PORTUGALIAE MATHEMATICA
Vol. 61 Fasc. 1 – 2004
Nova Série

WARING'S PROBLEM FOR POLYNOMIAL CUBES AND SQUARES OVER A FINITE FIELD WITH ODD CHARACTERISTIC

Luis Gallardo

Recommended by Arnaldo Garcia

Abstract: Let q be a power of an odd prime p. For $r \in \{1,2\}$ and $p \neq 3$, we give bounds for the minimal non-negative integer $g_r(3,2,\mathbf{F}_q[t]) = g$, such that every $P \in \mathbf{F}_q[t]$ is a strict sum of g cubes and r squares. Similarly we study for $p=3$, the number $g_1(2,3,\mathbf{F}_q[t]) = g$, such that every $P \in \mathbf{F}_q[t]$ is a strict sum of g squares and a cube. All bounds are obtained using explicit representations. Precisely our main results are:

(i) $2 \leq g_1(3,2,\mathbf{F}_q[t]) \leq 5$ when $p \neq 3$ and $q \notin \{7,13\}$.

(ii) $1 \leq g_2(3,2,\mathbf{F}_q[t]) \leq 4$ when $p \neq 3$ and for all $q \neq 7$.

(iii) $2 \leq g_1(2,3,\mathbf{F}_q[t]) \leq 3$ for all q when $p=3$.

The later item is of some interest since Serre gave an indirect proof of the fact that for $q \neq 3$ every polynomial in $\mathbf{F}_q[t]$ is a strict sum of 3 squares, and that for $q=3$ there are some exceptions (8 as precised by Webb) that require 4 squares.

1 – Introduction

The Waring's problem for cubes and squares for polynomials in $\mathbf{F}[t]$ over some field $\mathbf{F}$, is the analogue of the same problem over the integers $\mathbb{Z}$. If n is any integer we can represent it in the form

$$n = n_1^3 + \cdots + n_g^3 + m_1^2 + \cdots + m_h^2$$

for some non-negative integers g,h where the integers n_i, m_j for $i=1,...,g$ and $j=1,...,h$ have the same sign as n. So that $|n_i^3| \leq |n|$ for all $i=1,...,g$ and $|m_j^2| \leq |n|$ for all $j=1,...,h$.

Received: October 10, 2002; *Revised*: December 10, 2002.
AMS Subject Classification: 11T55, 11P05, 11D85.
Keywords: Waring's problem; polynomials; finite fields.

From Lagrange's theorem we can always take $h \leq 4$, and from Wieferich and Scholz work (See [Wi] and [Sc]) we can always take $g \leq 9$, so that we can say that the Waring's problem for cubes and squares over $\mathbb{Z}$ consists on determining or at least bounding the minimal such g, say $g_h(3,2,\mathbb{Z})$ when $h \leq 3$ is fixed, or vice versa, consists on determining or at least bounding the minimal such h, say $h_g(2,3,\mathbb{Z})$ when $g \leq 9$ is fixed.

Let us pass now to our problem: For the polynomials the notion of "positiveness" of the integers it is naturally replaced by conditions on degrees. We want to write all possible polynomials not barred by congruences as sums of cubes and squares in such a manner that the minimum cancellation occurs.

Let $\mathbf{F}$ be a field, and let $P \in \mathbf{F}[t]$ be a polynomial such that

$$P \,=\, c_1^3 + \cdots + c_s^3 + d_1^2 + \cdots + d_k^2$$

for some polynomials $c_1, ..., c_s, d_1, ..., d_k \in \mathbf{F}[t]$ such that $\deg(c_i^3) < \deg(P) + 3$ for all $i = 1, ..., s$ and $\deg(d_i^2) < \deg(P) + 2$ for all $i = 1, ..., k$. We then say that P is a strict sum of s cubes and k squares. For any $A \in \{c_1, ...c_s\}$, respectively $B \in \{d_1, ...d_k\}$, we say that A^3, respectively B^2 appear in the decomposition of P. We also say that a polynomial $Q \in \mathbf{F}[t]$ is a *strict* sum of cubes and squares if for some integers $r, s \geq 1$, Q is a strict sum of r cubes and s squares.

We denote for a fixed non-negative integer k, by $g_k(3,2,\mathbf{F}[t]) = g$, the minimal non-negative integer, if it exists, such that every P that is a strict sum of cubes and squares is a strict sum of g cubes and k squares; otherwise we put $g_k(3,2,\mathbf{F}[t]) = \infty$. Similarly, for a fixed non-negative integer s, we denote by $g_s(2,3,\mathbf{F}[t]) = h$ the minimal non-negative integer, if it exists, such that every P that is a strict sum of cubes and squares is a strict sum of s cubes and h squares; otherwise we put $g_s(2,3,\mathbf{F}[t]) = \infty$.

Let q be a power of an odd prime p and let $\mathbf{F}_q$ be the finite field with q elements. Set $S(q) = \{P \in \mathbf{F}_q[t] \ / \ P$ is a strict sum of cubes and squares in $\mathbf{F}_q[t]\}$.

From the celebrated result of Serre in [EH], see also Lemma 9.2, and from the results in [G] concerning the cubes, one has $h \leq 3$ when $q \neq 3$ and one has $g \leq 7$ when $p \neq 3$ and $q \notin \{7, 13\}$ and a sligthly higher bound for the other such q, so that the numbers $g_k(3,2,\mathbf{F}_q[t])$ and $g_s(2,3,\mathbf{F}_q[t])$ are well defined and bounded, so that, in particular, $S(q)$ equals the full ring $\mathbf{F}_q[t]$.

