

Every sum of cubes in $\mathbb{F}_2[t]$ is a strict sum of 6 cubes

Luis H. Gallardo^{a,*}, D.R. Heath-Brown^b

^a *Department of Mathematics, University of Brest, 6, Avenue Le Gorgeu, C.S. 93837, 29238 Brest Cedex 3, France*

^b *Oxford University, Mathematical Institute, 24-29 St Giles, Oxford OX1 3LB, England*

Received 17 December 2005

Available online 11 April 2007

Communicated by Peter Jau-Shyong Shiue

Abstract

It is easy to see that an element $P(t) \in \mathbb{F}_2[t]$ is a sum of cubes if and only if

$$P(t) \in M(2) := \{P(t) : P(t) \equiv 0 \text{ or } 1 \pmod{t^2 + t + 1}\}.$$

We say that $P(t)$ is a “strict” sum of cubes $A_1(t)^3 + \cdots + A_g(t)^3$ if we have $\deg(A_i^3) \leq \deg(P) + 2$ for each i , and we define $g(3, \mathbb{F}_2[t])$ as the least g such that every element of $M(2)$ is a strict sum of g cubes. Our main result is then that

$$5 \leq g(3, \mathbb{F}_2[t]) \leq 6.$$

This improves on a recent result $4 \leq g(3, \mathbb{F}_2[t]) \leq 9$ of the first named author.

© 2007 Elsevier Inc. All rights reserved.

Keywords: Waring’s problem; Polynomials; Forms; Cubes; Cubic forms; 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 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

* Corresponding author. Fax: +33 2 98 01 67 90.

E-mail addresses: luis.gallardo@univ-brest.fr (L.H. Gallardo), rhb@maths.ox.ac.uk (D.R. Heath-Brown).

every $r \in \mathbf{F}_4$, 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 $P \in \mathbf{F}_2[t]$ such that $P(\alpha) \in \mathbf{F}_2$, where α an element of a fixed algebraic closure of $\mathbf{F}_2 = \{0, 1\}$ such that $\alpha^2 = \alpha + 1$ (see [2]).

Let $v(3, \mathbf{F}_q[t]) = v \geq 0$ be the minimal integer such that every $P \in M(q)$ is a sum of v cubes. In 1933, Paley proved that

$$v(3, \mathbf{F}_q[t]) \leq 5$$

for $q \in \{2, 4\}$ (see [3,4]). Later, in 1991, Vaserstein improved the result for $q = 2$ to

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

(see [5]). Observing that $t^2 + t + 1$ requires 3 cubes one has indeed

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

The actual value of $v(3, \mathbf{F}_2[t])$ is unknown.

An analogue over $\mathbf{F}_q[t]$ of the “ g ” of the Waring’s problem for cubes over the integers is as follows. Let $g(3, \mathbf{F}_q[t]) = g \geq 0$ be the minimal integer such that every $P \in M(q)$ is a *strict* sum of g cubes. Here this means:

$$\deg(A^3) \leq \deg(P) + 2$$

when $P = A^3 + \dots$ 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 $\min\{n \in \mathbb{Z}: n \geq \alpha\}$. 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 $\deg(A)$.

An alternative description of the condition for a strict sum of cubes arises from asking which binary forms $F(X, Y)$ over \mathbf{F}_q are sums of cubes of binary forms. Clearly one needs the degree of F to be a multiple of 3. Moreover if $Y^3 \nmid F(X, Y)$ one sees that any representation of $F(X, Y)$ as a sum of cubes of binary forms over \mathbf{F}_q corresponds to a representation of $F(t, 1)$ as a strict sum of cubes of polynomials in $\mathbf{F}_q[t]$.

Before the present paper the best known results on $g(3, \mathbf{F}_q[t])$ for $q = 2$ and $q = 4$ were

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

(see the first author’s work [2]). These results are essentially based on some identities of Paley (see [3]).

The aim of this paper is to prove four results on strict representations for $q = 2$.

(I) We have

$$5 \leq g(3, \mathbf{F}_2[t]) \leq 6. \quad (1)$$

(See Corollaries 1 and 2.)

