Portugal. Math. (N.S.)
Vol. 67, Fasc. 1, 2010, 13–56
DOI 10.4171/PM/1856

Portugaliae Mathematica

Sums of $(2^r + 1)$-th powers in the polynomial ring $\mathbb{F}_{2^m}[T]$

Mireille Car

(Communicated by Rui Loja Fernandes)

Abstract. Let F be a finite field with 2^m elements and let $k = 2^r + 1$. We study representations and strict representations of polynomials $M \in F[T]$ by sums of k-th powers. A representation

$$M = M_1^k + \cdots + M_s^k$$

of $M \in F[T]$ as a sum of k-th powers of polynomials is strict if $k \deg M_i < k + \deg M$.

Mathematics Subject Classification (2010). Primary 11T55; Secondary 11R58.
Keywords. Finite fields, polynomials, Waring's problem.

1. Introduction

Let F be a finite field of characteristic p with p^m elements and let $k > 1$ be an integer. The similarity between the ring $\mathbb{Z}$ of rational integers and the polynomial ring $F[T]$ had led to investigate an analogue of the Waring problem for $F[T]$, ([18], [10], [15], [4], [16], [6], [2], [11]). Roughly speaking, Waring's problem over $F[T]$ consists in representing a polynomial $M \in F[T]$ as a sum

$$M = M_1^k + \cdots + M_s^k \tag{1.1}$$

with $M_1, \ldots, M_s \in F[T]$. Some obstructions to that may occur which led to consider Waring's problem over the subring $\mathscr{S}(F, k)$ formed by the polynomials of $F[T]$ which are sums of k-th powers. Two variants of Waring's problem over $\mathscr{S}(F, k)$ have been considered. The unrestricted Waring's problem ([15], [16]), consists in proving the existence of an integer $w = w(p^m, k)$ with the property that whenever $M \in \mathscr{S}(F, k)$ and $s \geq w(p^m, k)$, the equation (1.1) is solvable. Without degree conditions in (1.1), the problem of representing M as sum (1.1) is close to the so called easy Waring's problem for $\mathbb{Z}$. In order to have a problem close to the non easy Waring's problem, the degree conditions

$$\deg M_i \leq n \tag{1.2}$$

are required with n defined by the condition

$$k(n-1) < \deg M \leq kn. \tag{1.3}$$

With such degree conditions, the representation (1.1) is *strict* in opposition to representations without degree conditions. For the strict Waring's problem, analogue of the classical numbers $g_{\mathbb{N}}(k)$ and $G_{\mathbb{N}}(k)$ have been defined as follows. Let $g(p^m, k)$ respectively $G(p^m, k)$ denote the least integer s, if it exists, such that every polynomial $M \in \mathscr{S}(F, k)$, respectively every polynomial $M \in \mathscr{S}(F, k)$ of sufficiently large degree, may be written as a sum (1.1) satisfying the degree conditions (1.2) and (1.3). Otherwise, $g(p^m, k)$ respectively $G(p^m, k)$ is equal to ∞. This notation is possible since these numbers only depend on p^m and k. Waring's problem consists in determining or, at least, bounding the numbers $g(p^m, k)$ and $G(p^m, k)$. In [11], it was announced without proof that

if k and p^m are such that $p^m \geq 9k^6$, then $G(p^m, k) \leq k \log k - \frac{1}{2} \log k + 7$.

Proposition 4.5 in [1] and Corollary 3.8 below give examples of pairs $\{k, p^m\}$ for which these bounds are not valid. Bounds for $g(p^m, k)$ and $G(p^m, k)$ were given in [1] where the author described a process intoduced in [6] and performed in [2] to deal with the polynomial Waring's problem for cubes.

Some notations and definitions are necessary before stating the main results proved in [1].

If every $a \in F$ is a sum of k-th powers, the field F is called a Waring field for the exponent k or briefly, a k-Waring field. If F is a k-Waring field, let $\ell(p^m, k)$ denote the the least integer ℓ such that every element of F is the sum of ℓ k-th powers. Let $\lambda(p^m, k)$ denote the least integer s such that -1 is the sum of s k-th powers. Let $\Delta(p^m, k) = \gcd(p^m - 1, k)$.

Let $v(p^m, k)$ denote the least integer v, if it exists, such that T may be written as a sum $(a_1 T + b_1)^k + \cdots + (a_v T + b_v)^k$ with $a_i, b_i \in F$. Otherwise, let $v(p^m, k) = \infty$. If $v(p^m, k)$ is finite, every $P \in F[T]$ may be written as a sum

$$P = (a_1 P + b_1)^k + \cdots + (a_{v(p^m,k)} P + b_{v(p^m,k)})^k$$

so that $\mathscr{S}(F, k) = F[T]$ and F is a k-Waring field.

The two following theorems were proved in [1].

Theorem 1.1. *Let $k \geq 3$ be coprime with p. Let F be a k-Waring field with p^m elements and characteristic p. Suppose that $p^m > k$. Then $\mathscr{S}(F,k) = F[T]$,*

$$v(p^m,k) \leq k/\Delta(p^m,k) + \ell(p^m,k)\big(k - k/\Delta(p^m,k)\big), \tag{1.4}$$

$$G(p^m,k) \leq \frac{\log k}{\log\big(k/(k-1)\big)} + \max\big(\ell(p^m m,k), \lambda(p^m,k)+1\big) + v(p^m,k), \tag{1.5}$$

so that

$$\begin{aligned} G(p^m,k) &\leq \frac{\log k}{\log\big(k/(k-1)\big)} + k\ell(p^m,k) + 2 \\ &\leq k\log(k-1) + k\ell(p^m,k) + 3. \end{aligned} \tag{1.6}$$

Theorem 1.2. *Let $k \geq 3$ be coprime with p. Let F be a k-Waring field with p^m elements and characteristic p. If $p > k$, then*

$$g(p^m,k) \leq \ell(p^m,k)(k^3 - 2k^2 - k + 1). \tag{1.7}$$

The same result remains true in the case where $k = hp^v - 1 < p^m$, for some positive integers v and $h \leq p$.

The case of exponent $k = p^r + 1$ is not covered by these theorems. The aim of this paper is the study of Waring's problem in the case where $p = 2$, $k = 2^r + 1$. In this case, it is posible to compute the exact value of $v(2^m, 2^r+1)$. This yields an improvement for the bounds given in [1], see Corollary 3.5 below. The case of odd characteristic p is more difficult and will be studied further. It will appear that the numbers $g(p^m,k)$ and $G(p^m,k)$ are not sufficient to describe every possible case. Thus, we introduce new parameters.

From now on, F is a finite field with 2^m elements.

Let $\mathscr{S}^*(F,k)$ denote the set of polynomials in $F[T]$ which are strict sums of k-th powers. Let $g^*(2^m,k)$, respectively $G^*(2^m,k)$, denote the least integer s, if it exists, such that every polynomial $M \in \mathscr{S}^*(F,k)$, respectively, every polynomial $M \in \mathscr{S}^*(F,k)$ of sufficiently large degree, may be written as a strict sum

$$M = M_1^k + \cdots + M_s^k.$$

The main results proved in this work are summarized in the following theorems.

Theorem 1.3. *Suppose that $k = 2^r + 1 > 3$.*

(I) *If $m/\gcd(m,r) \geq 3$, then the set $\mathscr{S}(F,k)$ is equal to the whole ring $F[T]$,*

$$\mathscr{S}^*(F,k) = \mathscr{A}_0 \cup \mathscr{A}_\infty \cup \Big(\bigcup_{N=1}^{k-3} \mathscr{A}_N\Big),$$

where

$$\mathscr{A}_0 = F, \qquad \mathscr{A}_\infty = \{A \in F[T] \mid \deg A > k(k-3)\},$$

$$\mathscr{A}_N = \left\{A \in F[T] \mid A = \sum_{n=0}^{N}\sum_{i=0}^{N} x_{n,i} T^{i+n2^r}\right\}$$

with $x_{n,i} \in F$.

(II) *If m divides r, then*

$$\mathscr{S}^*(F,k) = \mathscr{S}(F,k) = \{A \in F[T] \mid A^{2^r} + A \equiv 0 \ (\mathrm{mod}\ T^{4^r} + T)\}.$$

(III) *If* $m/\gcd(m,r) = 2$, *then*

$$\mathscr{S}(F,k) = \{A \in F[T] \mid A^{2^r} + A \equiv 0 \ (\mathrm{mod}\ T^{4^r} + T)\}$$

and $\mathscr{S}^*(F,k)$ *is the set formed by the* $A \in \mathscr{S}(F,k)$ *such that either* $\deg A$ *is not multiple of* k, *or* $\deg A$ *is multiple of* k *and the leading coefficient of* A *is in the subfield of* F *of order* $2^{\gcd(m,r)}$.

This theorem is a consequence of Corollaries 3.3, 5.2 and 5.6 below.

Theorem 1.4. *Suppose that* $k = 2^r + 1 > 5$.

(I) (i) *If* $m/\gcd(m,r) \geq 3$, *then* $g(2^m,k) = \infty$.

(ii) *If* $m/\gcd(m,r) \geq 3$ *and* $m/\gcd(m,r) \neq 4$, *then*

$$G(2^m,k) = G^*(2^m,k) \leq 3k+2,$$

(iii) *if* $m/\gcd(m,r) = 4$, *then*

$$G(2^m,k) = G^*(2^m,k) \leq 3k+3,$$

(iv) *if* $m/\gcd(m,r)$ *is odd, then*

$$g^*(2^m,k) \leq 6k-6,$$

(v) *if* $m/\gcd(m,r)$ *is even and* > 4, *then*

$$g^*(2^m,k) \leq 6k-5,$$

(vi) *if* $m/\gcd(m,r) = 4$, *then*

$$g^*(2^m,k) \leq 7k-7.$$

(AutoPDF V7 28/1/10 12:48) EMS (170×240mm) Tmath J-2232 PMS, 67:1 (idp) PMU:(KN/)7/1/2010 AC1: WSL 22/01/2010 pp. 13–56 2232_67-1_02 (p. 16)

(II) *If m divides r, then*

$$G(2^m,k)=G^*(2^m,k)\le 3k-3,\qquad g(2^m,k)=g^*(2^m,k)\le 3k-3.$$

(III) *If $m/\gcd(m,r)=2$, then*

$$G(2^m,k)=g(2^m,k)=\infty,\qquad G^*(2^m,k)\le g^*(2^m,k)\le 2k.$$

This theorem is a consequence of Corollary 5.6 below. It shows that the analogy with the rational integers does not work completely since the following bounds hold for large exponents k ([19], [5], [9], ch. 21):

$$G_{\mathbb{N}}(k)\le k\big(\log k+\log(\log k)+O(1)\big);$$
$$2^k+[(3/2)^k]-2\le g_{\mathbb{N}}(k)\le 2^k+[(3/2)^k]+[(4/3)^k]-2.$$

The case $k=3$ is covered by Corollaries 3.3, 3.5, 5.2 and Proposition 5.5 below. Results given by Corollaries 3.3, 3.5, 5.2 and Proposition 5.5 do not improve those results that were already proved in [7] or [8]. In the case $k=5$, we show:

Theorem 1.5. (I) (i) *If $m/\gcd(m,2)\ge 3$, then $g(2^m,5)=\infty$.*

(ii) *If $m/\gcd(m,2)\ge 3$ and $m/\gcd(m,2)\ne 4$, then*

$$G(2^m,5)=G^*(2^m,5)\le 12,$$

(iii) *if $m/\gcd(m,2)$ is odd and >1, then*

$$g(2^m,5)=\infty,\qquad g^*(2^m,5)\le 24,$$

(iv) *if $m/\gcd(m,2)$ is even and >4, then*

$$g^*(2^m,5)\le 25,$$

(v) *if $m=8$, then*

$$g^*(2^m,5)\le 28,\qquad G(2^m,5)=G^*(2^m,5)\le 13.$$

(II) *If $m=4$, then*

$$G(2^m,5)=g(2^m,5)=\infty,\qquad G^*(2^m,5)\le g^*(2^m,5)\le 10.$$

(III) *If $m=1$ or 2, then*

$$G(2^m,5)=G^*(2^m,5),\qquad g(2^m,5)=g^*(2^m,5)\le 12.$$

This theorem is a consequence of Corollaries 3.5, and 5.6 below. For the positive integers, the corresponding bounds are $G_{\mathbb{N}}(5) \le 17$, $g_{\mathbb{N}}(5) \le 37$ ([17], [3]).

The paper is organized as follows. In order to get the exact value of $v(2^m, k)$ we have to prove that some algebraic equations have solutions in F. This is done in Section 2. In Section 3 we compute the numbers $v(2^m, k)$. Bounds for the numbers $G(2^m, k)$ follow. In Section 4 we prove some identities involving a caracterization of strict sums of small degrees. In Section 5 we describe a descent process and we conclude the proof.

We fix an algebraic closure $\bar{F}$ of the field F and for any positive integer n we denote by $\mathbb{F}_{2^n}$ the subfield of $\bar{F}$ with 2^n elements, so that $F = \mathbb{F}_{2^m}$. Our proofs often use the following facts:

The field F contains exactly $\Delta(2^m, k) = \gcd(2^m - 1, k) = \gcd(2^m - 1, 2^r + 1)$ k-th roots of 1. We introduce the notations

$$Q = 2^r = k - 1, \qquad q = 2^{\gcd(m,r)}, \tag{1.8}$$

$$d = \gcd(m, r), \tag{1.9}$$

so that

$$q = 2^d. \tag{1.10}$$

If x is a real number, we denote by $[x]$ its integral part and by $\lceil x \rceil$ the least integer $n \ge x$.

