# Waring's problem for cubes and squares over a finite field of even characteristic

Luis Gallardo

**Abstract**

Let $q$ be a power of a prime $p \neq 3$. We characterize the following two sets of polynomials: $M(q) = \{P \in \mathbf{F}_q[t]$ such that $P$ is a strict sum of cubes in $\mathbf{F}_q[t]\}$ and $S(q) = \{P \in \mathbf{F}_q[t]$ such that $P$ is a strict sum of cubes and squares in $\mathbf{F}_q[t]\}$. 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. Similarly let $g_1(3, 2, \mathbf{F}_q[t]) = g$ be the minimal integer such that every $P \in S(q)$ is a strict sum of $g$ cubes and a square. Our main result is:

i) $4 \leq g(3, \mathbf{F}_q[t]) \leq 9 \quad \text{for } q \in \{2, 4\}$.

ii) $3 \leq g_1(3, 2, \mathbf{F}_q[t]) \leq 4 \quad \text{for } q = 4$.

## 1 Introduction

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

$$n = n_1^3 + \ldots + n_g^3,$$

for some positive integer $g$, where the integers $n_i, i = 1, \ldots, g$ and $n$ have all the same sign, so that $|n_i^3| \leq |n|$ for all $i = 1, \ldots, g$. In particular no cancellation of any terms can occur in the above sum. Waring's problem for cubes over $\mathbf{Z}$ consists in determining or at least bounding the minimal such $g$, say $g(3, \mathbf{Z})$. It is well known by work of Wieferich, simplified by Scholz, that $g(3, \mathbf{Z}) = 9$, (See [17] and [11]). Two related problems arise.

Received by the editors September 2003.

Communicated by M. Van den Bergh.

2000 *Mathematics Subject Classification :* 11T55, 11P05, 11D85.

*Key words and phrases :* Waring's Problem, Polynomials, Finite Fields, Characteristic 2.

a) The (so called) "easy" Waring problem in which we allow negative and positive cubes to appear in the decomposition above. Let $v(3, \mathbf{Z})$ represent the analogue of $g(3, \mathbf{Z})$. The exact value of $v(3, \mathbf{Z})$ is unknown, however:

$$4 \leq v(3, \mathbf{Z}) \leq 5.$$

(See [8]).

b) The "asymptotic" Waring problem in which we restrict our attention to represent only "big" or "sufficiently large" integers, i.e., we try to represent all integers bigger than some bound $b$. Let $G(3, \mathbf{Z})$ represent the analogue of $g(3, \mathbf{Z})$. In (see [15]) Linnik and Watson proved that $G(3, \mathbf{Z}) \leq 7$.

Moreover, in (see [9]) Mc Curley proved that $d \leq exp(exp(13.94))$, where $d$ is the largest integer that requires eigth cubes for its representation.

Note that it might be necessary to restrict the integers to be represented since some congruence obstructions may appear. For example an integer congruent to 4 or 5 modulo 9 cannot be expressed as a sum of 3 cubes.

For polynomials, the notion of positivity used for integers, is 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

$$P = c_1^3 + \ldots + c_s^3$$

for some polynomials $c_1, \ldots, c_s \in \mathbf{F}[t]$ such that $\deg(c_i^3) < \deg(P) + 3$ for all $i = 1, \ldots, s$. We say that $P$ is a strict sum of $s$ cubes. Similarly, for any positive integer $k$ we say that $P$ is a strict sum of cubes and $k$ squares if there exist polynomials $d_1, \ldots, d_k \in \mathbf{F}[t]$ such that $\deg(d_i^2) < \deg(P) + 2$ for all $i = 1, \ldots, k$, and for which

$$P - (d_1^2 + \ldots + d_k^2)$$

is a sum of cubes $A^3$ with $\deg(A^3) < \deg(P) + 3$.

For any $A \in \{c_1, \ldots, c_s\}$ we say that $A^3$ appear in the decomposition of $P$. We also say that a polynomial $Q \in \mathbf{F}[t]$ is a *strict* sum of cubes if for some integer $r \geq 1$, $Q$ is a strict sum of $r$ cubes. Similarly we say that $Q$ is a *strict* sum of cubes and squares if for some integer $k \geq 1$, $Q$ is a strict sums of cubes and $k$ squares.
We denote by $g(3, \mathbf{F}[t]) = g$, the minimal positive integer, such that every $P$ that is a strict sum of cubes is a strict sum of $g$ cubes. If it does not exists, then we put $g(3, \mathbf{F}[t]) = \infty$. Similarly, we denote by $g_1(3, 2, \mathbf{F}[t]) = g$ the minimal positive integer such that every $P$ that is a strict sum of cubes and squares is a strict sum of $g$ cubes and a square. If it does not exists, then we put $g_1(3, 2, \mathbf{F}[t]) = \infty$.

Let $q$ be a power of a prime $p \neq 3$ and let $\mathbf{F}_q$ be the finite field with $q$ elements. Set

$$M(q) = \{P \in \mathbf{F}_q[t] \text{ such that } P \text{ is a strict sum of cubes in } \mathbf{F}_q[t]\},$$

and let $\alpha$ be a nontrivial 3-root of 1 in a fixed algebraic closure of $\mathbf{F}_q$.

