# AN ANALOGUE OF RUZSA'S CONJECTURE FOR POLYNOMIALS OVER FINITE FIELDS 

JASON P. BELL AND KHOA D. NGUYEN


#### Abstract

In 1971, Ruzsa conjectured that if $f: \mathbb{N} \rightarrow \mathbb{Z}$ with $f(n+k) \equiv f(n)$ $\bmod k$ for every $n, k \in \mathbb{N}$ and $f(n)=O\left(\theta^{n}\right)$ 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.


## 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 $f: \mathbb{N}_{0} \rightarrow \mathbb{Z}$ 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) $\limsup _{n \rightarrow \infty} \frac{\log |f(n)|}{n}<e$.
Then $f$ is necessarily a polynomial. The original form allows the version of (P1) in which $p$ is not necessarily a prime. Hall Hal71b 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 $f(0), \ldots, f(n-1)$ thanks to (P1). In 1971, Hall Hal71a] and Ruzsa Ruz71 independently proved the following result.

Theorem 1.1 (Hall-Ruzsa, 1971). Suppose that $f: \mathbb{N}_{0} \rightarrow \mathbb{Z}$ satisfies (P1) and

$$
\limsup _{n \rightarrow \infty} \frac{\log |f(n)|}{n}<e-1
$$

then $f$ is a polynomial.
The best upper bound was obtained in 1996 by Zannier Zan96 by extending earlier work of Perelli and Zannier [Zan82, PZ84]:

Theorem 1.2 (Zannier, 1996). Suppose that $f: \mathbb{N}_{0} \rightarrow \mathbb{Z}$ satisfies (P1) and

$$
\limsup _{n \rightarrow \infty} \frac{\log |f(n)|}{n}<e^{0.75}
$$

then $f$ is a polynomial.

[^0]In fact, the author remarked [Zan96, 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 Zan96] 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 $\mathbb{Q}(x))$ PZ84, Theorem 1.B] then applies deep results on the arithmetic of linear differential equations CC85, DGS94.

This paper is motivated by our recent work on D-finite series BNZ 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 $\operatorname{deg}: \mathcal{A} \rightarrow \mathbb{N}_{0} \cup\{-\infty\}$. A map $f: \mathcal{A} \rightarrow \mathcal{A}$ 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 $\mathcal{A}_{n}=\{A \in \mathcal{A}: \operatorname{deg}(A)=n\}, \mathcal{A}_{<n}=\{A \in \mathcal{A}: \operatorname{deg}(A)<n\}$, and $\mathcal{A}_{\leq n}=\{A \in \mathcal{A}: \operatorname{deg}(A) \leq n\}$. Let $\mathcal{P} \subset \mathcal{A}$ be the set of irreducible polynomials; the sets $\mathcal{P}_{n}, \mathcal{P}_{<n}$, and $\mathcal{P}_{\leq n}$ are defined similarly. The superscript + is used to denote the subset consisting of all the monic polynomials, for example $\mathcal{A}^{+}, \mathcal{A}_{n}^{+}$, $\mathcal{P}_{\leq n}^{+}$, etc. From the well-known identity [Ros01, pp. 8]:

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

we have

$$
\begin{equation*}
q^{n} \leq \operatorname{deg}\left(\prod_{P \in \mathcal{P}_{\leq n}^{+}} P\right)<2 q^{n} \tag{1}
\end{equation*}
$$

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 $f: \mathcal{A} \rightarrow \mathcal{A}$ satisfy the following 2 properties:
(P3) $f(A+B P) \equiv f(A) \bmod P$ for every $A, B \in \mathcal{A}$ and $P \in \mathcal{P}$;
(P4) $\limsup _{\operatorname{deg}(A) \rightarrow \infty} \frac{\log \operatorname{deg}(f(A))}{\operatorname{deg}(A)}<q$.
Is it true that $f$ is a polynomial map?
Note that (P3) should be the appropriate analogue of (P1): over the natural numbers, iterating $(\mathrm{P} 1)$ yields $f(n+b p) \equiv f(n) \bmod p$ 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 $\operatorname{deg}(A)<\operatorname{deg}(B)$. We define $g: \mathcal{A} \rightarrow \mathcal{A}$ 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:

$$
g(A) \equiv g\left(A_{1}\right) \bmod P \text { for every } A, A_{1} \prec B \text { and prime } P \mid\left(A-A_{1}\right)
$$

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

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

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 $\operatorname{deg}(g(B)) \in\left[q^{n}, 2 q^{n}\right)$ by (11). This latter property implies that $g$ cannot be a polynomial map.

