Journal of Number Theory 128 (2008) 2963–2972

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The strict Waring problem for polynomial rings

Luis H. Gallardo [a,*], Leonid N. Vaserstein [b]

[a] *Department of Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France*
[b] *Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, USA*

ARTICLE INFO

Article history:
Received 21 July 2006
Available online 1 October 2008
Communicated by David Goss

MSC:
11T55
11P05
11D85

Keywords:
Waring's problem
Polynomial rings
Finite fields

ABSTRACT

We prove among several results that under mild conditions any polynomial in $F_q[t]$ is a strict sum of k^4 kth powers improving on an exponential ($k^2 2^{k+1}$) bound of Car–Effinger–Hayes.

0. Introduction

For any ring A and any integer $k \geqslant 1$, let $A_k \subset A$ be the set of all sums of kth powers in A. For any $a \in A_k$, let $w_k(a, A)$ be the least s such that a is the sum of s kth powers. Let $w_k(A)$ be the supremum of $w_k(a)$ where a is ranges over A_k (possibly, $w_k(A) = \infty$).

If $pA = 0$ for a prime number p, then $w_k(A) = w_{pk}(A)$ for all $k \geqslant 1$.

Clearly, A_k is closed under addition and multiplication. When $a \in A_k$ is a unit in A, then $1/u \in A_k$.

For any finite field F of q elements, it is known that

(1) $w_2(F) = 1$ when q is even and $w_2(F) = 2$ when q is odd (obvious);
(2) $w_k(F) = 1$ when $\gcd(k, q-1) = 1$ (obvious);
(3) $w_k(F) \leqslant \gcd(k, q-1) \leqslant k$ for any k and q (Tornheim [12]);
(4) $w_k(F) \leqslant 2$ for any k when $q \geqslant k^4$ (Weil [18, p. 502]);
(5) $w_k(F) = k$ when $q = k+1$ is a prime number (obvious).

* Corresponding author.
E-mail addresses: luis.gallardo@univ-brest.fr (L.H. Gallardo), vstein@math.psu.edu (L.N. Vaserstein).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.07.009

For the integers $\mathbb{Z}$, It is known that

(6) $w_2(\mathbb{Z}) = 4$ for the integers $\mathbb{Z}$ (Gauss, Lagrange);
(7) $w_k(\mathbb{Z}) < \infty$ for all k (Hilbert);
(8) $w_k(\mathbb{Z}) \leqslant k(k3\ln(k) + 4.7)$ for any odd k where ln means the natural logarithm; better bounds are known for some k (Wooley [19]).

Of special interest in this paper is the ring $F[t]$ of polynomials in one variable t with coefficients in a finite field F of q elements. For this ring, it is known that

(9) $w_k(F[t]) < \infty$ for any k, q (Paley [10]);
(10) $w_k(F[x]) \leqslant 3k^2(k-1)/4 + k + 1$ for any k, q (Vaserstein [13, Theorem 5]);
(11) $w_k(F[t]) \leqslant k(k+1)/2$ for any k and $q \geqslant k^2 - k$; $w_k(F[t]) \leqslant 2k - 1$ for any k when $q \geqslant k^4$ (Vaserstein [13, Theorem 3(d)]);
(12) $w_k(F[t]) \leqslant 3k/2$ for any k when $q \geqslant R(k)$ (Vaserstein [15, Theorem 1(iii)]);
(13) $w_2(F[t]) = 1$ when q is even; $w_2(F[t]) = 2$ when q is odd and -1 is a square in F; $w_2(F[t]) = 3$ when q is odd and -1 is not a square in F;
(14) $w_3(F[t]) = 1$ when q is a power of 3; $3 \leqslant w_3(F[t]) \leqslant 4$ when q is not a power of 3 (Vaserstein [15, Theorem 3]); $w_3(F[t]) = 3$ when q is not a power of 3 and $q \neq 2, 4, 16$ (Vaserstein [14]).

Carlitz suggested to consider the problem of representation of a polynomial $a \in F[t]$ as a *strict sum*

$$a = x_1^k + \cdots + x_s^k$$

of kth powers in $F[t]$ where "strict" means that $\deg(x_i)^k \leqslant \deg(a) + k - 1$.

A reason for this restriction on the degrees is that this allows us to use the circle method which worked well for the integers $\mathbb{Z}$. The method gives a lower bound for the number of representations of large integers as sums of positive kth powers (showing that the number is nonzero for sufficiently many kth powers), and its analogue for $F[t]$ gives a lower bound for the number of strict representations of large degree polynomials. Another reason is that while no example with $w_k(A) > \max(3, w_k(F))$ is known, it could be easier to find lower bounds for the number of kth powers needed in the case of strict sums.

