ACTA ARITHMETICA
XCII.2 (2000)

On the restricted Waring problem over $\mathbb{F}_{2^n}[t]$

by

LUIS GALLARDO (Brest)

1. Introduction. The *Waring problem* for polynomial cubes over a finite field F of characteristic 2 consists in finding the minimal integer $m \geq 0$ such that every sum of cubes in $F[t]$ is a sum of m cubes. It is known that for F distinct from $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}$, each polynomial in $F[t]$ is a sum of three cubes of polynomials (see [3]).

If a polynomial $P \in F[t]$ is a sum of n cubes of polynomials in $F[t]$ such that each cube A^3 appearing in the decomposition has degree $< \deg(P)+3$, we say that P is a *restricted sum of n cubes*.

The *restricted Waring problem* for polynomial cubes consists in finding the minimal integer $m \geq 0$ such that each sum of cubes S in $F[t]$ is a restricted sum of m cubes.

The best known result for the above problem is that every polynomial in $\mathbb{F}_{2^n}[t]$ of sufficiently high degree that is a sum of cubes, is a restricted sum of eleven cubes. This result was obtained by the circle method in [1].

Here we improve this result using elementary methods. Let F be a finite field of characteristic 2, distinct from $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}$. In Theorem 7, we prove that every polynomial in $F[t]$ is a restricted sum of at most nine cubes, and that every polynomial in $\mathbb{F}_{16}[t]$ is a restricted sum of at most ten cubes.

We also prove, in Theorem 9, that by adding to a given $P \in \mathbb{F}_{2^n}[t]$ some square B^2 with $\deg(B^2) < \deg(P)+2$, the resulting polynomial is a restricted sum of at most four cubes, for all $n \neq 2$.

2. Sums of cubes. We consider a polynomial $P \in F[t]$ with F a field of characteristic 2. We want to write P as a restricted sum of cubes. In Lemma 5 we approach P by a sum of two cubes $A^3 + B^3$. This requires that F be distinct from $\mathbb{F}_4$. Applying two more times the same reduction we are reduced to writing a polynomial of degree $< \deg(P)/3+1$ as a sum of cubes. Specializing F to a finite field distinct from $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}$, we obtain Theorem 6,

---

2000 *Mathematics Subject Classification*: Primary 11T55.

using the Serre Identity (see Lemma 2). For $F=\mathbb{F}_{16}$ a specific identity is used. The reduction requires that P has degree higher than some constant integer n. We finish the reduction in Theorem 7, proving in a case by case manner the result for all polynomials of degree less than this constant n.

LEMMA 1. *Let F be a finite field of characteristic 2, $F \neq \mathbb{F}_4$ and $g \in F$, $g \neq 0$. There exist $a, b \in F$, $a \neq 0$, such that $g = a^3 + b^3$.*

Proof. See [2].

LEMMA 2 (Serre Identity). *Let F be a finite field of characteristic 2, distinct from $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}$. Every polynomial $P \in F[t]$ is a sum of three cubes, say $P = A^3 + B^3 + C^3$, with $A, B, C \in F[t]$, $\deg(A) = \deg(B) = \deg(C) = \deg(P)$.*

Proof. This follows from the Serre formula

$$b^6 + a^6 + abc^3t = (at + b^2)^3 + (bt + a^2)^3 + (ct)^3 \tag{1}$$

where a, b, c are nonzero elements in F such that $a^3 + b^3 + c^3 = 0$. See [3].

COROLLARY 3. *Let F be a finite field of characteristic 2, distinct from $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}$. There exist three linear polynomials $A, B, C \in F[t]$ such that $t^2 = A^3 + B^3 + C^3$.*

Proof. By a specialization of variables in formula (1) we obtain $t = U^3 + V^3 + W^3$, where $U, V, W \in F[t]$ and $\deg(U) = \deg(V) = \deg(W) = 1$. Replace t by $1/t$ in this last formula, and then multiply both sides by t^3.