It is easy to prove (See Lemma 5.2) that $M(q)$ equals the full ring $\mathbf{F}_q[t]$ if and only if $q \notin \{2,4\}$. In the same lemma we give the exact description of $M(4)$ and $M(2)$. It is also convenient to study

$$S(q) = \{P \in \mathbf{F}_q[t] \ / \ P \text{ is a strict sum of cubes and squares in } \mathbf{F}_q[t]\}.$$

It is easy to prove (See Lemma 5.3) that $S(q)$ equals the full ring $\mathbf{F}_q[t]$ if and only if $q \neq 4$. In the same lemma we give the exact description of $S(4)$.

The aim of this paper is to prove that:

a) Every polynomial $P \in \mathbf{F}_q[t]$, where $q \in \{2,4\}$, that is a strict sum of cubes, it is a strict sum of 9 cubes. Moreover, for $q \in \{2,4\}$, there are polynomials in $M(q)$ that are not strict sums of 3 cubes. In other words, we have

$$4 \leq g(3, \mathbf{F}_q[t]) \leq 9 \quad \text{for } q \in \{2,4\}.$$

(See Theorem 6.1).

b) Similarly, we have

$$3 \leq g_1(3, 2, \mathbf{F}_4[t]) \leq 4$$

(See Theorem 7.1).

For details on $g_1(3, 2, \mathbf{F}_q[t])$ for odd $q$, see our paper [7].

### 1.1 Upper bounds for $g(3, \mathbf{F}_q[t])$ and $g_1(3, 2, \mathbf{F}_q[t])$

Assume that $\gcd(3, q) = 1$ and that $M(q)$ is strictly included in the full ring $\mathbf{F}_q[t]$, i.e. assume that $q \in \{2,4\}$. There are not known upper bounds for the minimal length $g(3, \mathbf{F}_q[t])$ necessary to represent every polynomial $P \in M(q)$ as a strict sum of cubes.

The strongest bounds in restricted problems of this type usually stem from applications of the Hardy-Littlewood method, (circle method), suitably modified to apply in function fields, (see, e.g. [3]). Observe that conventional approaches are ineffective when the characteristic of the field in question divides 3!. The reason is that Weyl differencing becomes trivial as soon as this differencing operation causes all terms to be divisible by the field characteristic.

However, when $q$ is a power of 2, and the polynomials $P$ to be represented have *sufficiently large degree* and are sums of cubes (this is required only for $q < 8$) M.

Car and J. Cherly proved in [1] that 11 cubes suffice, (for $q < 8$ these polynomials were taken in $R(2)$ or in $R(4)$, see definitions in Lemma 5.1 ) by using a special variant of the circle method. No explicit value was given for the minimal degree $d$ for which $\deg(P) \geq d$, implies that $P$ is a sum of 11 cubes in $\mathbf{F}_q[t]$.

Furthermore, this analytic method does not give an explicit representation of the polynomials that is able to represent.

In [4],[5],[6],[2] there are explicit representations of *all* polynomials and also upper bounds for $g(3, \mathbf{F}_q[t])$ when $\gcd(q, 3) = 1$ and $M(q) = \mathbf{F}_q[t]$.

More precisely: For $q > 16$ and even, we have: $g(3, \mathbf{F}_q[t]) \leq 10$ when $\mathbf{F}_q$ contains $\mathbf{F}_4$ and $g(3, \mathbf{F}_q[t]) \leq 15$ otherwise. (See [4]). For $q > 4$ and even, we have: $g(3, \mathbf{F}_q[t]) \leq 9$ when $q \neq 16$ and $g(3, \mathbf{F}_{16}[t]) \leq 10$. (See [5]). For any $q > 4$, with $\gcd(q, 3) = 1$, we have: $g(3, \mathbf{F}_q[t]) \leq 7$ when $q \notin \{7, 13, 16\}$, $\max(g(3, \mathbf{F}_{13}[t]), g(3, \mathbf{F}_{16}[t])) \leq 8$, and $g(3, \mathbf{F}_7[t]) \leq 9$. (See [6] for the case $\gcd(q, 6) = 1$, and [2] for the general case).

The case where $q \in \{2, 4\}$ remained open.

In [5] it is proven that $g_1(3, 2, \mathbf{F}_q[t]) \leq 4$ for all even $q \neq 4$, leaving open the case where $q = 4$.

The analogue of our results (but without restrictions on degrees), i.e. the analogue of the “easy” Waring's problem over the integers $\mathbf{Z}$, was obtained by Vaserstein as a special case in [12,13], where it is proven that for $q \in \{2, 4\}$ the minimal length $w(3, \mathbf{F}_q[t]) = w$ necessary to represent every sum of cubes in $\mathbf{F}_q[t]$, as a sum of $w$ cubes in $\mathbf{F}_q[t]$, satisfy

$$3 \leq w(3, \mathbf{F}_q[t]) \leq 4, \quad \text{for } q \in \{2, 4\}.$$

Determining the exact value of $w(3, \mathbf{F}_q[t])$ or $g(3, \mathbf{F}_q[t])$ for $q \in \{2, 4\}$ seems to be a difficult task. The determination of the exact value of $g_1(3, 2, \mathbf{F}_q[t])$ for any $q$ with $\gcd(q, 3) = 1$ seems to be also of the same degree of difficulty (for us). Indeed, even the simpler problem of providing good lower bounds seems non trivial.