- (II) If $P(t) \in M(2)$ then $P(t)$ is a strict sum of at most 5 cubes except, possibly, if $\deg(P)$ is not a multiple of 3 and $t(t+1) \mid P(t)$. (See Theorem 2 and Corollary 3.)
- (III) Every polynomial $P \in M(2)$ which is a multiple of $t(t+1)$ can be written as

$$P = A_1 B_1 (A_1 + B_1) + A_2 B_2 (A_2 + B_2)$$

with $A_1, B_1, A_2, B_2 \in \mathbb{F}_2[t]$ and $\deg(A_i B_i (A_i + B_i)) \leq \deg(P)$ for $i = 1, 2$. (See Theorem 1.)

- (IV) Every polynomial $P \in M(2)$ is either a strict sum of 5 cubes or can be written as

$$P = A_1 B_1 (A_1 + B_1) + A_2 B_2 (A_2 + B_2)$$

with $\deg(A_1 B_1 (A_1 + B_1)), \deg(A_2 B_2 (A_2 + B_2)) \leq \deg(P)$.

It is easy to see that if a polynomial $P \in \mathbb{F}_2[t]$ can be written as a sum of terms $A_i B_i (A_i + B_i)$ then we must have $P \in M(2)$ and $t(t+1) \mid P(t)$. We also note that (IV) is an immediate consequence of (II) and (III).

The actual value of $g(3, \mathbb{F}_2[t])$ is unknown. However, a computation shows that all polynomials in $M(2)$ of degree less than or equal to 18 are indeed strict sums of 5 cubes (see Lemma 3(c)). While we have several examples of polynomials in $M(2)$ which require 5 cubes for a strict representation, we do not know whether or not there are infinitely many such cases.

Observe that for any $k > 2$ with $\gcd(k, p) = 1$, where p is the characteristic of \mathbb{F}_q , it is unknown what is the exact value of the minimal number $g(k, \mathbb{F}_q[t])$ of k th powers that are required in order to represent strictly every polynomial in $\mathbb{F}_q[t]$ that is a sum of k th powers.

The new idea for this paper arises from an observation of the second author. In its original form it used the simple identities

$$t^2 u + t u^2 = (t+u)^3 + t^3 + u^3 \quad \text{and} \quad v + v^2 = (1+v)^3 + 1^3 + v^3 \quad (2)$$

to write any admissible polynomial P as a sum of 6 cubes A^3 with

$$\deg(A^2) \leq \deg(P),$$

see Proposition 1. We obtain our results as a refinement of this idea.

2. Identities and representation by 6 unrestricted cubes

The following lemmas are the keys to obtaining our main results. First of all we have two simple identities based on the observation that $y \rightarrow y^2 + y$ is linear over \mathbb{F}_2 .

Lemma 1. *Let q_1, q_2, r_1, r_2, t be elements of a ring of characteristic 2. One has:*

$$(i) \quad q_1^3 + (q_1 + 1)^3 + q_2^3 + (q_2 + 1)^3 = (q_1 + q_2)^3 + (q_1 + q_2 + 1)^3 + 1. \quad (3)$$

$$(ii) \quad r_1^3 + (r_1 + t)^3 + r_2^3 + (r_2 + t)^3 = (r_1 + r_2)^3 + (r_1 + r_2 + t)^3 + t^3. \quad (4)$$

Secondly, a simple application of the identities (2) gives:

Lemma 2. *Let t be an element of a ring of characteristic 2 and let $n \geq 0$ be a non-negative integer. One has*

$$t^{2n} = t^n + 1 + (t^n)^3 + (t^n + 1)^3 \quad (5)$$

and

$$t^{2n+1} = t^{n+2} + t^3 + (t^n)^3 + (t^n + t)^3. \quad (6)$$

Our first result is the following.

