Math. Proc. Camb. Phil. Soc. (2019), **167**, 531–547 © *Cambridge Philosophical Society* 2018
doi:10.1017/S0305004118000452
First published online 20 June 2018

An explicit dense universal Hilbert set

BY MICHAEL FILASETA AND ROBERT WILCOX

Department of Mathematics, LeConte College, 1523 *Greene Street*
University of South Carolina, Columbia, SC 29208 *U.S.A.*
e-mails: filaseta@math.sc.edu, rwilcox5@gmail.com

(*Received* 25 *April* 2018)

Abstract

We provide the first explicit example of a universal Hilbert set $\mathcal{S}$ having asymptotic density 1 in the set of integers. More precisely, the number of integers *not* in $\mathcal{S}$ with absolute value $\leqslant X$ is bounded by $X/(\log X)^{\delta}$, where $\delta = 1 - (1 + \log\log 2)/(\log 2) = 0.086071\ldots$.

1. *Introduction*

Hilbert's Irreducibility Theorem in various forms states that an irreducible polynomial in several variables can find infinitely many specialisations of some preselected variables so that the resulting polynomial remains irreducible in the remaining variables. The theorem was introduced by Hilbert [**11**] to show the existence of polynomials of degree n having Galois group the symmetric group S_n for each positive integer n and to show the existence of polynomials of degree n having Galois group the alternating group A_n for each positive integer n. Since then, various versions of Hilbert's Theorem have been established. More can be said with regard to polynomials in two variables and that is our focus here. With regard to references for proofs and other variations of this theorem, we mention the books by Fried and Jarden [**7**], Hadlock [**9**], Schinzel [**13**, **14**] and Serre [**16**].

For $F(x, y) \in \mathbb{Z}[x, y]$, irreducible in $\mathbb{Q}[x, y]$ and with $\deg_x(F) \geqslant 1$, it can be shown that for almost all $y_0 \in \mathbb{Z}$, the polynomial $F(x, y_0)$ is irreducible in $\mathbb{Q}[x]$. Equivalently,

$$|\{y_0 \in \mathbb{Z} : |y_0| \leqslant Y, F(x, y_0) \text{ is reducible in } \mathbb{Q}[x]\}| = o(Y)$$

as $Y \to \infty$. As a consequence of Siegel's Lemma, stronger statements can be made, bounding the left-hand side by $O\left(Y^{\gamma}\right)$ for some $\gamma < 1$ (see [**12**]).

Our interest is in the related topic of universal Hilbert sets. A *universal Hilbert set* is an infinite set $\mathcal{S} \subseteq \mathbb{Z}$ having the property that for every $F(x, y) \in \mathbb{Z}[x, y]$ which is irreducible in $\mathbb{Q}[x, y]$ and satisfies $\deg_x(F) \geqslant 1$, we have that for all but finitely many $y_0 \in \mathcal{S}$, the polynomial $F(x, y_0)$ is irreducible in $\mathbb{Q}[x]$. Of significance here is the finiteness of the number of $y_0 \in \mathcal{S}$ with $F(x, y_0)$ irreducible and that $\mathcal{S}$ is fixed and so independent of $F(x, y) \in \mathbb{Z}[x, y]$.

The existence of universal Hilbert sets is credited to Gilmore and Robinson [**8**]. The first explicit example given by Sprindžuk [**18**] is the set

$$\left\{\left\lfloor \exp\left(\sqrt{\log\log n}\right)\right\rfloor + n!2^{n^2} : n \in \mathbb{Z}, n \geqslant 3\right\}.$$

A number of explicit examples of universal Hilbert sets have been shown to exist since then.

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

Some nice examples include

$$\{2^n + n : n \in \mathbb{N}\}, \quad \{2^n + 3^n : n \in \mathbb{N}\},$$
$$\{\lfloor \log\log |n| \rfloor + n^3 : n \in \mathbb{Z}, |n| \geqslant 3\} \quad \text{and} \quad \{p_n \prod_{p_i \leqslant \log\log n} p_i : n \in \mathbb{Z}, n \geqslant 3\},$$

where in the last example p_i denotes the ith prime. The first of these is due to Dèbes and Zannier [**5**], the second to Corvaja and Zannier [**4**], the third to Bilu [**1**] and the fourth to Zannier [**19**]. The last example is an explicit example with almost linear growth.

A natural pursuit is to determine how dense a universal Hilbert set can be. The papers by Bilu [**1**] and Dèbes and Zannier [**5**] give an answer to this by independently establishing that there exist sets of asymptotic density 1 in $\mathbb{Z}$ which are universal Hilbert sets. Bilu's argument further gives a method of constructing such a set. They do not, however, give explicit examples of universal Hilbert sets of density 1.

One goal in this paper is to give an explicit example, though not as aesthetically pleasing as the examples above, of a universal Hilbert set with density 1. To be more precise, let $w(X)$ be an arbitrary real valued function which tends to infinity with X. We obtain an explicit universal Hilbert set $\mathcal{S} \subset \mathbb{Z}$ for which

$$|\{m \in \mathbb{Z} : m \notin \mathcal{S}, |m| \leqslant X\}| \ll \frac{X w(X)}{(\log X)^{\delta} (\log\log X)^{3/2}} \tag{1·1}$$

as $X \to \infty$, where $\delta = 1 - (1 + \log\log 2)/(\log 2) = 0.086071\ldots$. For convenience of the presentation, we do this by giving details for an argument which instead gives

$$|\{m \in \mathbb{Z} : m \notin \mathcal{S}, |m| \leqslant X\}| \ll \frac{X}{(\log X)^{\delta}}, \tag{1·2}$$

and note that (1·1) can be obtained by modifying the expressions $\log\log j$ and $\log\log\log j$ in our definition of $\mathcal{S}$ below. Our main tools for establishing such upper bounds will be Siegel's Lemma [**17**] on the finiteness of integral points on a curve of genus $\geqslant 1$ and a theorem of Ford [**6**] which counts the number of integers with divisors in a given interval. We elaborate on these results in the next two sections.

We define our set $\mathcal{S}$ next. For integers $j \geqslant 3$, $k \geqslant 2$, ℓ and ℓ' with $\ell \neq 0$, set

$$Y(j,k,\ell,\ell') = \Bigg\{ m \in \mathbb{Z} : |m| \in (2^j, 2^{j+1}] \text{ and } |\ell m + \ell'| \text{ has no divisor in } \left(\frac{2^{j/k}}{\log\log j}, 2^{j/k} \log\log j \right] \Bigg\}.$$

For $j \geqslant 3$, let

$$M(j) = \max\{2, \log\log\log j\}.$$

Then, for the remainder of the paper, we set $\mathcal{S}$ to be

$$\mathcal{S} = \bigcup_{j=3}^{\infty} \bigcap_{2 \leqslant k \leqslant M(j)} \bigcap_{\substack{-M(j) \leqslant \ell \leqslant M(j) \\ \ell \neq 0}} \bigcap_{-M(j) \leqslant \ell' \leqslant M(j)} Y(j,k,\ell,\ell'). \tag{1·3}$$

The lower bound on j is simply to ensure that $\log\log j > 0$. If $m \in \mathcal{S}$, then $-m \in \mathcal{S}$. Since $j \geqslant 3$, the least positive element of $\mathcal{S}$ is 9. The first few integers $\geqslant 9$ which are *not* in $\mathcal{S}$ are

$$65537, \quad 65538, \quad 65641, \quad 65642, \quad 65645, \quad 65646 \quad \text{and} \quad 65647.$$

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

This starts around $2^{16} = 65536$ since for $j < 16$ the interval in the definition of $Y(j, k, \ell, \ell')$ is empty. There are 461845 elements of $\mathcal{S}$ up to 10^6. To put this in some perspective, although the expression $X/(\log X)^\delta$ on the right of (1·2) is $o(X)$ as X goes to infinity, it is $> X/2$ for $1 < X \leqslant 10^{1365}$.

Roughly, $\mathcal{S}$ is the set of integers m, with $|m| \geqslant 9$, such that every linear expression of the form $\ell m + \ell'$, with ℓ and ℓ' small positive integers, has no divisor around the kth root of $|m|$ for some $k \geqslant 2$ also small. Here, "small" means small relative to the size of $|m|$. For the arguments, we have some flexibility on what "small" is but we want "small" to tend to infinity as m tends to infinity. The smaller the better in terms of obtaining a bound of the form (1·1). We state our first result taking advantage of the above set-up.

