Universal Hilbert subsets

Pierre Dèbes and Umberto Zannier

Abstract

We show that the sequence $2^n + n$ is a universal Hilbert sequence. That is, for each polynomial $P(T, Y)$ irreducible in $\mathbb{Q}(T)[Y]$, the polynomial $P(2^n + n, Y)$ is irrreducible in $\mathbb{Q}[Y]$ for all but finitely many n. This answers a question of M. Yasumoto. Other examples, like $2^n + 5^n$, are given. They all are obtained as special cases of a more general result which is proved from classical diophantine arguments.

1. Introduction

A *universal Hilbert subset (or sequence)* S of $\mathbb{Q}$ is an infinite subset of $\mathbb{Q}$ with the following property: for each polynomial $P(T, Y)$ irreducible in $\mathbb{Q}(T)[Y]$, the polynomial $P(t, Y)$ is irrreducible in $\mathbb{Q}[Y]$ for all but finitely many $t \in S$. A classical argument shows that the existence of universal Hilbert subsets follows from Hilbert's irreducibility theorem. We show (see Addendum 2 at the end of the paper) that this argument can even be refined to show that there exists a universal Hilbert subset $S \subset \mathbb{N}$ of asymptotic density 1, that is, such that $\text{card}\{n \in S | n \leq T\} \sim T$ as $T \to \infty$ (the same observation was made independently by Bilu [**3**]).

That argument however only provides uneffective existence conclusions. The first explicit example was produced by Sprindžuk [**9**] who showed that the sequence $\left[\exp\sqrt{\log\log n}\right] + n!2^{n^2}$ satisfies the above universal property. Other examples of the form $a_m b^m$ where b is any integer distinct from 0, 1, -1 and a_m is a product of primes less than a certain explicit function of m were given in [**4**]. Further new examples appear in the recent paper by Bilu [**3**]. Using non-standard techniques, Yasumoto [**10**] proved a general criterion for

1991 *Mathematics Subject Classification.* Primary 12E25, 14H05; Secondary 11xx.

a sequence of rational numbers to be universal. As a consequence of his criterion, he obtains such simple examples as $2^n(n^3+1)$ and $2^n p_n$ where p_n is the nth prime. He then asks whether certain specific sequences such as 2^n+n, 2^n+3^n are universal sequences. Concerning the former, this paper gives a positive answer.

THEOREM 1 — *The sequence 2^n+n is a universal Hilbert sequence. More generally if b is any integer such that $|b|\geq 2$ and $p\in\mathbb{Z}[X]$ is any non constant polynomial, then the sequence $b^n+p(n)$ is a universal Hilbert sequence.*

As for the sequence 2^n+3^n, we have the following partial answer. Given a real number $\delta>1$, an infinite subset S of $\mathbb{Q}$ is said to be δ-universal if the following universal property holds: for each absolutely irreducible polynomial $P(T,Y)\in\mathbb{Q}[T,Y]$ with $\deg_Y P\geq\delta$, the polynomial $P(t,Y)$ has no root in $\mathbb{Q}$ for all but finitely many $t\in S$. Standard arguments ([**5**],[**7**]) show that a subset is a universal Hilbert subset if and only if it is 2-universal.

THEOREM 2 — *Let a and b be two integers such that $1<|a|<|b|$ and such that a and b are multiplicatively independent. Then the sequence a^n+b^n is δ-universal, for each real number δ such that*

$$\delta > \frac{\operatorname{Log}|b|}{\operatorname{Log}\left(\frac{|b|}{|a|}\right)}$$

In particular, if $|a|<\sqrt{|b|}$, then the sequence a^n+b^n is a universal Hilbert subset.

Thus Th.2 shows that the sequence 2^n+3^n is 3-universal. This reduces the question of whether 2^n+3^n is a universal Hilbert subset to checking the universal property for polynomials of degree 2 in Y. Further considerations (contained in this paper) actually show that the essential remaining case is that of polynomials $Y^2+\alpha T+\beta$ ($\alpha,\beta\in\mathbb{Z}$). On the other hand, Th.2 shows that 2^n+5^n is a universal Hilbert sequence. Note also that the condition "a and b multiplicatively independent" is necessary: indeed is $a^u=b^v$, then the polynomial Y^v+Y^u-T becomes reducible when T is specialized to $T=a^n+b^n$ with n a multiple of u.