A word on some classical notation used in the paper: Given some field $\mathbf{F}$, we say that a polynomial $P \in \mathbf{F}[t]$ is *monic* if his leading coefficient equals 1.

## 2 Method of proof

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

The method consists, for a given polynomial $P \in \mathbf{F}_q[t])$, say monic and of degree $3n > 6$,

$$P = t^{3n} + ... + a_0,$$

to be decomposed, say as a strict sum of cubes; 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 $R$ equal to a sum of cubes of polynomials $S^3$ in which the polynomials $S, R$ have the same degree.

Parts a) and b) are covered in section "Descent" and part c) in section "Identities". When our polynomial $P$ has small degree, i.e. when $\deg(P) \leq 6$, then an special analogue procedure is applied to represent it by a strict sum of 5 cubes (See Lemma 5.1).

## 3 Identities

All results in this section are easily checked by a computation.
First of all, we present Paley's identities (see [10]) (slightly modified).

*Lemma* 3.1. (Paley) – Suppose that $\mathbf{F}$ is a field of characteristic 2. Then the following identities hold in the ring $\mathbf{F}[x, y]$.

a) $y(x^4 + x) = (yx + x^2)^3 + (yx + 1)^3 + (y(x + 1) + x^2)^3 + (yx + y)^3 + 1^3$.

b) $y(x^4 + x) + x^3 + x^2 + x = (y(x + 1) + x^3 + x^2 + x)^3 + (y(x + 1) + x^3 + x^2 + x + 1)^3 + (y + x^2 + 1)^3 + y^3$.

c) $y(x^4 + x) + x^2 + x + 1 = (yx + x^2 + x + 1)^3 + (yx + x)^3 + (y(x + 1) + x^2 + x + 1)^3 + (y(x + 1) + x + 1)^3$.

d) $y(x^4 + x) + x^3 + 1 = (yx + x^3 + 1)^3 + (yx + x^3)^3 + (y + x^2)^3 + y^3$.

Secondly, we have the identity of Serre, (see [12]) (slightly modified), as well as two complementary identities covering some special cases.

*Lemma* 3.2. (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 $x \in \mathbf{F}$, $y \in \mathbf{F}$, with $xy \neq 0$. Then for any nonzero $p \in \mathbf{F}$ we have the identity

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

*Lemma* 3.3. – We have

a) $48t = (t+3)^3 + (t-3)^3 - (t+1)^3 - (t-1)^3$
over any field $\mathbf{F}$ and the identity

b) $t = (rt + r^5)^3 + (rt + r^5 + 1)^3 + (t + r^7)^3 + (t + r^2 + r^7)^3$
over a field $\mathbf{F}$ with 16 elements where $r \in \mathbf{F}$ satisfies $r^4 = r + 1$.

It is convenient to put together some identities (even if some of them are instances of some of the identities in Lemma 3.1 and some redundance occurs):

*Lemma* 3.4. – Assume that $\mathbf{F}$ is a field of characteristic 2, and let $a \in \mathbf{F}$. Then the following identities hold in $\mathbf{F}[t]$.

(a) $t = (t+1)^3 + t^3 + (t+1)^2$.

(b) $at^5 = (t^2 + at)^3 + (at)^3 + (t^3 + at^2)^2$.

(c) $t^2 + t = (t+1)^3 + t^3 + 1^3$.

*Lemma* 3.5. – Every sum of cubes equals 0 or 1 in the finite field with 4 elements $\mathbf{F}_4$, so that any nonzero sum of cubes equals 1.

## 4 Descent

*Lemma* 4.1. – Let $\mathbf{F}$ be a field of characteristic 2, in which every sum of cubes is a cube. Let $n \geq 0$ be an integer and let $P \in \mathbf{F}[t]$ be a polynomial that is a strict sum of cubes 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 there exist $A, B, R \in \mathbf{F}[t]$ such that

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

b) $\deg(A^3) < d + 3$, and $\deg(B^3) < d + 3$.

c) $R$ is monic and $r = \deg(R)$ is the least multiple of 3 that exceeds $2n - 1$.

d) If 3 divides $\deg(P)$ then $A = 0$.

*Proof*: Write $P = p_d t^d + \ldots + p_0$. We define $A = -t^n$ if 3 does not divide $d$ and $A = 0$ otherwise. Observe that $Q = P - A^3$ is a strict sum of cubes in $\mathbf{F}[t]$ and that $Q$ has degree $3n$. Then, the leading coefficient of $Q$ is a nonzero cube $c^3$, since it is a sum of cubes in $\mathbf{F}$. Set now $r$ equal to the least multiple of 3 that exceeds $2n - 1$ and let $B = ct^n + b_{n-1}t^{n-1} + \ldots + b_0$, with unknowns $b_{n-1}, \ldots, b_0$ 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 $t^{r+1}$, be equal to zero and such that the coefficient of $t^r$ in $R$ be equal to 1. This results on a triangular linear system over $\mathbf{F}$ in at most $n$ unknowns $b_{n-1}, \ldots, b_0$ soluble since $c \neq 0$.

