J. Korean Math. Soc. **49** (2012), No. 6, pp. 1139–1161
http://dx.doi.org/10.4134/JKMS.2012.49.6.1139

# SUMS OF $(p^r + 1)$-TH POWERS IN THE POLYNOMIAL RING $\mathbb{F}_{p^m}[T]$

Mireille Car

Abstract. Let $p$ be an odd prime number and let $F$ be a finite field with $p^m$ elements. We study representations and strict representations of polynomials $M \in F[T]$ by sums of $(p^r + 1)$-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 $k \deg M_i < k + \deg M$.

## 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 investigations of an analogue of the Waring problem for $F[T]$ (See [2], [6], [11], [14], [17], [19], [20], [21], [22] for general exponent $k$ or [4], [5], [8], [9], [10] for some particular exponents). Roughly speaking, Waring's problem over $F[T]$ is that of the representation of polynomials $M \in F[T]$ as sums

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

with $M_1, \ldots, M_s \in F[T]$. Some obstructions to that may occur which led to considering Waring's problem over the subring $\mathcal{S}(F, k)$ formed by the polynomials of $F[T]$ which are sums of $k$-th powers. Two variants of Waring's problem over $\mathcal{S}(F, k)$ have been considered. The unrestricted Waring's problem is the problem of proving the existence of an integer $w = w(p^m, k)$, with the property that whenever $M \in \mathcal{S}(F, k)$ and $s \geq w(p^m, k)$, the equation (1.1) is solvable. This problem is close to the so called easy Waring's problem for $\mathbb{Z}$ ([17], [18], [19], [20]). In order to have an analogue for the non easy Waring problem, the degree conditions

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

Received November 26, 2010; Revised July 8, 2012.
2010 *Mathematics Subject Classification.* Primary 11T55; Secondary 11R58.
*Key words and phrases.* finite fields, polynomials, Waring's problem.

©2012 The Korean Mathematical Society

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, analogues to the classical Waring's 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 $M \in \mathcal{S}(F, k)$, respectively, every polynomial $M \in \mathcal{S}(F, k)$ 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 $\infty$. This notation is possible since these numbers depend only on $p^m$ and $k$. Waring's problem consists of determining or, at least, bounding the numbers $g(p^m, k)$ and $G(p^m, k)$.

Gallardo's method introduced in [8] and performed in [5] to deal with Waring's problem for cubes was generalized in [2] and [11] where bounds for $g(p^m, k)$ and $G(p^m, k)$ were established when $p^m$ and $k$ satisfy some conditions. For instance, Theorem 1.2 in [2] and Theorem 1.4 in [11] require that every $a \in F$ is a sum of $k$-th powers and $p^m > k$. Theorem 1.3 in [2] gives a bound for the numbers $g(p^m, k)$ in the case where $p > k$ or in the case $k = hp^\nu - 1 < p^m$ for some positive integers $\nu$ and $h \leq p$.

The case of the exponent $k = p^r + 1$ is not covered by these theorems. The object of this paper is the study of Waring's problem in the case where $k = p^r + 1$ for odd $p$. It can be seen as a generalisation of [4] where sums of biquadrates over a field of characteristic 3 were studied. The easier case $p = 2$ has been studied in [3].

Some notations and definitions are necessary before stating the main results proved in this work.

The set $\mathcal{S}(F, k)$ and the numbers $g(p^m, k)$ and $G(p^m, k)$ are not sufficient to describe every possible case. Proposition 4.5 in [2] and Proposition 3.7 in [3] give examples of polynomials in $\mathcal{S}(F, k)$ which are not strict sums of $k$-th powers. Thus, we introduce new parameters.

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

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

From now on, $F$ is a finite field with $p^m$ elements. The main results proved in this work are summarized in the following theorems.

**Theorem 1.1.** *Let $k = p^r + 1$, where $p$ is an odd prime number and $r$ a positive integer.*

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

$$\mathcal{S}^{\times}(F,k) = \mathcal{A}_{\infty} \cup \left( \bigcup_{N=0}^{k-3} \mathcal{A}_N \right),$$

*where*

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

*and for $N = 1, \ldots, k-3$,*

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

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

(2) *If $m$ divides $r$,*

$$\mathcal{S}^{\times}(F,k) = \mathcal{S}(F,k) = \left\{ A \in F[T] \mid A^{p^r} - A \equiv 0 \pmod{T^{p^{2r}} - T} \right\}.$$

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

$$\mathcal{S}(F,k) = \left\{ A \in F[T] \mid A^{p^r} - A \equiv 0 \pmod{T^{p^{2r}} - T} \right\},$$

*and $\mathcal{S}^{\times}(F,k)$ is the set formed by the $A \in \mathcal{S}(F,k)$ 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 $p^{\gcd(m,r)}$.*

This theorem is a consequence of Corollary 3.3, Proposition 5.1, and Corollaries 5.4 and 5.6 below.

**Theorem 1.2.** *Let $k = p^r+1$, where $p$ is an odd prime number and $r$ a positive integer.*

(1) (a) *If $m/\gcd(m,r) \geq 3$, $m/\gcd(m,r) \neq 4$, and if $p^m$ is congruent to $1$ modulo $4$,*

$$G(p^m,k) = G^{\times}(p^m,k) \leq \min(\frac{\log k}{\log(k/(k-1))} + 5, 2k+3);$$

$$g^{\times}(p^m,k) \leq 5k-4.$$

(b) *If $m/\gcd(m,r) \geq 3$, and if $p^m$ is congruent to $3$ modulo $4$,*

$$G(p^m,k) = G^{\times}(p^m,k) \leq \min(\frac{\log k}{\log(k/(k-1))} + 6, 3k+3);$$

$$g^{\times}(p^m,k) \leq 6k-4.$$

(c) *If $m/\gcd(m,r) = 4$,*

$$G(p^m,k) = G^{\times}(p^m,k) \leq \min(\frac{\log k}{\log(k/(k-1))} + 6, 2k+4);$$

$$g^{\times}(p^m,k) \leq 6k-6.$$

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

(2) (a) *If $m$ divides $r$ and if $p^m$ is congruent to* 1 *modulo* 4*,*

$$G(p^m, k) = G^\times(p^m, k) \leq 2k;$$
$$g(p^m, k) = g^\times(p^m, k) \leq 3k - 6.$$

(b) *If $m$ divides $r$ and if $p^m$ is congruent to* 3 *modulo* 4*,*

$$G(p^m, k) = G^\times(p^m, k) \leq 3k;$$
$$g(p^m, k) = g^\times(p^m, k) \leq 3k.$$

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

$$G(p^m, k) = g(p^m, k) = \infty,$$
$$G^\times(p^m, k) \leq g^\times(p^m, k) \leq 2k.$$

This theorem is a consequence of Corollaries 3.5, 5.4 and 5.6 below. It shows that the analogy with the rational integers does not work completely since the following bounds hold for large exponents $k$:

$$G_{\mathbb{N}}(k) \leq k(\log k + \log(\log k) + O(1));$$

see [23] and

$$2^k + [(3/2)^k] - 2 \leq g_{\mathbb{N}}(k) \leq 2^k + [(3/2)^k] + [(4/3)^k] - 2$$

(see [7], [12, Chap. 21], [23]).

With the necessary adaptations, the proof follows the method used in [3] where we dealt with the case of characteristic 2. We omit the proofs in [3].

