Journal of Combinatorial Theory, Series A 178 (2021) 105337

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

An analogue of Ruzsa's conjecture for polynomials over finite fields

Jason P. Bell [a], Khoa D. Nguyen [b,*]

[a] *University of Waterloo, Department of Pure Mathematics, Waterloo, Ontario, N2L 3G1, Canada*
[b] *Department of Mathematics and Statistics, University of Calgary, AB T2N 1N4, Canada*

ARTICLE INFO

Article history:
Received 12 January 2020
Received in revised form 3 September 2020
Accepted 15 September 2020
Available online xxxx

Keywords:
Ruzsa's conjecture
Polynomials over finite fields
The Polynomial Method

ABSTRACT

In 1971, Ruzsa conjectured that if $f : \mathbb{N} \to \mathbb{Z}$ with $f(n+k) \equiv f(n) \bmod k$ for every $n, k \in \mathbb{N}$ and $f(n) = O(\theta^n)$ with $\theta < e$ then f is a polynomial. In this paper, we investigate the analogous problem for the ring of polynomials over a finite field using the Polynomial Method in combinatorics.

1. Introduction

Let $\mathbb{N}$ denote the set of positive integers and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. A strong form of a conjecture by Ruzsa is the following assertion. Suppose that $f : \mathbb{N}_0 \to \mathbb{Z}$ satisfies the following 2 properties:

(P1) $f(n+p) \equiv f(n) \bmod p$ for every prime p and every $n \in \mathbb{N}_0$;
(P2) $\limsup_{n\to\infty} \dfrac{\log|f(n)|}{n} < e$.

* Corresponding author.
E-mail addresses: jpbell@uwaterloo.ca (J.P. Bell), dangkhoa.nguyen@ucalgary.ca (K.D. Nguyen).

https://doi.org/10.1016/j.jcta.2020.105337
0097-3165/

Then f is necessarily a polynomial. The original form allows the version of (P1) in which p is not necessarily a prime. Hall [11] gave an example constructed by Woodall showing that the upper bound e in (P2) is optimal. The reasoning behind this upper bound as well as the Hall-Woodall example is the (equivalent version of the) Prime Number Theorem stating that the product of primes up to n is $e^{n+o(n)}$ and the fact that the residue class of $f(n)$ modulo this product is determined uniquely by $f(0), \dots, f(n-1)$ thanks to (P1). In 1971, Hall [10] and Ruzsa [15] independently proved the following result.

Theorem 1.1 *(Hall-Ruzsa, 1971). Suppose that $f : \mathbb{N}_0 \to \mathbb{Z}$ satisfies (P1) and*

$$\limsup_{n\to\infty} \frac{\log|f(n)|}{n} < e - 1$$

then f is a polynomial.

The best upper bound was obtained in 1996 by Zannier [18] by extending earlier work of Perelli and Zannier [17,13]:

Theorem 1.2 *(Zannier, 1996). Suppose that $f : \mathbb{N}_0 \to \mathbb{Z}$ satisfies (P1) and*

$$\limsup_{n\to\infty} \frac{\log|f(n)|}{n} < e^{0.75}$$

then f is a polynomial.

In fact, the author remarked [18, pp. 400–401] that the explicit upper bound $e^{0.75}$ was chosen to avoid cumbersome formulas and it was possible to increase it slightly. The method of [18] uses the fact that the generating series $\sum f(n)x^n$ is D-finite over $\mathbb{Q}$ (i.e. it satisfies a linear differential equation with coefficients in $\mathbb{Q}(x)$) [13, Theorem 1.B] then applies deep results on the arithmetic of linear differential equations [4,6].