Since $\gcd(q+1, q-1) = 1$, every $x \in \mathbb{F}_q$ is a $(q+1)$-th power.

2. Equations

Since a k-th power in F is a $\gcd(2^m - 1, k)$-th power, we begin this section by computing $\Delta = \gcd(2^m - 1, k)$. We continue by studying a sum of characters related to sums of Δ-th powers.

2.1. The greatest common divisor. I think that the results contained in the following proposition are well known, althought I am unable to give any reference for them, Lemma 4 in [12] only giving incomplete results. The proof given here differs from the original one. Its present simplified form is due to the referee.

Proposition 2.1. (i) *We have*

$$\gcd(2^m - 1, 2^r - 1) = 2^d - 1. \tag{2.1}$$

(ii) *The numbers $2^m - 1$ and $2^r + 1$ are not coprime if and only if m/d is even and, in that case,*

$$\gcd(2^m - 1, 2^r + 1) = 2^d + 1. \tag{2.2}$$

Proof. (i) Let a and b be positive integers with $a \geq b$. If $a = bc + \rho$ with $0 \leq \rho < b$, then

$$2^a - 2^\rho = 2^\rho(2^{bc} - 1) = 2^\rho(2^{b(c-1)} + \cdots + 2^b + 1)(2^b - 1),$$

so that

$$2^a - 1 = (2^b - 1)C + 2^\rho - 1,$$

with C a positive integer and $2^\rho - 1 < 2^b - 1$. The euclidean algorithm for $\gcd(2^m - 1, 2^r - 1)$ exactly mimics that for $\gcd(m, r)$. Thus,

$$\gcd(2^m - 1, 2^r - 1) = 2^{\gcd(m,r)} - 1.$$

(ii) Since $\gcd(2^r + 1, 2^r - 1) = 1$, we have

$$\gcd(2^m - 1, 2^{2r} - 1) = \gcd(2^m - 1, 2^r + 1)\gcd(2^m - 1, 2^r - 1).$$

From part (i),

$$\gcd(2^m - 1, 2^r + 1) = \frac{2^{\gcd(m,2r)} - 1}{2^{\gcd(m,r)} - 1}.$$

Let v_2 denote the 2-adic valuation. We have

$$\gcd(m, 2r) = \begin{cases} \gcd(m,r) & \text{if } v_2(m) \leq v_2(r), \\ 2\gcd(m,r) & \text{if } v_2(m) > v_2(r). \end{cases}$$

Therefore, $\gcd(2^m - 1, 2^r + 1) \neq 1$ if and only if $m/\gcd(m,r)$ is even, and in that case,

$$\gcd(2^m - 1, 2^r + 1) = 2^{\gcd(m,r)} + 1.$$ □

2.2. The system $\mathscr{E}(u, v, a, b)$

Lemma 2.2. *Let $(u, v) \in F^2$ be such that $uv \neq 0$ and $u^{Q^2-1} \neq v^{Q^2-1}$. For every ordered pair $(a, b) \in F^2$, the system $\mathscr{E}(u, v, a, b)$:*

$$\begin{cases} a = u^Q x + v^Q y, \\ b = u x^Q + v y^Q \end{cases} \tag{2.3}$$

has a unique solution in F^2.

Proof. Immediate. □

2.3. Exponential sums. In this subsection, we suppose that m/d is even, so that $\mathbb{F}_{q^2} \subset F$. Let

$$n = m/2d, \tag{2.4}$$

so that

$$F = \mathbb{F}_{q^{2n}}. \tag{2.5}$$

Let $\mathrm{tr} : F \to \mathbb{F}_2$ denote the absolute trace on F and let ψ be the character of the additive group of F defined by

$$\psi(x) = (-1)^{\mathrm{tr}(x)}. \tag{2.6}$$

Then ψ is not trivial. For a and b elements of F, let

$$\sigma(a,b) = \sum_{x \in F} \psi(ax^q + bx). \tag{2.7}$$

Proposition 2.3. *Let $a, b \in F$. Then*
(i) $\sigma(a,b) \in \{0, 2^m\}$,
(ii) $\sigma(a,b) = 2^m$ *if and only if* $a = b^q$.

Proof. Since q is a power of 2, the map $\gamma : x \mapsto (ax^q + bx)$ is additive and $\psi \circ \gamma$ is a character of the additive group of F. This proves (i). Let $b \in F$. Then

$$\sum_{a \in F} \sigma(a,b) = \sum_{a \in F} \sum_{x \in F} \psi(ax^q + bx).$$

Inverting the order of summation gives

$$\sum_{a \in F} \sigma(a,b) = \sum_{x \in F} \psi(bx) \sum_{a \in F} \psi(ax^q).$$

Since ψ is not trivial, the last inner sum is 0 if $x \neq 0$ and $|F| = 2^m$ if $x = 0$. Thus,

$$\sum_{a \in F} \sigma(a,b) = 2^m.$$

In view of the part (i), there exists one and only one $a \in F$ such that $\sigma(a,b) = 2^m$. For every $x \in F$, $\mathrm{tr}\big((bx)^q\big) = \mathrm{tr}\big((bx)^{2^d}\big) = \mathrm{tr}(bx)$ so that $\psi(b^q x^q + bx) = 1$. Thus, $\sigma(b^q, b) = 2^m$ and b^q is the unique $a \in F$ such that $\sigma(a,b) = |F|$. □

Let B denote the set of non-zero k-th powers in F. From Proposition 2.1 and (1.10),

$$|B| = \frac{2^m - 1}{q+1}. \tag{2.8}$$

For $t \in F$, let

$$f(t) = \sum_{x \in F} \psi(tx^{q+1}). \tag{2.9}$$

Proposition 2.4. (I) *We have* $f(0) = 2^m$.

(II) *Let* $t \in F^*$.

(i) *If* $t \in B$, *then* $f(t) = f(1)$ *and* $f(t)^2 = 2^m q^2$.

(ii) *If* $t \notin B$, *then* $f(t)^2 = 2^m$.

(iii) *If* $t \notin B$, *then* $qf(t) + f(1) = 0$.

Proof. (I) is obvious. Let $t \in F^*$. Then

$$f(t)^2 = \sum_{y \in F} \sum_{x \in F} \psi\big(t\big(y^{q+1} + (x+y)^{q+1}\big)\big) = \sum_{x \in F} \psi(tx^{q+1}) \sum_{y \in F} \psi\big(t(x^q y + xy^q)\big).$$

From the previous proposition, the inner sum is 0 or 2^m and is equal to 2^m if and only if $tx = t^q x^{q^2}$. The inner sum is equal to 2^m if and only if $x \in X(t)$, where

$$X(t) = \{x \in F \mid x = t^{q-1} x^{q^2}\}.$$

If t is not a $(q+1)$-th power, then $X(t) = \{0\}$ and $f(t)^2 = 2^m$, proving (II-ii). Suppose that $t = u^{q+1}$ with $u \in F$. The map $x \mapsto ux$ is a permutation of the field F. Thus,

$$f(t) = \sum_{x \in F} \psi\big((ux)^{q+1}\big) = \sum_{y \in F} \psi(y^{q+1}) = f(1).$$

Let $x \in F^*$. Then

$$x \in X(1) \Leftrightarrow 1 = x^{q^2-1} \Leftrightarrow x \in (\mathbb{F}_{q^2})^*.$$

There are exactly (q^2-1) non-zero elements $x \in X(1)$ and if x is one of them, then $x^{q+1} \in \mathbb{F}_q$ so that $\mathrm{tr}_{\mathbb{F}_{q^2}|\mathbb{F}_q}(x^{q+1}) = 0$. Thus, $\mathrm{tr}(x^{q+1}) = 0$ and $\psi(x^{q+1}) = 1$. Therefore, if $t \in B$, then

(AutoPDF V7 28/1/10 12:48) EMS (170×240mm) Tmath J-2232 PMS, 67:1 (idp) PMU:(KN/)7/1/2010 AC1: WSL 22/01/2010 pp. 13–56 2232_67-1_02 (p. 21)

$$f(t)^2 = q^2 2^m.$$

This proves (II)(i).

Let B' denote the set of non $(q+1)$-th powers in F. Then by (2.8),

$$|B'| = \frac{q(2^m - 1)}{q+1}. \tag{1}$$

If $t \in B$, then $f(t) = f(1)$. Let $c \in B'$. If $t \in B'$, then $|f(t)| = |f(c)|$. Set $f(t) = \varepsilon_t f(c)$. Observe that $\varepsilon_t = \pm 1$. We compute the sum

$$\Sigma = \sum_{t \in F^*} f(t)$$

by two different ways. Firstly,

$$\Sigma = \sum_{t \in F} f(t) - 2^m = \sum_{t \in F} \sum_{x \in F} \psi(tx^{q+1}) - 2^m.$$

Inverting the order of summation gives

$$\Sigma = 0. \tag{2}$$

On the other hand,

$$\Sigma = \sum_{t \in B} f(t) + \sum_{t \in B'} f(t).$$

Thus,

$$\Sigma = |B| f(1) + f(c) \sum_{t \in B'} \varepsilon_t. \tag{3}$$

By (2.8), (2) and (3),

$$\left| f(c) \sum_{t \in B'} \varepsilon_t \right| = \frac{2^m - 1}{q+1} |f(1)|.$$

From (II)(i), (II)(ii) and (1),

$$\left| \sum_{t \in B'} \varepsilon_t \right| = \frac{q(2^m - 1)}{q+1} = |B'|.$$

Hence, for each $t \in B'$ $\varepsilon_t = \varepsilon_c$ and $f(t) = f(c)$. From (2) and (3),

$$\frac{2^m-1}{q+1}f(1) + \frac{q(2^m-1)}{q+1}f(c) = 0.$$

Therefore, for every $t \in B'$,

$$\frac{2^m-1}{q+1}f(1) + \frac{q(2^m-1)}{q+1}f(t) = 0,$$

proving (II)(iii). □

For our purpose a knowledge of the values of $f(t)$ for all t is not necessary. It is sufficient to know the value of $f(1)$ in the case where $|F| = q^4$. This is done below. The proof provides the value of $f(1)$ in all cases. We have to introduce some new notations.

Let $t_{2,1}$ denote the trace from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. For $i \in \{1, 2, 2n\}$ let τ_i denote the absolute trace of $\mathbb{F}_{q^i}$. For $i \in \{1, 2, 2n\}$ let ψ_i be the character of the additive group of the field $\mathbb{F}_{q^i}$ defined by

$$\psi_i(x) = (-1)^{\tau_i(x)}. \tag{2.10}$$

Observe that the characters ψ_i are not trivial and

$$\tau_2 = \tau_1 \circ t_{2,1}, \qquad \mathrm{tr} = \tau_{2n}, \tag{2.11}$$

so that

$$\psi = \psi_{2n}. \tag{2.12}$$

For $i = 1, 2, 2n$, let

$$S_i = \sum_{x \in \mathbb{F}_{q^i}} \psi_i(x^{q+1}). \tag{2.13}$$

Note that

$$f(1) = S_{2n}. \tag{2.14}$$

Proposition 2.5. *We have*

$$S_1 = 0 \tag{2.15}$$

(AutoPDF V7 28/1/10 12:48) EMS (170×240mm) Tmath J-2232 PMS, 67:1 (idp) PMU:(KN/)7/1/2010 AC1: WSL 22/01/2010 pp. 13–56 2232_67-1_02 (p. 23)

and

$$S_{2n} = (-1)^{n+1} q^{n+1}. \tag{2.16}$$

for $n \geq 1$,

Proof. (I) Since $q-1$ and $q+1$ are coprime, the map $x \mapsto x^{q+1}$ is a permutation of the field $\mathbb{F}_q$. Since ψ_1 is not trivial,

$$S_1 = \sum_{x \in \mathbb{F}_q} \psi_1(x) = 0.$$

(II) If $x \in \mathbb{F}_{q^2}$, then $x^{q+1} \in \mathbb{F}_q$. Moreover, if z is a non-zero element in $\mathbb{F}_q$, there are exactly $(q+1)$ elements $x \in \mathbb{F}_{q^2}$ solutions of the equation $x^{q+1} = z$. Thus,

$$S_2 = 1 + \sum_{\substack{x \in \mathbb{F}_{q^2} \\ x \neq 0}} \psi_2(x^{q+1}) = 1 + (q+1) \sum_{\substack{y \in \mathbb{F}_q \\ y \neq 0}} \psi_2(y) = -q + (q+1) \sum_{y \in \mathbb{F}_q} \psi_2(y).$$

With (2.10) and (2.11) we obtain

$$S_2 = -q + (q+1) \sum_{y \in \mathbb{F}_q} (-1)^{\tau_2(y)} = -q + (q+1) \sum_{y \in \mathbb{F}_q} (-1)^{\tau_1(t_{2,1}(y))} = q^2.$$

This proves (2.16) in the case where $n = 1$.