Let $v(p^m, k)$ denote the least integer $v$, if it exists, such that $T$ may be written as a sum $(a_1T + b_1)^k + \cdots + (a_vT + b_v)^k$ 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

$$P = (a_1P + b_1)^k + \cdots + (a_{v(F,k)}P + b_{v(F,k)})^k$$

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

As in the case $p = 2$, it is possible to compute the exact value of $v(p^m, p^r + 1)$. This improves a theorem of Paley [15].

The paper is organized as follows. In order to get the exact value of $v(p^m, k)$ 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 $v(p^m, k)$. This yields a characterization of the fields $F$ for which the equality $\mathcal{S}(F, k) = F[T]$ holds. Some bounds for the Waring numbers $G(p^m, k)$ follow. In Section 4, we prove some key identities and we classify strict sums of degree $\leq k(k-2)$. In Section 5, we describe a descent process and we conclude the proof. We shall use two types of numbering. Pairs $(X.Y)$ will be used to number formulae occurring in definitions, propositions and theorems, single numbers $(z)$ will be used for formulae only used in the course of a proof.

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 least integer $\ell$ such that every element of $F$ is a sum of $\ell$

$k$-th powers. We shall denote by $\lambda(p^m, k)$ the least integer $s$ such that $-1$ is a sum of $s$ $k$-th powers. We write $\Delta(p^m, k)$ for $\gcd(p^m-1, k)$.

We fix an algebraic closure $\overline{F}$ of the field $F$. For a positive integer $n$, we denote by $\mathbb{F}_{p^n}$ the subfield of $\overline{F}$ with $p^n$ elements, so that $F = \mathbb{F}_{p^m}$. The proofs will often use the following facts:

- the field $F$ contains exactly $\Delta(p^m, k) = \gcd(p^m-1, k) = \gcd(p^m-1, p^r+1)$ $k$-th roots of 1;
- a $k$-th power in $F$ is a $\gcd(p^m-1, k)$-th power.

We introduce the notations

$$Q = p^r = k-1, \quad q = p^{\gcd(m,r)}, \tag{1.4}$$

$$d = \gcd(m, r), \tag{1.5}$$

so that

$$q = p^d. \tag{1.6}$$

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

## 2. Sums of $k$-th powers in the finite field $F$

Since a $k$-th power in $F$ is a $\gcd(p^m-1, k)$-th power, we begin this section by computing $\Delta = \Delta(p^m, k)$. We continue by a study of a sum of characters which will be useful to compute numbers of solutions of some equations.

The following proposition completes Lemma 4 in [15]. It is a special case of exercise 125 in De Koninck and Mercier's book. See [13, exercise 125, p. 23, solution p. 125].

**Proposition 2.1.** *One has*

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

*The greatest common divisor of $p^m-1$ and $p^r+1$ is an even number. Moreover, $\gcd(p^m-1, p^r+1) \neq 2$ if and only if $m/d$ is even and, in that case,*

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

### 2.1. The systems $\mathcal{E}(u,v,a,b)$ and $\mathcal{S}(a,b,c)$

**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 $\mathcal{E}(u,v,a,b)$ :*

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

*admits a unique solution in $F^2$.*

*Proof.* Immediate. ☐

**Lemma 2.3.** *Let* $(a,b,c) \in F^3$. *Then, the system* $\mathcal{S}(a,b,c)$ :

$$\left\{\begin{array}{l} a = x^2 + y^2 + z^2, \\ b = x\xi + y\eta + z\zeta, \\ c = \xi^2 + \eta^2 + \zeta^2, \end{array}\right. \tag{2.4}$$

*has a solution* $(x,y,z,\xi,\eta,\zeta)$ *in* $F^6$.

*Proof.* Serre's theorem asserts that with the exceptions of polynomials of degree 3 and 4 in the case $q = 3$, every polynomial in $F[T]$ is a strict sum of 3 squares ([6, Theorem 1.14, p. 7]). Applied to $P = aT^2 + 2bT + c$, Serre's theorem gives the existence of $(x,y,z,\xi,\eta,\zeta) \in F^6$ such that

$$aT^2 + 2bT + c = (xT + \xi)^2 + (yT + \eta)^2 + (zT + \zeta)^2,$$

so that $(x,y,z,\xi,\eta,\zeta)$ is a solution of $\mathcal{S}(a,b,c)$. □

When $m/d$ is odd, $\gcd(2^m - 1, k) = 2$, and the set of $k$-th powers in $F$ is the set of squares, so that the numbers $\nu_i(a)$ of representations of $a \in F$ as sums of $i$ $k$-th powers are well known (see e.g. [1]). We compute the numbers $\nu_i(a)$ in the case where $m/d$ is even. For that we introduce some character sums.

### 2.2. Sums of characters

In this subsection, we suppose that $m/d$ is even, so that $\mathbb{F}_{q^2} \subset F$. From Proposition 2.1, the set of $k$-th powers in $F$, resp. in $\mathbb{F}_{q^2}$ is the set of $(q+1)$-th powers in $F$, resp. in $\mathbb{F}_{q^2}$. Let

$$n = m/2d. \tag{2.5}$$

Let $\theta$ be a generator of the cyclic group $\mathbb{F}_{q^2}^{\times}$ and let

$$\alpha = \theta^{(q+1)/2}. \tag{2.6}$$

Let tr: $F \mapsto \mathbb{F}_p$ be the absolute trace on $F$ and let $\psi$ be the character of the additive group of $F$ defined by

$$\psi(x) = \exp\left(\frac{2\pi i \operatorname{tr}(x)}{p}\right). \tag{2.7}$$

Then $\psi$ is not trivial. For $t \in F$ let

$$f(t) = \sum_{x \in F} \psi(tx^{q+1}). \tag{2.8}$$

Let $B$ denote the set of non-zero $k$-th powers in $F$ or, equivalently, the set of non-zero $(q+1)$-th powers in $F$.

**Proposition 2.4.** (1) *If* $u \in \mathbb{F}_{q^2}$, *then* $u^{q+1} \in \mathbb{F}_q$.

(2) *For every* $u \in \mathbb{F}_q$, *there is* $v \in \mathbb{F}_{q^2}$ *such that* $u = v^{q+1}$.

(3) *One has*

$$f(0) = p^m. \tag{2.9}$$

(4) *Let* $t \in F^{\times}$.

(a) *If* $t \in \alpha B$*, then*

$$f(t) = f(\alpha) = (-q)^{n+1}. \tag{2.10}$$

(b) *If* $t \notin \alpha B$*, then*

$$qf(t) + f(\alpha) = 0. \tag{2.11}$$

*Proof.* (1) If $u \in \mathbb{F}_{q^2}$, then $(u^{q+1})^{q-1} = u^{q^2-1} = 1$, so that $u^{q+1} \in \mathbb{F}_q$.

(2) Since $\theta$ generates $\mathbb{F}_{q^2}^\times$, the cyclic group $\mathbb{F}_q^\times$ is generated by $\theta^{q+1}$, so that every $u \in F_q^\times$ is a power of $\theta^{q+1}$.

(3) Obvious.