This paper is motivated by our recent work on D-finite series [3] and a review of Ruzsa's conjecture. From now on, let $\mathbb{F}$ be the finite field of order q and characteristic p, let $\mathcal{A} = \mathbb{F}[t]$, and let $\mathcal{K} = \mathbb{F}(t)$. We have the usual degree map $\deg : \mathcal{A} \to \mathbb{N}_0 \cup \{-\infty\}$. A map $f : \mathcal{A} \to \mathcal{A}$ is called a polynomial map if it is given by values on $\mathcal{A}$ of an element of $\mathcal{K}[X]$. For every $n \in \mathbb{N}_0$, let $\mathcal{A}_n = \{A \in \mathcal{A} : \deg(A) = n\}$, $\mathcal{A}_{<n} = \{A \in \mathcal{A} : \deg(A) < n\}$, and $\mathcal{A}_{\le n} = \{A \in \mathcal{A} : \deg(A) \le n\}$. Let $\mathcal{P} \subset \mathcal{A}$ be the set of irreducible polynomials; the sets $\mathcal{P}_n$, $\mathcal{P}_{<n}$, and $\mathcal{P}_{\le n}$ are defined similarly. The superscript $+$ is used to denote the subset consisting of all the monic polynomials, for example $\mathcal{A}^+$, $\mathcal{A}_n^+$, $\mathcal{P}_{\le n}^+$, etc. From the well-known identity [14, pp. 8]:

$$\prod_{d|n} \prod_{P\in\mathcal{P}_d^+} P = t^{q^n} - t$$

we have

$$q^n \le \deg\left(\prod_{P\in\mathcal{P}^+_{\le n}} P\right) < 2q^n \tag{1}$$

for every $n \in \mathbb{N}$. In view of the reasoning behind Ruzsa's conjecture, it is natural to ask the following:

Question 1.3. *Let $f:\ \mathcal{A}\to\mathcal{A}$ satisfy the following 2 properties:*

(P3) $f(A+BP)\equiv f(A) \bmod P$ *for every* $A, B\in\mathcal{A}$ *and* $P\in\mathcal{P}$;
(P4) $\limsup\limits_{\deg(A)\to\infty} \dfrac{\log\deg(f(A))}{\deg(A)} < q$.

Is it true that f is a polynomial map?

Note that (P3) should be the appropriate analogue of (P1): over the natural numbers, iterating (P1) yields $f(n+bp)\equiv f(n) \bmod p$ for every $n, b\in\mathbb{N}_0$ and prime p. On the other hand, over $\mathcal{A}$, due to the presence of characteristic p, iterating the congruence condition $f(A+P)\equiv f(A) \bmod P$ for $A\in\mathcal{A}$ and $P\in\mathcal{P}$ is not enough to yield (P3). By the following example that is similar to the one by Hall-Woodall, we have that the upper bound q in (P4) cannot be increased. Fix a *total* order $\prec$ on $\mathcal{A}$ such that $A\prec B$ whenever $\deg(A)<\deg(B)$. We define $g:\ \mathcal{A}\to\mathcal{A}$ inductively. First, we assign arbitrary values of g at the constant polynomials. Let $n\in\mathbb{N}$, $B\in\mathcal{A}_n$, and assume that we have defined $g(A)$ for every $A\in\mathcal{A}$ with $A\prec B$ such that:

$$g(A)\equiv g(A_1) \bmod P \text{ for every } A, A_1\prec B \text{ and prime } P\mid (A-A_1).$$

For every $P\in\mathcal{P}^+_{\le n}$, let $R_P\in\mathcal{A}$ with $\deg(R_P)<\deg(P)$ such that $B\equiv R_P \bmod P$. By the Chinese Remainder Theorem, there exists a unique $R\in\mathcal{A}$ with $\deg(R)<\deg\left(\prod\limits_{P\in\mathcal{P}^+_{\le n}} P\right)$ such that $R\equiv f(R_P) \bmod P$ for every $P\in\mathcal{P}^+_{\le n}$. Then we define

$$g(B) := R + \prod_{P\in\mathcal{P}^+_{\le n}} P.$$

It is not hard to prove that g satisfies Property (P3) (with g in place of f) and for every $n\in\mathbb{N}$, $B\in\mathcal{A}_n$, we have $\deg(g(B))\in[q^n, 2q^n)$ by (1). This latter property implies that g cannot be a polynomial map.

Following Professor Ruzsa's suggestion, we have:

Definition 1.4. Property (P3) is called the prime congruence-preserving condition. A map $f:\ \mathcal{A}\to\mathcal{A}$ with this property is called a prime congruence-preserving map.