(III) From [13], formulas 4.13, 4.14, p. 119, there exist algebraic integers $\lambda_1, \dots, \lambda_q$ of modulus q such that

$$S_{2n} = -\sum_{i=1}^{q} \lambda_i^n.$$

We have $S_2 = q^2$. Thus, for each index i, $\lambda_i = -q$. Therefore,

$$S_{2n} = -q(-q)^n = (-1)^{n+1} q^{n+1}. \qquad \square$$

2.4. Sums of *k*-th powers in *F*. Let i be a positive integer. For $a \in F$, let $v_i(a)$ denote the number of solutions $(x_1, \dots, x_i) \in F^i$ of the equation

$$a = x_1^k + \cdots + x_i^k. \tag{2.17}$$

Proposition 2.6. *Suppose that* m/d *odd. Then, for any positive integer* i *and for any* $a \in F$,

$$v_i(a) = 2^{m(i-1)}.$$

Proof. From Proposition 2.1, $\gcd(k, |F|-1) = 1$, so that the map $a \mapsto a^k$ is a permutation of F. □

Proposition 2.7. *Suppose m/d even. Then*

$$v_1(0) = 1, \qquad v_2(0) = (q+1)2^m - q, \qquad v_3(0) = 2^{2m} + f(1)(q-1)(2^m-1)$$

and for $a \in F^*$ we have

$$v_1(a) = \begin{cases} q+1 & \text{if } a \in B, \\ 0 & \text{if } a \notin B, \end{cases}$$
$$v_2(a) = 2^m - q + (q-1)f(a),$$
$$v_3(a) = 2^{2m} - 2^m - (q-1)f(1) + (q-1)f(1)f(a) + 2^m v_1(a).$$

Proof. Observe that a k-th power in F is a $(q+1)$-th power. Let $a \in F^*$. If $a \notin B$, then $v_1(a) = 0$. If $a \in B$, then $v_1(a)$ is equal to the number of $(q+1)$-th roots of 1 in F, that is, $v_1(a) = q+1$. Let $i = 1, 2, 3$. By orthogonality,

$$v_i(a) = \sum_{x \in F} \frac{1}{|F|} \sum_{t \in F} \psi\big(t(a + x_1^{q+1} + \cdots + x_i^{q+1})\big).$$

Thus, after inverting the order of summation, we get with (2.9),

$$2^m v_i(a) = \sum_{t \in F} \psi(at) f(t)^i. \tag{1}$$

Let $i = 2, 3$. From Proposition 2.4,

$$2^m v_i(a) = 2^{im} + q^2 2^m \sum_{t \in B} \psi(at) f(t)^{i-2} + 2^m \sum_{\substack{t \in F^* \\ t \notin B}} \psi(at) f(t)^{i-2}.$$

Hence,

$$v_i(a) = 2^{(i-1)m} - 2^{(i-2)m} + (q^2-1) \sum_{t \in B} \psi(at) f(t)^{i-2} + \sum_{t \in F} \psi(at) f(t)^{i-2}. \tag{2}$$

Suppose that $i = 2$. Then with (2.8),

$$v_2(0) = 2^m - 1 + \frac{(2^m-1)(q^2-1)}{q+1} + 2^m = q2^m + 2^m - q.$$

Let $a \in F^*$. From (2),

$$v_2(a) = 2^m - 1 + (q^2 - 1) \sum_{t \in B} \psi(at).$$

If $t \in B$, the equation $t = u^{q+1}$ has $q + 1$ solutions. Thus,

$$v_2(a) = 2^m - 1 + (q - 1) \sum_{u \in F^*} \psi(au^{q+1}) = 2^m - q + (q - 1) \sum_{u \in F} \psi(au^{q+1}),$$

so that

$$v_2(a) = 2^m - q + (q - 1) f(a).$$

Suppose that $i = 3$. Then from (2) and (1),

$$v_3(a) = 2^{2m} - 2^m + (q^2 - 1) \sum_{t \in B} \psi(at) f(t) + 2^m v_1(a),$$

so that

$$v_3(a) = 2^{2m} - 2^m + (q - 1) \sum_{u \in F^*} \psi(au^{q+1}) f(u^{q+1}) + 2^m v_1(a).$$

From Proposition 2.4,

$$v_3(a) = 2^{2m} - 2^m + (q - 1) f(1) \sum_{u \in F^*} \psi(au^{q+1}) + 2^m v_1(a),$$

so that with (2.6),

$$v_3(a) = 2^{2m} - 2^m - (q - 1) f(1) + (q - 1) f(1) f(a) + 2^m v_1(a). \qquad \square$$

The following proposition completes Small's theorem ([14]), which states that if $m > 4r$, then F is a k-Waring field with $\ell(2^m, k) \leq 2$.

Proposition 2.8. (I) *F is a Waring field for the exponent k if and only if* $\frac{m}{d} \neq 2$.
(II) *If* $\frac{m}{d}$ *is odd, then* $\ell(2^m, k) = 1$.
(III) *If* $\frac{m}{d}$ *is even and if* $\frac{m}{d} \geq 4$, *then* $\ell(2^m, k) = 2$.
(IV) *If* $\frac{m}{d} = 2$, *every* $x \in F$ *which is a sum of k-th powers is a k-th power.*

Proof. From Proposition 2.1, if $\frac{m}{d}$ is odd, then $\Delta(2^m,k)=1$ and F is a k-Waring field with $\ell(2^m,k)=1$. Now we suppose $\frac{m}{d}$ even. Then $\Delta(2^m,k)=1+2^d$. Let $n=m/2d$. Since $\Delta(2^m,k)>1$, we have $\ell(2^m,k)\geq 2$. We prove that, with the exception $n=1$, F is a k-Waring field with $\ell(2^m,k)\leq 2$. Let $a\in F$ be different from a k-th power. From Propositions 2.7 and 2.4,

$$v_2(a)=2^m-q+(q-1)f(a)\geq 2^m-q-(q-1)2^{m/2}=q^{2n}-q-q^{n+1}+q^n.$$

If $n>1$, then $v_2(a)>0$, so that a is the sum of two k-th powers. Thus, if $a\in F$, either a is a k-th power, or a is a sum of two k-th powers. Hence, $\ell(2^m,k)=\ell(F,k)\leq 2$.

Now suppose that $F=\mathbb{F}_{q^2}$. If $x\in F$ is a $(q+1)$-th power, say $x=y^{q+1}$ with $y\in F$. Then $x^q=x$ and $x\in\mathbb{F}_q$. If $a\in F$ is a sum of $(q+1)$-th powers, then $a\in\mathbb{F}_q$ and a is a $(q+1)$-th power. □

Proposition 2.9. *For $a\in F$, let $N_3(a)$ denote the number of $(x,y,z)\in F^3$ such that*

$$\begin{cases} x^k+y^k+z^k=a, & (\mathrm{e}_1)\\ xy\neq 0, & (\mathrm{e}_2)\\ x^{Q^2-1}\neq y^{Q^2-1}. & (\mathrm{e}_3)\end{cases} \qquad (\mathscr{F}(a))$$

(I) *Suppose that m/d odd. Then, for $a\in F$, we have*

$$N_3(a)=(2^m-1)(2^m-q).$$

(II) *Suppose that m/d even. Then*

$$N_3(0)=2^{2m}-2^m(q^3+1)+q^3+(q-1)(2^m-1)f(1),$$

and for $a\in F^*$, we have

$$N_3(a)=\begin{cases} 2^{2m}+2^m(q^3-3q^2-1)+2q^3-(q-1)(q^2-q+1)f(1) & \text{if } a\in B,\\ 2^{2m}-2^m(2q^2-2q+1)+q^3-q^2+(q-1)(q-2)f(1) & \text{if } a\notin B,\end{cases}$$

where f is as in (2.9).

Proof. (I) Suppose that m/d odd. From Proposition 2.1, $\gcd(k,2^m-1)=1$, so that the map $x\mapsto x^k$ is bijective. Thus, for each pair $(x,y)\in F^2$ satisfying (e_2) and (e_3), there is one and only one $z\in F$ such that (x,y,z) is solution of $(\mathscr{F}(a))$. Therefore, $N_3(a)$ is the number of $(x,y)\in F^2$ satisfying (e_2) and (e_3). Let $(x,y)\in F^*\times F^*$. Then (x,y) does not satisfy (e_3) if and only if $(y/x)^{Q^2-1}=1$, that is, if and only if $(y/x)\in F\cap\mathbb{F}_{Q^2}$. Thus,

$$N_3(a)=|F^*|^2-|F^*|(q-1)=(2^m-1)(2^m-q).$$

(II) Suppose that m/d even. Let $\mathscr{A}(a)$ denote the set formed by the $(x, y, z) \in F^3$ satisfying conditions (e_1), (e_2) and (e_3). Then

$$N_3(a) = |\mathscr{A}(a)|. \tag{1}$$

Let

$$\mathscr{B}_0(a) = \{(x, y, z) \in F^3 \mid x^k + y^k + z^k = a, xy = 0\}$$

and

$$\mathscr{B}_1(a) = \{(x, y, z) \in F^3 \mid x^k + y^k + z^k = a, xy \neq 0, x^{Q^2-1} = y^{Q^2-1}\}.$$

Then

$$v_3(a) = |\mathscr{A}(a)| + |\mathscr{B}_0(a)| + |\mathscr{B}_1(a)|. \tag{2}$$

Firstly, we deal with $\mathscr{B}_0(a)$. We have

$$\mathscr{B}_0(a) = \mathscr{B}_{0,0}(a) \cup \mathscr{B}_{0,1}(a) \cup \mathscr{B}_{1,0}(a), \tag{3}$$

with the $\mathscr{B}_{i,j}(a)$ defined as follows. For $(x, y, z) \in \mathscr{B}_0(a)$,

$$\begin{aligned}
(x, y, z) \in \mathscr{B}_{0,0}(a) &\Leftrightarrow (x, y) = (0, 0),\\
(x, y, z) \in \mathscr{B}_{0,1}(a) &\Leftrightarrow y \neq 0,\\
(x, y, z) \in \mathscr{B}_{1,0}(a) &\Leftrightarrow x \neq 0.
\end{aligned}$$

Now $(0, 0, z) \in \mathscr{B}_{0,0}(a) \Leftrightarrow a = z^k$, so that

$$|\mathscr{B}_{0,0}(a)| = v_1(a) \tag{4}$$

and $(0, y, z) \in \mathscr{B}_{0,1}(a) \Leftrightarrow a = y^k + z^k$ with $y \neq 0$, so that

$$|\mathscr{B}_{0,1}(a)| = v_2(a) - v_1(a). \tag{5}$$

By symmetry, with (3), (4) and (5),

$$|\mathscr{B}_0(a)| = 2v_2(a) - v_1(a). \tag{6}$$

Now we deal with $\mathscr{B}_1(a)$. Let $(x, y) \in F^* \times F^*$. Then $x^{Q^2-1} = y^{Q^2-1} \Leftrightarrow y = ux$ with $u^{Q^2-1} = 1$. Thus,

$$|\mathscr{B}_1(a)| = \sum_{\substack{u \in F \\ u^{Q^2-1}=1}} n_u(a),$$

where $n_u(a)$ is the number of $(x,z) \in F^* \times F$ such that

$$a = x^k(1+u^k) + z^k. \tag{7}$$

Let $u \in F^*$. Then $u^{Q^2-1} = 1$ if and only if $u \in F^* \cap \mathbb{F}_{Q^2} = (\mathbb{F}_{q^2})^*$. Thus,

$$|\mathscr{B}_1(a)| = \sum_{\substack{u \in \mathbb{F}_{q^2} \\ u \neq 0}} n_u(a). \tag{8}$$

If $u \in (\mathbb{F}_{q^2})^*$, then $(u^{Q+1})^{Q-1} = 1$, so that $u^k = u^{Q+1} \in \mathbb{F}_Q \cap F$. Thus, $u^k \in (\mathbb{F}_q)^*$. Since $\gcd(q-1, Q+1) = 1$, there exists a unique element $w(u) \in \mathbb{F}_q$ such that $w(u)^k = 1 + u^k$. Let $x \in F^*$ and let $u \in (\mathbb{F}_{q^2})^*$. If $u^k = 1$, then (x,z) satisfies (7) if and only if $a = z^k$, so that

$$n_u(a) = |F^*| v_1(a).$$

If $u^k \neq 1$, then (x,z) satisfies (7) if and only if $a = x^k w(u)^k + z^k$, so that $n_u(a) = v_2(a) - v_1(a)$.

There are exactly $q+1$ elements $u \in (\mathbb{F}_{q^2})^*$ such that $u^k = 1$. Therefore, by (8),

$$|\mathscr{B}_1(a)| = (q^2-q-2)v_2(a) + \big((q+1)(2^m-1) - (q^2-q-2)\big)v_1(a). \tag{9}$$

Combining (1), (2), (6) and (9), we get

$$N_3(a) = v_3(a) - (q^2-q)v_2(a) - (q2^m + 2^m - q^2)v_1(a).$$

We conclude using Propositions 2.4 and 2.7. □

Corollary 2.10. *Let $a \in F$.*

(I) *If $a \neq 0$ and $m/d \geq 3$, or if $a = 0$ and $m/d \geq 3$ with $m/d \neq 4$, then $(\mathscr{F}(a))$ has solutions in F^3.*

(II) *If $m/d \leq 2$, then $(\mathscr{F}(a))$ has no solutions in F^3.*

(III) *Suppose that $m = 4d$. Then $(\mathscr{F}(0))$ has no solutions in F^3. Let $a \in F$. Then there exists $(x,y,z,u) \in F^4$ such that*

$$\begin{cases} x^k + y^k + z^k + u^k = a, & (\mathrm{e}_1), \\ xy \neq 0, & (\mathrm{e}_2), \\ x^{Q^2-1} \neq y^{Q^2-1}. & (\mathrm{e}_3). \end{cases} \tag{$\mathscr{G}(a)$}$$

Proof. Let $a \in F$. Suppose that m/d odd. From the previous proposition, part (I), $N_3(a) > 0 \Leftrightarrow m > d$. Thus $(\mathscr{F}(a))$ has solutions if and only if $m/d > 1$.