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

Theorem 1.4. Let $f: \mathcal{A} \rightarrow \mathcal{A}$ such that $f$ satisfies Property (P3) in Question 1.3 and

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

Then $f$ is a polynomial map.
There is nothing special about the constant $1 /(27 q)$ 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 $q^{\operatorname{deg}(A)} / \operatorname{deg}(A)$ 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 PZ84, Zan96] seem to be applicable in our situation. Obviously, the crucial result used in Zan96] that the generating series $\sum f(n) x^{n}$ is $D$-finite has no counterpart here. The proof of the main result of [PZ84 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 [PZ84 to obtain a recurrence relation of the form $c_{d} f\left(A+B_{d}\right)+\ldots+c_{0} f\left(A+B_{0}\right)=0$ 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 $\operatorname{deg}(A)$ 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 $\left[2 M_{0},(2+\epsilon) M_{0}\right.$ ] from the vanishing on $\left[0, M_{0}\right.$ ] (see [PZ84, pp. 11-12] and Zan96, pp. 396-397]) does not seem applicable here.

The proof of Theorem 1.4 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 $\operatorname{deg}(f(A))$ can be bounded above by a linear function in $\operatorname{deg}(A)$. The second step, which might be of independent interest, treats the more general problem in which $f$ satisfies ( P 3 ) and there exists a special sequence $\left(A_{n}\right)_{n \in \mathbb{N}_{0}}$ in $\mathcal{A}$ such that $\operatorname{deg}\left(f\left(A_{n}\right)\right)$ is bounded above by a linear function in $\operatorname{deg}\left(A_{n}\right)$. 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 BG06, Mas16 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 Gut16. This method has produced surprisingly short and elegant solutions of certain combinatorial problems over finite fields Dvi09, CLP17, EG17.

Acknowledgments. We wish to thank Professor Umberto Zannier for useful discussions. J. B is partially supported by an NSERC Discovery Grant. K. N. is partially supported by an NSERC Discovery Grant, a start-up grant at UCalgary, and a CRC tier-2 research stipend.

## 2. A NONTRIVIAL ALGEBRAIC RELATION

We start with the following simple lemma:
Lemma 2.1. Let $g: \mathcal{A} \rightarrow \mathcal{A}$ and assume that there exists $C_{1} \in \mathbb{N}_{0}$ such that the following 3 properties hold:
(a) $g(A+B P) \equiv g(A) \bmod P$ for every $A, B \in \mathcal{A}$ and $P \in \mathcal{P}$.
(b) $\operatorname{deg}(g(A)) \leq q^{\operatorname{deg}(A)}-1$ for every $A \in \mathcal{A}$ with $\operatorname{deg}(A)>C_{1}$.
(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 $D:=\operatorname{deg}(A)>C_{1}$. 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 $A-C P$ has degree strictly less than $D$, we have

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

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

Proposition 2.2. Let $f: \mathcal{A} \rightarrow \mathcal{A}$ be as in Theorem 1.4. Then there exists a nonzero 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 $\operatorname{deg}(f(A))<\frac{q^{\operatorname{deg}(A)}}{27 q \operatorname{deg}(A)}$ for every $A \in \mathcal{A}$ with $\operatorname{deg}(A) \geq N$. Let $M \geq N$ be a large positive integers that will be specified later. Consider $Q(X, Y) \in \mathcal{A}[X, Y]$ of the form:

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

where $c_{i j k} \in \mathbb{F}_{q}$. The number of unknowns $c_{i j k}$ is greater than $q^{2 M+1}$.
Put $g(A)=Q(A, f(A))$ for $A \in \mathcal{A}$ then $g$ satisfies the congruence condition:

$$
\begin{equation*}
g(A+B P) \equiv g(A) \bmod P \text { for every } A, B \in \mathcal{A} \text { and } P \in \mathcal{P} \tag{3}
\end{equation*}
$$

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

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

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 $\operatorname{deg}(f(A))$ for $A \in \mathcal{A}_{<N}$. Hence for every $A \in \mathcal{A}_{<N}$, we have

$$
\operatorname{deg}(g(A)) \leq \frac{q^{M}}{3}+\frac{N q^{M}}{3 M}+9 C_{2} q M<q^{M}
$$

