CONCENTRATION OF POINTS ON CURVES IN FINITE FIELDS

JAVIER CILLERUELO AND IGOR SHPARLINSKI

ABSTRACT. We obtain analogues of several recent bounds on the number of solutions of polynomial congruences modulo a prime with variables in short intervals in the case of polynomial equations in high degree extensions of finite fields. In these settings low-dimensional affine spaces play the role of short intervals and thus several new ideas are required.

1. INTRODUCTION

Recently there has been a series of results that give upper bounds on the number of solutions of polynomial s-variate congruences modulo a prime p that are contained in s-dimensional cubes of the form

$$[K_1 + 1, K_1 + M] \times \ldots \times [K_s + 1, K_s + M]$$

with a side length M that is small compared to p (so standard methods based on bounds of exponential sums do not apply), see [3, 4, 5, 6, 7, 8] and references therein.

Here we formulate and investigate several similar problems in the somewhat dual setting of finite fields that are large degree extensions of some small field. Note that many of the tools applicable in the case of congruences modulo p do not work or even exist in the case of general finite fields. For example, such important technical tools as analogues of the results of Bombieri and Pila [2] and Wooley [12, 13], do not exist in the settings of this work (more precisely, in the settings of function fields). So we use some alternative approaches.

Let $\mathbb{F}_q$ be a finite field of q elements and let $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ be an extension of $\mathbb{F}_q$ of degree n obtained by adjoining a root α of an irreducible polynomial ψ of degree n over $\mathbb{F}_q$.

In extension fields $\mathbb{F}_q$, instead of intervals, we consider the following linear subspaces

$$V_m = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \ : \ a_i \in \mathbb{F}_q, \ i = 0, \ldots, m-1\}, \quad 1 \le m \le n.$$

Here, for various polynomials $F(X, Y) \in \mathbb{F}_{q^n}$ we obtain non-trivial upper bounds for number of solutions to the equation

$$F(x, y) = 0, \qquad (x, y) \in P_0 + V_m \times V_m,$$

2010 *Mathematics Subject Classification.* 11D45, 11T06.

Key words and phrases. Finite fields, polynomials, rational points on curves.

for an arbitrary fixed point $P_0 = (x_0, y_0) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ and also of some related equations.

Although our argument can be made uniform with respect to all parameters, to simplify the exposition and results, we always assume that q is fixed, while $m \to \infty$. In particular, the implied constants in the symbols 'O' and '$\ll$' may depend on q and $d = \deg F$, but are uniform with respect to m and n (as usual, $U = O(V)$ and $U \ll V$ mean that $|U| \le cV$ with some constant $c > 0$).

Throughout the paper, for $z > 0$ we define $\log z$ as $\log z = \max\{\ln z, 1\}$, where $\ln z$ is the natural logarithm of z.

2. Polynomial Divisor Function

The following estimate is one of our principal tool. It is a polynomial analogue of the well-known bound on the classical divisor function.

Lemma 1. *The number of divisors of a polynomial $f \in \mathbb{F}_q[T]$ of degree s is $q^{O(s/\log s)}$*

Proof. This has been proved in [11] for $q = 2$, the general case is completely analogous. □

3. General Curves

Here we consider points in small subspaces on reasonably general polynomial curves. Our next result is an analogue of [5, Theorem 5] and [7, Theorem 1].

Theorem 2. *Let $f \in \mathbb{F}_{q^n}[X]$ be a polynomial of degree d with $p > d \ge 2$, where p is the characteristic of $\mathbb{F}_{q^n}$. For any positive integer $\ell, m \le n$ and point $P_0 = (x_0, y_0) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$, the number of solutions to the equation*

$$f(x) = y, \qquad (x, y) \in P_0 + V_\ell \times V_m,$$

is bounded by $q^{\ell + O(\ell/\log \ell)} \left(q^{-\ell/2^{d-1}} + q^{-(d\ell - m)/2^{d-1}} + q^{-(n-m)/2^{d-1}} \right)$.

Proof. Making a change of variables, without lost of generality, we can assume that $P_0 = (0, 0)$. We also assume that f is exactly of degree d, that is, its leading coefficient $A_0 \ne 0$.

Let J be the number of solutions to the corresponding equation. We claim that for any $k = 0, 1, \ldots, d$ there is a polynomial

$$F_k(X, Z_1, \ldots, Z_k) \in \mathbb{F}_{q^n}[X, Z_1, \ldots, Z_k]$$

of the form

$$F_k(X, Z_1, \ldots, Z_k) = A_k X^{d-k} Z_1 \cdots Z_k + G_k(X, Z_1, \ldots, Z_k),$$

where $A_k \in \mathbb{F}_{q^n}^*$, $\deg_X G_k < d - k$, where we assign the degree -1 to the identically zero polynomial (thus G_d is the zero polynomial) and such that

$$J^{2^k} \le q^{\ell(2^k - k - 1)} R_k, \tag{1}$$

where R_k is the number of solutions to

$$F_k(x, z_1, \ldots, z_k) = y$$

with $(x, z_1, \ldots, z_k) \in V_\ell^{k+1}$, $y \in V_m$.

