ACTA ARITHMETICA
112.1 (2004)

Sums of cubes of polynomials

by

MIREILLE CAR (Marseille) and LUIS GALLARDO (Brest)

1. Introduction. Let q be a power of a prime number p and let $\mathbb{F}_q$ be the finite field with q elements. One may formulate the Waring problem for the polynomial ring $\mathbb{F}_q[t]$ in the simplest way as follows. Let $k \geq 2$ be an integer. Does there exist an integer s such that *any* polynomial $P \in \mathbb{F}_q[t]$ is a sum of s kth powers of polynomials? If the answer to this question is positive, let $w(q,k)$ denote the smallest such integer s. Another question is to determine or to give a bound for this number $w(q,k)$. Such a question may be asked in any ring. Taking the polynomial structure into account, one may include degree conditions in the Waring problem for the ring $\mathbb{F}_q[t]$. One wants to avoid a maximum of possible cancellation of the terms of degree greater than the degree of P, appearing in the sum of kth powers that represents P. A solution was suggested by G. W. Effinger and D. R. Hayes (see [EH]) and is as follows. Let $P \in \mathbb{F}_q[t]$ be a polynomial such that

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

for some polynomials $c_1, \ldots, c_s \in \mathbb{F}_q[t]$ with $\deg(c_i^k) < \deg(P) + k$ for all $i = 1, \ldots, s$. We then say that P is a *strict sum* of s kth powers. We also say that a polynomial $Q \in \mathbb{F}_q[t]$ is a strict sum of kth powers if for some integer $r \geq 1$, Q is a strict sum of r kth powers.

The *strict* Waring problem for the polynomial ring $\mathbb{F}_q[t]$ is that of the existence of an integer s such that any polynomial $P \in \mathbb{F}_q[t]$ admits a strict representation as a sum of s kth powers. If such an integer s exists, denote by $g(q,k)$ the minimal such s. As above, a natural question is to determine or to bound $g(q,k)$.

If p divides k, only pth powers are sums of kth powers, and the answer to the two questions is negative. Therefore, one has to study Waring's problem for the ring $\mathbb{F}_q[t]$ only for exponents k coprime with the characteristic p. Even with this restriction, the complete answer to the two questions is unknown.

2000 *Mathematics Subject Classification*: Primary 11T06; Secondary 11T55.
Key words and phrases: Waring's problem, polynomials, finite fields.

However, the answer is completely known for the problem of the strict sums of *squares*, i.e. in the case $k = 2$. See [EH] for Serre's special proof of $g(q, 2) = 3$ for $q \neq 3$ by using Weil's theorem on curves over a finite field.

In this paper, we deal with the strict Waring problem for cubes, improving results of the second named author (see [Ga]). Thus, we assume that $p \neq 3$. According to Theorem 4 of [Va], $w(q, 3) = 3$ for $q \notin \{2, 4, 16\}$. Since the sums of cubes in the field $\mathbb{F}_4$ are 0 or 1, sums of cubes in the ring $\mathbb{F}_2[t]$ are congruent to 0 or 1 modulo the polynomial $t^2 + t + 1$, and sums of cubes in $\mathbb{F}_4[t]$ are congruent to 0 or 1 modulo every polynomial of degree 1. Hence, in what follows we may assume that $q > 4$.

Our main result (see Theorem 1) is an upper bound for the numbers $g(q, 3)$ when $q \notin \{2, 4\}$. Namely:

(a) Assume that $q > 4$ and that $\gcd(q, 3) = 1$. Then

$$g(q, 3) \leq 7 \quad \text{if } q \notin \{16, 7, 13\}.$$

(b) $g(q, 3) \leq 8$ if $q \in \{16, 13\}$.
(c) $g(7, 3) \leq 9$.

Our method led us to consider representations with tamed degree conditions defined as follows. A representation of $P \in \mathbb{F}_q[t]$ as a sum

$$P = c_1^k + \ldots + c_s^k,$$

where the polynomials $c_1, \ldots, c_s \in \mathbb{F}_q[t]$ are such that $\deg(c_i) \leq \deg(P)$ for all $i = 1, \ldots, s$, is called a *tamed representation* of P a sum of s kth powers. Clearly if the polynomial t admits a tamed representation as a sum of s kth powers, the same is true for any $P \in \mathbb{F}_q[t]$.