Our main result implies the affirmative answer to Question 1.3; in fact we can replace (P4) by the much weaker condition that $\deg(f(A))$ is not too small compared to $\frac{q^{\deg(A)}}{\deg(A)}$:

Theorem 1.5. *Let $f: \mathcal{A} \to \mathcal{A}$ be a prime congruence-preserving map such that*

$$\deg(f(A)) < \frac{q^{\deg(A)}}{27q\deg(A)} \text{ when } \deg(A) \text{ is sufficiently large.} \tag{2}$$

Then f is a polynomial map.

There is nothing special about the constant $1/(27q)$ in (2) and one can certainly improve it by optimizing the estimates in the proof. It is much more interesting to know if the function $q^{\deg(A)}/\deg(A)$ in (2) can be replaced by a larger function (see Section 4). There are significant differences between Ruzsa's conjecture and Question 1.3 despite the apparent similarities at first sight. Indeed none of the key techniques in the papers [13,18] seem to be applicable in our situation. Obviously, the crucial result used in [18] that the generating series $\sum f(n)x^n$ is D-finite has no counterpart here. The proof of the main result of [13] relies on a nontrivial linear recurrence relation of the form $c_d f(n+d) + \ldots + c_0 f(n) = 0$. Over the integers, such a relation will allow one to determine $f(n)$ for *every* $n \geq d$ once one knows $f(0), \ldots, f(n-1)$. On the other hand, for Question 1.3, while it seems possible to imitate the arguments in [13] to obtain a recurrence relation of the form $c_d f(A + B_d) + \ldots + c_0 f(A + B_0) = 0$ for $A \in \mathcal{A}$ with $d \in \mathbb{N}$ and $B_0, \ldots, B_d \in \mathcal{A}$, such a relation does not seem as helpful: when $\deg(A)$ is large, one cannot use the relation to relate $f(A)$ to the values of f at smaller degree polynomials. Finally, the technical trick of using the given congruence condition to obtain the vanishing on $[2M_0, (2+\epsilon)M_0]$ from the vanishing on $[0, M_0]$ (see [13, pp. 11–12] and [18, pp. 396–397]) does not seem applicable here.

The proof of Theorem 1.5 consists of 2 steps. The first step is to show that the points $(A, f(A))$ for $A \in \mathcal{A}$ belong to an algebraic plane curve over $\mathcal{K}$, then it follows that $\deg(f(A))$ can be bounded above by a linear function in $\deg(A)$. The second step, which might be of independent interest, treats the more general problem in which f is prime congruence-preserving and there exists a special sequence $(A_n)_{n\in\mathbb{N}_0}$ in $\mathcal{A}$ such that $\deg(f(A_n))$ is bounded above by a linear function in $\deg(A_n)$. Both steps rely on the construction of certain auxiliary polynomials; such a construction has played a fundamental role in diophantine approximation, transcendental number theory, and combinatorics. For examples in number theory, the readers are referred to [1,12] and the references therein. In combinatorics, the method of constructing polynomials vanishing at certain points has recently been called the *Polynomial Method* and is the subject of the book [9]. This method has produced surprisingly short and elegant solutions of certain combinatorial problems over finite fields [7,5,8].

Acknowledgments. We are grateful to Professor Imre Ruzsa for his interest and helpful suggestions. We wish to thank Dr. Carlo Pagano, Professor Umberto Zannier, and the

anonymous referee for the useful comments. J. B is partially supported by the NSERC Discovery Grant RGPIN-2016-03632. K. N. is partially supported by the NSERC Discovery Grant RGPIN-2018-03770, a start-up grant at UCalgary, and the CRC tier-2 research stipend 950-231716.

2. A nontrivial algebraic relation

We start with the following simple lemma:

Lemma 2.1. *Let $g : \mathcal{A} \to \mathcal{A}$ and assume that there exists $C_1 \in \mathbb{N}_0$ such that the following 3 properties hold:*

(a) $g(A + BP) \equiv g(A) \bmod P$ *for every* $A, B \in \mathcal{A}$ *and* $P \in \mathcal{P}$.
(b) $\deg(g(A)) \leq q^{\deg(A)} - 1$ *for every* $A \in \mathcal{A}$ *with* $\deg(A) > C_1$.
(c) $g(A) = 0$ *for every* $A \in \mathcal{A}_{\leq C_1}$.