THEOREM 1·1. *The set $\mathcal{S}$ in* (1·3) *is a universal Hilbert set satisfying* (1·2) *as $X \to \infty$, where $\delta = 1 - (1 + \log\log 2)/(\log 2) = 0.086071\ldots$.*

For our next result, some preliminary background related to Theorem 1·1 is instructive. Let $F(x, y) \in \mathbb{Z}[x, y]$ be irreducible in $\mathbb{Q}[x, y]$ with $n = \deg_x(F) \geqslant 1$. Write

$$F(x, y) = f_n(y)x^n + f_{n-1}(y)x^{n-1} + \cdots + f_2(y)x^2 + f_1(y)x + f_0(y),$$

where each $f_j(y)$ is in $\mathbb{Z}[y]$ and $f_n(y) \not\equiv 0$. We are interested in determining (or quantifying) the values of $y \in \mathbb{Z}$ for which $F(x, y)$ is reducible in $\mathbb{Q}[x]$. It will be convenient to work with a monic polynomial. A finite set of $y \in \mathbb{Z}$ can be ignored for our purposes. With that in mind, we use that, with $y \in \mathbb{Z}$ satisfying $f_n(y) \neq 0$, the polynomial $F(x, y)$ is reducible in $\mathbb{Q}[x]$ if and only if $f_n(y)^{n-1}F(x, y)$ is reducible in $\mathbb{Q}[x]$. Observe that

$$\begin{aligned} f_n(y)^{n-1}F(x, y) &= f_n(y)^{n-1}\sum_{j=0}^{n} f_j(y)x^j = \sum_{j=0}^{n} f_n(y)^{n-1-j}f_j(y)\big(f_n(y)x\big)^j \\ &= \big(f_n(y)x\big)^n + f_{n-1}(y)\big(f_n(y)x\big)^{n-1} \\ &\qquad + f_n(y)^{n-2}f_1(y)\big(f_n(y)x\big) + f_n(y)^{n-1}f_0(y). \end{aligned}$$

We define $g_j(y) = f_n(y)^{n-1-j}f_j(y)$ for $0 \leqslant j \leqslant n$ and consider

$$\begin{aligned} G(x, y) &= g_n(y)x^n + g_{n-1}(y)x^{n-1} + \cdots + g_2(y)x^2 + g_1(y)x + g_0(y) \\ &= x^n + g_{n-1}(y)x^{n-1} + \cdots + g_2(y)x^2 + g_1(y)x + g_0(y) \in \mathbb{Z}[y][x]. \end{aligned}$$

Note that $y \in \mathbb{Z}$ for which $F(x, y)$ is reducible in $\mathbb{Q}[x]$ and $f_n(y) \neq 0$ correspond to $y \in \mathbb{Z}$ for which $G(x, y)$ is reducible in $\mathbb{Q}[x]$ and $f_n(y) \neq 0$.

We view $G(x, y)$ as fixed as well as an integer k with $1 \leqslant k \leqslant n/2$. Suppose we want to say something about the integers $y_0 \in \mathbb{Z}$ for which there is a monic polynomial in $\mathbb{Z}[x]$ of degree k in x which divides $G(x, y_0)$. For this purpose, we write

$$H(x) = x^k + h_{k-1}x^{k-1} + \cdots + h_2x^2 + h_1x + h_0,$$

where the h_j are unknowns in $\mathbb{Z}$. We are interested in the integers $y_0 \in \mathbb{Z}$ such that there exist choices for the $h_j = h_j(y_0)$ for which $H(x)$ divides $G(x, y_0)$.

We divide $G(x, y)$ by $H(x)$ as a polynomial in x to obtain a remainder

$$R(x) = r_{k-1}x^{k-1} + r_{k-2}x^{k-2} + \cdots + r_1x + r_0.$$

The coefficients of $R(x)$ are in $\mathbb{Z}[h_0, \ldots, h_{k-1}, y]$, and we write $r_j = r_j(h_0, \ldots, h_{k-1}, y)$ for $0 \leqslant j \leqslant k - 1$. We deduce that for $y_0 \in \mathbb{Z}$, the following are equivalent:

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

(i) the polynomial $G(x, y_0)$ has a factor of degree k in $\mathbb{Z}[x]$;
(ii) there is a k-tuple $(h_0^*, \dots, h_{k-1}^*) \in \mathbb{Z}^k$ such that $r_j(h_0^*, \dots, h_{k-1}^*, y_0) = 0$ for every $j \in \{0, 1, \dots, k-1\}$.

Our interest is in showing that the latter holds for only finitely many $y_0 \in \mathcal{S}$, with $\mathcal{S}$ defined as above. In other words, we want to show that the variety

$$V(r_0, r_1, \dots, r_{k-1})$$

over $\mathbb{C}$ intersected with $\mathbb{Z}^{k+1}$ has finitely many elements with y component in $\mathcal{S}$.

This variety over $\mathbb{C}$ has a special property that will make this possible. For fixed y_0 in $\mathbb{C}$, there are only finitely many tuples $(h_0^*, \dots, h_{k-1}^*) \in \mathbb{C}^k$ such that $r_j(h_0^*, \dots, h_{k-1}^*, y_0) = 0$ for every $j \in \{0, 1, \dots, k-1\}$. To see this, simply observe that with the $h_j = h_j^*$ so chosen, $R(x) = 0$ so that the polynomial $H(x)$ is a factor of $G(x, y_0)$ and necessarily $H(x)$ has its k roots from among the n roots of $G(x, y_0)$. As there are a finite number of possibilities for these roots (for fixed y_0), there are a finite number of tuples $(h_0^*, \dots, h_{k-1}^*) \in \mathbb{C}^k$ as above.

With the above in mind, to prove Theorem 1·1, our next result will suffice. As we will establish Theorem 1·1 independently of our next result, we will not elaborate on the details, but the proofs of these two results will make the connection clear.

THEOREM 1·2. *Let $\mathcal{S}$ be as in* (1·3). *Let the variety*

$$V = V(r_0, r_1, \dots, r_{k-1}), \qquad \text{with } r_j = r_j(h_0, \dots, h_{k-1}, y) \in \mathbb{Z}[h_0, \dots, h_{k-1}, y],$$

over the complex numbers have the property that for each fixed $y_0 \in \mathbb{C}$, there are finitely many points $(h_0^*, \dots, h_{k-1}^*) \in \mathbb{C}^k$ such that $(h_0^*, \dots, h_{k-1}^*, y_0) \in V$. Suppose that there are infinitely many points $(h_0^*, \dots, h_{k-1}^*, y_0)$ in $V \cap \mathbb{Z}^{k+1}$ with $y_0 \in \mathcal{S}$. Then there exist $\hat{h}_t(y) \in \mathbb{Q}(y)$ for $t \in \{1, 2, \dots, k-1\}$ such that the set of

$$(\hat{h}_0(y_0), \dots, \hat{h}_{k-1}(y_0), y_0) \in V \cap \big(\mathbb{Z}^k \times \mathcal{S}\big)$$

is an infinite set.

2. *The asymptotic estimates*

In this section, we show that (1·2) holds. We make use of the following result by Ford [**6**].

THEOREM 2·1 (Ford, 2008). *Let x, y and z be real numbers with $x \geqslant 10^5$, $100 \leqslant y \leqslant \sqrt{x}$, $2y \leqslant z \leqslant y^2$ and $z \leqslant x$. Set $H(x, y, z)$ to be the number of positive integers $n \leqslant x$ for which some divisor d of n satisfies $d \in (y, z]$. Set*

$$u = \frac{\log z}{\log y} - 1,$$

and let $\delta = 1 - (1 + \log\log 2)/(\log 2) = 0.086071\dots$. Then

$$\frac{H(x, y, z)}{x} \asymp u^{\delta}\big(\log(2/u)\big)^{-3/2}.$$

We consider $j \geqslant j_0 = 10^{703}$ so that $M(j) = \log\log\log j > 2$. We take k, ℓ and ℓ' as in the definition of $\mathcal{S}$. Let $m \in \mathbb{Z}$ be such that $|m| \in (2^j, 2^{j+1}]$, and let $n = |\ell m + \ell'|$ in Theorem 2·1. Then

$$\begin{aligned} 2^{j-1} &\leqslant 2^j - \log\log\log j \leqslant |\ell||m| - |\ell'| \leqslant |n| \\ &\leqslant |\ell||m| + |\ell'| \leqslant 2^{j+1}\log\log\log j + \log\log\log j \leqslant 2^{j+2}\log\log\log j. \end{aligned}$$

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

We take $x = X = 2^{j+2}\log\log\log j$, $y = (2^{j/k})/(\log\log j)$ and $z = 2^{j/k}\log\log j$ in Theorem 2·1. Observe that n is a positive integer $\leqslant X$. Also, for a fixed $n \leqslant X$ and fixed ℓ and ℓ' as in (1·3), there are at most two choices of m satisfying $|m| \in (2^j, 2^{j+1}] \cap \mathbb{Z}$ and $n = |\ell m + \ell'|$. One checks that

$$u \sim \frac{2k\log\log\log j}{j\log 2}, \quad \text{as } j \to \infty.$$

For fixed j, k, ℓ and ℓ' as in (1·3) with j sufficiently large, Theorem 2·1 implies

$$|\{m \in \mathbb{Z} : |m| \in (2^j, 2^{j+1}], m \notin Y(j,k,\ell,\ell')\}| \ll \frac{k^\delta(\log\log\log j)^2 2^j}{(j\log 2)^\delta(\log j)^{3/2}}.$$

