ACTA ARITHMETICA
174.3 (2016)

On a problem of Sidon for polynomials over finite fields

by

Wentang Kuo and Shuntaro Yamagishi (Waterloo, ON)

1. Introduction. In the course of investigations on Fourier series by S. Sidon, several questions arose concerning the existence and nature of certain positive integer sequences ω for which

$$r_n(\omega) = |\{(a,b) \in \mathbb{N} \times \mathbb{N} : a, b \in \omega,\ a+b=n,\ 0<a<b\}|$$

is bounded or, in some sense, exceptionally small, where $|S|$ denotes the cardinality of the set S. In particular, he asked the following question in 1932, known as the *Sidon Problem* [1]:

Does there exist a sequence ω such that $r_n(\omega) > 0$ for all n sufficiently large and, for all $\epsilon > 0$,

$$\lim_{n\to\infty} \frac{r_n(\omega)}{n^\epsilon} = 0\ ?$$

In 1954, P. Erdős [1] answered this question positively by proving

Theorem (Erdős). *There exists a sequence ω such that*

$$\log n \ll r_n(\omega) \ll \log n \quad \textit{for } n \textit{ sufficiently large.}$$

In other words, there exists a "thin" set ω such that every sufficiently large positive integer can be represented as a sum of two elements in ω. In the other direction, Erdős and Rényi [2] proved that there exists a "thick" set ω such that $r_n(\omega)$ is bounded for all n.

Theorem (Erdős–Rényi). *For any $\varepsilon > 0$, there exists a positive number $G = G(\varepsilon)$ and a sequence ω such that $r_n(\omega) < G$ for all n and*

$$|\{m \in \omega : m \le n\}| > n^{1/2-\varepsilon} \quad \textit{for sufficiently large } n.$$

We note that the result is best possible up to the ε term. One way to see this is by applying the pigeonhole principle. Suppose we have $\omega_0 \subseteq \mathbb{N}$,

2010 *Mathematics Subject Classification*: 11K31, 11B83, 11T55.
Key words and phrases: Sidon sets, probabilistic number theory.
Received 7 August 2015; revised 15 February 2016.
Published online 12 July 2016.

DOI: 10.4064/aa8252-3-2016

where $r_n(\omega_0) < G$ for all $n \in \mathbb{N}$. Given any $m_1, m_2 \in \{m \in \omega_0 : m \le n\}$, we have $1 < m_1 + m_2 \le 2n$. Therefore, by the pigeonhole principle,

$$G > \max_{1<m\le 2n} r_m(\omega_0) \ge \frac{|\{m \in \omega_0 : m \le n\}|^2 - |\{m \in \omega_0 : m \le n\}|}{2(2n-1)}.$$

Consequently,

$$|\{m \in \omega_0 : m \le n\}| \ll n^{1/2}.$$

Sidon's questions and the above results have been extended in various directions (see the survey paper [5]).

In this paper, we prove an analogue of these results in the setting of $\mathbb{F}_q[T]$. Let ω be a sequence of polynomials in $\mathbb{F}_q[T]$. For each $h \in \mathbb{F}_q[T]$, we define

$$r_h(\omega) = |\{(f,g) \in \mathbb{F}_q[T] \times \mathbb{F}_q[T] : f, g \in \omega,\ h = f + g,\ \deg g \le \deg h, f \ne g\}|.$$

Here $\deg f$ is the degree of $f \in \mathbb{F}_q[T]$ with the convention that $\deg 0 = -\infty$. We prove the following results.

THEOREM 1. *There exists a sequence ω of polynomials in $\mathbb{F}_q[T]$ such that*

$$\deg h \ll r_h(\omega) \ll \deg h \quad \text{for } \deg h \text{ sufficiently large}$$

In the other direction, we prove that there exists a "thick" set ω with bounded value $r_h(\omega)$. We denote $\omega = \{f_i\}_{i\in\mathbb{N}}$, where $\deg f_i \le \deg f_j$ $(i < j)$.

THEOREM 2. *For each $\epsilon > 0$, there exists a sequence $\omega = \{f_i\}$ of polynomials in $\mathbb{F}_q[T]$ and a positive integer K such that $r_h(\omega) < K$ for all $h \in \mathbb{F}_q[T]$ and $q^{\deg f_i} \ll i^{2+\epsilon}$.*

For each $h \in \mathbb{F}_q[T]$, we define

$$t_h(\omega) = |\{(f,g) \in \mathbb{F}_q[T] \times \mathbb{F}_q[T] : f, g \in \omega,\ h = f - g,\ \deg f, \deg g \le \deg h\}|.$$

We also prove the following variation of the existence of thick sets.

THEOREM 3. *For each $\epsilon > 0$, there exists a sequence $\omega = \{f_i\}$ of polynomials in $\mathbb{F}_q[T]$ and a positive integer K' such that $t_h(\omega) < K'$ for all $h \in \mathbb{F}_q[T]$ and $q^{\deg f_i} \ll i^{2+\epsilon}$.*

We prove our theorems by using the probabilistic method of Erdős and Rényi in the form presented in [3, Chapter III]. Roughly speaking, we set up a probability space to study the probability of the events $\{\omega : r_h(\omega) = d\}$ for all non-negative integers d. Using the Borel–Cantelli lemma, we show that the sequences satisfy the desired properties with probability 1. We also remark that Theorems 2 and 3 have been generalized to m-fold sums and differences by K. E. Hare and the second author in [4, Corollary 3.6]. However, the above formulations of Theorems 2 and 3 use a different language

than in [4]. Moreover, with the same machinery needed to prove Theorem 1, we can prove Theorems 2 and 3 with a slight modification of the proof of Theorem 1, and therefore we supply these proofs.

The organization of this paper is as follows. In Section 2, we first review the basic probability theory and state the Borel–Cantelli lemma. Next, in Section 3, we state the equivalent statements of our theorems and set up the probability space used in our proof. In Section 4, we establish several technical lemmas. Finally, the remaining sections are devoted to the proof of our main results.