We prove (1) by induction on k.

Clearly (1) holds for $k = 0$ with $F_0(X) = f(X)$.

Now assume that (1) is correct for some $k < d$. For a set $\mathcal{S} \subseteq \mathbb{F}_{q^n}$ we denote by $\chi_{\mathcal{S}}$ the characteristic function of $\mathcal{S}$. We write

$$\begin{aligned} J^{2^{k+1}} &\le q^{\ell(2^{k+1}-2k-2)} R_k^2 \\ &= q^{\ell(2^{k+1}-2k-2)} \left(\sum_{x \in V_\ell} \sum_{z_1, \ldots, z_k \in V_\ell} \chi_{V_\ell} \left(F_k(x, z_1, \ldots, z_k) \right) \right)^2 . \end{aligned}$$

Thus, by the Cauchy inequality

$$J^{2^{k+1}} \le q^{\ell(2^{k+1}-k-2)} \sum_{z_1, \ldots, z_k \in V_\ell} \left(\sum_{x \in V_\ell} \chi_{V_\ell} \left(F_k(x, z_1, \ldots, z_k) \right) \right)^2 . \tag{2}$$

Furthermore

$$\begin{aligned} &\left(\sum_{x \in V_\ell} \chi_{V_\ell} \left(F_k(x, z_1, \ldots, z_k) \right) \right)^2 \\ &\quad = \sum_{x_1, x_2 \in V_\ell} \chi_{V_\ell} \left(F_k(x_1, z_1, \ldots, z_k) - F_k(x_2, z_1, \ldots, z_k) \right) \\ &\quad = \sum_{x \in V_\ell} \sum_{z_{k+1} \in V_\ell} \chi_{V_\ell} \left(F_k(x + z_{k+1}, z_1, \ldots, z_k) - F_k(x, z_1, \ldots, z_k) \right) . \end{aligned}$$

Recalling (2) we have

$$J^{2^{k+1}} \ll q^{\ell(2^{k+1}-k-2)} \sum_{x, z_1, \ldots, z_{k+1} \in V_\ell} \chi_{V_\ell} \left(F_{k+1}(x, z_1, \ldots, z_{k+1}) \right) , \tag{3}$$

where

$$\begin{aligned} F_{k+1}(X, Z_1, \ldots, Z_{k+1}) &= F_k(X + Z_{k+1}, Z_1, \ldots, Z_k) - F_k(X, Z_1, \ldots, Z_k) \\ &= A_k(d-k) X^{d-(k+1)} Z_1 \ldots Z_{k+1} + G_{k+1}(X, Z_1, \ldots, Z_{k+1}) \end{aligned}$$

and

$$\begin{aligned} G_{k+1}(X, Z_1, \ldots, Z_{k+1}) = A_k \sum_{j=2}^{d-k} \binom{d-k}{j} X^{d-k-j} Z_{k+1}^j Z_1 \cdots Z_k \\ + G_k(X + Z_{k+1}, Z_1, \ldots, Z_k) - G_k(X, Z_1, \ldots, Z_k). \end{aligned}$$

Since $\deg_X G_k(X, Z_1, \ldots, Z_k) < d-k$, then $\deg_X G_{k+1}(X, Z_1, \ldots, Z_{k+1}) < d-k-1$ and we conclude the proof of (1).

We now notice that F_{d-1} is of the form

$$F_{d-1}(X, Z_1, \ldots, Z_{d-1}) = A_{d-1} X Z_1 \ldots Z_{d-1} + g_{d-1}(Z_1, \ldots, Z_{d-1})$$

where $g_{d-1}(Z_1, \ldots, Z_{d-1}) \in \mathbb{F}_{q^n}[Z_1, \ldots, Z_{d-1}]$ does not depend on X.