Both Th.1 and Th.2 will be deduced from a more general result (Main Theorem), which is the main result of the paper. Clearly other examples of universal Hilbert subsets can be derived. Our method uses classical diophantine tools: the main ingredients are Siegel's theorem, Ridout's theorem and Baker's theorem. Our results are not completely effective, in contrast with those of Sprindžuk and Dèbes. Given an irreducible polynomial $P(T,Y)\in\mathbb{Q}(T)[Y]$, they can effectively determine the set of exceptional elements in the universal

Hilbert subset. Neither Yasumoto's method nor ours provide such an effective conclusion. However our method gives an effective upper bound for the *number* of exceptions.

2. Main results

In this section we state the Main Theorem and show how to derive both Th.1 and Th.2. The Main Theorem is proved in §3.

MAIN THEOREM — *Let b be integer such that $|b| \geq 2$ and ρ be a real number such that $0 < \rho < 1$. Consider the set*

$$S(b,\rho) = \{b^n + c \mid n \in \mathbb{N}, c \in \mathbb{Z},\ 0 < |c| \leq |b|^{\rho n}\}$$

Let $P(T,Y) \in \mathbb{Q}[T,Y]$ be an absolutely irreducible polynomial. Set $d = \deg_Y P$ and suppose that $d > 1/(1-\rho)$.

Assume that $P(t,Y)$ has a root $y \in \mathbb{Q}$ for each t in an infinite subset S of $S(b,\rho)$. Then there exist an integer r such that $0 \leq r < d$ and a polynomial $\phi(X)$ of degree $\deg \phi \leq d-2$ such that the set S contains infinitely many integers of the form

$$(*) \qquad b^{qd+r} + \phi(b^q) \quad \text{for some integer } q > 0$$

The condition obtained on S is a real obstruction to S being d-universal. Indeed the polynomial $P(T,Y) = b^r Y^d + \phi(Y) - T$ becomes reducible when T is specialized to any integer of the form (*).

Proof of Th.1 and Th.2. Consider a sequence $b^n + p(n)$ as in Th.1 and a sequence $a^n + b^n$ as in Th.2. For all but finitely many integers n, we have

$$\begin{cases} b^n + p(n) \in S(b,\rho) & \text{for } \rho = 1/3 \\ a^n + b^n \in S(b,\rho) & \text{for } \rho = \operatorname{Log}|a| / \operatorname{Log}|b| \end{cases}$$

Given ϕ and r, only finitely many integers $b^n + p(n)$ can be of the form (*): otherwise, for infinitely many integers n, we would have $p(n) = \phi(b^q)$, which gives $p(n) \gg 2^{n/d}$ or $p(n) \ll 1$, a contradiction. Similar arguments show the same is true for the sequence $a^n + b^n$ under the hypothesis "a and b multiplicatively independent".

Conclude from the Main Theorem that if $P(T,Y) \in \mathbb{Q}[T,Y]$ is any absolutely irreducible polynomial of degree $d = \deg_Y P > 1/(1-\rho)$, then $P(b^n + p(n), Y)$ (resp. $P(a^n + b^n, Y)$)

has no root $y \in \mathbb{Q}$, except possibly for finitely many n. In the case of the sequence $a^n + b^n$, we have $\rho = \operatorname{Log}|a| / \operatorname{Log}|b|$. Th.2 immediately follows.

In the case of the sequence $b^n + p(n)$, we have $\rho = 1/3$ and so $1/(1-\rho) = 3/2$. Thus the sequence $b^n + p(n)$ is 2-universal, which, as recalled in the introduction, is equivalent to being a universal Hilbert subset. □

3. Proof of the Main Theorem

Fix an integer b such that $|b| \geq 2$, a real number ρ such that $0 < \rho < 1$ and an absolutely irreducible polynomial $P(T, Y) \in \mathbb{Q}[T, Y]$. Suppose that $d = \deg_Y P > 1/(1-\rho)$ and that there exists an infinite subset S of $S(b, \rho)$ such that the polynomial $P(t, Y)$ has a root $y \in \mathbb{Q}$ for each $t \in S$. We wish to show that infinitely many elements of S are of the form (*). With no loss of generality we may assume that the polynomial $P(T, Y)$ is monic in Y.