The *tamed Waring problem* for the polynomial ring $\mathbb{F}_q[t]$ is that of the existence of an integer s such that any polynomial $P \in \mathbb{F}_q[t]$ admits a tamed representation as a sum of s kth powers. If such an integer s exists, denote by $t(q, k)$ the minimal such s. As above, a natural question is to determine or to bound $t(q, k)$.

We will prove that for all $q \notin \{2, 4\}$ the polynomial t is a tamed sum of cubes and we will determine all the numbers $t(q, 3)$.

2. Sums of cubes in $\mathbb{F}_q$. If there exist an integer s such that any $x \in \mathbb{F}_q$ is a sum $x = x_1^3 + \ldots + x_s^3$ with $x_1 \in \mathbb{F}_q, \ldots, x_s \in \mathbb{F}_q$, let $c(q, 3)$ be the least such integer s. We begin by computing these numbers.

PROPOSITION 1. *Let q be a power of a prime $p \neq 3$.*

(a) *Assume that $q \not\equiv 1 \pmod 3$. Then $c(q, 3) = 1$.*

(b) *The equation $1 = x^3 + y^3$ has a solution $(x, y) \in \mathbb{F}_q^2$ such that $xy \neq 0$ if and only if $q \in \{5, 8, 11\}$ or $q \geq 17$.*

(c) *If $q \geq 13$, then for any $a \in \mathbb{F}_q$ which is not a cube in the field $\mathbb{F}_q$, the equation $a = x^3 + y^3$ has a solution $(x, y) \in \mathbb{F}_q^2$ such that $xy \neq 0$.*

(d) *Assume that $q \equiv 1 \pmod 3$ and $q \neq 7$. Then $c(q, 3) = 2$.*

(e) *$c(7, 3) = 3$.*

Proof. For $a \in \mathbb{F}_q$, let $N(q, a)$ be the number of pairs $(x, y) \in \mathbb{F}_q^2$ such that $a = x^3 + y^3$, and $n(q, a)$ the number of pairs $(x, y) \in \mathbb{F}_q^2$ such that $a = x^3 + y^3$ and $xy \neq 0$. Assume that $q \not\equiv 1 \pmod 3$. Since every element of $\mathbb{F}_q$ is a cube, (a) holds. Moreover for any $a \in \mathbb{F}_q$ one has $N(q, a) = q$ and $n(q, 1) = q - 2 \geq 1$ for $q \neq 2$. Assume now that $q \equiv 1 \pmod 3$. It follows from Weil's theorem on curves over a finite field (see, e.g., [LN]) applied to the projective curve $az^3 = x^3 + y^3$ that

$$N(q, a) \geq q - 2q^{1/2} - 2. \tag{1}$$

Suppose, furthermore, that $q \geq 13$. We claim that $c(q, 3) = 2$. It is clear that (1) implies that $N(q, a) \geq 1$ for all $a \in \mathbb{F}_q$. Therefore $c(q, 3) \leq 2$. Since not all elements in $\mathbb{F}_q$ are cubes we also have $c(q, 3) \geq 2$, so (d) is proved. Moreover, observe that

$$N(q, 1) = n(q, 1) + 6, \tag{2}$$

and

$$N(q, a) = n(q, a) \tag{3}$$

for any $a \in \mathbb{F}_q$ that is not a cube. Suppose that $q \geq 17$. From (1) and (2) it follows that $n(q, a) \geq 1$. This establishes (c). Suppose that $q \geq 13$ and that a is not a cube. From (1) and (3) it follows that $n(q, a) \geq 1$. To complete the proof we shall now investigate the cases $q = 7$ and $q = 16$. Since the cubes in $\mathbb{F}_7$ are $0, 1$ and -1 it follows that $c(7, 3) = 3$. Let $a \in \mathbb{F}_4$ be such that $a^2 = a + 1$ and let $b \in \mathbb{F}_{16}$ be such that $b^2 = b + a$. Hence, the cubes in $\mathbb{F}_{16}$ are $0, 1, ab, ab + a, ab + 1 + b, ab + a + b$. This implies that $c(16, 3) = 2$, thereby proving the proposition.