Thus R_{d-1} is the number of solutions to the equation

$$xz_1 \ldots z_{d-1} + A_{d-1}^{-1} g_{d-1} = y, \qquad y \in A_{d-1}^{-1} V_m,\ x, z_1, \ldots, z_{d-1} \in V_\ell \tag{4}$$

If for some fixed $z_1, \ldots, z_{d-1}$ there is a solution (x_1, y_1) to (4), then for any other solution (x_2, y_2) (corresponding to the same $z_1, \ldots, z_{d-1}$), we obtain

$$(x_1 - x_2) z_1 \ldots z_{d-1} = y_1 - y_2.$$

Clearly $y_1 - y_2 \in A_{d-1}^{-1} V_m$. Thus, denoting $z_d = x_1 - x_2$, we obtain

$$R_{d-1} \le q^{\ell(d-1)} + Q_d, \tag{5}$$

where Q_d is the number of solutions to the equation

$$z_1 \ldots z_d = y, \qquad y \in A_{d-1}^{-1} V_m,\ z_1, \ldots, z_d \in V_\ell. \tag{6}$$

Since $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[T]/\psi(T)$ for some irreducible polynomial $\psi(T) \in \mathbb{F}_q[T]$ of degree n such that $\psi(\alpha) = 0$, we can identify any element $u \in \mathbb{F}_{q^n}$ with the corresponding polynomial $u(T) \in \mathbb{F}_q[T]$ of degree $\deg u \le n-1$ and thus the equation (6) is equivalent to the following polynomial congruence

$$z_1 \ldots z_d \equiv y \pmod{\psi},$$

that in turn implies that

$$z_1 \ldots z_d = y + u\psi, \qquad \deg z_1, \ldots, \deg z_d \le \ell - 1,$$

for some polynomial $u \in \mathbb{F}_q[T]$ such that

$$\deg u\psi \le \deg z_1 + \ldots + \deg z_d \le d(\ell - 1)$$

(and the equation is considered in the rings $\mathbb{F}_q[T]$). Hence, we infer that $\deg u \le \max\{-1, d(\ell-1) - n\}$, where as before we assign the degree -1 to the identically zero polynomial.

Therefore, there are at most

$$q^{\max\{-1, d(\ell-1)-n\}+1} q^{m+1} \ll \left(1 + q^{d\ell - n}\right) q^m$$

possibilities for the polynomial $w = y + u\psi$ on the right hand side of (3).

If the polynomial $w(T)$ vanishes, then we obviously have at most $dq^{\ell(d-1)}$ possibilities for each solution $(z_1, \ldots z_d)$.

Otherwise, by Lemma 1 we get $q^{O(d\ell/\log(d\ell))} = q^{O(\ell/\log \ell)}$ possibilities, for each polynomial $z_1, \ldots, z_{d-1}$, after which z_d is uniquely defined. Therefore

$$\begin{aligned} Q_d &\ll q^{\ell(d-1)} + \left(1 + q^{d\ell - n}\right) q^{m + O(\ell/\log \ell)} \\ &\ll q^{\ell(d-1)} + q^{m + O(\ell/\log \ell)} + q^{d\ell + m - n + O(\ell/\log \ell)}. \end{aligned}$$

Hence, by (5),

$$R_{d-1} \ll q^{\ell(d-1)} + q^{m+O(\ell/\log \ell)} + q^{d\ell+m-n+O(\ell/\log \ell)},$$

and using (1) with $k = d-1$ we conclude the proof. □

We remark that Theorem 2 is nontrivial only if $m < d\ell$, which is a rather natural condition. In fact the example of the polynomial $f(X) = X^d$ shows that such a condition is necessary.

Furthermore, we see that for a quadratic polynomial $f \in \mathbb{F}_{q^n}[X]$ and $\ell = m \le n/2$ the bound takes form $q^{m/2+o(m)}$, which is actually tight.

Remark 3. *We are grateful to the referee for the observation that the Lagrange interpolation can be used to show that the number of solutions to $y = f(x)$, $(x, y) \in V_m \times V_m$ is bounded by $q^{m/2+o(m)}$ (that is, exactly of the same shape as for $d = 2$) for any polynomial $f \in \mathbb{F}_{q^n}[X]$ of degree $d \ge 2$, provided that $m < 2n/(d^2+d+2)$. On the other hand, one perhaps may expect the bound $q^{m/d+o(m)}$.*

4. Hyperbolas

Here we consider several special curves for which we obtain improvements of the general estimate of Theorem 2.

For example, we have the following analogue of [6, Theorem 1].

Theorem 4. *For any positive integer $m \le n$, point $P_0 = (x_0, y_0) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$, and $\lambda \in \mathbb{F}_{q^n}^*$, the number of solutions of the equation*

$$xy = \lambda, \qquad (x, y) \in P_0 + V_m \times V_m,$$

is bounded by

(i) $\left(1 + q^{(4m-n)/3}\right) q^{O(m/\log m)}$ *for arbitrary x_0, y_0;*
(ii) $\left(1 + q^{(3m-n)/2}\right) q^{O(m/\log m)}$ *for $x_0 = y_0$.*