From Siegel's theorem, the curve $P(t, y) = 0$ has genus 0; more precisely it is birational to $\mathbb{P}^1$ over $\mathbb{Q}$. Equivalently the function field of the curve over $\mathbb{Q}$ is of the form $\mathbb{Q}(X)$, with X a certain non-constant rational function on the curve. Projections on the T-line and on the Y-line are respectively of the form $f(X)$, $g(X)$ with $f, g \in \mathbb{Q}(X)$. It follows that all but finitely many solutions $(t, y) \in \mathbb{Q}^2$ of the equation $P(t, y) = 0$ are of the form:

$$\begin{cases} t = f(x) \\ y = g(x) \end{cases}$$

for some $x \in \mathbb{Q}$.

Consider an arbitrary solution $(t, y) \in \mathbb{Q}^2$ of $P(t, y) = 0$ with $t \in S \subset S(b, \rho)$. Write

$$t = b^n + c \quad \text{with } n \in \mathbb{N}, c \in \mathbb{Z},\ 0 < |c| \leq |b|^{\rho n}$$

A further conclusion of Siegel's theorem is that the rational function f has at most 2 poles. We distinguish two cases, depending on whether f has one or two poles. We will show that, under our assumptions, only the former may occur, and that, in that case, we obtain the parametrization (*) of the Main Theorem.

3.1. 1st case: f has exactly one pole.

Since this pole is rational over $\mathbb{Q}$, we may assume that it is ∞, which means that $f \in \mathbb{Q}[X]$. Furthermore, $\deg(f) \geq 2$ (because $\deg_Y(P) \geq 2$). Changing X to $X - a$, we may also assume that

$$f(X) = \alpha X^d + \varphi(X) \quad \text{with} \begin{cases} \alpha \in \mathbb{Q},\ \alpha \neq 0 \\ \varphi \in \mathbb{Q}[X],\ \deg \varphi \leq d-2 \end{cases}$$

Since t is an integer, the corresponding x has a bounded denominator. Let $n = qd + r$ be the euclidean division of n by d. Write the equation $f(x) = t$ in the form

$$b^r \, (b^q)^d - \alpha x^d = \varphi(x) - c$$

The integer r is the same for infinitely many solutions. So we may assume that r is fixed. Write $b^r/\alpha = \xi^d$ with $\xi \in \mathbb{C}$. We obtain

$$\prod_{\zeta \in \mu_d} |\xi b^q - \zeta x| = \left| \frac{\varphi(x) - c}{\alpha} \right|$$

Consider the right-hand side. Since

$$b^n = f(x) - c \ll |x|^d + |b|^{\rho n})$$

we have $b^n \ll |x|^d$. Therefore

$$\left| \frac{\varphi(x) - c}{\alpha} \right| \ll |x|^{d-2} + |b|^{\rho n} \ll |x|^{d-2} + |x|^{\rho d} \tag{1}$$

Consider the left-hand side. All terms $|\xi b^q - \zeta x|$ ($\zeta \in \mu_d$) except possibly one are $\gg |x|$. As for the remaining term, since x is a rational number with bounded denominator, we may use Ridout's theorem [**6**]. Pick a real number β such that

$$0 < \beta < \min(1, d - 1 - d\rho) \tag{2}$$

(This is possible since we assumed $d > 1/(1-\rho)$). From Ridout's theorem, for suitably large x, we have

$$\text{either} \quad \left| \frac{\xi}{\zeta} - \frac{b^q}{x} \right| \gg |x|^{-(1+\beta)} \quad \text{or} \quad \frac{\xi}{\zeta} = \frac{b^q}{x}$$

The first possibility leads to

$$\left| \frac{\varphi(x) - c}{\alpha} \right| \gg |x|^{d-1-\beta}$$

Using (1) we obtain

$$|x|^{d-1-\beta} \ll |x|^{d-2} + |x|^{\rho d}$$

But (2) yields

$$d-1-\beta > d-1-\min(1, d-1-d\rho) = \max(d-2, \rho d)$$

whence $|x|$ is bounded. Thus the first possibility may occur only for finitely many x.

