Bull. Korean Math. Soc. **46** (2009), No. 5, pp. 941–947
DOI 10.4134/BKMS.2009.46.5.941

EVERY POLYNOMIAL OVER A FIELD CONTAINING $\mathbb{F}_{16}$ IS A STRICT SUM OF FOUR CUBES AND ONE EXPRESSION $A^2 + A$

Luis H. Gallardo

Abstract. Let q be a power of 16. Every polynomial $P \in \mathbb{F}_q[t]$ is a strict sum

$$P = A^2 + A + B^3 + C^3 + D^3 + E^3.$$

The values of A, B, C, D, E are effectively obtained from the coefficients of P. The proof uses the new result that every polynomial $Q \in \mathbb{F}_q[t]$, satisfying the necessary condition that the constant term $Q(0)$ has zero trace, has a strict and effective representation as:

$$Q = F^2 + F + tG^2.$$

This improves for such q's and such Q's a result of Gallardo, Rahavandrainy, and Vaserstein that requires three polynomials F, G, H for the strict representation $Q = F^2 + F + GH$. Observe that the latter representation may be considered as an analogue in characteristic 2 of the strict representation of a polynomial Q by three squares in odd characteristic.

1. Introduction

Serre proved that every polynomial of $\mathbb{F}_q[t]$, with q odd (with a small number of exceptions when $q = 3$), is a strict sum of three squares. Gallardo, Rahavandrainy, and Vaserstein [6] proved by using the same method, (apply Weil's theorem to an appropriate curve) that for even q all (but a finite number of polynomials when $q < 8$,) polynomials P of $\mathbb{F}_q[t]$ are of the form (we say that they are decomposable):

$$P = A^2 + A + BC, \tag{1}$$

where $A, B, C \in \mathbb{F}_q[t]$ satisfy the tight condition:

$$\max(\deg(A^2), \deg(B^2), \deg(C^2)) < \deg(P) + 2.$$

All these polynomials are explicitly stated in the paper [6]: more precisely there are exactly 52 exceptional polynomials over $\mathbb{F}_2$ and 32 over $\mathbb{F}_4$.

Received August 4, 2008.
2000 *Mathematics Subject Classification.* 11T55, 11T06.
Key words and phrases. Waring's problem, quadratic polynomials, cubes, finite fields, characteristic 2.

The exceptions E are well behaved in the sense that it is easy to prove that for all of them $E + 1^3$ over $\mathbb{F}_2$ and $E + t^3$ over $\mathbb{F}_4$ are decomposable. Thus, every polynomial in $\mathbb{F}_q[t]$ has a strict representation of the form:

$$P = A^2 + A + BC + D^3$$

(so that $\deg(D^3) < \deg(P) + 3$).

Moreover, for every even q the only quadratic polynomials in three variables X, Y, Z that represent strictly all (but a finite number) of polynomials of $\mathbb{F}_q[t]$ are

$$XY + Z, \ \ X^2 + X + YZ, \ \ X^2 + YZ.$$

Observe that strict representations by the first and the last quadratic polynomials are trivial.

What we mean by "strict representations"?:

A *strict representation* of a polynomial P, by a quadratic polynomial $Q(x_1, \ldots, x_r)$, $r \in \mathbb{N}^*$, is the decomposition:

$$P = Q(A_1, \ldots, A_r),$$

where for all j, A_j is a polynomial such that

$$\deg(A_j^2) < \deg(P) + 2.$$

An analogue of a strict representation of $P \in \mathbb{F}_q[t]$ by 3 squares when q is odd, (so that P is also of the form $yz + x^2$) is the strict representation of $P \in \mathbb{F}_q[t]$ by the quadratic polynomial $x^2 + x + yz$ when q is even.

Furthermore, when q is odd, the polynomial P has a strict representation by the quadratic polynomial $x^2 + x + yz$ if and only if $-(P + 1/4)$ has a strict representation by $x^2 + y^2 + z^2$, since $-(x^2 + x + yz + 1/4) = -(x + 1/2)^2 - yz$, and since the quadratic forms $-x^2 - yz$ and $x^2 + y^2 + z^2$ are equivalent (see [1]) over $\mathbb{F}_q$.

