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

A R T I C L E   I N F O

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

A B S T R A C T

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

© 2008 Elsevier Inc. All rights reserved.

0. Introduction

For any ring $A$ and any integer $k \geq 1$, let $A_k \subset A$ be the set of all sums of $k$th 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 $s$ $k$th 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 $k \geq 1$.

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) $w_k(F) \leq gcd(k, q - 1) \leq k$ for any $k$ and $q$ (Tornheim [12]);
(4) $w_k(F) \leq 2$ for any $k$ when $q \geq k^4$ (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 © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2008.07.009
For the integers \( \mathbb{Z} \), it is known that

\begin{enumerate}
  \item \( w_2(\mathbb{Z}) = 4 \) for the integers \( \mathbb{Z} \) (Gauss, Lagrange);
  \item \( w_k(\mathbb{Z}) < \infty \) for all \( k \) (Hilbert);
  \item \( w_k(\mathbb{Z}) \leq k(3 \ln(k) + 4.7) \) for any odd \( k \) where \( \ln \) means the natural logarithm; better bounds are known for some \( k \) (Wooley [19]).
\end{enumerate}

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

\begin{enumerate}
  \item \( w_k(F[t]) < \infty \) for any \( k, q \) (Paley [10]);
  \item \( w_k(F[x]) \leq 3k^2(k - 1)/4 + k + 1 \) for any \( k, q \) (Vaserstein [13, Theorem 5]);
  \item \( w_k(F[t]) \leq k(k+1)/2 \) for any \( k \) and \( q \geq k^2 - k \); \( w_k(F[t]) \leq 2k-1 \) for any \( k \) when \( q \geq k^4 \) (Vaserstein [13, Theorem 3(d)]);
  \item \( w_k(F[t]) \leq 3k/2 \) for any \( k \) when \( q \geq R(k) \) (Vaserstein [15, Theorem 1(iii)]);
  \item \( w_2(F[t]) = 1 \) 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 \( F \);
  \item \( w_3(F[t]) = 1 \) when \( q \) is a power of 3; \( 3 \leq w_3(F[t]) \leq 4 \) 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]).
\end{enumerate}

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

\[ a = x_1^k + \cdots + x_t^k \]

of \( k \)th powers in \( F[t] \) where “strict” means that \( \deg(x_i^k) \leq \deg(a) + k - 1 \).

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 \( k \)th powers (showing that the number is nonzero for sufficiently many \( k \)th 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 \( k \)th powers needed in the case of strict sums.

Here are some known results about strict sums of \( k \)th powers in \( F[t] \) where \( F \) is a finite field of \( q \) elements:

\begin{enumerate}
  \item when \( k = 2 \) and \( q \) is odd, every polynomial in \( F[t] \) is the strict sum of four squares (Cohen [5]);
  \item 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]]);
  \item 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;
  \item 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]);
  \item for any \( k \) there is an integer \( s(k) \) such that when \( p = \text{char}(F) > k \) every polynomial \( a \in F[t] \) is a strict sum of at most \( s(k) \) \( k \)th powers (Car [2], Webb [16], Kubota [9], Effinger and Hayes [6, Theorem 1.9]);
  \item when \( p = \text{char}(F) > k \) and the degree of a polynomial \( a \in F[t] \) is sufficiently large, then \( a \) is a strict sum of at most \( k^22^{k+1} \) \( k \)th powers (Car [3], Effinger and Hayes [6]).
\end{enumerate}


We write \( q = p^a k' \) with \( \gcd(k', p) = 1 \) where \( p = \text{char}(F) \) as above. In this paper for the ring \( A = F[t] \) we prove:
Theorem 1.1. proof of (6) implies that $-k$-powers. This includes any field $F_q$ (22) for $1$. Statement of main results

Moreover, if $F$ is infinite, then

when

(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

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

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 $p \leq k$.