3. A bound for $t(q, 3)$. We assume that q is a power of a prime $p \neq 3$ in all this section.

PROPOSITION 2. *We have*

(a) *$t(q, 3) = 3$ for $q \notin \{16, 7, 13\}$.*

(b) *$t(7, 3) = t(13, 3) = t(16, 3) = 4$.*

Proof. Let a and b be in $\mathbb{F}_q$. Suppose that q is odd. Since the polynomial $t - (at + b)^3$ has no triple roots, it follows that it is not the cube of a linear polynomial. Assume now that q is even, and take $(a, b) \neq (1, 0)$. Since the polynomial $t + (at + b)^3$ has no double roots, it follows that it is not the cube of a linear polynomial. Finally, observe that the polynomial $t + t^3$ is not the cube of a linear polynomial. Therefore

$$t(q,3) \geq 3.$$

We suppose that $q \notin \{16, 7, 13\}$. In view of Proposition 1, there exist a, b in $\mathbb{F}_q$ such that

$$1 = a^3 + b^3, \qquad ab \neq 0. \tag{4}$$

Thus, for any $P \in \mathbb{F}_q[t]$, one has the Serre Identity (see also [Va])

$$P = \left(\frac{1}{3a}(P + a^3 + 1)\right)^3 + \left(\frac{1}{3b}(P + a^3 - 2)\right)^3 + \left(\frac{-1}{3ab}(P - 2a^3 + 1)\right)^3.$$

Hence,

$$t(q,3) \leq 3.$$

In order to establish the proposition we investigate the remaining cases.

For $q = 7$, one has

$$P = (P+1)^3 + (P-1)^3 - (P+3)^3 - (P-3)^3.$$

For $q = 13$, one has

$$P = (P+1)^3 + (P-1)^3 - (P+4)^3 - (P-4)^3.$$

Let $a \in \mathbb{F}_4$ be such that $a^2 = a + 1$ and let $b \in \mathbb{F}_{16}$ be such that $b^2 = b + a$. Then for any $P \in \mathbb{F}_{16}[t]$ one has

$$P = (bP + a)^3 + (bP + a + 1)^3 + (P + ab^2)^3 + (P + (a+1)b^2)^3.$$

Hence,

$$t(q,3) \leq 4 \qquad \text{for } q \in \{7, 13, 16\}.$$

Assume now that $q \in \{7, 13, 16\}$. Suppose that $t = P_1^3 + P_2^3 + P_3^3$, where $P_i \in \mathbb{F}_q[t]$ and $\deg(P_i) \leq 1$ for $i = 1, 2, 3$. Since $t(q,3) \geq 3$, $\deg(P_i) = 1$ for each index i. But the coefficient of t^3 in the sum $P_1^3 + P_2^3 + P_3^3$ is equal to 0. This contradicts Proposition 1(b). Hence, $t(q,3) \geq 4$, thereby finishing the proof.

4. The descent. In all this section q denotes a power of a prime $p \neq 3$; for any nonzero polynomial $P \in \mathbb{F}_q[t]$, $\mathrm{sgn}(P)$ denotes the leading coefficient of P, and $[r]$ denotes the integer part of a real r.

PROPOSITION 3. *Let $Y \neq 0$ in $\mathbb{F}_q[t]$ be such that* $\deg(Y) \equiv 0 \pmod 3$ *and* $\mathrm{sgn}(Y)$ *is a cube in $\mathbb{F}_q$. Then there exist polynomials $Z, R \in \mathbb{F}_q[t]$ such that*

(a) $Y = Z^3 + R$,
(b) $\deg(Z^3) = \deg(Y)$,
(c) $\deg(R^3) < \deg(Y^2)$.