The second possibility gives

$$\begin{cases} x = \zeta^{-1}\xi b^q \\ c = \varphi(x) \end{cases}$$

which leads to condition (*) for infinitely many t.

We point out that the proof of this first case is somewhat similar to the proof of Lemma 2 of [**2**].

3.2. 2nd case: f has exactly two poles.

Let K be the field of definition of the two poles; K is at most a quadratic extension of $\mathbb{Q}$. By change of variable with coefficients in the field K, we may assume that the two poles of f are 0 and ∞. More specifically, f can be written

$$f(x) = \frac{\varphi(x)}{x^s} \quad \text{with} \begin{cases} \varphi \in K[X] \\ \varphi(0) \neq 0,\ d = \deg \varphi > s > 0 \end{cases}$$

Set $\varphi(X) = \varphi_o X^d + \varphi_1 X^{d-1} + \cdots + \varphi_d$ with $\varphi_o, \ldots, \varphi_d \in K$. The equation $f(x) = t$ rewrites

$$\frac{\varphi(x)}{x^s} = b^n + c$$

Note that in this case, x *a priori* is in K (and no longer in $\mathbb{Q}$).

Let v be a finite place of K. Since $b^n + c$ is an integer, we have

$$|\varphi(x)|_v \leq |x|_v^s$$

If $|x|_v < 1$, we obtain

$$|\varphi_d|_v \leq \max(1, |\varphi_o|_v, \ldots, |\varphi_{d-1}|_v)\ \ |x|_v$$

If $|x|_v > 1$, we obtain, since $d > s$,

$$|\varphi_o|_v \leq \max(1, |\varphi_1|_v, \ldots, |\varphi_d|_v) \quad \left|\frac{1}{x}\right|_v$$

Since $\varphi_o\varphi_d \neq 0$, the set of places v for which $|x|_v \neq 1$ is contained in a finite set independent of x. More precisely, there are only finitely many possibilities for the fractional ideal generated by x. We conclude that there exists a finite set $\{x_1, \ldots, x_N\}$ of elements of K such that x is necessarily of the form

$$x = x_i u$$

for some index i and with u a unit of K.

The case that $K = \mathbb{Q}$ or K is an imaginary quadratic field is easy: there are only finitely many units and so only finitely many possibilities for x, which contradicts our assumption.

Assume now that K is a real quadratic field. Let $\omega > 1$ be the fundamental unit. From above, we have that, for infinitely many solutions, x is of the form

$$x = \xi\omega^e$$

for some fixed $\xi \neq 0$ in K and $e \in \mathbb{Z}$. The equation $f(x) = t$ becomes

$$\varphi_o(\xi\omega^e)^{d-s} + \cdots + \varphi_d(\xi\omega^e)^{-s} = b^n + c$$

We may assume that $e \geq 0$: otherwise just rearrange the terms on the left-hand side in the opposite order. Note that both φ_o and φ_d are non-zero and that both s and $d - s$ are > 0. The above equation yields

$$\left|\varphi_o\xi^{d-s}\omega^{(d-s)e} - b^n\right| \ll \omega^{e(d-s-1)} + b^{\rho n}$$

On the other hand the theory of linear forms in three logarithms (*e.g.* [**1**;Ch2]) provides the following inequality: for each $\beta < 1$

$$\left|\varphi_o\xi^{d-s}\omega^{(d-s)e} - b^n\right| \gg \max(\omega^{(d-s)e}, b^n)^\beta \tag{3}$$

where the constant involved in "$\ll$" depends on β. Choosing β such that

$$1 > \beta > \max\left(\rho, \frac{d-s-1}{d-s}\right)$$

we obtain that both e and n are bounded, which contradicts our assumption. □

Remark 3.1. Inequality (3) can also be obtained by using the Ridout-Mahler theorem, for example as given in [**5**;pp.160–161] (see *e.g.* Cor.1.2).