LEMMA 4. *Let $F \neq \mathbb{F}_4$ be a field of characteristic 2. Let $n \geq 1$ be an integer, and $P \in F[t]$ a polynomial with $\deg(P) \in \{3n+3, 3n+2, 3n+1\}$. There exist polynomials $A, B, Q \in F[t]$ such that $P = A^3 + B^3 + Q$. Moreover $\deg(A) = n+1$, $\deg(B) \leq n+1$, $\deg(Q) \leq 2n+1$.*

Proof. Set $P = \sum_{j=0}^{3n+3} p_j t^j$, $d = \deg(P)$, $S = \sum_{j=0}^{n} s_j t^j$, $A = at^{n+1} + S$, $B = \alpha t^{n+1} + \beta t^n + \gamma t^{n-1}$, where the $\{s_j\}_{j=0,\ldots,n}$, and $a, \alpha, \beta, \gamma \in F$ are to be determined. If $d = 3n+3$, then we set $\beta = 0$, $\gamma = 0$. If $d = 3n+2$, then we set $s_n = 0$, $a = 1$, $\alpha = 1$, $\gamma = 0$. If $d = 3n+1$, then we set $s_n = 0$, $s_{n-1} = 0$, $a = 1$, $\alpha = 1$, $\beta = 0$. Set $Q = P + A^3 + B^3$. For j from $2n+2$ to $3n+3$, we force all coefficients q_j of Q to be 0, as follows. From the equations $q_{3n+3} = a^3 + \alpha^3 + p_{3n+3} = 0$, $q_{3n+2} = a^2 s_n + \beta\alpha^2 + p_{3n+2} = 0$, $q_{3n+1} = a^2 s_{n-1} + \beta^2\alpha + a s_n^2 + \alpha^2\gamma + p_{3n+1} = 0$, we obtain the missing values of $\alpha, a, \beta, \gamma, s_n, s_{n-1}$. More precisely, if $d = 3n+3$, then we get $a \neq 0$ from Lemma 1, α from the equation $q_{3n+3} = 0$, s_n from the equation $q_{3n+2} = 0$, and s_{n-1} from the equation $q_{3n+1} = 0$; if $d = 3n+2$, then we get β from the equation $q_{3n+2} = 0$, and s_{n-1} from the equation $q_{3n+1} = 0$; if $d = 3n+1$, then we get γ from the equation $q_{3n+1} = 0$. So the proof is finished for $n = 1$, and we now take $n \geq 2$. Given an integer k such that $1 \le k \le n-1$, suppose that we have determined s_n to s_{n-k} from the equations $q_{3n+3} = 0$ to $q_{3n-k+2} = 0$. We can then determine s_{n-k-1} from the equation $q_{3n-k+1} = 0 = a^2 s_{n-k-1} + p_{3n-k+1} + R$, where R is a cubic form in a, α, β, γ, and the $\{s_j\}_{n-k \le j \le n}$.

We now show the result of our reduction applied to a polynomial $P \in F[t]$, where F is a finite field of characteristic 2, distinct from $\mathbb{F}_4$:

LEMMA 5. *Let F be a finite field of characteristic* 2, $F \ne \mathbb{F}_4$, *and let $P \in F[t]$ be a polynomial of degree $d \ge 4$. There exist polynomials $A, B, Q \in F[t]$ such that $P = A^3 + B^3 + Q$. Moreover* $\deg(A^3) < d + 3$, $\deg(B^3) < d + 3$, $\deg(Q^3) \le 2d + e$, *where $e = -3$ if $d \equiv 0 \bmod 3$; $e = -1$ if $d \equiv 2 \bmod 3$; $e = 1$ if $d \equiv 1 \bmod 3$.*

P r o o f. This follows from Lemma 4.

THEOREM 6. *Let F be a finite field of characteristic* 2, *distinct from $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}$. Every polynomial $P \in F[t]$ with* $\deg(P) > 6$ *is a restricted sum of at most nine cubes. Every polynomial $P \in \mathbb{F}_{16}[t]$ with* $\deg(P) > 6$ *is a restricted sum of at most ten cubes.*

P r o o f. Suppose $F \ne \mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}$. If $\deg(P) > 9$, we apply Lemma 5 three times and Lemma 2 once. If $7 \le \deg(P) \le 9$, we apply Lemma 5 twice and Lemma 2 once. For $F = \mathbb{F}_{16}$ the proof is the same, upon replacing the Serre formula in Lemma 2 by the identity

$$t = (tr + s)^3 + (tr + s + 1)^3 + (t + sr^2)^3 + (t + (1 + s)r^2)^3, \tag{2}$$

where $r \in \mathbb{F}_{16}$ satisfies $r^4 = r + 1$, and $s = r^5$.