(4) It is a generalization of [4, Proposition 2.2]. See the proof of [3, Proposition 2.4(i)] and [3, Proposition 2.5] for the proof of (2.10); see the proof of [3, Proposition 2.4(iii)] for the proof of (2.11). □

## 2.3. Sums of $k$-th powers in $F$

Let $i$ be a positive integer. For $a \in F$, let $\nu_i(a)$ denote the number of solutions $(x_1, \dots, x_i) \in F^i$ of the equation

$$a = x_1^k + \cdots + x_i^k. \tag{2.12}$$

**Proposition 2.5.** *Suppose* $m/d$ *odd.*

- *If* $q \equiv 1 \pmod 4$*, then,*

$$\nu_2(0) = 2p^m - 1,$$
$$\nu_3(0) = p^{2m}$$

*and for* $a \in F^\times$*, one has*

$$\nu_2(a) = p^m - 1,$$
$$\nu_3(a) = \begin{cases} p^{2m} + p^m & \text{if} \quad a \in B, \\ p^{2m} - p^m & \text{if} \quad a \notin B. \end{cases}$$

- *If* $q \equiv 3 \pmod 4$*, then,*

$$\nu_2(0) = 1,$$
$$\nu_3(0) = p^{2m}$$

*and for* $a \in F^\times$*, one has*

$$\nu_2(a) = p^m + 1,$$
$$\nu_3(a) = \begin{cases} p^{2m} - p^m & \text{if} \quad a \in B, \\ p^{2m} + p^m & \text{if} \quad a \notin B. \end{cases}$$

*Proof.* Observe that $a \in F$ is a $k$-th power if and only if $a$ is a square. Apply the well-known results on sums of squares in a finite field, [1, exercise 5, pp. 175–176]. □

**Proposition 2.6.** *Suppose $m/d$ even. Then,*

$$\nu_2(0) = (q+1)p^m - q,$$

$$\nu_3(0) = p^{2m} + f(\alpha)(q-1)(p^m-1)$$

*and for $a \in F^\times$, one has*

$$\nu_1(a) = \begin{cases} q+1 & \text{if} \quad a \in B, \\ 0 & \text{if} \quad a \notin B, \end{cases}$$

$$\nu_2(a) = p^m - q + (q-1)f(a\alpha),$$

$$\nu_3(a) = p^{2m} - p^m + p^m\nu_1(a) - (q-1)f(\alpha) + (q-1)f(\alpha)f(a\alpha).$$

*Proof.* Similar to that of Proposition 2.7 in [3]. □

**Proposition 2.7.**
- *$F$ is a Waring field for the exponent $k = p^r + 1$ if and only if $\frac{m}{d} \neq 2$.*
- *If $\frac{m}{d} \neq 2$, then $\ell(p^m, k) = 2$.*

*Proof.* From Proposition 2.1, if $m/d$ is odd, then $\Delta(p^m, k) = 2$. From [2, Proposition 3.1], $F$ is a $k$-Waring field with $\ell(p^m, k) = 2$. Now, suppose $\frac{m}{d}$ even. Set $m = 2nd$. From Proposition 2.1, $\Delta(p^m, k) = 1 + p^d$. Since $\Delta(p^m, k) > 1$, we have $\ell(2^m, k) \geq 2$. We prove that, with the exception $n = 1$, $F$ is a $k$-Waring field with $\ell(p^m, k) \leq 2$. Let $a \in F$ be different from a $k$-th power. From Proposition 2.6, then Proposition 2.4,

$$\nu_2(a) = p^m - q + (q-1)f(a\alpha) \geq p^m - q - (q-1)p^{m/2} = q^{2n} - q - q^{n+1} + q^n.$$

If $n > 1$, then $\nu_2(a) > 0$ and $a$ 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, $\ell(p^m, k) = \ell(F, k) \leq 2$ (Note that Small had already established this bound in the case where $m > 4r$, [16]). □

*Remark* 2.8. We have $\lambda(p^m, k) = 1$ if and only if $p^m$ is congruent to 1 modulo 4.

*Proof.* If $\lambda(p^m, k) = 1$, then $-1$ is a $k$-th power in $F$, so that $-1$ is a square in $F$. Now, we suppose that $-1$ is a square in $F$. Firstly, we suppose $m/d$ odd. From Proposition 2.1, the set of $k$-th powers in $F$ is the set of squares in $F$, so that $-1$ is a $k$-th power in $F$. Secondly, suppose $m/d$ even. Then, $\mathbb{F}_{q^2} \subset F$. Since $\theta$ generates the cyclic group $\mathbb{F}_{q^2}$, we have

$$-1 = \theta^{(q^2-1)/2} = (\theta^{(q-1)/2})^{q+1}$$

with $\theta \in \mathbb{F}_{q^2} \subset F$. From Proposition 2.1, the set of $k$-th powers in $F$ is the set of $(q+1)$-th powers in $F$. Therefore $-1$ is a $k$-th power in $F$. □

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

$$(\mathcal{F}(a)) \qquad \begin{cases} x^k + y^k + z^k = a, & (e_1) \\ xy \neq 0, & (e_2) \\ x^{Q^2-1} \neq y^{Q^2-1}. & (e_3) \end{cases}$$

- *Suppose $m/d$ even. Then,*

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

*and for $a \in F^\times$, one has*

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

*where $\alpha$ is as in (2.6) and $f$ as in (2.8).*

- *Suppose $m/d$ odd. Then,*

$$N_3(0) = (p^m-1)(p^m-q)$$

*and for $a \in F^\times$,*

$$N_3(a) = \begin{cases} (p^m-2)(p^m-q) & \text{if} \quad a \in B, \\ p^m(p^m-q) & \text{if} \quad a \notin B. \end{cases}$$

*Proof.* The proof is a generalization of the proof of Proposition 2.6 in [4]. In the case of [4], $p=3$ and $k=4$, so that the proof only needs to distinguish two cases depending on the parity of $m$ . In the present general setting we have to distinguish different cases according to whether or not $F$ contains $\mathbb{F}_{q^2}$, and according to whether or not $-1$ is a $k$-th power in $F$. □

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

1. *If $a \neq 0$ and $m/d \geq 3$, or if $a = 0$ and $m/d \geq 3$ with $m/d \neq 4$, then $(\mathcal{F}(a))$ has solutions in $F^3$.*
2. *If $m/d \leq 2$, for any $a \in F$,$(\mathcal{F}(a))$ has no solutions in $F^3$.*
3. *Suppose $m = 4d$. Then $(\mathcal{F}(0))$ has no solutions in $F^3$. Let $a \in F$. Then, there exists $(x,y,z,u) \in F^4$ such that*

$$(\mathcal{G}(a)) \qquad \begin{cases} x^k + y^k + z^k + u^k = a, & (e_1) \\ xy \neq 0, & (e_2) \\ x^{Q^2-1} \neq y^{Q^2-1}. & (e_3) \end{cases}$$

*Proof.* If $m/d \leq 2$, then $F \subset \mathbb{F}_{q^2}$, so that $(e_3)$ is not satisfied in $F$. This proves the second claim. We prove the other claims.

