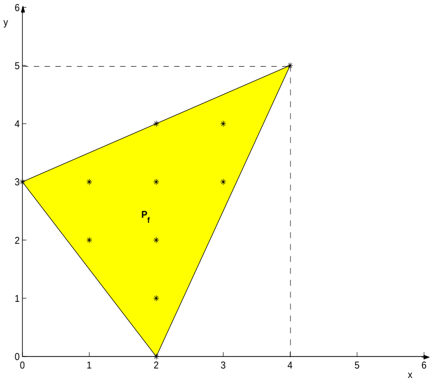

Fig. 1: The Newton polytope of $f = x^2 + y^3 + 3x^4y^5$.

hence both the sparsity and the shape of $f$ are incorporated in bound (2). To compare it with (1), note that $\|f\|_2 \leq \sqrt{t} \cdot H(f)$, and so (2) implies that

$$p > \left(\sqrt{(m^2+n^2)t} \cdot H(f)\right)^{2t-3} \tag{3}$$

is sufficient to preserve the absolute irreducibility of $f$ over $\mathbb{Z}_p$. Estimate (3) (and hence estimate (2)) improves Ruppert's bound (1) for $t \leq m(n-1)$, .

The proof of Theorem 1, presented in Section 2, is based on a partial differential equation used by Ruppert [9], and on a result of Gao [2] that characterizes the dimension of the solution space of this PDE as the number of absolutely irreducible factors of the given polynomial. We show that the shape of the solutions depends only on the Newton polytope of the polynomial, which yields a linear system of size depending on the number of integral points in the Newton polytope.

In Section 3 we give explicit examples showing the coefficient matrix of the linear system from which (2) is derived. We present polynomials that have the same Newton polytope and Euclidean norm, but have bad primes varying greatly in size.

## 2. Deriving the New Bound

In his study of irreducibility of polynomials Ruppert [9] presented a criterion for reducibility based on the existence of solutions of the partial differential equation

$$\frac{\partial}{\partial y}\left(\frac{g}{f}\right) = \frac{\partial}{\partial x}\left(\frac{h}{f}\right), \tag{4}$$

where $f \in \mathbb{F}[x,y]$ is given, $g, h \in \mathbb{F}[x,y]$ are unknown, $\mathbb{F}$ is an algebraically closed field, $\deg\ f = (m,n)$, $\deg\ g \leq (m-1,n)$, and $\deg\ h \leq (m, n-2)$.

A new method for factoring bivariate polynomials was recently developed by Gao [2] using PDE (4) with a slightly relaxed condition on the degree of $h$. He considered

$$\deg\ f = (m,n),\ \deg\ g \leq (m-1,n),\ \text{and}\ \deg\ h \leq (m,n-1), \tag{5}$$

and showed that the solutions $g, h$ of (4) and (5) have a special format, which we exploit to derive our bound for the size of good primes.

Let $\mathbb{F}$ be any field and $\overline{\mathbb{F}}$ its algebraic closure. Let $f \in \mathbb{F}[x, y]$ with bidegree $(m, n)$ and consider the solution spaces

$$\begin{aligned}\overline{G} &= \{g \in \overline{\mathbb{F}}[x, y] : (4) \text{ and } (5) \text{ hold for some } h \in \overline{\mathbb{F}}[x, y]\},\\ G &= \{g \in \mathbb{F}[x, y] : (4) \text{ and } (5) \text{ hold for some } h \in \mathbb{F}[x, y]\}.\end{aligned}$$

Note that $G$ and $\overline{G}$ are vector spaces over $\mathbb{F}$ and $\overline{\mathbb{F}}$, respectively, and $G \subseteq \overline{G}$.

**Theorem 2** (Gao [2])**.** *Suppose $f = f_1 f_2 \cdots f_r$, where $f_i \in \overline{\mathbb{F}}[x, y]$ are distinct and irreducible over $\overline{\mathbb{F}}$, and suppose $\gcd(f, f_x) = 1$. If $\mathbb{F}$ has characteristic either zero or greater than $(2m - 1)n$, then*

$$dim_{\mathbb{F}}(G) = dim_{\overline{\mathbb{F}}}(\overline{G}) = r,$$

*and each $g \in \overline{G}$ is of the form*

$$g = \sum_{i=1}^{r} \lambda_i E_i, \tag{6}$$

*where $\lambda_i \in \overline{\mathbb{F}}$ and*

$$E_i = \frac{f}{f_i} \frac{\partial f_i}{\partial x} \in \overline{\mathbb{F}}[x, y], \quad 1 \leq i \leq r.$$

A consequence of this result is a *criterion for irreducibility* depending on the dimension of the solution space $G$:

*$f$ is absolutely irreducible over $\mathbb{F}$ if and only if $dim_{\mathbb{F}}(G) = 1$,*

where $\mathbb{F}$ has characteristic either zero or greater than $(2m - 1)n$. A similar result for characteristic zero was obtained by Ruppert in [9].