We prove in this paper that for any power q of an odd prime p one has the following results. We assume that $p \neq 3$ in results i) to iii)

i) $2 \leq g_1(3,2,\mathbf{F}_q[t]) \leq 5$ when $q \notin \{7,13\}$; and $2 \leq g_1(3,2,\mathbf{F}_q[t]) \leq 6$ otherwise. (See Theorem 7.1).

ii) $1 \leq g_2(3,2,\mathbf{F}_q[t]) \leq 4$ for all $q \neq 7$ while $2 \leq g_2(3,2,\mathbf{F}_q[t]) \leq 4$ when $q \neq 7$ and $q \equiv 3 \pmod 4$. Moreover one has $2 \leq g_2(3,2,\mathbf{F}_q[t]) \leq 5$ when $q = 7$. (See Theorem 8.1).

iii) $1 \leq g_2(3,2,\mathbf{F}_q[t]) \leq 3$ when $q \equiv 1 \pmod 4$. (See Theorem 8.2).

iv) $2 \leq g_1(2,3,\mathbf{F}_q[t]) \leq 3$ for all q when $p = 3$; while $g_1(2,3,\mathbf{F}_q[t] = 3$ when $p = 3$ and $\mathbf{F}_q$ does not contain $\mathbf{F}_9$. (See Theorem 9.1).

The proof of the latest item shows how to explicitly represent every polynomial in $\mathbf{F}_{3^n}[t]$, for all positive integers n, as a strict sum of 3 squares and a cube. This is of some interest since Serre gave, in [EH], an indirect proof of the fact that for $q \neq 3$, or for $q = 3$, in this latter case, with the exception of 2 polynomials of degree 3 and of 6 polynomials of degree 4 that require 4 squares (as showed by Webb in [We]), every polynomial in $\mathbf{F}_q[t]$ is a strict sum of 3 squares.

The analogue of our results (but without restrictions on degrees), i.e. the analogue of the "easy" Waring's problem over the integers $\mathbb{Z}$, (see e.g. [HW]) is trivial and can be represented by the identity in Lemma 3.2 a) that shows every polynomial as a sum of 2 cubes and a square.

A word on some classic notation and conventions used: Given some field $\mathbf{F}$, we say that a polynomial $P \in \mathbf{F}[t]$ is *monic* if his leading coefficient equals 1. We also put $-\infty$ for the degree of the 0 polynomial so that $\deg(0) < n$ for all positive integers n.

2 – Method of proof

We choosed a wholly elementary method (linear algebra and identities, see here below) to get our results. Indeed, mathematically more interesting and powerful methods as the circle method or a generalization of Serre's method for studying the strict sums of squares decomposition of the polynomials in $\mathbf{F}_q[t]$ for $q \neq 3$, (see [EH]) seems to produce only weaker results on the particular problem of the Waring's problem for cubes and squares over $\mathbf{F}_q[t]$.

The method (say a “descending” one) consists, for a given polynomial $P \in \mathbf{F}_q[t]$, say of of degree $3n$,

$$P = a_{3n}\, t^{3n} + \cdots + a_0 \ ,$$

and with his leading coefficient a_{3n} beeing a cube in $\mathbf{F}_q$, roughly in:

a) Find a cube A^3 such that P and A^3 have a maximum of equal consecutive coefficients beginning by the leading coefficient.

b) Repeat a) with P replaced by $P-A^3$ till get a polynomial R which degree be less than $n+1$. Care is taken so that this can be done.

c) Apply some polynomial identities to R that show R as a sum of cubes S^3 and squares T^2 of polynomials with S, T of the same degree as R.

An “ascending” analogue method is also used in the paper.

3 – Identities

All results in this section are easily checked by a computation:

First of all, we have the identity of Serre, (see [V]) (slightly modified), and just after that some more specific identities.

Lemma 3.1 (Serre)**.** *Let* $\mathbf{F}$ *be a field of characteristic not equal to* 3*, such that the equation*

$$1 = x^3 + y^3$$

has at least one solution $x \in \mathbf{F}$, $y \in \mathbf{F}$, *such that* $xy \neq 0$. *Then for any nonzero* $p \in \mathbf{F}$ *we have the identity*

$$t = \left(\frac{p^6(x^3+1)+t}{3\,x\,p^4}\right)^3 + \left(\frac{-p^6(y^3+1)+t}{3\,y\,p^4}\right)^3 + \left(\frac{p^6(x^3-y^3)-t}{3\,x\,y\,p^4}\right)^3 . \ \blacksquare$$

Lemma 3.2. *Suppose that* $\mathbf{F}$ *is a field of characteristic* p. *Then the following identities hold.*

a) $t = (-3\,t - 1/9)^3 + (3\,t - 2/9)^3 + (3\,t + 1/9)^2$, *when* $p \neq 3$ *and*

b) $t^2 + 1/108 = (-t + 1/6)^3 + (t + 1/6)^3$ *when, furthermore,* $p \neq 2$.

c) $u\,w^2 = (u/6 + w)^3 + (-u/6)^3 + (u/6 - w)^3 + (-u/6)^3$ *when* $p \notin \{2, 3\}$.