Proof. First we consider the case of arbitrary x_0, y_0. After a change of variable we have an equivalent equation

$$xy + ax + by = c, \qquad x, y \in V_m \tag{7}$$

for some $a, b, c \in \mathbb{F}_{q^n}$. For any non-negative $s \le n-1$ we can write

$$\mathbb{F}_{q^n} \times \mathbb{F}_{q^n} = \{(u, v) + \alpha^{n-s}(w, z) \ : \ u, v \in V_{n-s},\ w, z \in V_s\}.$$

For each nonzero $t \in V_{2s+1}$ we write $(ta, tb) = (u_t, v_t) + \alpha^{n-s}(w_t, z_t)$ with $u_t, v_t \in V_{n-s}$ and $w_t, z_t \in V_s$. By the Dirichlet principle, there is a nonzero $t \in V_{2s+1}$ such that $(w_t, z_t) = (0, 0)$, so $at = u_0$, $bt = v_0$ for some $u_0, v_0 \in V_{n-s}$. Clearly, the equation (7) is equivalent to the equation

$$txy + u_0 x + v_0 y = w_0 \tag{8}$$

for some $w_0 \in \mathbb{F}_{q^n}$.

Again, we write $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[T]/\psi(T)$ for some irreducible polynomial $\psi(T) \in \mathbb{F}_q[T]$ of degree n such that $\psi(\alpha) = 0$, we can identify the elements of $\mathbb{F}_{q^n}$ with the corresponding polynomials in $\mathbb{F}_q[T]$ and the equation (8) is equivalent to the following equation in $\mathbb{F}_q[T]$:

$$t(T)x(T)y(T) + u_0(T)x(T) + v_0(T)y(T) - w_0(T) = z(T)\psi(T), \quad \deg x,\ \deg y \le m-1. \tag{9}$$

We observe that $\deg u_0, \deg v_0 \le n-s-1$ and $\deg t \le 2s$. Thus,

$$\begin{aligned} \deg z\psi &\le \max\{\deg txy, \deg u_0 x, \deg v_0 y, \deg w_0\} \\ &\le \max\{2s+2m-2, n+m-s-2, n-1\}. \end{aligned}$$

Then, either $z = 0$ or

$$\deg z \le \max\{2s+2m-n-2, m-s-2\}. \tag{10}$$

Multiplying (9) by t, we obtain an equivalent the equation (over $\mathbb{F}_q[T]$):

$$(tx+v_0)(ty+u_0) = \mu_z, \tag{11}$$

where $\mu_z = t(z\psi + w_0) + u_0 v_0$. Next, we give an upper bound for the number of solutions of (11) for each $z \in \mathbb{F}_q[T]$.

Clearly there are $O(1)$ solutions to $xy = \lambda$ with $(tx+v_0)(ty+u_0) = 0$.

We now always assume that $\mu_z \neq 0$ distingue two cases:

Case 1: $m \le n/4$. In this case we take $s = m$ and then $z = 0$. If $\deg \mu_0 \le 18m$ the number of solutions of (11) is bounded by the numbers of divisors of μ_0, which is $q^{O(m/\log m)}$. If $\deg \mu_0 > 18m$ we claim that (11) has, at most four solutions. Suppose that we have five solutions, say $(x_1, y_1), \ldots, (x_5, y_5)$. Renumbering the variables, can assume that either

$$\deg(tx_i + v_0) \ge \frac{1}{2}\deg \mu_0, \qquad i = 1,2,3. \tag{12}$$

or

$$\deg(ty_i + u_0) \ge \frac{1}{2}\deg \mu_0, \qquad i = 1,2,3. \tag{13}$$

We consider only the case (12) and the case (13) is completely analogous.

Since for $i = 1,2,3$, the polynomial $tx_i + u_0$ divides μ_0, it is clear that

$$\operatorname{lcm}[tx_1 + v_0, tx_2 + v_0, tx_3 + v_0] \mid \mu_0 \tag{14}$$

On the other hand,

$$\begin{aligned} &\operatorname{lcm}[tx_1 + v_0, tx_2 + v_0, tx_3 + v_0] \\ &\qquad = \frac{\prod_{1\le i\le 3}(tx_i + v_0)}{\prod_{1\le i<j\le 3}\gcd(tx_i + v_0, tx_j + v_0)} \cdot \gcd(tx_1 + v_0, tx_2 + v_0, tx_3 + v_0). \end{aligned}$$

We observe that if $r \mid (tx_i + v_0)$ and $r \mid (tx_j + v_0)$ then $r \mid t(x_i - x_j)$. Thus

$$\deg(tx_i + v_0, tx_j + v_0) \le m + 2s - 1 = 3m - 1 < \frac{1}{6}\deg \mu_0 - 1$$

and we get

$$\begin{aligned}\deg \mu_0 &\geq \deg \operatorname{lcm}[tx_1+v_0, tx_2+v_0, tx_3+v_0]\\ &\geq \frac{3}{2}\deg \mu_0 - 3\left(\frac{1}{6}\deg \mu_0 - 1\right) = \deg \mu_0 + 3.\end{aligned}$$

Case 2: $m > n/4$. In this case we take $s = \lfloor (n-m)/3 \rfloor$. By (10) we have

$$\deg z \leq \frac{4m-n}{3}.$$

For each z, the number of solutions of (11) is bounded by the number of divisors of μ_z, which is bounded by $q^{O(n/\log n)} = q^{O(m/\log m)}$ since $m > n/4$.