Note that the partial differential equation (4) can be rewritten as

$$f \cdot \frac{\partial g}{\partial y} - g \cdot \frac{\partial f}{\partial y} - f \cdot \frac{\partial h}{\partial x} + h \cdot \frac{\partial f}{\partial x} = 0, \tag{7}$$

which is a homogeneous system of linear equations for the coefficients of $g$ and $h$. Let us denote by $M$ the matrix of the system obtained by considering polynomials $g$ and $h$ satisfying (7) and condition (5) on the degrees. So the number $\rho$ of variables of the system is the total number of coefficients of $g$ and $h$, which is at most $2mn + m + n$. The irreducibility criterion given above can then be restated as follows.

**Corollary 3.** *$f$ is absolutely irreducible over $\mathbb{F}$ if and only if $rank(M) = \rho - 1$, assuming $\mathbb{F}$ has characteristic either zero or greater than $(2m - 1)n$.*

Another important consequence of Theorem 2 is that a possible solution $g \in G$ must be of the form (6). In addition, the same proof shows that the corresponding $h \in \overline{\mathbb{F}}[x, y]$ is of the form

$$h = \sum_{i=1}^{r} \lambda_i D_i, \tag{8}$$

where

$$D_i = \frac{f}{f_i}\frac{\partial f_i}{\partial y} \in \overline{\mathbb{F}}[x,y], \quad 1 \le i \le r.$$

Examining expressions (6) and (8), we show in Lemma 4 that they reveal information on the shape of the Newton polytopes of $g$ and $h$, which yields a bound on the number of nonzero coefficients of these polynomials.

**Lemma 4.** *Let $f$ be as in Theorem 2. Let $t$ be the number of integral points in $P(f)$, $t_x$ the number of integral points in $P(f)$ lying on the $x$-axis, and $t_y$ on the $y$-axis. Then, for all polynomials $g, h \in \overline{\mathbb{F}}[x,y]$ of the forms (6) and (8), respectively, we have*

$$P(xg) \subseteq P(f) \quad \text{and} \quad P(yh) \subseteq P(f), \tag{9}$$

*and $g$ and $h$ have at most $t - t_y$ and $t - t_x$ nonzero coefficients, respectively.*

In the proof of this result we apply the following well-known result by Ostrowski (1975), which states that the Newton polytope of a polynomial is the Minkowski sum[2] of the Newton polytopes of its factors.

**Lemma 5** (Ostrowski [7])**.** *Let $f, f_1, \cdots, f_r \in \mathbb{F}[x,y]$ with $f = f_1 \cdots f_r$. Then*

$$P(f) = P(f_1) + \cdots + P(f_r).$$

For a simple proof of this lemma see [1].

*Proof of Lemma 4.* Let $g, h \in \overline{\mathbb{F}}[x,y]$ of the forms (6) and (8), respectively. In (6) we have $E_i = \frac{f}{f_i}\frac{\partial f_i}{\partial x}$, for $i = 1, \ldots, r$. So,

$$P(xE_i) = P\Big(\frac{f}{f_i} \cdot x\frac{\partial f_i}{\partial x}\Big) = P\Big(\frac{f}{f_i}\Big) + P\Big(x\frac{\partial f_i}{\partial x}\Big),$$

by Lemma 5. Note that the exponent vectors of each polynomial $x\frac{\partial f_i}{\partial x}$ are of the form $(k,l)$, where $k \ge 1$ and $(k,l)$ is an exponent vector of $f_i$. Hence $P\Big(x\frac{\partial f_i}{\partial x}\Big) \subseteq P(f_i)$ and

$$P(\lambda_i x E_i) \subseteq P(xE_i) \subseteq P\Big(\frac{f}{f_i}\Big) + P(f_i) = P\Big(\frac{f}{f_i} \cdot f_i\Big) = P(f),$$

for $i = 1, \ldots, r$. Therefore,

$$P(xg) = P\Big(\sum_{i=1}^{r} \lambda_i x E_i\Big) \subseteq P(f).$$

Similarly, from (8) we obtain

$$P(yh) = P\Big(\sum_{i=1}^{r} \lambda_i y D_i\Big) \subseteq P(f).$$

Since $P(xg)$ is a subset of $P(f)$, all the nonzero terms of $xg$ have exponent vectors corresponding to integral points inside the Newton polytope of $f$. Besides, all of them have degree at least one in $x$, which implies that the Newton polytope of $xg$ does not have points lying on the $y$-axis. Thus $xg$ has at most $t - t_y$ nonzero