In both representation problems above, a question that is not yet answered, is about the explicit representation of P. Given P can we obtain in some manner the values of A, B, C depending explicitly on P? This seems to be a difficult question. However, when $q \in \{2, 4\}$, by using a modification of the method used by Gallardo and Heath-Brown in [5], we were able, [4], to obtain effectively such solutions (i.e., we give an algorithm that compute (without trying all possibilities!) such solutions) for some infinite families of given polynomials P (including all strict sums of cubes when $q = 4$).

Assume that the field $\mathbb{F}_q$ contains the field $\mathbb{F}_{16}$, i.e., that q has the form

$$q = 2^{4n}$$

for some positive integer $n > 0$. This is required to be able to use the crucial identity Id1 of Lemma 2, in order to represent every polynomial as a sum of two cubes and one expression $A^2 + A$.

In this paper we prove (see Theorem 1) that, given P such that $\mathrm{Tr}(P(0)) = 0$, we can take $C = tB$ so that the representation (1) of P require only two parameters A, B instead of three A, B, C. Moreover, we can obtain effectively A, B from the coefficients of P.

It turns out that from this result and from a result of Gallardo [2, Lemma 8], we get a representation theorem with cubes for such P's and such q's.

This is our main result in this paper. Namely, (see Theorem 2) we have:

Every polynomial of $\mathbb{F}_q[t]$ is a strict sum of one expression $A^2 + A$ plus four cubes.

As before, we get effectively A and the four cubes from the coefficients of P.

Observe that Gallardo' results [2, Theorem 9] and [3, Theorem 7.1] addresses the classical problem of representation by strict sums of cubes and squares while, here in this paper, we address an analogue problem in which the expressions $A^2 + A$ represent a reasonable alternative to a square in characteristic 2.

2. Main lemmas

2.1. Some identities and a descent

The following results are easily checked.

We have the identity of Serre (see [8]), (slightly modified).

Lemma 1 (Serre). *Let F be a field of characteristic not equal to* 3, *in which there are two elements x, y such that $1 = x^3 + y^3$ and $xy \neq 0$. Let p be a nonzero element of F. Then we have Serre's identity*:

$$t = \left(\frac{p^6(x^3+1)+t}{3xp^4}\right)^3 + \left(\frac{p^6(x^3-2)+t}{3yp^4}\right)^3 + \left(\frac{p^6(2x^3-1)-t}{3xyp^4}\right)^3. \tag{2}$$

Lemma 2. *Let F be a field of characteristic* 2 *that contains the finite field $\mathbb{F}_{16}$ with sixteen elements. Let $\delta \in \mathbb{F}_{16}$ be defined by $\delta^4 = \delta + 1$, so that $\mathbb{F}_{16} = \mathbb{F}_2[\delta]$. Let $s = \delta^5$. Then the following identities holds in $F[t]$:*

Id1)

$$t + \delta^6 = t^3 + (t + \delta^2)^3 + (\delta t)^2 + \delta t. \tag{3}$$

Id2)

$$t = (\delta t + s)^3 + (\delta t + s + 1)^3 + (t + s\delta^2)^3 + (t + (1+s)\delta^2)^3. \tag{4}$$

Id3)

$$t = 1^2 + 1 + t \cdot 1^2. \tag{5}$$

Lemma 3. *Let $\mathbb{F}$ be a finite field of characteristic* 2 *unequal to the finite field with four elements $\mathbb{F}_4$. Let $g \in \mathbb{F}$ such that $g \neq 0$. There exist $a, b \in \mathbb{F}$, with $a \neq 0$ such that*

$$g = a^3 + b^3. \tag{6}$$

Lidl and Niederreiter [7, pages 295 and 327] proved this lemma.

The following result is a descent one.

Lemma 4. *Let $n > 1$ be an integer. Let q be a power of* 16. *Let $P \in \mathbb{F}_q[t]$ 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) $\deg(R) \le 2n$,
d) $R(0)$ *has zero trace.*

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 $a_0 \in \mathbb{F}_q$ such that $P(0) - a_0^3$ has zero trace. This is always possible: If $P(0)$ has zero trace just pick $a_0 = 0$. Otherwise, $P(0)$ has trace equal to 1 : Observe that for some $b \in \mathbb{F}_q$, b^3 is forced to have trace 1 since every element of $\mathbb{F}_q$ is a sum of two cubes (see Lemma 3) and the trace is $\mathbb{F}_2$-linear. Choose then $a_0 = b$.