Thus, then number of solutions of (9) is bounded by $\left(1 + q^{(4m-n)/3}\right) q^{O(m/\log m)}$ which implies the desired bound in case of arbitrary $x_0, y_0 \in \mathbb{F}_{q^n}$.

In the "diagonal" case $P_0 = (x_0, x_0) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ instead of (8) we obtain $txy + u_0 x + u_0 y = w_0$ for some $t \in V_{s+1}$ and $u_0 \in V_{n-s}$. Repeating the same argument as in the case of arbitrary x_0, y_0, we conclude the proof. □

In turn, Theorem 4 can be used to estimate the number of solutions to the equation

$$x = \vartheta^u, \qquad x = x_0 + V_m,\ u \in [u_0, u_0 + M],$$

for $x_0 \in \mathbb{F}_{q^n}$ and some integers m, M and u_0, see [4, 6] for analogous results for congruences modulo p. We do not present this result as one can probably obtain stronger bounds by using the method of [4].

We now have the following analogue of [1, Theorem 1].

Theorem 5. *For any positive integer $m \leq n$ and a point $W_0 = (x_0, y_0, u_0, v_0) \in \mathbb{F}_{q^n}^4$, the number of solutions in $\mathbb{F}_{q^n}$ of $xy = uv$ with $x, y, u, v \in W_0 + V_m^4$ is bounded by $20q(nq^{2m} + q^{4m-n})$.*

Proof. The desired number of solutions is

$$J = \#\{(x, y, u, v) \in W_0 + V_m^4 : xy = uv\}.$$

After removing the solutions of $xy = uv = 0$ we obtain

$$J \leq 4q^{2m} + \#\{(x, y, u, v) \in W_0 + V_m^4 : x/u = v/y \neq 0\}.$$

For $a, b \in \mathbb{F}_q$ now define the set $(a + V_m)/(b + V_m)$ as

$$\frac{a+V_m}{b+V_m} = \left\{\frac{a+r}{b+s} \in \mathbb{F}_{q^n}^* \ :\ r, s \in V_m\right\}$$

and put

$$\mathcal{U} = \left(\frac{x_0+V_m}{u_0+V_m}\right) \bigcap \left(\frac{v_0+V_m}{y_0+V_m}\right).$$

Then

$$J \leq 4q^{2m} + \sum_{\lambda \in \mathcal{U}} N_{x_0,u_0}(\lambda) N_{v_0,y_0}(\lambda),$$

where $N_{a,b}(\lambda)$ is the number of solutions $(x,u) \in (a,b)+V_m \times V_m$ of the equation $x/u = \lambda$ in $\mathbb{F}_{q^n}$. We observe that the Dirichlet principle implies that for any $\lambda \in \mathbb{F}_{q^n}$ there exist $r, s \in V_{\lfloor n/2 \rfloor +1}$ such that

- $r(T)$ is monic;
- $r(T)$ and $s(T)$ are relatively prime polynomials;
- $\lambda = r/s$.

We choose, for each λ a unique such pair r, s.

On the other hand we observe that $r/s \in \mathcal{U}$. Thus, the set $\mathcal{R}$ of chosen pairs (r,s) is of cardinality

$$\#\mathcal{R} \le \#\mathcal{U} \le q^{2m}. \tag{15}$$

We now write

$$J \le 4q^{2m} + \sum_{(r,s)\in\mathcal{R}} N_{x_0,u_0}(r/s) N_{v_0,y_0}(r/s). \tag{16}$$

We observe that, after a change of variables, $N_{x_0,u_0}(r/s)$ is the number of solutions of $ry - sx = c$ in $\mathbb{F}_{q^n}$ for a suitable $c \in \mathbb{F}_{q^n}$, with $x, y \in V_m$. As before, we assume that $\mathbb{F}_{q^n} \simeq \mathbb{F}_q[T]/\psi(T)$, where $\psi(T) \in \mathbb{F}_q[T]$ is the minimal polynomial of α and write the above equation as an equation in $\mathbb{F}_q[T]$:

$$r(T)y(T) - s(T)x(T) = c(T) + u(T)\psi(T). \tag{17}$$

Thus $N_{x_0,u_0}(r/s)$ equals the number of solutions $x, y, u \in \mathbb{F}_q[T]$ to (17) with $\deg x, \deg y \le m-1$. We write also $\mathcal{R}$ for the set of pairs of admissible polynomials (r,s) (rather than for the set of $\mathbb{F}_{q^n}$ elements, as in (16)).