Then g is identically 0.

Proof. Otherwise, assume there is $A \in \mathcal{A}$ of smallest degree such that $g(A) \neq 0$. We have $D := \deg(A) > C_1$. Since $g(B) = 0$ for every $B \in \mathcal{A}_{<D}$ and since for every monic irreducible polynomial P of degree at most D there is some C such that $A - CP$ has degree strictly less than D, we have

$$g(A) \equiv 0 \bmod \prod_{P \in \mathcal{P}^+_{\leq D}} P.$$

Since $\deg\left(\prod_{P \in \mathcal{P}^+_{\leq D}} P\right) \geq q^D$ and $\deg(g(A)) < q^D$, we must have $g(A) = 0$, a contradiction. □

Proposition 2.2. *Let $f : \mathcal{A} \to \mathcal{A}$ be as in Theorem 1.5. Then there exists a non-zero polynomial $Q(X, Y) \in \mathcal{A}[X, Y]$ such that $Q(A, f(A)) = 0$ for every $A \in \mathcal{A}$.*

Proof. Let $N \in \mathbb{N}$ such that $\deg(f(A)) < \dfrac{q^{\deg(A)}}{27q \deg(A)}$ for every $A \in \mathcal{A}$ with $\deg(A) \geq N$. Let $M \geq N$ be a large positive integer that will be specified later. Consider $Q(X, Y) \in \mathcal{A}[X, Y]$ of the form:

$$Q(X, Y) = \sum_{0 \leq i \leq q^M/3} \sum_{0 \leq j \leq q^M/(3M)} \sum_{0 \leq k \leq 9qM} c_{ijk} t^i X^j Y^k$$

where $c_{ijk} \in \mathbb{F}_q$. The number of unknowns c_{ijk} is greater than q^{2M+1}.

Put $g(A) = Q(A, f(A))$ for $A \in \mathcal{A}$ then g satisfies the congruence condition:

$$g(A + BP) \equiv g(A) \bmod P \text{ for every } A, B \in \mathcal{A} \text{ and } P \in \mathcal{P}. \tag{3}$$

We prove that with a sufficiently large choice of M, we have $\deg(g(A)) < q^M$ for every $A \in \mathcal{A}$ with $\deg(A) \leq M$. Suppose $\deg(A) \in [N, M]$ then we have:

$$\deg(g(A)) < \frac{q^M}{3} + \frac{q^M \deg(A)}{3M} + \frac{9qMq^{\deg(A)}}{27q \deg(A)} \leq q^M$$

since the function q^x/x is increasing on $[2, \infty)$. Now let C_2 be a positive number that is at least the maximum of $\deg(f(A))$ for $A \in \mathcal{A}_{<N}$. Hence for every $A \in \mathcal{A}_{<N}$, we have

$$\deg(g(A)) \leq \frac{q^M}{3} + \frac{Nq^M}{3M} + 9C_2qM < q^M$$

when M is sufficiently large.

Note that $|\mathcal{A}_{\leq M}| = q^{M+1}$. Therefore the condition $g(A) = 0$ for every A with $\deg(A) \leq M$ is equivalent to the condition that the c_{ijk}'s satisfy a linear system of at most q^{2M+1} equations. Since the number of unknowns c_{ijk} is greater than the number of equations, there exist c_{ijk} not all zero such that $g(A) = 0$ for every $A \in \mathcal{A}$ with $\deg(A) < M$.