THEOREM 7. *Let F be a finite field of characteristic* 2, *distinct from $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}$. Every polynomial $P \in F[t]$ is a restricted sum of at most nine cubes. Every polynomial $P \in \mathbb{F}_{16}[t]$ is a restricted sum of at most ten cubes.*

P r o o f. From Theorem 6, we can assume that $\deg(P) \le 6$. Suppose $F \ne \mathbb{F}_{16}$. If $\deg(P) \le 1$ the result follows from the Serre identity in Lemma 2. Suppose $\deg(P) = 2$ and write $P = a_2 t^2 + a_1 t + a_0$. From Corollary 3, $a_2 t^2 = (a_2^{1/2} t)^2$ is a sum of 3 cubes of polynomials of degree 1, but $\deg(P + a_2 t^2) \le 1$, so $P = (P + a_2 t^2) + a_2 t^2$ is a sum of at most 6 cubes, each of degree ≤ 1. Suppose $\deg(P) = 3$ and write $P = a_3 t^3 + P_2$ with $\deg(P_2) \le 2$. By Lemma 1, $a_3 = a^3 + b^3$ with some $a, b \in F$; so $a_3 t^3 = (at)^3 + (bt)^3$; it follows that P is a sum of at most 8 cubes, each of degree ≤ 1. Suppose $\deg(P) = 4$ and write $P = t^3 P_1 + P_2$ with $\deg(P_1) = 1$ and $\deg(P_2) = 2$. Apply Lemma 2 to P_1 and P_2. We deduce that P is a sum of at most 6 cubes, each of degree ≤ 2. Suppose $\deg(P) = 5$. By Lemma 4, $P = A^3 + B^3 + P_3$ with $\deg(A) \le 2, \deg(B) \le 2$ and $\deg(P_3) \le 3$. By Lemma 1, $P_3 = (ct)^3 + (dt)^3 + P_2$ with some $c, d \in F$ and $\deg(P_2) \le 2$; so that by Lemma 2, P_2 is a sum of at most 3 cubes, each of degree ≤ 2. Hence P is a sum of at most 7 cubes, each of degree ≤ 2. Suppose

$\deg(P) = 6$. By Lemma 4, $P = A^3 + B^3 + P_4$ with $\deg(A) \le 2, \deg(B) \le 2$ and $\deg(P_4) \le 4$. So P is a sum of at most 8 cubes, each of degree ≤ 2. The proof is similar when $F = \mathbb{F}_{16}$, with the appeal to Lemma 2 replaced by the identity (2), and Corollary 3 replaced by a similar result obtained after replacing t by $1/t$ and multiplying both sides of (2) by t^3.

3. Allowing a square. We consider a polynomial $P \in F[t]$, where F is a perfect field of characteristic 2. We approach the square root S of the derivative of P relative to t by a sum of at most two polynomials, say U, V, of the form $A^2B + tB^3$. The reduced polynomial $Q = S + U + V$ is of degree close to $\deg(S)/3$ (see Lemma 8). This reduction requires that every element in F is a sum of at most two cubes. So we specialize F to a finite field other than $\mathbb{F}_4$, and we apply the identity $T = (T+1)^3 + T^3 + (T+1)^2$ to the polynomial tW^2. The main result is Theorem 9.

LEMMA 8. *Let F be a perfect field of characteristic 2 such that every element in F is a sum of at most two cubes. Let $n \ge 0$ be an integer, and $S \in F[t]$ be a polynomial with $\deg(S) \in \{3n+2, 3n+1, 3n\}$. There exist polynomials $A, B, C, D, Q \in F[t]$ such that*

$$S = A^2B + tB^3 + C^2D + tD^3 + Q,$$

where $\deg(B) = n, \deg(C) \le n$, $\deg(D) \le n, \deg(Q) < n-1$. *Moreover, if* $\deg(S) \in \{3n, 3n+1\}$ *then* $\deg(A) \le n$; *if* $\deg(S) = 3n+2$ *then* $\deg(A) = n+1$.

