Acta Math. Univ. Comenianae
Vol. LXXXIV, 1 (2015), pp. 13–26

SUMS OF SEVENTH POWERS OF POLYNOMIALS OVER A FINITE FIELD WITH 8 ELEMENTS

MIREILLE CAR

Abstract. Let F be a finite field with 8 elements. We study representations of polynomials over F as sums and strict sums of seventh powers.

1. Introduction

Let F be a finite field with q elements and let $k > 1$ be an integer. Roughly speaking, Waring's problem over $F[T]$ is the analogue of the same problem over the integers. It 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 ([**7**], [**14**]), leading to consider Waring's problem over the subring $\mathcal{S}(F[T], k)$ formed by the polynomials of $F[T]$ which are sums of k-th powers, ([**15**], [**12**]). Without degree conditions, the problem of representing M as the sum (1.1) is close to the so called easy Waring's problem for $\mathbf{Z}$. In order to have a problem close to the non-easy Waring's problem, the degree conditions

$$k \deg M_i < \deg M + k \tag{1.2}$$

are required. A representation (1.1) satisfying degree conditions (1.2) is called a *strict representation* in opposition to representations without degree conditions. Let $g(q,k)$ denote the least integer s, if it exists, such that every polynomial $M \in \mathcal{S}(F[T], k)$ may be written as a sum (1.1) satisfying degree conditions (1.2). Otherwise, we put $g(q,k) = \infty$. Similarly, $G(q,k)$ denotes the least integer s, if it exists, such that every polynomial $M \in \mathcal{S}(F[T], k)$ of sufficiently large degree may be written as a sum (1.1) satisfying degree conditions (1.2). Otherwise, $G(q,k) = \infty$. This notation is possible since these numbers only depend on q and k. The set $\mathcal{S}(F[T], k)$ and the parameters $G(q,k), g(q,k)$ are not sufficient to describe all possible cases, see [**1**, Proposition 4.4]. In [**2**] and [**3**], new parameters have been introduced. They are defined as follows.

Let $\mathcal{S}^{\times}(F[T], k)$ denote the set of polynomials in $F[T]$ which are strict sums of k-th powers. Let $g^{\times}(q,k)$ denote the least integer s, if it exists, such that every

Received November 15, 2013; revised April 11, 2014.
2010 *Mathematics Subject Classification.* Primary 11T55, 11P05.
Key words and phrases. Waring's problem; polynomials.

polynomial $M \in \mathcal{S}^\times(F[T], k)$ may be written as a strict sum

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

otherwise, we put $g^\times(q, k) = \infty$. Similarly, $G^\times(q, k)$ denotes the least integer satisfying the same condition for every polynomial $M \in \mathcal{S}^\times(F[T], k)$ of sufficiently large degree. Many articles were devoted to the case $k = 3$, see [**9**], [**6**], [**10**], [**11**]. In the case of an even characteristic, exponents $k = 2^r + 1$ were considered in [**2**]. The case $k = 7, q = 2^m$ with $m \notin \{1, 2, 3\}$ was covered by [**1**, Theorems 1.2 and 1.3] or by [**12**, Theorem 1.4]. For almost all $q = 2^m$, the bounds obtained in articles for the numbers $G(2^m, 7)$, are comparable with the bound $G_{\mathbf{N}}(7) \leq 33$, known for the corresponding Waring's number for the integers ([**16**]). The case of the numbers $g(2^m, 7)$ is different. In the case when $m \notin \{1, 2, 3\}$ [**1**, Theorem 1.3] as well as [**12**, Theorem 1.4] gives $g(2^m, 7) \leq 239\ell(2^m, 7)$ with $\ell(2^m, 7)$, the least integer s such that every $a \in F$ may be written as a sum of s seventh powers when, for the integers, it is known that $g_{\mathbf{N}}(7) = 143$, ([**8**]). In [**4**], we obtained better bounds for the numbers $g(2^m, 7)$ in the case when $m > 3$, the method yield also better bounds for the numbers $G(2^m, 7)$. In [**5**], we dealt with the case $k = 7, q = 4$. Nothing was known for the case $k = 7, q = 2$ or for the case $k = 7, q = 8$. In this paper, we study the case $k = 7, q = 8$ and we prove the following theorem.

Theorem 1.1. *Let F be a finite field with* 8 *elements. Then*

(1) *the set $\mathcal{S}(F[T], 7)$ is the set of polynomials $A \in F[T]$ such that $T^8 + T$ divides $A^2 + A$;*
(2) *the set $\mathcal{S}^\times(F[T], 7)$ is the subset of $\mathcal{S}(F[T], 7)$ formed by the polynomials $A \in \mathcal{S}(F[T], 7)$ such that either* $\deg A \not\equiv 0 \pmod 7$ *or* $\deg A \equiv 0 \pmod 7$ *and A is monic;*
(3) *we have $G(8, 7) = g(8, 7) = \infty$, $G^\times(8, 7) \leq 40$ and $g^\times(8, 7) \leq 40$.*

Our proof gives the same bound for the numbers $G^\times(8, 7)$ and $g^\times(8, 7)$ unlike the case when $q = 2^m$ with $m > 3$.

It is easy to see that $\mathcal{S}(F[T], 7)$ is a subring of the ring $\mathcal{A}$ formed by the polynomials $A \in F[T]$ such that $A^2 + A$ is multiple of $T^8 + T$. Indeed, if $A = A_1^7 + \cdots + A_s^7$ is a sum of seventh powers of polynomials $A_i \in F[T]$, for each $x \in F$ and each $i \in \{1, \ldots, s\}$, one has $A_i(x)^7 \in \{0, 1\}$, so that $A(x) \in \mathbb{F}_2$; thus, every $x \in F$ is a root of $A^2 + A$. The key tool of the proof of the inclusion $\mathcal{A} \subset \mathcal{S}(F[T], 7)$ is the following identity: For every $X \in F[T]$, one has

$$T^{3i}X^4 + T^{5i}X^2 + T^{6i}X = (X + T^i)^7 + (X + \beta^3 T^i)^7 + (X + \beta^5 T^i)^7 + (X + \beta^6 T^i)^7$$