ADDENDUM 1. The same method can be used to prove more general results. For instance let $p_1, \dots, p_h$ be h prime numbers. A more general form of our theorem can be stated with the set $S(b, \rho)$ replaced by the following set

$$S(p_1, \dots, p_h, \rho) = \{p_1^{r_1} \cdots p_h^{r_h} + c \mid c \in \mathbb{Z},\ 0 < |c| \le (p_1^{r_1} \cdots p_h^{r_h})^\rho\}$$

Yasumoto's criterion can also be shown to follow from similar principles, combined with some classical arguments about ideal factorizations in number fields. For example we sketch below how to prove by our method that $a_n := (n^3+1)2^n$ is universal.

Assume the contrary holds. As in the proof of the Main Theorem, it follows from Siegel's theorem that, for some rational function $f \in \mathbb{Q}(T)$ with at most two poles and degree ≥ 2, the equation $f(t) = a_n$ has a solution $t = t_n \in \mathbb{Q}$ for infinitely many integers n. Assume that f has one pole, the other case being even simpler. We may assume that f is a polynomial, in which case the rational numbers $\{t_n\}$ must have bounded denominators.

The factorization of a_n easily implies that f cannot have two or more distinct irreducible factors over $\mathbb{Q}$: indeed, for $n \gg 1$, all terms $g(t_n)$ with g irreducible factor of f are of the same order of growth (a power of t_n) and so must all be divisible by a large power of 2 (tending to ∞ with n); this is impossible if there are several gs. If $f = cf_1^h$, where c is constant and f_1 is irreducible, the equation $f(t_n) = a_n$ rewrites $(n^3+1)2^b = cy^h$ with $y \in \mathbb{Z}$ and where b is bounded. From well-known theorems, there are only finitely many solutions $(n, y) \in \mathbb{Z}^2$ to these equations if $h \ge 2$.

So, assume $h = 1$ and let γ be a root of f and $L = \mathbb{Q}(\gamma)$. Factoring $f(t_n)$ in L and comparing ideal factorizations of $f(t_n)$ and $a_n = (n^3+1)2^n$ in the ring of integers of L we deduce that the ideal generated by $t_n - \gamma$ has the form $A_n B^n$ for infinitely many n, where B is a prime ideal lying above 2, A_n is a fractional ideal with bounded denominator, whose norm is $\ll n^3$. Let q be the order of B in the ideal class group of L. By writing $n = qm + r$, $0 \le r < q$, we may write $A_n B^n = (A_n B^r)(B^q)^m = C_n D^m$, where C_n, D are principal, generated, say, resp. by α_n, β. We may even assume, multiplying α_n by a suitable unit, that α_n has height $\ll n^3$. Then $t_n - \gamma = \alpha_n \beta^m \mu_1^{n_1} \dots \mu_k^{n_k}$ for fixed units $\mu_1, \dots, \mu_k$ and integers $n_1, \dots, n_k$ (these depending on n).

Let γ_1, γ_2 be distinct roots of f and apply in both cases the procedure just described. We obtain equations for $t_n - \gamma_1, t_n - \gamma_2$ and, eliminating t_n, we find an equation

$$\alpha_n \beta^m \mu_1^{n_1} \dots \mu_k^{n_k} - \alpha_n^* \beta^{*m^*} \nu_1^{m_1} \dots \nu_h^{m_h} = \gamma_2 - \gamma_1 \ne 0$$

whence

$$0 < |\frac{\alpha_n \beta^m \mu_1^{n_1} \dots \mu_k^{n_k}}{\alpha_n^* \beta^{*m^*} \nu_1^{m_1} \dots \nu_h^{m_h}} - 1| \ll \frac{1}{|t_n - \gamma_2|} \ll e^{-\epsilon n}$$

where $\epsilon > 0$ does not depend on n. Since the height of α_n/α_n^* is $\ll n^6$, such inequality has finitely many solutions, by the generalized Ridout theorem (actually a special case of the generalized Roth's theorem given in [**5**]).