(AutoPDF V7 28/1/10 12:48) EMS (170×240mm) Tmath J-2232 PMS, 67:1 (idp) PMU:(KN/)7/1/2010 AC1: WSL 22/01/2010 pp. 13–56 2232_67-1_02 (p. 29)

Suppose that m/d even, say $m = 2nd$. The case $n = 1$ is obvious since the condition (e_3) is not satisfied in a field with $q^2 = 2^{2d}$ elements. For every $a \in F$, $(\mathscr{F}(a))$ has zero solutions. Suppose that $n > 1$. From the previous proposition, (2.14) and (2.16),

$$N_3(0) = (2^m - 1)\big(q^{2n} - q^3 + (-q)^{n+1}(q-1)\big).$$

If $n > 2$, then $N_3(0) > 0$, so that $(\mathscr{F}(0))$ has solutions. If $n = 2$, then $N_3(0) = 0$, so that $(\mathscr{F}(0))$ has zero solutions. Let $a \in B$. From Propositions 2.4 and 2.9,

$$\begin{aligned} N_3(a) &\geq 2^{2m} + 2^m(q^3 - 3q^2 - 1) + 2q^3 - (q-1)(q^2 - q + 1)q2^{m/2} \\ &> 2^{2m} + 2^m\big(q^3 - 3q^2 - 1 - q(q-1)(q^2 - q + 1)\big) \\ &= 2^{2m} - 2^m(q^4 - 3q^3 + 5q^2 - q + 1) > q^{4n} - q^{2n+4} \geq 0. \end{aligned}$$

Thus, $(\mathscr{F}(a))$ has solutions. Let $a \in F^* - B$. From Propositions 2.4 and 2.9,

$$\begin{aligned} N_3(a) &\geq 2^{2m} - 2^m(2q^2 - 2q + 1) + q^3 - q^2 - (q-1)(q-2)q2^{m/2} \\ &> 2^{2m} - 2^m(q^3 - q^2 + 1) \\ &> 2^{2m} - 2^m q^3 = q^{4n} - q^{2n+3} > 0. \end{aligned}$$

If $n \geq 2$, then $N_3(a) > 0$. Thus, $(\mathscr{F}(a))$ has solutions.

Suppose that $n = 2$. If $a \neq 0$, for each (x, y, z) solution of $(\mathscr{F}(a))$, $(x, y, z, 0)$ is a solution of $(\mathscr{G}(a))$; if $a = 0$, for each (x, y, z) solution of $(\mathscr{F}(1))$, $(x, y, z, 1)$ is a solution of $(\mathscr{G}(a))$. □

3. The numbers $v(2^m, k)$

Proposition 3.1. *We have* $v(2^m, k) \geq 3$. *Moreover, if* m *divides* $2r$, *then* $v(2^m, k) = \infty$.

Proof. Suppose that $v(2^m, k) = s$. Then there exists $(u_1, v_1, \ldots, u_s, v_s) \in F^{2s}$ such that

$$T = \sum_{i=1}^{s} (u_i T + v_i)^{Q+1},$$

so that

$$0 = \sum_{i=1}^{s} u_i^Q v_i \tag{1}$$

and

$$1 = \sum_{i=1}^{s} u_i v_i^Q. \tag{2}$$

Raising (1) to the power Q gives

$$0 = \sum_{i=1}^{s} u_i^{Q^2} v_i^Q.$$

If m divides $2r$, that is, if $F \subset \mathbb{F}_{Q^2}$, then $u_i^{Q^2} = u_i$ for all i, contradicting (2).

Suppose that $s = 2$. In that case there exists $(x, y, u, v) \in F^4$ such that

$$0 = x^k + u^k, \tag{3}$$

$$0 = x^Q y + u^Q v, \tag{4}$$

$$1 = xy^Q + uv^Q. \tag{5}$$

If $xu = 0$, (3) yields that $(x, u) = (0, 0)$ so that (5) is not satisfied. Thus, $xu \neq 0$. From (3), $u = xz$ with z a k-th root of 1, so that with (4), $v = zy$, and by (5), $1 = xy^Q + zx(zy)^Q = 0$, leading to a contradiction. □

Proposition 3.2. (I) *If* $m/d \notin \{1, 2, 4\}$, *then* $v(2^m, k) = 3$.

(II) *If* $m/d = 4$, *then* $v(2^m, k) = 4$.

Proof. (I) Suppose that $m/d \notin \{1, 2, 4\}$. From Proposition 3.1, it is sufficient to prove that $v(2^m, k) \leq 3$.

By Corollary 2.10 (I), there exists $(a_1, a_2, a_3) \in F^3$ such that

$$\begin{cases} (a_1)^k + (a_2)^k + (a_3)^k = 0, \\ a_1 a_2 \neq 0, \\ (a_1)^{Q^2-1} \neq (a_2)^{Q^2-1}. \end{cases}$$

Let $(b_1, b_2) \in F^2$ be a solution of $(\mathscr{E}(a_1, a_2, 0, 1))$ with $(\mathscr{E}(x, y, u, v))$ defined by (2.3). Then

$$(a_1)^Q b_1 + (a_2)^Q b_2 = 0,$$

$$a_1 (b_1)^Q + a_2 (b_2)^Q = 1,$$

so that

$$(a_1 T + b_1)^k + (a_2 T + b_2)^k + (a_3 T)^k = T + (b_1)^k + (b_2)^k.$$

Thus, $T + (b_1)^k + (b_2)^k$ is sum of three k-th powers of linear polynomials. Therefore, $v(F, k) \leq 3$.

(II) Suppose that $m/d = 4$. We first prove that $v(2^m, k) > 3$. Indeed, suppose $v(2^m, k) = v(F, k) = 3$. Then there is $(\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3, \beta_3) \in F^6$ such that

$$T = (\alpha_1 T + \beta_1)^k + (\alpha_2 T + \beta_2)^k + (\alpha_3 T + \beta_3)^k.$$

If $\alpha_3 = 0$, the change of the variable $U = T + \beta_3^k$ shows that $v(2^m, k) = 2$ and leads to a contradiction. Thus, $\alpha_3 \neq 0$. Now, the change $U = T + \beta_3 \alpha_3^{-1}$ shows that there exists $(a_1, a_2, b_1, b_2, a_3) \in F^4$ such that

$$T = (a_1 T + b_1)^k + (a_2 T + b_2)^k + (a_3 T)^k,$$

so that the system $\bigl(\mathscr{F}(0)\bigr)$ has a solution, contradicting Corollary 2.10. Thus, $v(2^m, k) > 3$.

By Corollary 2.10 (II), there exists $(a_1, a_2, a_3, a_4) \in F^4$ such that

$$\begin{cases} (a_1)^k + (a_2)^k + (a_3)^k + (a_4)^k = 0, \\ a_1 a_2 \neq 0, \\ (a_1)^{Q^2-1} \neq (a_2)^{Q^2-1}. \end{cases}$$

Let $(b_1, b_2) \in F^2$ be solution of $\bigl(\mathscr{E}(a_1, a_2, 0, 1)\bigr)$. Then

$$(a_1 T + b_1)^k + (a_2 T + b_2)^k + (a_3 T)^k + (a_4 T)^k = T + (b_1)^k + (b_2)^k,$$

so that T is sum of four k-th powers of linear polynomials. Therefore, $v(F, k) \leq 4$. □

Corollary 3.3. *We have $\mathscr{S}(F, k) = F[T]$ if and only if $m/d \geq 3$. More precisely, if either m/d is odd and $m \neq d$, or if m/d is even and $m/d > 4$, then every $A \in F[T]$ is sum of three k-th powers; if $m = 4d$, then every $A \in F[T]$ is sum of four k-th powers.*

We are ready to present our first result.

Proposition 3.4. *We suppose that m does not divide $2r$.*

(I) *Let $s \geq \left[\frac{\log k}{\log(k/(k-1))}\right]$. Then every $P \in F[T]$ of degree $\geq \delta(s, k) = k\left[\frac{k^2 - 2k - k^2\left(1 - \frac{1}{k}\right)^{s+1}}{1 - k\left(1 - \frac{1}{k}\right)^{s+1}}\right] - k + 1$ is the strict sum of $\bigl(s + v(2^m, k) + 2\bigr)$ k-th powers.*

Moreover, if $s \geq \frac{\log k}{\log(k/(k-1))}$, then $\delta(s, k) \leq k^4 - 3k^3 + 2k^2 - 2k + 1$.

(III) *Let $s \geq \frac{\log(k(k-1)/2)}{\log(k/(k-1))}$. Then every $P \in F[T]$ of degree $\geq k^3 - 3k + 1$ is the strict sum of $\bigl(s + v(2^m, k) + 2\bigr)$ k-th powers.*

(III) *Let $s \geq \frac{3 \log k}{\log(k/(k-1))} - 1$. Then every $P \in F[T]$ such that $k^3 - 2k^2 - k + 1 \leq \deg P \leq k^3 - 3k$ is the strict sum of $\bigl(s + v(2^m, k) + 2\bigr)$ k-th powers.*

(AutoPDF V7 28/1/10 12:48) EMS (170×240mm) Tmath J-2232 PMS, 67:1 (idp) PMU:(KN)7/1/2010 AC1: WSL 22/01/2010 pp. 13–56 2232_67-1_02 (p. 32)

Proof. From Propositions 2.8 and 3.2, F is a k-Waring field and $v(2^m,k)$ is finite. Let $w(m,k) = v(2^m,k) + \max\bigl(\ell(2^m,k), 1+\lambda(2^m,k)\bigr)$. From [1], Proposition 5.3, we have:

(I) Let $s \geq \left[\frac{\log k}{\log(k/(k-1))}\right]$. Then every $P \in F[T]$ of degree $\geq \delta(s,k) = k\left\lceil\frac{k^2-2k-k^2\left(1-\frac{1}{k}\right)^{s+1}}{1-k\left(1-\frac{1}{k}\right)^{s+1}}\right\rceil - k + 1$ is a strict sum of $s + w(m,k)$ k-th powers. Moreover, if $s \geq \frac{\log k}{\log(k/(k-1))}$, then $\delta(s,k) \leq k^4 - 3k^3 + 2k^2 - 2k + 1$.

(II) Let $s \geq \frac{\log(k(k-1)/2)}{\log(k/(k-1))}$. Then every $P \in F[T]$ of degree $\geq k^3 - 3k + 1$ is the strict sum of $s + w(m,k)$ k-th powers.

(III) Let $s \geq \frac{3\log k}{\log(k/(k-1))} - 1$. Then every $P \in F[T]$ such that

$$k^3 - 2k^2 - k + 1 \leq \deg P \leq k^3 - 3k$$

is the strict sum of $s + w(m,k)$ k-th powers.

From Proposition 2.8, $\ell(2^m,k) \leq 2$. We conclude the proof by noting that $\lambda(2^m,k) = 1$. □

Corollary 3.5. (I) *If m does not divide $2r$ and $m \neq 4d$, then $G(2^m,k) \leq k\log k + 5$.*

(II) *If $m = 4d$, then $G(2^m,k) \leq k\log k + 6$.*

Proof. Given by Proposition 3.4(I). □

Corollary 3.6. *For odd $m > 1$ or for even $m = 2n$ with odd $n > 1$, or for $m = 4n$ with $n > 2$, we have $G(2^m,5) \leq 12$ and we have $G(256,5) \leq 13$.*

The proof of the following proposition uses an argument already used in the proof of Proposition 4.4 in [1].

Proposition 3.7. *Suppose that $m = 2d$. Let $a \in F$ be such that $a \notin \mathbb{F}_q$. Let $b \in F$ be such that $b^Q = a$. For $n \geq Q$, let*

$$B_n = aT^{nk} + bT^{nk+1-Q^2}.$$

Then B_n is sum of three k-th powers and is not a strict sum of k-th powers.

Proof. We have

$$B_n = (bT^{n+1} + T^{n-Q})^k + (bT^{n+1})^k + (T^{n-Q})^k.$$

Since $m = 2d$, the field F has q^2 elements and a sum of k-th powers in F is in the subfield $\mathbb{F}_q$. Since a is not in $\mathbb{F}_q$, and B_n has degree multiple of k, B_n is not a strict sum of k-th powers. □

Corollary 3.8. *If $m = 2d$, then $G(2^m,k) = \infty$.*

(AutoPDF V7 28/1/10 12:48) EMS (170×240mm) Tmath J-2232 PMS, 67:1 (idp) PMU:(KN/)7/1/2010 AC1: WSL 22/01/2010 pp. 13–56 2232_67-1_02 (p. 33)

4. Identities and strict sums of small degree

First we begin by stating two simple and useful lemmas.

