Portugal. Math. (N.S.)
Vol. 65, Fasc. 2, 2008, 227–236

Portugaliae Mathematica

Every strict sum of cubes in $\mathbb{F}_4[t]$ is a strict sum of 6 cubes

Luis H. Gallardo

(Communicated by Arnaldo Garcia)

Abstract. It is easy to see that an element $P(t) \in \mathbb{F}_4[t]$ is a strict sum of cubes if and only if $P(t) \in M(4)$ where

$$M(4) = \{P(t) \in \mathbb{F}_4[t] \mid P(r) \in \{0,1\} \text{ for all } r \in \mathbb{F}_4 \text{ and such that either 3 does not divide } \deg(P(t)), \text{ or 3 does divide } \deg(P(t)) \text{ and } P(t) \text{ is monic}\}.$$

We say that $P(t)$ is a "strict" sum of cubes $A_1(t)^3 + \cdots + A_g(t)^3$ if $\deg(A_i^3) < \deg(P) + 3$ for each i, and we define $g(3, \mathbb{F}_4[t])$ as the least g such that every element of $M(4)$ is a strict sum of g cubes. The main result is that

$$g(3, \mathbb{F}_4[t]) \le 6.$$

This improves an earlier result of the author that $g(3, \mathbb{F}_4[t]) \le 9$.

Mathematics Subject Classification (2000). 11T55; 11C08, 11T06, 11E76, 11P05.

Keywords. Waring's problem, polynomials, forms, cubes, cubic forms, characteristic two, finite fields.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic 2 with q elements. It is easy to identify the set $M(q)$ of polynomials $P \in \mathbb{F}_q[t]$ that are strict sums of cubes. When $q > 4$ the set $M(q)$ is the entire ring $\mathbb{F}_q[t]$. For $q = 4$ the set $M(q)$ consists of polynomials $P \in \mathbb{F}_4[t]$ for which $P(r)$ lies in $\mathbb{F}_2$ for every $r \in \mathbb{F}_4$, and such that either 3 does not divide $\deg(P)$ or 3 divides $\deg(P)$ and P is monic. Finally $M(2)$ is the set of $P \in \mathbb{F}_2[t]$ such that $P \equiv 0$ or $P \equiv 1 \pmod{t^2 + t + 1}$; see [3].

Let $v(3, \mathbb{F}_q[t]) = v \ge 0$ be the minimal integer such that every P that is a sum of cubes is a sum of v cubes. In 1933, see [6], [7], Paley proved that

$$v(3, \mathbb{F}_q[t]) \le 5$$

for $q \in \{2,4\}$. Later, in [8], Vaserstein improved the result for $q = 2$ to

$$v(3, \mathbb{F}_2[t]) \leq 4.$$

The actual value of $v(3, \mathbb{F}_q[t])$ for $q \in \{2,4\}$ is unknown.

An analogue over $\mathbb{F}_q[t]$ of Waring's problem for cubes over the integers is that every $P \in M(q)$ is a *strict* sum of g cubes, with $g(3, \mathbb{F}_q[t]) = g \geq 0$ minimal. This means that

$$\deg(A^3) < \deg(P) + 3$$

when $P = A^3 + \cdots$ is written as a sum of cubes. We may re-write this condition as

$$\deg(A) \leq \left\lceil \frac{\deg(P)}{3} \right\rceil,$$

where $\lceil \alpha \rceil$ is defined as $\min\{n \in \mathbb{Z} \mid n \geq \alpha\}$. Notice that one can never write P as a sum of cubes with $\deg(A) < \lceil \deg(P)/3 \rceil$, so that the condition for a strict sum of cubes imposes the tightest possible constraint on the size of $\deg(A)$.

We may also let $c(3, \mathbb{F}_q[t]) = c \geq 0$ be the minimal integer such that every $P \in M(q)$ that is a strict sum of cubic forms $\Phi(X, Y) = XY(X+Y)$ is a *strict* sum of c cubic forms $\Phi(X, Y) = XY(X+Y)$. This means that

$$\deg(A^3) < \deg(P) + 3, \qquad \deg(B^3) < \deg(P) + 3,$$

when $P = AB(A+B) + \cdots$ is written as a sum of cubic forms $\Phi(X, Y) = XY(X+Y)$.

It is known that for $q = 2$ and for $q = 4$ one has

$$4 \leq g(3, \mathbb{F}_q[t]) \leq 9;$$

see [3]. These results are essentially based on some identities of Paley; see [6].