Here are some known results about strict sums of kth powers in $F[t]$ where F is a finite field of q elements:

(15) when $k = 2$ and q is odd, every polynomial in $F[t]$ is the strict sum of four squares (Cohen [5]);
(16) when $k = 2$, and q is odd, every polynomial in $F[t]$, except two polynomials of degree 3 and six polynomials of degree 4 in the case $q = 3$, is the strict sum of three squares (Serre (Effinger and Hayes [6, Theorem 1.14], Webb [17]));
(17) when $k = 3$, every strict sum of cubes in $F[t]$ is the strict sum of 9 cubes (Car and Gallardo [4], Gallardo [8]); when $q = 13$ or 16, the number 9 can be improved to 8; $q \neq 2, 4, 7, 13, 16$, every polynomial is the strict sum of 7 cubes;
(18) when $k = 4$, $\gcd(q, 6) = 1$, and $q \neq 5, 13, 17, 25, 29$, every polynomial in $F[t]$ is the strict sum of 16 biquadrates (Gallardo [7]);
(19) for any k there is an integer $s(k)$ such that when $p = \operatorname{char}(F) > k$ every polynomial $a \in F[t]$ is a strict sum of at most $s(k)$ kth powers (Car [2], Webb [16], Kubota [9], Effinger and Hayes [6, Theorem 1.9]);
(20) when $p = \operatorname{char}(F) > k$ and the degree of a polynomial $a \in F[t]$ is sufficiently large, then a is a strict sum of at most $k^2 2^{k+1}$ kth powers (Car [3], Effinger and Hayes [6]).

See Effinger and Hayes [6] for more results.

We write $q = p^\alpha k'$ with $\gcd(k', p) = 1$ where $p = \operatorname{char}(F)$ as above. In this paper for the ring $A = F[t]$ we prove:

(21) for any k, q, any polynomial a in A_k which is a strict sum of kth powers is a strict sum of at most k^6 k-th powers;
(22) for $q > (k-1)^2$ the bound k^6 can be improved to k^4;
(23) for large degree (depending on k) this bound k^6 can be improved to $k^3/2$;
(24) for large $\deg(a)$ and $q > (k-1)^2$ this bound k^6 can be improved to

$$k\bigl(\ln(k+1)+2\bigr)+1.$$

In particular, we can replace the exponential in k bound $k^2 2^{k+1}$ in (20) by a polynomial bound k^4, and our proof is much shorter. Also we extended (20) to the case $p \leqslant k$.

In fact in this paper, we replace the finite field F to be any field F such that -1 is a sum of kth powers. This includes any field F of finite characteristic. Also the condition holds when k is odd. This condition $-1 \in F_k$ is equivalent to the condition that F_k is a subring (or a subfield) of F. Hilbert's proof of (6) implies that $-1 \in F_k$ for all k provided that $-1 \in F_2$.

We obtain better bounds when the nonzero kth powers form a subgroup of finite index in the multiplicative group of F. In the case of a finite field F_q, the index is $\gcd(k, q-1)$ (cf. (3)).

1. Statement of main results

For the rest of the paper, $k \geqslant 2$, F is a field such that $w_k(-1, F) < \infty$, i.e., $-1 \in F_k$ (e.g., $p = \operatorname{char}(F) \neq 0$ or k is odd), and $A = F[t]$.

If $\operatorname{char}(F) = p \neq 0$ and $\gcd(p, k) \neq 1$, we can write $k = k' p^\alpha$ with $\alpha \geqslant 1$ and $\gcd(k', p) = 1$. Then F_{p^α} consists of p^α-powers in F, $F_k = (F_{p^\alpha})_{k'} = (F_{k'})_{p^\alpha}$, A_k consists of p^α-powers of polynomials in $A_{k'}$, $w_k(F) = w'_k(A)$, $w_k(A) = w_{k'} A$, the strict sums of kth powers in A are the p^αth powers of strict k'-powers in A. This justifies imposing the condition $kF \neq 0$ (e.g, $k \neq 0$ in F).