d) $u\,w = (u/4 + w)^2 + (u/(4s) + s\,w)^2$ *when* $p \neq 2$ *and* $-1 = s^2$ *for some* $s \in \mathbf{F}$. ∎

Lemma 3.3. *One has the following identities in the ring* $\mathbf{F}_3[t]$*:*

a) $p_1(t) = t^3 + 2\,t + 1 = (t + 1)^3 + (t + 1)^2 + (t + 1)^2 + (t - 1)^2$.

b) $p_3(t) = t^4 + t + 1 = (2\,t)^3 + ((t + 1)^2)^2$.

and also six more deduced from them by the relations:

$$\begin{aligned}
p_2(t) &= 2t^3 + t + 1 = p_1(-t)\ ;\\
p_4(t) &= t^4 + 2t + 1 = p_3(-t)\ ;\\
p_5(t) &= t^4 + t^3 + 1 = p_3(-t - 1)\ ;\\
p_6(t) &= t^4 + 2t^3 + 1 = p_3(t - 1)\ ;\\
p_7(t) &= t^4 + 2t^3 + t = p_3(-t + 1)\ ;\\
p_8(t) &= t^4 + t^3 + 2t = p_3(t + 1)\ . \ ∎
\end{aligned}$$

4 – Squares and cubes in $\mathbf{F}_q$

Lemma 4.1. *Let* $\mathbf{F}$ *be a finite field with* q *elements such that* $\gcd(q, 6) = 1$. *Then*

a) *Every element* a *of* $\mathbf{F}$ *is a sum of* 2 *cubes if* $q \neq 7$*; it is a sum of* 2 *cubes if* $q = 7$ *and* $a \notin \{3, 4\}$ *and it is a sum of a nonzero square and a cube if* $a \in \{3, 4\}$.

b) 1 *is a sum of two non-zero cubes if* $q \notin \{7, 13\}$.

Proof: The result for $q = 7$ is easily checked by direct computation. The rest of the first result follows from [LN, p. 327] that refers to [S]. Another proof of a) for $q \neq 7$, is obtained by specializing k to 3 in [LN, Example 6.38, p. 295]. The same specialization of k proves b). ∎

5 – Ascent and descent

The proof of our first lemma is an “ascent one”:

Lemma 5.1. *Let* $\mathbf{F}$ *be a field of characteristic* p.

a) *Assume that every element in it is either a sum of 2 cubes or a sum of a nonzero square and a cube, and assume also that $p \notin \{2,3\}$. Let $n \geq 0$ be an integer and let P be in $\mathbf{F}$ if $n = 0$ and let $P \in \mathbf{F}[t]$ be a polynomial of degree $d \in \{3n, 3n-1, 3n-2\}$ otherwise. Then there exist $\alpha, B, C, S \in \mathbf{F}[t]$ with $\alpha \in \mathbf{F}$ when $n \neq 1$, respectively, $\deg(\alpha) \leq 1$ when $n = 1$; such that $\deg(A^2) < d+2$; $\deg(B^3) < d+3$; and*

$$P - t^{2n}S \;=\; \alpha^3 + A^2 + B^3$$

if $p_0 = P(0)$ is a sum of 2 cubes, in which case one has also $\deg(S) = d - 2n$; or if p_0 is a sum of a nonzero square and a cube and n is even and $d \in \{3n, 3n-1\}$ in which case $\deg(S) = n$. While

$$P - t^{2n-2}S \;=\; \alpha^3 + A^2 + B^3 \quad \textit{otherwise,} \quad \textit{in which case } \deg(S) = n\ .$$

b) *Assume now that every element in $\mathbf{F}$ is a cube and that $p \neq 2$. Then for any given polynomial $H \in \mathbf{F}[t]$ of degree $e \in \{2n, 2n+1\}$ there exist $A, R, S \in \mathbf{F}[t]$ and $\gamma \in \mathbf{F}$, such that*

$$H = \gamma^3 - A^2 + RS\ ,$$

where $\deg(A) = n = \deg(R)$ and $\deg(S) = e - n$.

Proof: We prove the second affirmation first. First of all set $\beta = H(0) + 1$ and $\beta = \gamma^3$ using the property of $\mathbf{F}$, that also allow us to assume that $n \geq 1$; so that the polynomial $G = H - \gamma^3$ satisfy $G(0) = -1$. Write $A = 1 + a_1 t + \cdots + a_n t^n$, in which the coefficients are to be determined by the condition $\deg(G + A^2) \geq n$. This results in a triangular linear system in the unknowns $a_1, ..., a_n$ corresponding to make the coefficient of t^r in $G + A^2$ equal to zero for $r = 1$ to $r = n-1$. The system is soluble since $A(0) = 1 \neq 0$ and $p \neq 2$. Setting $R = t^n$ this implies $H = \gamma^3 - A^2 + RS$, for some S with $\deg(S) = e - n$.

In order to prove the first affirmation a), set $p_0 = P(0)$ and let us consider two cases: Case 1: $p_0 = a^3 + b^3$ for some $a, b \in \mathbf{F}, b \neq 0$; respectively, Case 2: $p_0 = a^3 + b^2$ for some $a, b \in \mathbf{F}$, $b \neq 0$. Observe that if $p_0 = a^3 + b^3$ for some $a, b \in \mathbf{F}$ we can take $b \neq 0$, since if $p_0 = 0$ we take $b = -1$, $a = 1$ and if $p_0 \neq 0$ one of a, b is nonzero. This allow us also to assume that $n \geq 1$.