It is also known that for even q such that $q \notin \{2, 4, 16\}$ one has

$$c(3, \mathbb{F}_q[t]) \leq 5;$$

see [2].

Recently, in [4], the author together with D. R. Heath-Brown proved that

$$5 \leq g(3, \mathbb{F}_q[t]) \leq 6$$

for $q = 2$ by using some simple identities in a new way. The same method cannot help very much for $q = 4$ since it is really tailored for $q = 2$.

However, using a slight variant of the method we succeeded recently in extending the result to $q = 4$. Moreover, we obtained immediately upper bounds for the representation of all possible polynomials as strict sums of cubic forms $\Phi(A, B) = AB(A + B)$.

More precisely, the main object of this paper is to prove

$$g(3, \mathbb{F}_4[t]) \leq 6; \tag{1}$$

see Corollary 1.

From this follows immediately that

$$c(3, \mathbb{F}_4[t]) \leq 3; \tag{2}$$

see Proposition 1.

The same method of proof gives immediately a result that completes earlier work of the author: We have

$$c(3, \mathbb{F}_2[t]) \leq 3; \tag{3}$$

see Proposition 3.

Using some results in [1] it is straightforward to obtain also

$$c(3, \mathbb{F}_q[t]) \leq 4, \tag{4}$$

when $q > 4$ is of the form $q = 2^{2n}$ for some positive integer $n > 1$; see Proposition 2.

The problem of giving non-trivial lower bounds (i.e. >2) for our functions g and c is not easy for general q. Even for a fixed small value of q to get a non-trivial lower bound may require some substantial computations (with computers) to be done. Also note that, unfortunately, our method does not allow us to improve the bound $g(3, \mathbb{F}_q[t]) \leq 7$ which holds even for $q > 16$ (see [3], Introduction, or [1], Theorem 1).

Some applications to the problem of the strict representation of a polynomial P as

$$P = A^2 + A + BC$$

(see [5]) are also included. See Proposition 4.

The new idea used to obtain the main result of this paper arises from a refinement of the (trivial) observation that every element of $\mathbb{F}_q$ is a square when q is even.

We denote by α a root of the polynomial $t^2 + t + 1$ in a fixed algebraic closure of $\mathbb{F}_2$ so that $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$.

All rings are assumed commutative and with 1.

2. Identities and descent

The following lemmas are crucial to obtain our main results. First of all we introduce some notation.

Lemma 1. *Let B be a ring of characteristic 2. Let $R = B[t]$ be the polynomial ring in one indeterminate t over B. Let $L : R \to R$ be defined by $L(y) = y^2 + y$, and let $C : R \to R$ be defined by $C(r) = rt(r + t)$. Then L and C are $\mathbb{F}_2$-linear functions.*

Secondly, using the same notations as in Lemma 1 we present two simple identities that hold when every element of the ground ring B is a perfect square (i.e., when B is perfect).

Lemma 2. *Let B be a perfect ring of characteristic 2. Let $R = B[t]$ be the polynomial ring in one indeterminate t over B. Let $a \in B$ be written as $a = s^2$ with $s \in B$, and let $n \geq 0$ be a non-negative integer. One has*

$$at^{2n} = (at^{2n} + st^n) + st^n = L(st^n) + st^n, \tag{5}$$

and

$$at^{2n+1} = (st^n)^2 t + (st^n)t^2 + st^{n+2} = C(st^n) + st^{n+2}. \tag{6}$$

Let us recall the following identities.

Lemma 3. *Let B be a perfect ring of characteristic 2. Let $R = B[t]$ be the polynomial ring in one indeterminate t over B. Let $y, r \in R$. Then:*

(i) $y^2 + y = (y + 1)^3 + y^3 + 1^3$.

(ii) *If B contains $\mathbb{F}_4$ then $y^2 + y = (y + \alpha)^3 + (y + \alpha + 1)^3$.*

(iii) $rt(r + t) = (r + t)^3 + r^3 + t^3$.

(iv) *If B contains $\mathbb{F}_4$ then $rt(r + t) = (r + t\alpha)^3 + (r + t + t\alpha)^3$.*

(v) *Assume that B contains $\mathbb{F}_4$ then we may rewrite* (iv) *as*

$$r^3 + y^3 = cd(c + d),$$

where $c = r\alpha^2 + y$ and $d = r + \alpha^2 y$.