where $\beta \in F$ is such that $\beta^3 = \beta + 1$. We observe that the map $X \to L_i(X) = T^{3i}X^4 + T^{5i}X^2 + T^{6i}X$ is linear. Starting with a polynomial $X = x_N T^N + x_{N-1}T^{N-1} + \ldots + x_1 T + x_0$ in $\mathcal{A}$ with $\deg X \leq 4n + 3$, we replace a monomial $x_k T^k$ by the sum of an appropriate $L_i(Y_k)$ and two monomials of lower degree. For instance, we write $aT^{4n} = L_0(a^2T^n) + a^4T^{2n} + a^2T^n$, $aT^{4n+3} = L_1(a^2T^n) + a^4T^{2n+5} + a^2T^{n+6}, \ldots$ We begin with $x_N T^N$, we continue with $x_{N-1}T^{N-1}, \ldots$, following decreasing degrees as long as the process gives monomials of lower degree. At the end of the process we obtain that $X = L_0(Y_0) + \cdots + L_3(Y_3) + Z$ with

$Y_0, \ldots, Y_3$ polynomials of degree $\leq n$ and Z of degree ≤ 21, so that X is a sum $X = Z_1^7 + \cdots + Z_{12}^7 + Z$ with polynomials Z_i of degree $\leq n$ and $Z \in \mathcal{A}$ of degree ≤ 21. The characterization of the set $\mathcal{S}(F[T], 7)$ reduces to the characterization of the set of sums of seventh powers of degree ≤ 21. This is our first descent process.

In this way, we do not get a strict representation. In order to get a strict representation, we improve the method using a descent process that was introduced by Gallardo [**9**] and improved in [**6**]. We observe that it suffices to deal with monic polynomials of degree multiple of 7. Indeed, if every monic $A \in \mathcal{A}$ of degree $7n$ is a strict sum of s seventh powers, then, writing a polynomial $X \in \mathcal{A}$ of degree $< 7n$ as $X = T^{7n} + (T^{7n} + A)$, we get that every polynomial $X \in \mathcal{A}$ of degree $< 7n$ is a sum of $s+1$ seventh powers, and that every $X \in \mathcal{A}$ with $7(n-1) < \deg X < 7n$ is a strict sum of $s+1$ seventh powers. We start with a monic polynomial $X \in F[T]$ of degree multiple of 7, say $\deg X = 7n$ with $n \geq 8$. We write $X_0 = X$ as a sum $X = X_0 = Y_0^7 + X_1$, where Y_0 is a monic polynomial of degree $n = n_0$ and X_1 a monic polynomial of degree $7n_1$ with n_1 the least integer such that $7n_1 \geq 6n - 1$. Then, we start again with X_1 at the place of X_0 and we continue until we get

$$X = Y_1^7 + Y_2^7 + \cdots + Y_{r-1}^7 + X_r$$

with X_r a monic polynomial of degree $7n_r$. For the last step, we write X_r as a sum $X_r = Y_{r+1}^7 + X_{r+1}$ with $\deg X_{r+1} < 6n_r$ with X_{r+1} not necessarily monic. We choose r in order to have $\deg X_{r+1} < 4n + 3$, so that we may apply the previous descent to X_{r+1}.

The problem becomes that of representation by sums and strict sums of seventh powers of degree ≤ 56. Its study needs other descent processes. The third descent process consists of writing a polynomial A of degree $< 7n$ with $n \geq 2$ as a sum

$$A = \sum_{i=1}^{6} (T^n + y_i T^{n-1} + z_i T^{n-2})^7 + B$$

with $y_1, z_1, \ldots, y_6, z_6 \in F$ and B a monic polynomial of degree $7(n-1)$.

The fourth descent process consists of writing a monic polynomial A of degree $7n \geq 28$ as a sum $A = A_1^7 + A_2^7 + A_3^7 + B$ with $A_1, A_2, A_3 \in F[T]$ of degree n and $B \in F[T]$ monic of degree $7(n-1)$. From case to case with the appropriate descent process, the study of sums (or strict sums) of degree $\leq 7n$ reduces to that of sums (or strict sums) of degree $\leq 7(n-1)$. All these descent processes are described in Section 3. Proving that polynomials of small degree are sums or strict sums of seventh powers and proving the validity of the descent processes require some results on the solvability of systems of algebraic equations over the finite field F. This is done in Section 2. In Section 4, we characterize the set $\mathcal{S}(F, 7)$ as well as the set formed by strict sums of seventh powers of degree ≤ 21 and we construct a sequence (P_n) of polynomials P_n of degree $7n$ which are sums of seventh powers and which, however, are not strict sums of seventh powers. In Section 5, we characterize the set $\mathcal{S}^\times(F, 7)$ and we get upper bounds for $G^\times(8, 7)$ and $g^\times(8, 7)$.

2. Equations

Proposition 2.1. *For every $(a,b) \in F \times F$, the system*

$$(\mathcal{A}(a,b)) \qquad \begin{cases} x_1 + x_2 + x_3 = a, \\ x_1^3 + x_2^3 + x_3^3 = b, \end{cases}$$

has solutions $(x_1, x_2, x_3) \in F^3$ such that $x_1 \neq x_2$. Moreover, if $b \neq a^3$, $(\mathcal{A}(a,b))$ admits solutions satisfying

$$(\mathcal{C}) \qquad x_1 \neq x_2, x_2 \neq x_3, x_3 \neq x_1.$$

Proof. Let $(a,b) \in F \times F$. From [**13**], $(\mathcal{A}(a,b))$ has a solution $(x_1, x_2, x_3) \in F^3$. Suppose $b \neq a^3$, every $(x_1, x_2, x_3) \in F^3$ solution of $(\mathcal{A}(a,b))$ satisfies $(\mathcal{C})$ so that it satisfies the weaker condition $x_1 \neq x_2$. If $b = a^3$, for every $x \in F$, (x, a, x) is a solution of $(\mathcal{A}(a,b))$. We choose $x \neq a$. □

Corollary 2.2. *For every $\mathbf{b} = (a, a', b, b', c, d) \in F^6$, the system*

$$(\mathcal{E}(\mathbf{b})) \qquad \begin{cases} y_1 + \cdots + y_6 = a, \\ y_1^3 + \cdots + y_6^3 = a', \\ z_1 + \cdots + z_6 = b \\ z_1^3 + \cdots + z_6^3 = b' \\ y_1^2 z_1 + \cdots + y_6^2 z_6 = c, \\ y_1^4 z_1 + \cdots + y_6^2 z_6 = d, \end{cases}$$

has solutions $(y_1, z_1, \ldots, y_6, z_6) \in F^{12}$.