Proposition 1. *Let $P \in \mathbb{F}_2[t]$ be a polynomial.*

- (a) *If $P \in M(2)$ then P is a sum of 6 cubes A^3 satisfying $\deg(A^2) \leq \deg(P)$.*
 (b) *We can write $P = A^2 + A + Bt(B+t) + \beta t^3 + \gamma t + \delta$ where*

$$\max\{\deg(A^2), \deg(B^2t)\} \leq \deg(P),$$

and $\beta, \gamma, \delta \in \mathbb{F}_2$.

Proof. We first prove that any $P \in \mathbb{F}_2[t]$ is a sum of (a large number of) terms of the form $q^3 + (q+1)^3$ and $r^3 + (r+t)^3$, together with a remainder of the form $at^3 + bt + c$, in such a way that $\deg(q^2) \leq \deg(P)$ and $\deg(r^2t) \leq \deg(P)$. This is trivial if $\deg(P) \leq 3$, and otherwise follows by induction on $\deg(P)$, since we may use either (5) or (6) as appropriate to remove the leading term of P . Repeated use of the identities in Lemma 1 shows that

$$P = q^3 + (q+1)^3 + r^3 + (r+t)^3 + a't^3 + bt + c'. \quad (7)$$

Since $S(\alpha)^3 = 0$ or 1 for any $S \in \mathbb{F}_2[t]$, where $\alpha^2 + \alpha + 1 = 0$, we see that $b = 0$ if $P \in M(2)$. This proves (a). Since

$$\begin{aligned} P &= q^3 + (q+1)^3 + r^3 + (r+t)^3 + a't^3 + bt + c' \\ &= q^2 + q + rt(r+t) + (a'+1)t^3 + bt + (c'+1) \end{aligned}$$

statement (b) also follows.

We can use part (b) of Proposition 1 to deduce our first theorem. \square

Theorem 1. *Let $P(t) \in \mathbb{F}_2[t]$ and suppose that $t(t+1) \mid P(t)$ and $P(\alpha) = 0$ or 1, where α lies in a quadratic extension of \mathbb{F}_2 and satisfies $\alpha^2 + \alpha + 1 = 0$. Then we can write*

$$P(t) = A_1 B_1 (A_1 + B_1) + A_2 B_2 (A_2 + B_2)$$

with $\deg(A_i B_i (A_i + B_i)) \leq \deg(P)$ for $i = 1, 2$.

Before proving this we make some remarks. Firstly, our proof shows that one can indeed take $B_1 = 1$ and $B_2 = t$. Secondly, if $Q(t) = AB(A+B)$ then it is easy to see that $t(t+1) \mid Q(t)$ and that $Q(\alpha) = 0$ or 1. Thus if P can be written as a sum of any number of terms $AB(A+B)$,

without restrictions on the degree, then Q will satisfy the conditions of the theorem, and hence will be a strict sum of just two such terms. Thirdly, we note that if $Q(t)$ is any irreducible polynomial of degree at least 3, satisfying $Q(\alpha) = 1$, then $P(t) = t(t+1)Q(t)$ will satisfy the conditions of the theorem, but will not be of the form $AB(A+B)$. Thus there are infinitely many admissible polynomials which require two such terms. Finally we point out that if q is a power of 2, but not equal to 2, 4 or 16, then every polynomial in $\mathbb{F}_q[t]$ is a strict sum of at most 5 terms of the form $AB(A+B)$. This is proven by the first author [1].

Proof. In view of part (b) of Proposition 1 it suffices to show that if

$$P = A^2 + A + Bt(B+t) + \beta t^3 + \gamma t + \delta$$

then $\beta = \gamma = \delta = 0$. If $Q = RS(R+S)$ with $R, S \in \mathbb{F}_2[t]$ then we will have $t \mid Q$ and $t+1 \mid Q$. Moreover we will also have $Q(\alpha) = 0$ or 1. We therefore see that $\beta t^3 + \gamma t + \delta$ must be divisible by both t and $t+1$, whence $\delta = 0$ and $\beta = \gamma$. Moreover we must have $\beta \alpha^3 + \gamma \alpha + \delta = 0$ or 1, whence $\gamma = 0$. These conditions imply that $\beta = \gamma = \delta = 0$ as required. \square

3. Main results

First of all we report some computer calculations, which used a Maple 8 program on a Sun Fire 280R machine.