[2] The Minkowski sum $A + B$ of two sets $A$ and $B \in \mathbb{R}^n$ is the set of all elements $a + b$ with $a \in A$ and $b \in B$.

coefficients and so does $g$, as they have the same nonzero coefficients. Similarly, the Newton polytope of $yh$ does not have points outside the Newton polytope of $f$ nor on the $x$-axis. Then $t-t_x$ is an upper bound for the number of nonzero coefficients of $yh$ and hence of $h$. □

From Lemma 4 it follows that the total number of nonzero coefficients of polynomials $g, h$ of the forms (6), (8) is bounded by

$$(t-t_x)+(t-t_y). \tag{10}$$

Thus, since the shape of the Newton polytope of $f$ reflects on the sizes of $t$, $t_x$ and $t_y$, (10) allow us to exploit the possible sparsity of $f$ to reduce the number of variables of the linear system on the coefficients of polynomials $g, h$ satisfying (4) and (5).

**Theorem 6.** *Let $f=\sum_{i,j} a_{ij}x^iy^j \in \mathbb{Z}[x,y]$, absolutely irreducible over $\mathbb{Q}$ with bidegree $(m,n)$, where $m,n \geq 1$. Then $f$ is absolutely irreducible over $\mathbb{Z}_p$ for every prime $p$ such that $\gcd(f, f_x)=1$ in $\mathbb{Z}_p[x,y]$ and*

$$p > \left(\sqrt{m^2+n^2}\cdot \|f\|_2\right)^{2t-(t_x+t_y)-1}, \tag{11}$$

*where $t$, $t_x$ and $t_y$ are as in Lemma 4.*

*Proof:* Since $m,n \geq 1$, we have $t-t_x \geq 1$ and $t-t_y \geq 1$ and so $2t-(t_x+t_y) \geq 2$. The case $2t-(t_x+t_y)=2$ is quite simple. It happens only if $f$ is of the form $ax+by+c$, $ax^m+by^n$ or $ax^my^n+b$, where $a, b$ and $c$ are nonzero and $\gcd(m,n)=1$. The first form is trivial. For the other two forms, $f$ remains irreducible over $\mathbb{Z}_p$ if $a$ and $b$ are nonzero modulo $p$. But this is guaranteed, since $t-t_x=1$ and $t-t_y=1$ in this case, and so for $p$ satisfying (11) we have

$$p > \sqrt{m^2+n^2}\cdot\|f\|_2 > H(f)=\max\{|a|,|b|\}.$$

We may henceforth assume that $2t-(t_x+t_y) \geq 3$. Then estimate (11) is at least

$$(m^2+n^2)\cdot\|f\|_2^2 \geq m^2+n^2 > (2m-1)n.$$

This means that Theorem 2 is applicable over $\mathbb{Z}_p$ if $p$ satisfies (11) and if $\gcd(f,f_x)=1$ in $\mathbb{Z}_p[x,y]$. Hence for every such prime $p$ all the solutions of (4) and (5) over $\mathbb{Z}_p$ are of the forms (6) and (8). Thus, when considering the linear system for the coefficients of polynomials $g, h \in \mathbb{Z}_p[x,y]$ satisfying (4) and (5), we only need to consider polynomials of the form (9). Certainly the same is also true over $\mathbb{Q}$.

Let $I=I(P_f)$ denote the set of integral points in the Newton polytope of $f$ and let $g, h \in \mathbb{Z}[x,y]$ be of the form (9), i.e.

$$g=\sum_{(i,j)\in I} b_{ij}x^{i-1}y^j \text{ and } h=\sum_{(i,j)\in I} c_{ij}x^iy^{j-1},$$

where $b_{ij}, c_{ij} \in \mathbb{Z}$ and $b_{0j}=c_{i0}=0$ for $0 \leq i \leq m$ and $0 \leq j \leq n$. Note that $I$ has $t$ points, $g$ has $t-t_y$ coefficients and $h$ has $t-t_x$ coefficients. Let $M$ be the matrix of the linear system obtained from PDE (4). By Corollary 3, since $f$ is absolutely irreducible over $\mathbb{Q}$, $M$ has rank $\rho-1$, where $\rho=2t-(t_x+t_y)$ is the total number of coefficients of $g$ and $h$. Therefore, $M$ has a nonsingular submatrix $M_{\rho-1}$ of order $\rho-1$. We wish to bound the size of primes $p$ so that $M_{\rho-1}$ remains nonsingular modulo $p$. Certainly it is sufficient to have $p$ larger than the determinant of $M_{\rho-1}$. To estimate the latter, we write down the entries of $M$ explicitly.