Theorem 1.1. *Let $-1 \in F_k$ and $kF \neq 0$. Then*:

(i) *when* $\operatorname{char}(F) = 0$, $w_k(F) \leqslant w_k(A) \leqslant k^2(k-1)(w_k(-1, F)+1)/4$;
(ii) *when* $\operatorname{char}(F) \neq 0$, $w_k(F) \leqslant k^2(k-1)/2$ *and*

$$w_k(A) \leqslant k+1+k^2(k-1)/2;$$

(iii) *when* $\operatorname{char}(F) = p \neq 0$, $w_k(F) \leqslant p(p-1)^2 k(\log_p(k)+3)$ *and*

$$w_k(A) \leqslant k+1+p(p-1)^2 k(\log_p(k)+3);$$

(iv) *every polynomial in A which is a strict sum of kth powers is the strict sum of at most k^6 kth powers*;
(v) *every polynomial in A_k of degree $\geqslant k^5-1$ is the strict sum of at most $k^3/2$ kth powers.*

Let F^* denote the multiplicative group of the field F and F^{*k} the subgroup of the kth powers.

Theorem 1.2. *Let $-1 \in F_k$ and $kF \neq 0$. Assume that $F^{*k} \cap F_k$ has a finite index K in $(F_k)^*$. Then*:

(i) $w_k(F) \leqslant K$.

Moreover, if F is infinite, then:

(ii) $F_k = F$ *and* $w_k(F) \leqslant 1 + w_k(-1, F,)$;
(iii) $A_k = A$ *and* $w_k(A) \leqslant k(K+1)/2$.

Notice that Theorem 1.2(i) implies (3). Since $w_k(F) \leqslant k$, we obtain

Corollary 1.3. *If F is a field of q elements and* $\mathrm{card}(F_k) = q_0$, *then*

(i) $w_k(F) \leqslant K = \gcd(k, q-1)(q_0 - 1)/(q-1) \leqslant \gcd(k, q-1) \leqslant k$;
(ii) *every polynomial in $F[t]$ which is a strict sum of kth powers is a strict sum of at most $(k^3 - 2k^2 - k + 1)w_k(F)$ kth powers.*

Theorem 1.4. *Let $-1 \in F_k$ and $kF \neq 0$. Assume that* $\mathrm{card}(F_k) \geqslant k$. *Then*:

(i) $w_k(A) \leqslant w_k(F)(k-1) + 1$;
(ii) *every polynomial $a \in A = F[t]$ of degree $D \geqslant k^4 - k^2 - k + 1$ is the strict sum of at most $k(w_k(F) + \ln(k+1)) + 1$ kth powers*;
(iii) *every polynomial $a \in A = F[t]$ of degree $D \geqslant k^3 - 2k^2 - k + 1$ is the strict sum of at most $k(w_k(F) + 3\ln(k)) + 2$ kth powers*;
(iv) *every polynomial $a \in A$ which is the strict sum of kth powers is the strict sum of $(k^3 - 2k^2 - k + 1)w_k(F)$ kth powers.*

Using (4) and the fact that $\mathrm{card}(F_k) \geqslant 1 + (q-1)/k$, we obtain (24) as a particular case of Theorem 1.4.

For large finite F, Theorem 1.4 can be improved by (4).

Corollary 1.5. *Assume that* $\mathrm{char}(F) \neq 0$, $\mathrm{card}(F) \geqslant k^4$, *and F is algebraic over its prime subfield F_0. Then*:

(i) $w_k(F) \leqslant 2$;
(ii) *every polynomial $a \in A = F[t]$ of degree $D \geqslant k^4 - k^2 - k + 1$ is the strict sum of at most $(\ln(k+1) + 2)k + 1$ kth powers*;
(iii) *every polynomial $a \in A = F[t]$ of degree $D \geqslant k^3 - 2k^2 - k + 1$ is the strict sum of at most $(3\ln(k) + 2)k + 2$ kth powers*;
(iv) *every polynomial $a \in A$ which is the strict sum of kth powers is the strict sum of $2(k^3 - 2k^2 - k + 1)$ kth powers.*

The rest of the paper is about proving Theorems 1.1, 1.2, and 1.4.

When $\mathrm{char}(F) = 0$ or $p = \mathrm{char}(F) > k$ (and $w_k(F) < \infty$), every polynomial in $F[t]$ is a strict sum of kth powers (Webb [16]) so the theorems can be simplified.

2. Proof of Theorem 1.2

(i) Set $H = F^{*k} \cap F_k$. If $a \in A_k$ and $w_k(a) > 1$, then dropping a kth power in a representation of a as the sum of $w_k(a, A)$ kth powers, we find an element $b \in A_k$ with $w_k(b, a) = w_k(a, A) - 1$. Thus, the function w_k on F_k takes all values between 0 and $w_k(A)$. Since $w_k(a, F)$ is constant on each coset aH, $w_k(F) \leqslant K$. So the first part of Theorem 1.2(i) is proved.