Case 1: First of all when $n = 1$, P has the form $P = a + bt + t^2(c + dt)$ for some $a, b, c, d \in \mathbf{F}$, so that the result follows from identity a) of Lemma 3.2 that shows $a+bt$ as a sum of 2 cubes and 1 square of degree at most 1. So that we assume that $n>1$.

Write $\alpha = a$ and $B = b + b_1 t + \cdots + b_n t^n$, in which the n unknown coefficients are determined by the condition $\deg(P - B^3 - \alpha^3) > n-2$ if $n \geq 3$ is odd, respectively by the condition $\deg(P - B^3 - \alpha^3) > n-1$ if $n \geq 2$ is even plus the supplementary condition that the coefficient of $Q = P - B^3 - \alpha^3$ in t^{n-1} when n is odd, respectively the coefficient of $Q = P - B^3 - \alpha^3$ in t^n be equal to 1 as in the proof of b) above. The corresponding system of linear equations is now soluble since $B(0) = b \neq 0$ and $p \neq 3$. So that we can set for some polynomial G with constant term equal to 1:

$$Q = (t^{(n-1)/2})^2 G \quad \text{if } n \text{ is odd}, \qquad Q = (t^{n/2})^2 G \quad \text{if } n \text{ is even}.$$

It remains to write $G = C^2 + t^n S$, when n is even, respectively $G = C^2 + t^{n+1} S$, when n is odd for some $C, S \in \mathbf{F}[t]$ where $\deg(C) \leq n$. This can be done as above by setting $C = 1 + c_1 t + \cdots + c_n t^n$, and solving the linear system of equations corresponding to the condition $\deg(G - C^2) > n$. The conditions $G(0) = 1$ and $p \neq 2$ shows that the above system is soluble.

Setting now $A = t^{(n-1)/2} C$ when n is odd, respectively $A = t^{n/2} C$ when n is even and $S = (P - \alpha^3 - A^2 - B^3)/t^{2n}$, we get the desired equality

$$P - t^{2n} S = \alpha^3 + A^2 + B^3 .$$

with α, A, B satisfying the desired conditions.

Case 2: The proof is similar to the above case. The main difference is that first we choose A and in a second step we choose B and finally S. Write $\alpha = a$ and $A = b + a_1 t + \cdots + a_e t^e$, in which the e unknowns coefficients are determined such that the coefficients of $P - \alpha^3 - A^2$ be all zero from the coefficient in t (the constant one is already zero from the choice of $A(0) = b$) to the coefficient in t^{e-1} and such that the coefficient of t^e be equal to 1. This results on a linear triangular system, soluble since $b \neq 0$ and $p \neq 2$. For the next step we need also that e be a multiple of 3. The value of e depend on d and the parity of n as follows: if $d = 3n-2$ and n is even we take $e = 3(n-2)/2$; if $d = 3n-2$ and n is odd we take $e = 3(n-1)/2$; while if $d \in \{3n-1, 3n\}$ then we take $e = 3n/2$ if n is even and $e = 3(n-1)/2$ if n is odd. With this choice of e one has $\deg(A^2) < \deg(P) + 2$ in all cases. It remains to find an $G, S \in \mathbf{F}[t]$ and integer f such that for

$$P - \alpha^3 - A^2 = (t^{e/3})^3 \, (G^3 + t^f S)$$

and $B = t^{e/3}G$, one has $\deg(B^3) < \deg(P) + 3$, and one get the corresponding formula in the lemma $P - t^{2n}S = \alpha^3 + A^2 + B^3$, or $P - t^{2n-2}S = \alpha^3 + A^2 + B^3$ with the right value of $\deg(S)$. We construct G in a similar manner as before, i.e. we write $G = 1 + g_1 t + \cdots + g_f t^f$, in which the f unknowns coefficients are determined such that the coefficients of $(P - \alpha^3 - A^2)/t^e - G^3$ be all zero from the coefficient in t (the constant one is already zero from the choice of $G(0) = 1$) to the coefficient in t^{f-1} and such that the coefficient of t^f be equal to 1. This determines also $S = ((P - \alpha^3 - A^2)/t^e - G^3))/t^f$. As before, this results on a linear triangular system, soluble since $G(0) = 1 \neq 0$ and $p \neq 3$. One get the following values of $f = \deg(G)$ and $\deg(S)$: $f = (n+2)/2$, $\deg(S) = n$ when $d = 3n-2$ and n is even; $f = (n-1)/2$, $\deg(S) = n$ when $d = 3n-2$ and n is odd; $f = n/2$, $\deg(S) = n$ when $d \in \{3n-1, 3n\}$ and n is even; $f = (n-1)/2$, $\deg(S) = n$ when $d \in \{3n-1, 3n\}$ and n is odd; so that all conditions are satisfied thereby finishing the proof of the lemma. ∎

The proof of our second lemma is a "descent one":

Lemma 5.2. *Let* $\mathbf{F}$ *be a field of characteristic* p, *with* $p \notin \{2, 3\}$, *in which every element is a sum of 2 cubes; respectively the elements that are not sum of 2 cubes are sums of 3 cubes. Let* $n \geq 0$ *be an integer and let* $P \in \mathbf{F}[t]$ *be a polynomial in* $\mathbf{F}[t]$, *that has degree* $d \in \{3n, 3n-1, 3n-2\}$ *for* $n \geq 1$ *and that satisfy* $P \in \mathbf{F}$ *for* $n = 0$. *Then each of the following affirmations holds for some* $A, B, S, C, R \in \mathbf{F}[t]$ *such that the showed representation of* $P - R$ *is a strict one:*