Proof. We have to consider three cases:

(i) $a' \neq a^3$ or $b' \neq b^3$;
(ii) $a' = a^3$, $b' = b^3$ and $(a,b) \neq (0,0)$;
(iii) $a' = a^3 = b' = b^3 = 0$.

Case (i): By symmetry we may suppose $a' \neq a^3$. Proposition 2.1 gives the existence of (y_1, y_2, y_3) in F^3 solution of $(\mathcal{A}(a, a'))$ satisfying $(\mathcal{C})$. Thus, the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ y_1^2 & y_2^2 & y_3^2 \\ y_1^4 & y_2^4 & y_3^4 \end{pmatrix}$$

is invertible. There is $(z_1, z_2, z_3) \in F^3$ solution of

$$\begin{cases} z_1 + z_2 + z_3 = b, \\ y_1^2 z_1 + y_2^2 z_2 + y_3^2 z_3 = c, \\ y_1^4 z_1 + y_2^4 z_2 + y_3^4 z_3 = d. \end{cases}$$

From the same proposition, there exists $(z_4, z_5, z_6) \in F^3$ solution of $(\mathcal{A}(0, u))$ with $u = b' + z_1^3 + z_2^3 + z_3^3$. Let $y_4 = y_5 = y_6 = 0$. Then $(y_1, z_1, \ldots, y_6, z_6)$ is solution of $(\mathcal{E}(\mathbf{b}))$.

Case (ii): By symmetry we may suppose $a \neq 0$. Let $u \in F - \{0, a\}$. The matrix

$$\begin{pmatrix} a^2 & u^2 \\ a^4 & u^4 \end{pmatrix}$$

is invertible. Let $(z_1, z_2) \in F^2$ be the unique solution of

$$\begin{cases} a^2 z_1 + u^2 z_2 = c, \\ a^4 z_1 + u^4 z_2 = d. \end{cases}$$

Proposition 2.1 gives the existence of $(z_4, z_5, z_6) \in F^3$ solution of $(\mathcal{A}(v, w))$, with $v = b + z_1 + z_2, w = b' + z_1^3 + z_2^3$. Then $(a, z_1, u, z_2, u, 0, 0, z_4, 0, z_5, 0, z_6)$ is solution of $(\mathcal{E}(\mathbf{b}))$.

Case (iii): Let $y_1, y_2 \in F$ be such that $y_1 y_2(y_1 + y_2) \neq 0$. As above, there is $(z_1, z_2) \in F^2$ solution of

$$\begin{cases} y_1^2 z_1 + y_2^2 z_2 = c, \\ y_1^4 z_1 + y_2^4 z_2 = d \end{cases}$$

so that $(y_1, z_1, y_2, z_2, y_1, 0, y_2, 0, 0, z_1, 0, z_2)$ is solution of $(\mathcal{E}(\mathbf{b}))$.

□

Proposition 2.3. *For every* $\mathbf{b} = (b_1, b_2, \ldots, b_7) \in F^7$, *the system*

$$(\mathcal{F}(\mathbf{b})) \qquad \begin{cases} b_1 = \sum_{i=1}^{5} x_i, & (e_1) \\ b_2 = \sum_{i=1}^{5} (y_i + x_i^2), & (e_2) \\ b_3 = \sum_{i=1}^{5} (z_i + x_i^3), & (e_3) \\ b_4 = \sum_{i=1}^{5} (x_i^2 y_i + y_i^2 + x_i^4), & (e_4) \\ b_5 = \sum_{i=1}^{5} (x_i^2 z_i + y_i^2 x_i + x_i^5), & (e_5) \\ b_6 = \sum_{i=1}^{5} (y_i^3 + z_i^2 + x_i^4 y_i + x_i^6), & (e_6) \\ b_7 = \sum_{i=1}^{5} (y_i^2 z_i + x_i z_i^2 + x_i^4 z_i + x_i^7) & (e_7) \end{cases}$$

has solutions $(x_1, y_1, z_1, \ldots, x_5, y_5, z_5) \in F^{15}$.

Proof. Let $x_1 = 1,\ x_2 = 1 + b_1,\ x_3 = x_4 = x_5 = 0,\ \ y_1 = a_4 + b_2^2,\ y_2 = 0,$ $z_1 = b_5 + y_1^2 + 1 + x_2^5,\ z_2 = 0$. Then, whatever the choice made for y_3, y_4, y_5, z_3, z_4, z_5, (e_1) and (e_5) are satisfied as well as

$$\sum_{i=1}^{5} x_i^2 y_i = b_4 + b_2^2.$$

Let $a = b_2 + b_1^2 + y_1$ and $b = b_6 + b_3^2 + y_1 + y_1^3$. Proposition 2.1 gives the existence of $(y_3, y_4, y_5) \in F^3$ solution of $(\mathcal{A}(a, b))$ with $y_3 \neq y_4$. Then, for any choice for z_3, z_4, z_5, (e_2) and (e_6) are satisfied as well as (e_4). Let $(z_3, z_4) \in F^2$ be solution of

$$\begin{cases} z_3 + z_4 = b_3 + 1 + x_2^3 + z_1, \\ y_3^2 z_3 + y_4^2 z_4 = b_7 + z_1^2 + z_1 + 1 + x_2^7 + y_1 z_1^2, \end{cases}$$

and let $z_5 = 0$. Then (e_7) and (e_3) are satisfied. □

Proposition 2.4. *For every* $\mathbf{b} = (b_1, b_2, \dots, b_7) \in F^7$, *the system*