2. Preliminaries. We start with probability theory. Let $\{X_j\}$ be a sequence of spaces and write

$$X = \prod_{j=0}^{\infty} X_j.$$

Let $\mathcal{M}_j$ be a σ-algebra of subsets of X_j. A *measurable rectangle* with respect to the sequence $\{\mathcal{M}_j\}$ is defined to be a subset W of X which is representable in the form

$$W = \prod_{j=0}^{\infty} W_j,$$

where $W_j \in \mathcal{M}_j$ and $W_j = X_j$ except for finitely many j. The following two theorems are standard in probability theory.

THEOREM 4 ([3, p. 123, Theorem 5]). *Let $\{(X_j, \mathcal{M}_j, P_j)\}_{j\geq 0}$ be a sequence of probability spaces, and write $X = \prod_{j=0}^{\infty} X_j$. Let $\mathcal{M}$ be the minimal σ-algebra of subsets of X containing every measurable rectangle with respect to $\{\mathcal{M}_j\}$. Then there exists a unique measure P on $\mathcal{M}$ such that for every non-empty measurable rectangle W,*

$$P(W) = \prod_{j=0}^{\infty} P_j(W_j), \tag{5}$$

where the W_j are defined by $W = \prod_{j=0}^{\infty} W_j$, $W_j \in \mathcal{M}_j$ $(j \geq 0)$. Here the product is, in essence, finite by the definition of measurable rectangle with respect to $\{\mathcal{M}_j\}$.

We remark that in the above theorem, since

$$P(X) = \prod_{j=0}^{\infty} P_j(X_j) = 1,$$

the σ-algebra $\mathcal{M}$ together with the measure P constitutes a probability space $(X, \mathcal{M}, P)$.

THEOREM 6 ([3, p. 135, Borel–Cantelli Lemma]). *Let $(X', \mathcal{M}', P')$ be a probability space. Let $\{W_\ell\}$ be a sequence of measurable events. If*

$$\sum_{\ell=1}^{\infty} P'(W_\ell) < \infty,$$

then, with probability 1*, at most finitely many of the events W_ℓ can occur, or equivalently,*

$$P'\Big(\bigcap_{i=1}^{\infty}\bigcup_{\ell=i}^{\infty} W_\ell\Big) = 0.$$

3. Probability space $(\Omega, \mathcal{M}, P)$. We let $q = p^s$ for a prime p, and denote by $\mathbb{F}_q$ the finite field of q elements. Let $\mathbb{F}_q[T]$ be the polynomial ring over $\mathbb{F}_q$. Let ι be any bijective map from $\mathbb{Z} \cap [0, q-1]$ to $\mathbb{F}_q$. We label each of the polynomials in $\mathbb{F}_q[T]$ as follows. Let $\mathbb{Z}_{\geq 0}$ be the set of all non-negative integers. For every $N \in \mathbb{Z}_{\geq 0}$, we define

$$p_N := \iota(c_0) + \iota(c_1)T + \cdots + \iota(c_n)T^n,$$

where $N = c_0 + c_1 q + \cdots + c_n q^n$ and $0 \leq c_i < q$ $(1 \leq i \leq n)$. It is clear that this gives a one-to-one correspondence between $\mathbb{Z}_{\geq 0}$ and $\mathbb{F}_q[T]$.

We use ω to denote a subsequence of the sequence of all polynomials in $\mathbb{F}_q[T]$, i.e. $p_0, p_1, p_2, p_3, \ldots$, and Ω to denote the space of all such sequences ω. By writing $f \in \omega$, we mean $f \in \mathbb{F}_q[T]$ appears in the sequence ω. Given $N \in \mathbb{Z}_{\geq 0}$ and $\omega \in \Omega$, we define

$$r_N(\omega) = |\{(a,b) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} : p_a, p_b \in \omega, \\ p_N = p_a + p_b,\ \deg p_a, \deg p_b \leq \deg p_N,\ a < b\}|,$$

and

$$t_N(\omega) = |\{(a,b) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} : p_a, p_b \in \omega, \\ p_N = p_a - p_b,\ \deg p_a, \deg p_b \leq \deg p_N\}|.$$

Our main theorems, Theorems 1, 2 and 3, are consequences of the following results.

THEOREM 7. *There exists a sequence ω of polynomials in $\mathbb{F}_q[T]$ such that*

$$\log N \ll r_N(\omega) \ll \log N \quad \text{for } N \text{ sufficiently large.}$$

THEOREM 8. *For each $\epsilon > 0$, there exists a sequence $\omega = \{p_{b_j}\}$ of polynomials in $\mathbb{F}_q[T]$ and a positive integer K_0 such that $r_N(\omega) < K_0$ for all $N \in \mathbb{Z}_{\geq 0}$ and $b_j \ll j^{2+\epsilon}$.*

THEOREM 9. *For each $\epsilon > 0$, there exists a sequence $\omega = \{p_{b_j}\}$ of polynomials in $\mathbb{F}_q[T]$ and a positive integer K_0' such that $t_N(\omega) < K_0'$ for all $N \in \mathbb{Z}_{\geq 0}$ and $b_j \ll j^{2+\epsilon}$.*

Since $\deg p_N \le \log_q N < \deg p_N + 1$, we can easily derive Theorems 1–3 from Theorems 7–9, respectively.

The following theorem is essentially [3, p. 141, Theorem 13].