## 5 Polynomials that are strict sums of cubes and squares

Let $q$ be a power of a prime number $p \neq 3$. When $q = 4$ we write

$$\mathbf{F}_4 = \mathbf{F}_2[\alpha]$$

with $\alpha$ an element of a fixed algebraic closure of $\mathbf{F}_2 = \{0, 1\}$ such that $\alpha^2 = \alpha + 1$.

First of all, we study the case where our polynomials are of small degree. For $q \in \{2, 4\}$ we show that every polynomial of degree $\leq 6$ not barred by congruences is represented by a strict sum of 5 cubes.

L*emma* 5.1. – Let

$$R(2) = \{P \in \mathbf{F}_2[t] \;/\; P(\alpha) \in \mathbf{F}_2\}.$$

Let

$R(4) = \{P \in \mathbf{F}_4[t] \;/\; P(r) \in \mathbf{F}_2$ for all $r \in \mathbf{F}_4$, and such that, either 3 does not divide $\deg(P)$, or 3 divides $\deg(P)$ and $P$ is monic$\}$.

and let $P \in R(2) \cup R(4)$, with $\deg(P) \leq 6$. Then $\deg(P) \neq 1$ and

a) If $\deg(P) = 0$ then $P$ is a cube.

b) If $\deg(P) = 2$ then $P$ is a strict sum of 3 cubes.

c) If $\deg(P) = 3$ then $P$ is a strict sum of 2 cubes.

d) If $\deg(P) = 4$ then $P$ is a strict sum of 5 cubes.

e) If $\deg(P) = 5$ then $P$ is a strict sum of 5 cubes.

f) If $\deg(P) = 6$ then $P$ is a strict sum of 4 cubes.

*Proof* : First of all, we assume that $P \in R(2)$.
Constant polynomials $\beta \in \mathbf{F}_2$ satisfy $\beta = \beta^3$ while polynomials of degree 1 are not in $R(2)$ by definition of $R(2)$. From Lemma 3.1 part $c$) with $y = 0$, or from Lemma 3.4 part $c$), we obtain $b$) since $t^2 + at + b \in R(2)$ forces $a = 1$. Now assume that $P = t^3 + at^2 + bt + c \in R(2)$. It follows from

$$P = (t + a)^3 + (b + a^2)t + (c + a^3)$$

that $b = a^2$, so that $P$ is a strict sum of 2 cubes.

Let $P$ be of degree 6 and write $P = t^6 + bt^5 + ct^4 + dt^3 + et^2 + ft + g$. By completing the cube one has

$$P = (t^2 + bt + (b^2 + c))^3 + C$$

with $\deg(C) \leq 3$. This result, together with $a), b)$ and $c$), proves $f$).

Finally, when $\deg(P) \in \{4, 5\}$, the polynomial $Q = t^6 + P$ has degree 6. Hence,

$$P = (t^2)^3 + Q$$

is a strict sum of $1 + 4 = 5$ cubes.

Now we take $P \in R(4)$.

If $\deg(P) \leq 1$ then $P = P(0) + bt$ with $P(0) \in \mathbf{F}_2$ and $b = P(1) - P(0) \in \mathbf{F}_2$. Hence, $P(\alpha) \in \mathbf{F}_2$ forces $b = 0$, i.e. $P \in \mathbf{F}_2$ so that $P = P(0)^3$ is a cube.
Assume that $P = at^2 + bt + c$ with $a \neq 0$. The condition $P(\alpha) \in \mathbf{F}_2$ gives $b = a^2$ so that $b^2 = a$ and $P = (bt)^2 + (bt) + c$ with $c = P(0) \in \mathbf{F}_2$. From formula $(c)$ of Lemma 3.4 it follows that $P$ is a strict sum of 3 cubes.

The rest of the proof is the same as the proof of the case where $P \in R(2)$, since polynomials of degree 3 in $R(4)$ and polynomials of degree 6 in $R(4)$ are monic.

In the following lemmas we characterize the polynomials in $\mathbf{F}_q[t]$, with $\gcd(q, 3) = 1$, that are strict sums of cubes or strict sums of cubes and squares. While in the corollary below, we compare the set of those polynomials with the full ring of polynomials $\mathbf{F}_q[t]$.

L*emma* 5.2. – We recall that

$$M(q) = \{P \in \mathbf{F}_q[t] \ / \ P \text{ is a strict sum of cubes in } \mathbf{F}_q[t]\}$$

and that $R(2)$ and $R(4)$ are defined in Lemma 5.1.
Let

$$R(q) = \mathbf{F}_q[t], \text{ for } q > 4.$$

Then $M(q) = R(q)$ for all $q$.

*Proof* : Case 1. First of all, we show the egality when $q \in \{2, 4\}$. The inclusion $M(q) \subseteq R(q)$ follows from Lemma 3.5. Take now $P \in R(q)$. It follows from Lemma 5.1 that we can take $\deg(P) > 6$. There are polynomials $Q, r \in \mathbf{F}_q[t]$ with either $r = 0$ or $\deg(r) < 3$, such that

$$P = t^3 Q + r = t^3(Q + r) + (t^3 + 1)r. \tag{1}$$

This implies clearly that $Q + r \in R(q)$ so that we can assume by induction that $Q + r \in M(q)$. Since $\deg((t^3 + 1)r) < 6$, it follows from (1) and from Lemma 5.1 that the polynomial $(t^3 + 1)r \in M(q)$, i.e. we are done by induction.