Proof. Write

$$Y = y_0 + \ldots + y_n t^n,$$

so that $y_n = \alpha^3$ for some $\alpha \in \mathbb{F}_q$, $\alpha \neq 0$. Moreover, $n = 3m$ where m is a nonnegative integer. We consider the relations:

$$(\mathrm{r}_0) \qquad z_m = \alpha,$$

$$(\mathrm{r}_1) \qquad 3z_m^2 z_{m-1} = y_{n-1},$$

$$(\mathrm{r}_j) \qquad 3z_m^2 z_{m-j} + \sum_{a,b,c\in]m-j,m],\, a+b+c=3m-j} z_a z_b z_c = y_{n-j},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(\mathrm{r}_m) \qquad 3z_m^2 z_0 + \sum_{a,b,c\in]0,m],\, a+b+c=2m} z_a z_b z_c = y_{n-m},$$

that define $z_m, z_{m-1}, \ldots, z_1, z_0$. Define the polynomials Z, R by

$$Z = z_0 + z_1 t + \ldots + z_m t^m, \qquad R = Y - Z^3.$$

It is clear now that (a) and (b) hold. By construction of Z it follows that $\deg(R) < n - m$, thereby finishing the proof.

PROPOSITION 4. *Let* $Y \neq 0$ *in* $\mathbb{F}_q[t]$ *be such that* $\deg(Y) \equiv 0 \pmod 3$ *and* $\mathrm{sgn}(Y)$ *is a cube in* $\mathbb{F}_q$. *Then there exist polynomials* $Z, R \in \mathbb{F}_q[t]$ *such that*

(a) $Y = Z^3 + R$,
(b) $\deg(Z^3) = \deg(Y)$,
(c) $\deg(R^3) \leq 6 + \deg(Y^2)$,
(d) R *is monic and* $\deg(R) \equiv 0 \pmod 3$. *More precisely, one has*

$$\deg(R) = 3(\deg(Y)/3 - [\deg(Y)/9]).$$

Proof. We keep the notations of the above proof. We set $s = [m/3]$, the integer part of $m/3$. Observe that $3s \leq m$. We consider here the equations $(\mathrm{r}_0), (\mathrm{r}_1), \ldots, (\mathrm{r}_{3s-1})$, and instead of the equation (r_{3s}), we consider the equation

$$(\varrho_{3s}) \qquad 3z_m^2 z_{m-3s} + \sum_{a,b,c\in]m-3s,m],\, a+b+c=3m-3s} z_a z_b z_c = y_{n-3s} - 1.$$

The relations $(\mathrm{r}_0), (\mathrm{r}_1), \ldots, (\mathrm{r}_{3s-1})$ and (ϱ_{3s}) define $z_m, z_{m-1}, \ldots, z_{m-3s+1}$, z_{m-3s}. Again, define

$$Z = z_{m-3s} t^{m-3s} + z_{m-3s+1} t^{m-3s+1} + \ldots + z_m t^m, \qquad R = Y - Z^3.$$

It is now clear that (a) and (b) hold. Now we show (d). Firstly, since $z_m, z_{m-1}, \ldots, z_{m-3s+1}, z_{m-3s}$ satisfy $(\mathrm{r}_0), (\mathrm{r}_1), \ldots, (\mathrm{r}_{3s-1})$, it follows that $\deg(R) \leq n - 3s$. Secondly, since $z_m, z_{m-1}, \ldots, z_{m-3s+1}, z_{m-3s}$ satisfy (ϱ_{3s}) it follows that $\deg(R) = n - 3s = 3(m - s)$ and $\mathrm{sgn}(R) = 1$, finishing the proof of (d). Finally, observe that $3s > m - 3$, so that $\deg(R) < 2m + 3$. This proves (c) and hence the proposition.

PROPOSITION 5. *Let* $Y \neq 0$ *in* $\mathbb{F}_q[t]$ *be such that* $\deg(Y) \equiv 0 \pmod 3$ *and* $\operatorname{sgn}(Y)$ *is a cube in* $\mathbb{F}_q$. *If* $\deg(Y) \neq 6$, *then there exist polynomials* $Z_1, Z_2, Z_3 \in \mathbb{F}_q[t]$ *such that*

(a) $3\deg(Y - Z_1^3 - Z_2^3 - Z_3^3) \leq \deg(Y)$,
(b) $3\max(\deg(Z_1), \deg(Z_2), \deg(Z_3)) \leq \deg(Y)$.

