

THE UNRESTRICTED VARIANT OF WARING'S PROBLEM IN FUNCTION FIELDS

YU-RU LIU¹ AND TREVOR D. WOOLEY²

In honorem Jean-Marc Deshouillers annos LX nati

ABSTRACT. Let $\mathbb{J}_q^k[t]$ denote the additive closure of the set of k th powers in the polynomial ring $\mathbb{F}_q[t]$, defined over the finite field \mathbb{F}_q having q elements. We show that when $s \geq k+1$ and $q \geq k^{2k+2}$, then every polynomial in $\mathbb{J}_q^k[t]$ is the sum of at most s k th powers of polynomials from $\mathbb{F}_q[t]$. When k is large and $s \geq (\frac{4}{3} + o(1))k \log k$, the same conclusion holds without restriction on q . Refinements are offered that depend on the characteristic of \mathbb{F}_q .

1. Introduction. Investigations concerning Waring's problem in function fields have focused on two variants, a *restricted* problem in which the degrees of the polynomials employed in the representation are confined to be as small as is possible, and the corresponding *unrestricted* problem in which no such constraints are imposed. Let $\mathbb{F}_q[t]$ denote the polynomial ring defined over the finite field \mathbb{F}_q having q elements, and, when k is a natural number, define $\mathbb{J}_q^k[t]$ to be the additive closure of the set of k th powers in $\mathbb{F}_q[t]$. In 1933, Paley [8] considered the unrestricted variant of Waring's problem, showing that a natural number s exists with the property that every polynomial in $\mathbb{J}_q^k[t]$ may be represented as the sum of s k th powers of polynomials from $\mathbb{F}_q[t]$. Let $w_q(k)$ denote the least permissible choice for such a number s . In this paper we make progress on bounds for $w_q(k)$ in two directions. On one hand, we apply estimates stemming from Deligne's resolution of the Weil conjectures so as to obtain sharp bounds valid when q is sufficiently large in terms of k . On the other hand, making use of the Hardy-Littlewood method, we derive weaker bounds valid uniformly in q .

Before proceeding further, we require some notation. When k is a natural number and p is a prime number, we define the integer k_p as follows. We write k in base p , say

$$k = a_0 + a_1p + \cdots + a_n p^n, \tag{1}$$

where $0 \leq a_i < p$ ($0 \leq i \leq n$), and then put $k_p = \prod_{i=0}^n (a_i + 1) - 1$. It is apparent that $k_p \leq k$ for every k , and that $k_p = k$ if and only if $k < p$, or else $k = p^m - 1$ for some natural number m . In §2 we derive the bound for $w_q(k)$ recorded in the following theorem.

2000 *Mathematics Subject Classification.* 11P05, 11T55, 11P55.

Key words and phrases. Waring's problem, Function fields.

¹Research supported in part by an NSERC discovery grant.

²Research supported in part by NSF grant DMS-0601367.

Theorem 1. *Let k be a natural number, and suppose that \mathbb{F}_q is a finite field of characteristic p . Then whenever $q \geq k^{2k_p} k_p^2$, one has $w_q(k) \leq k_p + 1$.*

For comparison, Theorems 1(iii) and 4(iii) of Vaserstein [12] show that when $q \geq k^4$, and in addition q exceeds a certain Ramsey number defined in terms of k , then $w_q(k) \leq 3k_p/2$. In addition to providing a sharper bound for $w_q(k)$, the conclusion of Theorem 1 has the merit of replacing the potentially astronomical Ramsey number in the condition on q by an explicit function of k of terrestrial magnitude. Now observe that -1 is a sum of k th powers in \mathbb{F}_q (consider $q - 1$ copies of 1^k for example), and so the set of polynomials that are the sum of some finite number of terms of the form $\pm x^k$, with $x \in \mathbb{F}_q[t]$, is equal to $\mathbb{J}_q^k[t]$. Let $v_q(k)$ denote the least natural number s with the property that, whenever $m \in \mathbb{J}_q^k[t]$, then m is the sum of at most s such terms. Theorem 1(iii) of Vaserstein [12] shows that when q is larger than a certain Ramsey number defined in terms of k , then $v_q(k) \leq k_p$. For odd k one has $w_q(k) = v_q(k)$, and so the latter conclusion supercedes the upper bound on $w_q(k)$ provided by Theorem 1 for odd k , albeit with a potentially severe constraint on q . On the other hand, the trivial relation $v_q(k) \leq w_q(k)$ leads from Theorem 1 to the bound $v_q(k) \leq k_p + 1$, provided only that $q \geq k^{2k_p} k_p^2$. See [10] and [11] for further bounds on $v_q(k)$ and $w_q(k)$ valid for intermediate ranges of q .