(vi) *If B contains $\mathbb{F}_4$ then $y^3 = y(\alpha y)(y + \alpha y)$.*

The following is a simple but useful lemma:

Lemma 4. *Let B be a perfect ring of characteristic 2. Let $R = B[t]$ be the polynomial ring in one indeterminate t over B. Let $r \in R$ be an element of R.*

Then

$$rt(r+t)+t^3=(r+t\alpha)t(r+t\alpha+t). \tag{7}$$

Our first result (for the case $q=2$ see also [4], Proposition 1b)) is:

Lemma 5. *Let $n>0$ be a positive integer. Let $q=2^n$ and let $P\in\mathbb{F}_q[t]$ be a polynomial. Then there exist $a,b,c\in\mathbb{F}_q$ and $A,Q\in\mathbb{F}_q[t]$ such that*

$$P=A^2+A+Qt(Q+t)+at^3+bt+c \tag{8}$$

where

$$\max\{\deg(A^2),\deg(Q^2t)\}\le\deg(P).$$

Proof. If $\deg(P)\le 3$ we choose $A=Q=0$. If $\deg(P)>3$, the claim follows by induction from the reduction formulae of Lemma 2 used to remove the leading term of P together with the addition properties proved in Lemma 1. More precisely, we can collect all terms containing the function L, and by doing the same for all terms where the function C appears we obtain the result. □

Now (recall that $L(y)=y^2+y$) it follows a lemma concerning membership in $M(4)$ of polynomials of small degree.

Lemma 6. *Let $a,b,c,d\in\mathbb{F}_4$ such that $K(t)=ct^3+dt^2+at+b$ is a sum of cubes. One has: If $d=0$ then*

(i) $K(t)=t^3$ *or* $K(t)=t^3+1^3$ *or*

(ii) $K(t)=1^3$ *or* $K(t)=0^3$.

If $d\neq 0$ and $c\neq 0$ then

(iii) $K(t)=t^3+L(t)=(t+1)^3+1^3$ *or* $K(t)=t^3+L(t)+1=(t+1)^3$ *or*

(iv) $K(t)=t^3+L(\alpha t)=(\alpha t+1)^3+1^3$ *or* $K(t)=t^3+L(\alpha t)+1=(\alpha t+1)^3$ *or*

(v) $K(t)=t^3+L(\alpha^2t)=(\alpha^2t+1)^3+1^3$ *or* $K(t)=t^3+L(\alpha^2t)+1=(\alpha^2t+1)^3$.

If $d\neq 0$ and $c=0$ then

(vi) $K(t)=L(t)=(t+\alpha)^3+(t+\alpha+1)^3$ *or* $K(t)=L(t)+1=(t+1)^3+t^3$ *or*

(vii) $K(t)=L(\alpha t)=(t+1)^3+(t+\alpha)^3$ *or* $K(t)=L(\alpha t)+1=(\alpha t+1)^3+t^3$ *or*

(viii) $K(t)=L(\alpha^2t)=(t+1)^3+(t+\alpha+1)^3$ *or* $K(t)=L(\alpha^2t)+1=(\alpha^2t+1)^3+t^3$.

(ix) $K(t)$ *is a strict sum of* 2 *cubes.*

Proof. The proof of parts (i) to (viii) is clear from Lemma 3, the definition of L and the fact that the only sums of cubes in $\mathbb{F}_4$ are 0 and 1. Part (ix) follows from parts (i) to (viii). $\square$

We are ready to present our descent results. First of all a descent lemma for cubes:

Lemma 7. *Let $n > 1$ be an integer. Let q be a power of 2. Let $P \in M(q)$ be a monic polynomial of degree $d = 3n$. Then there exist polynomials $A, R \in \mathbb{F}_q[t]$ such that*

(a) $P = A^3 + R$,

(b) $\deg(A) = n$,

(c) $\deg(R) \leq 2n$,

(d) $R(0) = 0$ *when* $q = 4$.

Proof. Set $A = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ with unknown coefficients $a_j \in \mathbb{F}_q$. Now fix any $a_0 \in \mathbb{F}_q$ and choose $a_{n-1}, \ldots, a_1 \in \mathbb{F}_q$ so that $R = P - A^3$ has degree at most equal to $2n$. This gives a soluble triangular linear system of $n - 1$ equations in $n - 1$ unknowns, and (a), (b) and (c) are proven.