Case 2. We assume that $q > 4$. Observe that Lemma 3.2 applies exactly when $q \notin \{7, 13, 16\}$ (See [12]). By putting $w = 1$ in the Serre identity in Lemma 3.2 and in the identities in Lemma 3.3, we obtain that every polynomial $u$ of degree at most 1 is in $M(q)$. These latter identities cover the special cases when $q \in \{7, 13, 16\}$. Similarly, by putting $u = 1$ and $w = p_2 t$ where $p_2 \in \mathbf{F}_q$, in the Serre identity in

Lemma 3.2 and in the identities in Lemma 3.3, we obtain that every monomial $p_2^2t^2$ is in $M(q)$. Observe that every element $a$ of $\mathbf{F}_q$ is a sum of 2 squares. Therefore, every monomial $at^2$ with $a \in \mathbf{F}_q$ is in $M(q)$. It follows that every polynomial $P$ with $\deg(P) \leq 2$ is an element of $M(q)$. The result follows by induction for the polynomials $P$ of degree $\geq 3$, by observing that any such $P = \sum_{r=0}^{n} p_r t^r$ can be written as

$$P = t^3(p_n t^{n-3} + ... + p_3) + p_2t^2 + p_1t + p_0.$$

Another proof, that applies for even $q > 4$, follows from Theorem 7 in [5].

L*emma* 5.3. – Let $q$ be a power of a prime number $p \neq 3$. We recall that $S(q) = \{P \in \mathbf{F}_q[t] \ / \ P$ is a strict sum of cubes and squares in $\mathbf{F}_q[t]\}$. Then

$$S(q) = \mathbf{F}_q[t]$$

unless $q = 4$.
Let define the subsets $T_i$ of $\mathbf{F}_4[t]$ for $i \in \{1, 2, 3, 4, 5\}$ by:

a) $T_1 = \{P \in \mathbf{F}_4[t] \ / \ \deg(P) \in \{0, 1, 2\}\}$.

b) $T_2 = \{P \in \mathbf{F}_4[t] \ / \ \deg(P) = 3$ and $P$ is monic $\}$.

c) $T_3 = \{P \in \mathbf{F}_4[t] \ / \ \deg(P) \in \{4, 5, 6\}$ and the coefficient $p_3$ of $t^3$ in $P$ satisfy $p_3 \in \{0, 1\}\}$.

d) $T_4 = \{P \in \mathbf{F}_4[t] \ / \ \deg(P) \geq 7, \ \deg(P) \equiv 3 \pmod 6$ and $P$ is monic $\}$.

e) $T_5 = \{P \in \mathbf{F}_4[t] \ / \ \deg(P) \geq 7, \ \deg(P) \not\equiv 3 \pmod 6 \ \}$.

and define $T$ as the union of all the above $T_i$'s, i.e. $T = \bigcup_{i=1}^{5} \ T_i$.

Then

$$S(4) = T.$$

*Proof*: It is well known that every polynomial in $\mathbf{F}_q[t]$ is a strict sum of 4 squares when $q$ is odd. If $q$ is even and $q \neq 4$ the result follows from [5, Theorem 9] where we proved that for all $q$ even such that $q \neq 4$, every polynomial $P \in \mathbf{F}_q[t]$ is a strict sum of 4 cubes and a square. For the rest of the proof we assume that $q = 4$.
First step: we claim that $S(4) \subseteq T$. Let $P = \sum_{r=0}^{n} p_r t^r \in S(4)$.
If $n \in \{0, 1, 2\}$, then $P \in T_1 \subseteq T$. Suppose that $n = 3$. At least one cube $A^3$ appear in the decomposition of $P$ since $n = 3$ is odd. Hence, we obtain $\deg(A) \leq 1$ from $\deg(A^3) < n + 3 = 6$.

Therefore, the leading coefficient $p_3 \neq 0$ of $P$ is a sum of cubes in $\mathbf{F}_4$. From Lemma 3.5 we obtain $p_3 = 1$, so that $P \in T_2 \subseteq T$.
Suppose now that $n \in \{4, 5, 6\}$. If $A^3$ appear in the decomposition of $P$ then $\deg(A) \leq 2$. The coefficient $p_3$ of $t^3$ in $P$ is a sum of cubes in $\mathbf{F}_4$ since for $a+bt+ct^2 \in \mathbf{F}_4[t]$ one has

$$(a + bt + ct^2)^3 = c^3t^6 + bc^2t^5 + c(ac + b^2)t^4 + b^3t^3 + a(ac + b^2)t^2 + a^2bt + a^3.$$

It follows from Lemma 3.5 that $p_3 \in \{0, 1\}$, so that $P \in T_3 \subseteq T$.
Suppose that $n = 6k+3$ for some integer $k \geq 1$; we claim that $P$ is monic. Since $n$ is

odd and $p_n \neq 0$, at least one $A^3$ with $\deg(A) = 2k+1$ appear in the decomposition of $P$. The leading coefficient $p_n$ of $P$ is the sum of all the leading coefficients of the cubes $B^3$ appearing in the decomposition of $P$ such that $\deg(B) = 2k+1$. Therefore $p_n$ is a nonzero sum of cubes in $\mathbf{F}_4$. It follows from Lemma 3.5 that $p_n = 1$. Hence, $P \in T_4 \subseteq T$.
To finish the first step, we suppose now that $\deg(P) \geq 7$ and that $n \not\equiv 3 \pmod 6$. Then $P \in T_5 \subseteq T$. Hence, $S(4) \subseteq T$.