Addendum 2. We end this paper with a proof of the result mentioned in the introduction about the existence of a universal Hilbert subset $S \subset \mathbb{N}$ of asymptotic density 1. Let $P_1(T,Y), P_2(T,Y), \dots$ be some enumeration of all the irreducible polynomials in $\mathbb{Q}[T,Y]$. For each integer $m > 0$, denote the set of integers $n \in \mathbb{N}$ such that $P_m(n,Y)$ is reducible in $\mathbb{Q}[Y]$ by E_m. For every set $T \subset \mathbb{N}$ and every real number x, denote the set of integers $n \in T$ such that $n \leq x$ by $T(x)$. It follows from the quantitative form of Hilbert's irreducibility theorem (*e.g.* [**8**;§9.7]) that, for each $m > 0$, we have $\mathrm{card}(E_m(x)) = O(\sqrt{x})$. In particular, for each $m > 0$, $\mathrm{card}(E_m(x))/x \to 0$ as $x \to \infty$, hence E_m has density 0. Thus it is sufficient to prove the following lemma.

Lemma 3.2 — *Let $E_1, E_2, \dots$ be a sequence of subsets of $\mathbb{N}$ of density 0. Then there exists a subset $E \subset \mathbb{N}$ such that*

(i) $E_m - E$ is finite for each integer m.

(ii) E is of density 0.

This lemma proved, it suffices to take $S = \mathbb{N} - E$.

Proof. We first construct subsets $E_1^* \subset E_1, E_2^* \subset E_2, \dots$ and positive real numbers $T_1 < T_2 \dots$ with the following properties: for each integer $m > 0$

(a) $E_m - E_m^*$ is finite

(b) If $R_m = E_1^* \cup \dots \cup E_m^*$, then we have $\mathrm{card}(R_m(x)) < x/2^m$ for $x \geq T_m$

(c) $E_m^*(T_m) = \emptyset$.

Set $E_1^* = E_1$ and take T_1 to be an integer such that $\mathrm{card}(E_1(x)) < x/2$ for $x \geq T_1$: this is clearly possible. Suppose now $E_1^*, \dots, E_m^*, T_1, \dots, T_m$ constructed. Since each E_i has density 0, the same is true of E_i^*. So R_m is also of density 0. Hence there exists $\tau > 0$ such that

$$\mathrm{card}(R_m(x)) < \frac{x}{2^{m+2}} \text{ for } x \geq \tau$$

Also there exists $\tau' > 0$ such that

$$\mathrm{card}(E_{m+1}(x)) < \frac{x}{2^{m+2}} \text{ for } x \geq \tau'$$

Set $T_{m+1} = \max(\tau, \tau', 2T_m)$ and $E^*_{m+1} = E_{m+1} - [1, T_{m+1}]$. Conditions (a), (b) and (c) obviously hold for $m+1$ in place of m.

Define now E to be

$$E = \bigcup_{m=1}^{\infty} E^*_m$$

Condition (i) of Lemma 3.2 clearly holds. Let x be a real number such that $x > T_1$. Consider the integer m such that $T_m < x \leq T_{m+1}$. Since $E^*_n(T_{m+1}) = \emptyset$ for $n \geq m+1$ we have $E(x) = R_m(x)$. From (b) above, we conclude that

$$\mathrm{card}(E(x)) \leq \frac{x}{2^m}$$

For $x \to \infty$, we obtain what we want. □

REFERENCES

[1] A. Baker, *Transcendental Number Theory*, Cambridge university press, (1975).

[2] D. Berend and Ch. F. Osgood, *On the equation $P(x) = n!$ and a question of Erdös*, J. Number Th., **42** (1992), 189–193.

[3] Y. Bilu, *A note on universal Hilbert sets*, preprint, Max-Planck-Institut (Bonn), (1995).

[4] P. Dèbes, Résultats récents liés au théorème d'irréductibilité de Hilbert, *Sém. Th. Nombres, Paris, 1985-86*, Birkhauser, (1987).

[5] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, (1983).

[6] D. Ridout, The p-adic generalization of the Thue-Siegel-Roth theorem, *Mathematika*, **4**, (1957).

[7] A. Schinzel, Selected Topics in Polynomials, Ann Arbor, The university of Michigan, (1982).

[8] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, translated by M.Brown from notes by M.Waldschmidt, Vieweg, (1990).

[9] V.G. Sprindžuk, Diophantine equations with unknown prime numbers, Trudy MIAN SSSR, **158**, (1981) (English translation in *Proc. Steklov Inst. Math.*, **4**, (1983), 197–214).

[**10**] M. Yasumoto, Hilbert Irreducibility Sequences and Nonstandard Arithmetic, *J. Number theory*, **26**, (1987).