$$(\mathcal{G}(\mathbf{b})) \qquad \begin{cases} b_1 = \sum_{i=1}^{3} u_i, & (e_1) \\ b_2 = \sum_{i=1}^{3} (x_i + u_i^2), & (e_2) \\ b_3 = \sum_{i=1}^{3} (y_i + u_i^3), & (e_3) \\ b_4 = \sum_{i=1}^{3} (z_i + u_i^2 x_i + u_i^4 + x_i^2), & (e_4) \\ b_5 = \sum_{i=1}^{3} (u_i^2 y_i + u_i x_i^2 + u_i^5), & (e_5) \\ b_6 = \sum_{i=1}^{3} (u_i^2 z_i + x_i^3 + u_i^4 x_i + u_i^6 + y_i^2), & (e_6) \\ b_7 = \sum_{i=1}^{3} (x_i^2 y_i + u_i y_i^2 + u_i^4 y_i + u_i^7) & (e_7) \end{cases}$$

has solutions $(u_1,\, x_1,\, y_1,\, z_1,\, \dots,\, u_3,\, x_3,\, y_3,\, z_3) \in F^{12}$

Proof. Let $u_1 \in F - \{0, b_1\}, u_2 \in F - \{0, b_1, u_1, u_1 + b_1\}$ and $u_3 = b_1 + u_1 + u_2$. Then (e_1) is satisfied as well as the condition

$$(\dagger) \qquad u_1 u_2 u_3 (u_1 + u_2)(u_2 + u_3)(u_3 + u_1) \neq 0.$$

Let $y_1 \in F$ and $y_2 \in F$ be such that

$$y_1(u_3 + u_1) + y_2(u_2 + u_3) \neq (u_1 + u_2)(b_3 + \sum_{i=1}^{3} u_i^3).$$

Let

$$y_3 = y_1 + y_2 + b_3 + \sum_{i=1}^{3} u_i^3.$$

Then (e_3) is satisfied and $(\dagger)$ insures that the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ u_1^4 & u_2^4 & u_3^4 \\ y_1^4 & y_2^4 & y_3^4 \end{pmatrix}$$

is invertible. Let $(x_1, x_2, x_3) \in F^3$ be defined by

$$\begin{cases} x_1 + x_2 + x_3 = b_2 + b_1^2, \\ u_1^4 x_1 + u_2^4 x_2 + u_3^4 x_3 = b_5^4 + \sum_{i=1}^{3} (u_i^2 y_i + u_i^5)^4 \\ y_1^4 x_1 + y_2^4 x_2 + y_3^4 x_3 = b_7^4 + \sum_{i=1}^{3} (u_i y_i^2 + u_i^4 y_i)^4. \end{cases}$$

Then (e_2), (e_5) and (e_7) are satisfied. For the matrix

$$\begin{pmatrix} 1 & 1 \\ u_1^2 & u_2^2 \end{pmatrix}$$

being invertible, there exists $(z_1, z_2) \in F^2$ such that

$$\begin{cases} z_1 + z_2 = b_4 + b_2^2 + \sum_{i=1}^{3} u_i^2 x_i, \\ u_1^2 z_1 + u_2^2 z_2 = b_6 + b_3^2 + \sum_{i=1}^{3} (u_i^4 x_i + x_i^3). \end{cases}$$

Then with $z_3 = 0$, (e_4) and (e_6) are satisfied. □

3. Identities and descent processes

For i a non-negative integer and $X \in F[T]$, let

$$L_i(X) = T^{3i} X^4 + T^{5i} X^2 + T^{6i} X. \tag{3.1}$$

The following lemma is the key of the proof.

Lemma 3.1. *The map L_i is linear over $\mathbb{F}_2$ and one has*

$$L_i(X) = (X + T^i)^7 + (X + \beta^3 T^i)^7 + (X + \beta^5 T^i)^7 + (X + \beta^6 T^i)^7, \tag{3.2}$$

where $\beta \in F$ satisfies $\beta^3 = \beta + 1$.

A simple application of (3.1) gives the following lemma.

Lemma 3.2. *Let n be a non-negative integer and let $a \in F$. Then, we have*

$$aT^{4n} = L_0(a^2 T^n) + a^4 T^{2n} + a^2 T^n, \tag{3.3}$$

$$aT^{4n+3} = L_1(a^2 T^n) + a^4 T^{2n+5} + a^2 T^{n+6}. \tag{3.4}$$

If $n > 0$, then

$$aT^{4n+2} = L_2(a^2 T^{n-1}) + a^4 T^{2n+8} + a^2 T^{n+11}. \tag{3.5}$$

If $n > 1$, then

$$aT^{4n+1} = L_3(a^2 T^{n-2}) + a^4 T^{2n+11} + a^2 T^{n+16}. \tag{3.6}$$

The next proposition makes use of Gallardo's descent.

Proposition 3.3. *Let $H \in F[T]$ be monic with degree $7n \geq 56$.*
If $n \geq 16$ or $n = 9, 10, 11, 14$, there exist $X_0, \ldots, X_3, Y_0, \ldots, Y_3, Z$ in $F[T]$ with $\deg X_i \leq n, \deg Y_j \leq n$ and $\deg Z \leq 21$ such that

$$H = X_0^7 + \cdots + X_3^7 + L_0(Y_0) + \cdots + L_3(Y_3) + Z. \tag{3.7}$$

If $n = 8$, then there exist $X_0, X_1, X_2, Y_0, \ldots, Y_3, Z$ in $F[T]$ with $\deg X_i \leq n$, $\deg Y_j \leq n$ and $\deg Z \leq 21$ such that

$$H = X_0^7 + \cdots + X_2^7 + L_0(Y_0) + \cdots + L_3(Y_3) + Z. \tag{3.7'}$$

If $n = 12, 13, 15$, then there exist $X_0, \ldots, X_4, Y_0, \ldots, Y_3, Z$ in $F[T]$ with $\deg X_i \leq n$, $\deg Y_j \leq n$ and $\deg Z \leq 21$ such that

$$H = X_0^7 + \cdots + X_4^7 + L_0(Y_0) + \cdots + L_3(Y_3) + Z. \tag{3.7''}$$

Proof. From [**1**, Lemma 5.2-(ii))], there is a sequence $H_0, H_1, \dots, H_i, \dots$ of monic polynomials of degree $7n_0, 7n_1, \dots, 7n_i, \dots$ and a sequence $X_0, X_1, \dots, X_i, \dots$ of polynomials of degree $n_0, n_1, \dots, n_i, \dots$ such that $H = H_0$ and such that for each index i,

