Czechoslovak Mathematical Journal, 71 (146) (2021), 555–562

SIDON BASIS IN POLYNOMIAL RINGS OVER FINITE FIELDS

Wentang Kuo, Waterloo, Shuntaro Yamagishi, Utrecht

Received December 21, 2019. Published online September 24, 2020.

Abstract. Let $\mathbb{F}_q[t]$ denote the polynomial ring over $\mathbb{F}_q$, the finite field of q elements. Suppose the characteristic of $\mathbb{F}_q$ is not 2 or 3. We prove that there exist infinitely many $N \in \mathbb{N}$ such that the set $\{f \in \mathbb{F}_q[t] \colon \deg f < N\}$ contains a Sidon set which is an additive basis of order 3.

Keywords: Sidon set; additive basis; polynomial rings over finite fields

MSC 2020: 11K31, 11B83, 11T55

1. Introduction

Let $\mathbb{N}$ denote the set of positive integers and $A \subseteq \mathbb{N}$. For $k \geqslant 2$ we define

$$r_k(A,n) = \#\{(a_1,\dots,a_k) \in A^k \colon a_1+\ldots+a_k = n,\, a_1 \leqslant \ldots \leqslant a_k\}.$$

We say A is a *Sidon set* if $r_2(A,n) \leqslant 1$ for all $n \in \mathbb{N}$, and say A is an *asymptotic basis of order* k if there exists $C > 0$ such that $r_k(A,n) > 0$ for all $n > C$. Following [2] we say A is a *Sidon basis of order* k if A is a Sidon set and an asymptotic basis of order k. We refer the reader to [11] for a survey on Sidon sets. Given any $\varepsilon > 0$ and $n > n_0(\varepsilon)$, a Sidon set can have at most $(1+\varepsilon)\sqrt{n}$ elements less than or equal to n, see [6]; therefore, it follows that there cannot be a Sidon basis of order 2. Erdős, Sárközy and Sós asked the following conjecture in [4], [5].

Conjecture 1.1. *There exists a Sidon basis of order* 3.

Wentang Kuo is supported by an NSERC discovery grant RGPIN-2015-03709. Shuntaro Yamagishi is supported by the NWO Veni Grant `016.Veni.192.047`.

DOI: 10.21136/CMJ.2020.0543-19

There has been much progress toward this conjecture. Deshoulliers and Plagne in [3] constructed a Sidon basis of order 7, and Kiss in [7] proved the existence of a Sidon basis of order 5. Kiss, Rozgonyi and Sándor in [8] proved that there exists a Sidon basis of order 4.

Studying the analogies between function fields and number fields is an important aspect of number theory. In the function field setting, Theorem 1.2 below is known regarding Conjecture 1.1. Let G be an abelian group and A a subset of G. We say A is a *Sidon set* if the representation of each element of G as a sum of two elements of A is unique if it exists. In other words, if for some $a, b, c, d \in A$ we have $a + b = c + d$, then either we have $(a, b) = (c, d)$ or $(a, b) = (d, c)$. Also we say A is an *additive basis of order* k if for any $g \in G$ there exist $a_1, \ldots, a_k \in A$ such that $g = a_1 + \ldots + a_k$. Let $\mathbb{F}_q$ denote the finite field of q elements.

Theorem 1.2. *Let p be a prime, $p > 2$, $h \in \mathbb{N}$, and $q = p^h$. Then there exists a Sidon set $S \subseteq \mathbb{F}_q[t]$ which is an additive basis of order 2.*

This result is an immediate consequence of [9]; we can apply [9], Theorem 1 when $p \neq 2$, because $\varphi_2 \colon \mathbb{F}_q[t] \to \mathbb{F}_q[t]$ defined by $\varphi_2(f) = 2f$ is a one-to-one correspondence, and also $\mathbb{F}_q[t]$ is not a direct sum of a group of exponent 3 and a group of order 2. We note that there does not exist a Sidon set $S \subseteq \mathbb{F}_{2^h}[t]$ which is an additive basis of order 2; this is explained in the paragraph after the statement of [9], Theorem 1.