Lemma 4.1. *For each $a \in \mathbb{F}_q$, there exists $\alpha \in \mathbb{F}_{q^2}$ such that $a = \alpha^q + \alpha$. Let $\theta \in \mathbb{F}_{q^2}$ be such that*

$$\theta^q + \theta = 1. \tag{4.1}$$

Suppose that $\mathbb{F}_{q^2} \subset F$. Then for every positive odd integer j and every pair (X, Y) of polynomials in $F[T]$, we have

$$\theta^{q^j} + \theta = 1 \tag{4.2}$$

and

$$X^{q^j}Y + XY^{q^j} = (\theta X + Y)^{q^j+1} + \big((\theta + 1)X + Y\big)^{q^j+1}. \tag{4.3}$$

Proof. The trace map $x \mapsto x^q + x$ from $\mathbb{F}_{q^2}$ to its subfield $\mathbb{F}_q$ is onto. There is $\theta \in \mathbb{F}_{q^2}$ such that $\theta^q + \theta = 1$. On the other hand, $\theta^{q^2} = \theta$, so that, by induction, for every positive integer s, we have $\theta^{q^{2s}} = \theta$ and $\theta^{q^{2s+1}} = (\theta^{q^{2s}})^q = \theta^q = \theta + 1$.

Identity (4.3) is an immediate consequence of (4.2). □

Lemma 4.2. *For $i \in \{0, \dots, Q-1\}$ and $X \in F[T]$, let*

$$L_i(X) = X^Q T^i + XT^{Qi}. \tag{4.4}$$

Then the map $X \mapsto L_i(X)$ is additive, and the following identities are satisfied:

$$L_i(X) = (X + T^i)^{Q+1} + X^{Q+1} + T^{(Q+1)i}. \tag{4.5}$$

For every $b \in F$,

$$L_i(X + bT^i) = L_i(X) + (b^Q + b)T^{i(Q+1)}. \tag{4.6}$$

Moreover, if $F \subset \mathbb{F}_{Q^2}$, then, for every $c \in F^*$,

$$L_i(X) + c^{Q+1}T^{(Q+1)i} = \left(\frac{1}{c^Q}X + cT^i\right)^{Q+1} + \left(\frac{1}{c^Q}X\right)^{Q+1}, \tag{4.7}$$

If $\mathbb{F}_{q^2} \subset F$, then

$$L_i(X) = (\theta X + T^i)^{Q+1} + (\theta X + X + T^i)^{Q+1}. \tag{4.8}$$

Proof. The proof of (4.5) and (4.6) is immediate. The proof of (4.7) follows from observing that $c^{Q^2} = c$. We use (4.3) to prove (4.8). □

Proposition 4.3. *Suppose that* $m/d \geq 3$.

(I) *Let* $0 < N < k-2$ *and let*

$$A = \sum_{n=0}^{kN} a_n T^n$$

be a polynomial of $F[T]$ *such that*

$$k(N-1) < \deg A \leq kN.$$

Then A *is a strict sum of* k*-th powers if and only if* $a_n = 0$ *for each* $n \in \bigcup_{i=0}^{N-1} [iQ+N+1, (i+1)Q-1]$. *Thus, if* $k > 3$, *then* $\mathscr{S}(F,k) \neq \mathscr{S}^*(F,k)$ *and* $g(2^m,k) = \infty$.

(II) *Let* $A \in F[T]$ *be such that*

$$k(k-3) < \deg A \leq k(k-2).$$

Then A *is a strict sum of* k*-th powers.*

(III) *Let* $A \in F[T]$ *of degree* $\leq k(k-2)$ *be a strict sum of* k*-th powers. Then* A *is a strict sum of* $v(2^m,k)\left\lceil \frac{\deg A}{k} \right\rceil + \ell(2^m,k)$ k*-th powers.*

(IV) *Let* $A \in F[T]$ *of degree* $\leq k(k-2)$. *Then*

$$A = \sum_{i=1}^{s} (X_i)^k$$

with $s = v(2^m,k)(k-2) + \ell(2^m,k)$ *and* $\deg X_i \leq k-2$ *for* $i = 1, \dots, s$.

Proof. By Propositions 2.8 and 3.2, the numbers $\ell(2^m,k)$ and $v(2^m,k)$ are finite. Let N be a positive integer such that $N < Q$. Let $A \in F[T]$ with $k(N-1) < \deg A \leq kN$ be a strict sum of s k-th powers. Thus,

$$A = \sum_{i=1}^{s} (Y_i)^{Q+1},$$

where for $i = 1, \dots, s$,

$$Y_i = \sum_{n=0}^{N} y_{i,n} T^n$$

with $y_{i,n} \in F$. Then

$$A = \sum_{i=1}^{s} \sum_{n=0}^{N} (y_{i,n})^{Q} T^{Qn} Y_i = \sum_{n=0}^{N} T^{Qn} \Big(\sum_{i=1}^{s} (y_{i,n})^{Q} Y_i \Big).$$

Let

$$X_n = \sum_{i=1}^{s} (y_{i,n})^{Q} Y_i.$$

Then

$$A = \sum_{n=0}^{N} X_n T^{nQ}.$$

If $N < Q - 1$, in the above sum, there are no monomials $\alpha_i T^i$ with exponent i in the intervals $[N+1, Q-1], [Q+N+1, 2Q-1], \ldots, [(N-1)Q+N+1, NQ-1]$. The necessary condition in (I) is proved. Moreover, if $Q \neq 2$, there exist polynomials of degree $\leq k(Q-2)$ which are not strict sums of k-th powers. By Corollary 3.3, $\mathscr{S}(F,k) = F[T]$. If $k > 3$, then $\mathscr{S}(F,k) \neq \mathscr{S}^*(F,k)$ and $g(2^m, k) = \infty$.

Now let $A \in F[T]$ with $\deg A \leq k(k-2)$, that is, $\deg A \leq Q^2 - 1$. Let N be defined by

$$k(N-1) < \deg A \leq kN. \tag{1}$$

Let

$$A = \sum_{n=0}^{Q^2-1} a_n T^n.$$

In addition, if $N < Q - 1$, we suppose that $a_n = 0$ for each $n \in \bigcup_{i=0}^{N-1} J_i$ with

$$J_i = [iQ + N + 1, (i+1)Q - 1].$$

In order to prove parts (I) and (II), we shall prove that there is a positive integer s and, for $i = 1, \ldots, s$, there are polynomials

$$X_i = \sum_{n=0}^{N} x_{i,n} T^n$$

such that

$$A = \sum_{i=0}^{s} (X_i)^{Q+1}. \tag{2}$$

The proof will show that (2) is solvable when $s = v(2^m, k)N + \ell(2^m, k)$, proving the part (III) of the proposition.

Let

$$I = I(N) = \begin{cases} \{0, \dots, Q^2 - 1\} & \text{if } N = Q - 1, \\ \{0, \dots, kN\} - \bigcup_{i=0}^{N-1} J_i & \text{if } N < Q - 1. \end{cases}$$

Observe that

$$I = \{n = Q\beta + \rho \,|\, 0 \le \beta, \rho \le N\}.$$

We begin by proving that there is a positive integer s such that the system $(r_n)_{n \in I}$ is solvable, where (r_n) denotes the equation

$$a_n = \sum_{i=1}^{s} \sum_{\substack{n = Q\beta + \rho \\ 0 \le \beta \le N \\ 0 \le \rho \le N}} (x_{i,\beta})^Q x_{i,\rho} \tag{r_n}$$

with unknowns $x_{i,\beta} \in F$, $1 \le i \le s$, $0 \le \beta \le N$.

Let $v = v(2^m, k)$. From Proposition 3.2,

$$v = \begin{cases} 3 & \text{if } m/d \ne 4, \\ 4 & \text{if } m/d = 4. \end{cases}$$

For each non negative integer $n \le Q^2 - 1$, there is a unique ordered pair (β, ρ) such that

$$n = Q\beta + \rho, \qquad 0 \le \beta \le Q - 1,\ 0 \le \rho \le Q - 1,$$

and a unique $\bar{n} \le Q^2 - 1$ with $\bar{n} = Q\rho + \beta$. The map $n \mapsto \bar{n}$ is bijective with fixed points the integers n which are divisible by $Q + 1 = k$. We distinguish two classes of equations (r_n), the special ones and the ordinary ones. The special equations are the equations (r_n) with index n multiple of $Q + 1$. The ordinary equations will be considered by pairs $\{r_n, r_{\bar{n}}\}$. We introduce a notation. Let $(u, w) \in F^2$ be such that $uw \ne 0$ and $u^{Q^2-1} \ne w^{Q^2-1}$. By Lemma 2.2, for each $(\alpha, \beta) \in F^2$, there exists a unique $(x, y) \in F^2$ solution of $\mathscr{E}(u, w, \alpha, \beta)$, that is (x, y) satisfies

$$\begin{cases} \alpha = u^Q x + w^Q y, \\ \beta = u x^Q + w y^Q. \end{cases}$$

We put

$$(x, y) = \varphi(u, w, \alpha, \beta).$$

We construct a solution recursively. At each step, we consider a special equation together with some pairs of ordinary equations. If $v = 3$, we denote $\big(\mathscr{F}(a)\big)$ by $\big(\mathscr{H}(a)\big)$, and if $v = 4$, we denote $\big(\mathscr{G}(a)\big)$ by $\big(\mathscr{H}(a)\big)$, with $\big(\mathscr{F}(a)\big)$ and $\big(\mathscr{G}(a)\big)$ defined as in Corollary 2.10.

Level N: Corollary 2.10 implies the existence of $(x_{1,N}, \dots, x_{v,N})$ solution of $\big(\mathscr{H}(a_{kN})\big)$, that is,

$$b_N = a_{kN} = (x_{1,N})^k + \cdots + (x_{v,N})^k$$

with

$$x_{1,N} x_{2,N} \neq 0$$

and

$$(x_{1,N})^{Q^2-1} \neq (x_{2,N})^{Q^2-1}.$$

For $j = 1, \dots, N$, let $(x_{1,N-j}, x_{2,N-j}) = \varphi(x_{1,N}, x_{2,N}, a_{kN-j}, a_{\overline{kN-j}})$, and let $x_{i,N-j} = 0$ for $2 < i \leq v$. At this step, with $s = v$, equations (r_n) and $(r_{\bar{n}})$ are satisfied by $(x_{i,j})_{1 \leq i \leq v}$ for $n \in \{QN, \dots, kN\}$. Observe that for each $j = 1, \dots, N$, we have $\overline{kN-j} = Q(N-j) + N$, so that $k(N-1)$ is the greatest $n \in I$ for which the exponent n has not been considered.

Level $N-1$: Set

$$b_{N-1} = a_{k(N-1)} + \sum_{i=1}^{v} (x_{i,N-1})^k.$$

Corollary 2.10 implies the existence of $(x_{v+1,N-1}, \dots, x_{2v,N-1})$ solution of $\big(\mathscr{H}(b_{N-1})\big)$. For $j = 1, \dots, N-1$, let $(x_{v+1,N-1-j}, x_{v+2,N-1-j}) = \varphi(x_{v+1,N-1}, x_{v+2,N-1}, \alpha, \beta)$ with

$$\alpha = (x_{1,N-1})^Q x_{1,N-1-j} + (x_{2,N-1})^Q x_{2,N-1-j} + a_{k(N-1)-j},$$
$$\beta = x_{1,N-1}(x_{1,N-1-j})^Q + x_{2,N-1}(x_{2,N-1-j})^Q + a_{\overline{k(N-1)-j}},$$

and let $x_{i,N-j} = 0$ for $2 + v < i \leq 2v$. At this step, with $s = 2v$, equations (r_n) and $(r_{\bar{n}})$ are satisfied by $(x_{i,j})_{1 \leq i \leq 2v}$ for $n \in \{QN, \dots, kN\} \cup \{Q(N-1), \dots, k(N-1)\}$. Observe that for each $j = 1, \dots, N-1$, we have $\overline{k(N-1)-j} =$

$Q(N-1-j)+N-1$, so that $k(N-2)$ is the greatest $n \in I$ for which the exponent n has not been considered.

Levels $N-2, \dots, N-h$, with $h < N$: The level $N-h$ deals with exponents n and $\bar{n}$ for $n \in \{Q(N-h), \dots, k(N-h)\}$.

Suppose that the previous steps have given $(x_{i,j})_{1 \le i \le hv}$ satisfying equations (r_n) and $(r_{\bar{n}})$ with $s = hv$ and n running through $\bigcup_{i=N-h+1}^{N} \{Qi, \dots, ki\}$. Let

$$b_{N-h} = a_{k(N-h)} + \sum_{i=1}^{vh} (x_{i,N-h})^k.$$

Let $(x_{hv+1,N-h}, \dots, x_{(h+1)v,N-h})$ be solution of $(\mathscr{H}(b_{N-h}))$. For $j = 1, \dots, N-h$, let

$$(x_{hv+1,N-h-j}, x_{hv+2,N-h-j}) = \varphi(x_{hv+1,N-h}, x_{hv+2,N-h}, \alpha_j, \beta_j)$$

with

$$\alpha_j = a_{k(N-h)-j} + \sum_{v=1}^{vh} (x_{v,N-h})^Q x_{v,N-h-j},$$

$$\beta_j = a_{\overline{k(N-h)-j}} + \sum_{v=1}^{vh} x_{v,N-h} (x_{v,N-h-j})^Q,$$

and let $x_{i,N-j} = 0$ for $2 + hv < i \le (h+1)v$. At this step, with $s = (h+1)v$, we have obtained $(x_{i,j})_{1 \le i \le s}$ satisfying equations (r_n) for n and $(r_{\bar{n}})$ with n running over $\bigcup_{i=N-h}^{N} \{Qi, \dots, ki\}$. We note that for each $j = 1, \dots, N-h$, we have $\overline{Q(N-h)-j} = k(N-h-j) + N-h$, so that $k(N-h-1)$ is the greatest $n \in I$ for which the exponent n has not been considered. Thus, the process goes on.