$$H_i = X_i^7 + H_{i+1}, \tag{3.8}$$

$$6n_i \leq 7n_{i+1} < 6n_i + 7. \tag{3.9}$$

Moreover, for each index $i \geq 0$, there is $W_i \in F[T]$ of degree n_i such that

$$\deg(H_i + W_i^7) < 6n_i. \tag{3.10}$$

Let r be the least integer such that $6n_r - 1 \leq 4n + 3$. The sequence $((n, 4n+3, n_1 n_2, n_3, 6n_3 - 1))_{42 \geq n \geq 8}$ is given in [**4**, p. 313]. We have $r = 3$ for $n \geq 16$, $r = 2$ for $n = 8$, and $r = 4$ for $n = 12, 13, 15$. We suppose $n \geq 16$. Using (3.8) for $i = 0, 1, 2$, then (3.10) for $i = 3$, we get $H = X_0^7 + \cdots + X_3^7 + Y$ with $\deg Y \leq 4n + 3$. Using (3.3), (3.4), (3.5) and (3.6), as for [**4**, Proposition 5.4], we get that $Y = L_0(Y_0) + \cdots + L_3(Y_3) + Z$ with $Y_0, \dots, Y_3, Z \in F[T]$ satisfying the degree conditions $\deg Y_i \leq n$, $\deg Z \leq 21$. The proof runs in the same way for the other cases. □

We shall use two other descent processes described below.

Proposition 3.4. *Let $n \geq 2$ be an integer and let $A \in F[T]$ be such that $\deg A < 7n$, Then there exists $(y_1, z_1, \dots, y_6, z_6) \in F^{12}$ such that*

$$\deg\Big(A + T^{7(n-2)} \sum_{i=1}^{6} (T^2 + y_i T + z_i)^7)\Big) \leq 7(n-1).$$

Proof. We note that for $(y, z) \in F^2$,

$$\begin{aligned}(\star) \qquad \deg\big((T^2 + yT + z)^7 + T^{14} + yT^{13} + (y^2 + z)T^{12} + y^3 T^{11} +\\ + (y^4 + y^2 z + z^2)T^{10} + (y^5 + yz^2)T^9 + (y^6 + y^4 z + z^3)T^8\big) \leq 7.\end{aligned}$$

Suppose that $A = \sum\limits_{i=0}^{13} a_i T^i$. Corollary 2.2 gives the existence of $(y_1, z_1, \dots, y_6, z_6) \in F^{12}$ solution of $(\mathcal{E}(\mathbf{b}))$ with $\mathbf{b} = (a_{13}, a_{11}, a_{12} + a_{13}^2, a_8 + a_9^4, a_{10} + a_{12}^2, a_9^4 + a_{11}^2)$, so that with $(\star)$,

$$\deg\Big(A + \sum_{i=1}^{6} (T^2 + y_i T + z_i)^7\Big) \leq 7.$$

Now, let $A = \sum\limits_{i=0}^{7n-1} a_i T^i$ with $n > 2$. We have

$$\deg\Big(A + T^{7(n-2)}\Big(\sum_{i=8}^{13} a_{i+7(n-2)} T^i\Big)\Big) \leq 7(n-1).$$

There exists $(y_1, z_1, \dots, y_6, z_6) \in F^{12}$ such that

$$\deg\Big(\Big(\sum_{i=8}^{13} a_{i+7(n-2)}T^i\Big) + \Big(\sum_{i=1}^{6}(T^2 + y_iT + z_i)^7\Big)\Big) \le 7.$$

Then

$$\deg\Big(A + T^{7(n-2)}\sum_{i=1}^{6}(T^2 + y_iT + z_i)^7\Big)\Big) \le 7(n-1).$$

□

Proposition 3.5. *Let $n \ge 4$ be an integer and $A \in F[T]$ be monic of degree $7n$. Then, there exist $A_1, A_2, A_3 \in F[T]$ of degree n such that $A + A_1^7 + A_2^7 + A_3^7$ is a monic polynomial of degree $7(n-1)$.*

Proof. Suppose

$$A = T^{7n} + \sum_{i=0}^{7n-1} a_iT^i.$$

Proposition 2.4 gives the existence of $(u_1, x_1, y_1, z_1, \dots, u_3, x_3, y_3, z_3) \in F^{12}$ solution of $\mathcal{G}(a_{7n-1}, \dots, a_{7n-6}, a_{7n-7} + 1)$, so that

$$B = A + \sum_{i=1}^{3}(T^4 + u_iT^3 + x_iT^2 + y_iT + z_i)^7$$

is a monic polynomial of degree $7(n-1)$. □

4. The set $\mathcal{S}(F[T], 7)$

In this section, we shall prove that $\mathcal{S}(F[T], 7) = \mathcal{A}$.

4.1. Sums and strict sums of degree less than 21

Proposition 4.1. *Let $A \in \mathcal{A}$ of degree ≤ 7. Then,*

(i) *there exists $(u, v, a, b) \in \mathbb{F}_2 \times \mathbb{F}_2 \times F \times F$ such that*

$$A = uT^7 + aT^6 + a^2T^5 + b^4T^4 + a^4T^3 + b^2T^2 + bT + v;$$

(ii) *A is a strict sum of 4 seventh powers.*

Proof. Let

$$A = a_7T^7 + a_6T^6 + \cdots + a_0$$

be such that $T^8 + T$ divides $A^2 + A$. We have

$$\begin{aligned}(a_7^2 + a_7)T^7 + (a_3^2 + a_6)T^6 + (a_6^2 + a_5)T^5 + (a_2^2 + a_4)T^4 + (a_5^2 + a_3)T^3 \\ + (a_1^2 + a_2)T^2 + (a_4^2 + a_1)T + (a_0^2 + a_0) \equiv A^2 + A \equiv 0 \pmod{T^8 + T},\end{aligned}$$