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

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

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

since the function $q^{x} / x$ is increasing on $[M, \infty)$. Therefore the map $g: \mathcal{A} \rightarrow \mathcal{A}$ 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 $f: \mathcal{A} \rightarrow \mathcal{A}$ be as in Theorem 1.4. Then there exist $C_{3}, C_{4}>0$ depending only on $q$ and $f$ such that

$$
\operatorname{deg}(f(A)) \leq C_{3} \operatorname{deg}(A)+C_{4} \text { for every } A \in \mathcal{A} \backslash\{0\}
$$

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 $A \in R$. We must have $n>0$ since otherwise $P_{0}(A)=0$ for every $A$ would force $P_{0}=0$ as well. Let $C_{3}=\max _{0 \leq i \leq n} \operatorname{deg}\left(P_{i}\right)$ and let $C_{4}$ be the maximum of the degrees of the coefficients of the $P_{i}$ 's so that $\operatorname{deg}\left(P_{i}(A)\right) \leq C_{3} \operatorname{deg}(A)+C_{4}$ for every $A \in \mathcal{A} \backslash\{0\}$. If $\operatorname{deg}(f(A))>C_{3} \operatorname{deg}(A)+C_{4}$ then $\operatorname{deg}\left(P_{n}(A) f(A)^{n}\right)$ is greater than $\operatorname{deg}\left(P_{n-1}(A) f(A)^{n-1}+\ldots+P_{0}(A)\right)$, 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 $\operatorname{deg}\left(f\left(A_{n}\right)\right)$ where $\left(A_{n}\right)_{n \geq 0}$ is a special sequence in $\mathcal{A}$. Moreover, the next theorem together with Corollary 2.3 yield Theorem 1.4

Theorem 3.1. Let $f: \mathcal{A} \rightarrow \mathcal{A}$ satisfy the congruence condition

$$
f(A+B P) \equiv f(A) \bmod P \text { for every } A, B \in \mathcal{A} \text { and } P \in \mathcal{P}
$$

Assume there exist $U \in \mathcal{A}$ with $U^{\prime} \neq 0$ (i.e. $U$ is not the $p$-th power of an element of $\overline{\mathbb{F}}[t])$ and positive integers $C_{5}$ and $C_{6}$ such that $\operatorname{deg}\left(f\left(U^{n}\right)\right) \leq C_{5} n+C_{6}$ 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 $\Delta_{m, n, U}=\left(U^{n}-1\right)\left(U^{n-1}-1\right) \ldots\left(U^{n-m}-1\right)$ and let $d_{m, n, U}=\operatorname{deg}\left(\operatorname{rad}\left(\Delta_{m, n, U}\right)\right)$. We start with the following:

Lemma 3.2. Let $U(t) \in \mathcal{A}$ such that $U^{\prime} \neq 0$. Write $\delta=\operatorname{deg}(U)$.
(a) Let $M, \epsilon>0$. There exists a positive constant $C_{7}(\epsilon, M, p, U)$ depending only on $\epsilon, M, p$, and $U$ such that for every $n \geq 1$ :

$$
d_{m, n, U} \geq \delta M n^{2-\epsilon}-C_{7}(\epsilon, M, p)
$$

(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:

$$
d_{m, n, U} \geq \delta\left(1-\frac{1}{p}+\frac{1}{p^{2}}-\frac{1}{p^{3}}\right) m n-C_{8}(p, U) n-C_{9}(m, p, U)
$$

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

For part (a), $d_{n-1, n, U}$ is at least the number of the preimages under $U$ of the roots of unity (in $\overline{\mathbb{F}}^{*}$ ) whose order is at most $n$. For each $\ell$ with $p \nmid \ell$, there are exactly $\varphi(\ell)$ roots of unity of order $\ell$. Since $\varphi(\ell)$ dominates $\ell^{1-\epsilon}$, 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:

$$
\begin{gathered}
T=\left\{0 \leq i \leq m: n-i \not \equiv 0 \bmod p^{2}\right\} \\
A_{i}=\left\{\zeta \in \overline{\mathbb{F}}^{*}: \zeta^{n-i}=1\right\} \text { for each } i \in T
\end{gathered}
$$

We have:

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

Note that $\left|A_{i}\right|=\frac{n-i}{p^{k}}$ where $p^{k} \| n-i$. Let:

$$
\begin{gathered}
S_{0}=\sum_{0 \leq i \leq m}(n-i)=\frac{(2 n-m)(m+1)}{2} \\
S_{1}=\sum_{0 \leq i \leq m, p \mid n-i}(n-i)=p \frac{(\lfloor n / p\rfloor+\lceil(n-m) / p\rceil)(\lfloor n / p\rfloor-\lceil(n-m) / p\rceil+1)}{2} \\
S_{2}=\sum_{0 \leq i \leq m, p^{2} \mid n-i}(n-i) \\
=p^{2} \frac{\left(\left\lfloor n / p^{2}\right\rfloor+\left\lceil(n-m) / p^{2}\right\rceil\right)\left(\left\lfloor n / p^{2}\right\rfloor-\left\lceil(n-m) / p^{2}\right\rceil+1\right)}{2}
\end{gathered}
$$