THEOREM 10. *Let $\alpha_0, \alpha_1, \alpha_2, \dots,$ be real numbers satisfying $0 \le \alpha_i \le 1$ $(i \ge 0)$. Then there exists a probability space $(\Omega, \mathcal{M}, P)$ with the following properties:*

(i) *For every non-negative integer m, the event $\mathfrak{B}_m = \{\omega \in \Omega : p_m \in \omega\}$ is measurable and $P(\mathfrak{B}_m) = \alpha_m$.*
(ii) *The events $\mathfrak{B}_0, \mathfrak{B}_1, \mathfrak{B}_2, \dots$ are independent.*

Proof. Let Y be the space of two elements, y_0 and y_1 say. With each sequence ω we associate the sequence $\{x_j\}$ of elements of Y defined by

$$x_j = \begin{cases} y_0 & \text{if } p_j \notin \omega, \\ y_1 & \text{if } p_j \in \omega, \end{cases}$$

for $j \ge 0$. The space X consisting of all the sequences $x = \{x_j\}$ is given by

$$X = \prod_{j=0}^{\infty} X_j,$$

where $X_j = Y$ for $j \ge 0$. Let $\mathcal{M}_j = \{\phi, \{y_0\}, \{y_1\}, X_j\}$, the non-trivial σ-algebra of X_j, and let P_j be the probability measure on $\mathcal{M}_j$ such that $P_j(\{y_1\}) = \alpha_j$.

We apply Theorem 4 to the sequence $\{X_j, \mathcal{M}_j, P_j\}$ of probability spaces. In view of the one-to-one correspondence between the elements of X and Ω, we may denote the resulting probability space as $(\Omega, \mathcal{M}, P)$.

Now, we prove $(\Omega, \mathcal{M}, P)$ has properties (i) and (ii). Clearly,

$$\mathfrak{B}_m = \{\omega \in \Omega : p_m \in \omega\} = \prod_{j=0}^{\infty} W_j,$$

where $W_j = X_j$ for all j except $j = m$ and $W_m = \{y_1\}$. Thus, (i) follows, because $\mathfrak{B}_m \in \mathcal{M}$ by the definition of $\mathcal{M}$, and by (5) we have

$$P(\mathfrak{B}_m) = \prod_{j=0}^{\infty} P_j(W_j) = P_m(\{y_1\}) = \alpha_m.$$

For (ii), we consider any finite subset of $\{\mathfrak{B}_j\}$, say $\mathfrak{B}_{j_1}, \dots, \mathfrak{B}_{j_\ell}$. Then

$$\bigcap_{i=1}^{\ell} \mathfrak{B}_{j_i} = \{\omega \in \Omega : p_{j_i} \in \omega \ (1 \le i \le \ell)\} = \prod_{j=0}^{\infty} W_j,$$

where $W_j = X_j$ for all j except $j = j_1, \dots, j_\ell$ and $W_{j_i} = \{y_1\}$ for $1 \le i \le \ell$.

Thus, by (5) and (i) we obtain

$$P\Big(\bigcap_{i=1}^{\ell}\mathfrak{B}_{j_i}\Big)=\prod_{j=0}^{\infty}P_j(W_j)=\prod_{i=1}^{\ell}P_{j_i}(\{y_1\})=\prod_{i=1}^{\ell}\alpha_{j_i}=\prod_{i=1}^{\ell}P(\mathfrak{B}_{j_i}),$$

from which (ii) follows. ∎

4. Technical lemmas. For each $N\in\mathbb{Z}_{\geq 0}$, let $p_N\in\mathbb{F}_q[T]$ be as prescribed in the previous section. Define

$$n:=n(N)=\deg p_N=\lfloor\log_q N\rfloor.$$

Suppose $p\neq 2$. Since $\mathbb{F}_q=2\mathbb{F}_q$, we know there exists p_{N_0} such that $p_N=p_{N_0}+p_{N_0}$. It is clear that $\deg p_{N_0}=n$; therefore, $q^n\leq N_0<q^{n+1}$. Since $\mathbb{F}_q[T]$ is closed under addition, we can uniquely pair up the rest of polynomials of degree less than or equal to n by

$$p_N=p_a+p_{\widetilde{a}},$$

where $a,\widetilde{a}\in\mathbb{Z}_{\geq 0}$, $a<\widetilde{a}$. We collect all such pairs $(a,\widetilde{a})$ and form

$$A_N=\{a\in\mathbb{Z}_{\geq 0}: p_N=p_a+p_{\widetilde{a}},\ a<\widetilde{a},\ \text{and}\ \deg p_a,\deg p_{\widetilde{a}}\leq n\},$$
$$\widetilde{A}_N=\{\widetilde{a}\in\mathbb{Z}_{\geq 0}: p_N=p_a+p_{\widetilde{a}},\ a<\widetilde{a},\ \text{and}\ \deg p_a,\deg p_{\widetilde{a}}\leq n\}.$$

We have $|A_N|=|\widetilde{A}_N|=(q^{n+1}-1)/2$, and

$$\{0,\dots,q^{n+1}-1\}=A_N\cup\widetilde{A}_N\cup\{N_0\},$$

where the union is disjoint. Further, $\{0,1,\dots,q^n-1\}\subseteq A_N$, because if $0\leq a<q^n$, then p_a has degree at most $n-1$. Thus, the corresponding $p_{\widetilde{a}}$ must have degree n; therefore, $q^n\leq\widetilde{a}<q^{n+1}$. Hence,

$$\widetilde{A}_N\subseteq\{q^n,q^n+1,\dots,q^{n+1}-1\}. \tag{11}$$

Let $M:=M(N)=(q^{n+1}-1)/2$. For convenience we label the M elements of A_N by a_i, where $1\leq i\leq M$, and the corresponding elements of $\widetilde{A}_N$ by $\widetilde{a}_i$.

We also define

$$\lambda_N=\sum_{1\leq i\leq M}\alpha_{a_i}\alpha_{\widetilde{a}_i},\qquad \lambda'_N=\sum_{1\leq i\leq M}\frac{\alpha_{a_i}\alpha_{\widetilde{a}_i}}{1-\alpha_{a_i}\alpha_{\widetilde{a}_i}}.$$

Note that when $p=2$, for $N>0$, we do not have to consider the polynomial p_{N_0} as above. Thus we let $M:=M(N)=q^{n+1}/2$ and we can argue in a similar manner.