Second step: we claim that $T \subseteq S(4)$. Let $P = \sum_{r=0}^{n} p_r t^r \in T$.
First of all, if $n < 2$ then the identity *a*) of Lemma 3.4 proves that $P \in S(4)$. It follows that $P \in S(4)$ for $n = 2$, since $P = (q_0 + q_2 t)^2 + p_1 t$. Therefore, $T_1 \subseteq S(4)$. If $P \in T_2$, and we set $Q = P + t^3$, then $\deg(Q) = 2$ so $Q \in S(4)$ by the preceding result. It follows that $P = t^3 + Q \in S(4)$. So $T_2 \subseteq S(4)$. Suppose now that $P \in T_3$, so that

$$P = (q_6 t^3 + q_4 t^2)^2 + p_5 t^5 + R.$$

where $p_6 = q_6^2,\ p_4 = q_4^2,$ and $R = p_3 t^3 + p_2 t^2 + p_1 t + p_0 \in T_2 \cup T_1$. By the identity *b*) in Lemma 3.4 it follows that $p_5 t^5 \in S(4)$. Therefore, $P \in S(4)$, and then $T_3 \subseteq S(4)$. Suppose now that $P \in T_4$. We will prove by induction on $n = \deg(P)$ that $P \in S(4)$. If $n = 9$ then $P = t^6 A + B$ where

$$A = t^3 + p_8 t^2 + p_7 t + p_6 \in S(4) \text{ and } B = p_5 t^5 + \ldots + p_0 \in S(4).$$

Since $A$ and $B$ are elements of $S(4)$ we obtain $P \in S(4)$. Suppose that the result is true when $\deg(P) = 6k+3$ for $k \geq 1$. We will prove it for $P$ with $\deg(P) = 6(k+1)+3 = 6k+9$. Observe that the division of $P$ by $t^6$ with quotient $K$ and remainder $L$ give $P = t^6 K + L$, where

$$K = t^{6k+3} + \sum_{j=6}^{6k+8} \ p_j t^{j-6} \text{ and } L = p_5 t^5 + \ldots + p_0.$$

Now by induction $K \in S(4)$ and we have already proved that $L \in S(4)$. Therefore $P \in S(4)$. It follows that $T_4 \subseteq S(4)$.
The proof that $T_5 \subseteq S(4)$ is similar. It follows that $T \subseteq S(4)$. This result together with the result of the first step $S(4) \subseteq T$ give the equality $S(4) = T$, thereby finishing the proof of the lemma.

In the following corollary we compare $M(q)$, $S(q)$ and the full ring $\mathbf{F}_q[t]$ :

C*orollary* 5.4. – Let $q$ be a power of a prime number $p \neq 3$. We recall that $M(q) = \{P \in \mathbf{F}_q[t] \ / \ P$ is a strict sum of cubes in $\mathbf{F}_q[t]\}$, and that $S(q) = \{P \in \mathbf{F}_q[t] \ / \ P$ is a strict sum of cubes and squares in $\mathbf{F}_q[t]\}$. Then

a) If $q \notin \{2,4\}$ then $M(q) = S(q) = \mathbf{F}_q[t]$.

b) $M(2)$ is strictly included in $S(2) = \mathbf{F}_2[t]$.

c) $M(4)$ is strictly included in $S(4)$ and $S(4)$ is strictly included in $\mathbf{F}_4[t]$.

*Proof* : The proof of the first result follows from Lemmas 5.2 and 5.3. All the other inclusions are trivial. To finish the proof observe that the same two lemmas implies the following. Since $t \notin M(2)$, $M(2)$ is strictly included in $S(2) = \mathbf{F}_2[t]$. Observe that $t \in S(4)$ but $t \notin M(4)$ so that $M(4)$ is a strict subset of $S(4)$. Finally $\alpha t^3 \notin S(4)$ where $\mathbf{F}_4 = \mathbf{F}_2[\alpha]$ since $\alpha t^3$ is not monic.

The following lemma generalizes the results in Lemma 8 of [5].