Writing $f$ as $f = \sum_{(k,l)\in I} a_{k,l} x^k y^l$, we have

$$\begin{aligned} f\frac{\partial g}{\partial y} &= \Big(\sum_{(k,l)\in I} a_{kl}x^k y^l\Big)\Big(\sum_{(i,j)\in I} jb_{ij}x^{i-1}y^{j-1}\Big) \\ &= \sum_{\substack{(i,j)\in I\\(k,l)\in I}} ja_{kl}b_{ij}x^{i+k}y^{j+l}x^{-1}y^{-1} \\ &= \sum_{(r,s)\in 2I}\left(\sum_{\substack{i+k=r\\j+l=s\\(i,j),(k,l)\in I}} ja_{kl}b_{ij}\right)x^r y^s x^{-1}y^{-1}, \end{aligned}$$

where $2I = I + I$ is the Minkowski sum of $I$ with itself. Also

$$\begin{aligned} g\frac{\partial f}{\partial y} &= \Big(\sum_{(i,j)\in I} b_{ij}x^{i-1}y^{j}\Big)\Big(\sum_{(k,l)\in I} la_{kl}x^k y^{l-1}\Big) \\ &= \sum_{(r,s)\in 2I}\left(\sum_{\substack{i+k=r\\j+l=s\\(i,j),(k,l)\in I}} la_{kl}b_{ij}\right)x^r y^s x^{-1}y^{-1}. \end{aligned}$$

Hence

$$f\frac{\partial g}{\partial y} - g\frac{\partial f}{\partial y} = \sum_{(r,s)\in 2I}\left(\sum_{\substack{i+k=r\\j+l=s\\(i,j),(k,l)\in I}} (j-l)a_{kl}b_{ij}\right)x^r y^s x^{-1}y^{-1}. \tag{12}$$

Similarly,

$$f\frac{\partial h}{\partial x} - h\frac{\partial f}{\partial x} = \sum_{(r,s)\in 2I}\left(\sum_{\substack{i+k=r\\j+l=s\\(i,j),(k,l)\in I}} (i-k)a_{kl}c_{ij}\right)x^r y^s x^{-1}y^{-1}. \tag{13}$$

Let $A_{rs}$ and $B_{rs}$ denote the inner sums in (12) and (13), respectively. Then PDE (7) becomes

$$\sum_{(r,s)\in 2I}(A_{rs} - B_{rs})x^r y^s x^{-1}y^{-1} = 0,$$

or equivalently,

$$A_{rs} - B_{rs} = 0, \quad \text{for all } (r,s) \in 2I.$$

For each $(r,s) \in 2I$ we obtain a row of $M$ in which there are at most $t - t_y$ entries of the form $(j-l)a_{kl}$ corresponding to the coefficients $b_{ij}$ of $g$ and at most $t - t_x$ entries of the form $(k-i)a_{kl}$ from the coefficients $c_{ij}$ of $h$. Thus the $L_2$-norm of any row of the submatrix $M_{\rho-1}$ of $M$ is at most

$$\begin{aligned}\sqrt{\sum (j-l)^2 a_{kl}^2 + \sum (k-i)^2 a_{kl}^2} &\leq \sqrt{(n^2+m^2)\sum a_{kl}^2} \\ &\leq \sqrt{n^2+m^2}\cdot \|f\|_2.\end{aligned}$$

as $0 \leq j, l \leq n$, $0 \leq i, k \leq m$, and $\sum a_{kl}^2 \leq \|f\|_2$. Applying Hadamard's inequality, we obtain

$$|\det(M_{\rho-1})| \leq \left(\sqrt{n^2+m^2}\cdot\|f\|_2\right)^{\rho-1} = \left(\sqrt{n^2+m^2}\cdot\|f\|_2\right)^{2t-(t_x+t_y)-1}.$$

Therefore, for any prime $p$ such that

$$p > \left(\sqrt{m^2+n^2}\cdot\|f\|_2\right)^{2t-(t_x+t_y)-1},$$

$M_{\rho-1}$ has nonzero determinant modulo $p$, which implies that $M$ has rank $\rho-1$ over $\mathbb{Z}_p$. By Corollary 3 we then conclude that $f$ is absolutely irreducible over $\mathbb{Z}_p$. □

Theorem 1 follows from Theorem 6 and Lemma 7 below.