Define

$$s^*_N(\omega)=\sum_{m=0}^{N}\mathbf{1}_{\mathfrak{B}_m}(\omega),$$

where $\mathbf{1}_{\mathfrak{B}_m}$ is the characteristic function of $\mathfrak{B}_m$. Let $E(f)$ denote the expectation of a random variable f, defined by $E(f) = \int_X f\,dP$. We define

$$m_N^* = E(s_N^*) = \sum_{m=0}^{N} \alpha_m.$$

We will also assume that our sequence $\{\alpha_j\}$ satisfies:

HYPOTHESIS A. *The sequence $\{\alpha_j\}$ of probabilities (introduced in Theorem 10) satisfies the following conditions: $0 < \alpha_j < 1$ $(j \geq 0)$, $\{\alpha_j\}$ is monotonic and decreasing from some point onward (i.e. for $j \geq j_1$), and $\alpha_j \to 0$ as $j \to \infty$.*

We have the following result for $s_N^*(\omega)$ and its expected value m_N^*.

LEMMA 12. *If, in addition to Hypothesis* A,

$$m_N^* \to \infty \tag{13}$$

as $N \to \infty$, and

$$\sum_{N=0}^{\infty} \frac{\alpha_N}{(m_N^*)^2} < \infty, \tag{14}$$

then with probability 1, *we have $s_N^*(\omega) \sim m_N^*$ as $N \to \infty$.*

Proof. We denote by $D^2(f)$ the variance of a random variable f, defined by

$$D^2(f) = E\Big(\big(f - E(f)\big)^2\Big).$$

The proof is basically an application of the following variant of the strong law of large numbers [3, p. 140, Theorem 11]. Let $\{f_j\}$ be a sequence of independent random variables, and let

$$s_i(\omega) = \sum_{j=0}^{i} f_j(\omega) \qquad (i \geq 0).$$

Suppose that

$$E(f_j) > 0 \quad (j \geq 0), \qquad \lim_{i\to\infty} E(s_i) = \infty, \qquad \sum_{i=0}^{\infty} \frac{D^2(f_i)}{\big(E(s_i)\big)^2} < \infty.$$

Then, with probability 1,

$$s_i(\omega) = \big(1 + \mathbf{o}(1)\big)E(s_i)$$

as $i \to \infty$. We know that the sets $\mathfrak{B}_j$ are independent, which is equivalent to $\mathbf{1}_{\mathfrak{B}_j}(\omega)$ being independent. Thus we apply this theorem with $f_j(\omega) = \mathbf{1}_{\mathfrak{B}_j}(\omega)$, and obtain our result. ∎

As mentioned in Section 1, for every $N, d \in \mathbb{Z}_{\geq 0}$, we need to study the probability of the event

$$\mathfrak{e}(N,d)=\{\omega\in\Omega : r_N(\omega)=d\}.$$

We start with the following lemma.

LEMMA 15. *For all non-negative integers N and d, we have*

$$P\big(\mathfrak{e}(N,d)\big)=\Big(\prod_{1\le k\le M}(1-\alpha_{a_k}\alpha_{\widetilde{a}_k})\Big)\widetilde{\sigma}_d(N), \tag{16}$$

where $\widetilde{\sigma}_0(N)=1$ and, if $d\ge 1$,

$$\widetilde{\sigma}_d(N)=\sum_{1\le k_1<\cdots<k_d\le M}\ \prod_{1\le i\le d}\frac{\alpha_{a_{k_i}}\alpha_{\widetilde{a}_{k_i}}}{1-\alpha_{a_{k_i}}\alpha_{\widetilde{a}_{k_i}}}. \tag{17}$$

Proof. We begin with the case $d=0$. It is easy to see that

$$\mathfrak{e}(N,0)=\bigcap_{1\le k\le M}(\mathfrak{B}_{a_k}\cap\mathfrak{B}_{\widetilde{a}_k})^{\mathbf{c}},$$

where $\mathbf{c}$ denotes complement. Since the sets $\mathfrak{B}_j$ $(j\ge 0)$ are independent, so are $\mathfrak{B}_{a_k}\cap\mathfrak{B}_{\widetilde{a}_k}$ $(1\le k\le M)$, as $\{a_k : 1\le k\le M\}\cap\{\widetilde{a}_k : 1\le k\le M\}=\emptyset$. Thus, $(\mathfrak{B}_{a_k}\cap\mathfrak{B}_{\widetilde{a}_k})^{\mathbf{c}}$ $(1\le k\le M)$ are also independent. Hence,

$$P\big(\mathfrak{e}(N,0)\big)=\prod_{1\le k\le M}P\big((\mathfrak{B}_{a_k}\cap\mathfrak{B}_{\widetilde{a}_k})^{\mathbf{c}}\big)=\prod_{1\le k\le M}(1-\alpha_{a_k}\alpha_{\widetilde{a}_k}).$$

Suppose $1\le d\le M$ and $\omega'\in\mathfrak{e}(N,d)$. Then there exist $k_1,\dots,k_d$ such that $1\le k_i\le M$, $a_{k_i},\widetilde{a}_{k_i}\in\omega'$ $(1\le i\le d)$, and further, if $k\ne k_i$ and $1\le k\le M$, then either $a_k\notin\omega'$ or $\widetilde{a}_k\notin\omega'$. From this observation, we can deduce that

$$P\big(\mathfrak{e}(N,d)\big)=\sum_{1\le k_1<\cdots<k_d\le M}P\big(\mathfrak{E}(k_1,\dots,k_d)\big),$$

where

$$\mathfrak{E}(k_1,\dots,k_d)=\bigcap_{1\le i\le d}(\mathfrak{B}_{a_{k_i}}\cap\mathfrak{B}_{\widetilde{a}_{k_i}})\cap\bigcap_{\substack{1\le k\le M\\ k\ne k_i\,(1\le i\le d)}}(\mathfrak{B}_{a_k}\cap\mathfrak{B}_{\widetilde{a}_k})^{\mathbf{c}}.$$

Again, by independence,

$$\begin{aligned}P\big(\mathfrak{E}(k_1,\dots,k_d)\big)&=\prod_{1\le i\le d}P(\mathfrak{B}_{a_{k_i}}\cap\mathfrak{B}_{\widetilde{a}_{k_i}})\cdot\prod_{\substack{1\le k\le M\\ k\ne k_i\,(1\le i\le d)}}P\big((\mathfrak{B}_{a_k}\cap\mathfrak{B}_{\widetilde{a}_k})^{\mathbf{c}}\big)\\&=\prod_{1\le i\le d}\alpha_{a_{k_i}}\alpha_{\widetilde{a}_{k_i}}\cdot\prod_{\substack{1\le k\le M\\ k\ne k_i\,(1\le i\le d)}}(1-\alpha_{a_k}\alpha_{\widetilde{a}_k})\\&=\prod_{1\le k\le M}(1-\alpha_{a_k}\alpha_{\widetilde{a}_k})\cdot\prod_{1\le i\le d}\frac{\alpha_{a_{k_i}}\alpha_{\widetilde{a}_{k_i}}}{1-\alpha_{a_{k_i}}\alpha_{\widetilde{a}_{k_i}}},\end{aligned}$$

from which the desired result follows.