(A) Suppose $m/d$ even, say $m = 2nd$ with $n > 1$. From Proposition 2.9,

$$N_3(0) = q^{4n} - q^{2n}(q^3+1) + q^3 + (q-1)(q^{2n}-1)f(\alpha).$$

By (2.10),

$$N_3(0) = q^{4n} - q^{2n}(q^3+1) + q^3 + (q-1)(q^{2n}-1)(-q)^{n+1}.$$

If $n > 2$, then $N_3(0) > 0$, so that $(\mathcal{F}(0))$ has a solution. If $n = 2$, then $N_3(0) = 0$, so that $(\mathcal{F}(0))$ has no solutions. Let $a \in B$. From Propositions 2.9 and 2.4,

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

Thus, $(\mathcal{F}(a))$ has a solution. Let $a \in F^\times \setminus B$. From Propositions 2.4 and 2.9,

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

If $n \geq 2$, then $N_3(a) > 0$. Thus, $(\mathcal{F}(a))$ has a solution. Suppose $n = 2$. If $a \neq 0$, for every $(x, y, z)$ solution of $(\mathcal{F}(a))$, $(x, y, z, 0)$ is a solution of $(\mathcal{G}(a))$; if $a = 0$, for every $(x, y, z)$ solution of $(\mathcal{F}(-1))$, $(x, y, z, 1)$ is a solution of $(\mathcal{G}(a))$.

(B) Suppose $m/d$ odd. From Proposition 2.9, $N_3(a) > 0 \Leftrightarrow m > d$. Thus $(\mathcal{F}(a))$ has a solution if and only if $m/d > 1$. □

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

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

*Proof.* Similar to the proof of Proposition 3.1 in [3]. □

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

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

*Proof.* If $m/d \notin \{1, 2, 4\}$, Corollary 2.10 implies the existence of $(a_1, a_2, a_3) \in F^3$ solution of $(\mathcal{F}(0))$. If $m/d = 4$, Corollary 2.10 implies the existence of $(a_1, a_2, a_3, a_4) \in F^4$ solution of $(\mathcal{G}(0))$. Let $(b_1, b_2) \in F^2$ be a solution of $(\mathcal{E}(a_1, a_2, 0, 1))$, with $(\mathcal{E})$ defined by (2.3). As for the proof of Proposition 3.2 in [3], we get:

(1) If $m/d \notin \{1, 2, 4\}$, then

$$(a_1T + b_1)^k + (a_2T + b_2)^k + (a_3T)^k = T + (b_1)^k + (b_2)^k,$$

so that $T$ is a sum of three $k$-th powers of linear polynomials.

(2) If $m/d = 4$, then

$$(a_1T + b_1)^k + (a_2T + b_2)^k + (a_3T)^k + (a_4T)^k = T + (b_1)^k + (b_2)^k,$$

so that $T$ is a sum of four $k$-th powers of linear polynomials.

In the first case, Proposition 3.1 gives $v(p^m, k) = 3$. In the second case, we have $v(p^m, k) \leq 4$. We end the proof by proving that $v(p^m, k) > 3$ as we did in the proof of Proposition 3.2 in [3]. □

**Corollary 3.3.** *We have* $\mathcal{S}(F,k)=F[T]$ *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 a sum of four* $k$*-th powers.*

We are ready to present our first result.

**Proposition 3.4.** *Assume that* $m$ *does not divide* $2r$. *Let*

$$\gamma(m)=\begin{cases}2 & \text{if}\quad p^m\equiv 1 \pmod 4,\\ 3 & \text{if}\quad p^m\equiv 3 \pmod 4.\end{cases} \tag{3.1}$$

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

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

(2) *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 a strict sum of* $s+\gamma(m)+v(p^m,k)$ $k$*-th powers.*

(3) *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* $s+\gamma(m)+v(p^m,k)$ $k$*-th powers.*

*Proof.* From Propositions 2.7 and 3.2, $F$ is a $k$-Waring field and $v(p^m,k)$ is finite. Let $w(m,k)=v(p^m,k)+\max(\ell(p^m,k),1+\lambda(p^m,k))$. From [2, Proposition 5.3], we have the following facts:

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

(2) 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.

(3) 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 2.7, $\ell(2^m,k)=2$. From Remark 2.8, $\lambda(p^m,k)=1$ or 2 according as $p^m\equiv 1$ or 3 (mod 4), so that, with (3.1), $w(m,k)=v(p^m,k)+\gamma(m)$. □

**Corollary 3.5.** (1) *Suppose* $p^m\equiv 1 \pmod 4$.

(a) *If either,* $m/d$ *is odd and* $m\notin\{1,r\}$, *or, if* $m/d$ *is even and* $m/d>4$, *then* $G(p^m,k)\leq[\frac{\log k}{\log(k/(k-1))}]+5\leq k\log k+5$.

(b) *If* $m/d=4$, *then* $G(p^m,k)\leq[\frac{\log k}{\log(k/(k-1))}]+6\leq k\log k+6$.

(2) *Suppose* $p^m\equiv 3 \pmod 4$. *If* $m\notin\{1,r\}$, *then* $G(p^m,k)\leq[\frac{\log k}{\log(k/(k-1))}]+6\leq k\log k+6$.

*Proof.* Apply the first of part of the previous proposition. □

The following proposition gives an example of an infinite sequence of polynomials which are sums of $k$-th powers and not strict sums of $k$-th powers.

**Proposition 3.6.** *Suppose $m = 2d$. 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 a sum of three $k$-th powers and is not a strict sum of $k$-th powers.*

*Proof.* Similar to the proof of Proposition 3.7 in [3]. □

**Corollary 3.7.** *If $m/d = 2$, then $G(p^m, k) = \infty$.*

## 4. Strict sums of degree $\leq k(k-2)$

The two following propositions form the key of the proof.

**Proposition 4.1.** *For $i \in \{0, \dots, Q-1\}$ and $X \in F[T]$ let*

$$L_i(X) = X^Q T^i + XT^{Qi}. \tag{4.1}$$

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

$$L_i(X) = (X + \frac{1}{2}T^i)^{Q+1} - (X - \frac{1}{2}T^i)^{Q+1}. \tag{4.2}$$

*For every $b \in F$,*

$$L_i(X + bT^i) = L_i(X) + (b^Q + b)T^{i(Q+1)}. \tag{4.3}$$

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

$$L_i(X) + c^{Q+1}T^{(Q+1)i} = \left(\frac{1}{c^Q}X + cT^i\right)^{Q+1} - \left(\frac{1}{c^Q}X\right)^{Q+1}. \tag{4.4}$$

*Proof.* The proof of (4.2) and (4.3) is immediate. We get (4.4) from observing that $c^{Q^2} = c$. □

**Proposition 4.2.** *Suppose $F = \mathbb{F}_q$.*

(1) *For every $(a, b, c) \in F^3$, the polynomial $c + bT + bT^Q + aT^{Q+1}$ is a strict sum of three $k$-th powers.*

(2) *Let $c \in F$. There exists $(\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3) \in F^6$ such that for $i \in \{0, \dots, Q-1\}$ and $X \in F[T]$,*

$$L_i(X) + cT^{(Q+1)i} = (\alpha_1 X + \beta_1 T^i)^k + (\alpha_2 X + \beta_2 T^i)^k + (\alpha_3 X + \beta_3 T^i)^k. \tag{4.5}$$

*Proof.* (1) Let $(a, b, c) \in F^3$ and let

$$A = a + bT + bT^Q + cT^{Q+1}.$$

From Lemma 2.3, there is $(x,y,z,\xi,\eta,\zeta)\in F^6$ such that

$$(\dagger)\qquad \begin{cases} a = x^2+y^2+z^2,\\ b = x\xi+y\eta+z\zeta,\\ c=\xi^2+\eta^2+\zeta^2.\end{cases}$$

Since $F\subset \mathbb{F}_Q$, for every $u\in F$, we have $u^Q=u$, so that,

$$\begin{cases} a = x^{Q+1}+y^{Q+1}+z^{Q+1},\\ b = x^Q\xi+y^Q\eta+z^Q\zeta,\\ c=\xi^{Q+1}+\eta^{Q+1}+\zeta^{Q+1}.\end{cases}$$

Hence,

$$a+bT+bT^Q+cT^{Q+1}=(x+\xi T)^{Q+1}+(y+\eta T)^{Q+1}+(z+\zeta T)^{Q+1},$$

so that $A$ is a strict sum of three $k$-th powers.