**Lemma 7.** *Let $f \in \mathbb{Z}[x,y]$ with bidegree $(m,n)$, where $m,n \geq 1$, and let $t$ be the number of integral points in $P(f)$. If $\gcd(f, f_x) = 1$ in $\mathbb{Q}[x,y]$ and $p$ is a prime such that*

$$p > \left(\sqrt{m^2+n^2}\cdot\|f\|_2\right)^{2t-3}, \tag{14}$$

*then $\gcd(f, f_x) = 1$ over $\mathbb{Z}_p$.*

The proof of this Lemma is similar to that of Theorem 6, although we consider a different linear system. We first introduce some notation. For a nonzero polynomial $f = \sum_{i,j} a_{ij}x^iy^j \in \mathbb{F}[x,y]$, where $\mathbb{F}$ is any field, we define the *weighted degree* of $f$ to be the maximum of the weighted degrees of its terms, where the weighted degree of a term $a_{ij}x^iy^j$ is $i + \pi j$ (here $\pi = 3.1415\ldots$). Since different terms have different exponent vectors, it follows that all the terms of a polynomial have different weighted degrees. Also, $\mathrm{wdeg}(f\cdot g) = \mathrm{wdeg}(f) + \mathrm{wdeg}(g)$, for any nonzero $f, g \in \mathbb{F}[x,y]$.

*Proof of Lemma 7.* Consider the linear system

$$fg_1 - f_xf_1 = 0, \tag{15}$$

where $f_1, g_1 \in \mathbb{Z}[x,y]$ satisfy

$$P(f_1) \subseteq P(f), \quad \mathrm{wdeg}(f_1) < \mathrm{wdeg}(f), \tag{16}$$

and

$$P(g_1) \subseteq P(f_x), \quad \mathrm{wdeg}(g_1) < \mathrm{wdeg}(f_x). \tag{17}$$

Note that if $\gcd(f, f_x) = 1$ then (15) implies that $f \mid f_1$ and $f_x \mid g_1$, thus (16) and (17) can not be satisfied for nonzero $f_1$ and $g_1$. Also note that if $h = \gcd(f, f_x)$ has at least two terms, then the linear system of (15), (16) and (17) has a nonzero solution, e.g. $f_1 = x^\alpha y^\beta f/h$ and $g_1 = x^\alpha y^\beta f_x/h$, where $x^\alpha y^\beta$ is any monomial in $h$ different from its leading monomial. To verify that $f_1, g_1$ is in fact a solution note that $(x^\alpha y^\beta)f = f_1h$ and so

$$(\alpha,\beta) + P(f) = P(f_1) + P(h) \supseteq P(f_1) + (\alpha,\beta),$$

by Lemma 5. Hence $P(f) \supseteq P(f_1)$. Besides,

$$(\alpha + \pi\beta) + \mathrm{wdeg}(f) = \mathrm{wdeg}(f_1) + \mathrm{wdeg}(h) > \mathrm{wdeg}(f_1) + (\alpha + \pi\beta),$$

as $\alpha + \pi\beta = \mathrm{wdeg}(x^\alpha y^\beta) < \mathrm{wdeg}(h)$. Thus $\mathrm{wdeg}(f) > \mathrm{wdeg}(f_1)$. Similarly for $g_1$. Therefore, if the linear system of (15), (16) and (17) has no nonzero solution then $\gcd(f, f_x)$ must be a monomial $x^s y^t$, where $s, t \geq 0$.

We write $f = \sum_{(k,l)\in I} a_{kl} x^k y^l$, where $a_{kl} \in \mathbb{Z}$ and $I = I(f)$ is the set of integral points in the Newton polytope of $f$. Then $f_x = \sum_{(k,l)\in I} k a_{kl} x^{k-1} y^l$. Let $f_1$ and $g_1 \in \mathbb{Z}[x, y]$ of the forms (16) and (17), respectively, $f_1 = \sum_{(i,j)\in I} b_{ij} x^i y^j$ and $g_1 = \sum_{(i,j)\in I} c_{ij} x^{i-1} y^j$, where $c_{0j} = 0$, $\mathrm{wdeg}(f_1) < \mathrm{wdeg}(f)$ and $\mathrm{wdeg}(g_1) < \mathrm{wdeg}(f_x)$. Note that $f_1$ has at most $t - 1$ coefficients, as it has weighted degree smaller than $f$. Also, since $\gcd(f, f_x) = 1$, $P(f)$ contains at least one point on the $y$-axis and so $P(f_x)$ has at most $t - 1$ points. Hence $g_1$ has at most $t - 2$ coefficients. So the total number of coefficients of $f_1$ and $g_1$, which we denote by $\rho$, is at most $2t - 3$.