Now, we choose $a_{n-1}, \ldots, a_1 \in \mathbb{F}_q$ in such a manner that $R = P - A^3$ has degree at most equal to $2n$. This results on a soluble triangular system of $n-1$ equations in $n-1$ unknowns. This proves a), b), c) and d). □

2.2. Other useful lemmata

First one is a trivial but useful lemma:

Lemma 5. *Let $\mathbb{F}$ be a perfect field of characteristic* 2. *Let $n \ge 0$ be a non-negative integer. Let $P \in F[t]$ be a polynomial of degree $\deg(P) \in \{2n+1, 2n\}$. Then there exist polynomials $A, B \in F[t]$, such that*

a)

$$P = A^2 + tB^2, \tag{7}$$

b) $\deg(A) = n$ *and* $\deg(B) < n$ *if* $\deg(P) = 2n$, *while* $\deg(A) \le n$ *and* $\deg(B) = n$ *if* $\deg(P) = 2n+1$. *So that*:
c)

$$\max(\deg(A^2), \deg(B^2)) < \deg(P) + 2.$$

We call A the even part of P and we call B the odd part of P.

Proof. Just take for A^2 the sum of all monomials of even degree that appear in P, and take for tB^2 the sum of all monomials of odd degree that appear in P. □

Now, we recall (see [2, Lemma 8]) the crucial lemma:

Lemma 6. *Let $\mathbb{F}$ be a perfect field of characteristic* 2 *such that every element in F is a sum of two cubes. Let $n \ge 0$ be a non-negative integer, and let $S \in F[t]$ be a polynomial with $\deg(S) \in \{3n+2, 3n+1, 3n\}$. Then there exist polynomials $A, B, C, D, Q \in \mathbb{F}[t]$ such that*

$$S = B(A^2 + tB) + D(C^2 + tD^2) + Q, \tag{8}$$

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

Next lemma is key:

Lemma 7. *Let* $\mathbb{F}$ *be a perfect field of characteristic* 2. *Let* $n \geq 0$ *be a non-negative integer. Assume that any polynomial* Q *in* $\mathbb{F}[t]$, *such that* $\mathrm{Tr}(Q(0)) = 0$, *is of the form*

$$Q = A^2 + A + tB^2 \tag{9}$$

for some polynomials $A, B \in \mathbb{F}[t]$ *with*

$$\max(\deg(A^2), \deg(B^2)) < \deg(P) + 2.$$

Let $P \in F[t]$ *be a polynomial of degree* $\deg(P) \in \{3n+2, 3n+1, 3n\}$. *Then there exist polynomials* $C, D, E, R \in F[t]$, *such that*

a)

$$P = C^3 + D^3 + E^2 + E + R, \tag{10}$$

b)

$$\max(\deg(C^3), \deg(D^3), \deg(E^2), \deg(R^3)) < \deg(P) + 3.$$

Proof. From Lemma 5 we write $P = P_0^2 + tP_1^2$, and $C = C_0^2 + tC_1^2$, $D = D_0^2 + tD_1^2$, $E = E_0^2 + tE_1^2$, $R = R_0^2 + tR_1^2$, where $C_0, \ldots, R_1$ are polynomials to be determined.

Observe (see Lemma 5) that CC_0 is the even part of C^3 and that CC_1 is the odd part of C^3. So, by comparing odd and even parts in both sides of (10), we see that the relation (10) is equivalent to the two relations:

$$P_0 = C_0C + D_0D + E + E_0 + R_0, \tag{11}$$

$$P_1 = C_1C + D_1D + E_1 + R_1. \tag{12}$$

Now, apply Lemma 6 to $P_1 + E_1$ to obtain suitable (i.e., polynomials that have the right degrees) C_0, C_1, D_1, D_0 and R_1.

So relation (12) holds.

By choosing R_0 such that $Q = P_0 + C_0C + D_0D + R_0$ has zero trace and by (9) applied to Q, we get suitable (polynomials that have the right degrees) E_0, E_1 so that the relation (11) also holds with polynomials of the right degrees. This proves the lemma. □

3. Main results

Theorem 1. *Let* $\mathbb{F}$ *be a finite field of characteristic* 2 *that contains the finite field with sixteen elements* $\mathbb{F}_{16}$. *Let* $P \in \mathbb{F}[t]$ *be any polynomial such that* $\mathrm{Tr}(P(0)) = 0$. *Then, there exist polynomials* $A, B \in \mathbb{F}[t]$ *which coefficients may be obtained from the coefficients of* P, *and such that*

$$P = A^2 + A + tB^2, \tag{13}$$

is a strict representation of P*, i.e., one has* $\deg(A^2) < \deg(P)+2$ *and* $\deg(B^2) < \deg(P) + 2$.