(2) Apply $(\dagger)$ with $a=0,b=1$. There exists $(\alpha_1,\alpha_2,\alpha_3,\beta_1,\beta_2,\beta_3)\in F^6$ such that

$$\begin{cases} \alpha_1^k+\alpha_2^k+\alpha_3^k=0,\\ \alpha_1^Q\beta_1+\alpha_2^Q\beta_2+\alpha_3^Q\beta_3=\alpha_1\beta_1^Q+\alpha_2\beta_2^Q+\alpha_3\beta_3^Q=1,\\ \beta_1^k+\beta_2^k+\beta_3^k=c.\end{cases}$$

Thus,

$$(\alpha_1X+\beta_1T^i)^k+(\alpha_2X+\beta_2T^i)^k+(\alpha_3X+\beta_3T^i)^k=cT^{(Q+1)i}+X^QT^i+XT^{Qi}.$$

□

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

- *Let $0<N<k-2$ and let*

  $$A=\sum_{n=0}^{kN}a_nT^n$$

  *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, $\mathcal{S}(F,k)\neq\mathcal{S}^\times(F,k)$ and $g(p^m,k)=\infty$.*
- *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.*
- *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 $v(p^m,k)\lceil\frac{\deg A}{k}\rceil+2$ $k$-th powers of polynomials of degree $\leq k-2$.*

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

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

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

*Proof.* The proof is similar to that of Proposition 4.3 in [3]. It makes use of Lemma 2.2 and Corollary 2.10 as the proof of Proposition 4.3 in [3] makes use of Lemma 2.2 and Corollary 2.10 in [3]. □

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

*Proof.* As for Lemma 4.4 in [3]. □

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

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

*be a polynomial of $F[T]$ with $\deg A < Q^2$ and such that $T^{Q^2} - T$ divides $A^Q - A$.*

- *For every $n = Qj + i$ with $0 \leq j < Q, 0 \leq i < Q$, one has*

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

  *where $\bar{n} = Qi + j$.*
- *For every $n = kj$ with $0 \leq j \leq Q-1$, $a_n \in F \cap \mathbb{F}_Q$.*
- *If $\deg A \leq Q+1$, then $A$ is a strict sum of three $k$-th powers.*
- (A) *If $F \subset \mathbb{F}_Q$ and $Q+1 < \deg A < Q^2$, then $A$ is a strict sum of $3k-6$ $k$-th powers.*

  (B) *If $F \not\subset \mathbb{F}_Q$ and $Q+1 < \deg A < Q^2$, then $A$ is a strict sum of $2k-3$ $k$-th powers (If, in addition, $k$ divides $\deg A$, then $a_{\deg A} \in \mathbb{F}_q$).*

*Proof.* Making use of Lemma 4.4, the proof of the first part is similar to that of Proposition 4.5-(I) in [3]. Let $n = kj$ with $0 \leq j \leq Q-1$. Then $\bar{n} = n$, so that $a_n \in F_Q$. Let $0 \leq i, j < Q$ and let $n = Qj + i \leq Q^2 - 2$ be non divisible by $Q+1$. Then

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

so that,

$$\begin{aligned} A &= \sum_{i=0}^{Q-1} a_{(Q+1)i} T^{(Q+1)i} + \sum_{i=0}^{Q-2} \sum_{j=i+1}^{Q-1} L_i(a_{Qi+j} T^j) \\ &= \sum_{i=0}^{Q-1} a_{(Q+1)i} T^{(Q+1)i} + \sum_{j=1}^{Q-1} \sum_{i=0}^{j-1} L_j(a_{Qj+i} T^i). \end{aligned} \tag{1}$$

(A) Suppose $F \subset \mathbb{F}_Q$, that is $F = \mathbb{F}_q$. Firstly, we suppose $\deg A \leq Q+1$. Then,

$$A = a + bT + bT^Q + cT^{Q+1}$$

with $a, b, c \in F$. From Proposition 4.2, $A$ is a strict sum of three $k$-th powers. This proves the second part.

Now, we suppose $Q+1 < \deg A \leq Q^2 - 1$. By (1),

$$A = a_0 + L_1(a_Q) + a_{Q+1}T^{Q+1} + \sum_{j=2}^{Q-1}(a_{(Q+1)j}T^{(Q+1)j} + L_j(B_j))$$

with

$$B_j = \sum_{i=0}^{j-1} a_{Qj+i}T^i. \tag{2}$$

From Proposition 4.2, for every $j = 2, \ldots, Q-1$, there exist $(\alpha_{j,1}, \alpha_{j,2}, \alpha_{j,3}, \beta_{j,1}, \beta_{j,2}, \beta_{j,3}) \in F^6$ such that

$$a_{(Q+1)j}T^{(Q+1)j} + L_j(B_j) = \sum_{\nu=1}^{3}(\alpha_{j,\nu}B_j + \beta_{j,\nu})^k. \tag{3}$$

Thus, $B = A - (a_0 + L_1(a_Q) + a_{Q+1}T^{Q+1})$ is a sum of $3(Q-2)$ $k$-th powers. From Lemma 4.4, $B^Q - B$ is divisible by $T^{Q^2} - T$, so that, $(a_0 + L_1(a_Q) + a_{Q+1}T^{Q+1})^Q - (a_0 + L_1(a_Q) + a_{Q+1}T^{Q+1})$ is divisible by $T^{Q^2} - T$. Since $\deg(a_0 + L_1(a_Q) + a_{Q+1}T^{Q+1}) \leq Q+1$, $a_0 + L_1(a_Q) + a_{Q+1}T^{Q+1}$ is a strict sum of three $k$-th powers. Thus, by (3), $A$ is a sum of $3 + 3(Q-2)$ $k$-th powers.

We consider the degrees. Suppose that

$$\deg A = (Q+1)N - \rho. \tag{4}$$

with

$$0 \leq \rho \leq Q. \tag{5}$$

Observe that

$$N < Q. \tag{6}$$

Let $j \in \{2, \ldots, Q-1\}$ be such that $j > N$. Then, $(Q+1)j > (Q+1)N - \rho$, so that $a_{(Q+1)j} = 0$. We have $Qj + i \geq (Q+1)N + Q - N + i > (Q+1)N - \rho$, so that $a_{Qj+i} = 0$. Hence, $B_j = 0$. Thus, the $(\alpha_{j,\nu}B_j + \beta_{j,\nu})$ occurring in (3) are zero polynomials. If $2 \leq j \leq N$, then by (2), $\deg B_j \leq N$. Thus, the sum (3) is a strict one.