The focus of this paper is on the following theorem in [2] related to Conjecture 1.1.

Theorem 1.3 ([2], Theorem 2.1)**.** *There exist infinitely many $N \in \mathbb{N}$ for which there exists a Sidon set $S \subseteq \mathbb{Z}/N\mathbb{Z}$ such that the following holds. Given any $v \in \mathbb{Z}/N\mathbb{Z}$, there exist $s_1, s_2, s_3 \in S$ with $s_i \neq s_j$ $(i \neq j)$ such that*

$$s_1 + s_2 + s_3 = v.$$

In [2], this result and its Corollary 2.1 are key ingredients in proving the following two interesting results toward Conjecture 1.1 via probabilistic methods. In these applications, the pairwise distinct condition is crucial.

Theorem 1.4 ([2], Theorem 1.2)**.** *There exists $A \subseteq \mathbb{N}$ which is an asymptotic basis of order 3 and $r_2(A, n) \leqslant 2$ for all $n \in \mathbb{N}$.*

For any $\varepsilon > 0$, we say $A \subseteq \mathbb{N}$ is an *asymptotic basis of order* $k + \varepsilon$ if there exists $C > 0$ such that

$$\#\Big\{(a_1, \ldots, a_{k+1}) \in A^{k+1} \colon\ n = a_1 + \ldots + a_{k+1},\ \min_{1 \leqslant i \leqslant k+1} a_i \leqslant n^{\varepsilon}\Big\} \geqslant 1$$

for all $n > C$.

Theorem 1.5 ([2], Theorem 1.3)**.** *For any $\varepsilon > 0$, there exists a Sidon basis of order $3 + \varepsilon$.*

In this paper, we prove an $\mathbb{F}_q[t]$-analogue of Theorem 1.3 when the characteristic is not 2 or 3. For each $N \in \mathbb{N}$, let $\mathcal{P}_N = \{f \in \mathbb{F}_q[t] \colon \deg f < N\}$. Clearly, $\mathcal{P}_N$ is a group under addition.

Theorem 1.6. *Let p be a prime, $p > 3$, $h \in \mathbb{N}$, and $q = p^h$. Then for $M \in \mathbb{N}$ sufficiently large, there exists a Sidon set $S = S(q, M) \subseteq \mathcal{P}_{4M}$ such that the following holds. Given any $v \in \mathcal{P}_{4M}$, there exist $s_1, s_2, s_3 \in S$ with $s_i \neq s_j$ $(i \neq j)$ such that*

$$s_1 + s_2 + s_3 = v.$$

In this paper, we also prove Theorem 2.1, where we have a simpler proof under less restricting assumptions at the cost of relaxing the pairwise distinct condition[1], and Corollary 2.3, which is an analogue of [2], Corollary 2.1. Though we do not explore it here, the results of this paper can be used to obtain analogues of Theorems 1.4 and 1.5 by following the approach in [2] (with similar quantitative estimates as in their proof). We choose not to prove these results here, because the proofs are quite long and technical.

2. Proof of the results

Let G be an abelian group. For any subset $A \subseteq G$ and $x \in G$, we let

$$r_{A-A}(x) = \#\{(a, a') \in A^2 \colon x = a - a'\}.$$

It can be verified easily that the statement "$A \subseteq G$ satisfies $r_{A-A}(x) \leqslant 1$ whenever $x \neq 0$" is equivalent to A being a Sidon set. We begin with the proof of the following theorem.

Theorem 2.1. *Let p be a prime, $p > 3$, $h \in \mathbb{N}$, and $q = p^h$. Then for any $M \in \mathbb{N}$, there exists a Sidon set $S = S(q, M) \subseteq \mathcal{P}_{2M}$ such that the following holds. Given any $v \in \mathcal{P}_{2M}$, there exist $s_1, s_2, s_3 \in S$ such that*

$$s_1 + s_2 + s_3 = v.$$

[1] We would like to thank the anonymous referee for pointing this out to us, and also for providing the argument.