When F is infinite, every element of F has the form $a^k - b^k$ (Bergelson and Shapiro [1]), so (using the condition $-1 \in F$) $F_k = F$ and $w_k(F) \leqslant 1 + w_k(-1, F)$. So Theorem 1.2(i) is proved.

(ii) The fact that w_k takes on $(F_k)^*$ all values between 1 and $w_k(A)$ implies that increasing if necessary the values, we can make them $1, 2, \ldots, K$ which gives the following result about an average value of w_k on nonzero elements of F:

Proposition 2.1. *Let $\{f_1, \ldots, f_K\}$ be the cossets $(F_k)^*/(F_k \cap F^{*k})$. Then for any nonzero $a \in F_k$,*

$$\sum_{i=1}^{K} w_k(af_i, F) \leqslant K(K+1)/2.$$

Assume now that F is infinite.

(ii) By Bergelson and Shapiro [1], every $x \in F$ has the form $x_1^k - x_2^k$. Writing -1 as the sum of $w_k(-1, F)$ kth powers, we see that every $x \in F$ is the sum of $1 + w_k(-1, F)$ kth powers.

(iii) We pick distinct $a_1, \dots, a_k \in F$ and, using Vandermonde's determinants, write

$$\sum_{i=1}^{k} (t + a_i)^k / b_i = kt + c_0 \tag{1}$$

with $b_i = \prod_{j \neq i}(a_i - a_j)$. By (i), we can write each $1/b_i$ as the sum of K kth powers. Moreover, by Proposition 2.1, multiplying (1) by a nonzero element f of F, we can write each $1/b_i$ as a sum of kth powers, with the total number of kth powers is at most $k(K+1)/2$. So $w_k(ft, A) \leqslant k(K+1)/2$. Since ft here can be replaced by any $a \in A = F[t]$, we obtain that $w_k(a) \leqslant k(K+1)/2$ for every $a \in A$, i.e., $w_k(A) \leqslant k(K+1)/2$.

3. Proof of Theorem 1.4

We assume in this section that $k \neq 0$ in F and that $-1 \in A_k$.

Lemma 3.1. *Assume that $k \neq 0$ in F. Let $d \geqslant 1$ be an integer, a be a monic polynomial in $F[t]$ of degree dk. Then there is a polynomial $x \in F[t]$ of degree d such that* $\deg(a - x^k) \leqslant dk - d - 1$.

Proof. Let $x = \sum_{i=0}^{d} x_i t^i$ with unknown coefficients $x_i \in F$. We take $x_d = 1$ so $\deg(a - x^k) \leqslant kd - 1$. Then, to find x_{d-1} such that $\deg(a - x^k) \leqslant kd - 2$, we have a linear equation of the form

$$kx_{d-1} = \text{a given element of } F.$$

Similarly we find $x_{d-2}, \dots, x_0$. $\square$

Corollary 3.2. *Under the conditions of Lemma* 3.1*, let d' be an integer such that $dk - d \leqslant d'k \leqslant dk - 1$. Then there is $c \in F[t]$ such that $a - c^k$ is a monic polynomial of degree $d'k$.*

Proof. Apply Lemma 3.1 to $a - t^{d'k}$. $\square$

For any rational number x, we denote by $\lceil x \rceil$ the least integer s satisfying $x \leqslant s$. For any integer $d \geqslant 1$, we define $f(d) = \lceil d(k-1)/k \rceil$. Inductively, we define, $f^s(d) = f(f^{d-1}(d))$. Note that $f(d) < d$ for $d \geqslant k$ and $f(d) = d$ when $d \leqslant k - 1$.

Lemma 3.3. *For any integers $d, s \geqslant 1$*

$$f^s(d) \leqslant d\big((k-1)/k\big)^s + (k-1)\big(1 + (k-1)/k + \dots + \big((k-1)/k\big)^{s-1}\big)/k.$$

Proof. It is easy by induction on s using that

$$f(d) = \lceil d(k-1)/k \rceil \leqslant d(k-1)/k + (k-1)/k. \qquad \square$$

Corollary 3.4. *For any integers $d, s \geqslant 1$*

$$f^s(d) < d/e^{s/k} + k - 1.$$

Proof. It is well known that $(k-1)/k \leqslant e^{-1/k}$ (Pólya and Szegö [11, Problem 171]) and that

$$1 + (k-1)/k + \big((k-1)/k\big)^2 + \big((k-1)/k\big)^3 + \dots = k. \qquad \square$$

Proposition 3.5. *Let $a \in F[t]$ be a polynomial of degree $D \geqslant k^4 - k^2 - k + 1$ Set $d = \lceil D/k \rceil$. Then there are $n = \lceil k\ln(k+1) \rceil + w_k(F)$ polynomials $x_i \in F[t]$ of degree $\leqslant d$ each such that* $\deg(a - \sum a_i^k) < d$.