As there are $\ll \log\log\log j$ choices for each of k, ℓ and ℓ' in (1·3), we deduce that for j fixed as in (1·3), we have

$$\big|\{m \in \mathbb{Z} : |m| \in (2^j, 2^{j+1}], m \notin \mathcal{S}\}\big| \ll \frac{(\log\log\log j)^6 2^j}{(j\log 2)^\delta(\log j)^{3/2}}.$$

Hence,

$$\begin{aligned}\big|\{m \in \mathbb{Z} : m \notin \mathcal{S}, |m| \leqslant X\}\big| &\ll \sum_{\substack{j \geqslant j_0 \\ 2^j \leqslant X}} \frac{(\log\log\log j)^6 2^j}{(j\log 2)^\delta(\log j)^{3/2}} \ll \sum_{\substack{j \geqslant j_0 \\ 2^j \leqslant X}} \frac{2^j}{(j\log 2)^\delta} \\ &\ll \sum_{j_0 \leqslant j \leqslant (\log_2 X)/2} \frac{2^j}{(j\log 2)^\delta} + \sum_{(\log_2 X)/2 < j \leqslant \log_2 X} \frac{2^j}{(j\log 2)^\delta} \\ &\ll \sum_{j_0 \leqslant j \leqslant (\log_2 X)/2} \frac{\sqrt{X}}{(j_0\log 2)^\delta} + \sum_{(\log_2 X)/2 < j \leqslant \log_2 X} \frac{2^j}{((\log X)/2)^\delta} \\ &\ll \sqrt{X}\log X + \frac{X}{(\log X)^\delta} \ll \frac{X}{(\log X)^\delta},\end{aligned}$$

and (1·2) holds.

Before proceeding, we comment that a weakened form of (1·2), implying the left-hand side there is $o(X)$, can be obtained in another way. A classical asymptotic estimate in Number Theory is

$$\sum_{n \leqslant X} \big(\omega(n) - \log\log n\big)^2 \ll X\log\log X, \tag{2·1}$$

where $\omega(n)$ is the number of prime divisors (included to their multiplicity) of n (see [**10**]). This is often stated in proofs that the *normal order* of the number of prime divisors of n is $\log\log n$. Loosely speaking, (2·1) implies that asymptotically almost all n have around $\log\log n$ prime factors.

Fix j, k, ℓ and ℓ' as in (1·3). Let $m \in \mathbb{Z}$ be such that $|m| \in (2^j, 2^{j+1}]$. Suppose that $|\ell m + \ell'| = d_1 d_2$ where

$$d_1 \in \left(\frac{2^{j/k}}{\log\log j}, 2^{j/k}\log\log j\right].$$

Then

$$\omega(|\ell m + \ell'|) = \omega(d_1) + \omega(d_2).$$

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

One can use (2·1) to show that typically the size of $\omega(|\ell m + \ell'|)$ forces either $\omega(d_1)$ to be small compared to $\log\log d_1$ or $\omega(d_2)$ to be small compared to $\log\log d_2$. This in turn is enough to establish that the left-hand side of (1·2) is $o(X)$ (and a bit smaller). We omit the details.

3. *Siegel's Lemma*

We will make use of a classical result of Siegel [**17**] which we state as follows.

THEOREM 3·1 (Siegel's Lemma). *Let $f(x, y)$ be in $\mathbb{Z}[x, y]$ with $f(x, y)$ irreducible in $\mathbb{C}[x, y]$. If there are infinitely many points $(x_0, y_0) \in \mathbb{Z}^2$ such that $f(x_0, y_0) = 0$, then there exist polynomials $u_j(t)$ and $v_j(t)$ in $\mathbb{Z}[t]$ for $j \in \{1, 2\}$ satisfying both of the following*:

(i) *for all but finitely many $(x', y') \in \mathbb{C}^2$ satisfying $f(x', y') = 0$, the equations $x' = u_1(t)/v_1(t)$ and $y' = u_2(t)/v_2(t)$ hold for some $t \in \mathbb{C}$;*

(ii) *for all but finitely many $(x', y') \in \mathbb{Q}^2$ and $t \in \mathbb{C}$ such that $x' = u_1(t)/v_1(t)$ and $y' = u_2(t)/v_2(t)$, we have $t \in \mathbb{Q}$.*

A more succinct form of Siegel's Lemma is that there are finitely many integral points on the curve $f(x, y) = 0$ if $f(x, y) \in \mathbb{Z}[x, y]$ is irreducible in $\mathbb{C}[x, y]$ and of genus $\geqslant 1$. Observe that the condition in Theorem 3·1 that there are infinitely many points $(x_0, y_0) \in \mathbb{Z}^2$ such that $f(x_0, y_0) = 0$ together with (i) imply that

$$f\left(\frac{u_1(t)}{v_1(t)}, \frac{u_2(t)}{v_2(t)}\right) \equiv 0.$$

In other words, if one expands the left-hand side above, then the numerator of the resulting fraction will be identically 0.

Theorem 3·1 requires $f(x, y)$ to be irreducible in $\mathbb{C}[x, y]$, and our interest is in more general polynomials in $\mathbb{Q}[x, y]$. The following provides us with this flexibility.

LEMMA 3·2. *Let $f(x, y)$ be in $\mathbb{Z}[x, y]$ with $f(x, y)$ irreducible in $\mathbb{Q}[x, y]$. Suppose that $f(x, y)$ is reducible in $\mathbb{C}[x, y]$. Then there are finitely many rational points on the curve $f(x, y) = 0$.*

This result is well-known (see for example [**2**, footnote 7]).

4. *Properties of $\mathcal{S}$*

The main new aspect of our approach to obtaining information on universal Hilbert sets is this section. Our aim here is to show an important property of $\mathcal{S}$ that connects it to integer points on curves (Lemma 4·2 below).

LEMMA 4·1. *Let $f(x)$ and $g(x)$ be relatively prime polynomials in $\mathbb{Z}[x]$. Let $w(x)$ be an arbitrary non-constant polynomial in $\mathbb{Z}[x]$. Then there is at most one $y \in \mathbb{Z}$ such that $f(x) + yg(x)$ has the factor $w(x)$ in $\mathbb{Z}[x]$.*

Proof. Assume otherwise. By replacing $w(x)$ with $w(x)$ divided by its content, we may take the content of $w(x)$ to be 1 and do so. Then there are two distinct integers y_1 and y_2 and polynomials $h_1(x)$ and $h_2(x)$ in $\mathbb{Z}[x]$ such that $f(x) + y_j g(x) = w(x)h_j(x)$ for $j \in \{1, 2\}$. Hence,

$$(y_1 - y_2)g(x) = f(x) + y_1 g(x) - f(x) - y_2 g(x) = w(x)(h_1(x) - h_2(x)).$$

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

Since the content of $w(x)$ is 1, we deduce that $w(x)$ divides $g(x)$. But then $w(x)$ divides both $f(x) + y_1 g(x)$ and $y_1 g(x)$, and hence $w(x)$ divides their difference $f(x)$. This contradicts that $\gcd(f(x), g(x)) = 1$.

LEMMA 4·2. *Let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$ with*

$$\gcd(f, g) = 1 \quad \textit{and} \quad \max\{\deg f, \deg g\} \geqslant 2. \tag{4·1}$$

Let $\mathcal{S}$ be as in (1·3). *Let $\mathcal{Y}$ be the set of $y \in \mathbb{Z}$ for which $f(x) + yg(x)$ has a linear factor in $\mathbb{Z}[x]$. Then $\mathcal{Y} \cap \mathcal{S}$ is finite. Furthermore, if $\deg f > \deg g \geqslant 1$, then $\mathcal{Y}$ is finite.*

Before beginning the proof, we note that (4·1) implies that both $f(x)$ and $g(x)$ are non-zero. The lemma is indicating that the two conditions in (4·1) on $f(x)$ and $g(x)$ are sufficient to conclude that the set of $y \in \mathbb{Z}$ which are in $\mathcal{S}$ satisfying $f(x) + yg(x)$ has a linear factor in $\mathbb{Z}[x]$ is a finite set. In other words, if $f(x)$ and $g(x)$ are non-zero polynomials in $\mathbb{Z}[x]$ with $\gcd(f, g) = 1$ and if there are infinitely many $y \in \mathcal{S}$ satisfying $f(x) + yg(x)$ has a linear factor in $\mathbb{Z}[x]$, then each of $f(x)$ and $g(x)$ is either a constant or a linear polynomial.

Proof of Lemma 4·2. For a non-zero polynomial $w(x)$, we denote by d_w the degree of $w(x)$, by ℓ_w the leading coefficient of $w(x)$, and by h_w the height of $w(x)$ (the maximum of the absolute values of the coefficients of $w(x)$). For two polynomials $w_1(x)$ and $w_2(x)$, we denote the resultant of $w_1(x)$ and $w_2(x)$ by $\mathrm{Res}(w_1, w_2)$.