In fact in this paper, we replace the finite field $F$ to be any field $F$ such that $-1$ is a sum of $k$th 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 $k$th 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, $k \geq 2$, $F$ is a field such that $w_k(-1, F) < \infty$, i.e., $-1 \in F_k$ (e.g., $p = \text{char}(F) \neq 0$ or $k$ is odd), and $A = F[t]$.

If $\text{char}(F) = p \neq 0$ and $\gcd(p, k) \neq 1$, we can write $k = k'p^\alpha$ with $\alpha \geq 1$ and $\gcd(k', p) = 1$. Then $F_{p^{\alpha}}$ consists of $p^\alpha$-powers in $F$, $F_k = (F_{p^{\alpha}})_K = (F_{k'})_{p^{\alpha}}$. $A_k$ consists of $p^\alpha$-powers of polynomials in $A_{k'}$, $w_k(F) = w_k'(A)$, $w_k(A_k) = w_k'A$, the strict sums of $k$th powers in $A$ are the $p^\alpha$th 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 $\text{char}(F) = 0$, $w_k(F) \leq w_k(A) \leq k^2(k - 1)(w_k(-1, F) + 1)/4$;

(ii) when $\text{char}(F) \neq 0$, $w_k(F) \leq k^2(k - 1)/2$ and

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

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

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

(iv) every polynomial in $A$ which is a strict sum of $k$th powers is the strict sum of at most $k^6$ $k$th powers;

(v) every polynomial in $A_k$ of degree $\geq k^3 - 1$ is the strict sum of at most $k^3/2$ $k$th powers.

Let $F^*$ denote the multiplicative group of the field $F$ and $F^{*k}$ the subgroup of the $k$th 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) $w_k(F) \leq K$.

Moreover, if $F$ is infinite, then:

(ii) $F_k = F$ and $w_k(F) \leq 1 + w_k(-1, F, )$;

(iii) $A_k = A$ and $w_k(A) \leq k(K + 1)/2$. 

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

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

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

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

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

Using (4) and the fact that \( \text{card}(F_k) \geq 1 + (q - 1)/k \), 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 \( \text{char}(F) \neq 0 \), \( \text{card}(F) \geq k^4 \), and \( F \) is algebraic over its prime subfield \( F_0 \). Then:

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

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

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

2. *Proof of Theorem 1.2*

(i) Set \( H = F^{sk} \cap F_k \). If \( a \in A_k \) and \( w_k(a) > 1 \), then dropping a \( k \)th power in a representation of \( a \) as the sum of \( w_k(a, A) \) \( k \)th 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 \( aH, w_k(F) \leq K \). 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 \( w_k(F) \leq 1 + w_k(1, F) \)). So Theorem 1.2(i) is proved.

(ii) The fact that \( w_k \) takes \( F_k^* \) all values between 1 and \( w_k(A) \) implies that increasing if necessary, we can make them 1, 2, ..., \( K \) 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 \( (F_k)^*/(F_k \cap F^{sk}) \). Then for any nonzero \( a \in F_k \),

\[
\sum_{i=1}^{K} w_k(af_i, F) \leq K(K + 1)/2.
\]
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 $a_1, \ldots, a_k \in F$ and, using Vandermonde’s determinants, write

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

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 $k$th powers, with the total number of $k$th powers is at most $k(K + 1)/2$. So $w_k(ft, A) \leq k(K + 1)/2$. Since $ft$ here can be replaced by any $a \in A = F[t]$, we obtain that $w_k(a) \leq k(K + 1)/2$ for every $a \in A$, i.e., $w_k(A) \leq k(K + 1)/2$.

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 $d \geq 1$ 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 $\deg(a - x^k) \leq d(k - d) - 1$.

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

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

Similarly we find $x_{d-2}, \ldots, x_0$. □

Corollary 3.2. Under the conditions of Lemma 3.1, let $d'$ be an integer such that $dk - d \leq d'k \leq dk - 1$. 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 $a - t^{dk}$. □

For any rational number $x$, we denote by $\lfloor x \rfloor$ the least integer $s$ satisfying $x \leq s$. For any integer $d \geq 1$, we define $f(d) = \lfloor d(k - 1)/k \rfloor$. Inductively, we define, $f^s(d) = f\left(f^{d-1}(d)\right)$. Note that $f(d) < d$ for $d \geq k$ and $f(d) = d$ when $d \leq k - 1$.