Proof. Note that $d \geqslant k(k^2-1)$. Let a_{dk} be the degree of the dk coefficient in a (it is 0 if $D < dk$.) We write $a_{dk} - 1$ as the sum of $m = w_k(F)$ kth powers c_i^k in F and set $x_i = c_i t^d$ for $i \leqslant m$. Then $b = a - \sum x_i^k$ is a monic polynomial of degree dk.

We set $s = \lceil k\ln(k+1) \rceil$ and apply s times Lemma 3.1. So there are s polynomials x_i ($m+1 = w_k(F)+1 \leqslant i \leqslant m+s = n$) such that $\deg(x_i) \leqslant d$ and $\deg(b - \sum_{m+1}^n x_i^k) \leqslant kf^s(d)$.

By Corollary 3.4,

$$f^s(d) < d/e^{s/k} + k - 1 \leqslant d/(k+1) + k - 1 \leqslant d/k.$$

since $d \geqslant k(k^2-1)$. So

$$\deg\left(a - \sum_1^n x_i^k\right) \leqslant kf^s(dk) = \deg\left(b - \sum_{m+1}^n x_i^k\right) \leqslant kf^s(d) < d. \qquad \square$$

Lemma 3.6. *Let $c_i \in F_k$ be k distinct elements. Then there are $k+1$ nonzero elements $d_i \in F_k$ such that*

$$\sum_{i=1}^k d_i(d_0 t + a_i)^k = t \tag{2}$$

and $d_1 = 1$, where t is an indeterminate.

Proof. We can take d_i to be Vandermonde's determinants and obtain

$$\sum_{i=1}^k (t + c_i)^k = \text{a polynomial of degree 1}.$$

After this, we can divide the last equality by d_1 and make an affine change of variables. (See Vaserstein [15].) $\square$

Corollary 3.7. *Every polynomial $b \in A$ is the sum of at most $1 + (k-1)w_k(F)$ k-powers y_i^k with* $\deg(y_i) = \deg(b)$.

Proof. Replace t in (2) by b. $\square$

Proof of Theorem 1.4(i). See Proposition 3.8. $\square$

Remark. In fact, Lemma 3.6 implies that $A'_k = A'$ and $w_k(A') \leqslant w_k(F[t])$ for every F-algebra A' assuming that $-1 \in F_k$ and $\operatorname{card}(F_k) \geqslant k$. Indeed, we can replace t in Lemma 3.6 by an arbitrary element of any F-algebra A' (assuming the condition of Lemma 3.6) and every d_i is a sum of kth powers (assuming that $-1 \in F_k$).

Proof of Theorem 1.4(ii). Combine Proposition 3.5 and Corollary 3.7. $\square$

Proposition 3.8. *Let $a \in F[t]$ be a polynomial of degree $D \geqslant k^3 - 2k^2 - k + 1$ Set $d = \lceil D/k \rceil$. Then there are $n = \lceil 3k\ln(k) \rceil + w_k(F)$ polynomials $x_i \in F[t]$ of degree $\leqslant d$ each such that* $\deg(a - \sum a_i^k) < d$.

Proof. In view of Proposition 3.5 (using that $3\ln(k) > \ln(k+1)$) we can assume that $D < k^4$, hence $d \leqslant k^3$.

We set $s = \lceil 3k\ln(k)\rceil$. As in the proof of Proposition 3.5, we find $n = w_k(F) + s$ polynomials $x_i \in A$ with $\deg(x_i) \leqslant d$ such that $b = a - \sum_1^n x_i^k$ is a monic polynomial of degree $f^s(d)k$ and

$$f^s(d) < d/e^{s/k} + k - 1 \leqslant d/k^3 + k - 1 < k$$

hence $f^s(d) = k - 1$. Now we use Lemma 3.1 and find $x_{n+1} \in A$ of degree $k-1$ such that $\deg(b - x_{n+1}^k) \leqslant k(k-2) \leqslant d/k$. $\square$