We have:

$$
\sum_{i \in T}\left|A_{i}\right|=S_{0}-S_{1}+\frac{1}{p}\left(S_{1}-S_{2}\right)=\left(1-\frac{1}{p}+\frac{1}{p^{2}}-\frac{1}{p^{3}}\right) m n+O_{p}(1) n+O_{m, p}(1)
$$

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

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

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 $p^{2 r}-1$ such that every solution $(x, y) \in(\Gamma \times \Gamma) \backslash(\overline{\mathbb{F}} \times \overline{\mathbb{F}})$ has the form $x=x_{0}^{p^{k}}$ and $y=y_{0}^{p^{k}}$ for some $\left(x_{0}, y_{0}\right) \in \mathscr{X}$ and $k \in \mathbb{N}_{0}$.

Proof. This is well-known; see Vol98 or BN18, Proposition 2.6].
Proof of Theorem 3.1. Recall that we are given $\operatorname{deg}\left(f\left(U^{n}\right)\right) \leq C_{5} n+C_{6}$. Let $\delta=$ $\operatorname{deg}(U)$. 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 $D_{1} / \delta$ (respectively $\left.\left(D_{1}-C_{5}\right) / \delta\right)$ 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 $q^{D_{1} D_{2} / \delta} q^{\left(D_{1}-C_{5}\right)\left(D_{2}-C_{6}\right) / \delta}$ many choices for the pair $(P, Q)$. Note that $g$ satisfies the congruence condition:

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

We have $\operatorname{deg}\left(g\left(U^{n}\right)\right) \leq D_{1} n+D_{2}$ for every $n$. Hence there are at most

$$
\prod_{n=0}^{N} q^{D_{1} n+D_{2}+1}=q^{\left(D_{1} N(N+1) / 2\right)+D_{2}(N+1)+N+1}
$$

possibilities for the tuple $\left(g(1), g(U), \ldots, g\left(U^{N}\right)\right)$. Fix a small positive $\epsilon$ 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

$$
\begin{aligned}
\frac{D_{1} N(N+1)}{2}+D_{2}(N+1)+N+1 & =\frac{1}{\delta}\left(\left(\epsilon D_{1} D_{2} / 2\right)+(2-\epsilon) D_{1} D_{2}+(2-\epsilon) D_{1}\right) \\
& <\frac{1}{\delta}\left(D_{1} D_{2}+\left(D_{1}-C_{5}\right)\left(D_{2}-C_{6}\right)\right)
\end{aligned}
$$

By the pigeonhole principle, there exist two distinct choices of $(P, Q)$ giving rise to the same tuple $\left(g(1), \ldots, g\left(U^{N}\right)\right)$. Taking the difference, we conclude that there exist such $P$ and $Q$ so that $g\left(U^{i}\right)=P\left(U^{i}\right) f\left(U^{i}\right)+Q\left(U^{i}\right)=0$ for $0 \leq i \leq N$. For every $n>N$, we have $g\left(U^{n}\right) \equiv 0 \bmod \operatorname{rad}\left(\Delta_{N, n, U}\right)$. 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 $\epsilon$, 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:

$$
\begin{aligned}
\delta\left(1-\frac{1}{p}+\frac{1}{p^{2}}-\frac{1}{p^{3}}\right) N n-C_{8}(p, U) n-C_{9}(N, p, U) & >\frac{\delta}{2-\epsilon}(N+1) n+D_{2} \\
& =D_{1} n+D_{2}
\end{aligned}
$$

Since the right-hand side of the preceding inequality is at least $\operatorname{deg}\left(g\left(U^{n}\right)\right)$ while the left-hand side is at most $\operatorname{deg}\left(\Delta_{N, n, U}\right)$ by Lemma 3.2 we have $g\left(U^{n}\right)=0$ for all sufficiently large $n$. Let $N_{1}$ be such that $g\left(U^{n}\right)=0$ for every $n \geq N_{1}$.