- **a)** $\deg(R) \leq 2n$ *and* $P - R = A^3 + B^3$ *if every element in* $\mathbf{F}$ *is a sum of 2 cubes; respectively* $P - R = A^3 + B^3 + S^3$ *if the elements in* $\mathbf{F}$ *that are not sum of 2 cubes are sums of 3 cubes.*
- **b)** $\deg(R) \leq n$ *and* $P - R = A^3 + B^3 + C^2$ *if every element in* $\mathbf{F}$ *is a sum of 2 cubes, respectively* $P - R = A^3 + B^3 + S^3 + C^2$ *if the elements in* $\mathbf{F}$ *that are not sum of 2 cubes are sums of 3 cubes.*
- **c)** *For* $d \neq 4$ *one has* $\deg(R^2) < d + 2$ *and* $P - R = A^3 + B^3 + C^3$ *if every element in* $\mathbf{F}$ *is a sum of 2 cubes, respectively* $P - R = A^3 + B^3 + S^3 + C^3$ *if the elements in* $\mathbf{F}$ *that are not sum of 2 cubes are sums of 3 cubes. While for* $d = 4$ *one has furthermore a* $W \in \mathbf{F}[t]$ *such that* $\deg(W) \leq 2$ *while* $\deg(R) = 2$ *and where* $\deg(A) \leq 1$ *and* $B, S \in \mathbf{F}$ *in such a manner that* $P = RW + A^3 + B^3$ *if every element in* $\mathbf{F}$ *is a sum of 2 cubes, respectively* $P = RW + A^3 + B^3 + S^3$ *if the elements in* $\mathbf{F}$ *that are not sum of 2 cubes are sums of 3 cubes.*

Proof: For $n = 0$ all results are trivially true so that we assume that $n \geq 1$. Write $P = p_d\, t^d + \cdots + p_0$. Assume that 3 does not divide d. We define $A = -t^n$ so that $Q = P - A^3$ has degree $3n$ and it is monic. Assume that $d \equiv 0 \pmod 3$, so that by hypothesis the leading coefficient p_d of P satisfy $p_d = a^3 + b^3 + s^3$ where we can always choose $a \neq 0$ and one has $s = 0$ if every element in $\mathbf{F}$ is a sum of 2 cubes; define $A = (bt)^n$ and $S = (st)^n$ and set $Q = P - A^3 - S^3$. In all cases Q has degree $3n$ and its leading coefficient $c \in \{1, a^3\}$ is a nonzero cube in $\mathbf{F}$. Let $B = c\, t^n + b_{n-1}t^{n-1} + \cdots + b_0$, with unknowns $b_{n-1}, ..., b_0$ in $\mathbf{F}$ to determine in such a manner that all coefficients of $R = Q - B^3$, from the coefficient of t^{3n-1}, to those of t^{2n+1} if any, be equal to zero. This results on a triangular linear system of $n-1$ equations over $\mathbf{F}$ in n unknowns $b_{n-1}, ..., b_0$ soluble since $c \neq 0$, and $p \neq 3$, thereby finishing the proof of a).

To prove c) first of all we study the special case when $d = 4$: Set $p_0 = P(0) = a^3 + r^3 + s^3$ with $a, r, s \in \mathbf{F}$ and $a \neq 0$. We can determine $b \in \mathbf{F}$ such that for the polynomial $A = a + bt$ one has $P - r^3 - s^3 = A^3 + q_2t^2 + q_3t^3 + q_4t^4$ for some $q_2, q_3, q_4 \in \mathbf{F}$ since $A^3 = a^3 + 3\,a^2bt + 3\,ab^2t^2 + b^3t^3$ and $a \neq 0$ and $p \neq 3$. Setting $R = t^2$ and $W = q_2 + q_3t + q_4t^2$ and setting $B = r,\ S = s$, one obtain the result. So that we assume $d \neq 4$ for the rest of the proof of c).

Observe that for $n \in \{1, 2\}$ the proof above of a) proves also c) provided $d \neq 4$ that is true, so that we take $n > 2$. Take A, Q, S, c as above and set now $3r$ equal to the least multiple of 3 that exceeds $2n-1$ and let $B = c\, t^n + b_{n-1}t^{n-1} + \cdots + b_0$, with unknowns $b_{n-1}, ..., b_0$ in $\mathbf{F}$ to determine in such a manner that all coefficients of $R_1 = Q - B^3$, from the coefficient of t^{3n-1}, to those of t^{3r+1} if any, be equal to zero and such that the coefficient of t^{3r} in R_1 be equal to 1. This results on a triangular linear system over $\mathbf{F}$ in at most n unknowns $b_{n-1}, ..., b_0$ soluble since $c \neq 0$ and $p \neq 3$. Similarly we determine C as a monic polynomial of degree r such that all coefficients of $R = R_1 - C^3$, from the coefficient of t^{3r}, to those of t^{2r} if any, be equal to zero. This proves c). For example in the worst case, say $3r = 2n + 2$ and $d = 3n - 2$ one has $\deg(C^3) = 2n + 2 < 3n + 1 = d + 3$ and $\deg(R^2) \leq 4r - 2 = (8n + 2)/3 < 3n = d + 2$.