When $g \in \mathbb{F}_q[t]$, let $\text{ord } g$ denote the degree of g . We say that m admits a *strict representation* as a sum of s k th powers when, for some $x_i \in \mathbb{F}_q[t]$ with $\text{ord } x_i \leq \lceil (\text{ord } m)/k \rceil$ ($1 \leq i \leq s$), one has $m = x_1^k + \cdots + x_s^k$. Here, as usual, we write $\lceil \theta \rceil$ for the least integer greater than or equal to θ . When k and q are natural numbers exceeding 1, define $G_q(k)$ to be the least integer s with the property that, whenever $m \in \mathbb{J}_q^k[t]$ has degree sufficiently large in terms of k and q , then m admits a strict representation as the sum of s k th powers. By reference to the argument underlying Theorem 1.4(ii) of Gallardo and Vaserstein [3], we obtain the following direct consequence of Theorem 1 in §3.

Corollary 2. *Let k be an integer exceeding 3, and suppose that \mathbb{F}_q is a finite field of characteristic p . Then whenever $q \geq k^{2k_p} k_p^2$, one has $G_q(k) < k \log k + k_p - \frac{1}{2} \log k + 4$.*

For comparison, Theorem 1.4(ii) of [3] shows that when $q > k^4$, one has $G_q(k) < k \log(k + 1) + 2k + 1$. The conclusion of Corollary 2 is modestly sharper at the expense of requiring q to be rather larger.

For smaller values of q , the most problematic cases are those wherein the characteristic p of \mathbb{F}_q is smaller than k . By employing work of Kubota [5,6], the paper of Chinburg [1] comes closest to providing bounds uniform in q , though the focus is on $v_q(k)$ rather than $w_q(k)$. In §4 we apply our recent work [7] to establish a uniform bound on $w_q(k)$. Define the integer $A = A_q(k)$ as follows. Let k_0 be the largest divisor of k coprime to q . Write k in base p as in (1), take $\gamma = a_0 + a_1 + \cdots + a_n$, and then set $A = (1 - 2^{-\gamma})^{-1}$ when $p < k_0$, and $A = 1$ when $p > k_0$. Finally, when x is a positive number, write $\text{Log } x$ for $\max\{1, \log x\}$, and put

$$\widehat{G}_q(k) = Ak_0(\text{Log } k_0 + \text{Log Log } k_0 + 2 + A \text{Log Log } k_0 / \text{Log } k_0).$$

Theorem 3. *There is a positive absolute constant C with the property that whenever k is a natural number and \mathbb{F}_q is a finite field, then $w_q(k) \leq \widehat{G}_q(k) + Ck_0\sqrt{\text{Log } k_0}/\text{Log } k_0$.*

The conclusion of Theorem 3 implies that the bound $w_q(k) \leq (\frac{4}{3} + o(1))k \log k$ holds uniformly in k and q . For a specific exponent k and finite field \mathbb{F}_q , moreover, the algorithm associated with Theorem 14.2 of [7] provides an explicit upper bound for $w_q(k)$. We avoid providing the lengthy details of this algorithm in the interests of concision. We note also that since $v_q(k) \leq w_q(k)$, the bound supplied by Theorem 3 for $w_q(k)$ applies also to $v_q(k)$.

The authors are grateful to Professors Gallardo and Vaserstein for making available their preprint [3], without which the conclusion recorded in Corollary 2 could not have been presented.