Now consider an arbitrary $A \in \mathcal{A} \backslash\{0\}$ then fix an integer $M>\operatorname{deg}(g(A))$. 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 $g(A) \equiv g\left(U^{n}\right)=0(\bmod T)$, 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 $\Gamma$ 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 $\overline{\mathbb{F}}[t]$, 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 $\mathscr{S}:=\left\{n \geq N_{1}: n v(U)-v(A) \not \equiv 0 \bmod p\right\}$ 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 $\Gamma$. Whenever $A-U^{n}=B$ has only irreducible factors of degree less than $M$, we have that $\left(U^{n} / A, B / A\right)$ 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 $p^{2 r}-1$ 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 $A \in \mathcal{A} \backslash\{0\}$ 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 1.4 by replacing the function $q^{\operatorname{deg}(A)} / \operatorname{deg}(A)$ in (2) by a larger function. Let

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

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 $f: \mathcal{A} \rightarrow \mathcal{A}$ such that $f(A+B P) \equiv f(A) \bmod P$ for every $A, B \in \mathcal{A}$ and $P \in \mathcal{P}$ 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

$$
\operatorname{deg}(f(A)) \leq(1-\epsilon) d_{n}
$$

Is it true that $f$ is a polynomial map?

## References

[BG06] E. Bombieri and W. Gubler, Heights in Diophantine geometry, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.
[BN18] J. P. Bell and K. D. Nguyen, Some finiteness results on monogenic orders in positive characteristic, Int. Math. Res. Not. 2018 (2018), 1601-1637.
[BNZ] J. P. Bell, K. D. Nguyen, and U. Zannier, D-finiteness, rationality, and height, arXiv:1905.06450.
[CC85] D. V. Chudnovsky and G. V. Chudnovsky, Applications of Padé approximations to the Grothendieck conjecture on linear differential equations, Number Theory (New York, NY, USA 1983-1984), Lecture Notes in Math., no. 1135, Springer-Verlag, 1985, pp. 52100.
[CLP17] E. Croot, V. F. Lev, and P. P. Pach, Progression-free sets in $\mathbb{Z}_{4}^{n}$ are exponentially small, Ann. of Math. (2) 185 (2017), 331-337.
[DGS94] B. Dwork, G. Gerotto, and F. J. Sullivan, An introduction to G-Functions, Annals of Mathematics Studies 133, Princeton University Press, Princeton, 1994.
[Dvi09] Z. Dvir, On the size of Kakeya sets in finite fields, Jour. Amer. Math. Soc. 22 (2009), 1093-1097.
[EG17] J. S. Ellenberg and D. Gijswijt, On large subsets of $\mathbb{F}_{q}^{n}$ with no three-term arithmetic progression, Ann. of Math. (2) 185 (2017), 339-343.
[Gut16] L. Guth, Polynomial methods in combinatorics, University Lecture Series, vol. 64, American Mathematical Society, Providence, 2016.
[Hal71a] R. R. Hall, On pseudo-polynomials, Mathematika 18 (1971), 71-77.
[Hal71b] , On the probability that $n$ and $f(n)$ are relatively prime II, Acta Arith. 19 (1971), 175-184.
[Mas16] D. Masser, Auxiliary polynomials in number theory, Cambridge Tracts in Mathematics, vol. 207, Cambridge University Press, Cambridge, 2016.
[PZ84] A. Perelli and U. Zannier, On recurrent mod p sequences, J. Reine Angew. Math. 348 (1984), 135-146.
[Ros01] M. Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer, New York, 2001.
[Ruz71] I. R. Ruzsa, On congruence preserving functions (Hungarian), Mat. Lapok. 22 (1971), 125-134.
[Vol98] J. F. Voloch, The equation $a x+b y=1$ in characteristic p, J. Number Theory 73 (1998), 195-200.
[Zan82] U. Zannier, A note on recurrent mod p sequences, Acta. Arith. 41 (1982), 277-280.
[Zan96] $\quad$ _ On periodic mod $p$ sequences and $G$-functions, Manuscripta Math. 90 (1996), 391-402.

Jason P. Bell, University of Waterloo, Department of Pure Mathematics, Waterloo, Ontario, Canada N2L 3G1

E-mail address: jpbell@uwaterloo.ca
Khoa D. Nguyen, Department of Mathematics and Statistics, University of Calgary, AB T2N 1N4, Canada

E-mail address: dangkhoa.nguyen@ucalgary.ca


[^0]:    2010 Mathematics Subject Classification. Primary: 11T55.
    Key words and phrases. Ruzsa's conjecture, polynomials, finite fields.