Finally, if $A \in \mathcal{A}$ with $D := \deg(A) > M$, we have

$$\deg(g(A)) \leq \frac{q^M}{3} + \frac{Dq^M}{3M} + \frac{Mq^D}{3D} < q^D$$

since the function q^x/x is increasing on $[M, \infty)$. Therefore the map $g : \mathcal{A} \to \mathcal{A}$ satisfies all the conditions of Lemma 2.1 with $C_1 = M$, we have that $g(A) = 0$ for every $A \in \mathcal{A}$ and this finishes the proof. □

Corollary 2.3. *Let $f : \mathcal{A} \to \mathcal{A}$ be as in Theorem 1.5. Then there exist $C_3, C_4 > 0$ depending only on q and f such that*

$$\deg(f(A)) \leq C_3 \deg(A) + C_4 \text{ for every } A \in \mathcal{A} \setminus \{0\}.$$

Proof. By Proposition 2.2, there exist $n \geq 0$ and polynomials $P_0(X), \ldots, P_n(X) \in \mathcal{A}[X]$ with $P_n \neq 0$ such that:

$$P_n(A)f(A)^n + P_{n-1}(A)f(A)^{n-1} + \ldots + P_0(A) = 0$$

for every $A \in \mathcal{A}$. We must have $n > 0$ since otherwise $P_0(A) = 0$ for every A would force $P_0 = 0$ as well. Let $C_3 = \max_{0 \leq i \leq n} \deg(P_i)$ and let C_4 be the maximum of the degrees of the coefficients of the P_i's so that $\deg(P_i(A)) \leq C_3 \deg(A) + C_4$ for every $A \in \mathcal{A} \setminus \{0\}$. If $\deg(f(A)) > C_3 \deg(A) + C_4$ then $\deg(P_n(A)f(A)^n)$ is greater than $\deg(P_{n-1}(A)f(A)^{n-1} + \ldots + P_0(A))$, contradiction. □

3. A result under a linear bound

In this section, we consider a related result in which the inequality (2) is replaced by a much stronger linear bound on $\deg(f(A_n))$ where $(A_n)_{n\geq 0}$ is a special sequence in $\mathcal{A}$. Moreover, the next theorem together with Corollary 2.3 yield Theorem 1.5.

Theorem 3.1. *Let $f:\ \mathcal{A}\to\mathcal{A}$ be a prime congruence-preserving map. Assume there exist $U\in\mathcal{A}$ with $U'\neq 0$ (i.e. U is not the p-th power of an element of $\bar{\mathbb{F}}[t]$) and positive integers C_5 and C_6 such that $\deg(f(U^n))\leq C_5 n+C_6$ for every $n\in\mathbb{N}_0$. Then f is a polynomial map.*

For every non-constant $A\in\mathcal{A}$, let $\operatorname{rad}(A)$ denote the product of the distinct monic irreducible factors of A. For integers $0\leq m<n$ and non-constant $U\in\mathcal{A}$, let $\Delta_{m,n,U}=(U^n-1)(U^{n-1}-1)\dots(U^{n-m}-1)$ and let $d_{m,n,U}=\deg(\operatorname{rad}(\Delta_{m,n,U}))$. We start with the following:

Lemma 3.2. *Let $U(t)\in\mathcal{A}$ such that $U'\neq 0$. Write $\delta=\deg(U)$.*

(a) *There exist a positive constant $C_7(p,U)$ depending only on p and U and a positive constant C_7' depending on C_7 such that for every $n\geq 1$:*

$$d_{n-1,n,U}\geq C_7(p,U)n^2-C_7'.$$

(b) *Let $0\leq m<n$ be integers. There exist positive constants $C_8(p,U)$ depending only on p and U and $C_9(m,p,U)$ depending only on m, p, and U such that:*

$$d_{m,n,U}\geq \delta\left(1-\frac{1}{p}+\frac{1}{p^2}-\frac{1}{p^3}\right)mn-C_8(p,U)n-C_9(m,p,U).$$

Proof. Since $U'\neq 0$, it has only finitely many roots. For $\alpha\in\bar{\mathbb{F}}$ that is not the value of U at any of those roots, we have $|U^{-1}(\alpha)|=\delta$.

For part (a), $d_{n-1,n,U}$ is at least the number of the preimages under U of the roots of unity (in $\bar{\mathbb{F}}^*$) whose order is at most n. For each ℓ with $p\nmid\ell$, there are exactly $\varphi(\ell)$ roots of unity of order ℓ. Since $\displaystyle\sum_{\ell\leq n,p\nmid\ell}\varphi(\ell)\gg n^2$, this proves part (a).