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

$$a_{(Q+1)j} = b_j^q + b_j.$$

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

$$a_{(Q+1)j} = b_j^Q + b_j.$$

Moreover, from Proposition 2.4, each $x \in \mathbb{F}_q$ is a $(q+1)$-th power, so that there is $c_j \in F$ such that $a_{(Q+1)j} = (c_j)^k = (c_j)^{Q+1}$.

Suppose $\deg A \leq Q+1$. Then

$$A = b_0 + b_0^Q + L_0(a_1 T) + (c_1 T)^{Q+1}.$$

By (4.3),

$$A = L_0(a_1 T + b_0) + (c_1 T)^{Q+1},$$

then by (4.2),

$$A = (a_1 T + b_0 + \frac{1}{2})^{Q+1} - (a_1 T + b_0 - \frac{1}{2})^{Q+1} + (c_1 T)^{Q+1}. \tag{7}$$

Suppose $\deg A > Q+1$. Then,

$$\begin{aligned} A &= c_0^{Q+1} + \sum_{j=1}^{Q-1} \left( \left( b_j^Q + b_j \right) T^{j(Q+1)} + \sum_{i=0}^{j-1} L_j(a_{Qj+i} T^i) \right) \\ &= c_0^{Q+1} + \sum_{j=1}^{Q-1} \left( \left( b_j^Q + b_j \right) T^{j(Q+1)} + L_j(B_j) \right), \end{aligned}$$

with $B_j$ defined by (2). By (4.3),

$$A = c_0^{Q+1} + \sum_{j=1}^{Q-1} L_j \left( B_j + b_j T^j \right).$$

Then, by (4.2),

$$A = c_0^k + \sum_{j=1}^{Q-1} \left( (B_j + b_j T^j + \frac{1}{2} T^j)^k - (B_j + b_j T^j - \frac{1}{2} T^j)^k \right). \tag{8}$$

From Remark 2.8, $-1$ is a $k$-th power, so that (7) is a sum of three $k$-th powers and (8) is a sum of $(1 + 2(Q-1))$ $k$-th powers. We observe that (7) is a strict sum and we finish the proof, proving as above that (8) is a strict sum. □

## 5. The descent process

In this section, we use the descent process already used in [3] and [4].

**Proposition 5.1.** *Suppose $F \subset \mathbb{F}_{Q^2}$. Then $\mathcal{S}(F, k)$ is the subset of $F[T]$ formed by the polynomials $A$ such that $T^{Q^2} - T$ divides $A^Q - A$.*

*Proof.* The proof is similar to those of Proposition 5.1 and Corollary 5.2 in [3]. □

**Lemma 5.2.** *Let $n$ be a positive integer and let $H \in F[T]$ be such that*

$$k(n-1) < \deg H \leq kn. \tag{5.1}$$

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

$$H = \sum_{i=1}^{1+\lambda} B_i^k + \sum_{i=0}^{Q-1} L_i(Y_i) + R, \tag{5.2}$$

*with $\lambda = \lambda(p^m, k)$ and where $B_1, \ldots, B_{\lambda+1}, Y_0, \ldots, Y_{Q-1}, R \in F[T]$ with*

$$\deg B_1, \ldots, \deg B_{\lambda+1} \leq n, \tag{5.3}$$

$$\deg Y_0, \ldots, \deg Y_{Q-1} < n, \tag{5.4}$$

$$\deg R < Q^2, \tag{5.5}$$

$$R = \sum_{i=0}^{Q-1} \sum_{j=0}^{i} x_{Qj+i} T^{Qj+i}, \tag{5.6}$$

*with $x_{Qj+i} \in F$ for all $i$ and $j$. Moreover, if $\lambda(p^m, k) = 2$ and $\deg H = kn$, or if $m = 2d$ and $\deg H = kn$, then $B_1 = 0$.*

*Proof.* (I) Suppose $m \neq 2d$. From Proposition 2.7, $F$ is a $k$-Waring field with $\ell(p^m, k) = 2$, so that $\max(\ell(p^m, k) - 1, \lambda(p^m, k)) = \lambda(p^m, k) = \lambda$. From [2, Lemma 5.1], there exist $B_1, \ldots, B_\lambda, P \in F[T]$ such that

$$H = B_1^k + \cdots + B_\lambda^k + P, \tag{1}$$

with

$$\deg B_1, \ldots, \deg B_\lambda \leq n, \quad \deg P = kn,$$

the leading coefficient of $P$ being a $k$-th power. Observe that in the case when $\deg H = kn$, the leading coefficient of $H$ is a sum of two $k$-th powers, so that, when $\lambda = 2$ and $\deg H = kn$, in (1), we can take $B_1 = 0$.

(II) Suppose $m = 2d$. From Remark 2.8, $-1$ is a $k$-th power in $\mathbb{F}_{q^2} = F$, say $-1 = b^k$. Thus $\lambda = 1$. If $\deg H < kn$, then

$$H = -T^{kn} + P,$$

with $P$ monic of degree $kn$, so that (1) is true with $\lambda = 1$ and $B_1 = bT^n$. If $\deg H = kn$, the hypothesis insures that (1) is true with $B_1 = 0$.

Ending the proof as for Lemma 5.3 in [3], we get the identity (5.2) with degree conditions (5.3)-(5.5). □

We are now ready to present our second result.

**Proposition 5.3.** *Suppose that $m/d \geq 3$. Then*:

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

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

*Proof.* The last claim is given by the third part of Proposition 4.3. We prove the other ones. Set $\lambda = \lambda(p^m, k)$. Let $H \in F[T]$ and let $n$ be the integer such that

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

From Lemma 5.2,

$$H = \sum_{i=1}^{1+\lambda} B_i^k + \sum_{i=0}^{Q-1} L_i(Y_i) + R, \tag{2}$$

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

$$\deg B_1, \ldots, \deg B_{1+\lambda} \leq n, \tag{3}$$

$$\deg Y_0, \ldots, \deg Y_{Q-1} < n, \tag{4}$$

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

By (4.2),

$$L_i(Y_i) = (Y_i + \frac{1}{2}T^i)^k - (Y_i - \frac{1}{2}T^i)^k.$$

Since $-1$ is a sum of $\lambda$ $k$-th powers, for each index $i = 0, \ldots, Q-1$, there is $Z_{i,1}, \ldots, Z_{i,1+\lambda} \in F[T]$, such that

$$L_i(Y_i) = (Z_{i,1})^k + (Z_{i,2})^k + \cdots + (Z_{i,1+\lambda})^k, \tag{6}$$

and such that

$$\deg Z_{i,j} \leq \max(i, n-1). \tag{7}$$

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

$$R = (a_1 R + b_1)^k + \cdots + (a_v R + b_v)^k. \tag{8}$$

By (2), (6) and (8),

$$H = \sum_{i=1}^{1+\lambda} B_i^k + \sum_{i=0}^{Q-1} \left((Z_{i,1})^k + \cdots + (Z_{i,1+\lambda})^k\right)$$
$$+ (a_1 R + b_1)^k + \cdots + (a_v R + b_v)^k,$$

so that $H$ is a sum of $((\lambda+1)(Q+1) + v)$ $k$-th powers of polynomials. By (3), (4), (5), (7) and (8), these polynomials have their degrees bounded by $\max(n, Q^2 - 1)$. In view of (1), if $n \geq Q^2 - 1$, the above sum is a strict one. This proves the first part.