L*emma* 5.5. – Let $\mathbf{F}$ be a perfect field of characteristic 2 in which every sum of cubes is a sum of 2 cubes. Let $n \geq 1$ be an integer and let $S \in \mathbf{F}[t]$ be a polynomial of degree $m \in \{3n+2, 3n+1, 3n\}$, such that $tS^2$ is a strict sum of cubes and squares. Then there exist polynomials $A, B, C, D, Q \in \mathbf{F}[t]$ such that

$$S = A^2B + C^2D + t(B^3 + D^3) + Q,$$

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

*Proof* : Set $m = 3n + 2$ and $S = p_m t^m + ... + p_0$. We can find polynomials $A, B, C, D \in \mathbf{F}[t]$ of the following form: $A = at^{n+1} + \sum_{k=0}^{n} a_k t^k,\ B = ct^n + et^{n-1},\ C = \sum_{k=0}^{n} c_k t^k,\ D = dt^n + t^{n-1}$, satisfying the conditions of the lemma. By equating coefficients of $t^k$, in the expansion of $A^2B + C^2D + t(B^3 + D^3)$ in powers of $t$, with those of $S$, for $k$ descending from $3n+2$ to $3n+1$ we obtain $a, c, d, e$ and for $k$ descending from $3n$ to $n-1$, we obtain $a_n, ..., a_0, c_n, ..., c_0$ in the order $c_n, a_n, c_{n-1}, a_{n-1}, ...$ corresponding to the values $3n-1, 3n, 3n-3, 3n-2, ...$ of $k$, by solving the corresponding linear equations in which the condition $c \neq 0$ guarantees the resolution.
We give the details to find $a, c, d, e \in \mathbf{F}$ with $c \neq 0$ : Suppose that $\deg(S) \neq 3n + 1$. If $p_m = 0$, then $\deg(S) = 3n$ and we take $a = 0, c = 1, d = 1, e = 0$. If $p_m \neq 0$, then $\deg(S) = m$ and we take $a = 1, c = p_{3n+2}, d = 0, e = p_{3n+1} - c^3$. Therefore, we may assume that $\deg(S) = 3n + 1$, and take $a = 0, e = 0$. Hence, it suffices to show that $p_{3n+1} = c^3 + d^3$ with $c, d \in \mathbf{F}$ and $c \neq 0$. To prove the claim, we note that $K(t) = tS(t)^2$ has odd degree $6n + 3$. The leading coefficient of $K(t)$ is a sum of cubes in $\mathbf{F}$ since $K(t)$ is a strict sum of cubes and squares.

It follows that the same result is true for the polynomial $L(t) = (K(t^2))^{1/2}$. But the leading coefficients of the polynomials $L(t)$ and $S$ are equal, thereby finishing the proof of the lemma.

## 6 Representation by cubes for $q \leq 4$

First of all, we observe that for $3\,|\,q$ the problem is trivial and for $q > 4$, there are already results on it in [4],[5],[6] and [2]. Hence, we assume that $q \in \{2, 4\}$ in this section.

*Theorem* 6.1. – Every polynomial $P \in \mathbf{F}_q[t]$, where $q \in \{2, 4\}$ and that is a strict sum of cubes, is a strict sum of 9 cubes. Moreover for $q \in \{2, 4\}$ there are polynomials in $M(q)$ that are not strict sums of 3 cubes. In other words, we have

$$4 \leq g(3, \mathbf{F}_q[t]) \leq 9 \quad \text{for } q \in \{2, 4\}.$$

*Proof* : The lower bound follows from a computer computation. The result is already proved in Lemma 5.1 when $\deg(P) \leq 6$. We assume then that $\deg(P) > 6$. The upper bound follows readily from Lemma 4.1 applied three times. Indeed, one get at most 4 cubes that appear in the strict representation of $P - R$, where $\deg(R^3) < \deg(P) + 3$. The proof is finished applying the identities of Paley in Lemma 3.1 to the above rest $R$. That shows at most 5 new cubes with the right degrees to represent $R$, and so appearing in the strict representation of $P$. Note that this can be done since the class modulo $t^4 + t$ of $P$ do not change, or is translated by 1 when substracting cubes to $P$.

## 7 Representation by a square and cubes

It is not known if every positive integer $n$ can be expressed as a sum of a square and 5 cubes. However, G.L. Watson proved in [16] that this is true for every sufficiently large integer $n$ and R.C. Vaughan showed in [14] 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 $n$ is a sum of a square and five cubes for all $n \geq d$ .

For the far less demanding analogue problem, where the integer $n$ is replaced by a suitable polynomial $P$ with coefficients in a finite field $\mathbf{F}_q$, with $q$ even, we prove here below that every such polynomial $P$ is a strict sum of 4 cubes and a square.

Note that this has been proved in [5, Theorem 9] when $q \neq 4$. It remains the case $q = 4$ :

*Theorem* 7.1. – Every polynomial $P \in \mathbf{F}_4[t]$ that is a strict sum of cubes and squares is a strict sum of 4 cubes and a square. Moreover, there are polynomials in $M(4)$ that are not strict sums of 2 cubes and a square. In other words, we have

$$3 \leq g_1(3, 2, \mathbf{F}_4[t]) \leq 4$$

*Proof* : The lower bound follows from some computer calculations. We prove here below the upper bound.

For any $H \in \mathbf{F}_4[t]$ we write $H'$ for the derivative of $H$ relative to $t$. Put $P' = S^2$, and $s = \deg(S) \in \{3n+2, 3n+1, 3n\}$ for some integer $n \geq 0$. Since $(tP)'$ is a square in $\mathbf{F}_4[t]$ of degree $< \deg(P) + 2$ and $P = (tP)' + tP'$ it suffices to prove the result for $tP'$.