Proof. First of all, observe that $\deg(Y)$ can be written as

$$\deg(Y) = 27n + 9m + 3k, \qquad \text{where } 0 \leq m, k \leq 2.$$

The main argument is as follows. We apply Proposition 4 twice. Firstly, we obtain the existence of polynomials Z_1 and Y_1 such that

$$Y = Z_1^3 + Y_1,$$
$$\deg(Z_1) = 9n + 3m + k, \qquad \deg(Y_1) = 18n + 6m + 3k, \qquad \operatorname{sgn}(Y_1) = 1.$$

Secondly, we obtain the existence of polynomials Z_2 and Y_2 such that

$$Y_1 = Z_2^3 + Y_2,$$
$$\deg(Z_2) = 6n + 2m + k, \qquad \deg(Y_2) = 12n + 3(m + a), \qquad \operatorname{sgn}(Y_2) = 1,$$

where the nonnegative integer a is defined in the following manner:

$$a = \begin{cases} 0 & \text{if } (m,k) = (0,0), \\ 1 & \text{if } (m,k) \in \{(0,1), (1,0), (1,1), (2,0)\}, \\ 2 & \text{if } (m,k) \in \{(0,2), (1,2), (2,1), (2,2)\}. \end{cases}$$

Finally, we apply Proposition 3. Therefore there exist polynomials Z_3 and Y_3 such that

$$Y_2 = Z_3^3 + Y_3,$$
$$\deg(Z_3) = 4n + m + a, \qquad \deg(Y_3) < 8n + 2m + 2a.$$

It remains to be shown that $3\deg(Y_3) \leq \deg(Y)$. Suppose that $2a < n + m + k + 2$. The result follows from the inequality $\deg(Y_3) < 8n + 2m + 2a$. But the case where $2a \geq n + m + k + 2$ may occur only if $n = 0, m = 0, k = 2$, i.e. when $\deg(Y) = 6$. This case has been excluded by the hypothesis.

PROPOSITION 6. *Let* $r = r(q) = \max(1, c(q,3) - 1)$. *Let* $Y \in \mathbb{F}_q[t]$ *be a nonzero polynomial. Then for* $1 \leq i \leq r$ *there exist polynomials* $Z_i \in \mathbb{F}_q[t]$ *such that*

(a) $3\deg(Z_i) < \deg(Y) + 3$,
(b) $\deg(Y - Z_1^3 - \ldots - Z_r^3) \equiv 0 \pmod 3$ *and* $\operatorname{sgn}(Y - Z_1^3 - \ldots - Z_r^3)$ *is a cube in the field* $\mathbb{F}_q$,
(c) *if* $\deg(Y) \notin \{4,5,6\}$ *then* $\deg(Y - Z_1^3 - \ldots - Z_r^3) \neq 6$.

Proof. If $\deg(Y) \in \{3n-1, 3n-2\}$ for some integer $n \geq 1$, we take $Z_1 = -t^n, Z_2 = \ldots = Z_r = 0$. Suppose now that $\deg(Y) = 3n$. If $q \not\equiv 1 \pmod 3$, then $\mathrm{sgn}(Y)$ is a cube in $\mathbb{F}_q$ so that we take $Z_1 = \ldots = Z_r = 0$, otherwise it follows from Proposition 1 that there exist $a_1 \in \mathbb{F}_q, \ldots, a_{r+1} \in \mathbb{F}_q$ such that $\mathrm{sgn}(Y) = a_1^3 + \ldots + a_{r+1}^3$ with $a_{r+1} \neq 0$. Thus, in this latter case we let $Z_i = a_i t^n$ for $i = 1, \ldots, r$. In all cases we conclude that $\deg(Y - Z_1^3 - \ldots - Z_r^3) = 3n$ and $\mathrm{sgn}(Y - Z_1^3 - \ldots - Z_r^3)$ is a cube in $\mathbb{F}_q$.

Remark 1. From Proposition 1 it follows that $r(q) = 1$ for $q \neq 7$ and $r(7) = 2$.

Proposition 7. *Let $s = s(q) = 2c(q,3)$ and let $Y \in \mathbb{F}_q[t]$ be a polynomial of degree 6. Then for $1 \leq i \leq s$ there exist polynomials $Z_i \in \mathbb{F}_q[t]$ such that*

(a) $\deg(Y - Z_1^3 - \ldots - Z_s^3) \leq 2$,
(b) $\max(\deg(Z_1), \ldots, \deg(Z_s)) \leq 2$.