The linear system of (15), (16) and (17) can be written as

$$\sum_{(r,s)\in 2I} (A_{rs} - B_{rs}) x^r y^s x^{-1} y^{-1} = 0,$$

where

$$A_{rs} = \sum_{\substack{i+k=r \\ j+l=s \\ (i,j),(k,l)\in I}} a_{kl} c_{ij} \quad \text{and} \quad B_{rs} = \sum_{\substack{i+k=r \\ j+l=s \\ (i,j),(k,l)\in I}} k a_{kl} b_{ij}.$$

Therefore,

$$A_{rs} - B_{rs} = 0, \quad \forall (r, s) \in 2I.$$

Let $M$ be the coefficient matrix of the system above. For each $(s, t) \in 2I$ we obtain a row of $M$ in which there are at most $t - 2$ entries of the form $a_{kl}$ corresponding to the coefficients $c_{ij}$ of $g_1$ and at most $t - 1$ entries of the form $-k a_{kl}$ corresponding to the coefficients $b_{ij}$ of $f_1$. So the $L_2$-norm of any row of $M$ is at most

$$\sqrt{\sum a_{kl}^2 + \sum k^2 a_{kl}^2} = \sqrt{\sum (1 + k^2) a_{kl}^2} \leq \sqrt{1 + m^2} \cdot \|f\|_2, \tag{18}$$

as $k \leq m$ and $\sum a_{kl}^2 \leq \|f\|_2$.

Since $\gcd(f, f_x) = 1$ in $\mathbb{Q}[x, y]$, the linear system has no nonzero solution. So $M$ has a nonsingular submatrix $M_\rho$ of order $\rho$. By Hadamard's inequality, the absolute value of the determinant of $M_\rho$ is at most

$$\left(\sqrt{1 + m^2} \cdot \|f\|_2\right)^\rho \leq \left(\sqrt{n^2 + m^2} \cdot \|f\|_2\right)^{2t-3}.$$

Therefore, for any prime $p$ satisfying (14), $M_\rho$ has nonzero determinant modulo $p$, so the linear system has no nonzero solution modulo $p$ and thus $\gcd(f, f_x)$ over $\mathbb{Z}_p$ is a monomial $x^s y^t$ for some $s, t \geq 0$.

Since $\gcd(f, f_x) = 1$ in $\mathbb{Q}[x, y]$, $f$ and $f_x$ have no nonconstant common factor over $\mathbb{Q}$, particularly no nonconstant monomial factor. Note that any $p$ satisfying (14) is greater than $H(f)$ and $H(f_x)$, and so the Newton polytopes of $f$ and $f_x$

modulo $p$ remain the same. Hence $f$ and $f_x$ cannot have a common nonconstant monomial factor in $\mathbb{Z}_p[x, y]$. Therefore, $\gcd(f, f_x) = 1$ in $\mathbb{Z}_p[x, y]$. □

**Remarks. (i)** In the proof above, the $L_2$-norm in (18) of a row of the matrix $M$ can be alternatively estimated as

$$\begin{aligned}\sqrt{\sum a_{kl}^2 + \sum k^2 a_{kl}^2} &\le \sqrt{(t-2)H(f)^2 + m^2(t-1)H(f)^2} \\ &< \sqrt{(1+m^2)(t-1)} \cdot H(f),\end{aligned}$$

since $|a_{kl}| \le H(f)$, and there are at most $t-2$ elements in the first sum and $t-1$ in the second. Hence Lemma 7 holds with

$$p > \left(\sqrt{(m^2+n^2)(t-1)} \cdot H(f)\right)^{2t-3} \tag{19}$$

replacing (14). Together with a similar change in the proof of Theorem 6, we obtain that (19) is also a lower bound for good primes. Note that (19) is a slight improvement of estimate (3). It also improves (2) in the special case when $f$ has $t$ nonzero coefficients with the same absolute value.

**(ii)** We should also mention that Lemma 7 can be generalized to the following result for any two polynomials, with a slight modification on its proof.

**Proposition 8.** *Let $f, g \in \mathbb{Z}[x, y]$ be any nonzero polynomials with $\gcd(f, g) = 1$. Then $\gcd(f, g) = 1$ in $\mathbb{Z}_p[x, y]$ for all primes $p$ satisfying*

$$p > \left(\|f\|_2^2 + \|g\|_2^2\right)^{(t_1+t_2-2)/2},$$

*where $t_1$ and $t_2$ denote the numbers of integral points in the Newton polytopes of $f$ and $g$, respectively.*

## 3. Examples

In the derivation of bound (2) in the previous section, we see that it guarantees that the rank $\rho - 1$ of the matrix $M$ of the system obtained from PDE (4) is preserved modulo $p$, where $\rho$ is the number of variables in the system. Indeed, bound (2) assures that every $(\rho-1) \times (\rho-1)$ nonsingular submatrix of $M$ remains nonsingular when reduced modulo $p$. However, for a polynomial $f$ to have a good reduction at $p$ it is sufficient that *one* of these submatrices remains nonsingular. For a given polynomial $f$, since $M$ is integral we may compute its Smith normal form, and its invariant factors tell us precisely how the rank of $M$ changes when reduced modulo $p$. In particular, primes of bad reduction must divide the largest invariant factor of $M$, so if a prime $p$ that does not divide it then $p$ is good for $f$.