To prove b) take A, Q, S, c as in the proof of a), let as above $B = c\, t^n + b_{n-1}t^{n-1} + \cdots + b_0$, with unknowns $b_{n-1}, ..., b_0$ in $\mathbf{F}$ to determine in such a manner that all coefficients of $R_1 = Q - B^3$, from the coefficient of t^{3n-1}, to those of t^{2n+1} if any, be equal to zero and such that the coefficient of t^{2n} in R_1 be equal to 1. This results on a triangular linear system of n linear equations over $\mathbf{F}$ in at most n unknowns $b_{n-1}, ..., b_0$ soluble since $c \neq 0$ and $p \neq 3$. Similarly we determine C

as a monic polynomial of degree n such that that all coefficients of $R = R_1 - C^2$, from the coefficient of t^{2n}, to those of t^{n+1} be equal to zero. This finishes the proof of the lemma. ∎

6 – Trivial lower bounds for $g_r(a, b, \mathbf{F}_q[t])$

Proposition 6.1. *Let q be a power of a prime p and $n > 2$, an integer. Then there exists a polynomial $P \in \mathbf{F}_q[t]$ of degree $6n$ such that P is not a strict sum of a cube and a square. So that one has: $g_1(a, b, \mathbf{F}_q[t]) \geq 2$ for $(a, b) \in \{(3, 2), (2, 3)\}$.*

Proof: Observe that there are q^{5n+2} couples (a, b) of polynomials such that $\deg(a) \leq 2n$ and $\deg(b) \leq 3n$. Therefore there are at most q^{5n+2} sums $a^3 + b^2$ with $\deg(a) \leq 2n$ and $\deg(b) \leq 3n$. Hence, for $(q, n) \neq (2, 2)$, among the $(q-1)q^{6n}$ polynomials of degree $6n$, some of them are not strict sums of a cube and a square. ∎

In the special case of a field of characteristic 3 we can say more:

Proposition 6.2. *Let $\mathbf{F}$ be a field of characteristic 3. Then any element of the infinite family $\{td^6\}$ where d is any nonzero polynomial in $\mathbf{F}[t]$ cannot be expressed as a square plus a cube in $\mathbf{F}[t]$; in particular one has $g_1(2, 3, \mathbf{F}[t]) \geq 2$.*

Proof: We assume that $td^6 = a^2 + b^3$ for some polynomials $a, b \in \mathbf{F}[t]$. Take derivative; then $d^6 = -aa'$. It cannot be the case that a is a cube for then $a^2 + b^3$ is a cube and t is a cube, a contradiction. Therefore some irreducible factor f of a occurs to a power n prime to 3. Then aa' is exactly divisible by f^{2n-1}, a contradiction since $2n - 1$ is not a multiple of 6. ∎

Proposition 6.3. *Let q be a power of an odd prime p. One has $g_2(3,2,\mathbf{F}_q[t]) \geq 1$. Furthermore, one has $g_2(3, 2, \mathbf{F}_q[t]) \geq 2$ and $g_1(2, 3, \mathbf{F}_q[t]) \geq 3$ when $q \equiv 3 \pmod 4$.*

Proof: Assume that $q \equiv 3 \pmod 4$ so that -1 is not a square in $\mathbf{F}_q$. Then the polynomial t cannot be written as a strict sum of 2 squares, necessarily of degree 1, and a cube, necessarily constant. This implies the two latest affirmations. On the other hand when $q \equiv 1 \pmod 4$ any irreducible polynomial $P \in \mathbf{F}_q[t]$ cannot be a strict sum of 2 squares $A^2 + B^2 = (A + Bi)(A - Bi)$, with $i^2 = -1$ in $\mathbf{F}_q$, so that we obtain the first affirmation. ∎

7 – Representation by a square and cubes

It is not known if every positive integer n is a sum of a square and 5 cubes. However, G.L. Watson proved in [Wa] that this is true for every sufficiently large integer n and R.C. Vaughan showed in [Vg] that the number of such representations is $\gg n^{7/6}$. No value is given in these two papers for the minimal large integer d such that for all $n \geq d$ one has that n is a sum of a square and five cubes.

For the far less demanding analogue problem, where the integer n is replaced by a polynomial P with coefficients in a finite field $\mathbf{F}_q$, and the representation is a strict one, one has:

Theorem 7.1. *Let $\mathbf{F}_q$ be a finite field of characteristic $p \notin \{2,3\}$, and let $P \in \mathbf{F}_q[t]$. Then P is a strict sum of 5 cubes and a square if $q \notin \{7,13\}$. A supplementary cube is required for $q \in \{7,13\}$. Indeed one has: $2 \leq g_1(3,2,\mathbf{F}_q[t]) \leq 5$ when $q \notin \{7,13\}$ and $2 \leq g_1(3,2,\mathbf{F}_q[t]) \leq 6$ when $q \in \{7,13\}$.*