First, we consider the case that $d_f > d_g \geqslant 1$. To prove $\mathcal{Y}$ is finite, we show that if $y \in \mathbb{Z}$ with $|y|$ sufficiently large, then $f(x) + yg(x)$ does not have a linear factor in $\mathbb{Z}[x]$. Since $d_f > d_g$, there are $f_0(x)$ and $g_0(x)$ in $\mathbb{Z}[x]$ with $f_0(\ell_f x) = \ell_f^{d_f - 1} f(x)$ and $g_0(\ell_f x) = \ell_f^{d_f - 1} g(x)$. Furthermore, $f_0(x)$ is monic, $d_{f_0} = d_f$, $d_{g_0} = d_g$, and $f_0(x)$ and $g_0(x)$ are relatively prime in $\mathbb{Z}[x]$. Observe that $f(x) + yg(x)$ has a linear factor in $\mathbb{Z}[x]$ if and only if

$$F_y(x) = f_0(x) + yg_0(x) = \ell_f^{d_f - 1}(f(x/\ell_f) + yg(x/\ell_f))$$

has a linear factor in $\mathbb{Z}[x]$. Since $d_f > d_g$ and $f_0(x)$ is monic, we have $F_y(x)$ is monic. Thus, if $F_y(x)$ has a linear factor in $\mathbb{Z}[x]$, then $F_y(x)$ has an integer root. Let $R = \mathrm{Res}(f_0, g_0)$. Since $f_0(x)$ and $g_0(x)$ are relatively prime in $\mathbb{Z}[x]$, $R \neq 0$ and there are polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ satisfying

$$f_0(x)u(x) + g_0(x)v(x) = R. \tag{4·2}$$

Let $m \in \mathbb{Z}$ be such that $|m|$ is sufficiently large so that $|g_0(m)| > R$. Note this is possible since $d_g \geqslant 1$. We claim that $x - m$ cannot be a factor of $F_y(x)$ for any integer y. Indeed, if $F_y(m) = 0$, then $f_0(m) = -yg_0(m)$ and $g_0(m)$ divides $f_0(m)$. This contradicts (4·2) since $|g_0(m)| > R$ and $R \neq 0$. Therefore, there are finitely many $m \in \mathbb{Z}$ such that $x - m$ can be a factor of $F_y(x)$. Lemma 4·1 now implies there are finitely many $y \in \mathbb{Z}$ such that $F_y(x)$ and, hence, $f(x) + yg(x)$ has a linear factor. Thus, if $y \in \mathbb{Z}$ is sufficiently large, then $f(x) + yg(x)$ does not have a linear factor in $\mathbb{Z}[x]$. Hence, $\mathcal{Y}$ is finite.

Next, we consider the case that $g(x)$ is a constant. Since $\max\{d_f, d_g\} \geqslant 2$, we have here that $d_f \geqslant 2$. As $\gcd(f, g) = 1$, we see that $g(x) = \ell_g \neq 0$. We work with $F_y(x) = f_0(x) + yg_0(x)$, as above, so that $f_0(x) = \ell_f^{d_f - 1} f(x/\ell_f)$ and $g_0(x) = \ell_f^{d_f - 1} \ell_g$. Recall that $f_0(x)$ is monic and in $\mathbb{Z}[x]$. Further, if $f(x) + yg(x)$ has a linear factor in $\mathbb{Z}[x]$, then $F_y(x) = f_0(x) + yg_0(x)$ has an integer root, say r. The constant term of $F_y(x)$ is $f_0(0) + y\ell_f^{d_f - 1}\ell_g$ and each coefficient other than this constant term has absolute value $\leqslant h_{f_0}$. Also, $f_0(0)$ and h_{f_0} only depend on $f(x)$.

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

We restrict to

$$|y| > \frac{|f_0(0)| + h_{f_0} d_f((3h_{f_0})^{d_f} + 1)}{|\ell_f|^{d_f-1}|\ell_g|}. \tag{4·3}$$

For $z \in \mathbb{C}$ with $|z| < 3h_{f_0}$, we deduce from (4·3) that

$$\begin{aligned} |F_y(z)| &\geqslant |f_0(0) + y\ell_f^{d_f-1}\ell_g| - h_{f_0}(|z|^{d_f} + |z|^{d_f-1} + \cdots + |z|) \\ &\geqslant |\ell_f|^{d_f-1}|\ell_g||y| - |f_0(0)| - h_{f_0} d_f(|z|^{d_f} + 1) \\ &> |\ell_f|^{d_f-1}|\ell_g||y| - |f_0(0)| - h_{f_0} d_f((3h_{f_0})^{d_f} + 1) > 0. \end{aligned}$$

Hence, the zeroes of $F_y(x)$ have absolute value $\geqslant 3h_{f_0}$. In particular, we must have $|r| \geqslant 3h_{f_0}$. This in turn implies

$$\begin{aligned} h_{f_0}(|r|^{d_f-1} + |r|^{d_f-2} + \cdots + |r|) &\leqslant h_{f_0}|r|^{d_f}\left(\frac{1}{|r|} + \frac{1}{|r|^2} + \frac{1}{|r|^3} + \cdots\right) \\ &\leqslant |r|^{d_f}\left(\frac{1}{3} + \frac{1}{3^2} + \frac{1}{3^3} + \cdots\right) = \frac{|r|^{d_f}}{2}. \end{aligned}$$

Hence,

$$\begin{aligned} 0 = |F_y(r)| &\geqslant |f_0(0) + y\ell_f^{d_f-1}\ell_g| - |r|^{d_f} - h_{f_0}(|r|^{d_f-1} + |r|^{d_f-2} + \cdots + |r|) \\ &\geqslant |y||\ell_f|^{d_f-1}|\ell_g| - |f_0(0)| - \frac{3|r|^{d_f}}{2}. \end{aligned}$$

Since $|r| \geqslant 3h_{f_0} \geqslant 3f_0(0)$, we have

$$\begin{aligned} 3|r|^{d_f} &\geqslant 2|y||\ell_f|^{d_f-1}|\ell_g| - 2|f_0(0)| \\ &\geqslant 2|y||\ell_f|^{d_f-1}|\ell_g| - \frac{2|r|}{3} \geqslant 2|y||\ell_f|^{d_f-1}|\ell_g| - \frac{2|r|^{d_f}}{3} \end{aligned}$$

implying

$$|r| \geqslant \left(\frac{6}{11}\right)^{1/d_f} |\ell_f|^{1-(1/d_f)}|\ell_g|^{1/d_f}|y|^{1/d_f}.$$

We also have

$$\begin{aligned} 0 = |F_y(r)| &\geqslant |r|^{d_f} - |f_0(0) + y\ell_f^{d_f-1}\ell_g| - h_{f_0}(|r|^{d_f-1} + |r|^{d_f-2} + \cdots + |r|) \\ &\geqslant |r|^{d_f} - |y||\ell_f|^{d_f-1}|\ell_g| - \frac{|r|^{d_f}}{3} - \frac{|r|^{d_f}}{2} \end{aligned}$$

so that

$$|r|^{d_f} \leqslant 6|y||\ell_f|^{d_f-1}|\ell_g| \implies |r| \leqslant 6^{1/d_f}|\ell_f|^{1-(1/d_f)}|\ell_g|^{1/d_f}|y|^{1/d_f}.$$

We therefore have positive constants $c_1 = c_1(f, g)$ and $c_2 = c_2(f, g)$ for which

$$c_1|y|^{1/d_f} < |r| < c_2|y|^{1/d_f}.$$

Observe that $F_y(r) = 0$ implies that the constant term of $F_y(x)$, that is $f_0(0) + y\ell_f^{d_f-1}\ell_g$, has the divisor r. Let $J = J(f, g) \in \mathbb{Z}^+$ be such that

$$\frac{1}{\log\log J} < c_1, \quad \log\log J > 2c_2$$

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

and

$$\log\log\log J > \max\{|f_0(0)|, |\ell_f|^{d_f-1}|\ell_g|, d_f\}.$$

Then for $|y| > 2^J$, there is a $j \geqslant J$, for which

$$2^j < |y| \leqslant 2^{j+1}.$$

For such j, we consider $k = d_f$, $\ell = \ell_f^{d_f-1}\ell_g$ and $\ell' = f_0(0)$ in (1·3). Observe that the conditions in (1·3) that

$$2 \leqslant k \leqslant \log\log\log j, \quad -\log\log\log j \leqslant \ell \leqslant \log\log\log j, \quad \ell \neq 0,$$

and

$$-\log\log\log j \leqslant \ell' \leqslant \log\log\log j$$

are all satisfied. We claim

$$y \notin Y(j, k, \ell, \ell').$$

We have that $|\ell y + \ell'| = |\ell_f^{d_f-1}\ell_g y + f_0(0)|$ has the divisor $|r|$. Also,

$$\frac{2^{j/k}}{\log\log j} \leqslant \frac{2^{j/d_f}}{\log\log J} < c_1 2^{j/d_f} < c_1|y|^{1/d_f} < |r| < c_2|y|^{1/d_f}$$
$$\leqslant c_2 2^{(j+1)/d_f} < 2c_2 2^{j/d_f} < 2^{j/d_f}\log\log J \leqslant 2^{j/k}\log\log j.$$

Hence, the definition of $Y(j, k, \ell, \ell')$ implies $y \notin Y(j, k, \ell, \ell')$ as claimed. The above holds for all $y \in \mathbb{Z}$ satisfying (4·3) and $|y| > 2^J$ with $F_y(x)$ having a linear factor. We deduce that such y are not in $\mathcal{S}$. Therefore, the elements of $\mathcal{Y} \bigcap \mathcal{S}$ are bounded, and $\mathcal{Y} \bigcap \mathcal{S}$ is a finite set.