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

$$f^s(d) \leq d((k-1)/k)^s + (k-1)(1+(k-1)/k+\cdots+(k-1)/k^{s-1})/k.$$

Proof. It is easy by induction on $s$ using that

$$f(d) = \lfloor d(k-1)/k \rfloor \leq d(k-1)/k + (k-1)/k.$$ □

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

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

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

$$1 + (k-1)/k + \left(\frac{(k-1)/k}{k}\right)^2 + \left(\frac{(k-1)/k}{k}\right)^3 + \cdots = k.$$ □
Proposition 3.5. Let \( a \in F[t] \) be a polynomial of degree \( D \geq k^4 - k^2 - k + 1 \) 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 \( \leq d \) each such that \( \deg(a - \sum d_i^k) < d \).

Proof. Note that \( d \geq k(k^2 - 1) \). 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 \( i \leq m \). 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 \( x_i \) \( (m + 1 = w_k(F) + 1 \leq i \leq m + s = n) \) such that \( \deg(x_i) \leq d \) and \( \deg(b - \sum \text{ deg}(x_i^k)) \leq \text{deg}(d) \).

By Corollary 3.4,
\[
f^s(d) < d/e^s/k + k - 1 \leq d/(k + 1) + k - 1 \leq d/k.
\]
since \( d \geq k(k^2 - 1) \). So
\[
\deg\left(a - \sum_{i=1}^{n} x_i^k\right) \leq \text{deg}(d) < d. \quad \Box
\]

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
\[
\sum_{i=1}^{k} d_i (d_0 t + a_i)^k = t
\]
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].) \( \Box \)

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 \( b \). \( \Box \)

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

Remark. In fact, Lemma 3.6 implies that \( A'_k = A' \) and \( w_k(A') \leq w_k(F[t]) \) for every \( F \)-algebra \( A' \) assuming that \( -1 \in F_k \) and card(\( F_k \)) \( \geq k \). 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. \( \Box \)

Proposition 3.8. Let \( a \in F[t] \) be a polynomial of degree \( D \geq k^4 - 2k^2 - k + 1 \) 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 \( \leq d \) each such that \( \deg(a - \sum d_i^k) < d \).
Proof. In view of Proposition 3.5 (using that $3 \ln(k) > \ln(k+1)$) we can assume that $D < k^4$, hence $d \leq k^3$.

We set $s = [3k \ln(k)]$. As in the proof of Proposition 3.5, we find $n = w_k(F) + s$ polynomials $x_i \in A$ with $\deg(x_i) \leq d$ such that $b = a - \sum_{i=1}^n x_i^k$ is a monic polynomial of degree $f^s(d) k$ and

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

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 $\deg(b - x_{n+1}^k) \leq k(k-2) \leq d/k$. \qed

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

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

Remark. When the $k$th powers in the multiplicative group of $F$ have a finite index $K$ (e.g., $\text{card}(F) = g < \infty$ in which case $K = \gcd(k, q - 1)$) then $w_k(F) \leq K$ 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

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

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

Therefore,

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

hence

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

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

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

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

where

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

and $c_0 \in F[y]$. 
We set \( h = \prod_{i=1}^{p/(r+1) - 1} a_i \). Then \( h = \text{lcm}(b_1, \ldots, b_k) \). Moreover,

\[
h/b_i = \prod_{j=k}^{p/(r+1) - 1} (a_i - a_j).
\]

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

\[
\sum_{i=0}^{k-1} (t+a_i)^k f h'/b'_i = kf h't + h'f c_0.
\]

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

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

for some \( f \in F^* \).

When \( F \) is infinite, \( kf h't + h'f c_0 \) 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, \( w_k(F) \leq k \leq k^2(k-1)/2 \).