As examples, we consider polynomials of the form $f = a\,x + b\,x^3 + c\,y + d\,xy^2 \in \mathbb{Z}[x, y]$, where $a, b, c$ and $d$ are nonzero. The Newton polytope of $f$ is shown in Figure 2 and we see that it has $t = 7$ integral points. When $f$ is absolutely irreducible over $\mathbb{Q}$, Theorem 1 guarantees that for any $p > (\sqrt{13} \cdot \|f\|_2)^{11}$, it remains absolutely irreducible over $\mathbb{Z}_p$.

For this $f$, polynomials $g, h \in \mathbb{Z}_p[x, y]$ of the form (9) can be written as

$$g = b_{10} + b_{20}\,x + b_{30}\,x^2 + b_{11}\,y + b_{21}\,xy + b_{12}\,y^2,$$

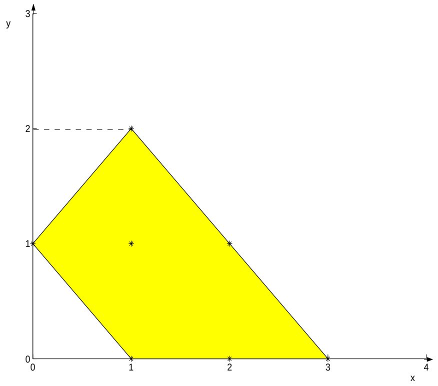

Fig. 2: The Newton polytope of $f$.

and

$$h = c_{01} + c_{11}\,x + c_{21}\,x^2 + c_{12}\,xy.$$

So $g$ and $h$ together have 10 coefficients (unknowns):

$$b_{10},\, b_{20},\, b_{30},\, b_{11},\, b_{21},\, b_{12},\, c_{01},\, c_{11},\, c_{21},\, c_{12}.$$

With the unknowns in this order, the coefficient matrix of the linear system is given by

$$M = \begin{bmatrix} c & 0 & 0 & 0 & 0 & 0 & -a & 0 & 0 & 0 \\ 0 & 0 & 0 & d & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -c & -d & 0 & 0 & c \\ 0 & 0 & 0 & -b & 0 & 0 & 0 & -2\,b & 0 & 0 \\ 0 & 0 & 0 & 0 & d & 0 & 0 & 0 & d & 0 \\ 0 & 2\,d & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -b & 0 & 0 & 0 & -b & 0 \\ 0 & 0 & 2\,d & 0 & 0 & -2\,b & 0 & 0 & 0 & -2\,b \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & c & 0 & -a & 0 & -3\,b & 0 & a & 0 \\ 0 & c & 0 & -a & 0 & 0 & 0 & 0 & 0 & 0 \\ 2\,d & 0 & 0 & 0 & 0 & -2\,a & 0 & 0 & 2\,c & 0 \end{bmatrix}$$

In particular, let us consider the following instances of $f$:

$$f_1 = x + x^3 - 2001\,y + xy^2,$$
$$f_2 = x + x^3 + 2001\,y - xy^2,$$

and

$$f_3 = x + 2001\,x^3 - y - xy^2.$$

These polynomials are absolutely irreducible over the rationals, since for each of them $M$ has rank 9. They have the same Euclidean norm: $\sqrt{4004004}$.

For polynomial $f_1$, $M$ has invariant factors

$$1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 2,\ \text{and } 32048032008,$$

where the largest has factorization

$$32,048,032,008 = 2^3 \cdot 3 \cdot 23 \cdot 29 \cdot 2002001.$$

Hence $f_1$ has a good reduction at all primes $p$ different from 2, 3, 23, 29 and 2002001. Note that

$$\begin{aligned} f_1 &\equiv (x - 2001y)(x^2 + 2001xy + 1) \quad \text{mod } 2002001, \\ f_1 &\equiv x\,(x^2 + y^2 + 1) \quad \text{mod } 29,\ 23,\ 3, \\ f_1 &\equiv (x + y)(x^2 + xy + 1) \quad \text{mod } 2. \end{aligned}$$

So the prime divisors of the largest invariant factor of $M$ are all bad for $f_1$.