We are left with the case that $d_f \leqslant d_g$, and suppose that this inequality holds now. Let y be an integer satisfying

$$|y| > \max\left\{2h_f, \frac{|\ell_f|}{|\ell_g|}\left(h_f/|\ell_f| + h_g/|\ell_g| + 3\right)^{d_f}\right\}. \tag{4·4}$$

Suppose $F(x) = f(x) + yg(x) = u(x)v(x)$ where $u(x)$ and $v(x)$ are in $\mathbb{Z}[x]$ with $d_u \geqslant 1$ and $d_v \geqslant 1$. We show next that

$$|\ell_u| \geqslant \left(\frac{|y|}{2h_f\left(h_g/|\ell_g| + 2\right)^{d_f}}\right)^{d_u/d_g}. \tag{4·5}$$

To establish (4·5), we assume first that there is a root θ of $u(x)$ and, hence, of $F(x)$ that satisfies

$$|\theta| \geqslant h_g/|\ell_g| + 2. \tag{4·6}$$

From $F(\theta) = 0$, we deduce

$$f(\theta) = -yg(\theta). \tag{4·7}$$

For some α_j and β_j in $\mathbb{C}$, we can write

$$f(x) = \ell_f(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_{d_f}),$$
$$g(x) = \ell_g(x - \beta_1)(x - \beta_2)\cdots(x - \beta_{d_g}).$$

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

A classical bound of Cauchy [**3**] implies that the roots of $f(x)$ have absolute value $\leqslant (h_f/|\ell_f|) + 1$ and the roots of $g(x)$ have absolute value $\leqslant (h_g/|\ell_g|) + 1$. Thus,

$$|\theta - \alpha_j| \leqslant |\theta| + |\alpha_j| \leqslant |\theta| + h_f/|\ell_f| + 1 \quad \text{for } 1 \leqslant j \leqslant d_f$$

and

$$|\theta - \beta_j| \geqslant |\theta| - |\beta_j| \geqslant |\theta| - h_g/|\ell_g| - 1 \quad \text{for } 1 \leqslant j \leqslant d_g.$$

Hence,

$$|f(\theta)| \leqslant |\ell_f|\big(|\theta| + h_f/|\ell_f| + 1\big)^{d_f}$$

and

$$|g(\theta)| \geqslant |\ell_g|\big(|\theta| - h_g/|\ell_g| - 1\big)^{d_g}.$$

We obtain a contradiction to (4·7) if

$$|\ell_f|\big(|\theta| + h_f/|\ell_f| + 1\big)^{d_f} < |y||\ell_g|\big(|\theta| - h_g/|\ell_g| - 1\big)^{d_g}$$

or equivalently if

$$|y| > \frac{|\ell_f|\big(|\theta| + h_f/|\ell_f| + 1\big)^{d_f}}{|\ell_g|\big(|\theta| - h_g/|\ell_g| - 1\big)^{d_g}}.$$

Since the right-hand side of this inequality is equal to

$$\frac{|\ell_f|\left(1 + \dfrac{h_f/|\ell_f| + h_g/|\ell_g| + 2}{|\theta| - h_g/|\ell_g| - 1}\right)^{d_f}}{|\ell_g|\big(|\theta| - h_g/|\ell_g| - 1\big)^{d_g - d_f}} \leqslant \frac{|\ell_f|}{|\ell_g|}\big(h_f/|\ell_f| + h_g/|\ell_g| + 3\big)^{d_f},$$

where this last inequality follows from (4·6), we obtain a contradiction from (4·4). In other words, (4·6) cannot hold. Thus,

$$u(\theta) = 0 \implies |\theta| < h_g/|\ell_g| + 2. \tag{4·8}$$

Observe that $f(x)$ and $g(x)$ being relatively prime polynomials implies that $u(x)$ and $g(x)$ have no common roots (i.e., any common root of $u(x)$ and $g(x)$ must be a root of $f(x)$ by (4·7)). Using the notation $\theta_1, \ldots, \theta_{d_u}$ for the roots of $u(x)$ counted to their multiplicity, we obtain

$$\left|\ell_u^{d_g} \prod_{j=1}^{d_u} g(\theta_j)\right| = \big|\mathrm{Res}(u, g)\big| \geqslant 1,$$

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

and, from (4·8),

$$\begin{aligned}\left|\ell_u^{d_g}\prod_{j=1}^{d_u} f(\theta_j)\right| &\leqslant |\ell_u|^{d_g}\prod_{j=1}^{d_u}\left|h_f\cdot\sum_{j=0}^{d_f}\left(h_g/|\ell_g|+2\right)^j\right| \\ &\leqslant |\ell_u|^{d_g}\prod_{j=1}^{d_u}\left|h_f\cdot\left(h_g/|\ell_g|+2\right)^{d_f}\sum_{j=0}^{d_f}\frac{1}{\left(h_g/|\ell_g|+2\right)^{d_f-j}}\right| \\ &\leqslant |\ell_u|^{d_g}\prod_{j=1}^{d_u}\left|h_f\cdot\left(h_g/|\ell_g|+2\right)^{d_f}\sum_{j=0}^{d_f}\frac{1}{2^{d_f-j}}\right| \\ &\leqslant |\ell_u|^{d_g}\prod_{j=1}^{d_u}\left|2h_f\cdot\left(h_g/|\ell_g|+2\right)^{d_f}\right| \\ &= |\ell_u|^{d_g}2^{d_u}h_f^{d_u}\left(h_g/|\ell_g|+2\right)^{d_f d_u}.\end{aligned}$$

Since each θ_j is a root of $F(x)$, we deduce from (4·7) that

$$\left|\ell_u^{d_g}\prod_{j=1}^{d_u} f(\theta_j)\right| = |y|^{d_u}\left|\ell_u^{d_g}\prod_{j=1}^{d_u} g(\theta_j)\right|,$$

from which we obtain

$$|y|^{d_u} \leqslant |\ell_u|^{d_g}2^{d_u}h_f^{d_u}\left(h_g/|\ell_g|+2\right)^{d_f d_u}.$$

The inequality (4·5) now follows.

Next, we obtain a lower bound on $|\ell_u|$ as follows. Recalling $F(x) = u(x)v(x)$, we can replace the role of $u(x)$ with $v(x)$ above to deduce that

$$|\ell_v| \geqslant \left(\frac{|y|}{2h_f\left(h_g/|\ell_g|+2\right)^{d_f}}\right)^{d_v/d_g}$$

in place of (4·5). The condition $d_f \leqslant d_g$ and the inequality $|y| > 2h_f$ coming from (4·4) imply $d_F = d_g$. Hence, $d_u + d_v = d_g$. Furthermore, $|y| > 2h_f$ implies

$$|\ell_F| \leqslant |y|\,|\ell_g| + |\ell_f| \leqslant |y|\,|\ell_g| + h_f < |y|(|\ell_g|+1).$$

We obtain

$$|y|(|\ell_g|+1) > |\ell_F| = |\ell_u|\cdot|\ell_v| \geqslant |\ell_u|\cdot\left(\frac{|y|}{2h_f\left(h_g/|\ell_g|+2\right)^{d_f}}\right)^{d_v/d_g}$$

so that

$$\begin{aligned}|\ell_u| &< |y|^{1-(d_v/d_g)}(|\ell_g|+1)2^{d_v/d_g}h_f^{d_v/d_g}\left(h_g/|\ell_g|+2\right)^{d_f d_v/d_g} \\ &< |y|^{d_u/d_g}(|\ell_g|+1)2^{d_v/d_g}h_f^{d_v/d_g}\left(h_g/|\ell_g|+2\right)^{d_f d_v/d_g}.\end{aligned}$$

In the case that $d_u = 1$ and, hence, $d_v = d_g - 1$, we can combine the last inequality with

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

(4·5) to deduce

$$\frac{|y|^{1/d_g}}{2^{1/d_g}h_f^{1/d_g}\big(h_g/|\ell_g|+2\big)^{d_f/d_g}} \leqslant |\ell_u| \\ < |y|^{1/d_g}(|\ell_g|+1)2^{(d_g-1)/d_g}h_f^{(d_g-1)/d_g}\big(h_g/|\ell_g|+2\big)^{d_f(d_g-1)/d_g}. \tag{4·9}$$

Let $\ell'_f = \ell_f$ if $d_f = d_g$ and $\ell'_f = 0$ otherwise. Then the leading coefficient of $F(x)$ is $\ell'_f + y\ell_g$, and this leading coefficient has ℓ_u as a divisor. Of interest to us here is that, as a consequence of (4·9), there are positive constants $c_1 = c_1(f, g)$ and $c_2 = c_2(f, g)$ for which

$$c_1|y|^{1/d_g} < |\ell_u| < c_2|y|^{1/d_g}.$$

Note that ℓ_u depends on y, but c_1 and c_2 only depend on the given polynomials $f(x)$ and $g(x)$. Also, the condition $\max\{d_f, d_g\} \geqslant 2$ in the statement of the lemma and the current case where $d_f \leqslant d_g$ imply $d_g \geqslant 2$.