After level 1, with $s = vN$, we have obtained $(x_{i,j})_{1 \le i \le s}$ satisfying the equations (r_n) for all $n \in I$ apart from $n = 0$. For $i = 1, \dots vN$, let

$$X_i = \sum_{v=0}^{N} x_{i,v} T^v. \tag{3}$$

Level 0: Let

$$b_0 = a_0 + \sum_{i=1}^{Nv} (x_{i,0})^k.$$

Then by (3),

$$A + \sum_{i=1}^{Nv} (X_i)^k = b_0. \tag{4}$$

Since F is a k-Waring field, b_0 is sum of $\ell = \ell(2^m, k)$ k-th powers, say

$$b_0 = (z_1)^k + \cdots + (z_\ell)^k. \tag{5}$$

From (4) and (5),

$$A = \sum_{i=1}^{Nv} (X_i)^k + \sum_{i=1}^{\ell} (z_i)^k.$$

From (1) and (5), A is a strict sum of $(vN + \ell)$ k-th powers.

Observe that, if $\deg A \le k(k-3)$, the same process works with $Q-1$ at the place of N. In that case we get that

$$A = \sum_{i=1}^{(Q-1)v} (X_i)^k + \sum_{i=1}^{\ell} (z_i)^k$$

with $\deg X_i \le Q-1$ for $i = 1, \ldots, (Q-1)v$. This remark proves the part (IV). □

Lemma 4.4. *Suppose that $F \subset \mathbb{F}_{Q^2}$. Let $A \in F[T]$ be a sum of k-th powers. Then $T^{Q^2} + T$ divides $A^Q + A$.*

Proof. Let $x \in \mathbb{F}_{Q^2}$. Since $A \in \mathbb{F}_{Q^2}[T]$, $A(x)$ is a sum of k-th powers in $\mathbb{F}_{Q^2}$, so that $A(x) \in \mathbb{F}_Q$. Thus, $A(x)^Q + A(x) = 0$. Therefore, $A^Q + A$ is divisible by $(T + x)$ for each $x \in \mathbb{F}_{Q^2}$ and

$$T^{Q^2} + T = \prod_{x \in \mathbb{F}_{Q^2}} (T + x)$$

divides $A^Q + A$. □

Proposition 4.5. *Suppose that $F \subset \mathbb{F}_{Q^2}$. Let*

$$A = \sum_{n=0}^{Q^2-1} a_n T^n$$

be a polynomial of $F[T]$ with $\deg A < Q^2$ *such that $A^Q + A$ is multiple of $T^{Q^2} + T$. Then*

(I) *for every* $n = Qj + i$ *with* $0 \le j < Q$, $0 \le i < Q$, *we have*

$$a_n = (a_{\bar{n}})^Q,$$

where $\bar{n} = Qi + j$;

(II) *if* $F \subset \mathbb{F}_Q$, *then* A *is a strict sum of* $(3k - 5)$ k*-th powers;*

(III) *if* $F \not\subset \mathbb{F}_Q$, *then* A *is a strict sum of* $(2k - 3)$ k*-th powers.*

Proof. Let

$$A = A_0 + A_1 T^Q + \cdots + A_{Q-1} T^{(Q-1)Q}$$

be the expansion of A in base T^Q. Thus, for $j = 0, \dots, Q-1$,

$$A_j = a_{Qj} + a_{Qj+1} T + \cdots + a_{Qj+Q-1} T^{Q-1}.$$

Then

$$A^Q = \sum_{j=1}^{Q-1} (A_j)^Q (T^{jQ^2} + T^j) + \sum_{j=0}^{Q-1} (A_j)^Q T^j.$$

For $j = 1, \dots, Q-1$, $T^{jQ^2} + T^j$ is congruent to 0 $(\operatorname{mod} T^{Q^2} + T)$. Thus,

$$A^Q \equiv \sum_{j=0}^{Q-1} (A_j)^Q T^j \quad (\operatorname{mod} T^{Q^2} + T)$$

and

$$A + A^Q \equiv \sum_{j=0}^{Q-1} \big((A_j)^Q T^j + A_j T^{Qj}\big) \quad (\operatorname{mod} T^{Q^2} + T). \tag{1}$$

For $j = 0, \dots, Q-1$, $\deg\big((A_j)^Q T^j + A_j T^{Qj}\big) \le Q^2 - 1$, so that by (1),

$$\sum_{j=0}^{Q-1} \big((A_j)^Q T^j + A_j T^{Qj}\big) = 0,$$

that is,

$$\sum_{j=0}^{Q-1} \sum_{i=0}^{Q-1} \big((a_{Qj+i})^Q T^{Qi+j} + a_{Qj+i} T^{Qj+i}\big) = 0. \tag{2}$$

Let $n \in \{0, \dots, Q^2 - 1\}$. Then n is uniquely written as $n = Q\alpha + \rho$, with $\alpha, \rho < Q$. By (2),

$$a_n = a_{Q\alpha+\rho} = (a_{Q\rho+\alpha})^Q = (a_{\bar{n}})^Q. \tag{3}$$

This proves (I).

Let $n \in \{1, \dots, Q^2 - 2\}$ be non-divisible by $Q+1$. If $n = Qj + i$, with $0 \le i < Q$, $0 \le j < Q$, then

$$a_n T^n + a_{\bar{n}} T^{\bar{n}} = (a_{Qi+j})^Q T^{Qj+i} + (a_{Qi+j}) T^{Qi+j} = L_i(a_{Qi+j} T^j)$$

and so

$$A = \sum_{i=0}^{Q-1} a_{(Q+1)i} T^{i(Q+1)} + \sum_{i=0}^{Q-2} \sum_{j=i+1}^{Q-1} L_i(a_{Qi+j} T^j). \tag{4}$$

For n divisible by $Q+1$, equality (2) gives $a_n = (a_n)^Q$, proving that $a_n \in \mathbb{F}_Q$, this fact being obvious when $F \subset \mathbb{F}_Q$.

(A) Suppose that $F \subset \mathbb{F}_Q$, that is $F = \mathbb{F}_q$ or equivently, $m \mid r$. By Proposition 2.1, $\Delta(2^m, k) = 1$. For every $i = 0, \dots, Q-1$, there is $c_i \in F$ such that

$$a_{(Q+1)i} = (c_i)^k = (c_i)^{Q+1}.$$

Therefore, by (4),

$$\begin{aligned} A &= \sum_{i=0}^{Q-1} (c_i T^i)^{Q+1} + \sum_{i=0}^{Q-2} \sum_{j=i+1}^{Q-1} L_i(a_{Qi+j} T^j) \\ &= (c_{Q-1} T^{Q-1})^{Q+1} + \sum_{i=0}^{Q-2} \big((c_i T^i)^{Q+1} + L_i(B_i)\big), \end{aligned}$$

with

$$B_i = \sum_{j=i+1}^{Q-1} a_{Qi+j} T^j. \tag{5}$$

By (4.5) and (4.7),

$$\begin{aligned} A = (c_{Q-1} T^{Q-1})^k &+ \sum_{\substack{i=0 \\ a_{(Q+1)i}=0}}^{Q-2} \big((B_i + T^i)^k + (B_i)^k + (T^i)^k\big) \\ &+ \sum_{\substack{i=0 \\ a_{(Q+1)i}\neq 0}}^{Q-2} \left(\frac{1}{c_i^Q} B_i + c_i T^i\right)^k + \left(\frac{1}{c_i^Q} B_i\right)^k, \end{aligned} \tag{6}$$

so that A is sum of $\big(1 + 3(Q-1)\big)$ k-th powers of polynomials.

We consider the degrees. Suppose that

$$\deg A = d = (Q+1)N - \rho. \tag{7}$$

with

$$0 \le \rho < N. \tag{8}$$

We have $a_{(Q+1)i} = 0$ for $i > N$. Thus, the monomials $c_i T^i$ which occur in (6) have degree $\le N$. For $j > N$ or for $j = N$ and $i > N - \rho$, we have $a_{Qj+i} = 0$ so that, by part (I), $a_{Qi+j} = 0$. Let $i > N$. From (5), we have $B_i = 0$, so that the terms $(B_i + T^i)^k + (T^i)^k$ which occur in (6) cancel. By (7) and (8), the sum (6) is strict. This proves (II) in the case where $F \subset \mathbb{F}_Q$.

(B) Suppose that $F \not\subset \mathbb{F}_Q$. Since $F \subset \mathbb{F}_{Q^2}$, we have $F = \mathbb{F}_{q^2}$. Thus, $m = 2d$ and r/d is odd. The trace map $x \mapsto x^q + x$ from $F = \mathbb{F}_{q^2}$ to $\mathbb{F}_q$ is onto. For every $i = 0, \dots, Q-2$, $a_{(Q+1)i} \in F \cap \mathbb{F}_Q = \mathbb{F}_q$, so that there is $b_i \in F$ such that

$$a_{(Q+1)i} = b_i^q + b_i.$$

For every $y \in \mathbb{F}_{q^2}$, we have $y^{q^2} = y$, so that, by induction, for every positive integer j, we have $y^{q^{2j}} = y$ and $y^{q^{2j+1}} = y^q$. Since $Q = q^{r/d}$ with r/d odd, for every $i = 0, \dots, Q-2$, we have

$$a_{(Q+1)i} = b_i^Q + b_i.$$

Moreover, since $a_{Q^2-1} \in \mathbb{F}_Q$, a_{Q^2-1} is a k-th power of an element $c_{Q-1} \in \mathbb{F}_{Q^2} = F$. Thus,

$$a_{(Q+1)i} T^{(Q+1)i} = \big((b_i)^Q + b_i\big) T^{(Q+1)i} \qquad \text{for } 0 \le i \le Q-2,$$

and

$$a_{Q^2-1} T^{Q^2-1} = (c_{Q-1} T^{Q-1})^k.$$

Therefore,

$$\begin{aligned} A &= (c_{Q-1} T^{Q-1})^k + \sum_{i=0}^{Q-2} \Big(\big((b_i)^Q + b_i\big) T^{(Q+1)i} + \sum_{j=i+1}^{Q-1} L_i(a_{Qi+j} T^j) \Big) \\ &= (c_{Q-1} T^{Q-1})^k + \sum_{i=0}^{Q-2} \big(\big((b_i)^Q + b_i\big) T^{(Q+1)i} + L_i(B_i) \big), \end{aligned}$$

with B_i defined by (5). By (4.6),

$$A = (c_{Q-1}T^{Q-1})^k + \sum_{i=0}^{Q-2} L_i(B_i + b_iT^i).$$

Let $\theta \in \mathbb{F}_{q^2}$ be as in Lemma 4.1. In view of identity (4.8), identity (6) above may be replaced by

$$A = (c_{Q-1}T^{Q-1})^k + \sum_{i=0}^{Q-2}\left(\left(\theta B_i + (\theta b_i + 1)T^i\right)^k + \left(\theta B_i + B_i + (\theta b_i + b_i + 1)T^i\right)^k\right), \qquad (6')$$

so that A is sum of $1 + 2(Q-1)$ k-th powers of polynomials. We finish the proof of the part (II) proving as above that $(6')$ is a strict sum. □

5. The descent

In this section we generalize a descent process used in [8] and [7] to deal with the case $k = 3$. Using formula (4.5), for a given polynomial

$$X = \sum_{i=0}^{N} x_iT^i,$$

we replace the monomial x_NT^N by the sum of an appropriate $L_i(Y)$ and two monomials of lower degree. Then we repeat the process. The method is described in the following proposition.

Proposition 5.1. *Let n be a positive integer and let $X \in F[T]$ with degree $< Qn$. Then there exist $Y_0, Y_1, \dots, Y_{Q-1}, R \in F[T]$ such that*

$$X = \sum_{i=0}^{Q-1} L_i(Y_i) + R, \qquad (5.1)$$

$$\deg(Y_i) < n \quad \text{if } 0 \le i \le Q-1, \qquad (5.2)$$

$$\deg R < Q^2, \qquad (5.3)$$

$$R = \sum_{i=0}^{Q-1}\sum_{j=0}^{i} a_{Qj+i}T^{Qj+i}, \qquad (5.4)$$

with $a_0, \dots, a_{Q^2-1} \in F$.