For $f_2$, the invariant factors of $M$ are:

$$1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 2,\ \text{and } 32048016000,$$

and the largest is quite *smooth*:

$$32,048,016,000 = 2^7 \cdot 3 \cdot 5^3 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29.$$

We have

$$\begin{aligned} f_2 &\equiv x\,(x^2 - y^2 + 1) \quad \text{mod } 29,\ 23,\ 3, \\ f_2 &\equiv (x - y)(x^2 + xy + 1) \quad \text{mod } 13,\ 11,\ 7, \\ f_2 &\equiv (x + y)(x^2 - xy + 1) \quad \text{mod } 5, \\ f_2 &\equiv (x + y)(x^2 + xy + 1) \quad \text{mod } 2. \end{aligned}$$

Hence all the prime divisors of the largest invariant factor of $M$ are bad for $f_2$, and any other prime is good. In particular, $f_2$ has a good reduction at all primes $p > 29$.

For polynomial $f_3$, the corresponding matrix $M$ has a much smaller invariant factor:

$$8,000 = 2^6 \cdot 5^3.$$

So $f_3$ has a good reduction at all primes $p > 5$, and the only bad primes are 2 and 5:

$$\begin{aligned} f_3 &\equiv (x - y)(x^2 + xy + 1) \quad \text{mod } 5, \\ f_3 &\equiv (x + y)(x^2 + xy + 1) \quad \text{mod } 2. \end{aligned}$$

Finally, for the polynomial $f = x^2 + y^3 + 3x^4y^5$ mentioned in the introduction, the invariant factors of $M$ are:

$$1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 2,\ 2,\ 12,\ 24,\ \text{and } 48 = 2^4 \cdot 3.$$

So 2 and 3 are the only possible bad primes for $f$. However, the Newton polytope of $f$ mod $p$ is always indecomposable (when $p = 3$, it becomes a line segment), hence $f$ remains absolutely irreducible modulo $p$ for every prime $p$. So this polynomial has a good reduction at all primes!

These examples indicate how the size of good primes (or equivalently the size of bad primes) may vary, even for polynomials of the same shape and Euclidean norm. Some polynomials may have really large bad primes, some may have many small bad primes, while others none at all. Our bound (2) gives an upper bound for all possible bad primes of polynomials with the same shape and the same Euclidean norm.

*Acknowledgement.* The authors would like to thank a referee for his or her useful comments on the previous version of the paper. In particular, the current version of the bound in Theorem 1, which follows from the proof of our original bound (19), was pointed out by the referee.

## References

[1] S. Gao, Absolute irreducibility of polynomials via Newton polytopes, *Journal of Algebra* **237** (2001), 501-520.

[2] S. Gao, Factoring multivariate polynomials via partial differential equations, to appear in *Mathematics of Computation.* (28 pages)

[3] S. Gao and A. G.B. Lauder, Decomposition of polytopes and polynomials, *Discrete and Computational Geometry* **26** (2001), 89–104.

[4] E. Kaltofen, Fast parallel absolute irreducibility testing, *J. Symbolic Computation* **1** (1985), 57-67.

[5] E. Kaltofen, Effective Noether irreducibility forms and applications, *J. Comput. System Sci.* **5**, No.2 (1995), 274-295.

[6] A. Ostrowski, Zur arithmetischen theorie der algebraischen grössen, *Nachr. K. Ges. Wiss. Göttingen* (1919), 273-298.

[7] A. Ostrowski, On multiplication and factorization of polynomials, I. Lexicographic ordering and extreme aggregates of terms, *Aequationes Math.***13** (1975), 201-228.

[8] W. M. Ruppert, Reduzibilität ebener kurven, *J. Reine Angew. Math.* **369** (1986), 167-191.

[9] W. M. Ruppert, Reducibility of polynomials $f(x, y)$ modulo $p$, *Journal of Number Theory* **77** (1999), 62-70.

[10] A. Schinzel, "Polynomials with Special Regard to Reducibility", Encyclopedia of Mathematics and its Applications, Vol. 77, Cambridge Univ. Press, Cambridge, UK, 2000.

[11] W. M. Schmidt, "Equations over Finite Fields. An Elementary Approach", Lec. Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin, 1976.

[12] U. Zannier, On the reduction modulo $p$ of an absolutely irreducible polynomial $f(x, y)$, *Arch. Math.* **68** (1997), 129-138.

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, USA *E-mail address*: sgao@ces.clemson.edu

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, USA, and Faculdade de Matemática, PUCRS, Av. Ipiranga, 6681, Porto Alegre, RS 90619-900, Brazil *E-mail address*: vrodrig@ces.clemson.edu