2. Methods applicable for larger q . In order to bound $w_q(k)$ for larger q , we consider the polynomial equation

$$x_1^k(t + y_1)^k + \cdots + x_s^k(t + y_s)^k = at + b. \tag{2}$$

For suitable elements $a, b \in \mathbb{F}_q$, with a non-zero, we seek a solution $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^s$ of the equation (2). It transpires that when q is sufficiently large, such a solution may be shown to exist when s is taken to be $k_p + 1$, which we henceforth assume. Fix any such solution of (2), and consider a given polynomial $m(t) \in \mathbb{F}_q[t]$. A representation of $m(t)$ as the sum of s k th powers of elements of $\mathbb{F}_q[t]$ is obtained by replacing t by $a^{-1}(m(t) - b)$ in (2), and thereby we confirm that $w_q(k) \leq s$. Considering the coefficients of powers of t in (2), we derive a system of equations over \mathbb{F}_q which we investigate by means of Deligne's resolution of the Weil conjectures.

The proof of Theorem 1. Let k and q be natural numbers satisfying the hypotheses of the statement of Theorem 1, and let p be the characteristic of \mathbb{F}_q . Plainly, there is nothing to prove when $k = 1$. Moreover, when $p|k$ one has

$$x_1^k + \cdots + x_s^k = (x_1^{k/p} + \cdots + x_s^{k/p})^p \in \mathbb{F}_q[t^p].$$

Writing k_0 for the largest divisor of k coprime to q , we deduce that $w_q(k) = w_q(k_0)$. There is consequently no loss in supposing that $k \geq 2$ and $(k, p) = 1$, as we assume henceforth. Next write k in base p as in (1). We recall that the binomial coefficient $\binom{k}{r}$ is coprime to p if and only if the base p expansion of r takes the form $r = b_0 + b_1p + \cdots + b_n p^n$, with $0 \leq b_i \leq a_i$ ($0 \leq i \leq n$) (this follows from Lucas' criterion; see, for example, the argument of the proof of Lemma 8.1 of [7]). Write \mathcal{R} for the set of integers r , with $0 \leq r \leq k$, for which $\binom{k}{r}$ is not divisible by p . Note that since $p \nmid k$, one has $k - 1 \in \mathcal{R}$. We may suppose that $\mathcal{R} = \{r_1, r_2, \dots, r_s\}$, with $0 = r_1 < r_2 < \cdots < r_s = k$. For the sake of concision, we write \mathcal{R}_1 for $\mathcal{R} \setminus \{k\}$, and \mathcal{R}_2 for $\mathcal{R} \setminus \{k - 1, k\}$.

When ε is 1 or 2, and $\mathbf{y} \in \mathbb{F}_q^s$, we denote by $N_\varepsilon(\mathbf{y})$ the number of distinct \mathbb{F}_q -rational projective solutions \mathbf{x} of the system

$$x_1^k y_1^r + \cdots + x_s^k y_s^r = 0 \quad (r \in \mathcal{R}_\varepsilon). \tag{3.ε}$$

Here, we interpret z^0 as unity for every z in \mathbb{F}_q . We seek to establish that \mathbf{y} may be chosen from \mathbb{F}_q^s in such a manner that $N_2(\mathbf{y}) > N_1(\mathbf{y})$. In such circumstances, a solution \mathbf{x} of (3.2) necessarily exists for which the expression $x_1^k y_1^{k-1} + \cdots + x_s^k y_s^{k-1}$ is non-zero, and hence the equation (2) is satisfied with $a \neq 0$. From this, as we have already noted in the discussion following (2), the desired conclusion $w_q(k) \leq s$ follows at once.