Proof. Set

$$X = \sum_{j=0}^{Qn-1} x_j T^j$$

with $x_j \in F$ for $j = 0, \dots, Qn-1$. For $j = 0, \dots, Qn-1$, let $\xi_j \in F$ be defined by

$$\xi_j^Q = x_j.$$

(I) Suppose that $n \le Q$. Put $x_j = \xi_j = 0$ if $j \ge Qn$. Then

$$X = \sum_{r=0}^{Q-2} T^r \Big(\sum_{j=r+1}^{Q-1} \xi_{Qj+r} T^j \Big)^Q + \sum_{r=0}^{Q-1} T^r \Big(\sum_{j=0}^{r} x_{Qj+r} T^{Qj} \Big)$$

and by (4.4),

$$X = \sum_{r=0}^{Q-2} \left(L_r \Big(\sum_{j=r+1}^{Q-1} \xi_{Qj+r} T^j \Big) + \sum_{j=r+1}^{Q-1} \xi_{Qj+r} T^{Qr+j} \right) + \sum_{r=0}^{Q-1} \sum_{j=0}^{r} x_{Qj+r} T^{Qj+r},$$

that is,

$$X = \sum_{r=0}^{Q-1} L_r\big(Y_r(X)\big) + R(X) \tag{1}$$

with $R(X)$ of the form

$$R(X) = \sum_{r=0}^{Q-1} \sum_{j=0}^{r} a_{Qj+r} T^{Qj+r}, \tag{2}$$

with $Y_{Q-1} = 0$ and

$$Y_r(X) = \sum_{j=r+1}^{Q-1} \xi_{Qj+r} T^j$$

for $r = 0, \dots, Q-2$. If $n < Q$, then for each r and for each $j \ge n$, we have $Qj + r \ge Qn$ and so $\xi_{Qj+r} = 0$ so that $\deg Y_r(X) < n$.

(II) Suppose that $n = Q+1$. Then

$$X = X' + \sum_{r=0}^{Q-1} x_{Q^2+r} T^{Q^2+r}$$

with

$$\deg X' < Q^2. \tag{3}$$

Thus with (4.4),

$$X = X' + x_{Q^2} T^{Q^2} + \sum_{r=1}^{Q-1} \big(L_r(\xi_{Q^2+r} T^Q) + \xi_{Q^2+r} T^{Q(r+1)} \big),$$

so that

$$X = X'' + (x_{Q^2} + \xi_{Q^2+Q-1}) T^{Q^2} + \sum_{r=1}^{Q-1} L_r(\xi_{Q^2+r} T^Q), \tag{4}$$

with

$$\deg X'' < Q^2. \tag{5}$$

Set $(x_{Q^2} + \xi_{Q^2+Q-1}) = \eta^Q$. Then

$$(x_{Q^2} + \xi_{Q^2+Q-1}) T^{Q^2} = L_0(\eta T^Q) + \eta T^Q,$$

so that with (4) and (5),

$$X = Y + L_0(\eta T^Q) + \sum_{r=1}^{Q-1} L_r(\xi_{Q^2+r} T^Q).$$

From (3), we have $\deg Y < Q^2$. By (1) and (2),

$$X = \sum_{r=0}^{Q-1} L_r\big(Y_r(X)\big) + R(X), \tag{6}$$

with $R(X)$ of the required form (2) and $\deg Y_r(X) \le Q$ for $r = 0, \dots, Q-1$.

(III) Suppose that $n > Q + 1$. Let (n_j) be the sequence of integers defined by the conditions:

$$n_0 = n, \qquad n_j = \left\lceil \frac{n_{j-1}}{Q} \right\rceil + Q - 1, \tag{7}$$

(AutoPDF V7 28/1/10 12:48) EMS (170×240mm) Tmath J-2232 PMS, 67:1 (idp) PMU:(KN/)7/1/2010 AC1: WSL 22/01/2010 pp. 13–56 2232_67-1_02 (p. 46)

If $n_j > Q+1$, then $n_j > n_{j+1}$. Let s denote the least integer such that $n_s \le Q+1$. We set $X_0 = X$ and we shall prove by induction on j, that for every $j \ge 0$,

$$X = \sum_{r=0}^{Q-1} L_r(B_{r,j}) + X_j \tag{8}$$

where $B_{0,j}, \dots, B_{Q-1,j}$, $X_j \in F[T]$ satisfy the degree conditions

$$\deg X_j < Qn_j, \qquad \deg B_{r,j} < n. \tag{9}$$

Then we shall conclude the proof, taking $j = s$.

We start taking $X_0 = X$ and $B_{0,0} = \cdots = B_{Q-1,0} = 0$. Let $j \in \{0, \dots, s-1\}$. We suppose that relations (8) and (9) are satisfied. We set $v = n_j$ and

$$X_j = \sum_{\alpha=0}^{Qv-1} y_\alpha T^\alpha.$$

For $\alpha = 0, \dots, Qv-1$, let $\eta_\alpha \in F$ be such that $y_\alpha = (\eta_\alpha)^Q$. For $r = 0, \dots, Q-1$, let

$$Z_r = \sum_{\alpha=0}^{v-1} \eta_{Q\alpha+r} T^\alpha$$

and

$$X_{j+1} = \sum_{r=0}^{Q-1} Z_r T^{Qr},$$

so that

$$\deg Z_r < v, \qquad \deg X_{j+1} \le v + Q^2 - Q - 1. \tag{10}$$

By (8) and (4.4),

$$X = \sum_{r=0}^{Q-1} L_r(B_{r,j} + Z_r) + X_{j+1}.$$

We consider the degrees. We have $\deg(B_{r,j} + Z_r) < \max(n, n_j) = n$, and, by (7), $\deg X_{j+1} < n_j + Q^2 - Q + 1 \le Qn_{j+1}$. □

Corollary 5.2. *Suppose that $F \subset \mathbb{F}_{Q^2}$. Then $\mathscr{S}(F,k)$ is the subset of $F[T]$ formed by the polynomials A such that $T^{Q^2}+T$ divides A^Q+A.*

Proof. From Lemma 4.4,

$$\mathscr{S}(F,k) = \mathscr{S}(F,Q+1) \subset \{A \in F[T] : (T^{Q^2}+T) \mid A^Q + A\}.$$

Conversely, let $X \in F[T]$ be such that $T^{Q^2}+T$ divides X^Q+X. From (5.1) and (5.3), X may be written as a sum

$$X = \sum_{r=0}^{Q-1} L_r(Y_r) + R \tag{1}$$

with $Y_1, \dots, Y_{Q-1}$, $R \in F[T]$ and

$$\deg R < Q^2. \tag{2}$$

By (4.5), for $r = 0, \dots, Q$, L_r is a sum of k-th powers and by Lemma 4.4, $\left(L_r(Y_r)\right)^Q + L_r(Y_r)$ is multiple of $T^{Q^2}+T$. By (1), R^Q+R is multiple of $T^{Q^2}+T$. From (2) and Proposition 4.5, R is a sum of k-th powers so that X is a sum of k-th powers. □

Lemma 5.3. *Let n be a positive integer and let $H \in F[T]$ be such that*

$$k(n-1) < \deg H \le kn. \tag{5.5}$$

In addition, in the case where $m = 2d$ and $\deg H = kn$, we suppose that the leading coefficient of H is a k-th power. Then we have

$$H = B_1^k + B_2^k + \sum_{i=0}^{Q-1} L_i(Y_i) + R, \tag{5.6}$$

where $B_1, B_2, Y_0, \dots, Y_{Q-1}$, $R \in F[T]$ with

$$\deg B_1, \deg B_2 \le n, \tag{5.7}$$

$$\deg Y_0, \dots, \deg Y_{Q-1} < n, \tag{5.8}$$

$$\deg R < Q^2, \tag{5.9}$$

$$R = \sum_{i=0}^{Q-1} \sum_{j=0}^{i} x_{Qj+i} T^{Qj+i}, \tag{5.10}$$

with $x_{Qj+i} \in F$ for all i and j.

Moreover, if $\deg H = kn$, and if either m divides $2d$, or m/d is odd, then $B_1 = 0$.

Proof. Suppose that $m/d \geq 3$. From Proposition 2.8, F is a k-Waring field with $\ell(2^m, k) \leq 2$, so that $\max(\ell(2^m, k) - 1, 1) = 1$. By [1], Lemma 5.1, there exist B_1, $P \in F[T]$ such that

$$H = B_1^k + P \tag{1}$$

with

$$\deg B_1 \leq n, \qquad \deg P = kn,$$

the leading coefficient of P being a k-th power.

Suppose that $m/d \leq 2$. From Proposition 2.8, if $m = d$, then F is a k-Waring field with $\ell(2^m, k) = 1$, so that the leading coefficient of H is a k-th power. If $m = 2d$ and if $\deg H = kn$, by hypothesis, the leading coefficient of H is a k-th power. Let $P \in F[T]$ be defined by

$$H = \varepsilon(H) T^{kn} + P, \tag{2}$$

where

$$\varepsilon(H) = \begin{cases} 0 & \text{if } \deg H = kn, \\ 1 & \text{if } \deg H < kn. \end{cases} \tag{3}$$

We note that the leading coefficient of P is a k-th power and that (1) is true with $B_1 = 0$ in the case where $\deg H = kn$.

By [1], Lemma 5.2, there exists B_2, $X \in F[T]$ such that

$$P = B_2^k + X, \qquad \deg X < (k-1)n = Qn, \ \deg B_2 = n. \tag{4}$$

By Proposition 5.1, there exist $Y_0, Y_1, \ldots, Y_{Q-1}$, $R \in F[T]$ such that

$$X = \sum_{i=0}^{Q-1} L_i(Y_i) + R, \tag{5}$$

with

$$\deg(Y_i) < n$$

for $0 \leq i < Q$,

$$\deg R < Q^2,$$

and R of the form

$$R = \sum_{i=0}^{Q-1} \sum_{j=0}^{i} x_{Qj+i} T^{Qj+i}.$$

We get (5.6) from (1), (4) and (5), the degree conditions (5.7) being satisfied. □

(AutoPDF V7 28/1/10 12:48) EMS (170×240mm) Tmath J-2232 PMS, 67:1 (idp) PMU:(KN/)7/1/2010 AC1: WSL 22/01/2010 pp. 13–56 2232_67-1_02 (p. 49)

We are now ready to present our second result.

Proposition 5.4. *Suppose that $m/d \geq 3$. Then the following holds:*

(I) *Every polynomial $H \in F[T]$ with degree $\geq k^3 - 2k^2 + 1$ is the strict sum of $3k + v(2^m, k) - 1$ k-th powers.*

(II) *Every polynomial $H \in F[T]$ with degree $\geq k^2 - 3k + 1$ is the strict sum of $(k-2)v(2^m, k) + 3k + \ell(2^m, k) - 1$ k-th powers. Moreover, if $H \in F[T]$ is such that $k^2 - 3k + 1 \leq \deg H \leq k^2 - 2k$, then H is the strict sum of $(k-2)v(2^m, k) + \ell(2^m, k)$ k-th powers.*

Proof. The last claim in (II) is given by Proposition 4.3 (III). We prove the other ones. Let $H \in F[T]$ and let n be the integer defined by

$$k(n-1) < \deg H \leq kn.$$

From (5.6)–(5.9),

$$H = B_1^k + B_2^k + \sum_{i=0}^{Q-1} L_i(Y_i) + R,$$

where $B_1, B_2, Y_0, \ldots, Y_{Q-1}, R \in F[T]$ with

$$\deg B_1, \deg B_2 \leq n, \qquad \deg Y_0, \ldots, \deg Y_{Q-1} < n, \tag{1}$$

$$\deg R < Q^2. \tag{2}$$

By (4.5),

$$L_i(Y_i) = (Y_i + T^i)^k + Y_i^k + (T^i)^k.$$

Thus,

$$H = B_1^k + B_2^k + \sum_{i=0}^{Q-1} \left((Z_{i,1})^k + (Z_{i,2})^k + (Z_{i,3})^k \right) + R, \tag{3}$$

with $Z_{i,1}$, $Z_{i,2}$, $Z_{i,3}$ polynomials such that

$$\deg Z_{i,1}, \deg Z_{i,2}, \deg Z_{i,3} \leq \max(i, n-1). \tag{4}$$

Set $v = v(2^m, k)$. Then there exist $a_1, b_1, \ldots, a_v, b_v$ in F such that

$$R = (a_1 R + b_1)^k + \cdots + (a_v R + b_v)^k. \tag{5}$$

By (3) and (5),

$$H = B_1^k + B_2^k + \sum_{i=0}^{Q-1}\big((Z_{i,1})^k + (Z_{i,2})^k + (Z_{i,3})^k\big)$$
$$+ (a_1R+b_1)^k + \cdots + (a_vR+b_v)^k, \tag{6}$$

so that H is a sum of $2+v+3Q$ k-th powers of polynomials. By (1), (2), (4) and (5), these polynomials have their degrees bounded by $\max(n, Q^2-1)$. If $n \ge Q^2-1$, then (6) is a strict sum. This proves (I).

By Proposition 4.3 (IV), since $\deg R < Q^2$, R is a sum of

$$s = (Q-1)v(2^m,k) + \ell(2^m,k)$$

k-th powers $V_1^k, \ldots, V_s^k$ with $\deg V_i \le Q-1$. Thus, by (3), H is a sum of $2+3Q+s = (k-2)v(2^m,k) + 3k + \ell(2^m,k) - 1$ k-th powers. If $n \ge Q-1$, this sum is strict. This proves (II). □

Proposition 5.5. (I) *If m divides r, then every $H \in \mathscr{S}(F,k)$ with degree multiple of k is a strict sum of $(3k-4)$ k-th powers.*

(II) *If m divides r, then every $H \in \mathscr{S}(F,k)$ with degree non multiple of k is a strict sum of $(3k-3)$ k-th powers.*

(III) *If $m/d = 2$ every $H \in \mathscr{S}(F,k)$ with degree multiple of k and whose leading coefficient is a k-th power in the field F is a strict sum of $(2k-1)$ k-th powers.*

(IV) *If If $m/d = 2$, every $H \in \mathscr{S}(F,k)$ of degree non multiple of k is a strict sum of $(2k)$ k-th powers.*

Proof. Suppose that $F \subset \mathbb{F}_{Q^2}$. Then m divides $2r$. If m does not divide r, then $m/d = 2$.