To show (d) set $q = 4$. Take $a_0 = P(0)$. Choose $a_{n-1}, \ldots, a_1 \in \mathbb{F}_4$ as before. Since $P \in M(4)$ it is clear that $a_0 \in \{0, 1\}$, hence $P(0) = a_0 = a_0^3$ and so $R(0) = P(0) - a_0^3 = 0$. $\square$

Secondly, we present a descent lemma for cubic forms.

Lemma 8. *Let $n > 1$ be an integer. Let $P \in \mathbb{F}_2[t]$ be a polynomial of degree $d \in \{3n - 1, 3n - 2\}$. Then there exist polynomials $B, R \in \mathbb{F}_2[t]$ such that*

(a) $P = t^n B(t^n + B) + R$,

(b) $\deg(B) = n$,

(c) $\deg(R) < 2n$.

Proof. Determine the coefficients of $B = t^n + b_{n-1}t^{n-1} + \cdots + b_0$ in $\mathbb{F}_2$ such that $R = P + t^n B(t^n + B)$ be of degree $< 2n$. This results in a soluble triangular linear system of n equations with n unknowns. $\square$

3. Main results

We are now ready to present our key result.

Theorem 1. *Any polynomial $P \in M(4)$ with* $\deg(P)$ *a multiple of* 3 *is a strict sum of* 5 *cubes.*

Proof. Suppose that $\deg(P) = 3n$. The case $n = 0$ is trivial, so assume that $n \geq 1$. If $n = 1$ then the result follows by part (ix) of Lemma 6. Assume now that $n \geq 2$. Then by Lemma 7 we obtain that $P = A^3 + R$ so that we can apply Lemma 5 to R to get

$$P = A^3 + B_1(B_1 + 1) + B_2 t(B_2 + t) + at^3 + bt. \tag{9}$$

It follows that $K(t) = at^3 + bt$ is a sum of cubes. So, by Lemma 6(i) or (ii), we get $a \in \{0, 1\}$ and $b = 0$. By (7) in Lemma 4 we have

$$S = B_2 t(B_2 + t) + at^3 + bt = (B_2 + t\alpha)t\big((B_2 + t\alpha) + t\big).$$

if $a = 1$, and $S = B_2 t(B_2 + t)$ if $a = 0$.

Thus, by Lemma 3(ii), $B_1(B_1 + 1)$ is a sum of 2 cubes. Moreover, Lemma 3(iv) implies that S equals a sum of 2 cubes.

It follows that P is a strict sum of 5 cubes. □

Corollary 1. *Any polynomial $P \in M(4)$ is a strict sum of* 6 *cubes.*

Proof. This follows from Theorem 1 when $\deg(P) = 3n$. If $\deg(P) = 3n - 1$ or $3n - 2$ one applies Theorem 1 to $P - t^{3n}$. □

Proposition 1. *Any polynomial $P \in M(4)$ is a strict sum of* 3 *cubic forms $\Phi(X, Y) = XY(X + Y)$.*

Proof. This follows from Corollary 1 together with the formula in part (v) of Lemma 3. More precisely, the formula shows that a sum of 2 cubes requires only 1 cubic form $\Phi(X, Y)$. □

More generally we have the following result.

Proposition 2. *Let $n > 1$ be an integer. Any polynomial $P \in \mathbb{F}_{2^{2n}}[t]$ is a strict sum of* 4 *cubic forms $\Phi(X, Y) = XY(X + Y)$.*

Proof. Set $q = 2^{2n}$. Observe that every polynomial in $\mathbb{F}_q[t]$ is a strict sum of 7 cubes when $q \neq 16$ and that every polynomial in $\mathbb{F}_{16}[t]$ is a strict sum of 8 cubes; see [1], Theorem 1. Thus the result follows from the formulae in (v) and (vi) of Lemma 3. The former formula shows that a sum of 2 cubes requires two cubic forms to be represented. The latter formula shows that one cube requires only one cubic form to be represented. □

Now we study representations by cubic forms $\Phi(X, Y) = XY(X + Y)$ for $q = 2$.