Finally, if $d > M$, then the sum $\widetilde{\sigma}_d(N)$ is empty, and both sides of (16) are 0. ∎

To estimate $\widetilde{\sigma}_d(N)$, we use the following result on elementary symmetric functions.

LEMMA 18 ([3, p. 147, Lemma 13]). *Let $y_1, \dots, y_{M'}$ be M' non-negative real numbers. For each positive integer $d \le M'$, let*

$$\sigma_d = \sum_{1 \le k_1 < \cdots < k_d \le M'} y_{k_1} \cdots y_{k_d}$$

be the dth elementary symmetric function of the y_k's. Then, for each d,

$$\frac{1}{d!}\sigma_1^d\left(1 - \binom{d}{2}\frac{1}{\sigma_1^2}\sum_{k=1}^{M'} y_k^2\right) \le \sigma_d \le \frac{1}{d!}\sigma_1^d \tag{19}$$

(where $\binom{d}{2}$ is 0 for $d = 1$).

The next lemma gives bounds on the probability of $\mathfrak{e}(N,d)$ in terms of λ_N and λ'_N.

LEMMA 20. *Let N and d be non-negative integers. Then*

$$P\big(\mathfrak{e}(N,d)\big) \le \frac{(\lambda'_N)^d}{d!}e^{-\lambda_N}. \tag{21}$$

Furthermore, if $d \le M$, then

$$P\big(\mathfrak{e}(N,d)\big) \ge \frac{(\lambda'_N)^d}{d!}e^{-\lambda'_N}\left(1 - \binom{d}{2}(\lambda'_N)^{-2}Q^*\right), \tag{22}$$

where

$$Q^* = \sum_{1 \le k \le M}\left(\frac{\alpha_{a_k}\alpha_{\widetilde{a}_k}}{1 - \alpha_{a_k}\alpha_{\widetilde{a}_k}}\right)^2$$

(and $\binom{d}{2}$ is 0 for $d = 0, 1$).

Proof. If $d > M$, then $\mathfrak{e}(N,d) = \emptyset$ and (21) is trivial. Suppose $1 \le d \le M$. We apply (19) with $M' = M$ and $y_k = \alpha_{a_k}\alpha_{\widetilde{a}_k}/(1 - \alpha_{a_k}\alpha_{\widetilde{a}_k})$ to estimate $\widetilde{\sigma}_d(N)$ in (16); noting that $\widetilde{\sigma}_1(N) = \lambda'_N$, we obtain

$$P\big(\mathfrak{e}(N,d)\big) \le \Big(\prod_{1 \le k \le M}(1 - \alpha_{a_k}\alpha_{\widetilde{a}_k})\Big)\frac{(\lambda'_N)^d}{d!},$$

and

$$P\big(\mathfrak{e}(N,d)\big) \ge \Big(\prod_{1 \le k \le M}(1 - \alpha_{a_k}\alpha_{\widetilde{a}_k})\Big)\frac{(\lambda'_N)^d}{d!}\left(1 - \binom{d}{2}(\lambda'_N)^{-2}Q^*\right).$$

Applying the inequality $e^{-t/(1-t)} < 1-t < e^{-t}$ (which holds for $0<t<1$) with $t = \alpha_{a_k}\alpha_{\widetilde{a}_k}$ $(1 \le k \le M)$, we obtain

$$e^{-\lambda'_N} < \prod_{1\le k\le M} (1 - \alpha_{a_k}\alpha_{\widetilde{a}_k}) < e^{-\lambda_N}, \tag{23}$$

and our result follows. When $d = 0$, we have

$$P\big(\mathfrak{e}(N,d)\big) = \prod_{1\le k\le M} (1 - \alpha_{a_k}\alpha_{\widetilde{a}_k}),$$

and the result is immediate from (23). ∎

To estimate λ_N and λ'_N, we first prove the following lemma.

LEMMA 24. *If Hypothesis* A *is satisfied, then*

$$\lambda'_N \sim \lambda_N \quad \text{as } N \to \infty. \tag{25}$$

Proof. Recall from (11) that if $1 \le k \le M$, then $q^n \le \widetilde{a}_k < q^{n+1}$. Consequently,

$$\alpha_{a_k}\alpha_{\widetilde{a}_k} < \alpha_{\widetilde{a}_k} \le \alpha_{q^n} = \mathbf{o}(1)$$

as $N \to \infty$. Therefore,

$$\begin{aligned}\lambda'_N - \lambda_N &= \sum_{1\le k\le M} \alpha_{a_k}\alpha_{\widetilde{a}_k}\left(\frac{1}{1-\alpha_{a_k}\alpha_{\widetilde{a}_k}} - 1\right)\\ &= \sum_{1\le k\le M} \alpha_{a_k}\alpha_{\widetilde{a}_k}\left(\frac{\alpha_{a_k}\alpha_{\widetilde{a}_k}}{1-\alpha_{a_k}\alpha_{\widetilde{a}_k}}\right) \le \alpha_{q^n}\lambda'_N,\end{aligned}$$

from which the result follows. ∎

Hence, it is enough to estimate λ_N. The following lemma gives an estimate sufficient for our purposes.