Next we estimate $N_{x_0,u_0}(r/s)$ for $\deg s \le \deg r$. We observe that

$$\deg u\psi \le \max\{\deg ry, \deg sx, \deg c\} \le \max\{\deg r + m - 1, n-1\}.$$

Thus $\deg u \le \max\{m + \deg r - n - 1, -1\}$.

For each u we consider a solution (x_u, y_u) (in the case it has it). Thus, any solutions to (17) is of the form $(x,y) = (x_u + rt, y_u + st)$ with $t \in \mathbb{F}_{q^n}[T]$, and since $\deg x, \deg y \le m-1$ we have that $\deg t \le m - 1 - \deg r$. Thus

$$\begin{aligned} N_{x_0,u_0}(r/s) &\le \sum_{\substack{u\in\mathbb{F}_q[T] \\ \deg u \le \max\{m+\deg r - n - 1, -1\}}} \left(1 + q^{m-\deg r}\right) \\ &\le \left(1 + q^{m-\deg r}\right)\left(1 + q^{m-n+\deg r}\right). \end{aligned}$$

Similarly, for $\deg r \le \deg s$ we have

$$N_{x_0,u_0}(r/s) \le \left(1 + q^{m-\deg s}\right)\left(1 + q^{m-n+\deg s}\right).$$

Since this estimate does not depend on (x_0, u_0) and since the case $\deg r \leq \deg s$ can be studied similarly, we see from (16) that

$$\begin{aligned} J &\leq 4q^{2m} + 2 \sum_{\substack{(r,s)\in\mathcal{R} \\ \deg s \leq \deg r \leq \lfloor n/2 \rfloor}} \left(1 + q^{m-\deg r}\right)^2 \left(1 + q^{m-n+\deg r}\right)^2 \\ &\leq 4q^{2m} + 8 \sum_{\substack{(r,s)\in\mathcal{R} \\ \deg s \leq \deg r \leq \lfloor n/2 \rfloor}} \left(1 + q^{2m-2\deg r}\right) \left(1 + q^{2m-2n+2\deg r}\right) \\ &\leq 4q^{2m} + 8 \sum_{\substack{(r,s)\in\mathcal{R} \\ \deg s \leq \deg r \leq \lfloor n/2 \rfloor}} \left(1 + q^{2m-2\deg r} + q^{2m-2n+2\deg r} + q^{4m-2n}\right) \\ &\leq 4q^{2m} + 8\#\mathcal{R}\left(1 + q^{2m-n}\right) + 8 \sum_{\substack{s,r\in\mathbb{F}_q[T] \\ r \text{ monic} \\ \deg s \leq \deg r \leq \lfloor n/2 \rfloor}} \left(q^{2m-2\deg r} + q^{4m-2n}\right). \end{aligned}$$

Using (15) we obtain

$$J \leq 12q^{2m} + 8q^{4m-n} + 8 \sum_{\substack{s,r\in\mathbb{F}_q[T] \\ r \text{ monic} \\ \deg s \leq \deg r \leq \lfloor n/2 \rfloor}} \left(q^{2m-2\deg r} + q^{4m-2n}\right). \tag{18}$$

Furthermore,

$$\begin{aligned} &\sum_{\substack{s,r\in\mathbb{F}_q[T] \\ r \text{ monic} \\ \deg s \leq \deg r \leq \lfloor n/2 \rfloor}} \left(q^{2m-2\deg r} + q^{4m-2n}\right) \\ &\qquad \leq \sum_{\substack{r\in\mathbb{F}_q[T] \\ r \text{ monic} \\ \deg r \leq \lfloor n/2 \rfloor}} \left(q^{2m-\deg r+1} + q^{4m-2n+\deg r+1}\right) \\ &\qquad \leq \sum_{d=0}^{\lfloor n/2 \rfloor} \sum_{\substack{r\in\mathbb{F}_q[T] \\ r \text{ monic} \\ \deg r = d}} \left(q^{2m-d+1} + q^{4m-2n+d+1}\right) \\ &\qquad \leq \sum_{d=0}^{\lfloor n/2 \rfloor} \left(q^{2m+1} + q^{4m-2n+2d+1}\right) \leq \left(\lfloor n/2 \rfloor + 1\right) q^{2m+1} + 2q^{4m-n+1}. \end{aligned}$$

Recalling (18), we derive

$$\begin{aligned} J &\leq 12q^{2m} + 8q^{4m-n} + 8\left(\left(\lfloor n/2 \rfloor + 1\right) q^{2m+1} + 2q^{4m-n+1}\right) \\ &\leq 6q^{2m+1} + 4q^{4m-n+1} + 8\left(\left(\lfloor n/2 \rfloor + 1\right) q^{2m+1} + 2q^{4m-n+1}\right) \\ &\leq 18nq^{2m+1} + 20q^{4m-n+1}, \end{aligned}$$

which concludes the proof. □

Certainly the constant in the bound of Theorem 5 can easily be improved.