Proof. Suppose that $n \ge 1$. Set $S = \sum_{j=0}^{3n+3} p_{3n+3-j}\, t^{3n+3-j}$, $A = at^{n+1} + \sum_{k=0}^{n} a_k t^k$, $B = ct^n$, $C = \sum_{k=0}^{n} c_k t^k$, $D = dt^n + t^{n-1}$. If $p_{3n+1} = 0$, then we set $c = d = 1$. If $p_{3n+1} \ne 0$, then by hypothesis we obtain $c, d \in F$, $c \ne 0$, such that $p_{3n+1} = c^3 + d^3$. If $p_{3n+2} = 0$, then we take $a = 0$. If $p_{3n+2} \ne 0$, then we take $c \ne 0$ from $ca^2 = p_{3n+2}$. We now determine the $\{c_k, a_k\}_{0 \le k \le n}$ such that all monomials $\{r_s t^s\}_{n \le s \le 3n}$ of $S + A^2B + tB^3 + C^2D + tD^3$ are 0, as follows. From the linear equation $r_{3n-1} = c_n^2 + d + p_{3n-1} = 0$, we obtain c_n, then from the linear equation $r_{3n} = ca_n^2 + d^2 + c_n^2 d + p_{3n} = 0$, we obtain a_n. From the linear equation $r_{3n-3} = c_{n-1}^2 + p_{3n-3} = 0$, we obtain c_{n-1}, then from the linear equation $r_{3n-2} = ca_{n-1}^2 + 1 + c_{n-1}^2 d + p_{3n-2} = 0$, we obtain a_{n-1}. This finishes the proof for $n = 1$, and so we now take $n \ge 2$. From the linear equation $r_{3n-5} = c_{n-2}^2 + p_{3n-5} = 0$, we obtain c_{n-2}, then from the linear equation $r_{3n-4} = ca_{n-2}^2 + c_{n-2}^2 d + p_{3n-4} = 0$, we obtain $a_{n-2}, \ldots$ Finally, we obtain c_0 from the linear equation $r_{n-1} = c_0^2 + p_{n-1} = 0$, and a_0 from the linear equation $r_n = ca_0^2 + dc_0^2 = 0$. So the resulting polynomial $Q = S + A^2B + tB^3 + C^2D + tD^3$ is of degree less than or equal to $n-2$, finishing the proof. The proof for $n = 0$ is similar by setting $A = at + a_0,\ B = c,\ C = c_0,\ D = d$.

THEOREM 9. *Let F be a finite field of characteristic* 2, *distinct from* $\mathbb{F}_4$, *and let* $P \in F[t]$. *There exists a square* B^2 *in* $F[t]$ *with* $\deg(B^2) < \deg(P)+2$ *such that* $P + B^2$ *is a restricted sum of at most four cubes.*

Proof. For any $H \in F[t]$ we write H' for the derivative of H relative to t. Put $P' = S^2$, and $d = \deg(S) \in \{3n+2, 3n+1, 3n\}$ for some integer $n \geq 0$. Now $P = (tP)' + tP'$, where $(tP)'$ is a square in $F[t]$ of degree $< \deg(P)+2$. So it suffices to prove the result for tP'. Applying Lemmas 1 and 8 to S we get

$$(tP')' = S^2 = K^2K' + L^2L' + Q^2 \tag{3}$$

with $K = A^2 + tB^2,\ L = C^2 + tD^2$. Then $\deg(L) \leq 2n + 1$. Also $\deg(K) = 2n + 1$ if $d \equiv 0$ or $1 \bmod 3$; $\deg(K) = 2n + 2$ if $d \equiv 2 \bmod 3$. Furthermore, $\deg(Q) < n - 1$. Integrating (3) over t, we get

$$R^2 + tP' = K^3 + L^3 + tQ^2$$

for some $R \in F[t]$. We have $\deg(L^3) \leq 6n + 3 < 6n + 4 \leq \deg(tP') + 3$. If $d \equiv 0 \bmod 3$ or $d \equiv 1 \bmod 3$ then $\deg(K^3) \leq 6n+3 < 6n+4 \leq \deg(tP')+3$. If $d \equiv 2 \bmod 3$ then $\deg(K^3) = 6n + 6 < 6n + 8 \leq \deg(tP') + 3$. Now $\deg((tQ^2)^2) \leq \deg((tQ^2)^3) < 6n - 3 < \deg(tP') + 2 < \deg(tP') + 3$. If $d \equiv 0 \bmod 3$ or $d \equiv 1 \bmod 3$ then, using $R^2 = tP' + K^3 + L^3 + tQ^2$, we obtain $\deg(R^2) \leq 6n + 3$; i.e. $\deg(R^2) < 6n + 3 \leq \deg(tP') + 2$. Similarly, $\deg(R^2) \leq 6n + 6 < 6n + 7 \leq \deg(tP') + 2$ when $d \equiv 2 \bmod 3$. From the identity $T = (T + 1)^3 + T^3 + (T + 1)^2$, we obtain

$$tP' = K^3 + L^3 + (tQ^2 + 1)^3 + (tQ^2)^3 + (R + tQ^2 + 1)^2.$$

This establishes the result.

References

[1] M. Car et J. Cherly, *Sommes de cubes dans l'anneau* $\mathbb{F}_{2^h}[X]$, Acta Arith. 65 (1993), 227–241.

[2] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, 1984, pp. 327 and 295.

[3] L. N. Vaserstein, *Sums of cubes in polynomial rings*, Math. Comp. 56 (1991), 349–357.

Department of Mathematics
University of Brest
6, Avenue le Gorgeu
29285, Brest Cedex, France
E-mail: Luis.Gallardo@univ-brest.fr

Received on 20.2.1998
and in revised form on 29.9.1999 (3340)