so that $a_7^2 = a_7,\ a_0^2 = a_0;\ a_3^2 = a_6,\ a_6^2 = a_5,\ a_5^2 = a_3;\ a_2^2 = a_4,\ a_1^2 = a_2,\ a_4^2 = a_1$. This proves (i). For $a \in F$, let

$$P_a = a^4T^4 + a^2T^2 + aT,\ Q_a = aT^6 + a^2T^5 + a^4T^3.$$

For $a \neq 0$, we have

$$(*) \qquad P_a = \begin{cases} (T+a^6)^7 + (T+\beta^3 a^6)^7 + (T+\beta^5 a^6)^7 + (T+\beta^6 a^6)^7, \\ T^7 + 1 + (T+\beta a^6)^7 + (T+\beta^2 a^6)^7 + (T+\beta^4 a^6)^7, \end{cases}$$

and

$$(**) \qquad Q_a = \begin{cases} (T+a)^7 + (T+\beta^4 a)^7 + (T+\beta^2 a)^7 + (T+\beta a)^7, \\ T^7 + 1 + (T+\beta^6 a)^7 + (T+\beta^5 a)^7 + (T+\beta^3 a)^7. \end{cases}$$

Thus $P_a, P_a + T^7, P_a + 1, Q_a, Q_a + T^7, Q_a + 1$ are sums of 4 seventh powers, and $P_a + T^7 + 1, Q_a + T^7 + 1$ are sums of 3 seventh powers. With $(*)$ and $(**)$, we have

$$P_a + Q_{a^6} = (aT+1)^7 + T^7 + 1,$$

so that $P_a + Q_{a^6}$ is a sum of 3 seventh powers, $P_a + Q_{a^6} + T^7, P_a + Q_{a^6} + 1$ are sums of 2 seventh powers and $P_a + Q_{a^6} + T^7 + 1 = (aT+1)^7$ is of a seventh power. With $(*)$ and $(**)$, we have

$$P_a + Q_{\beta a^6} = \begin{cases} (T+a^6)^7 + (T+\beta a^6)^7 + (T+\beta^2 a^6)^7 + (T+\beta^6 a^6)^7, \\ T^7 + 1 + (T+\beta^3 a^6)^7 + (T+\beta^4 a)^7 + (T+\beta^5 a^6)^7, \end{cases}$$

so that $P_a + Q_{a\beta^6}$ is a sum of 4 seventh powers, $P_a + Q_{\beta a^6} + T^7, P_a + Q_{\beta a^6} + 1$ are sums of 4 seventh powers and $P_a + Q_{\beta a^6} + T^7 + 1$ is a sum of 3 seventh powers;

$$P_a + Q_{\beta^2 a^6} = \begin{cases} (T+a^6)^7 + (T+\beta^2 a^6)^7 + (T+\beta^4 a^6)^7 + (T+\beta^5 a^6)^7, \\ T^7 + 1 + (T+\beta a^6)^7 + (T+\beta^3 a^6)^7 + (T+\beta^6 a^6)^7, \end{cases}$$

so that $P_a + Q_{\beta^2 a^6}$ is a sum of 4 seventh powers, $P_a + Q_{\beta^2 a^6} + T^7, P_a + Q_{\beta^2 a^6} + 1$ are sums of 4 seventh powers and $P_a + Q_{\beta^2 a^6} + T^7 + 1$ is a sum of 3 seventh powers;

$$P_a + Q_{\beta^3 a^6} = (T+\beta^4 a^6)^7 + (T+\beta^6 a^6)^7,$$

so that $P_a + Q_{\beta^3 a^6}$ is a sum of 2 seventh powers, $P_a + Q_{\beta^3 a^6} + T^7, P_a + Q_{\beta^2 a^6} + 1$ are sums of 3 seventh powers and $P_a + Q_{\beta^3 a^6} + T^7 + 1$ is a sum of 4 seventh powers;

$$P_a + Q_{\beta^4 a^6} = \begin{cases} (T+a^6)^7 + (T+\beta a^6)^7 + (T+\beta^3 a^6)^7 + (T+\beta^4 a^6)^7, \\ T^7 + 1 + (T+\beta^2 a^6)^7 + (T+\beta^5 a^6)^7 + (T+\beta^6 a^6)^7, \end{cases}$$

so that $P_a + Q_{\beta^4 a^6}$ is a sum of 4 seventh powers, $P_a + Q_{\beta^4 a^6} + T^7, P_a + Q_{\beta^2 a^6} + 1$ are sums of 4 seventh powers and $P_a + Q_{\beta^3 a^6} + T^7 + 1$ is a sum of 3 seventh powers;

$$P_a + Q_{\beta^5 a^6} = (T+\beta^2 a^6)^7 + (T+\beta^3 a^6)^7,$$

so that $P_a + Q_{\beta^5 a^6}$ is a sum of 2 seventh powers, $P_a + Q_{\beta^5 a^6} + T^7, P_a + Q_{\beta^5 a^6} + 1$ are sums of 3 seventh powers and $P_a + Q_{\beta^5 a^6} + T^7 + 1$ is a sum of 4 seventh powers;

$$P_a + Q_{\beta^6 a^6} = (T+\beta a^6)^7 + (T+\beta^5 a^6)^7,$$

so that $P_a + Q_{\beta^6 a^6}$ is a sum of 2 seventh powers, $P_a + Q_{\beta^6 a^6} + T^7, P_a + Q_{\beta^6 a^6} + 1$ are sums of 3 seventh powers and $P_a + Q_{\beta^6 a^6} + T^7 + 1$ is a sum of 4 seventh powers. We note that all these sums are strict sums. From the (i) part of the proposition, every $A \in \mathcal{A}$ of degree ≤ 7 is a sum $A = uT^7 + Q_a + P_b + v$ with $a, b \in F$ and

$u, v \in \mathbb{F}_2$. Thus every $A \in \mathcal{A}$ of degree ≤ 7 is a strict sum of at most 4 seventh powers. □

Corollary 4.2. *Every $A \in \mathcal{A}$ such that $7 < \deg A < 14$ is a strict sum of 10 seventh powers, so that every monic polynomial $A \in \mathcal{A}$ of degree 14 is a strict sum of 11 seventh powers.*

