REMARKS ON THE VISIBILITY PROBLEM IN THE FUNCTION FIELD CASE

SUKUMAR DAS ADHIKARI AND FRANCESCO PAPPALARDI

ABSTRACT. We extend results of [1, 2, 3] on the visibility problem for lattice points in $\mathbb{Z}^d$ to the case of function fields over finite fields which are related to important questions regarding the corresponding q-Jacobsthal function.

RÉSUMÉ. Nous étendons résultats de [1, 2, 3] sur le probleme de la visibilité des points du réseau entier $\mathbb{Z}^d$ au cas des corps de fonctions sur un corps fini, en rapport avec la fonction de q-Jacobsthal.

1. INTRODUCTION

Denote by $\mathbb{F}_q[x]$ the ring of polynomials with coefficients in the fixed finite field $\mathbb{F}_q$. Furthermore for $n \in \mathbb{N}$ set

$$\Delta_n = \Delta_n(q) = \left\{(f,g) \in \mathbb{F}_q[x]^2, \text{ such that } \deg f \leq n \text{ and } \deg g \leq n\right\}.$$

Clearly $|\Delta_n| = q^{2(n+1)}$. Given distinct $P_1 = (f_1, g_1), P_2 = (f_2, g_2) \in \Delta_n$, as in the classical case, we say that P_1 is *visible* from P_2 if $(f_1 - f_2, g_1 - g_2) = 1$. This is equivalent to say that there are no elements of Δ_n in the line connecting P_1 and P_2. Similarly, if $S \subseteq \Delta_n$, we say that Δ_n is visible from S if for any $P \in \Delta_n$, there is $Q \in S$ such that P is visible from Q. We are interested in the following function:

$$\mathcal{F}_q(n) = \min\{|S|, S \subseteq \Delta_n, \Delta_n \text{ is visible from } S\}. \tag{1}$$

We will prove the following result which is analogous to [2, Theorem 1]:

Theorem 1. *Let q be fixed and let $\beta_q > 4q^2/(1-\alpha_q)^2$ (where $\alpha_q = \alpha_q^3$ is defined in part (2) Lemma 1) be any number. Then for all n large enough one can explicitly construct a subset $X_n(q)$ of Δ_n such that Δ_n is visible from $X_n(q)$ and*

$$|X_n(q)| \leq \beta_q \frac{n \log\log n}{\log_q n}.$$

Therefore, in particular $\mathcal{F}_q(n) \leq \beta_q \frac{n \log\log n}{\log_q n}$, for all n large enough.

It is natural to generalize the concept of visibility to the d–dimensional space. If we write $\Delta_n^d = \left\{(f_1, \dots, f_d) \in (\mathbb{F}_q[x])^d, \deg f_i \leq n\right\}$, then $|\Delta_n^d| = q^{d(n+1)}$. It is obvious what one means by saying that two points of Δ_n^d are visible from each other.

We will prove, as in the [3, Theorem 3], that Theorem 1 can be improved in the higher dimensional case:

Date: February 1, 2002.

1991 *Mathematics Subject Classification.* Primary 11T55; Secondary 11N37.

Key words and phrases. function fields, visibility, Jacobsthal's function.

Theorem 2. *Let q be fixed, $d \geq 3$ and let $\gamma_q > q/(1-\alpha_q^d)$ be any number. Then for all n large enough one can explicitly construct a subset $X_n^d(q)$ of Δ_n^d such that Δ_n^d is visible from $X_n^d(q)$ and $|X_n^d(q)| \leq \gamma_q \frac{n}{\log_q n}$. Therefore, if we define $\mathcal{F}_q^d(n)$ as the minimum number of elements in a subset of Δ_n^d, from which Δ_n^d is visible, we have for n large enough,*

$$\mathcal{F}_q^d(n) \leq \gamma_q \frac{n}{\log_q n}.$$

Further, let $\delta_q < \frac{1}{q}$ be any positive number. Then for all n large enough

$$\mathcal{F}_q^d(n) \geq \delta_q \frac{n}{\log_q n}.$$

We will need the following facts about distribution of polynomials in finite fields. The proofs can be found in the book of Lidl and Nieddereiter [10]. See also the book of Shparlinski [12]. The last statement can be found in [6]:

Lemma 1. *Let q be a fixed power of a fixed prime and denote by $\mathcal{I}(q)$ the set of monic irreducible polynomials in $\mathbb{F}_q[x]$, by $\mathcal{I}_k(q)$ the set of irreducible monic polynomials of degree k and by $I_k(q)$ the order $|\mathcal{I}_k(q)|$. Then*

1. $I_k(q) = \frac{1}{k}\left(q^k + O(q^{k/2})\right)$;
2. *If $d \geq 3$, the series $\alpha_q^d = \sum_{k=1}^{\infty} \frac{I_k(q)}{q^{(d-1)k}}$ converges to a number less than 1;*
3. $\sum_{k\leq m} \frac{I_k(q)}{q^k} = (1+o(1)) \log m$;
4. $\sum_{k\leq m} kI_k(q) = \frac{q}{q-1} q^m + O(q^{m/2})$.
5. *Let $m \in \mathbb{F}_q[x]$, and denote by $\omega_q(m)$ the number of distinct monic irreducible polynomials which divide m. If the degree of m is at most n, then if n is large enough, we have*
$$\omega_q(m) \leq \frac{n}{\log_q n - 3}. \square$$

Lemma 2. *Given $a, b \in \mathbb{F}_q[x]$, the number of polynomials with degree up to s which are congruent to a modulo b is at most $q^{s+1-\deg b} + 1$.* $\square$

2. Proof of the lower bound in Theorem 2

We follow the proof of Abbott [1]. Suppose $S \subset \Delta_n^d$ is visible from every point of Δ_n^d, assume that $|S| = r$ and $S = \{\underline{f}_1, \dots, \underline{f}_r\}$ where we write $\underline{f}_i = (f_{i1}, \dots, f_{id})$ $(i = 1, \dots, d)$. Let m be the least integer defined by the property that

$$\sum_{k\leq m} I_k(q) \geq r \qquad (2)$$

and let $p_1, \dots, p_r$ be monic irreducible polynomials with degree less or equal than m. Next consider polynomials $f_{01}, \dots f_{0d}$ which are respectively the solutions of the system of equations

$$\begin{cases} X \equiv f_{i1} \bmod p_i \\ i = 1, \dots, r \end{cases} \quad \dots \quad \text{and} \quad \begin{cases} X \equiv f_{id} \bmod p_i \\ i = 1, \dots, r \end{cases}$$

with the property that $\underline{f}_0 = (f_{01}, \dots f_{0d}) \notin S$. Indeed, by the chinese remainder theorem one can find such a solution with $\deg f_{0j} \leq ([\log_q r]+1) + \sum_{i\leq r} \deg p_i, j = 1, \dots, d$. In fact if $\underline{\tilde{f}}_0 = (\tilde{f}_{01}, \dots \tilde{f}_{0d})$ is a fundamental solutions and $P = p_1 \cdots p_r$, then the set of solutions $\{(\tilde{f}_{01} + hP, \dots, \tilde{f}_{0d} + hP) \mid \deg(h) \leq [\log_q r] + 1\}$ contains more then r elements therefore it contains one at least outside S. Now from part (4) Lemma 1 and from the inequality (2) above we deduce

$$\sum_{i\le r}\deg p_i \le \sum_{k\le m} kI_k(q) = (1+o(1))\frac{q}{q-1}q^m.$$

Furthermore $r \ge \sum_{k\le m-1} I_k(q) \ge \frac{1}{m-1}\sum_{k\le m-1} kI_k(q) = (1+o(1))\frac{q^{m+1}}{q(q-1)(m-1)}$ implies that $([\log_q r]+1)+\sum_{i\le r}\deg p_i \le (q+o(1))r\log_q r$. Therefore all $\deg f_{01},\dots,$ $\deg f_{0d}$ are less than or equal to $(q+o(1))\,r\log_q r$, which is smaller than n for $r \le (\frac{1}{q}+o(1))\frac{n}{\log_q n}$.