Let $H \in \mathscr{S}(F,k)$ be such that

$$k(n-1) < \deg H \le kn. \tag{1}$$

In addition, in the case where $m = 2d$ and $\deg H = kn$, we suppose that the leading coefficient of H is a k-th power. From (5.6)–(5.10),

$$H = B^k + Y^k + \sum_{i=0}^{Q-1} L_i(Y_i) + R$$

where $B, Y, Y_0, \ldots, Y_{Q-1}, R \in F[T]$ with

$$\deg B \le n, \qquad \deg Y = n, \tag{2}$$

$$\deg Y_0, \dots, \deg Y_{Q-1} < n, \tag{3}$$

$$R = \sum_{i=0}^{Q-1} \sum_{j=0}^{i} x_{Qj+i} T^{Qj+i}. \tag{4}$$

Moreover, from Lemma 5.3, if $\deg H = kn$, we have $B = 0$. In view of (4.5), $R + H$ is a sum of k-th powers. Since $H \in \mathcal{S}(F, k)$, R is also a sum of k-th powers. From (4) and Proposition 4.5(I), if $v \in \{0, \dots, Q^2 - 1\}$ is not multiple of $(Q+1)$, then $x_v = 0$, and if $v \in \{0, \dots, Q^2 - 1\}$ is multiple of $Q+1$, then $x_v \in F \cap \mathbb{F}_Q$. Thus,

$$H = B^k + Y^k + \sum_{i=0}^{Q-1} \bigl(L_i(Y_i) + x_{(Q+1)i} T^{(Q+1)i}\bigr) \tag{5}$$

with

$$x_{(Q+1)i} \in \mathbb{F}_Q \qquad \text{for } 0 \le i \le Q-1.$$

(A) Suppose that m divises r so that $F = \mathbb{F}_q \subset \mathbb{F}_Q$. Then for each $i = 0, \dots, Q-1$,

$$x_{(Q+1)i} = y_i^{Q+1}. \tag{6}$$

Let $u, v \in F$ be defined by

$$u^2 = x_{Q+1} + 1, \qquad v^2 = x_0 + 1 \tag{7}$$

and let

$$Z = Y + uT + v. \tag{8}$$

Observe that $u^Q = u$ and $v^Q = v$. Then

$$Z^k = Z^{Q+1} = Y^k + Y^Q(uT + v) + Y(uT^Q + v) + u^2 T^{Q+1} + uvT^Q + uvT + v^2.$$

From (5), (6) and (7), if $Q > 2$,

$$\begin{aligned} H = B^k + Z^k &+ \sum_{i=2}^{Q-1} \bigl(L_i(Y_i) + x_{(Q+1)i} T^{ki}\bigr) \\ &+ L_0(Y_0 + vY) + 1 + L_1(Y_1 + uY + uv) + T^k, \end{aligned}$$

and if $Q = 2$, then

$$H = B^k + Z^k + L_0(Y_0 + vY) + 1 + L_1(Y_1 + uY + uv) + T^k.$$

Suppose that $Q > 2$. Then by (6),

$$H = B^k + Z^k + \sum_{i=2}^{Q-1} \big(L_i(Y_i) + y_i^{(Q+1)i} T^{(Q+1)i}\big) + L_0(Y_0 + vY) + 1 + L_1(Y_1 + uY + uv) + T^{Q+1}. \tag{9}$$

Let $i = 2, \dots, Q-1$. From (4.5) or (4.7), according as $y_i = 0$ or $y_i \neq 0$, $L_i(Y_i) + y_i^{(Q+1)i} T^{(Q+1)i}$ is a sum of three or two k-th powers of polynomials. By (3), these polynomials have degree $\leq \mu = \max(n, Q-1)$. By (4.7), (2) and (3), $L_0(Y_0 + vY) + 1$ and $L_1(Y_1 + uY + uv) + T^k$ are also sums of two k-th powers of polynomials of degree $\leq \mu$.

By (9) and (2), H is a sum of $\big(\chi(H) + 3(Q-2) + 5\big)$ k-th powers of polynomials with degree bounded by μ with $\chi(H) = 0$ or 1 according as $\deg H = kn$ or $\deg H \neq kn$. In view of (1), when $n \geq Q-1$, this sum is strict. This remains true if $Q = 2$. Now, if $n < Q-1$, then $\deg H < Q^2 - 1$. From Proposition 4.5 (II), H is a strict sum of $(3Q-2)$ k-th powers.

(B) Suppose that $m = 2d$. Then Q is an odd power of q and $\mathbb{F}_{q^2} \subset F$. For $i = 0, \dots, Q-1$, we have $x_{(Q+1)i} \in \mathbb{F}_q$, so that there is $y_i \in \mathbb{F}_{q^2}$ such that $x_{(Q+1)i} = y_i + (y_i)^q = y_i + (y_i)^Q$. Thus, by (4.6), $L_i(Y_i) + x_{(Q+1)i} T^{(Q+1)i} = L_i(Y_i + y_i T^i)$. From (4.8) we get that $L_i(Y_i) + x_{(Q+1)i} T^{(Q+1)i}$ is sum of two k-th powers. By (5), H is a sum of $\big(\chi(H) + 2Q + 1\big)$ k-th powers. In the case where $n < Q-1$ we conclude with Lemma 4.4 and Proposition 4.5. □

Corollary 5.6. *Suppose that $k > 3$.*

(I) *Suppose that m does not divide $2r$. Then*

$$\mathscr{S}^*(F, k) = \mathscr{A}_0 \cup \mathscr{A}_\infty \cup \Big(\bigcup_{N=1}^{k-3} \mathscr{A}_N\Big)$$

where

$$\mathscr{A}_0 = F, \qquad \mathscr{A}_\infty = \{A \in F[T] : \deg A > k(k-3)\},$$

$$\mathscr{A}_N = \Big\{A \in F[T] : A = \sum_{n=0}^{N} \sum_{i=0}^{N} x_{n,i} T^{i+nQ}\Big\}$$

with $x_{n,i} \in F$. Moreover:

(AutoPDF V7 28/1/10 12:48) EMS (170×240mm) Tmath J-2232 PMS, 67:1 (idp) PMU:(KN)7/1/2010 AC1: WSL 22/01/2010 pp. 13–56 2232_67-1_02 (p. 53)

(i) *If* $m/d \geq 3$ *and* $m/d \neq 4$, *then*

$$G(2^m, k) = G^*(2^m, k) \leq 3k + 2.$$

(ii) *If* $m/d = 4$, *then*

$$G(2^m, k) = G^*(2^m, k) \leq 3k + 3.$$

(iii) *If* m/d *is odd and* > 1, *then*

$$g(2^m, k) = \infty, \qquad g^*(2^m, k) \leq 6k - 6.$$

(iv) *if* m/d *is even and* > 4, *then*

$$g(2^m, k) = \infty, \qquad g^*(2^m, k) \leq 6k - 5.$$

(v) *If* $m/d = 4$, *then*

$$g(2^m, k) = \infty, \qquad g^*(2^m, k) \leq 7k - 7.$$

(II) *Suppose that* m *divises* r. *Then*

$$\begin{aligned} \mathscr{S}^*(F, k) &= \mathscr{S}(F, k) = \{A \in F[T] : A^Q + A \equiv 0 \ (\mathrm{mod}\ T^{Q^2} + T)\}, \\ G(2^m, k) &= G^*(2^m, k) \leq 3k - 3, \\ g(2^m, k) &= g^*(2^m, k) \leq 3k - 3. \end{aligned}$$

(III) *Suppose that* $m/d = 2$. *Then*

$$\mathscr{S}(F, k) = \{A \in F[T] : A^Q + A \equiv 0 \ (\mathrm{mod}\ T^{Q^2} + T)\},$$

$\mathscr{S}^*(F, k)$ *is the set of* $A \in \mathscr{S}(F, k)$ *such that either* $\deg A$ *is not multiple of* k, *or* $\deg A$ *is multiple of* k *and the leading coefficient of* A *is in the field* $\mathbb{F}_q$,

$$G(2^m, k) = g(2^m, k) = \infty, \qquad G^*(2^m, k) \leq g^*(2^m, k) \leq 2k.$$

Proof. Apply Propositions 4.3, 4.5, Corollary 5.2, Propositions 5.4 and 5.5. □

Remarks. (1) In the case $Q = 2$, Proposition 5.5 gives $g(2, 3) \leq 6$, which is the upper bound proved in [8].

(2) In the case $Q = 4$, Corollary above gives $g(2, 5) \leq 12$, $g(4, 5) \leq 12$, $g(16, 5) = \infty$ and $g^*(16, 5) \leq 10$.

(3) For $k = 2^r$ tending to ∞, we have $G^*(2^m, k) \ll k$ as well as $g^*(2^m, k) \ll k$ unlike to the classical Waring numbers $G_{\mathbb{N}}(k)$ and $g_{\mathbb{N}}(k)$. Indeed, by [5] or [9], we have $g_{\mathbb{N}}(k) \gg 2^k$, while by [19], we have $G_{\mathbb{N}}(k) \ll k \log k$.

References

[1] M. Car, New bounds on some parameters in the Waring problem for polynomials over a finite field. In *Finite fields and applications*, Contemp. Math. 461, Amer. Math. Soc., Providence, RI, 2008, 59–77. Zbl 05575551 MR 2436325

[2] M. Car and L. Gallardo, Sums of cubes of polynomials. *Acta Arith.* **112** (2004), 41–50. Zbl 1062.11078 MR 2040591

[3] J. Chen, Waring's problem for $g(5) = 37$. *Sci. Sinica* **13** (1964), 1547–1568; also appeared as *Chinese Math.* **6** (1965), 105–127. Zbl 0146.27303 MR 0200236

[4] G. W. Effinger and D. R. Hayes, *Additive number theory of polynomials over a finite field*. Oxford Math. Monogr., The Clarendon Press, Oxford 1991. Zbl 0759.11032 MR 1143282

[5] W. J. Ellison, Waring's problem. *Amer. Math. Monthly* **78** (1971), 10–36. Zbl 0205.35001 MR 0414510

[6] L. Gallardo, On the restricted Waring problem over $\mathbb{F}_{2^n}[t]$. *Acta Arith.* **92** (2000), 109–113. Zbl 0948.11034 MR 1750311

[7] L. H. Gallardo, Every strict sum of cubes in $\mathbb{F}_4[t]$ is a strict sum of 6 cubes. *Port. Math.* **65** (2008), 227–236. MR 2428416

[8] L. Gallardo and D. R. Heath-Brown, Every sum of cubes in $\mathbb{F}_2[t]$ is a strict sum of 6 cubes. *Finite Fields Appl.* **13** (2007), 981–987. Zbl 1172.11045 MR 2360534

[9] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*. 4th ed., Oxford University Press, Oxford 1960. Zbl 0086.25803

[10] R. M. Kubota, Waring's problem for $\mathbf{F}_q[x]$. *Dissertationes Math.* (*Rozprawy Mat.*) **117** (1974). Zbl 0298.12008 MR 0376581

[11] Y.-R. Liu and T. D. Wooley, The unrestricted variant of Waring's problem in function fields. *Funct. Approx. Comment. Math.* **37** (2007), 285–291. Zbl 05257399 MR 2363827

[12] R. E. A. C. Paley, Theorems on polynomials in a Galois field. *Quart. J. Math. Oxford Ser.* **4** (1933), 52–63. JFM 59.0929.01 Zbl 0006.24703

[13] J.-P. Serre, Majorations de sommes exponentielles. Astérisque **41–42** (1977), 111–126. Zbl 0406.14014 MR 0447142

[14] C. Small, Sums of powers in large finite fields. *Proc. Amer. Math. Soc.* **65** (1977), 35–36. Zbl 0328.12016 MR 0485801

[15] L. N. Vaserstein, Waring's problem for algebras over fields. *J. Number Theory* **26** (1987), 286–298. Zbl 0624.10049 MR 901241

[16] L. N. Vaserstein, Ramsey's theorem and Waring's problem for algebras over fields. In *The arithmetic of function fields*, Ohio State Univ. Math. Res. Inst. Publ. 2, Walter de Gruyter, Berlin 1992, 435–442. Zbl 0817.12002 MR 1196531

[17] R. C. Vaughan and T. D. Wooley, Waring's problem: a survey. In *Number theory for the millennium III*, A K Peters, Natick, MA, 2002, 301–340. Zbl 1044.11090 MR 1956283

[18] W. A. Webb, Waring's problem in GF$[q, x]$. *Acta Arith.* **22** (1973), 207–220. Zbl 0258.12014 MR 0313190

[19] T. D. Wooley, Large improvements in Waring's problem. *Ann. of Math.* (2) **135** (1992), 131–164. Zbl 0754.11026 MR 1147960

Received November 26, 2008; revised April 4, 2009

Mireille Car, Laboratoire d'Analyse, Topologie, Probabilités UMR 6632, Université Paul Cézanne—Aix-Marseille III, Faculté des Sciences et Techniques, Avenue Escadrille Normandie-Niemen, 13397 Marseille Cedex 20, France

E-mail: mireille.car@univ-cezanne.fr