For part (b), $d_{m,n,U}$ is at least the number of the preimages under U of the roots of unity whose order divides $n-i$ for some $0\leq i\leq m$. Define:

$$T=\{0\leq i\leq m:\ n-i\not\equiv 0 \bmod p^2\}$$
$$A_i=\{\zeta\in\bar{\mathbb{F}}^*:\ \zeta^{n-i}=1\}\text{ for each }i\in T.$$

We have:

$$d_{m,n,U} \geq \delta |\bigcup_{i\in T} A_i| + O_U(1) \geq \delta \left(\sum_{i\in T} |A_i| - \sum_{i,j\in T, i<j} |A_i \cap A_j| \right) + O_U(1).$$

Note that $|A_i| = \dfrac{n-i}{p^k}$ where $p^k \parallel n-i$. Let:

$$S_0 = \sum_{0\leq i\leq m} (n-i) = \frac{(2n-m)(m+1)}{2},$$

$$S_1 = \sum_{0\leq i\leq m, p|n-i} (n-i) = p\frac{(\lfloor n/p\rfloor + \lceil (n-m)/p\rceil)(\lfloor n/p\rfloor - \lceil (n-m)/p\rceil + 1)}{2},$$

$$\begin{aligned} S_2 &= \sum_{0\leq i\leq m, p^2|n-i} (n-i) \\ &= p^2 \frac{(\lfloor n/p^2\rfloor + \lceil (n-m)/p^2\rceil)(\lfloor n/p^2\rfloor - \lceil (n-m)/p^2\rceil + 1)}{2}. \end{aligned}$$

We have:

$$\sum_{i\in T} |A_i| = S_0 - S_1 + \frac{1}{p}(S_1 - S_2) = \left(1 - \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3}\right) mn + O_p(1)n + O_{m,p}(1).$$

For $i < j$ in T, we have $A_i \cap A_j \subseteq \{\zeta : \zeta^{j-i} = 1\}$ hence $|A_i \cap A_j| \leq m$. Overall, we have

$$d_{m,n,U} \geq \delta \left(1 - \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3}\right) mn + O_{p,U}(1)n + O_{m,p,U}(1)$$

and this finishes the proof. □

We will need the following result on S-unit equations over characteristic p:

Proposition 3.3. *Let $\Gamma \subset \mathcal{K}^*$ be a finitely generated subgroup of rank r and consider the equation $x + y = 1$ with $(x, y) \in \Gamma \times \Gamma$. Then there exists a finite subset $\mathscr{X}$ of $\mathcal{K}^* \times \mathcal{K}^*$ of cardinality at most $p^{2r} - 1$ such that every solution $(x, y) \in (\Gamma \times \Gamma) \setminus (\bar{\mathbb{F}} \times \bar{\mathbb{F}})$ has the form $x = x_0^{p^k}$ and $y = y_0^{p^k}$ for some $(x_0, y_0) \in \mathscr{X}$ and $k \in \mathbb{N}_0$.*

Proof. This is well-known; see [16] or [2, Proposition 2.6]. □

Proof of Theorem 3.1. Recall that we are given $\deg(f(U^n)) \leq C_5 n + C_6$. Let $\delta = \deg(U)$. Let N, D_1, and D_2 be large positive integers that will be specified later. Consider the auxiliary function:

$$g(A) = P(A)f(A) + Q(A)$$

where $Q(X) \in \mathcal{A}[X]$ (respectively $P(X) \in \mathcal{A}[X]$) has degree at most D_1/δ (respectively $(D_1 - C_5)/\delta$) and each of its coefficients is an element of $\mathcal{A}$ with degree at most D_2 (respectively $D_2 - C_6$). There are at least $q^{D_1 D_2/\delta} q^{(D_1 - C_5)(D_2 - C_6)/\delta}$ many choices for the pair (P, Q). Note that g satisfies the congruence condition:

$$g(A + BC) \equiv g(A) \bmod C \text{ for every } A, B \in \mathcal{A} \text{ and } C \in \mathcal{P}.$$