Finally if $r < \delta_q\frac{n}{\log_q n}$ and n is large enough, $\underline{f}_0 \in \Delta_n^d$. Therefore $r \ge \delta_q\frac{n}{\log_q n}$ and this completes the proof. □

3. Proof of Theorem 1

We will need the following:

Lemma 3. *Suppose that n is large enough, let $\beta > 0$ be any fixed number and let t be the least integer such that $q^{t+1} \ge \beta\log\log n$. Then for every given $f \in \Delta_n$ there exists $g \in \mathbb{F}_q[x]$ with $\deg g \le t$ such that*

$$\sum_{\substack{p\in\mathcal{I}(q)\\ p|f-g}}\frac{1}{q^{\deg p}} < \alpha_q + \frac{1}{\beta} + o(1). \tag{3}$$

Proof of Lemma 3. Consider the sum

$$\sum_{\substack{\deg g\le t\\ g\ne f}}\ \sum_{\substack{p\in\mathcal{I}(q)\\ p|f-g}}\frac{1}{q^{\deg p}}. \tag{4}$$

We split the sum in three sums Σ_1, Σ_2 and Σ_3 where Σ_1 counts the irreducibles p with $\deg p \le t$, the second counts those with $t < \deg p \le (\log n)\log\log n$ and the third counts those with $(\log n)\log\log n < \deg p \le n$.

$$\begin{aligned}\text{Now } \Sigma_1 &\le \sum_{\substack{p\in\mathcal{I}(q)\\ \deg p\le t}}\ \sum_{\substack{\deg g\le t\\ g\ne f, p|f-g}}\frac{1}{q^{\deg p}}\\ &\le \sum_{\substack{p\in\mathcal{I}(q)\\ \deg p\le t}}\frac{1}{q^{\deg p}}\left(\frac{q^{t+1}}{q^{\deg p}}+1\right) = \sum_{k\le t}\left(q^{t+1}\frac{I_k(q)}{q^{2k}}+\frac{I_k(q)}{q^k}\right)\end{aligned}$$

by Lemma 2 and from Lemma 1 we obtain

$$\Sigma_1 \le q^{t+1}(\alpha_q + o(1)) + (1+o(1))\log t) = q^{t+1}(\alpha_q+o(1)). \tag{5}$$

As for Σ_2, note that there are no irreducible dividing $f-g'$ and $f-g''$ with degree larger then t. Therefore, from part (3) of Lemma 1,

$$\Sigma_2 \le \sum_{\substack{p\in\mathcal{I}(q)\\ \deg p\le\log n\log\log n}}\frac{1}{q^{\deg p}} = (1+o(1))\log\log n. \tag{6}$$

Furthermore

$$\Sigma_3 \le \sum_{\substack{\deg g\le t\\ g\ne f}}\frac{1}{q^{\log n\log\log n}}\sum_{\substack{p\in\mathcal{I}(q)\\ p|f-g}}1 \ll \frac{q^{t+1}}{q^{\log n\log\log n}}\frac{n}{\log n} = o(1) \tag{7}$$

Finally by (5), (6) and (7) we deduce that the sum in (4) is

$$\leq q^{t+1}(\alpha_q + o(1)) + (\beta + o(1)) \log\log n + o(1) \leq q^{t+1}(\alpha_q + \frac{1}{\beta} + o(1)).$$

Hence, for some $g \in \mathbb{F}_q[x]$ with $\deg g < t$, (3) is satisfied. $\square$

We define the *q–Jacobsthal function* of $m \in \mathbb{F}_q[x]$ as follows

$$\mathcal{J}_q(m) = \min\{t \mid \forall a \in \mathbb{F}_q[x], \exists h \in \mathbb{F}_q[x], \deg h < t, \gcd(a+h, m) = 1\}. \tag{8}$$

It is immediate to see that $\mathcal{J}_q(m)$ is well defined and that $\mathcal{J}_q(m) < \deg m$. Indeed, for any $a \in \mathbb{F}_q[x]$, if r is the remainder of the division of $1-a$ by m, then it clear that $\deg r < \deg m$ and $\gcd(a + r, m) = 1$. We will need the following:

Lemma 4. *Suppose $m \in \mathbb{F}_q[x]$ and that $\gamma = \sum_{\substack{p\in\mathcal{I}(q)\\ p\mid m}} \frac{1}{q^{\deg p}} < 1$. Then for n large enough, $q^{\mathcal{J}_q(m)+1} \leq (1-\gamma)^{-1}\,\omega_q(m)$.*

Proof of Lemma 4. For any $a \in \mathbb{F}_q[x]$, consider the set $S = \{a + h \mid h \in \mathbb{F}_q[x], \deg h \leq k\}$. Then $|S| = q^{k+1}$. We want to estimate the size of the set

$$S_m = \{y \in S \mid \gcd(y, m) \neq 1\}.$$

Note that by Lemma 2

$$\begin{aligned} \#S_m &\leq \sum_{\substack{p\in\mathcal{I}(q)\\ p\mid m}} \#\{h \in \mathbb{F}_q[x] \mid \deg h < k, p|h+k\} \\ &\leq \sum_{\substack{p\in\mathcal{I}(q)\\ p\mid m}} \left(q^{k+1-\deg p} + 1\right) \leq q^{k+1}\gamma + \omega(m). \end{aligned}$$

which is smaller than q^{k+1} if $q^{k+1} > (1-\gamma)^{-1}\omega(m)$. Finally, there is an element of S not in S_m if k satisfies the above, so that

$$q^{\mathcal{J}_q(m)+1} \leq (1-\gamma)^{-1}\omega(m). \ \square$$

We are now ready to prove Theorem 1. Consider the set

$$X_n(q) = \{(f, g) \in \Delta_n, \deg f \leq t, \deg g \leq s\}$$

where t is the least integer such that $q^{t+1} > \frac{2}{1-\alpha_q}\log\log n$ and s is the least integer such that $q^{s+1} > (\frac{1-\alpha_q}{2} + \epsilon)\frac{n}{\log_q n - 3}$ where $\epsilon > 0$ is small and will be chosen later.

Then (if ϵ is small enough)

$$|X_n(q)| = q^{s+1}q^{t+1} \leq \beta_q \frac{n \log\log n}{\log_q n}.$$

We need to show that Δ_n is visible from X_n for n large enough. Indeed, for $(a, b) \in \Delta_n$, from Lemma 3 we know that there exists $g \in \mathbb{F}_q[x]$ with $\deg g \leq t$ such that $\sum_{\substack{p\in\mathcal{I}(q)\\ p\mid a-g}} \frac{1}{q^{\deg g}} \leq (\alpha_q + 1)/2 + o(1)$. Furthermore Lemma 4 implies that $q^{\mathcal{J}_q(a-g)+1} \leq (1-\alpha_q)/2 + o(1))\omega_q(a-g)$. Note that from the fifth part of Lemma 1, for n large enough

$$\left(\frac{1-\alpha_q}{2} + o(1)\right)\omega_q(a-g) \leq \left(\frac{1-\alpha_q}{2} + \epsilon\right)\frac{n}{\log_q n} \leq q^{s+1}.$$

Therefore $\mathcal{J}_q(a-g) \leq s$ and this implies that there exists $h \in \mathbb{F}_q[x]$ with $\deg h \leq s$ such that $\gcd(a-g, b-h) = 1$. So, (a, b) and (f, h) are visible from each other and this concludes that proof. $\square$

4. Proof of the upper bound in Theorem 2

In this section we follow the method of [3] to investigate the concept of visibility in higher dimensional space. For $d \geq 3$, consider the set

$$X_n^d = \left\{(g_1, \dots, g_{d-1}, g_d) \in (\mathbb{F}_q[x])^d, \deg g_i \leq s \text{ for } i < d \text{ and } \deg g_d = 0\right\}.$$

Clearly $|X_n^d| = q^{(d-1)*(s+1)+1}$.