We now derive an analogue of the estimates of the 4th moment of character sums from [1, 9, 10]. In fact in the case of finite fields this bound is more explicit and precise.

Corollary 6. *For any positive integer $m \le n$ and an element $x_0 \in \mathbb{F}_{q^n}$ we have*

$$\sum_{\chi} \left| \sum_{x \in x_0 + V_m} \chi(x) \right|^4 \le 20q(nq^{2m+n} + q^{4m}),$$

where χ runs through all multiplicative characters of $\mathbb{F}_{q^n}$.

From Corollary 6 we immediately obtain the following analogue of [8, Theorem 5].

Theorem 7. *For any positive integers k, j, for any positive integer $m \le n$ and a point $W_0 = (x_0, y_0, u_0, v_0) \in \mathbb{F}_{q^n}^4$, the number of solutions in $\mathbb{F}_{q^n}$ of $x^k y^j = u^k v^j$ with $(x, y, u, v) \in W_0 + V_m^4$ is bounded by $40\sqrt{kj}q(nq^{2m} + q^{4m-n})$.*

Proof. The number of solutions of $x^k y^j = u^k v^j = 0$ with $(x, y, u, v) \in W_0 + V_m^4$ is, at most, $4q^{2m}$. Writing $T_{kj}(W_0, m)$ for the number of solutions of the equation $x^k y^j = u^k v^j,\ (x, y, u, v) \in W_0 + V_m^4,\ xyuv \ne 0$ we have

$$\begin{aligned} T_{kj}(W_0, m) &= \frac{1}{q^n - 1} \sum_{\substack{x \in x_0 + V_m \\ x \ne 0}} \sum_{\substack{y \in y_0 + V_m \\ y \ne 0}} \sum_{\substack{u \in u_0 + V_m \\ u \ne 0}} \sum_{\substack{v \in v_0 + V_m \\ v \ne 0}} \sum_{\chi} \chi(x^k y^j u^{-k} v^{-j}) \\ &= \frac{1}{q^n - 1} \sum_{\chi} \sum_{\substack{x \in x_0 + V_m \\ x \ne 0}} \chi^k(x) \sum_{\substack{y \in y_0 + V_m \\ y \ne 0}} \chi^j(y) \sum_{\substack{u \in u_0 + V_m \\ u \ne 0}} \overline{\chi}^k(u) \sum_{\substack{v \in v_0 + V_m \\ v \ne 0}} \overline{\chi}^j(v). \end{aligned}$$

Using Hölder inequality, we obtain

$$\begin{aligned} T_{kj}^4(W_0, m) \le \frac{1}{(q^n - 1)^4} &\sum_{\chi} \left| \sum_{x \in x_0 + V_m} \chi^k(x) \right|^4 \cdot \sum_{\chi} \left| \sum_{y \in y_0 + V_m} \chi^j(y) \right|^4 \\ &\cdot \sum_{\chi} \left| \sum_{u \in u_0 + V_m} \chi^k(u) \right|^4 \cdot \sum_{\chi} \left| \sum_{v \in v_0 + V_m} \chi^j(v) \right|^4. \end{aligned} \tag{19}$$

We observe that there exist, at most, k characters χ such that χ^k is a given character. Using this and Corollary 6, we obtain

$$\sum_{\chi} \left| \sum_{x \in x_0 + V_m} \chi^k(x) \right|^4 \le k \sum_{\chi} \left| \sum_{x \in x_0 + V_m} \chi(x) \right|^4 \le 20kq(nq^{2m+n} + q^{4m}).$$

Putting this estimate, and similar estimates for the other there sums, in (19) and using that $q^n - 1 \ge q^n/2$ we derive

$$T_{kj}(W_0, m) \le 40\sqrt{kj}q(nq^{2m} + q^{4m-n}).$$

Adding the solutions of $x^k y^j = u^k v^j = 0$ we get the desired estimate. □

5. Further Questions

Here we mention several possible directions for further study.

Problem 8. *Obtain an upper bound on the number of solutions to* $x^2 = \lambda y^3$ *with* $(x, y) \in P_0 + V_m \times V_m$ *for some point* $P_0 \in \mathbb{F}_{q^n}^2$.