We remark that in comparison to the statement of Theorem 1.6, we do not require M to be sufficiently large, and we have $\mathcal{P}_{2M}$ instead of $\mathcal{P}_{4M}$, but we no longer have that s_1, s_2 and s_3 are pairwise distinct.

P r o o f. We have the following group isomorphisms when we only consider the additive properties

$$\mathcal{P}_{2M} \cong (\mathbb{F}_q)^{2M} \cong (\mathbb{Z}/p\mathbb{Z})^{2hM} \cong \mathbb{F}_{q'} \times \mathbb{F}_{q'},$$

where $q' = p^{hM}$. Therefore, if we can find a Sidon set with the desired properties in $\mathbb{F}_{q'} \times \mathbb{F}_{q'}$, then we are done.

Let $S = \{(x, x^2)\colon\ x \in \mathbb{F}_{q'}\}$. Then, by [1] we know that S is a Sidon set in $\mathbb{F}_{q'} \times \mathbb{F}_{q'}$. For the sake of completeness, we present the proof from [1] here. We have to check that given $(0,0) \neq (e_1, e_2) \in \mathbb{F}_{q'} \times \mathbb{F}_{q'}$, the equation $(x_1, x_1^2) - (x_2, x_2^2) = (e_1, e_2)$ uniquely determines x_1 and x_2 in $\mathbb{F}_{q'}$, or that it has no solution. If $e_1 = 0$, then it is clear that there do not exist x_1 and x_2 in $\mathbb{F}_{q'}$ satisfying the equation. On the other hand, suppose $e_1 \neq 0$. Since $x_1 = e_1 + x_2$, we have that $e_2 = (x_2 + e_1)^2 - x_2^2 = 2e_1x_2 + e_1^2$, which uniquely determines x_2 if $p \neq 2$. Once x_2 is determined, there is only one choice for x_1. Therefore, we have shown that $r_{S-S}((e_1, e_2)) \leqslant 1$, and hence S is a Sidon set.

Now we show that S is an additive basis of order 3; this is equivalent to showing that for any $(a, b) \in \mathbb{F}_{q'} \times \mathbb{F}_{q'}$, the system

$$x + y + t = a \quad \text{and} \quad x^2 + y^2 + t^2 = b \tag{2.1}$$

has a solution in $\mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_{q'}$. Let us fix a choice of $(a, b) \in \mathbb{F}_{q'} \times \mathbb{F}_{q'}$.

Since $p > 2$, it can be verified easily that given any $c, d \in \mathbb{F}_{q'}$, the system

$$x + y = c \quad \text{and} \quad x^2 + y^2 = d$$

has a solution in $\mathbb{F}_{q'} \times \mathbb{F}_{q'}$ if and only if there exists $z \in \mathbb{F}_{q'}$ such that $z^2 = 2d - c^2$. Therefore, it follows that the system (2.1) has a solution in $\mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_{q'}$ if and only if there exist $t, z \in \mathbb{F}_{q'}$ such that

$$2(b - t^2) - (a - t)^2 = -3t^2 + 2at + (2b - a^2) = z^2. \tag{2.2}$$

Since $p \neq 3$, every value represented by $-3t^2 + 2at + (2b - a^2)$ is represented by at most two values of $t \in \mathbb{F}_{q'}$. Consequently, we have

$$\#\{-3t^2 + 2at + (2b - a^2)\colon\ t \in \mathbb{F}_{q'}\} \geqslant \tfrac{1}{2}(q' - 1) + 1.$$

There are precisely $\frac{1}{2}(q'-1)$ elements in $\mathbb{F}_{q'}$ that are non-squares. Therefore, it follows that there exists at least one $t \in \mathbb{F}_{q'}$ such that $-3t^2 + 2at + (2b - a^2)$ is a square; there exist $t, z \in \mathbb{F}_{q'}$ satisfying (2.2). As a result, we obtain that there exists a triple $(x, y, t) \in \mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_{q'}$ satisfying (2.1). Since the argument holds for an arbitrary choice of $(a, b) \in \mathbb{F}_{q'} \times \mathbb{F}_{q'}$, this completes the proof. □

We can in fact replace $\mathcal{P}_{2M}$ in the statement of Theorem 2.1 with $\mathcal{P}_M$ when h is even.