We want to show that for a suitable choice of s, Δ_n^d is visible from X_n^d. Clearly all the elements of Δ_n^d which have a degree 0 polynomial in the last coordinate are visible from X_n^d. Therefore fix $(f_1, \dots, f_d) \in \Delta_n^d$ such that $\deg f_d \geq 1$. We want to estimate the size of the set

$$\mathcal{A} = \left\{(g_1, \dots, g_{d-1}, g_d) \in X_n^d, \deg((f_1 - g_1, f_2 - g_2, \dots, f_d - g_d)) \geq 1\right\}.$$

First of all, we observe that

$$\begin{aligned} |\mathcal{A}| &\leq \sum_{\substack{g_1,\dots,g_{d-1} \\ \deg g_i \leq s,\ g_d \in \mathbb{F}_q}} \sum_{\substack{p \in \mathcal{I}(q) \\ p \mid \gcd(f_1-g_1, f_2-g_2, \dots, f_d-g_d)}} 1 \\ &= \sum_{g_d \in \mathbb{F}_q} \sum_{\substack{p \in \mathcal{I}(q) \\ p \mid f_d - g_d}} \sum_{\substack{g_1,\dots,g_{d-1} \\ \deg g_i \leq s, p \mid (f_i - g_i)}} 1 = \sum_{g_d \in \mathbb{F}_q} \sum_{\substack{p \in \mathcal{I}(q) \\ p \mid f_d - g_d}} \prod_{i=1}^{d-1} \left(\sum_{\deg g_i \leq s, p \mid (f_i - g_i)} 1 \right). \end{aligned}$$

From Lemma 2 we deduce that

$$|\mathcal{A}| \leq \sum_{g_d \in \mathbb{F}_q} \sum_{\substack{p \in \mathcal{I}(q) \\ p \mid f_d - g_d}} \left(1 + \frac{q^{s+1}}{q^{\deg p}}\right)^{d-1}.$$

Now we have

$$\begin{aligned} |\mathcal{A}| &\leq \sum_{g_d \in \mathbb{F}_q} \sum_{\substack{p \in \mathcal{I}(q) \\ p \mid f_d - g_d}} \sum_{j=0}^{d-1} \binom{d-1}{j} \left(\frac{q^{s+1}}{q^{\deg p}}\right)^j \\ &\leq \sum_{g_d \in \mathbb{F}_q} \sum_{\substack{p \in \mathcal{I}(q) \\ p \mid f_d - g_d}} 1 + \sum_{\substack{p \in \mathcal{I}(q) \\ \deg(p) \leq n}} \sum_{j=1}^{d-2} \binom{d-1}{j} \left(\frac{q^{s+1}}{q^{\deg p}}\right)^j + |X_n^d| \sum_{p \in \mathcal{I}(q)} \frac{1}{q^{(d-1)\deg p}}. \end{aligned}$$

We evaluate each of the three terms separately. For the last one, we have to use part (2) of Lemma 1. For the middle one just uses part (3) of Lemma 1 observing that

$$\begin{aligned} \sum_{\substack{p \in \mathcal{I}(q) \\ \deg(p) \leq n}} \sum_{j=1}^{d-2} \binom{d-1}{j} \left(\frac{q^{s+1}}{q^{\deg p}}\right)^j &\leq 2^{d-1} q^{(s+1)(d-2)} \sum_{\substack{p \in \mathcal{I}(q) \\ \deg(p) \leq n}} \frac{1}{q^{\deg p}} \\ \leq 2^{d-1} q^{(s+1)(d-2)} \sum_{j \leq n} \frac{I_j(q)}{q^j} &\leq (1 + o(1)) 2^{d-1} \left(\frac{|X_n^d|}{q}\right)^{(d-2)/(d-1)} \log n, \end{aligned}$$

and for the first sum we use the fifth part of Lemma 1. Putting all these together we obtain:

$$|\mathcal{A}| \leq q \frac{n}{\log_q n - 3} + \alpha_q^d |X_n^d| + (1 + o(1)) \log n \left(\frac{|X_n^d|}{q}\right)^{(d-2)/(d-1)}$$