Proof. Let $A \in \mathcal{A}$ be such that $7 < \deg A < 14$. From Proposition 3.4, there exists $A_1, \dots, A_6, B \in F[T]$ such that

$$A = \sum_{i=1}^{6} A_i^7 + B, \quad \deg A_1 = \dots = \deg A_6 = 2, \quad \deg B \leq 7.$$

Then $B \in \mathcal{A}$, so that from Proposition 4.1, B is a strict sum of 4 seventh powers. □

Proposition 4.3. *Let $A \in \mathcal{A}$ be monic of degree 21. Then A is a strict sum of 15 seventh powers.*

Proof. Let $A = T^{21} + a_{20}T^{20} + a_{20}T^{20} + \dots + a_1T + a_0$ be a monic polynomial in $\mathcal{A}$. Let $(x_1, y_1, z_1, \dots, x_5, y_5, z_5) \in F^{15}$ be solution of $\mathcal{F}(a_{20}, a_{19}, \dots, a_{14})$, (c.f. Proposition 2.3), and let

$$B = A + \sum_{i=1}^{5} (T^3 + x_iT^2 + y_iT + z_i)^7.$$

Then, $B \in \mathcal{A}$ and $\deg B < 14$. We conclude with Corollary 4.2. □

Proposition 4.4. *Let $A \in \mathcal{S}(F[T], 7)$ be monic of degree 28. Then A is a strict sum of 18 seventh powers.*

Proof. Proposition 3.5 gives the existence of $A_1, A_2, A_3 \in F[T]$ of degree 4 such that $B = A + A_1^7 + A_2^7 + A_3^7$ is a monic polynomial of degree 21. Since $B \in \mathcal{A}$, we conclude with Proposition 4.3. □

4.2. The set $\mathcal{S}(F[T], 7)$

Theorem 4.5. *The set $\mathcal{S}(F[T], 7)$ is the set of polynomials $A \in F[T]$ such that $T^8 + T$ divides $A^2 + A$.*

Proof. We have to prove that $\mathcal{A} \subset \mathcal{S}(F[T], 7)$. Let $A \in \mathcal{A}$. Suppose $\deg A \leq 21$. Then $(T^{28} + A) \in \mathcal{A}$. From Proposition 4.4, $(T^{28} + A) \in \mathcal{S}(F[T], 7)$, so that $A \in \mathcal{S}(F[T], 7)$. For $n \geq 4$, the proof goes by induction. We suppose that every $P \in \mathcal{A}$ of degree $\leq 7(n-1)$ lies in $\mathcal{S}(F[T], 7)$. Let $A \in \mathcal{A}$ with $7(n-1) < \deg A \leq 7n$. If $\deg A < 7n$, Proposition 3.4 gives the existence of $A_1, \dots, A_6 \in F[T]$ such that $\deg(A + A_1^7 + \dots + A_6^7) \leq 7(n-1)$. Since $(A + A_1^7 + \dots + A_6^7) \in \mathcal{A}$, $(A + A_1^7 + \dots + A_6^7) \in \mathcal{S}(F[T], 7)$, so that $A \in \mathcal{S}(F[T], 7)$. If $\deg A = 7n$, using Proposition 3.5 at the place of Proposition 3.4, the proof is similar. □

Corollary 4.6. *We have*

$$g(8, 7) = G(8, 7) = \infty.$$

Proof. We prove the existence of a sequence of polynomials P_n with $\deg(P_n)$ tending to $+\infty$, such that for each index n, $P_n \in \mathcal{S}(F[T], 7)$ and $P_n \notin \mathcal{S}^{\times}(F[T], 7)$. We note that $a^7 \in \mathbb{F}_2$ for every $a \in F$. Thus, a strict sum of seventh powers of degree multiple of 7 is a monic polynomial. Let $P_n = \beta T^{7n} + \beta T^{7(n-1)}$. Since P_n is not monic and has degree $7n$, P_n is not a strict sum of seventh powers. On the other hand, $P_n = \beta T^{7n-8}(T^8 + T)$, so that $T^8 + T$ divides $P_n^2 + P_n$. Thus, $P_n \in \mathcal{S}(F[T], 7)$. □

5. The set $\mathcal{S}^{\times}(F[T], 7)$

In this section, we bound the length of strict representations of polynomials $P \in \mathcal{S}^{\times}(F[T], 7)$. As it was noted in the introduction, it suffices to deal with monic polynomials. Firstly, we consider polynomials $P \in \mathcal{S}^{\times}(F[T], 7)$ of degree ≤ 189.

Proposition 5.1. *Let $A \in \mathcal{S}(F[T], 7)$ be a monic polynomial of degree multiple of 7 and ≤ 189.*

(i) *If $\deg A = 28$, then A is a strict sum of 18 seventh powers.*
(ii) *If $\deg A = 35$, then A is a strict sum of 21 seventh powers.*
(iii) *If $\deg A = 42$, then A is a strict sum of 24 seventh powers.*
(iv) *If $\deg A = 7n$ with $7 \leq n < 14$, then A is a strict sum of $n + 18$ seventh powers.*
(v) *If $\deg A = 7n$ with $14 \leq n < 21$, then A is a strict sum of $n + 17$ seventh powers.*
(vi) *If $\deg A = 7n$ with $21 \leq n < 28$, then A is a strict sum of $n + 16$ seventh powers.*

Proof. Proposition 4.4 gives (i). Suppose that $\deg A = 7k$ with $k = 5, 6$. Proposition 3.5 gives the existence of $X_1, X_2, X_3 \in F[T]$ of degree k such that $A + \sum_{i=1}^{3} X_i^7$ is monic of degree $7(k-1)$. Then (ii) falls from (i), and (iii) falls from (ii).