Let $J = J(f, g) \in \mathbb{Z}^+$ be such that

$$\frac{1}{\log\log J} < c_1, \quad \log\log J > 2c_2 \quad \text{and} \quad \log\log\log J > \max\{|\ell'_f|, |\ell_g|, d_g\}.$$

Then for $|y| > 2^J$, there is a $j \geqslant J$, for which

$$2^j < |y| \leqslant 2^{j+1}.$$

For such j, we consider $k = d_g$, $\ell = \ell_g$ and $\ell' = \ell'_f$ in (1·3). The conditions in (1·3) that

$$2 \leqslant k \leqslant \log\log\log j, \quad -\log\log\log j \leqslant \ell \leqslant \log\log\log j, \quad \ell \neq 0,$$

and

$$-\log\log\log j \leqslant \ell' \leqslant \log\log\log j$$

are all satisfied. We justify that

$$y \notin Y(j, k, \ell, \ell').$$

Indeed, this follows from the definition of $Y(j, k, \ell, \ell')$, the fact that $|\ell y + \ell'| = |\ell_g y + \ell'_f|$ has the divisor $|\ell_u|$, and the inequalities

$$\frac{2^{j/k}}{\log\log j} \leqslant \frac{2^{j/d_g}}{\log\log J} < c_1 2^{j/d_g} < c_1|y|^{1/d_g} < |\ell_u| < c_2|y|^{1/d_g} \\ \leqslant c_2 2^{(j+1)/d_g} < 2c_2 2^{j/d_g} < 2^{j/d_g}\log\log J \leqslant 2^{j/k}\log\log j.$$

Since j is such that $|y| \in (2^j, 2^{j+1}]$, we deduce that $y \notin \mathcal{S}$. We obtain that the elements of $\mathcal{Y} \cap \mathcal{S}$ are bounded, and hence $\mathcal{Y} \cap \mathcal{S}$ is a finite set.

This completes the proof of Lemma 4·2.

The above lemma summarized our use of the definition of $\mathcal{S}$. The next lemma summarises our use of Theorem 3·1. In particular, after this next lemma, the definition of $\mathcal{S}$ and Theorem 3·1 will only come into play when we apply this lemma.

LEMMA 4·3. *Let $f(x, y)$ be in $\mathbb{Z}[x, y]$ with $f(x, y)$ irreducible in $\mathbb{C}[x, y]$. Let $\mathcal{S}$ be as in* (1·3). *Let $\mathcal{Y}'$ be the set of $y_0 \in \mathbb{Z}$ such that $f(x_0, y_0) = 0$ for some $x_0 \in \mathbb{Z}$. Then there is a rational function $\hat{h}(y) \in \mathbb{Q}(y)$ such that for all but finitely many $y_0 \in \mathcal{Y}' \cap \mathcal{S}$, the only*

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

integer x_0 satisfying $f(x_0, y_0) = 0$ is $x_0 = \hat{h}(y_0)$. Furthermore, in the case that $\mathcal{Y}' \bigcap \mathcal{S}$ is an infinite set, for all but finitely many $y_0 \in \mathbb{C}$, if $f(x_0, y_0) = 0$ for some $x_0 \in \mathbb{C}$, then $x_0 = \hat{h}(y_0)$.

Proof. Since $f(x, y)$ is in $\mathbb{Z}[x, y]$ and irreducible in $\mathbb{C}[x, y]$, we can apply Theorem 3·1. As there is nothing to prove if $\mathcal{Y}' \bigcap \mathcal{S}$ is finite, we consider only the case that $\mathcal{Y}' \bigcap \mathcal{S}$ is an infinite set. We let $u_1(t)$, $u_2(t)$, $v_1(t)$ and $v_2(t)$ be in $\mathbb{Z}[t]$ such that Theorem 3·1 (i) and (ii) hold. We may and do suppose that $\gcd(u_1, v_1) = \gcd(u_2, v_2) = 1$.

By Theorem 3·1 (ii), we have that except for finitely many $(x_0, y_0) \in \mathbb{Z}^2$ with $f(x_0, y_0) = 0$, there is a $t_0 \in \mathbb{Q}$ for which $x_0 = u_1(t_0)/v_1(t_0)$ and $y_0 = u_2(t_0)/v_2(t_0)$. Thus, except for finitely many possibilities for $y_0 \in \mathbb{Z}$, if $(x_0, y_0) \in \mathbb{Z}^2$ is such that $f(x_0, y_0) = 0$, then the polynomial $u_2(t) - y_0 v_2(t)$ has a linear factor in $\mathbb{Q}[t]$, namely $t - t_0$ with t_0 as described. In particular, since $\mathcal{Y}' \bigcap \mathcal{S}$ is an infinite set, there are infinitely many $y_0 \in \mathcal{S}$ such that $u_2(t) - y_0 v_2(t)$ has a linear factor.

We are now in a position to appeal to Lemma 4·2. We deduce that each of $u_2(t)$ and $v_2(t)$ is either a constant or linear in t. We write $u_2(t) = a + bt$ and $v_2(t) = c + dt$, where a, b, c and d are integers. As we are interested in $t_0 \in \mathbb{Q}$ such that $y_0 = u_2(t_0)/v_2(t_0)$, at least one of c and d is non-zero. We justify that $d = 0$ and, hence, $c \neq 0$. Assume $d \neq 0$. Then $u_2(t)/v_2(t) \to b/d$ as $t \to \pm\infty$. In particular, $|u_2(t)/v_2(t)|$ is bounded from above. Therefore, there are only finitely many integers of the form $u_2(t_0)/v_2(t_0)$ and hence only finitely many $y_0 \in \mathbb{Z}$ such that $u_2(t) - y_0 v_2(t)$ has a linear factor in $\mathbb{Q}[t]$. This contradiction implies $d = 0$ and, hence, $c \neq 0$. Thus, we consider only $c \neq 0$ and $d = 0$. If $b = 0$, then the only y_0 of the form $u_2(t_0)/v_2(t_0)$ is a/c, which is impossible. Therefore, $b \neq 0$. Now, we apply Theorem 3·1 (i). We see that except for finitely many pairs $(x_0, y_0) \in \mathbb{C}^2$ with $f(x_0, y_0) = 0$, we have a $t_0 \in \mathbb{C}$ for which

$$y_0 = \frac{u_2(t_0)}{v_2(t_0)} = \frac{a + bt_0}{c} \implies t_0 = \frac{-a + cy_0}{b}.$$

Furthermore, we obtain

$$x_0 = \frac{u_1(t_0)}{v_1(t_0)} = \frac{u_1\big((-a + cy_0)/b\big)}{v_1\big((-a + cy_0)/b\big)}.$$

Setting $\hat{h}(y) = u_1\big((-a + cy)/b\big)/v_1\big((-a + cy)/b\big)$, the lemma follows.

5. *A proof of Theorem* 1·1

The previous section contained our main new ideas involving the set $\mathcal{S}$. The ideas in this section and the next are similar to work done in the past.

As discussed in the introduction, Theorem 1·2 implies Theorem 1·1. In the next section, we will prove Theorem 1·2 based on the material from the previous sections. It is however possible to give a separate argument for Theorem 1·1, still based on the previous sections, but also taking advantage of a simple argument using elementary symmetric functions. We explain this argument here, also setting up most of the ideas for the proof of Theorem 1·2.