Proof. From Lemma 5 we have $P = P_0^2+tP_1^2$, and $A = A_0^2+tA_1^2$, $B = B_0^2+tB_1^2$, where $A_0, \dots, B_1$ are polynomials to be determined.

The condition (13) is equivalent to the system:

$$P_0 = A + A_0 = A_0^2 + A_0 + tA_1^2, \tag{14}$$

$$P_1 = B + A_1. \tag{15}$$

Observe that if relation (14) is solved for A_0, A_1, then we get immediately $B = P_1 + A_1$ from relation (15) so that we get also the values of B_0 and B_1.

So, it suffices by induction to prove that the relation (14) holds when P_0 has the minimal possible degree, (i.e., ≤ 1). But observe that the identity Id3 of Lemma 2 says that

$$P_0 = V^2 + V + tW^2,$$

where $V, W \in \mathbb{F}[t]$ have degree at most equal to the degree of P_0. This proves the theorem. $\square$

Observe that by using Serre's identity (2) in Lemma 2, we get immediately that any polynomial $P \in \mathbb{F}_{16^n}[t]$, $n > 1$, is an unrestricted sum of three cubes (four cubes over $\mathbb{F}_{16}$) plus one (albeit trivial, by setting $A = 1$) expression $A^2 + A$.

A better result follows immediately from identity Id1) in Lemma 2: namely any polynomial $P \in \mathbb{F}_{16^n}[t]$, is an unrestricted sum of two cubes plus one expression $A^2 + A$, (just replace t by $P - \delta^6$ in both sides of identity Id1).

Another observation is the following. It is easy to see that any polynomial $P \in \mathbb{F}_{16^n}[t]$, $n > 1$, is a strict sum of five cubes (six cubes over $\mathbb{F}_{16}$) plus one expression $A^2 + A$:

As a first step use Lemma 3 and (the descent in) Lemma 4 as to output two cubes and a remainder R with zero trace. As a second step apply Theorem 1 to the remainder R. As a third step use the identity (2) (or Id2) in Lemma 2 when $q = 16$).

The object of the next theorem is to improve on this. We give the best available result for the strict representations of P :

Theorem 2. *Let* $\mathbb{F}$ *be a finite field of characteristic* 2 *that contains the finite field with sixteen elements* $\mathbb{F}_{16}$*. Let* $P \in \mathbb{F}[t]$ *be any polynomial. Then* P *is a strict sum of four cubes plus one expression* A^2+A *with* $\deg(A^2) < \deg(P)+2$*. The coefficients of A and of each of such cubes are obtained from the coefficients of P.*

Proof. From Theorem 1 and Lemma 7 we have that:

$$P = C^3 + D^3 + E^2 + E + R, \tag{16}$$

with polynomials $C, D, E, R \in \mathbb{F}[t]$ of the right degree. Just apply now to the remainder R the identity Id1 to get

$$R = S^2 + S + U^3 + V^3, \tag{17}$$

where the polynomials $S, U, V \in \mathbb{F}[t]$ have degree bounded above by the degree of R. Combining the two relations (16) and (17) we obtain the result. $\square$

Acknowledgments. The author thanks the mathematician (that prefer to stay anonymous) that shared with the author some useful thoughts on a first version of the manuscript.

References

[1] E. Artin, *Geometric Algebra*, Wiley (Interscience), 1957.

[2] L. H. Gallardo, *On the restricted Waring problem over* $\mathbb{F}_{2^n}[t]$, Acta Arith. **92** (2000), no. 2, 109–113.

[3] ———, *Waring's problem for cubes and squares over a finite field of even characteristic*, Bull. Belg. Math. Soc. Simon Stevin **12** (2005), no. 3, 349–362.

[4] ———, *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.

[5] 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.

[6] L. H. 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), no. 3, 648–658.

[7] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, 20. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983.

[8] L. N. Vaserstein, *Sums of cubes in polynomial rings*, Math. Comp. **56** (1991), no. 193, 349–357.

[9] ———, *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.

Department of Mathematics
University of Brest
6, Avenue Le Gorgeu, C. S. 93837
29238 Brest Cedex 3, France
E-mail address: Luis.Gallardo@univ-brest.fr