Corollary 2.2. *Let p be a prime, $p > 3$, $h \in \{2n\colon n \in \mathbb{N}\}$, and $q = p^h$. Then for any $M \in \mathbb{N}$, there exists a Sidon set $S = S(q, M) \subseteq \mathcal{P}_M$ such that the following holds. Given any $v \in \mathcal{P}_M$, there exist $s_1, s_2, s_3 \in S$ such that*

$$s_1 + s_2 + s_3 = v.$$

P r o o f. We have the following group isomorphisms when we only consider the additive properties

$$\mathcal{P}_M \cong (\mathbb{F}_q)^M \cong (\mathbb{Z}/p\mathbb{Z})^{hM} \cong \mathbb{F}_{q'} \times \mathbb{F}_{q'},$$

where $q' = p^{hM/2}$. Then we can find a Sidon set with the desired properties in $\mathbb{F}_{q'} \times \mathbb{F}_{q'}$ as in the proof of Theorem 2.1. □

Next, we present the proof of Theorem 1.6.

P r o o f of Theorem 1.6. We have the following group isomorphisms when we only consider the additive properties

$$\mathcal{P}_{4M} \cong (\mathbb{F}_q)^{4M} \cong (\mathbb{Z}/p\mathbb{Z})^{4hM} \cong \mathbb{F}_{q'} \times \mathbb{F}_{q'},$$

where $q' = p^{2hM}$. Therefore, if we can find a Sidon set with the desired properties in $\mathbb{F}_{q'} \times \mathbb{F}_{q'}$, then we are done.

Recall that we have explained in the beginning of the proof of Theorem 2.1 that $S = \{(x, x^2)\colon x \in \mathbb{F}_{q'}\}$ is a Sidon set in $\mathbb{F}_{q'} \times \mathbb{F}_{q'}$. Now we show that S is an additive basis of order 3. Again, this is equivalent to showing that for any $(a, b) \in \mathbb{F}_{q'} \times \mathbb{F}_{q'}$, the system

$$x + y + t = a \quad \text{and} \quad x^2 + y^2 + t^2 = b \tag{2.3}$$

has a solution in $\mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_{q'}$.

We consider the polynomial

$$f(x, y) = x^2 + y^2 + (x + y - a)^2 - b = 2(x^2 + y^2 + xy - ax - ay) + a^2 - b$$

constructed from (2.3), and its homogenization

$$F(x,y,z) = 2(x^2+y^2+xy-axz-ayz)+(a^2-b)z^2.$$

Suppose F is reducible over $\bar{\mathbb{F}}_{q'}$, where $\bar{\mathbb{F}}_{q'}$ is the algebraic closure of $\mathbb{F}_{q'}$, in which case F decomposes into two lines L_1 and L_2 with coefficients in $\bar{\mathbb{F}}_{q'}$. Without loss of generality, let

$$F(x,y,z) = 2(x+\alpha_1 y+\beta_1 z)(x+\alpha_2 y+\beta_2 z),$$

where $\alpha_1,\beta_1,\alpha_2,\beta_2 \in \bar{\mathbb{F}}_{q'}$. By multiplying out the factors, we see from the coefficients of y^2, xy, xz, and yz that $\alpha_1\alpha_2 = 1$, $\alpha_1+\alpha_2 = 1$, $\beta_1+\beta_2 = -a$, and $\alpha_1\beta_2+\alpha_2\beta_1 = -a$, respectively. Since $q' = p^{2hM}$ and $2|(2hM)$, we have $\mathbb{F}_{p^2} \subseteq \mathbb{F}_{q'}$. From the first and the second equation, we obtain that α_1 and α_2 are nonzero, and

$$\alpha_1,\alpha_2 \in \mathbb{F}_{p^2} \subseteq \mathbb{F}_{q'}.$$

Since the characteristic of $\mathbb{F}_{q'}$ is not 3, we also obtain $\alpha_1 \neq \alpha_2$. Then from the third and the fourth equation, we can deduce that