In order to make a suitable choice for \mathbf{y} , we introduce for $\varepsilon = 1$ and 2 the determinant $\mathfrak{V}(\mathbf{z}; \mathcal{B}_\varepsilon, \mathcal{R}_\varepsilon)$, which we define for $(s - \varepsilon)$ -element subsets \mathcal{B}_ε of $\{1, 2, \dots, s\}$ by $\mathfrak{V}(\mathbf{z}; \mathcal{B}_\varepsilon, \mathcal{R}_\varepsilon) = \det(z_i^{r_j})$, where the entries are indexed by $i \in \mathcal{B}_\varepsilon$ and $j \in \{1, \dots, s - \varepsilon\}$ (in numerically increasing order). Consider the polynomial $\mathfrak{F}(\mathbf{z})$ given by the product of the polynomials $\mathfrak{V}(\mathbf{z}; \mathcal{B}_\varepsilon, \mathcal{R}_\varepsilon)$ over all $(s - \varepsilon)$ -element subsets \mathcal{B}_ε of $\{1, \dots, s\}$, for $\varepsilon = 1$ and 2 . The degree of $\mathfrak{F}(\mathbf{z})$ is at most ks^3 , and so it follows from Lemma 1 of Schmidt [9] that whenever $q > ks^3$, then a choice for $\mathbf{y} \in \mathbb{F}_q^s$ exists with the property that $\mathfrak{V}(\mathbf{y}; \mathcal{B}_\varepsilon, \mathcal{R}_\varepsilon) \neq 0$ for every $(s - \varepsilon)$ -element subset \mathcal{B}_ε of $\{1, \dots, s\}$, for $\varepsilon = 1, 2$. We now fix a choice for \mathbf{y} with the latter property, and we consider the system (3.2).

We claim that the complete intersection defined by (3.2) is non-singular. Suppose to the contrary that a singular solution \mathbf{x} exists. Then whenever $\mathcal{B}_2 = \{u_1, u_2, \dots, u_{s-2}\}$, with $1 \leq u_1 < u_2 < \cdots < u_{s-2} \leq s$, one must have $\det(kx_{u_i}^{k-1}y_{u_i}^{r_j})_{1 \leq i, j \leq s-2} = 0$, whence

$$k^{s-2}(x_{u_1}x_{u_2}\cdots x_{u_{s-2}})^{k-1}\mathfrak{V}(\mathbf{y}; \mathcal{B}_2, \mathcal{R}_2) = 0.$$

But by hypothesis, one has $\mathfrak{V}(\mathbf{y}; \mathcal{B}_2, \mathcal{R}_2) \neq 0$, and so x_{u_i} must be zero for some index i with $1 \leq i \leq s-2$. Considering such implications as arise from all possible $(s-2)$ -element subsets of $\{1, 2, \dots, s\}$, we infer that x_j is necessarily zero for at least 3 distinct indices j with $1 \leq j \leq s$. Temporarily relabelling variables so that x_{s-1} and x_s are zero, we set $\mathcal{B}_2 = \{1, 2, \dots, s-2\}$ and examine (3.2). Since \mathbf{x} defines a projective solution of (3.2), the variables x_1, \dots, x_{s-2} cannot all be zero, and so one must have $\mathfrak{V}(\mathbf{y}; \mathcal{B}_2, \mathcal{R}_2) = 0$. But in view of our earlier choice of \mathbf{y} , this is impossible. We therefore arrive at a contradiction, and are forced to conclude that the variety X defined by the system (3.2) is non-singular.

The projective non-singular complete intersection (3.2) is defined by $s-2$ equations of degree k in s variables, so the components of X each have dimension 1. Since we have established that this variety is non-singular, it follows that X is regular in codimension one, and hence irreducible (see, for example, the preamble to Corollary 6.2 of [4]). We therefore deduce from Theorem 6.1 of Ghorpade and Lachaud [4] that $|N_2(\mathbf{y}) - (q+1)| \leq b_1\sqrt{q}$, where, in view of Example 4.3(ii) of [4], the Betti number b_1 is equal to $k^{s-2}(k(s-2)-s)+2$ (see also Theorem 8.1 of Deligne [2]). We may conclude thus far, therefore, that

$$N_2(\mathbf{y}) \geq q + 1 - k^{s-1}(s-2)\sqrt{q}. \quad (4)$$

Next we consider the system (3.1). Set $\mathcal{B}_1 = \{1, 2, \dots, s-1\}$. In view of our choice for \mathbf{y} , one has $\mathfrak{V}(\mathbf{y}; \mathcal{B}_1, \mathcal{R}_1) \neq 0$. Therefore, if we fix any non-zero choice for x_s , we deduce that the system

$$x_1^k y_1^r + \cdots + x_{s-1}^k y_{s-1}^r = -x_s^k y_s^r \quad (r \in \mathcal{R}_1),$$

uniquely determines $(x_1^k, \dots, x_{s-1}^k)$. There are consequently at most k^{s-1} possible such choices for (x_1, \dots, x_{s-1}) . When $x_s = 0$, meanwhile, the same argument shows that