As in the introduction, we let $F(x, y) \in \mathbb{Z}[x, y]$ be irreducible in $\mathbb{Q}[x, y]$ with $n = \deg_x(F)$. One checks that Theorem 1·1 holds in the case that $n = 1$, so we work only with $n \geqslant 2$. We consider $k \in [1, n/2] \bigcap \mathbb{Z}$. To establish that $\mathcal{S}$ is a universal Hilbert set, it suffices to show that, regardless of the value of $k \in [1, n/2] \bigcap \mathbb{Z}$, there are only finitely many $y_0 \in \mathcal{S}$

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

for which the polynomial $F(x, y_0)$ has a factor of degree k in $\mathbb{Z}[x]$. Following the ideas from the introduction, we replace $F(x, y)$ with the polynomial $G(x, y)$ in $\mathbb{Z}[x, y]$ defined by

$$G(x, y) = f_n(y)^{n-1} F(x/f_n(y), y),$$

where $f_n(y)$ is the coefficient of x^n when we view $F(x, y)$ as a polynomial in x. The polynomial $G(x, y)$ has the added property that it is monic as a polynomial in x. Since $F(x, y) \in \mathbb{Z}[x, y]$ is irreducible in $\mathbb{Q}[x, y]$ with degree n in x, the polynomial $G(x, y)$ is irreducible in $\mathbb{Q}[x, y]$ with degree n in x. Also, with the added condition that $f_n(y_0) \neq 0$, we have $F(x, y_0)$ has a factor of degree k in $\mathbb{Z}[x]$ if and only if $G(x, y_0)$ has a *monic* factor of degree k in $\mathbb{Z}[x]$. Hence, we can write as before such a factor of $G(x, y_0)$ in the form

$$H(x) = x^k + h_{k-1}x^{k-1} + \cdots + h_2x^2 + h_1x + h_0,$$

where we write $h_j = h_j(y_0) = h_{j,k}(y_0)$ to indicate that the h_j depend on y_0 (and not that h_j is a polynomial in y_0). We are interested in the case that each $h_j \in \mathbb{Z}$. We set

$$A(\mathcal{S}) = \big\{(h_0^*, \ldots, h_{k-1}^*, y_0) \in \mathbb{Z}^k \times \mathcal{S} : x^k + h_{k-1}^* x^{k-1} + \cdots + h_1^* x + h_0^* \text{ divides } G(x, y_0)\big\}.$$

Note that there are only finitely many points $(h_0^*, \ldots, h_{k-1}^*, y_0) \in A(\mathcal{S})$ for a given $y_0 \in \mathcal{S}$ (see the introduction). Our interest then is in showing that $A(\mathcal{S})$ is finite. For the purposes of obtaining a contradiction, we assume now that $A(\mathcal{S})$ is infinite.

For each $t \in \{0, 1, \ldots, k-1\}$, we will now construct a curve containing points $(h_t(y), y) \in \mathbb{Z}^2$ which correspond to possible choices for y and $h_t(y)$ where $H(x)$ divides $G(x, y)$. Viewing y as fixed, we let $\alpha_j(y)$ for $1 \leqslant j \leqslant n$ denote the roots of $G(x, y)$. For each $U \subseteq \{1, 2, \ldots, n\}$ with $|U| = k$, we construct the numbers

$$h_{k-1}(y, U) = -\sum_{j \in U} \alpha_j(y), \quad h_{k-2}(y, U) = \sum_{\substack{i,j \in U \\ i<j}} \alpha_i(y)\alpha_j(y),$$

$$\ldots, h_0(y, U) = (-1)^k \prod_{j \in U} \alpha_j(y).$$

For $t \in \{0, 1, \ldots, k-1\}$, we define

$$H_t(z) = H_t(z, y) = \prod_{\substack{U \subseteq \{1,2,\ldots,n\} \\ |U|=k}} \big(z - h_t(y, U)\big).$$

The coefficients of $H_t(z)$ are symmetric polynomials in the roots $\alpha_j(y)$ of $G(x, y)$, and $G(x, y)$ is monic. Hence, $H_t(z)$ can be written in terms of the coefficients of $G(x, y)$ viewed as a polynomial in x, and $H_t(z, y) \in \mathbb{Z}[z, y]$. If y_0 is an integer for which $F(x, y_0)$ has a factor in $\mathbb{Z}[x]$ of degree k and $f_n(y_0) \neq 0$, then $G(x, y_0)$ has a factor $H(x) \in \mathbb{Z}[x]$ of degree k as before for some $h_t(y_0)$. Also, there is some $U \subseteq \{1, 2, \ldots, n\}$ with $|U| = k$ such that $h_t(y_0) = h_t(y_0, U)$. We deduce $H_t(z, y) = 0$ is an algebraic curve which passes through the integral point $\big(h_t(y_0), y_0\big)$.

The main difference in this section and the next are the curves constructed to complete the argument. We just made use of elementary symmetric functions to obtain curves associated with the coefficients of a possible polynomial divisor $H(x)$ of $G(x, y)$. For the proof of Theorem 1·2 in the next section, we will not have the set-up of $H(x)$ being a factor of $G(x, y)$ to formulate our curves. Instead, we will appeal to ideas from elimination theory via Gröbner bases.

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

The above gives us a curve $H_t(z, y) = 0$ for every $t \in \{0, 1, \ldots, k-1\}$. Our assumption implies that there are infinitely many $(h_0^*, \ldots, h_{k-1}^*, y_0) \in A(\mathcal{S})$ for which (h_t^*, y_0) lies on the curve $H_t(z, y) = 0$ for each $t \in \{0, 1, \ldots, k-1\}$. For each of the k values of t, we choose an irreducible factor $I_t(z, y)$ of $H_t(z, y)$ in $\mathbb{Q}[z, y]$ in such a way that there are infinitely many $(h_0^*, \ldots, h_{k-1}^*, y_0) \in A(\mathcal{S})$ for which (h_t^*, y_0) lies on the curve $I_t(z, y) = 0$ for all $t \in \{0, 1, \ldots, k-1\}$. This is possible by the pigeon-hole principle. Since there are only finitely many points $(h_0^*, \ldots, h_{k-1}^*, y_0) \in A(\mathcal{S})$ for a given $y_0 \in \mathcal{S}$, we deduce that, for each $t \in \{0, 1, \ldots, k-1\}$, we have infinitely many points (h_t^*, y_0) as above lying on the curve $I_t(z, y) = 0$.

With t fixed, we want to apply Lemma 4·3 with $x = z$ and $f(x, y) = I_t(z, y)$. As Lemma 4·3 requires $I_t(z, y)$ to be irreducible in $\mathbb{C}[z, y]$, we first appeal to Lemma 3·2. As there are infinitely many points $(h_t^*, y_0) \in \mathbb{Z} \times \mathcal{S}$ lying on the curve $I_t(z, y) = 0$, we see that $I_t(z, y)$ is in fact irreducible in $\mathbb{C}[z, y]$.

Now, we show that for integral points $(h_t(y_0), y_0)$ on the curve $I_t(z, y) = 0$, with $y_0 \in \mathcal{S}$, the values of $h_t(y_0)$, with finitely many exceptions, are the values of a rational function in y_0. We apply Lemma 4·3 with $x = z$ and $f(x, y) = I_t(z, y)$. Since $I_t(z, y)$ is irreducible in $\mathbb{C}[z, y]$, Lemma 4·3 implies that there is an $\hat{h}_t(y) \in \mathbb{Q}(y)$, such that, except for finitely many pairs, each $(z_0, y_0) \in \mathbb{Z} \times \mathcal{S}$ satisfying $I_t(z_0, y_0) = 0$ also satisfies $z_0 = \hat{h}_t(y_0)$. We apply the above process to each $t \in \{0, 1, \ldots, k-1\}$. We deduce that there are infinitely many $(h_0^*, \ldots, h_{k-1}^*, y_0) \in A(\mathcal{S})$ for which $h_t^* = \hat{h}_t(y_0)$ for all $t \in \{0, 1, \ldots, k-1\}$. In other words, there are infinitely many $y_0 \in \mathcal{S}$ such that $x^k + \hat{h}_{k-1}(y_0)x^{k-1} + \cdots + \hat{h}_1(y_0)x + \hat{h}_0(y_0)$ is a factor of $G(x, y_0)$.

The final part of the argument is to obtain a contradiction. We consider now the remainder when we divide $G(x, y)$ by the polynomial $H(x)$ with its coefficients h_t replaced by $\hat{h}_t(y)$. Thus, we want the remainder when we divide $G(x, y)$ by

$$H(x, y) = x^k + \hat{h}_{k-1}(y)x^{k-1} + \cdots + \hat{h}_1(y)x + \hat{h}_0(y) \in \mathbb{Q}(y)[x].$$

Call this remainder $R(x, y)$. Since $G(x, y) \in \mathbb{Z}[x, y]$ and $H(x, y) \in \mathbb{Q}(y)[x]$, we deduce that $R(x, y) \in \mathbb{Q}(y)[x]$. Furthermore, there are infinitely many $y_0 \in \mathcal{S}$ such that $R(x, y_0) \equiv 0$. If $R(x, y) \not\equiv 0$, then there is at least one non-zero coefficient of $R(x, y)$ viewed as a polynomial in x. This coefficient is in $Q(y)$, so it has finitely many zeroes, giving a contradiction (since each $y_0 \in \mathcal{S}$ with $R(x, y_0) \equiv 0$ will be a zero of this coefficient). Hence, we must have $R(x, y) \equiv 0$. But then $G(x, y)$ has the factor $H(x, y)$ in $\mathbb{Q}(y)[x]$ with $\deg_x H(x, y)$ of degree $k \in [1, n/2]$ and $\deg_x G(x, y)$ of degree n. Therefore, $G(x, y)$ is reducible in $\mathbb{Q}(y)[x]$, contradicting our assumption that $G(x, y)$ is irreducible in $\mathbb{Q}[x, y]$ (by Gauss's Lemma). This then provides a proof that $\mathcal{S}$ is a universal Hilbert set. The asymptotic estimate in Theorem 1·1 was established earlier as a consequence of Ford's Theorem 2·1. Hence, Theorem 1·1 holds.