Proof of Theorem 1.4(iii). Combine Proposition 3.8 and Corollary 3.7. $\square$

Proof of Theorem 1.4(iv). By (ii), we can assume that $\deg(a) \leqslant k^3 - 2k^2 - k$. Consider the (F_k)-vector space spanned by x^k with $\deg(x) \leqslant k^2 - 2k - 1$. Its dimension over F_k is at most $k^3 - 2k^2 - k + 1$. $\square$

Remark. When the kth powers in the multiplicative group of F have a finite index K (e.g., $\mathrm{card}(F) = g < \infty$ in which case $K = \gcd(k, q-1)$) then $w_k(F) \leqslant K$ and as in Vaserstein [13], we can replace $1 + (k-1)w_k(F)$ in Corollary 3.7 by $k(K+1)/2$.

4. Proof of Theorem 1.1

(i) By Vaserstein [13, Section 2] we have

$$\sum_{i=1}^{\alpha(k)} (t+a_i)^k - (t+b_i)^k = kct + c_0,$$

with $a_i, b_i, c, c_0 \in F$, $c \neq 0$, $\alpha(k) = k-1$ for $k \leqslant 11$, $\alpha(k) \leqslant k(k-1)\ln(k)$ for all $k \geqslant 2$. Note that $2\alpha(k) \leqslant k^2(k-1)/2$ for all $k \geqslant 2$.

Therefore,

$$w_k(kct + c_0, A) \leqslant \alpha(x)\big(w_k(-1, F) + 1\big) \leqslant k^2(k-1)\big(w_k(-1, F) + 1\big)/4$$

hence

$$w_k(A) \leqslant k^2(k-1)\big(w_k(-1, F) + 1\big)/4$$

for any F-algebra A including $A = F[t]$.

(ii) We write $k = \sum_{j=0}^{l} r_i p^i$ in base p with $r_l \neq 0$. By Theorem 1.4, we can assume that $k > p$, i.e., $l \geqslant 1$. Here $l = \lceil \log_p(k)\rceil$.

Let F_0 be the prime subfield of F, so $F_0 = \mathbb{Z}/p\mathbb{Z}$. For every integer $i \geqslant 0$ we write $i = \sum d_j p^j$ in base p and define $a_i = \sum d_j y^j \in F[y]$. In particular, $a_0 = 0$. We have

$$\sum_{i=0}^{k-1} (t+a_i)^k / b_i = kt + c_0 \tag{3}$$

where

$$b_i = \prod_{j\neq i} (a_i - a_j) \in F[y],$$

and $c_0 \in F[y]$.

We set $h = \prod_{i=1}^{p^l(r_l+1)-1} a_i$. Then $h = \operatorname{lcm}(b_1, \ldots, b_k)$. Moreover,

$$h/b_i = \prod_{j=k}^{p^l(r_l+1)-1} (a_i - a_j).$$

So $\deg(h/b_i) \leqslant l(k-2)$. The total number of coefficients in all $b_0, \ldots, b_{k-1}$ is at most $k(k-2)l + k \leqslant k(k-1)l$. Now we replace y in (3) by y^k and multiply it by a nonzero element $f \in F_0$:

$$\sum_{i=0}^{k-1} (t + a_i)^k f h'/b'_i = kfh't + h'fc_0. \tag{4}$$

Since the mean of $w_k(fd, F_0)$ for a nonzero $d \in F_0$ where f ranges over F_0^* is at most $p/2$, we obtain that

$$w_k\big(fkh't, F[t,y]\big) \leqslant k(k-1)lp/2 \leqslant k(k-1)^2/2 < k^2(k-1)/2$$

for some $f \in F^*$.

When F is infinite, $kfh't + h'fc_0$ can be specialized to an arbitrary element of F, so $w_k(F) < k^2(k-1)/2$ (recall that we consider the case $k > p$; when $k = 2 < p$, $w_k(F)$ could be 2). When F is finite, $w_k(F) \leqslant k \leqslant k^2(k-1)/2$.

Using that $w_k(A/h'A) \leqslant k+1$ (Vaserstein [13, Theorem 5]), we obtain that $w_k(A) \leqslant k + k^2(k-1)/2$ for any commutative F-algebra A of transcendence degree 1 including $A = F[t]$.