$(x_1, \dots, x_{s-1}) = \mathbf{0}$. We therefore deduce that the number of projective solutions of the system (3.1) counted by $N_1(\mathbf{y})$ is at most k^{s-1} . On combining the latter estimate with (4), we find that

$$N_2(\mathbf{y}) - N_1(\mathbf{y}) \geq q + 1 - k^{s-1}(s-2)\sqrt{q} - k^{s-1}.$$

But by hypothesis, we may suppose that $q \geq k^{2s-2}(s-1)^2$, and thus we conclude that $N_2(\mathbf{y}) > N_1(\mathbf{y})$. In view of the discussion following equation (3.ε) above, we infer that $w_q(k) \leq s$, and this completes the proof of Theorem 1.

3. The method of Gallardo and Vaserstein. The conclusion of Corollary 2 follows from Theorem 1 by means of a direct application of the methods of Gallardo and Vaserstein [3], additional refinements stemming only from careful book-keeping. Consider a polynomial $m \in \mathbb{J}_q^k[t]$ of sufficiently large degree d . As reported in [3], it is a consequence of work of Weil [13] that when $q \geq k^4$, then every element of \mathbb{F}_q is the sum of two k th powers from \mathbb{F}_q . Let

$$n = \left\lceil \frac{\log k}{\log(k/(k-1))} \right\rceil + 2. \tag{5}$$

Then an inspection of the argument of the proof of Proposition 3.5 of [3] reveals that there exist polynomials $x_i \in \mathbb{F}_q[t]$ ($1 \leq i \leq n$), each of degree not exceeding $\lceil (\text{ord } m)/k \rceil$, with the property that the polynomial $m_0 = m - x_1^k - \dots - x_n^k$ has degree at most D , where $D = k \lfloor d/k \rfloor (1 - 1/k)^{n-2} + k(k-1)$. When $k > 2$, the quotient $(\log k)/(\log(k/(k-1)))$ is not an integer, and hence there is a positive number $\delta = \delta_k$ for which $D \leq (1 - \delta)d/k + k^2$. We note that the latter is at most d/k whenever d is sufficiently large in terms of k . It follows from (5), moreover, that for $k \geq 4$ one has $n < k \log k - \frac{1}{2} \log k + 3$.

We next recall that since -1 is a sum of k th powers in \mathbb{F}_q , then m_0 is the sum of some number of k th powers from $\mathbb{F}_q[t]$, that is $m_0 \in \mathbb{J}_q^k[t]$. Consequently, when $q \geq k^{2k_p} k_p^2$ and $u \geq k_p + 1$, the conclusion of Theorem 1 demonstrates that the polynomial m_0 is represented in the shape $m_0 = y_1^k + \dots + y_u^k$, with $y_i \in \mathbb{F}_q[t]$ ($1 \leq i \leq u$). An inspection of the proof of Theorem 1 in §2, moreover, confirms that one may constrain the polynomials y_i ($1 \leq i \leq u$) employed in the latter representation to have degree at most that of m_0 , namely $D \leq d/k$. We conclude that m possesses the representation $m = x_1^k + \dots + x_n^k + y_1^k + \dots + y_u^k$, with $x_i \in \mathbb{F}_q[t]$ ($1 \leq i \leq n$) each of degree at most $\lceil (\text{ord } m)/k \rceil$, and with $y_j \in \mathbb{F}_q[t]$ ($1 \leq j \leq u$) each of degree $d/k \leq \lceil (\text{ord } m)/k \rceil$. In particular, the polynomial m has a restricted representation as the sum of $(n + u)$ k th powers of polynomials from $\mathbb{F}_q[t]$. We conclude that $G_q(k) \leq n + u$, and so on recalling our upper bound on n , we find that

$$G_q(k) < (k \log k - \frac{1}{2} \log k + 3) + (k_p + 1).$$

This completes the proof of Corollary 2.