Proof. With $c = c(q,3)$ one finds $a_1 \in \mathbb{F}_q, \ldots, a_c \in \mathbb{F}_q$ such that $\mathrm{sgn}(Y) = a_1^3 + \ldots + a_c^3$ with $a_c \neq 0$. For $i = 1, \ldots, c-1$ define the polynomials Z_i by $Z_i = a_i t^2$. Then $\deg(Y - Z_1^3 - \ldots - Z_{c-1}^3) = 6$ and $\mathrm{sgn}(Y - Z_1^3 - \ldots - Z_{c-1}^3)$ is a cube.

It follows now from Proposition 3 that there exists a polynomial Z_c such that

$$\deg(Y - Z_1^3 - \ldots - Z_{c-1}^3 - Z_c^3) \leq 3.$$

In order to finish the proof, we will define the polynomials $Z_{c+1}, \ldots, Z_{2c}$ as follows. If $\deg(Y - Z_1^3 - \ldots - Z_{c-1}^3 - Z_c^3) < 3$, then we let $Z_{c+1} = \ldots = Z_{2c} = 0$. If not, let $a_{c+1} \in \mathbb{F}_q, \ldots, a_{2c} \in \mathbb{F}_q$ be such that

$$\mathrm{sgn}(Y - Z_1^3 - \ldots - Z_{c-1}^3 - Z_c^3) = a_{c+1}^3 + \ldots + a_{2c}^3.$$

Then we let $Z_i = a_i t$ for $i = c+1, \ldots, 2c$, so that

$$\deg(Y - Z_1^3 - \ldots - Z_c^3 - Z_{c+1}^3 - \ldots - Z_{2c}^3) \leq 2.$$

Proposition 8. *Let $m = m(q) = 2 + c(q,3)$ and let $Y \in \mathbb{F}_q[t]$ be such that* $\deg(Y) \in \{4,5\}$. *Then for $1 \leq i \leq m$ there exist polynomials $Z_i \in \mathbb{F}_q[t]$ such that*

(a) $\deg(Y - Z_1^3 - \ldots - Z_m^3) \leq 2$,
(b) $\max(\deg(Z_1), \ldots, \deg(Z_m)) \leq 2$.

Proof. Let $Z = t^6 + Y$. By Proposition 3, there exists a polynomial Z_1 such that

$$\deg(Z_1) \leq 2, \quad \deg(Z - Z_1^3) \leq 3.$$

We conclude the proof as above.

5. A bound for $g(q,3)$. The above notations remain valid. We obtain the following propositions.

PROPOSITION 9. *Let $g = g(q) = \max(1, c(q,3) - 1) + t(q,3) + 3$ and let $Y \neq 0$ in $\mathbb{F}_q[t]$ be such that $\deg(Y) \notin \{4,5,6\}$. Then for $1 \leq i \leq g$ there exist polynomials $Y_i \in \mathbb{F}_q[t]$ such that*

(a) $Y = Y_1^3 + \ldots + Y_g^3$,
(b) $3\max(\deg(Y_1), \ldots, \deg(Y_g)) < 3 + \deg(Y)$.

Proof. Let

$$r = r(q), \quad t_3 = t(q,3).$$

By Proposition 6, for $1 \leq i \leq r$ there exist polynomials $Y_i \in \mathbb{F}_q[t]$ such that

(i) $3\deg(Y_i) < \deg(Y) + 3$,
(ii) $\deg(Y - Y_1^3 - \ldots - Y_r^3) \equiv 0 \pmod 3$,
(iii) $\operatorname{sgn}(Y - Y_1^3 - \ldots - Y_r^3)$ is a cube in the field $\mathbb{F}_q$,
(iv) $\deg(Y - Y_1^3 - \ldots - Y_r^3) \neq 6$.

By Proposition 5, for $1 \leq i \leq 3$ there exist polynomials $Z_i \in \mathbb{F}_q[t]$ such that

$$3\deg(Y - Y_1^3 - \ldots - Y_r^3 - Z_1^3 - Z_2^3 - Z_3^3) \leq \deg(Y - Y_1^3 - \ldots - Y_r^3),$$

and

(v) $3\max(\deg(Z_1), \deg(Z_2), \deg(Z_3)) \leq \deg(Y - Y_1^3 - \ldots - Y_r^3)$.