As in [8] (see also [5]) we note that the equation of Problem 8 is related to studying the distribution of Weierstrass equations of isomorphic elliptic curves. The methods of [5, 8] are based on the bound of Bombieri and Pila [2, Theorem 4] for the number of integral points on plane algebraic curves. Obtaining an analogue of this bound in function is certainly of independent interest.

Problem 9. *Let* $K = \mathbb{F}_q(T)$ *and Let* $F(X, Y) \in K[X, Y]$ *be an absolutely irreducible polynomial of degree* d *over* K. *Obtain an upper bound on the number of solutions to the equations* $F(x, y) = 0$ *in polynomials* $x(T), y(T) \in \mathbb{F}_q[T]$ *of degree at most* n *(as* $n \to \infty$*).*

Motivated by some algorithmic applications, several congruences with products of variables from small intervals have been considered in [3, 4]. These questions are also of interest in extensions of finite fields and also have the same algorithmic implications as in [3].

Problem 10. *Obtain tight upper bounds on the number of solutions to symmetric and one-sided equations*

$$x_1 \dots x_\nu = y_1 \dots y_\nu \qquad \text{and} \qquad x_1 \dots x_\nu = \lambda,$$

where $\lambda \in \mathbb{F}_{q^n}$, *with variables* $(x_1, \dots, x_\nu) \in P_0 + V_m \times \dots \times V_m$ *and* $(y_1, \dots, y_\nu) \in Q_0 + V_m \times \dots \times V_m$.

Obtaining the analogues of other results of [3, 4] for high degree extensions of finite fields is of interest too.

Acknowledgement

The authors are very grateful to the referee for the careful reading on the manuscript and many useful comments that led to improvements of some the results of this work. In particular, the idea behind the bound of Remark 3 belongs to the referee.

This work started during a very pleasant visit by I. S. to the Universidad Autónoma de Madrid; the support and hospitality of this institution are gratefully acknowledged.

During the preparation of this paper, J. C. was supported by MICINN Grant MTM2011-22851 (Spain) and I. S. by ARC grant DP130100237 (Australia) and by NRF Grant CRP2-2007-03 (Singapore).

References

[1] A. Ayyad, T. Cochrane and Z. Zheng, 'The congruence $x_1x_2 \equiv x_3x_4 \pmod p$, the equation $x_1x_2 = x_3x_4$ and the mean value of character sums', *J. Number Theory*, **59** (1996), 398–413.

[2] E. Bombieri and J. Pila, 'The number of integral points on arcs and ovals', *Duke Math. J.*, **59** (1989), 337–357.

[3] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On the hidden shifted power problem', *SIAM J. Comp.*, **41** (2012), 1524–1557.

[4] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On congruences with products of variables from short intervals and applications', *Proc. Steklov Math. Inst.*, (to appear).

[5] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, 'Points on curves in small boxes and applications', *Preprint*, (available from `http://arxiv.org/abs/1111.1543`).

[6] J. Cilleruelo and M. Z. Garaev, 'Concentration of points on two and three dimensional modular hyperbolas and applications', *Geom. and Func. Anal.*, **21** (2011), 892–904.

[7] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, 'On the concentration of points of polynomial maps and applications', *Math. Zeit.*, **272** (2012) 825–837.

[8] J. Cilleruelo, I. E. Shparlinski and A. Zumalacárregui, 'Isomorphism classes of elliptic curves over a finite field in some thin families', *Math. Res. Letters*, **19** (2012), 335–343.

[9] T. Cochrane and S. Sih, 'The congruence $x_1x_2 \equiv x_3x_4 \pmod p$ and mean values of character sums', *J. Number Theory*, **130** (2010), 767–785.

[10] M. Z. Garaev and V. Garcia, 'The equation $x_1x_2 = x_3x_4 + \lambda$ in fields of prime order and applications', *J. Number Theory*, **128** (2008), 2520–2537.

[11] Ph. Piret, 'On the number of divisors of a polynomial over GF(2)', *Proc. AAECC-2*, Lecture Notes in Comp. Sci., vol. 228, 1986, 161–168.

[12] T. D. Wooley, 'Vinogradov's mean value theorem via efficient congruencing', *Ann. Math.*, **175** (2012), 1575–1627.

[13] T. D. Wooley, 'Vinogradov's mean value theorem via efficient congruencing, II', *Duke Math. J.* (to appear).

Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049, Madrid, España

E-mail address: `franciscojavier.cilleruelo@uam.es`

Department of Computing, Macquarie University, Sydney NSW 2109, Australia

E-mail address: `igor.shparlinski@mq.edu.au`