Finally, in order to have $|\mathcal{A}| < |X_n^d|$ for n large enough, it is enough to choose s in such a way that $(1-\alpha_q^d)|X_n^d| > q^{\frac{n}{\log_q n - 3}}$. and this gives the claim. □

5. Final remarks. The order of the q-Jacobsthal function.

The classical Jacobsthal function has been investigated in [4, 7, 8, 9, 13, 14]. We have already defined in (8) the natural analogue of the Jacobsthal function for $\mathbb{F}_q[x]$. If we set

$$Y_n = \left\{ (0,h) \in \Delta_n, \deg h \leq \max_{g\in\mathbb{F}_q[x], \deg g \leq n} \mathcal{J}_q(g) \right\},$$

then clearly Δ_n is visible from Y_n as for every $(f,g) \in \Delta_n$ there is an $h \in Y_n$ (also $-h \in Y_n$) and $\gcd(f, g-h) = 1$ so that (f,g) is visible from $(0,h)$.

It is conjectured (see [11]) that for any $m \in \mathbb{F}_q[x]$, $\mathcal{J}_q(m) \leq \log_q \deg m$. This would imply that $\mathcal{F}_q(n) \leq n$. which is weaker than the upper bound in Theorem 1.

Acknowledgements. The major part of the work had been done when the second author was visiting Harish-Chandra Research Institute, Allahabad, India. The work was completed when the first author came to Università Roma Tre. They are thankful to these institutes for hospitality. The authors would also like to thank Igor Shparlinski for some useful suggestions.

References

[1] H. L. Abbott, *Some results in combinatorial Geometry.* Discrete Math. **9** (1974), 199–204.
[2] S. D. Adhikari and R. Balasubramanian, *On a question regarding visibility of lattice points.* Mathematika **43** (1996), no. 1, 155–158.
[3] S. D. Adhikari and Y.-G. Chen, *On a question regarding visibility of lattice points. II.* Acta Arith. **89** (1999), no. 3, 279–282.
[4] P. Erdős,*On the integers relatively prime to n and on a number-theoretic function considered by Jacobsthal*, Math. Scand. **10** (1962), 163–170.
[5] P. Erdös, P. M. Gruber and J. Hammer, *Lattice points*, Longman Sci. Tech., Harlow, 1989.
[6] M. Kaminski M. and N. M. Bshouty, *Multiplicative complexity of polynomial multiplication over finite.* J. ACM, (1989), v. 36, 150–170.
[7] H. Iwaniec, *On the error term in the linear sieve.* Acta Arith. **19** (1971), 1–30.
[8] H. Iwaniec,*On the problem of Jacobsthal.* Demonstratio Math. **11** (1978), no. 1, 225–231.
[9] H.-J. Kanold, *Über eine zahlentheoretische Funktion von Jacobsthal* Math. Ann. **156** (1964), 393–395.
[10] R. Lidl and H. Niederreiter, *Finite fields*, Second edition, Cambridge Univ. Press, 1997.
[11] T. Mulders and A. Storjohann, *The Modulo N Extended GCD Problem for Polynomials.* Proceedings of ISSAC'98, ACM Press, 1998, 105–112.
[12] I. E. Shparlinski, *Finite fields: theory and computation*, Kluwer Acad. Publ., 1999.
[13] H. Stevens,*On Jacobsthal's $g(n)$-function.* Math. Ann. **226** (1977), no. 1, 95–97.
[14] R. C. Vaughan,*On the order of magnitude of Jacobsthal's function.* Proc. Edinburgh Math. Soc. (2) **20** (1976/77), no. 4, 329–331.

(Adhikari) Harish-Chandra Research Institute, (Former Mehta Research Institute) Chhatnag Road, Jhusi, Allahabad 211 019, INDIA.
E-mail address, Adhikari: `adhikari@mri.ernet.in`

(Pappalardi) Dipartimento di Matematica, Università Roma TRE, Largo S. L. Murialdo 1, I–00146 Rome, ITALY
E-mail address, Pappalardi: `pappa@mat.uniroma3.it`