LEMMA 26. *Suppose that the sequence* $\{\alpha_j\}$ *in Theorem* 10 *is such that*

$$\alpha_j = \alpha\frac{(\log j)^{c'}}{j^c}$$

for $j \ge j_0$, *where* j_0, α, c, c' *are constants such that* $\alpha > 0$, $0 < \alpha_j < 1$ $(j \ge 0)$, $0 < c < 1$, *and* $c' \ge 0$. *Then, for sufficiently large* H, *there exist positive constants* D_1 *and* D_2, *which depend at most on* c, c', *and* q, *such that*

$$\alpha^2 D_1(\log N)^{2c'} q^{n(1-2c)} < \lambda_N < \alpha^2 D_2(\log N)^{2c'} q^{n(1-2c)} \tag{27}$$

for all $N > H$. *Furthermore,*

$$m^*_N \sim \frac{\alpha}{1-c}(\log N)^{c'} N^{1-c}. \tag{28}$$

Finally, if $c'=0$, then with probability 1, the numbers b_j in $\omega=\{p_{b_j}\}$ satisfy

$$b_j \sim \left(\frac{1-c}{\alpha}j\right)^{1/(1-c)} \qquad \text{as } j\to\infty. \tag{29}$$

Proof. We begin by finding a lower bound for λ_N. We assume $p\neq 2$; the case $p=2$ can be treated in a similar manner. Suppose $N>q(j_0+1)$, which implies $q^n>j_0$. Let C_0 and C_0' be the positive constants defined by

$$C_0=\sum_{1\le j<j_0}\alpha_j, \qquad C_0'=\sum_{1\le j<j_0}\frac{(\log j)^{c'}}{j^c}.$$

Since $q^n\le \widetilde{a}_i < q^{n+1}$, $0\le a_i<q^{n+1}$, and $(\log x)^{c'}/x^c$ is a decreasing function, we obtain

$$\begin{aligned}\lambda_N=\sum_{1\le i\le M}\alpha_{a_i}\alpha_{\widetilde{a}_i} &> \frac{\alpha(\log q^{n+1})^{c'}}{q^{(n+1)c}}\sum_{1\le i\le M}\alpha_{a_i}\\ &> \frac{\alpha^2(\log q^{n+1})^{c'}}{q^{(n+1)c}}\Bigg(\sum_{j=(q^{n+1}-1)/2}^{q^{n+1}-1}\frac{(\log j)^{c'}}{j^c}-C_0'\Bigg)\\ &> \frac{\alpha^2(\log q^{n})^{2c'}}{q^{(n+1)c}}\Bigg(\sum_{j=(q^{n+1}-1)/2}^{q^{n+1}-1}\frac{1}{j^c}-C_0'\Bigg).\end{aligned}$$

We know that for all $s,t\in\mathbb{N}$ with $0<s<t$,

$$\begin{aligned}&\frac{1}{1-c}(t+1)^{1-c}-\frac{1}{1-c}s^{1-c}\\ &\qquad\le\sum_{s\le j\le t}\frac{1}{j^c}\le\frac{1}{1-c}t^{1-c}-\frac{1}{1-c}(s-1)^{1-c}.\end{aligned} \tag{30}$$

Thus

$$\begin{aligned}\lambda_N &> \frac{\alpha^2(\log q^n)^{2c'}}{q^{(n+1)c}}\left(\frac{1}{1-c}(q^{n+1})^{1-c}-\frac{1}{1-c}\left(\frac{q^{n+1}-1}{2}\right)^{1-c}-C_0'\right)\\ &= \frac{\alpha^2(\log q^n)^{2c'}}{(1-c)q^c}q^{n(1-2c)}\left(q^{1-c}-\left(\frac{q}{2}-\frac{1}{2q^n}\right)^{1-c}-\frac{1-c}{q^{n(1-c)}}\cdot C_0'\right).\end{aligned} \tag{31}$$

Since $q^n\le N<q^{n+1}$, we have $\log N(1-\log q/\log N)<\log q^n$. It follows from (31) that taking H sufficiently large, we obtain

$$\lambda_N>\alpha^2\frac{q^{1-2c}}{2(1-c)}\left(1-\frac{1}{2^{1-c}}\right)(\log N)^{2c'}q^{n(1-2c)} \tag{32}$$

for all $N>H$.

Next, we would like to find an upper bound for λ_N. Again, since $q^n \le \widetilde{a}_i < q^{n+1}$ and $0 \le a_i < q^{n+1}$, by similar calculations we find

$$\lambda_N < \frac{\alpha(\log q^{n+1})^{c'}}{q^{nc}} \sum_{1\le i\le M} \alpha_{a_i} < \frac{\alpha(\log q^{n+1})^{c'}}{q^{nc}} \left(C_0 + \alpha \sum_{j=1}^{M} \frac{(\log q^{n+1})^{c'}}{j^c} \right).$$

Thus, by (30),

$$\begin{aligned}\lambda_N &< \frac{\alpha^2(\log q^{n+1})^{2c'}}{q^{nc}} \left(\frac{C_0}{\alpha(\log q^{n+1})^{c'}} + \frac{1}{1-c} \left(\frac{q^{n+1}-1}{2} \right)^{1-c} \right) \\ &= \frac{\alpha^2(\log q^{n+1})^{2c'}}{1-c} q^{n(1-2c)} \left(\frac{C_0(1-c)}{\alpha(\log q^{n+1})^{c'} q^{n(1-c)}} + \left(\frac{q}{2} - \frac{1}{2q^n} \right)^{1-c} \right).\end{aligned}$$

Hence, for H sufficiently large, we obtain

$$\lambda_N < \alpha^2 \frac{2^{2c'+1}}{(1-c)} \left(\frac{q}{2} \right)^{1-c} (\log q^n)^{2c'} q^{n(1-2c)}$$

for all $N > H$. Since $q^n \le N < q^{n+1}$, the first part of the lemma is proved.