We have $\deg(g(U^n)) \leq D_1 n + D_2$ for every n. Hence there are at most

$$\prod_{n=0}^{N} q^{D_1 n + D_2 + 1} = q^{(D_1 N(N+1)/2) + D_2(N+1) + N + 1}$$

possibilities for the tuple $(g(1), g(U), \ldots, g(U^N))$. Fix a small positive ϵ that will be specified later. Now we choose a large D_1, then let:

$$N + 1 = \frac{2 - \epsilon}{\delta} D_1 \text{ and } D_2 = \frac{\delta}{\epsilon} N(N+1),$$

so that

$$\begin{aligned} \frac{D_1 N(N+1)}{2} + D_2(N+1) + N + 1 &= \frac{1}{\delta}\left((\epsilon D_1 D_2/2) + (2-\epsilon) D_1 D_2 + (2-\epsilon) D_1\right) \\ &< \frac{1}{\delta}\left(D_1 D_2 + (D_1 - C_5)(D_2 - C_6)\right). \end{aligned}$$

By the pigeonhole principle, there exist two distinct choices of (P, Q) giving rise to the same tuple $(g(1), \ldots, g(U^N))$. Taking the difference, we conclude that there exist such P and Q so that $g(U^i) = P(U^i) f(U^i) + Q(U^i) = 0$ for $0 \leq i \leq N$. For every $n > N$, we have $g(U^n) \equiv 0 \bmod \operatorname{rad}(\Delta_{N,n,U})$. Recall the constants $C_8(p, U)$ and $C_9(N, p, U)$ from Lemma 3.2. Since $1 - \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3} > \frac{1}{2}$, by choosing a sufficiently large D_1 (which implies that N is sufficiently large) and sufficiently small ϵ, we have:

$$1 - \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3} - \frac{C_8(p, U)}{\delta N} > \frac{N+1}{(2-\epsilon)N}.$$

This implies that for all sufficiently large n, we have:

$$\begin{aligned} \delta\left(1 - \frac{1}{p} + \frac{1}{p^2} - \frac{1}{p^3}\right) Nn - C_8(p, U) n - C_9(N, p, U) &> \frac{\delta}{2-\epsilon}(N+1)n + D_2 \\ &= D_1 n + D_2. \end{aligned}$$

Since the right-hand side of the preceding inequality is at least $\deg(g(U^n))$ while the left-hand side is at most $\deg(\operatorname{rad}(\Delta_{N,n,U}))$ by Lemma 3.2, we have $g(U^n) = 0$ for all sufficiently large n. Let N_1 be such that $g(U^n) = 0$ for every $n \geq N_1$.

Now consider an arbitrary $A \in \mathcal{A} \setminus \{0\}$ then fix an integer $M > \deg(g(A))$. We claim that there exists $n \geq N_1$ such that $A - U^n$ has an irreducible factor T of degree at least M; once this is done we have that $g(A) \equiv g(U^n) = 0 \pmod{T}$, and this forces $g(A) = 0$, since the degree of T is strictly larger than the degree of $g(A)$. To see why there exists such an irreducible factor T, let Γ denote the subgroup of $\mathcal{K}^*$ generated by U, A, and all the irreducible polynomials of degree less than M. Since U is not the p-th power of an element in $\bar{\mathbb{F}}[t]$, there exists an irreducible polynomial in $\mathcal{A}$ whose exponent in the unique factorization of U is not divisible by p, i.e. $v(U) \not\equiv 0 \bmod p$ where v is the associated discrete valuation. Therefore the set $\mathscr{S} := \{n \geq N_1 : \ nv(U) - v(A) \not\equiv 0 \bmod p\}$ is infinite and for every $n \in \mathscr{S}$, we have U^n/A is not the p-th power of an element in $\mathcal{K}$. Let r denote the rank of Γ. Whenever $A - U^n = B$ has only irreducible factors of degree less than M, we have that $(U^n/A, B/A)$ is a solution of the equation $x + y = 1$ with $(x, y) \in \Gamma \times \Gamma$. By Proposition 3.3, there can be at most $p^{2r} - 1$ elements $n \in \mathscr{S}$ such that $A - U^n$ has only irreducible factors of degree less than M and this proves our claim.