We prove (iv), (v) and (vi) by induction. Suppose that for $n \geq 7$, every monic polynomial of degree $7k$ with $k < n$ is a strict sum of $s(k)$ seventh powers. Let $A \in F[T]$ be monic of degree $7n$. From [**1**, Lemma 5.2-(ii)], there is a polynomial $X \in F[T]$ of degree n such that $A + X^7$ is a monic polynomial of degree $7m(n)$ with $m(n)$ defined by the condition $6n \leq 7m(n) < 6n + 7$. We have

$$m(n) = \begin{cases} n-1 & \text{if } 7 \leq n < 14, \\ n-2 & \text{if } 14 \leq n < 21 \\ n-3 & \text{if } 21 \leq n < 28. \end{cases}$$

From the induction assumption, $A + X^7$ is a strict sum of $s(m(n))$ seventh powers, so that A is a strict sum of $s(m(n)) + 1$ seventh powers. We have $s(6) = 24$. Thus,

$$s(n) = \begin{cases} n+18 & \text{if } 7 \leq n < 14, \\ n+17 & \text{if } 14 \leq n < 21, \\ n+16 & \text{if } 21 \leq n < 28. \end{cases}$$

□

Now, we consider polynomials with large degree.

Proposition 5.2. *Let $H \in \mathcal{S}(F[T], 7)$ be a monic polynomial of degree multiple of* 7*.*

(i) *If $\deg H \geq 112$ or $\deg H \in \{63, 70, 77, 98\}$, then H is a strict sum of* 39 *seventh powers.*
(ii) *If $\deg H = 56$, then H is a strict sum of* 38 *seventh powers.*
(iii) *If $\deg H \in \{84, 91, 105\}$, H is a strict sum of* 40 *seventh powers.*

Proof. Let $\deg H = 7N$. Suppose $N \geq 9, N \neq 12, 13, 15$. Proposition 3.3 gives the existence of $X_0, \dots, X_3, Y_0, \dots, Y_3, Z \in F[T]$ with $\deg X_i \leq N, \deg Y_j \leq N$ and $\deg Z \leq 21$ such that

$$H = X_0^7 + \cdots + X_3^7 + L_0(Y_0) + \cdots + L_3(Y_3) + Z.$$

Lemma 3.1 and Proposition 4.4 give the existence of polynomials $Y_{0,1}, \dots, Y_{0,4}$, $\dots, Y_{3,1}, \dots, Y_{3,4}$ of degree $\leq N$, and polynomials $Z_1, \dots, Z_{19}$ of degree ≤ 4 such that

$$H = X_0^7 + \cdots + X_3^7 + \sum_{i=0}^{3} \sum_{j=1}^{4} Y_{i,j}^7 + \sum_{i=1}^{19} Z_i^7.$$

Thus H is a strict sum of 39 seventh powers. For $N = 8$, resp., for $N = 12, 13, 15$, the proof is similar, with (3.7'), resp. (3.7") at the place of (3.7). □

We are ready to prove our main theorem.

Theorem 5.3.

(1) *The set $\mathcal{S}^\times(F[T], 7)$ is the subset of $\mathcal{S}(F[T], 7)$ formed by the polynomials $A \in \mathcal{S}(F[T], 7)$ such that either $\deg A \not\equiv 0 \pmod 7$ or $\deg A \equiv 0 \pmod 7$ and A is monic.*
(2) *We have*

$$G^\times(8, 7) \leq 40, \quad g^\times(8, 7) \leq 40.$$

Proof. The comparison of the results provided by Propositions 4.1, 4.2, 4.3, 4.4, 5.1 and 5.2 gives that every monic $H \in \mathcal{S}(F[T], 7)$ of degree multiple of 7 lies in $\mathcal{S}^\times(F[T], 7)$ and that $g^\times(8, 7) \leq 40$. Proposition 5.2(i) gives that $G^\times(8, 7) \leq 40$. □

References

1. Car M., *New Bounds on Some Parameters in the Waring Problem for polynomials over a finite field*, Contemporary Mathematics **461** (2008), 59–77.

2. ———, *Sums of* (2^r+1)*-th powers in the polynomial ring* $\mathbb{F}_{2^m}[T]$, Port. Math. (N.S), **67(1)** (2010), 13–56.

3. ———, *Sums of fourth powers of polynomials over a finite field of characteristic 3*, Func. and Approx **38(2)** (2008), 195–220.

4. ———, *Sums of seventh powers in the polynomial ring* $\mathbb{F}_{2^m}[T]$, Port. Math. (N.S) **68(3)** (2011), 297–316.

5. ———, *Sums of seventh powers in the ring of polynomials over the finite field with four elements*, Acta Math. Univ. Comenianae, **82(1)** (2013), 39–67.

6. Car M. and Gallardo L. H., *Sums of cubes of polynomials*, Acta Arith. **112**, (2004), 41–50.

7. Effinger G. and Hayes D., *Additive Number Theory of Polynomials Over a Finite Field.* Oxford Mathematical Monographs, Clarendon Press, Oxford 1991.
8. Ellison W. J., *Waring's problem,* Amer. Math. Monthly **78(10)** (1971), 10–36.
9. Gallardo L. H., *On the restricted Waring problem over* $\mathbb{F}_{2^n}[t]$, Acta Arith. **42** (2000), 109–113.
10. ———, *Every sum of cubes in* $\mathbb{F}_4[t]$ *is a strict sum of 6 cubes*, Port. Math. **65(2)** (2008), 227–236.
11. Gallardo L.H. and Heath-Brown D. R., *Every sum of cubes in* $\mathbb{F}_2[t]$ *is a strict sum of 6 cubes*, Finite Fields and App. **13(4)** (2007), 977–980.
12. Gallardo L. H. and Vaserstein L. N., *The strict Waring problem for polynomials rings*, J. Number Theory **128** (2008), 2963–2972.
13. Moreno O. and Castro F., *Divisiblity properties for covering radius of certain cyclic codes* IEEE Trans. Inform. Theory **49** (2003), 3299–3303.
14. Paley R. E. A. C, *Theorems on polynomials in a Galois field*, Quarterly J. of Math. **4** (1933), 52–63.
15. Vaserstein L. N., *Waring's problem for algebras over fields*, J. Number Theory **26** (1987), 286–298.
16. Vaughan R. C. and Wooley T. D., *Waring's problem: a survey*, In Number Theory for the millenium, III (Urbana, IL, 2000), 301–240.

Mireille Car, Laboratoire de Mathématiques de Marseille, CNRS, UMR 7373 CMI, 39 rue F. Joliot Curie, F-13453 Marseille Cedex 13, France, *e-mail*: `mireille.car@univ-amu.fr`