Replacing y, t in (4) by t and an arbitrary polynomial in $F[t]$ and looking at the degrees, we obtain

Corollary 4.1. *Every polynomial $a \in A$ of degree $D \geqslant kl = k\lceil \log_p(k) \rceil$ is the sum of $k^2(k-1)/2$ kth powers of degree $\leqslant Dk + k(k-2)\lceil \log_p(k) \rceil$ each.*

(iii) We follow the proof of Theorem 3(c) in Vaserstein [13]. Set $K = \gcd(k, p-1)$. Find an integer c such that $1 \leqslant c \leqslant p-1$ and $kc \equiv K \bmod p$. Set $m(p-1)$ to be the sum of p-digits of $kc(p-1)/K$. Note that m is an integer and $m < \log_p(kc(p-1)/K) + 1 < \log_p(k) + 3$.

Let $X(m)$ denote the set of all linear forms $y = c_1 y_1 + \cdots + c_m y_m$ in m variables y_i with coefficients c_i in the prime subfield F_0. Note that $\operatorname{card}(X(m)) = p^m < p(p-1)^2 k/K$.

We have

$$\sum_{y \in X(m)} (x+y)^{kc(p-1)/K} y = \big(kc(p-1)/K\big) x Y\big(kc(p-1)/K, m\big) \tag{5}$$

where $Y(s,m) = \sum_{y \in X(m)} y^s \neq 0$ (note that $Y(s,m) = 0$ unless the sum of p-digits of s is divisible by $p-1$ and is at least $m(p-1)$).

If F is infinite, we can replace the variables y_i in (5) by a_i^k with $a_i \in F$ such that the specialization of the polynomial $Y(kc(p-1)/K, m)$ stays nonzero. Then the left-hand side of (5) becomes the sum of at most $p^m mK$ kth powers while the right-hand side represents an arbitrary element in any F-algebra A. In particular,

$$w_k(F) \leqslant w_k\big(F[t]\big) \leqslant p^m mK < \big(p(p-1)^2 k/K\big)\big(\log_p(k) + 3\big)K = p(p-1)^2 k\big(\log_p(k) + 3\big).$$

Assume now that F is finite. Then $w_k(F) \leqslant k < p(p-1)^2 k(\log_p(k) + 3)$. To bound $w_k(A)$, we replace the variables in (4) by a_i^k where $a_i \in F[z]$ have degrees $\leqslant \log_p(k) + 1$ and such that the specialization b_0 of $Y(kc(p-1)/K, m)$ stays nonzero. We used that the total degree of $Y(kc(p-1)/K, m)$ is

$kc(p-1)/K \leqslant k(p-1)^2/K$ and this number is less than the number $p^{\lfloor \log_p(k)+2 \rfloor}/K$ of all a_i^k with $a_i \in F[z]$ of degrees $\leqslant \log_p(k)+1$. Thus, we obtain an identity

$$\sum_{i=1}^{p^m} (x+b_i)^{kc(p-1)/K} b_i = \big(kc(p-1)/K\big) x b_0 \tag{6}$$

with each $b_i \in F[z]$, of degree $\leqslant k(\log_p(k)+1)$ being the sum of mK kth powers in $F[z]$ for $1 \leqslant i \leqslant p^m$ and with $b_0 \neq 0$ of degree $\leqslant k^2(p-1)^2(\log_p(k)+1)$.

Now it is clear that the sums of $p^m mK$ kth powers contain a nonzero ideal I of A. Using that $w_k(A/I) \leqslant k+1$, we obtain that $w_k(A) \leqslant k+1+p(p-1)^2(\log_p(k)+3)$. Moreover, the bounds on the degrees of b_i in (6) give the following

Corollary 4.2. *Every polynomial $a \in A_k$ of degree $D \geqslant k(\log_p(k)+1)$ is the sum of at most $k+1+p(p-1)^2(\log_p(k)+3)$ kth powers of degree $\leqslant D(k(p-1)^2+1)$ each.*

(v) By Theorem 1.4(ii), we can assume that $\mathrm{card}(F_k) < k$, hence $k > p = \mathrm{char}(F)$. Let $a \in A$ and $D = \deg(a) \geqslant k^4 \log_p(k)$. Set $d = \lceil D/k \rceil$. Then $d \geqslant k^3 \log_p(k)$. Let a_{dk} be the degree dk coefficient in a (it is 0 if $D < dk$.) We write $a_{dk} - 1$ as the sum of $m = w_k(F)$ kth powers c_i^k in F and set $x_i = c_i t^d$ for $i \leqslant m$. Then $b = a - \sum x_i^k$ is a monic polynomial of degree dk.

We set $s = \lceil k \ln(k+1) \rceil$ and apply s times Lemma 3.1. So there are s polynomials x_i ($m+1 = w_k(F)+1 \leqslant i \leqslant m+s = n$) such that $\deg(x_i) \leqslant d$ and $\deg(b - \sum_{m+1}^n x_i^k) \leqslant k f^s(d)$.