Proof: The lower bounds came from Proposition 6.1. Set $d = \deg(P)$. First of all assume that $q \notin \{7,13\}$. Lemma 4.1 and Lemma 5.2 b) tell us that there is an $R \in \mathbf{F}_q[t]$ such that $\deg(R^3) < d+3$ for which one has the strict decomposition: $P - R = A^3 + B^3 + C^2$. Finally Lemma 4.1 b) allow us to apply Serre's identity in Lemma 3.1 to R, to yield 3 more cubes; this yields the claimed 5 cubes and 1 square for the strict representation of P. For $q = 13$ the proof is similar, the only change consists in using the identity c) of Lemma 3.2 with $u = R$ and $w = 1$ to get 4 more cubes, instead of applying Serre's identity. An analogue proof for $q = 7$ yields 7 cubes in the representation of P. In order to get instead 6 cubes, our proof below for $q = 7$ is slightly different since it require the use of the "ascent" in Lemma 5.1. In more detail, the Lemma 4.1 a) allows us to apply Lemma 5.1 a) to P to get $P = \alpha^3 + A^2 + B^3 + t^{2n}S$ where $\deg(S) = d - 2n$; or $P = \alpha^3 + A^2 + B^3 + t^{2n-2}S$ where $\deg(S) = n$; and always $\deg(A^2) < d + 2$; $\deg(B^3) < d + 3$; in which $d = \deg(P)$ satisfies $d = 0$ or $d \in \{3n, 3n-1, 3n-2\}$ otherwise. By setting $u = S$ and $w = t^n$, respectively $w = t^{n-1}$, in identity c) of Lemma 3.2 we obtain a strict decomposition of $t^{2n}S$, respectively of $t^{2n-2}S$, as a sum of 4 cubes. It follows that this yields the claimed 6 cubes and a square for the strict representation of P when $q = 7$. ∎

8 – Representation by 2 squares and cubes

In 1931 Stanley (see [St]) proved that every large integer is a sum of 4 non-negative cubes and 2 squares. We study here below the analogue decomposition of any polynomial in $\mathbf{F}_q[t]$.

Theorem 8.1. *Let $\mathbf{F}_q$ be a finite field of characteristic $p \notin \{2,3\}$, and let $P \in \mathbf{F}_q[t]$. Then P is a strict sum of 4 cubes and 2 squares when $q \neq 7$ and P is a strict sum of 5 cubes and 2 squares when $q = 7$. Indeed one has: $1 \leq g_2(3,2,\mathbf{F}_q[t]) \leq 4$ for $q \neq 7$; while $2 \leq g_2(3,2,\mathbf{F}_q[t]) \leq 4$ when $q \neq 7$ and $q \equiv 3$ (mod 4); respectively $2 \leq g_2(3,2,\mathbf{F}_q[t]) \leq 5$ for $q = 7$.*

Proof: The lower bounds came from Propositions 6.1 and 6.3. From Lemma 4.1 and from Lemma 5.2 a), (replacing R by $R+1/108$) we obtain the following strict decompositions $P-R-1/108 = a^3+b^3$ when $q \neq 7$, and $P-R-1/108 = a^3+b^3+c^3$ when $q = 7$. We will show two strict decompositions of P, the first one is non-effective since uses Serre's Lemma 9.2 to give a strict decomposition of R, say $R = d^2+e^2+f^2$ in which Lemma 3.3 gives $f^2+1/108 = (f+1/6)^3 + (-f+1/6)^3$. So that we have the strict decomposition of P

$$P \;=\; a^3+b^3+(f+1/6)^3+(-f+1/6)^3+d^2+e^2, \quad \text{when} \;\; q \neq 7$$

and similarly we obtain the strict decomposition of P

$$P \;=\; a^3+b^3+c^3+(f+1/6)^3+(-f+1/6)^3+d^2+e^2, \quad \text{when} \;\; q = 7\;.$$

To obtain our explicit second strict decomposition of P first of all we get a polynomial R with $\deg(R)^3 < \deg(P)+3$ from Lemmas 4.1 and 5.2 b). The following decompositions of $P-R$ are strict ones

$$P-R = A^3+B^3+C^2 \quad \text{for} \;\; q \neq 7, \quad \text{and}$$
$$P-R = A^3+B^3+S^3+C^2 \quad \text{for} \;\; q = 7\;.$$

The proof is finished by applying the identity a) of Lemma 3.2 to R. For example when $q \neq 7$ one get the following strict decomposition of P:

$$P \;=\; A^3+B^3+C^2+(-3R-1/9)^3+(3R-2/9)^3+(3R+1/9)^2\;. \;\blacksquare$$

In the special case when $q \equiv 1 \pmod 4$, i.e. when -1 is a square in $\mathbf{F}_q$ the upper bounds above are improved by 1 as follows:

Theorem 8.2. *Let $\mathbf{F}_q$ be a finite field of characteristic $p \notin \{2,3\}$, such that $q \equiv 1 \pmod 4$ and let $P \in \mathbf{F}_q[t]$. Then P is a strict sum of 3 cubes and 2 squares. Indeed one has: $1 \le g_2(3,2,\mathbf{F}_q[t]) \le 3$ for all such q.*

Proof: Assume $d = \deg(P) \neq 4$. From Lemma 5.2 c), that applies by Lemma 4.1, it follows that for some $R \in \mathbf{F}_q[t]$ with $\deg(R^2) < \deg(P) + 2$ one has that $P - R$ is a strict sum of 3 cubes. Finally identity d) in Lemma 3.2 shows R as a sum of two squares of the same degree that R. The lower bound follows from Proposition 6.3. The same proof works when $d = 4$ but replacing R by RW where $\deg(R) = 2$ and $\deg(W) \le 2$. ∎

Question 8.1: Is $g_2(3,2,\mathbf{F}_q[t])$ bounded above by 3 when $\gcd(q,6) = 1$ and $q \equiv 3 \pmod 4$?