6. *A proof of Theorem* 1·2

We finish the paper with a proof of Theorem 1·2. We assume that there are infinitely many points $(h_0^*, \ldots, h_{k-1}^*, y_0)$ in $V \cap \mathbb{Z}^{k+1}$ with $y_0 \in \mathcal{S}$. We take advantage of the condition that for each fixed $y_0 \in \mathbb{C}$, there are finitely many points $(h_0^*, \ldots, h_{k-1}^*) \in \mathbb{C}^k$ such that $(h_0^*, \ldots, h_{k-1}^*, y_0) \in V$ to clarify how we can eliminate variables and replace $h_t(y)$ with $\hat{h}_t(y)$ for $t \in \{0, 1, \ldots, k-1\}$ as in the previous section. We eliminate variables to determine $V = V(r_0, r_1, \ldots, r_{k-1})$ by constructing a Gröbner basis with the field of

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

coefficients $\mathbb{Q}(y)$ and using a lexicographic ordering on the exponents of monomials with the order of the variables $h_0, \dots, h_{k-1}$. This is equivalent to treating y as a constant and constructing a Gröbner basis for which there are a finite number of solutions for complex $h_0, \dots, h_{k-1}$ (with y fixed). The finiteness of the number of solutions implies that, for each $t \in \{0, 1, \dots, k-1\}$, the resulting Gröbner basis, say G, will include a polynomial in $\mathbb{Q}(y)[h_t, h_{t+1}, \dots, h_{k-1}]$ that is not in $\mathbb{Q}(y)[h_{t+1}, \dots, h_{k-1}]$, where $\mathbb{Q}(y)[h_{t+1}, \dots, h_{k-1}]$ is to be interpreted as $\mathbb{Q}(y)$ when $t = k-1$.

We take a $w(h_{k-1}, y) \in G \bigcap \mathbb{Q}(y)[h_{k-1}]$, multiply it by a polynomial in $\mathbb{Q}[y]$ to obtain a polynomial in $\mathbb{Q}[h_{k-1}, y]$, factor the result into irreducibles in $\mathbb{Q}[h_{k-1}, y]$, and apply Lemma 3·2 and Lemma 4·3 as in the previous section to see that there is an $\hat{h}_{k-1}(y) \in \mathbb{Q}(y)$ for which there are infinitely many

$$(h_0^*, \dots, h_{k-2}^*, \hat{h}_{k-1}(y_0), y_0) \in V \bigcap \big(\mathbb{Z}^k \times \mathcal{S}\big).$$

Next, we take $w(h_{k-2}, \hat{h}_{k-1}(y), y)$ where

$$w(h_{k-2}, h_{k-1}, y) \in G \bigcap \mathbb{Q}(y)[h_{k-2}, h_{k-1}] \quad \text{and} \quad w(h_{k-2}, h_{k-1}, y) \notin G \bigcap \mathbb{Q}(y)[h_{k-1}],$$

multiply it by a polynomial in $\mathbb{Q}[y]$ to obtain a polynomial in $\mathbb{Q}[h_{k-2}, y]$, factor the result into irreducibles in $\mathbb{Q}[h_{k-2}, y]$, and apply Lemma 3·2 and Lemma 4·3 again to deduce there is an $\hat{h}_{k-2}(y) \in \mathbb{Q}(y)$ for which there are infinitely many

$$(h_0^*, \dots, h_{k-3}^*, \hat{h}_{k-2}(y_0), \hat{h}_{k-1}(y_0), y_0) \in V \bigcap \big(\mathbb{Z}^k \times \mathcal{S}\big).$$

We continue with

$$w(h_{k-3}, h_{k-2}, h_{k-1}, y) \in G \bigcap \mathbb{Q}(y)[h_{k-3}, h_{k-2}, h_{k-1}]$$

and

$$w(h_{k-3}, h_{k-2}, h_{k-1}, y) \notin G \bigcap \mathbb{Q}(y)[h_{k-2}, h_{k-1}],$$

and so on, until we have an $\hat{h}_t(y) \in \mathbb{Q}(y)$, for $t \in \{0, 1, \dots, k-1\}$, such that the set of

$$(\hat{h}_0(y_0), \dots, \hat{h}_{k-1}(y_0), y_0) \in V \bigcap \big(\mathbb{Z}^k \times \mathcal{S}\big)$$

is an infinite set, completing the proof.

Acknowledgement. The authors express their gratitude to Alex Duncan for a number of useful discussions in writing this paper.

REFERENCES

[**1**] Y. BILU. A note on universal Hilbert sets. *J. Reine Angew. Math.* **479** (1996), 195–203.
[**2**] Y. BILU. The many faces of the subspace theorem [after Adamczewski, Bugeaud, Corvaja, Zannier. . .], Séminaire Bourbaki. Vol. 2006/2007. *Astérisque*, No. 317 (2008), Exp. No. 967, vii, 1–38.
[**3**] A. L. CAUCHY. Résolution des équations numériques et sur la théorie de l'élimination. *Exercices de Mathématiques, Œuvres Complétes D'Augustin Cauchy, Série 2*, **9** (1891), 87–161 (Gauthier-Villars et Fils).
[**4**] P. CORVAJA and U. ZANNIER. Diophantine equations with power sums and universal Hilbert sets, *Indag. Math.* (N.S.) **9** (1998), 317–332.
[**5**] P. DÈBES and U. ZANNIER. Universal Hilbert subsets, *Math. Proc. Camb. Phil. Soc.* **124** (1998), 127–134.
[**6**] K. FORD. The distribution of integers with a divisor in a given interval, *Ann. of Math. (2)* **168** (2008), 367–433.

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press

[**7**] M. D. FRIED and M. JARDEN. Field arithmetic. *Ergeb. Math. Grenzgeb*. **3**. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], Vol. 11, third Edition (Springer-Verlag, Berlin, 2008).
[**8**] P. C. GILMORE and A. ROBINSON. Metamathematical considerations on the relative irreducibility of polynomials. *Canad. J. Math.* **7** (1955), 483–489.
[**9**] C. R. HADLOCK. *Field Theory and Its Classical Problems*. Carus Math. Monogr. Math. Assoc. of America (Washington, DC, 1978).
[**10**] G. H. HARDY and E. M. WRIGHT. *An Introduction to the Theory of Numbers*. Fifth Edition (The Clarendon Press, Oxford University Press, New York, 1979).
[**11**] D. HILBERT. Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.* **110** (1892), 104–129.
[**12**] S. LANG. *Fundamentals of Diophantine Geometry* (Springer-Verlag, New York, 1983).
[**13**] A. SCHINZEL. *Selected Topics on Polynomials* (University of Michigan Press, Ann Arbor, Mich., 1982).
[**14**] A. SCHINZEL. *Polynomials with Special Regard to Reducibility*, with an appendix by Umberto Zannier. Encyclopedia of Mathematics and its Applications, Vol. 77 (Cambridge University Press, Cambridge, 2000).
[**15**] A. SCHINZEL and U. ZANNIER. The least admissible value of the parameter in Hilbert's irreducibility theorem. *Acta Arith.* **69** (1995), 293–302.
[**16**] J.–P. SERRE. *Topics in Galois Theory*. Research Notes in Mathematics, Vol. 1, second Edition. With notes by Henri Darmon (A K Peters, Ltd., Wellesley, MA, 2008).
[**17**] C. L. SIEGEL. Über einige Anwendungen Diophantischer Approximationen. *Abh. Preuss Akad. Wiss. Phys.-Math. Kl.* **1** (1929), 1–70.
[**18**] V. G. SPRINDŽUK. Diophantine equations involving unknown prime numbers. *Trudy Math. Inst. Steklov* 158 (1981), 180–196; English transl. in *Proc. Steklov Inst. Math.* (1983), Issue 4, 197–214.
[**19**] U. ZANNIER. Note on dense universal Hilbert sets. *C. R. Acad. Sci. Paris Sér. I Math.* **322** (1996), 703–706.

https://doi.org/10.1017/S0305004118000452 Published online by Cambridge University Press