We have $\deg R < Q^2$. From the fourth part of Proposition 4.3, $R$ is a sum of

$$s = (k-2)v(p^m, k) + 2$$

$k$-th powers of polynomials of degree $\le Q-1$. Thus by (2) and (6), $H$ is a sum of

$$k(\lambda+1) + s = (k-2)v(p^m, k) + k(\lambda+1) + 2$$

$k$-th powers of polynomials of degree $\le \max(n, Q-1)$. In view of (1), if $n \ge Q-1$, the sum is a strict representation. This proves the second part. $\square$

**Corollary 5.4.** *Suppose that $m/d \ge 3$. Then,*

$$\mathcal{S}^\times(p^m, k) = \mathcal{A}_\infty \cup \left( \bigcup_{N=0}^{k-3} \mathcal{A}_N \right),$$

*where*

$$\begin{aligned} \mathcal{A}_\infty &= \{A \in F[T] \mid \deg A > k(k-3)\}, \\ \mathcal{A}_0 &= F, \end{aligned}$$

*and for $N = 1, \dots, k-3$,*

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

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

(1) *if $p^m$ is congruent to 1 modulo 4 and $m/d \neq 4$,*

$$G(p^m, k) = G^\times(p^m, k) \le 2k+3;$$

(2) *if $p^m$ is congruent to 3 modulo 4,*

$$G(p^m, k) = G^\times(p^m, k) \le 3k+3;$$

(3) *if $m/d = 4$,*

$$G(p^m, k) = G^\times(p^m, k) \le 2k+4;$$

(4) *if $p^m$ is congruent to 1 modulo 4 and $m/d \neq 4$,*

$$g(p^m, k) = \infty, \quad g^\times(p^m, k) \le 5k-4;$$

(5) *if $p^m$ is congruent to 3 modulo 4,*

$$g(p^m, k) = \infty, \quad g^\times(p^m, k) \le 6k-4;$$

(6) *if $m/d = 4$,*

$$g(p^m, k) = \infty, \quad g^\times(p^m, k) \le 6k-6.$$

*Proof.* The first assertion is given by Propositions 4.3 and 5.3. From Corollary 3.3, $\mathcal{S}^\times(p^m,k) \neq \mathcal{S}(p^m,k)$, so that $g(p^m,k) = \infty$. The bounds for $G(p^m,k)$ are obtained by noting that from Proposition 2.7, $\lambda(p^m,k) \in \{1,2\}$ and from Remark 2.8, $\lambda(p^m,k) = 1$ when $p^m$ is congruent to 1 modulo 4. We deduce from Propositions 4.3 and 5.3 that

$$g^\times(p^m,k) \leq (k-2)v(p^m,k) + k(\lambda(p^m,k)+1) + 2.$$

Bounds for $g^\times(p^m,k)$ in parts $4-6$ are given by Propositions 3.4, 4.3 and 5.3. □

*Remark* 5.5. If $k \geq 20$, or if $k = 18, 14$, for all $m$, the bounds for the numbers $G(p^m,k)$ given by this corollary are better than those given by Corollary 3.5; if $k = 4, 6$, the old bounds are better in all cases. If $k = 12, 10, 8$, the new bounds are better when $m/d$ is even.

**Proposition 5.6.** *Suppose $m/d \leq 2$.*

(A) (a) *If $m = d$ and if $p^m$ is congruent to* 1 *modulo* 4*, every $H \in \mathcal{S}(F,k)$ with degree $\geq k^2 - 3k + 1$ is a strict sum of $2k$ $k$-th powers.*

(b) *If $m = d$ and if $p^m$ is congruent to* 3 *modulo* 4*, every $H \in \mathcal{S}(F,k)$ with degree multiple of $k$ is a strict sum of $3k-1$ $k$-th powers; every $H \in \mathcal{S}(F,k)$ with degree non multiple of $k$ is a strict sum of $3k$ $k$-th powers.*

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

*Proof.* Let $H \in \mathcal{S}(F,k)$ be such that

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

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

We have

$$H = \sum_{i=1}^{1+\lambda} B_i^k + \sum_{i=0}^{Q-1} L_i(Y_i) + R, \tag{2}$$

where $B_1, \ldots, B_{1+\lambda}, Y_0, \ldots, Y_{Q-1}, R \in F[T]$ are as in Lemma 5.2, so that

$$R = \sum_{i=0}^{Q-1} \sum_{j=0}^{i} x_{Qj+i} T^{Qj+i}. \tag{3}$$

In view of (4.2), $H - R$ is a sum of $k$-th powers. Since $H \in \mathcal{S}(F,k)$, $R$ is also a sum of $k$-th powers. From (3), Lemma 4.4 and Proposition 4.5, if

$n \in \{0, \ldots, Q^2-1\}$ is not a multiple of $Q+1$, then $x_n = 0$; if $n \in \{0, \ldots, Q^2-1\}$ is a multiple of $Q+1 = k$, then $x_n \in F \cap \mathbb{F}_Q = \mathbb{F}_q$. Thus,

$$H = \sum_{i=1}^{1+\lambda} B_i^k + \sum_{i=0}^{Q-1} \left( L_i(Y_i) + x_{ki} T^{ki} \right), \tag{4}$$

with

$$x_{ki} \in \mathbb{F}_q \quad \text{for} \quad 0 \le i \le Q-1.$$

(A) Suppose that $m$ divides $r$ so that $F = \mathbb{F}_q$. From (4.2) or (4.4), every $L_i(Y_i)+x_{ki}T^{ki}$ in (4) is a sum of $1+\lambda$ $k$-th powers. By (2), (5.3), (5.4), (3) and (4), $H$ is a sum of $(\theta(q,H)+(1+\lambda)Q)$ $k$-th powers of polynomials of degree $\le \mu = \max(n, Q-1)$ with

$$\theta(q,H) = \begin{cases} 2 & \text{if} \quad \deg H = kn, \\ 2 & \text{if} \quad \deg H < kn \quad \text{and} \quad q \equiv 1 \pmod 4, \\ 3 & \text{if} \quad \deg H < kn \quad \text{and} \quad q \equiv 3 \pmod 4. \end{cases}$$

In view of (1), if $n \ge Q-1$, the sum is a strict one. Suppose $p^m \equiv 3 \pmod 4$. If $n < Q-1$, then $\deg H < Q^2-1$. From Proposition 4.5, $H$ is a strict sum of $3k-6 \le (\theta(q,H)+(1+\lambda)Q)$ $k$-th powers.