By Corollary 3.4,

$$f^s(d) < d/e^{s/k} + k - 1 \leqslant d/(k+1) + k - 1 \leqslant d/k.$$

since $d \geqslant k^3 \log_p(k)$. So

$$\deg\left(a - \sum_1^n x_i^k\right) \leqslant k f^s(dk) = \deg\left(b - \sum_{m+1}^n x_i^k\right) \leqslant k f^s(d) < d.$$

(iv) By Theorem 1.4(iv), we can assume that $\mathrm{card}(F_k) < k$, hence $k > p = \mathrm{char}(F)$. Let $a \in A$ be a strict sum of kth powers and $D = \deg(a)$. We want to prove that a is the strict sum of $k^5 \log_p(K)$ kth powers.

By Theorem 1.1(v), we can assume that $D \leqslant k^4 \log_p(k) - 1$. Then we can write a as a linear combination of at most $D \leqslant k^4 \log_p(k)$ kth powers each of degree $\leqslant D+k-1$. Writing every coefficient in F as the sum of k kth powers, we obtain a as the strict sum of at most k^6 kth powers.

References

[1] V. Bergelson, D.B. Shapiro, Multiplicative subgroups of finite index in a ring, Proc. Amer. Math. Soc. 116 (4) (1992) 885–896.
[2] M. Car, Le problème de Waring pour l'anneau des polynômes sur un corps fini, C. R. Acad. Sci. Paris Sér. A–B 273 (1971) A141–A144.
[3] M. Car, Le problème de Waring pour l'anneau des polynômes sur un corps fini, Séminaire de Théorie des Nombres, 1972–1973, Univ. Bordeaux I, Talence, Exp. No. 6, 13 pp. Lab. Théorie des Nombres, Centre Nat. Recherche Sci., Talence, 1973.
[4] M. Car, L. Gallardo, Sums of cubes of polynomials, Acta Arith. 112 (1) (2004) 41–50.
[5] E. Cohen, Sums of an even number of squares in GF[p^n, x], Duke Math. J. 14 (1947) 251–267.
[6] G.W. Effinger, D.R. Hayes, Additive Number Theory of Polynomials Over a Finite Field, Oxford Math. Monogr., Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, ISBN 0-19-853583-X, 1991, xvi+157 pp.
[7] L. Gallardo, Sums of biquadrates and cubes in $F_q[t]$, Rocky Mountain J. Math. 33 (3) (2003) 865–873.
[8] L. Gallardo, Waring's problem for cubes and squares over a finite field of even characteristic, Bull. Belg. Math. Soc. Simon Stevin 12 (3) (2005) 349–362.
[9] R.M. Kubota, Waring's problem for $F_q[x]$, Dissertationes Math. (Rozprawy Mat.) 117 (1974) 60.
[10] R.E.A.C. Paley, Theorems on polynomials in a Galois field, Q. J. Math. 4 (1933) 52–63.

[11] G. Pólya, G. Szegö, Problems and Theorems in Analysis, I. Series, Integral Calculus, Theory of Functions, translated from the German by Dorothee Aeppli, reprint of the 1978 English translation, Classics in Mathematics, Springer-Verlag, Berlin, ISBN 3-540-63640-4, 1998, xx+389 pp.
[12] L. Tornheim, Sums of n-th powers in fields of prime characteristic, Duke Math. J. 4 (1938) 359–362.
[13] L.N. Vaserstein, Waring's problem for algebras over fields, J. Number Theory 26 (1987) 286–298.
[14] L.N. Vaserstein, Sums of cubes in polynomial rings, Math. Comp. 56 (1991) 349–357.
[15] L.N. Vaserstein, Ramsey's theorem and the Waring's problem for algebras over fields, in: Proc. of Workshop on the Arithmetic of Function Fields, Ohio State Univ., 1991, de Gruyter, Berlin, 1992, pp. 435–442.
[16] W.A. Webb, Waring's problem in GF[q,x], Acta Arith. 22 (1973) 207–220.
[17] W.A. Webb, Numerical results for Waring's problem in GF[q,x], Math. Comp. 27 (1973) 193–196.
[18] A. Weil, Numbers of solutions of equations in finite fields, Bull. Amer. Math. Soc. 55 (1949) 497–508.
[19] T.D. Wooley, Large improvements in Waring's problem, Ann. of Math. (2) 135 (1) (1992) 131–164.