Clearly,

$$m_N^* = \sum_{j=1}^{N} \alpha \frac{(\log j)^{c'}}{j^c} + \mathbf{O}(1) = \big(1 + \mathbf{o}(1)\big) \frac{\alpha}{1-c} (\log N)^{c'} N^{(1-c)},$$

and this proves (28). We note (28) shows that (13) and (14) are satisfied.

The final assertion of the lemma follows from (28), in view of Lemma 12 and the fact that $s_{b_j}^*(\omega) = j$ for $\omega = \{p_{b_j}\}_{j\in\mathbb{N}}$; for if $c' = 0$, with probability 1 we have

$$j = s_{b_j}^*(\omega) \sim m_{b_j}^* \sim \frac{\alpha}{1-c} b_j^{1-c},$$

or equivalently $b_j \sim \big(\frac{1-c}{\alpha} j\big)^{1/(1-c)}$. ∎

We will also make use of the following lemma.

Lemma 33 ([3, p. 149, Lemma 17]). *If $0 < \xi \le U$, then*

$$\sum_{d\ge U} \frac{\xi^d}{d!} \le \left(\frac{e\xi}{U} \right)^U,$$

and if $0 < V \le \xi$, then

$$\sum_{0\le d\le V} \frac{\xi^d}{d!} \le \left(\frac{e\xi}{V} \right)^V.$$

5. Proof of Theorem 7. Let $c = c' = 1/2$. We choose a number $\alpha > 0$ to satisfy

$$\alpha^2 \frac{q^{1-2c}}{2(1-c)} \left(1 - \frac{1}{2^{1-c}} \right) > 1.$$

We then define a sequence $\{\alpha_j\}$ by

$$\alpha_j = \alpha\left(\frac{\log j}{j}\right)^{1/2} \tag{34}$$

for all $j \geq j_0$, where j_0 is a positive integer so large that the expression in (34) is less than $1/2$ for all $j \geq j_0$. For $1 \leq j < j_0$, we let $\alpha_j = 1/2$. The precise value of α_j for small j is unimportant, but the above choices ensure $0 < \alpha_j < 1$, so that Hypothesis A is satisfied. By (32), for all N sufficiently large we have

$$\lambda_N \geq \alpha^2 D_1 \log N > \log N. \tag{35}$$

Hence, there exists $\delta > 0$ such that

$$e^{-\lambda_N} \ll N^{-1-\delta}. \tag{36}$$

We establish the theorem by showing that, with probability 1, $\log N \ll r_N(\omega) \ll \log N$ for large N, or equivalently (in view of Lemmas 24 and 26)

$$\lambda'_N \ll r_N(\omega) \ll \lambda'_N \tag{37}$$

for $N > N_0(\omega)$. We apply the Borel–Cantelli lemma twice to prove that each of the two assertions of (37) holds with probability 1. For this purpose, we must show that if C_1, C_2 are suitably chosen positive constants, then

$$\sum_{N=0}^{\infty} P(\{\omega \in \Omega : r_N(\omega) > C_1\lambda'_N\}) < \infty, \tag{38}$$

$$\sum_{N=0}^{\infty} P(\{\omega \in \Omega : r_N(\omega) < C_2\lambda'_N\}) < \infty. \tag{39}$$

By Lemmas 20 and 33, we have

$$P(\{\omega \in \Omega : r_N(\omega) > C_1\lambda'_N\}) \leq e^{-\lambda_N} \sum_{d \geq C_1\lambda'_N} \frac{(\lambda'_N)^d}{d!} \leq e^{-\lambda_N}\left(\frac{e}{C_1}\right)^{C_1\lambda'_N},$$

provided $C_1 \geq 1$. Thus, by choosing $C_1 = e$, we obtain a bound $e^{-\lambda_N}$ for the summand of (38), and the inequality (38) follows from (36).

On the other hand, again by Lemmas 20 and 33,

$$P(\{\omega \in \Omega : r_N(\omega) < C_2\lambda'_N\}) \leq e^{-\lambda_N} \sum_{0 \leq d \leq C_2\lambda'_N} \frac{(\lambda'_N)^d}{d!} \leq e^{-\lambda_N}\left(\frac{e}{C_2}\right)^{C_2\lambda'_N},$$

provided $C_2 \leq 1$. Thus, it suffices to show that C_2 can be chosen to satisfy, in addition to $0 < C_2 \leq 1$,

$$\left(\frac{e}{C_2}\right)^{C_2\lambda'_N} \ll N^{\delta/2};$$

for (39) will then follow from (36). By Lemmas 24 and 26, there exists $D > 0$ such that $\lambda'_N \le D \log N$ for N sufficiently large. Therefore, we only need to choose a small positive constant C_2 satisfying

$$\left(\frac{e}{C_2}\right)^{C_2} \le e^{\delta/(2D)},$$

which is certainly possible since $(e/t)^t \to 1$ as $t \to 0+$.

We have now shown that ω has each of the desired properties with probability 1, and this proves the theorem. ∎

6. Proof of Theorem 8. Let $\epsilon > 0$ be given. We define a sequence $\{\alpha_j\}$ by $\alpha_0 = 1/2$ and

$$\alpha_j = \frac{1}{2j^{1-1/(2+\epsilon)}}$$

for $j \ge 1$. It then follows by Lemma 26 (with $\alpha = 1/2$, $c = 1 - 1/(2+\epsilon)$, and $c' = 0$) that, with probability 1, $\omega = \{p_{b_j}\}$ satisfies $b_j \sim c^* j^{2+\epsilon}$, where c^* is some positive constant.

Since the sequence $\{\alpha_j\}$ satisfies Hypothesis A, we have $\lambda'_N \sim \lambda_N$ by Lemma 24. Thus, by Lemma 26 there exist positive constants D_1 and D_2 such that

$$D_1 q^{-\epsilon n/(2+\epsilon)} < \lambda_N, \lambda'_N < D_2 q^{-\epsilon n/(2+\epsilon)} \tag{40}$$

for N sufficiently large.