(B) Suppose $m = 2d$. In this case, $-1$ is a $k$-th power in $F$, $\mathbb{F}_{q^2} \subset F$ and $x_{ki} \in \mathbb{F}_q$ for each $i = 0, \ldots, Q-1$, so that, for each $i = 0, \ldots, Q-1$, there exists $y_i \in \mathbb{F}_{q^2}$ such that $x_{ki} = y_i^k$. From (4.2) or (4.4), $L_i(Y_i) + (x_{ki})T^{ki} = L_i(Y_i) + (y_{ki})^{Q+1}T^{ki}$ is a sum of two $k$-th powers. Moreover, if $\deg H = kn$, then, in (4) we have $B_1 = 0$, so that $H$ is a sum of $(\eta(H)+2Q)$ $k$-th powers, where

$$\eta(H) = \begin{cases} 1 & \text{if} \quad \deg H = kn, \\ 2 & \text{if} \quad \deg H < kn. \end{cases}$$

As above, if $n \ge Q-1$, the sum is strict. In the case when $n < Q-1$ we conclude with Proposition 4.5. □

**Corollary 5.7.** • *Suppose that $m$ divides $r$. Then,*

$$\mathcal{S}^\times(p^m,k) = \mathcal{S}(p^m,k) = \left\{ A \in F[T] \mid A^Q - A \equiv 0 \pmod{T^{Q^2} - T} \right\}.$$

*Moreover,*

(1) *if $p^m$ is congruent to 1 modulo 4,*

$$G(p^m,k) = G^\times(p^m,k) \le 2k,$$
$$g(p^m,k) = g^\times(p^m,k) \le 3k-6;$$

(2) *if $p^m$ is congruent to 3 modulo 4,*

$$G(p^m,k) = G^\times(p^m,k) \le 3k,$$
$$g(p^m,k) = g^\times(p^m,k) \le 3k.$$

- *Suppose that $m/d = 2$. Then,*

$$\mathcal{S}(p^m, k) = \left\{A \in F[T] \mid A^Q - A \equiv 0 \pmod{T^{Q^2} - T}\right\},$$

*$\mathcal{S}^\times(p^m, k)$ is the set of $A \in \mathcal{S}(p^m, k)$ such that either* $\deg A$ *is not a multiple of $k$, or* $\deg A$ *is a multiple of $k$ and the leading coefficient of $A$ is in the field $\mathbb{F}_q$. Moreover, we have*

$$G(p^m, k) = g(p^m, k) = \infty, \quad G^\times(p^m, k) \le g^\times(p^m, k) \le 2k.$$

*Proof.* With Propositions 4.3, 4.5, Propositions 5.1, 5.3 and 5.5. In the case where $m$ divides $r$ and $p^m$ is congruent to 1 modulo 4, we get

$$g(p^m, k) = g^\times(p^m, k) \le \max(2k, 3k - 6).$$

Observe that $\max(2k, 3k - 6) = 3k - 6$ since $2k > 3k - 6$ implies $k = 4, p = 3, m = 1$, a contradiction. □

*Remark* 5.8. (1) In the case $k = 4$, we have $p = 3, r = d = 1$. Corollaries 3.5 and 5.4 give $G(3^m, 4) = G^\times(3^m, 4) \le 9$ for even $m > 4$ and $G(3^m, 4) = G^\times(3^m, 4) \le 10$ for odd $m > 1$ or for $m = 4$. These bounds were proved in [4]. It also gives $g^\times(3^m, 4) \le 16$ for even $m > 4$, $g^\times(3^m, 4) \le 20$ for odd $m > 1$ and $g^\times(81, 4) \le 18$. In the case of even $m$, this improves the bounds obtained in [4].

(2) In the case $k = 4$, Corollary 5.6 gives the following bounds:

$$G(3, 4) = G^\times(3, 4) \le 12, \quad g(3, 4) = g^\times(3, 4) \le 12;$$

$$G(9, 4) = \infty, \quad G^\times(9, 4) \le 8, \quad g(9, 4) \le \infty, \quad g^\times(9, 4) \le 8;$$

which are the bounds given in [4].

(3) For $k = p^r + 1$ tending to $\infty$, we have $G^\times(p^m, k) << k$ as well as $g^\times(p^m, k) << k$ unlike to the classical Waring numbers $G_{\mathbb{N}}(k)$ and $g_{\mathbb{N}}(k)$. Indeed, from [7], $g_{\mathbb{N}}(k) >> 2^k$ when from [23], $G_{\mathbb{N}}(k) << k \log k$.

**Acknowledgements.** I thank an unknown referee for useful remarks, specially for the information concerning the existence of De Konninck and A. Mercier's book

## References

[1] N. Bourbaki, *Éléments de mathématique, Fasc. XXIII*, Livre II: Algébre. Chapitre 8: Modules et anneaux semi-simples. Nouveau tirage de l'édition de 1958. Actualités Scientifiques et Industrielles, No. 1261. Hermann, Paris, 1973.

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

[3] ———, *Sums of* $(2^r + 1)$*-th powers of polynomials over a finite field of characteristic two*, Port. Math., to appear.

[4] ———, *Sums of fourth powers of polynomials over a finite field of characteristic* 3, Funct. Approx. Comment. Math. **38** (2008), part 2, 195–220.

[5] M. Car and L. Gallardo, *Sums of cubes of polynomials*, Acta Arith. **112** (2004), no. 1, 41–50.

[6] G. Effinger and D. R. Hayes, *Additive Number Theory of Polynomials over a Finite Field*, Oxford Mathematical Monographs, Clarendon Pres, Oxford, 1991.
[7] W. J. Ellison, *Waring's problem*, Amer. Math. Monthly **78** (1971), no. 1, 10–36.
[8] L. H. Gallardo, *On the restricted Waring problem over* $\mathbb{F}_{2^n}[t]$, Acta Arith. **42** (2000), no. 2, 109–113.
[9] ———, *Every strict sum of cubes in* $\mathbb{F}_4[t]$ *is a strict sum of 6 cubes*, Port. Math. **65** (2008), no. 2, 227–236.
[10] L. H. 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), no. 4, 981–987.
[11] L. H. Gallardo and L. N. Vaserstein, *The strict Waring problem for polynomials rings*, J. Number Theory **128** (2008), no. 12, 2963–2972.
[12] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 4th. Ed., 1960.
[13] J.-M. De Konninck and A. Mercier, *1001 problems in classical number theory*, Trans. from the French by J.-M. De Konninck, (English), Providence, RI: (AMS) xii, (2007).
[14] R. M. Kubota, *Waring's problem for* $\mathbb{F}_q[x]$, Dissertationes Math. (Rozprawy Mat.) **117** (1974), 60 pp.
[15] R. E. A. C. Paley, *Theorems on polynomials in a Galois field*, The Quarterly Journal of Mathematics. **4** (1933), 52–63.
[16] C. Small, *Sums of powers in large finite fields*, Proc. Amer. Math. Soc. **65** (1977), no. 1, 35–36.
[17] L. N. Vaserstein, *Waring's problem for algebras over fields*, J. Number Theory **26** (1987), no. 3, 286–298.
[18] ———, *Waring's problem for commutative rings*, J. Number Theory **26** (1987), no. 3, 299–307.
[19] ———, *Sums of cubes in polynomial rings*, Math. Comput. **56** (1991), no. 193, 349–357.
[20] ———, *Ramsey's theorem and Waring's problem for algebras over fields*, The arithmetic of function fields (Columbus, OH, 1991), 435–441, Ohio State Univ. Math. Res. Inst. Publ., 2, de Gruyter, Berlin, 1992.
[21] Y.-R. Yu and T. Wooley, *The unrestricted variant of Waring's problem in function fields*, Funct. Approx. Comment. Math. **37** (2007), part 2, 285–291.
[22] W. A. Webb, *Waring's problem in* $GF[q,x]$, Acta Arith. **22** (1973), 207–220.
[23] T. Wooley, *Large improvements in Waring's problem*, Ann. of Math. (2) **135** (1992), no. 1, 131–164.

LATP-UMR CNRS 6632
Amu, Case Cour A
Avenue Escadrille Normandie-Niemen
F-13397 Marseille Cedex 20, France
*E-mail address*: mireille.car@univ-amu.fr