If $s = 0$ then $S$ is constant, so that $tP' = tS^2$ is a sum of 2 cubes and 1 square by the identity (a) in Lemma 3.4. If $s = 1$ then $S = p_0 + p_1 t$ has degree 1 so that $tP'$ is a polynomial of degree 3 that is a strict sum of cubes and squares. Therefore $tP'$ is monic by Lemma 5.3 b). It follows that $tP' = tS^2 = p_0^2 t + t^3$ so that by the preceding result it follows that $tP'$ is a strict sum of at most 3 cubes and 1 square. If $s = 2$ then $S = p_2 t^2 + p_1 t + p_0$ with $p_2 \neq 0$ hence $tP'$ has degree 5, say $tP' = q_2 t^5 + q_1 t^3 + q_0 t$. From Lemma 5.3 c) it follows that $q_1 \in \{0, 1\}$, so that $q_1 t^3 = (q_1 t)^3$ is a cube in $\{0, t^3\}$. By the identity b) in Lemma 3.4 the monomial $q_2 t^5$ is a sum of 2 cubes and 1 square, and by the identity a) in the same lemma $q_0 t$

is a sum of 2 cubes and 1 square. Therefore

$$tP' = (t^2+q_2t)^3+(q_2t)^3+(q_1t)^3+(q_0t+1)^3+(q_0t)^3+(t^3+q_2t^2+q_0t+1)^2.$$

Observe that by Lemma 3.5 one has $q_2^3+q_1^3+q_0^3 \in \{0,1\}$, so that the above formula shows indeed at most 3 cubes.

We may then assume that $n \geq 1$. Since $P$ is a strict sum of cubes and squares and $(tP)'$ is a square we see that $tS^2 = P + (tP)'$ is also a strict sum of cubes and squares. Therefore it follows from Lemma 5.5 that

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

where $K = A^2 + tB^2,\ \ L = C^2 + tD^2$. We also have $\deg(L) \leq 2n+1$ and $\deg(Q) < n-1$, while $\deg(K) = 2n+1$ if $d \not\equiv 2 \pmod 3$ and $\deg(K) = 2n+2$ if $d \equiv 2 \pmod 3$. Integrating (2) over $t$ and using identity (a) in Lemma 3.4, we obtain

$$tP' = K^3 + L^3 + (tQ^2+1)^3 + (tQ^2)^3 + (R+tQ^2+1)^2 \tag{3}$$

for some $R \in \mathbf{F}_4[t]$.

The rest of the proof consists in checking up that the decomposition of $tP'$ in (3) is a strict one . We give the detail when $s = \deg(S) \not\equiv 2 \pmod 3$; in the other case the proof is similar. First of all $\deg(tQ^2)^2) \leq \deg(tQ^2)^3 < 6n-3 < \deg(tP')+2 < \deg(tP')+3$. We also have $\deg(L^3) \leq 6n+3 < 6n+4 \leq \deg(tP')+3$, and similarly $\deg(K^3) \leq 6n+3 < 6n+4 \leq \deg(tP')+3$. Therefore, rewriting (3) as $R^2 = tP' + K^3 + L^3 + tQ^2$, we obtain $\deg(R^2) \leq 6n+3$. It follows that $\deg(R^2) < 6n+3 \leq \deg(tP')+2$ since $6n+3$ is odd, thereby finishing the proof of the theorem.

## 8 Acknowledgments

We thank Mireille Car for useful conversations.

## References

[1] M. Car and J. Cherly, Sommes de cubes dans l'anneau $F_{2^h}[X]$, Acta Arith. 65, Number 3 (1993), 227-241.

[2] M. Car and L. Gallardo, Sums of cubes of Polynomials. To appear in Acta Arithmetica.

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

[4] L. Gallardo, Une variante du problème de Waring sur $F_{2^n}[t]$, (An $F_{2^n}[t]-$ variant of Waring's problem), C.R.A.S, t. 327, Série I, (1998), 117-121.

[5] L. Gallardo, On the restricted Waring problem over $F_{2^n}[t]$. Acta Arith. XCII.2, (2000), 109-113.

[6] L. Gallardo, Sums of biquadrates and cubes in $\mathbf{F}_q[t]$. Rocky Mt. J. Math. 33, no. 3, (2003), 865-873.

[7] L. Gallardo, Waring's problem for Polynomial cubes and squares over a finite field with odd characteristic. Port. Math. (N.S.) 61, no. 1, (2004), 35-49.

[8] G.H. Hardy and E.M. Wright, "An Introduction to the Theory of Numbers", Oxford at The Clarendon Press, fourth edition, 1960, reprinted 1968.

[9] Kevin S. Mc Curley, An effective seven cubes theorem, J. Number Theory 19, no. 2, (1984), 176-183.

[10] R.E.A.C. Paley, Thorems on polynomials in a Galois field, Quart. J. Math. 4 (1933), 52-63.

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

[12] L.N. Vaserstein, Sums of cubes in polynomial rings, Math. of Comp 56, $n^o$ 193, (1991), 349-357.

[13] L.N. Vaserstein, Ramsey's theorem and the Waring's problem for algebras over fields, pp. 435-442 in proceedings of workshop "The Arithmetic of Function Fields", 1991, Ohio State University, Walter de Gruyter Verlag, 1992.

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

[15] G.L. Watson, A proof of the seven cubes theorem, J. Lond. Math. Soc., 26 (1951), 153-156.

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

[17] A. Wieferich, Math. Annalen, 66, 1909, 95-101.

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