$$\beta_1,\beta_2 \in \mathbb{F}_{q'}.$$

(Here if the characteristic of $\mathbb{F}_{q'}$ was 3, then we obtain $\alpha_1 = \alpha_2$, from which it follows that $a = 0$ and also that the third and the fourth equation are scalar multiples of one another. Consequently, we cannot conclude that $\beta_1,\beta_2 \in \mathbb{F}_{q'}$ in this case.) Therefore, F is in fact reducible over $\mathbb{F}_{q'}$, and hence f decomposes into two linear factors over $\mathbb{F}_{q'}$ as follows

$$f(x,y) = F(x,y,1) = 2(x+\alpha_1 y+\beta_1)(x+\alpha_2 y+\beta_2).$$

Thus we see that (2.3) has at least q' solutions in $\mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_{q'}$ in this case.

On the other hand, suppose F is irreducible over $\bar{\mathbb{F}}_{q'}$. Let $V(F)$ be the hypersurface in $\mathbb{P}^2_{\bar{\mathbb{F}}_{q'}}$ defined by F. In this case, we may invoke a theorem by Lang and Weil, see [10], and obtain that $V(F)$ has $q'+O(1)$ rational points over $\mathbb{F}_{q'}$. We know that $F(x,y,0) = 2(x^2+y^2+xy)$ decomposes into two linear factors over $\bar{\mathbb{F}}_{q'}$, because it is a quadratic form in two variables. Then we can verify that $F(x,y,0)$ has at most $O(1)$ solutions in $\mathbb{P}^1_{\bar{\mathbb{F}}_{q'}}$. Therefore, it follows that $V(F)$ contains $q'+O(1)$ points of the form $[x_0 : y_0 : 1]$ from which we deduce (2.3) has $q'+O(1)$ solutions in $\mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_{q'}$.

In both cases, we have that (2.3) has at least $q'+O(1)$ solutions. Suppose $(x,y,t) = (x_1,x_2,x_3)$ is a solution to (2.3) such that $x_i = x_j$ for some $i \neq j$; without loss of

generality, let $i = 1$ and $j = 2$. Then, the number of such solutions is equal to the number of solutions to

$$x + x + y = a \quad \text{and} \quad x^2 + x^2 + y^2 = b. \tag{2.4}$$

Since the equation $2x^2+(a-2x)^2 = b$ has at most 2 solutions in $\mathbb{F}_{q'}$, we have that (2.4) has at most 2 solutions. Hence, the number of solutions (x_1, x_2, x_3) to (2.3) such that $x_i = x_j$ for some $i \neq j$ is $O(1)$. Therefore, for each $(a, b) \in \mathbb{F}_{q'} \times \mathbb{F}_{q'}$ we can find a solution (x_1, x_2, x_3) to (2.3) satisfying $x_i \neq x_j$ $(i \neq j)$, provided q' is sufficiently large. □

Let us remark that the above argument does not work when $p = 3$. For if $a = 0$, then the equations (2.3) reduce to solving

$$x^2 + y^2 + (x + y)^2 = b,$$

which further reduces to

$$(x - y)^2 = \tfrac{1}{2}b.$$

However, not all elements of $\mathbb{F}_{q'}$ are squares. (Consider the group homomorphism from $\mathbb{F}_{q'} \setminus \{0\}$ to $\mathbb{F}_{q'} \setminus \{0\}$ which sends x to x^2, and notice that the kernel of this map is $\{\pm 1\}$.) Hence, there exists $b \in \mathbb{F}_{q'}$ for which the above equation does not have a solution.

We now prove the following corollary which holds when $p = 3$ as well.