Lemma 3. Denote by $M(2, r)$ the set of all polynomials in $M(2)$ of degree less than or equal to r , and let $N(2, s, g)$ be the number of polynomials which are sums of g cubes A^3 with $\deg(A) \leq s$.

- (a) We have $N(2, 3, 2) = 115$, $N(2, 3, 3) = 416$ and $N(2, 3, 4) = 512$. Thus, since $\#M(2, 9) = 512$, all polynomials in $M(2, 9)$ are strict sums of 4 cubes, while 96 of them are not strict sum of 3 cubes. An explicit polynomial that requires 4 cubes is $X_1(t) = t^7 + t^2$.
- (b) We have $N(2, 4, 4) = 4082$ and $\#M(2, 12) = 4096$. Thus $M(2, 12)$ contains 14 polynomials which are not strict sums of 4 cubes. These polynomials are:

$$Y_1(t) = t^{12} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^5 + t^3 + t^2 + 1,$$

$$Y_2(t) = t^{12} + t^{10} + t^9 + t^7 + t^5 + t^4 + t^3 + t^2 + t + 1,$$

$$Y_3(t) = t^{12} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^6 + t^4 + t,$$

$$Y_4(t) = t^{12} + t^{11} + t^8 + t^7 + t^6 + t^4 + t^3 + t^2 + t,$$

$$Y_5(t) = t^{12} + t^{10} + t^9 + t^8 + t^7 + t^6 + t,$$

$$Y_6(t) = t^{12} + t^8 + t^7 + t^6 + t^3 + t^2 + t,$$

$$Y_7(t) = t^{12} + t^{11} + t^8 + t^7 + t^5 + 1,$$

$$Y_8(t) = t^{12} + t^7 + t^5 + t^4 + t + 1$$

and

$$Z_1(t) = t^{11} + t^{10} + t^9 + t^8 + t^6 + t^5 + t^4 + t + 1,$$

$$Z_2(t) = t^{11} + t^8 + t^6 + t^5 + t^4 + t^3 + t^2 + t + 1,$$

$$Z_3(t) = t^{11} + t^{10} + t^9 + t^6 + t^5 + t^4 + 1,$$

$$Z_4(t) = t^{11} + t^6 + t^5 + t^4 + t^3 + t^2 + 1,$$

$$Z_5(t) = t^{11} + t^{10} + t^9 + t^8 + t^6 + t,$$

$$Z_6(t) = t^{11} + t^6 + t^4 + t^3 + t^2 + t.$$

Moreover, these polynomials may be obtained from only $Z_1(t)$, $Z_3(t)$ and $Z_5(t)$ by the relations

$$Y_1(t) = t^{12}Z_1(1/t),$$

$$Y_2(t) = (t+1)^{12}Z_1(1/(t+1)),$$

$$Y_3(t) = t^{12}Z_3((t+1)/t),$$

$$Y_4(t) = t^{12}Z_1(1/t),$$

$$Y_5(t) = t^{12}Z_1((t+1)/t),$$

$$Y_6(t) = t^{12}Z_3(1/t),$$

$$Y_7(t) = (t+1)^{12}Z_3(t/(t+1)),$$

$$Y_8(t) = (t+1)^{12}Z_3(1/(t+1)),$$

$$Z_2(t) = Z_3(t+1), \quad Z_4(t) = Z_1(t+1), \quad Z_6(t) = Z_5(t+1).$$

We have independently verified, by hand, that $X_1(t)$ and $Z_5(t)$ require 4 and 5 cubes, respectively.

- (c) All 2^{15} polynomials in $M(2, 15)$ are strict sums of 5 cubes. In addition we have $N(2, 5, 2) = 1933$ and $N(2, 5, 3) = 22\,245$. Moreover we have $N(2, 6, 2) = 7814$ and $N(2, 6, 3) = 171\,904$. There are 84 805 polynomials of degree 16, 17 and 18 that are not strict sums of 3 cubes, and all these are strict sums of 5 cubes. Thus every element of $M(2, 18)$ (i.e., every admissible polynomial of degree at most equal to 18 in $\mathbf{F}_2[t]$) is a strict sum of 5 cubes.