4. Methods applicable for smaller q . The upper bound presented in Theorem 3 may be established cheaply by making use of our recent work [7] concerning the restricted variant of Waring's problem. The argument is familiar, but we provide details for the

sake of completeness. Observe first that when the characteristic of \mathbb{F}_q divides k , one has $w_q(k) = w_q(k_0)$, in which k_0 is the largest divisor of k coprime to q . It therefore suffices to bound $w_q(k)$ for $(k, q) = 1$, as we henceforth assume. Suppose that $m \in \mathbb{J}_q^k[t]$, so that m is the sum of some number of k th powers from $\mathbb{F}_q[t]$. Let x_0 be an element of $\mathbb{F}_q[t]$ of degree sufficiently large in the context of the methods of [7], and consider the polynomial $m_0 = m - x_0^k$. In accordance with our opening observation in the final paragraph of §3, one has $m_0 \in \mathbb{J}_q^k[t]$. Let C_0 be a suitable positive absolute constant, and write $v = [\widehat{G}_q(k) + C_0 k \sqrt{\text{Log Log } k / \text{Log } k}]$. Then since m_0 has sufficiently large degree, the conclusion of Theorem 1.1 of [7] ensures that m_0 is the sum of at most v k th powers from $\mathbb{F}_q[t]$, say $m_0 = x_1^k + \cdots + x_v^k$. But then one has $m = x_0^k + x_1^k + \cdots + x_v^k$, whence m is the sum of at most $v + 1$ k th powers from $\mathbb{F}_q[t]$. This completes the proof of Theorem 3.

We remark that the methods of §§2–14 of [7] may be used to count the number of solutions of the equation $m = x_1^k + \cdots + x_u^k$, with $x_i \in \mathbb{F}_q[t]$ of degree B sufficiently large in terms of k ($1 \leq i \leq u$). When u is at least as large as the integer v above, for a suitable absolute constant C_0 , an asymptotic lower bound for the number of solutions may be obtained which confirms that m has infinitely many representations as the sum of u k th powers whenever $m \in \mathbb{J}_q^k[t]$. In some sense, therefore, the additional k th power employed in the first paragraph is redundant, and may be eliminated in a more refined analysis of this problem.

REFERENCES

1. T. Chinburg, “Easier” Waring problems for commutative rings, *Acta Arith.* **35** (1979), 303–331.
2. P. Deligne, *La conjecture de Weil. I*, *Inst. Hautes Études Sci. Publ. Math.* **43** (1974), 273–307.
3. L. Gallardo and L. Vaserstein, *The strict Waring problem for polynomial rings* (preprint).
4. S. R. Ghorpade and G. Lachaud, *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields*, *Mosc. Math. J.* **2** (2002), 589–631.
5. R. M. Kubota, *Waring’s problem for $\mathbb{F}_q[x]$* , Ph. D. Thesis, University of Michigan, Ann Arbor, 1971.
6. R. M. Kubota, *Waring’s problem for $\mathbb{F}_q[x]$* , *Dissertationes Math. (Rozprawy Mat.)* **117** (1974), 60pp.
7. Y.-R. Liu and T. D. Wooley, *Waring’s problem in function fields* (submitted).
8. R. E. A. C. Paley, *Theorems on polynomials in a Galois field*, *Quart. J. Math.* **4** (1933), 52–63.
9. W. M. Schmidt, *A lower bound for the number of solutions of equations over finite fields*, *J. Number Theory* **6** (1974), 448–480.
10. L. N. Vaserstein, *Waring’s problem for algebras over fields*, *J. Number Theory* **26** (1987), 286–298.
11. L. N. Vaserstein, *Waring’s problem for commutative rings*, *J. Number Theory* **26** (1987), 299–307.
12. L. N. Vaserstein, *Ramsey’s theorem and Waring’s problem for algebras over fields*, *The arithmetic of function fields* (Columbus, OH, 1991), Ohio State Univ. Math. Res. Inst. Publ. 2, de Gruyter, Berlin, 1992, pp. 435–441.
13. A. Weil, *Numbers of solutions of equations in finite fields*, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.

YU-RU LIU: DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF WATERLOO, WATERLOO, ON, CANADA N2L 3G1

E-mail address: yrliu@math.uwaterloo.ca

TREVOR D. WOOLEY: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, 2074 EAST HALL, 530 CHURCH STREET, ANN ARBOR, MI 48109-1043, U.S.A.

E-mail address: wooley@umich.edu