Again the Borel–Cantelli lemma implies that if a positive number K satisfies

$$\sum_{N=0}^{\infty} P(\{\omega \in \Omega : r_N(\omega) \ge K\}) < \infty, \tag{41}$$

then, with probability 1,

$$r_N(\omega) < K \quad \text{for } N > N_0(\omega).$$

We note that, by (40), $\lambda_N \to 0$ and $\lambda'_N \to 0$ as $N \to \infty$. Thus, by Lemmas 20 and 33,

$$P(\{\omega \in \Omega : r_N(\omega) \ge K\}) \le e^{-\lambda_N} \sum_{d \ge K} \frac{(\lambda'_N)^d}{d!} \le e^{-\lambda_N} \left(\frac{e\lambda'_N}{K}\right)^K \ll (\lambda'_N)^K$$

for N sufficiently large. Since $q^n \le N < q^{n+1}$, we have

$$(\lambda'_N)^K \le D_2^K q^{-\epsilon n K/(2+\epsilon)} \ll N^{-\epsilon K/(2+\epsilon)}.$$

Therefore, provided $\epsilon K/(2+\epsilon) > 1$, or equivalently

$$K > 1 + 2\epsilon^{-1},$$

it is clear that (41) is achieved. Accordingly, with probability 1,

$$r_N(\omega) < 2(1+\epsilon^{-1})$$

for $N > N_1(\epsilon,\omega)$. ∎

7. Proof of Theorem 9. Recall we defined

$$t_N(\omega) = |\{(a,b) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} : p_a, p_b \in \omega,\ p_N = p_a - p_b, \\ \deg p_a, \deg p_b \leq \deg p_N\}|.$$

As before, given $p_N \in \mathbb{F}_q[T]$, we let $n := n(N) = \deg p_N = \lfloor \log_q N \rfloor$. It is clear that for $p_N \neq 0$, there exist q^{n+1} pairs of polynomials (p_a, p_b) such that $p_N = p_a - p_b$ and $\deg p_a, \deg p_b \leq n$. Also, every polynomial of degree $\leq n$ will appear as p_a and p_b exactly once. Let $S_{\widehat{u},n}$ denote the set of all polynomials in $\mathbb{F}_q[T]$ of degree $\leq n$, and whose coefficient of T^n is $\widehat{u} \in \mathbb{F}_q$. Clearly, $|S_{\widehat{u},n}| = q^n$. If we consider each polynomial in $S_{\widehat{u},n}$ as p_b, then the corresponding set of p_a's is $S_{u,n}$ for some $u \neq \widehat{u}$ as $\deg p_N = n$.

For each $u \in \mathbb{F}_q$, we consider

$$t_{N,u}(\omega) = |\{(a,b) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} : p_N = p_a - p_b,\ p_a, p_b \in \omega \text{ and } p_a \in S_{u,n}\}|.$$

If $p_N = p_a - p_b$, we relabel p_b as $p_{\widehat{a}}$ to make its correspondence with p_a more explicit. We form the following two disjoint sets:

$$\mathcal{A}_N = \{a \in \mathbb{Z}_{\geq 0} : p_a \in S_{u,n}\} = \{\iota^{-1}(u)q^n, \dots, (\iota^{-1}(u)+1)q^n - 1\},$$
$$\widehat{\mathcal{A}}_N = \{\widehat{a} \in \mathbb{Z}_{\geq 0} : p_{\widehat{a}} \in S_{\widehat{u},n}\} = \{\iota^{-1}(\widehat{u})q^n, \dots, (\iota^{-1}(\widehat{u})+1)q^n - 1\}.$$

Let $M_0 := M_0(N) = |\mathcal{A}_N| = |\widehat{\mathcal{A}}_N| = q^n$. For convenience, we label the M_0 elements of $\mathcal{A}_N$ by a_i $(1 \leq i \leq M_0)$, and the corresponding elements of $\widehat{\mathcal{A}}_N$ by $\widehat{a}_i$, in other words we have $p_N = p_{a_i} - p_{\widehat{a}_i}$ $(1 \leq i \leq M_0)$.

We also define

$$\lambda_{N,u} = \sum_{1 \leq i \leq M_0} \alpha_{a_i}\alpha_{\widehat{a}_i}, \qquad \lambda'_{N,u} = \sum_{1 \leq i \leq M_0} \frac{\alpha_{a_i}\alpha_{\widehat{a}_i}}{1 - \alpha_{a_i}\alpha_{\widehat{a}_i}}.$$

With this set-up we can recover analogues of all the previous lemmas in terms of M_0, $\lambda_{N,u}$, $\lambda'_{N,u}$, and $t_{N,u}(\omega)$, in place of M, λ_N, λ'_N, and $r_N(\omega)$, respectively. Therefore, by a similar argument we obtain Theorem 8 with $t_{N,u}(\omega)$ in place of $r_N(\omega)$. Since this result holds with probability 1, and

$$t_N(\omega) = \sum_{u \in \mathbb{F}_q} t_{N,u}(\omega),$$

we have our result. ∎

Acknowledgements. The authors would like to thank the anonymous referee for careful reading and making many useful suggestions on writing and references.

The research of the first author was partially supported by an NSERC discovery grant.

References

[1] P. Erdős, *On a problem of Sidon in additive number thoery*, Acta Sci. Math. (Szeged) 15 (1954), 255–259.
[2] P. Erdős and A. Rényi, *Additive properties of random sequences of positive integers*, Acta Arith. 6 (1960), 83–110.
[3] H. Halberstam and K. F. Roth, *Sequences*, Springer, New York, 1983.
[4] K. E. Hare and S. Yamagishi, *A generalization of a theorem of Erdős–Rényi to m-fold sums and differences*, Acta Arith. 166 (2014), 55–67.
[5] A. Sárközy and V. T. Sós, *On additive representation functions*, in: The Mathematics of Paul Erdős, I, 2nd ed., Springer, New York, 2013, 233–262.

Wentang Kuo, Shuntaro Yamagishi
Department of Pure Mathematics
University of Waterloo
Waterloo, ON, N2L 3G1, Canada
E-mail: wtkuo@uwaterloo.ca
syamagis@uwaterloo.ca