Hence $g(A) = 0$ for every $A \in \mathcal{A} \setminus \{0\}$ and the congruence condition on g gives $g(A) = 0$ for every $A \in \mathcal{A}$. Hence $P(A)f(A) + Q(A) = 0$ for every $A \in \mathcal{A}$. We must have $P(X) \neq 0$; since otherwise $P(X) = Q(X) = 0$. For all $A \in \mathcal{A}$ except the finitely many A such that $P(A) = 0$, we have $Q(A)/P(A) = -f(A) \in \mathcal{A}$. This implies that $P(X) \mid Q(X)$ in $\mathcal{K}[X]$, hence f is a polynomial map, as desired. □

4. A further question

As mentioned in the introduction, it is an interesting problem to strengthen 1.5 by replacing the function $q^{\deg(A)}/\deg(A)$ in (2) by a larger function. Let

$$d_n := \deg\left(\prod_{P \in \mathcal{P}^+_{\leq n}} P\right)$$

which is the degree of the product of all monic irreducible polynomials of degree at most n. It seems reasonable to ask the following:

Question 4.1. *Suppose $f : \mathcal{A} \to \mathcal{A}$ is a prime congruence-preserving map and there exists $\epsilon \in (0, 1)$ such that for all sufficiently large n, for all $A \in \mathcal{A}$ of degree n, we have*

$$\deg(f(A)) \leq (1 - \epsilon)d_n.$$

Is it true that f is a polynomial map?

References

[1] E. Bombieri, W. Gubler, Heights in Diophantine Geometry, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

[2] J.P. Bell, K.D. Nguyen, Some finiteness results on monogenic orders in positive characteristic, Int. Math. Res. Not. 2018 (2018) 1601–1637.
[3] J.P. Bell, K.D. Nguyen, U. Zannier, D-finiteness, rationality, and height, arXiv:1905.06450.
[4] D.V. Chudnovsky, G.V. Chudnovsky, Applications of Padé approximations to the Grothendieck conjecture on linear differential equations, in: Number Theory, New York, NY, USA 1983–1984, in: Lecture Notes in Math., vol. 1135, Springer-Verlag, 1985, pp. 52–100.
[5] E. Croot, V.F. Lev, P.P. Pach, Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small, Ann. Math. (2) 185 (2017) 331–337.
[6] B. Dwork, G. Gerotto, F.J. Sullivan, An Introduction to G-Functions, Annals of Mathematics Studies, vol. 133, Princeton University Press, Princeton, 1994.
[7] Z. Dvir, On the size of Kakeya sets in finite fields, J. Am. Math. Soc. 22 (2009) 1093–1097.
[8] J.S. Ellenberg, D. Gijswijt, On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression, Ann. Math. (2) 185 (2017) 339–343.
[9] L. Guth, Polynomial Methods in Combinatorics, University Lecture Series, vol. 64, American Mathematical Society, Providence, 2016.
[10] R.R. Hall, On pseudo-polynomials, Mathematika 18 (1971) 71–77.
[11] R.R. Hall, On the probability that n and $f(n)$ are relatively prime II, Acta Arith. 19 (1971) 175–184.
[12] D. Masser, Auxiliary Polynomials in Number Theory, Cambridge Tracts in Mathematics, vol. 207, Cambridge University Press, Cambridge, 2016.
[13] A. Perelli, U. Zannier, On recurrent mod p sequences, J. Reine Angew. Math. 348 (1984) 135–146.
[14] M. Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer, New York, 2001.
[15] I.R. Ruzsa, On congruence preserving functions (Hungarian), Mat. Lapok 22 (1971) 125–134.
[16] J.F. Voloch, The equation $ax + by = 1$ in characteristic p, J. Number Theory 73 (1998) 195–200.
[17] U. Zannier, A note on recurrent mod p sequences, Acta Arith. 41 (1982) 277–280.
[18] U. Zannier, On periodic mod p sequences and G-functions, Manuscr. Math. 90 (1996) 391–402.