Using that \( w_k(A/h'A) \leq k+1 \) (Vaserstein [13, Theorem 5]), we obtain that \( w_k(A) \leq k+k^2(k-1)/2 \) 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 \( D \geq kl = k[\log_p(k)] \) is the sum of \( k^2(k-1)/2 \) \( k \)th powers of degree \( \leq Dk + k(k-2)[\log_p(k)] \) 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 \( 1 \leq c \leq p-1 \) and \( kc \equiv K \mod p \). Set \( m(p-1) \) to be the sum of \( p \)-digits of \( kp(p-1)/K \).

Note that \( m \) is an integer and \( m < \log_p(kkp(p-1)/K) + 1 < \log_p(k) + 3 \).

Let \( X(m) \) denote the set of all linear forms \( y = c_1y_1 + \cdots + c_my_m \) in \( m \) variables \( y_i \) with coefficients \( c_i \) in the prime subfield \( F_0 \). Note that \( \text{card}(X(m)) = p^m < p(p-1)^2k/K \).

We have

\[
\sum_{y} (x + y)^{kc(p-1)/K} y = (kc(p-1)/K)xY(kc(p-1)/K, m)
\]

where \( Y(s, m) = \sum_{y \in X(m)} y^k \neq 0 \) (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 \( y_1 \) 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 \( p^mK \) \( k \)th powers while the right-hand side represents an arbitrary element in any \( F \)-algebra \( A \). In particular,

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

Assume now that \( F \) is finite. Then \( w_k(F) \leq k < p(p-1)^2k(\log_p(k) + 3) \). To bound \( w_k(A) \), we replace the variables in (4) by \( a_i^k \) where \( a_i \in F[z] \) have degrees \( \leq \log_p(k) + 1 \) 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
$kc(p-1)/K \leq k(p-1)^2/K$ and this number is less than the number $p^{[\log_p(k)+2]}/K$ of all $a_i^k$ with $a_i \in F[z]$ of degrees $\leq \log_p(k)+1$. Thus, we obtain an identity

$$
\sum_{i=1}^{p^m} (x+b_i)^{kc(p-1)/K}/b_i = (kc(p-1)/K)xb_0
$$

(6)

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

Now it is clear that the sums of $p^mMK$ $k$th powers contain a nonzero ideal $I$ of $A$. Using that $w_k(A/I) \leq k+1$, we obtain that $w_k(A) \leq k+1+p(p-1)^2(\log_p(k)+3)$. Moreover, the bounds on the degrees of $b_1$ in (6) give the following

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

(v) By Theorem 1.4(ii), we can assume that $\text{card}(F_k) < k$, hence $k > p = \text{char}(F)$. Let $a \in A$ and $D = \text{deg}(a) > k^3 \log_p(k)$. Let $\alpha_0$ be the degree $dk$ coefficient in $a$ (it is 0 if $D < dk$). We write $\theta(\alpha_0)$ as the sum of $m = w_k(F)$ $k$th powers $c_i^d$ in $F$ and set $x_i = c_i d$ for $i \leq m$. Then $b = a - \sum x_i^k$ is a monic polynomial of degree $dk$.

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

By Corollary 3.4,

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

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

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

(iv) By Theorem 1.4(iv), we can assume that $\text{card}(F_k) < k$, hence $k > p = \text{char}(F)$. Let $a \in A$ be a strict sum of $k$th powers and $D = \text{deg}(a)$. We want to prove that $a$ is the strict sum of $k^3 \log_p(K)$ $k$th powers.

By Theorem 1.4(v), we can assume that $D \leq k^4 \log_p(k) - 1$. Then we can write $a$ as a linear combination of at most $D \leq k^4 \log_p(k)$ $k$th powers each of degree $\leq D - k + 1$. Writing every coefficient in $F$ as the sum of $k$ $k$th powers, we obtain $a$ as the strict sum of at most $k^6$ $k$th powers.

References