Corollary 2.3. *Let p be a prime, $p > 2$, $h \in \mathbb{N}$, and $q = p^h$. Then for $M \in \mathbb{N}$ sufficiently large, there exists a Sidon set $S = S(q, M) \subseteq \mathcal{P}_{4M}$ such that the following holds. Given any $v \in \mathcal{P}_{4M}$, there exist $s_1, s_2, s_3, s_4 \in S$ with $s_i \neq s_j$ $(i \neq j)$ such that*

$$s_1 + s_2 + s_3 + s_4 = v.$$

P r o o f. Let $\mathbb{F}_{q'}$ and $S \subseteq \mathbb{F}_{q'} \times \mathbb{F}_{q'}$ be as in the proof of Theorem 1.6. We show that S satisfies the required conditions. From the proof of Theorem 1.6, we know that for any $(a, b) \in \mathbb{F}_{q'} \times \mathbb{F}_{q'}$, the system

$$x + y + t + (a - 1) = a \quad \text{and} \quad x^2 + y^2 + t^2 + (a - 1)^2 = b \tag{2.5}$$

has at least $q' + O(1)$ solutions of the form $(x, y, t) = (x_1, x_2, x_3) \in \mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_{q'}$, where $x_i \neq x_j$ $(i \neq j)$. Note that since the equations (2.5) reduce to

$$x + y + t = 1 \neq 0 \quad \text{and} \quad x^2 + y^2 + t^2 = b - (a - 1)^2,$$

we see that in fact we may assume the characteristic of $\mathbb{F}_{q'}$ to be 3 as well.

We observe that all of these solutions except those with at least one of x_1, x_2, x_3 being $a-1$ satisfy the conditions. Without loss of generality, suppose $x_3 = a-1$. Then, (2.5) reduces to solving

$$x + y = -a + 2 \quad \text{and} \quad x^2 + y^2 = b - 2(a-1)^2, \tag{2.6}$$

which further reduces to solving a quadratic equation. Thus it follows that the number of solutions (x_1, x_2, x_3) to (2.5) with at least one of x_1, x_2, x_3 being $a-1$ is $O(1)$. Therefore, it follows that there exist at least $q' + O(1)$ solutions in $\mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_{q'}$ which satisfy the desired conditions. □

References

[1] *J. Cilleruelo*: Combinatorial problems in finite fields and Sidon sets. Combinatorica *32* (2012), 497–511. zbl MR doi

[2] *J. Cilleruelo*: On Sidon sets and asymptotic bases. Proc. Lond. Math. Soc. (3) *111* (2015), 1206–1230. zbl MR doi

[3] *J.-M. Deshouillers, A. Plagne*: A Sidon basis. Acta Math. Hung. *123* (2009), 233–238. zbl MR doi

[4] *P. Erdős, A. Sárközy, V. T. Sós*: On additive properties of general sequences. Discrete Math. *136* (1994), 75–99. zbl MR doi

[5] *P. Erdős, A. Sárközy, V. T. Sós*: On sum sets of Sidon sets I. J. Number Theory *47* (1994), 329–347. zbl MR doi

[6] *P. Erdős, P. Turán*: On a problem of Sidon in additive number theory, and on some related problems. J. Lond. Math. Soc. *16* (1941), 212–215. zbl MR doi

[7] *S. Z. Kiss*: On Sidon sets which are asymptotic basis. Acta Math. Hung. *128* (2010), 46–58. zbl MR doi

[8] *S. Z. Kiss, E. Rozgonyi, C. Sándor*: On Sidon sets which are asymptotic bases of order 4. Funct. Approximatio, Comment. Math. *51* (2014), 393–413. zbl MR doi

[9] *S. V. Konyagin, V. F. Lev*: The Erdős-Turán problem in infinite groups. Additive Number Theory. Springer, New York, 2010, pp. 195–202. zbl MR doi

[10] *S. Lang, A. Weil*: Number of points of varieties in finite fields. Am. J. Math. *76* (1954), 819–827. zbl MR doi

[11] *K. O'Bryant*: A complete annotated bibliography of work related to Sidon sequences. Electron. J. Comb. *DS11* (2004), 39 pages. zbl

Authors' addresses: Wentang Kuo, Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON N2L 3G1, Canada, e-mail: wtkuo@uwaterloo.ca; Shuntaro Yamagishi (corresponding author), Mathematical Institute, Utrecht University, Budapestlaan 6, 3584 CD Utrecht, The Netherlands, e-mail: s.yamagis@uu.nl.