9 – Representation by squares and a cube when q is a power of 3

Let q be a power of 3. We will study here the number $g_1(2,3,\mathbf{F}_q[t]) = g$, namely the least positive integer g such that every polynomial in $\mathbf{F}_q[t]$ is a strict sum of a cube and g squares.

First of all we recall two results proved in [EH]. The first is a classic lemma:

Lemma 9.1. *The quadratic forms $yz - x^2$ and $x^2 + y^2 + z^2$ are equivalent over a finite field of odd characteristic.* ∎

The second is a celebrated result of Serre (see Theorem 1.14 in [EH]) and Webb (see [W]):

Lemma 9.2 (Serre–Webb)**.** *Let q be be a power of an odd prime number. Except for the 2 polynomials $p_1(t), p_2(t)$ of degree 3 and the 6 polynomials $p_i(t)$, $i = 3, ..., 8$ of degree 4 in $\mathbf{F}_3[t]$ listed in Lemma 3.3 that require 4 squares, every $P \in \mathbf{F}_q[t]$ is the strict sum of 3 squares.* ∎

In particular one has:

Corollary 9.1. *Assume that q is a power of 3. Let $P \in \mathbf{F}_q[t]$, be any polynomial. Then P is a strict sum of 3 squares and a cube.*

Proof: Follows from Lemma 9.2 for all polynomials but the 8 polynomials $p_i[t] \in \mathbf{F}_3[t]$ in Lemma 3.3. This same lemma shows each of them as a strict sum of 3 squares plus a cube. ∎

Since the proof of the Serre–Webb's Lemma 9.2 is an indirect one, we show here below a constructive version of Corollary 9.1.

Theorem 9.1. *Assume that q is a power of 3. Let $P \in \mathbf{F}_q[t]$ be any polynomial. Then P is a strict sum of 3 squares and a cube. Moreover, the coefficients of the cubes and squares appearing in the decomposition of P can explicitly be given in terms of the coefficients of P. Indeed one has:*

$$2 \leq g_1(2,3,\mathbf{F}_q[t]) \leq 3 \quad \textit{for all} \;\; q$$

and $g_1(2,3,\mathbf{F}_q[t]) = 3$ when $\mathbf{F}_q$ does not contain the finite field $\mathbf{F}_9$.

Proof: The lower bound follows from Proposition 6.1; (it also follows from Proposition 6.2). Assume that $e = \deg(P) \in \{2n, 2n+1\}$. From Lemma 5.1 b) there are $A_1, R_1, S_1 \in \mathbf{F}[t]$ and $\gamma \in \mathbf{F}$, such that $P - \gamma^3 = -A_1^2 + R_1 S_1$, where $\deg(A) = n = \deg(R_1)$ and $\deg(S_1) = e - n$. This together with Lemma 9.1 applied to the right hand side of the above equality shows $P - \gamma^3$ as a strict sum of 3 squares.

Assume that $\mathbf{F}_q$ does not contain the finite field $\mathbf{F}_9$ holds, so that $q \equiv 3 \pmod 4$. It follows from Proposition 6.3 together with the later result, that one has $g_1(2,3,\mathbf{F}_q[t]) = 3$. ∎

Question 9.1: What is the value of $g_1(2,3,\mathbf{F}_q[t])$ when $\mathbf{F}_q$ does contain the finite field $\mathbf{F}_9$?

ACKNOWLEDGEMENTS – We thank Mireille Car for useful conversations.

REFERENCES

[EH] Effinger, G. and Hayes, D. – *Additive Number Theory of Polynomials Over a Finite Field*, Oxford Mathematical Monographs, Clarendon Press, Oxford, 1991.

[G] Gallardo, L. – Sums of biquadrates and cubes in $\mathbf{F}_q[t]$, *Rocky Mountain J. Math.,* 33(3), Fall (2003), 865–873.

[HW] Hardy, G.H. and Wright, E.M. – *An Introduction to the Theory of Numbers*, Oxford at The Clarendon Press, Fourth Edition, 1960, reprinted 1968.

[LN] Lidl, R. and Niederreiter, H. – *Finite Fields*, Encyclopedia of Mathematics and its Applications, Volume 20, Cambridge University Press, 1984, reprinted 1987.

[S] Singh, S. – Analysis of each integer as sum of two cubes in a finite integral domain, *Indian J. Pure Appl. Math.,* 6 (1975), 29–35.

[Sc] Scholz, B. – Bemerkung zu einem Beweis von Wieferich, *Jber. Deutsch. Math. Verein.,* 58 (1955), Abt. 1, 45–48.

[St] Stanley, G.K. – The representation of a number as a sum of squares and cubes, *J. Lond. Math. Soc.,* 6 (1931), 194–197.

[V] Vaserstein, L.N. – Sums of cubes in polynomial rings, *Math. Comp. 56,* 193 (1991), 349–357.

[Vg] Vaughan, R.C. – On Waring's problem: One square and five cubes, *Q.J. Math., Oxf. II. Ser.,* 37 (1986), 117–127.

[W] Webb, William A. – Numerical results for Waring's problem in $GF[q,x]$, *Math. Comp. 27,* 121, January (1973), 193–196.

[Wa] Watson, G.L. – On sums of a square and five cubes, *J. Lond. Math. Soc., II. Ser.,* 5 (1972), 215–218.

[Wi] Wieferich, A. – *Math. Annalen,* 66 (1909), 95–101.

Luis 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`