Observe (see [4]) that for $q = 2$ the set S of sums of cubic forms $\Phi(X, Y) = XY(X + Y)$ is the following subset of $M(2)$:

$$S = \{P \in M(2) \mid (t^2 + t) \mid P\}. \tag{10}$$

Take $P \in S$. Using Lemma 8 together with Lemma 8 we obtain the strict decomposition

$$P = AB(A + B) + A_1^2 + A_1 + B_1 t(B_1 + t) + at^3 + bt + c,$$

where $a, b, c \in \mathbb{F}_2$ and we may take $A = 0$ when $d = \deg(P) < 4$. But since $A = t^n$ is a positive power of t for $d \geq 4$, the condition $P \in S$ forces $c = P(0) = 0$ and also $a + b = P(1) = 0$. Finally, using Lemma 3(iii) observe that that $CD(C + D)$ takes values 0, 1 if $t = \alpha$. So $a\alpha^3 + b\alpha + P(\alpha) \in \{0, 1\}$, i.e., $a + b\alpha \in \mathbb{F}_2$, but this forces $b = 0$. Hence $a = b = c = 0$.

This proves

Proposition 3.

$$c(3, \mathbb{F}_2[t]) \leq 3.$$

Now we present a couple of applications of Lemma 5.

In [5] it was asked to give explicit strict representations of $P \in \mathbb{F}_q[t]$, q even, in the form

$$P = A^2 + A + BC.$$

This question may have some interest since using an indirect method of Serre we were able to prove the existence of such representations, with some exceptions when $q \in \{2, 4\}$; see [5]. The answer seems to be non-trivial. It may also have some interest to construct some algorithm which computes the values of A, B, C for given P as above.

We can now address the latter question in the cases where $q \in \{2, 4\}$ by constructing infinite subsets of polynomials in $M(2)$ (respectively in $M(4)$) for which we can compute in finite time values of A, B, C as above for every P that is a member of such subsets.

Proposition 4. *Let*

$$S_2 = \{P \in M(2) \mid P(0) = 0 = P(1)\},$$

and let

$$S_4 = M(4).$$

Then:

(a) *Every* $P \in S_2$ *has a computable strict representation as* $P = A^2 + A + BC$.

(b) *Every* $P \in S_4$ *has a computable strict representation as* $P = A^2 + A + BC$.

(c) S_2 *and* S_4 *are infinite.*

Proof. The sets S_4 and S_2 both contains $t^{3n}(t^{3n}+1)$ for all $n > 0$, so they are infinite. This proves (c).

From Lemma 5 we have a strict decomposition

$$P = A^2 + A + Bt(B+t) + at^3 + bt + c \tag{11}$$

for some $a, b, c \in \mathbb{F}_q$ with $q \in \{2, 4\}$. Assume that $P \in S_4$. Since $P(0) \in \mathbb{F}_2$, we deduce from (11) that $c \in \{0, 1\}$. If $c = 1 = \alpha(\alpha+1)$ then we replace A by $A + \alpha$. So we may assume that $c = 0$. From (11) we obtain that $at^3 + bt + c \in M(4)$, so by Lemma 6(i) or (ii), one has $b = 0$ and $a \in \{0, 1\}$. If $a = 0$ then (11) gives the desired result since $a = b = c = 0$. If $a = 1$ then we recall from (7) in Lemma 4 that

$$Bt(B+t) + t^3 = (B + t\alpha)t(B + t\alpha + t).$$

Thus (11) gives the desired representation, i.e., we have proved (b).

Now for $q = 2$, i.e., for $P \in S_2$, observe that $S_2 = S$ as defined in (10). The proof of Proposition 3 applies here to show that $a = b = c = 0$, so that we obtain the assertion. This shows (a), and the proof is finished. □

Acknowledgments. We thank the referee for fruitful criticism.

References

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

[2] L. Gallardo, Une variante du problème de Waring sur $\mathbb{F}_{2^n}[t]$. *C. R. Acad. Sci. Paris Sér. I Math.* **327** (1998), 117–121. Zbl 0922.11107 MR 1645076

[3] L. Gallardo, Waring's problem for cubes and squares over a finite field of even characteristic. *Bull. Belg. Math. Soc. Simon Stevin* **12** (2005), 349–362. Zbl 1111.11059 MR 2173698

[4] 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), 981–987. Zbl 05228792 MR 2360534

[5] L. Gallardo, O. Rahavandrainy and L. Vaserstein, Representations of polynomials over finite fields of characteristic two as $A^2 + A + BC + D^3$. *Finite Fields Appl.* **13** (2007), 648–658. Zbl 1127.11079 MR 2332492

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

[7] L. N. Vaserstein, Sums of cubes in polynomial rings. *Math. Comp.* **56** (1991), 349–357. Zbl 0711.11013 MR 1052104

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

Received November 11, 2006; revised February 7, 2007

L. H. Gallardo, Department of Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France

E-mail: Luis.Gallardo@univ-brest.fr