By (i), (ii) and (v) we obtain

$$3\max(\deg(Z_1), \deg(Z_2), \deg(Z_3)) < \deg(Y) + 3.$$

Next, define the polynomial U by

(vi) $U = Y - Y_1^3 - \ldots - Y_r^3 - Z_1^3 - Z_2^3 - Z_3^3$.

It is clear that

$$3\deg(U) < \deg(Y) + 3,$$

so that, by definition of the number $t_3 = t(q,3)$, there exist $U_i \in \mathbb{F}_q[t]$, $1 \leq i \leq t_3$, such that

$$U = U_1^3 + \ldots + U_{t_3}^3,$$

with every U_i satisfying $\deg(U_i) \leq \deg(U)$, and we may therefore apply (vi) to conclude the proof.

PROPOSITION 10. *Let $\gamma = \gamma(q) = \max(s(q), m(q)) + t(q,3)$ and let $Y \in \mathbb{F}_q[t]$ be such that $\deg(Y) \in \{4,5,6\}$. Then for $1 \leq i \leq \gamma$ there exist polynomials $Y_i \in \mathbb{F}_q[t]$ such that*

(a) $Y = Y_1^3 + \ldots + Y_\gamma^3$,
(b) $3\max(\deg(Y_1), \ldots, \deg(Y_\gamma)) < 3 + \deg(Y)$.

Proof. Let $n = \max(2 + c(q,3), 2c(q,3))$ and $t_3 = t(q,3)$. Propositions 7 and 8 show that there exist $Y_i \in \mathbb{F}_q[t]$, $1 \le i \le n$, such that

$$\deg(Y - Y_1^3 - \ldots - Y_n^3) \le 2, \quad \deg(Y_i) \le 2.$$

Define the polynomial V by

$$V = Y - Y_1^3 - \ldots - Y_n^3,$$

so that, by definition of t_3, there exist $V_i \in \mathbb{F}_q[t]$, $1 \le i \le t_3$, such that

$$V = V_1^3 + \ldots + V_{t_3}^3, \quad \deg(V_i) \le \deg(V) \le 2,$$

finishing the proof.

6. Main result. Now we may show our main result.

THEOREM 1. *Let q be a power of a prime number $p \neq 3$. Then*

(a) $g(q,3) \le 7$ *for* $q \notin \{2,4,16,7,13\}$,
(b) $\max(g(13,3), g(16,3)) \le 8$,
(c) $g(7,3) \le 9$.

Proof. Suppose that $q \notin \{2,4,16,7,13\}$. Then $t(q,3) = 3$ and $r(q) = 1$. Proposition 9 shows that any polynomial whose degree is different from $4,5,6$ admits a strict representation as a sum of 7 cubes. On the other hand, Proposition 10 shows that a polynomial of degree $4,5$ or 6 admits a strict representation as a sum of 6 or 7 cubes according to the value of q modulo 3.

The other relations are obtained similarly from the equalities

$$t(7,3) = t(13,3) = t(16,3) = 4, \quad c(7,3) = 3, \quad c(13,3) = c(16,3) = 2,$$

thus completing the proof of the theorem.

Acknowledgments. We thank the G.D.R. "Théorie Analytique des Nombres" of Bordeaux (director: Jean-Marc Deshouillers), for financial support of a short stay of the authors at Bordeaux, where the main part of this work was done.

References

[EH] G. W. Effinger and D. R. Hayes, *Additive Number Theory of Polynomials over a Finite Field*, Oxford Math. Monogr., Clarendon Press, Oxford, 1991.

[Ga] L. Gallardo, *On the restricted Waring problem over* $\mathbb{F}_{2^n}[t]$, Acta Arith. 92 (2000), 109–113.

[LN] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Cambridge Univ. Press, 1984. Reprinted 1987.

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

Department of Mathematics
University Aix-Marseille III
Avenue Escadrille Normandie-Niemen
13397 Marseille Cedex 20, France
E-mail: mireille.car@univ.u-3mrs.fr

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

Received on 4.3.2002 (4242)