The following corollary is immediate.

Corollary 1.

$$g(3, \mathbf{F}_2[t]) \geq 5.$$

We are now ready to present our key result.

Theorem 2. Any polynomial $P \in M(2)$ with $3 \mid \deg(P)$ is a strict sum of 5 cubes.

Proof. Suppose that $\deg(P) = 3n$. The case $n = 0$ is trivial, so suppose $n \geq 1$. Choose g so that $P - g^3$ has degree at most $2n - 1$. We will have $\deg(g) = n$. Set $A = P(0) + g(0) + 1$, $B = P(1) + g(1) + A$, and $h(t) = g(t) + Bt + A$. Then $P(0) = h(0) + 1$ and $P(1) = h(1)$. Moreover $P - h^3$ has degree at most $2n + 1$. Thus, as in (7), one can write $P - h^3 = j^2 + j + tk^2 + t^2k + r$, with $\deg(j^2) \leq 2n + 1$ and $\deg(k^2t) \leq 2n + 1$, and $r = at^3 + bt + c$. Thus $\deg(j) \leq n$ and $\deg(k) \leq n$. Moreover $j^2 + j + tk^2 + t^2k$ vanishes at both $t = 0$ and $t = 1$, while $P - h^3$ takes the values 1 and 0, respectively. Hence $c = 1$ and $a + b + c = 0$. Thus $P = h^3 + j^3 + (j+1)^3 + k^3 + (k+t)^3 + bt^3 + bt$. Since $P(\alpha) = 0$ or 1, and $m(\alpha)^3 = 0$ or 1

for any polynomial $m(t)$, we must have $b\alpha = 0$ or 1 , whence $b = 0$. Hence P is a strict sum of 5 cubes, as claimed. \square

Corollary 2. *Any polynomial $P \in M(2)$ is a strict sum of 6 cubes.*

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

Corollary 3. *Let $P \in M(2)$ and suppose that either $t \nmid P(t)$ or $t + 1 \nmid P(t)$. Then P is a strict sum of 5 cubes.*

Proof. Suppose that $\deg(P) = 3n$, $3n - 1$ or $3n - 2$, and consider the polynomial $Q(t) = t^{3n} P(t^{-1})$. If $t \nmid P(t)$ then we will have $\deg(Q) = 3n$ so that Q is a strict sum of 5 cubes $A_i(t)^3$, say, by Theorem 2. In particular we will have $\deg(A_i) \leq n$. Set $B_i(t) = t^n A_i(t^{-1})$. Then $\deg(B_i) \leq n$, and P will be a strict sum of the 5 cubes B_i^3 , as required. For the case $t + 1 \nmid P(t)$ we argue similarly with $Q(t) = (t + 1)^{3n} P((t + 1)^{-1})$. \square

References

- [1] L. Gallardo, Une variante du problème de Waring sur $\mathbf{F}_{2^n}[t]$ (An $\mathbf{F}_{2^n}[t]$ -variant of Waring's problem), C. R. Acad. Sci. Paris Sér. I Math. 327 (1998) 117–121.
- [2] L. Gallardo, Waring's problem for polynomial cubes and squares over a finite field of even characteristic, Bull. Belg. Math. Soc. Simon Stevin 12 (3) (2005) 349–362.
- [3] R.E.A.C. Paley, Theorems on polynomials in a Galois field, Quart. J. Math. 4 (1933) 52–63.
- [4] L.N. Vaserstein, Sums of cubes in polynomial rings, Math. Comp. 56 (1991) 349–357.
- [5] L.N. Vaserstein, Ramsey's theorem and the Waring's problem for algebras over fields, in: Proc. of Workshop on the Arithmetic of Function Fields, Ohio State Univ., 1991, de Gruyter, Berlin, 1992, pp. 435–442.