Bull. Aust. Math. Soc. **106** (2022), 376–384
doi:10.1017/S0004972722000752

ON LINEARISED POLYNOMIALS, SIDON ARRAYS AND FAST CONSTRUCTION OF SIDON SETS

CESAR ANDRADE, YAMIDT BERMUDEZ✉ and CARLOS TRUJILLO

(Received 11 February 2022; accepted 5 July 2022; first published online 30 August 2022)

Abstract

A Sidon set is a subset of an Abelian group with the property that the sums of two distinct elements are distinct. We relate the Sidon sets constructed by Bose to affine subspaces of $\mathbb{F}_{q^2}$ of dimension one. We define Sidon arrays which are combinatorial objects giving a partition of the group $\mathbb{Z}_{q^2}$ as a union of Sidon sets. We also use linear recurring sequences to quickly obtain Bose-type Sidon sets without the need to use the discrete logarithm.

2020 *Mathematics subject classification*: primary 11B13; secondary 11T06.

Keywords and phrases: Sidon sets, linear recurrences, finite fields.

1. Introduction

In number theory, a Sidon set (or Sidon sequence), named after the Hungarian mathematician Szimon Szidon, is a set $A = \{a_0, a_1, a_2, \ldots\}$ of natural numbers in which all pairwise sums $a_i + a_j$ $(i \leq j)$ are different. Sidon introduced the concept in his investigations of Fourier series. This notion has been generalised: in an abelian group G, a subset A is a $B_h[g]$-set if, for any element x of G, the number of h-tuples of elements of A of sum x is less than or equal to g. The main problem in the study of Sidon sets is to find the largest number of elements a Sidon set can have which are smaller than some given number x.

There are several constructions of Sidon sets (for a complete summary, see [9]). We will concentrate on the construction of Bose [1] using finite affine geometry. Let q be any prime power and γ a generator of $\mathbb{F}_{q^2}^{\times}$ and define the set

$$B(q, \gamma) := \{a \in [q^2 - 1] \colon \gamma^a - \gamma \in \mathbb{F}_q\}.$$

Bose [1] showed that $B(q, \gamma)$ is a Sidon set.

The discrete logarithm function is defined by

$$\begin{aligned} \mathrm{Log}_\gamma : (\mathbb{F}_{q^2}^*, \times) &\longrightarrow (\mathbb{Z}_{q^2-1}, +) \\ \gamma^k &\longmapsto \mathrm{Log}_\gamma(\gamma^k) = k. \end{aligned}$$

So the Sidon set $B(q,\gamma)$ is $B(q,\gamma) = \{\mathrm{Log}_\gamma(\alpha + a) : a \in \mathbb{F}_q\}$.

However, the condition $\gamma^a - \gamma \in \mathbb{F}_q$ implies that $(\gamma^a - \gamma)^q = \gamma^a - \gamma$, or equivalently

$$(\gamma^a)^q - \gamma^a - (\gamma^q + \gamma) = 0,$$

which means that γ^a is a root of the polynomial $f(x) = x^q - x + \beta$ where $\beta = \gamma^q + \gamma$. This fact will be used in our construction later.

We relate the Sidon sets constructed by Bose [1] with affine subspaces of $\mathbb{F}_{q^2}$ of dimension one. We define *Sidon arrays* which are combinatorial objects giving a partition of the group $\mathbb{Z}_{q^2}$ as a union of Sidon sets. Sidon arrays are related to the Sidon spaces constructed in [10] and used there to describe cyclic subspace codes. We take a different approach inspired by Bose's construction of Sidon sets. We also use linear recurring sequences to quickly obtain Bose-type Sidon sets without the need to use the discrete logarithm. Our method is as fast as the one described in [7], at least when q is a prime.

The article is organised as follows. In Section 2, we review facts about linearised polynomials and their relation with subspaces of $\mathbb{F}_{q^2}$ defined over $\mathbb{F}_q$ and we prove our main result Theorem 2.5. In Section 3, we define the concept of Sidon array and we give some examples. Section 4 is devoted to the fast construction of Bose-type Sidon sets.

2. Linearised polynomials and Sidon sets

We start by recalling some elementary facts about linearised polynomials (for a detailed exposition, we refer to [6, Ch. 3]).

Let $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ be the finite fields with q and q^m elements, respectively, where q is a prime or a prime power. Polynomials over $\mathbb{F}_{q^m}$ of the form

$$L(x) := \sum_{i=0}^{n} c_i x^{q^i}, \quad n \in \mathbb{N},$$

are often known as q-polynomials or linearised polynomials. This terminology stems from the following property: if F is an arbitrary extension field of $\mathbb{F}_{q^m}$, then

$$\begin{aligned} L(\alpha+\beta) &= L(\alpha) + L(\beta) \quad \text{for all } \alpha,\beta \in F, \\ L(c\alpha) &= cL(\alpha) \quad \text{for all } c \in \mathbb{F}_q \text{ and all } \alpha \in F. \end{aligned}$$

So these special polynomials induce linear transformations of $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$. An important example of a linearised polynomial is the so-called trace polynomial

$$\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{q^i}$$

defining the trace function of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. The following well-known theorem shows the special character of the set of roots of a linearised polynomial.

https://doi.org/10.1017/S0004972722000752 Published online by Cambridge University Press

THEOREM 2.1 [6, Ch. 3]. *Let $L(x)$ be a nonzero linearised polynomial over $\mathbb{F}_{q^m}$ and let the extension field $\mathbb{F}_{q^s}$ of $\mathbb{F}_{q^m}$ contain all the roots of $L(x)$. Then each root of $L(x)$ has the same multiplicity, which is either 1 or a power of q, and the roots form a linear subspace of $\mathbb{F}_{q^s}$, regarded as a vector space over $\mathbb{F}_q$. Reciprocally, let U be a linear subspace of $\mathbb{F}_{q^m}$, considered as a vector space over $\mathbb{F}_q$. Then for any nonnegative integer k, the polynomial*

$$L(x) = \prod_{\beta \in U} (x - \beta)^k$$

is a linearised polynomial over $\mathbb{F}_{q^m}$.

A polynomial of the form $A(x) = L(x) + \alpha$, where $L(x)$ is a linearised polynomial over $\mathbb{F}_{q^m}$ and $\alpha \in \mathbb{F}_{q^m}$, is called an *affine q-polynomial* over $\mathbb{F}_{q^m}$. As in the case of linearised polynomials, there is an analogue of Theorem 2.1.

THEOREM 2.2 [6, Ch. 3]. *Let $A(x)$ be an affine q-polynomial over $\mathbb{F}_{q^m}$ and let the extension field $\mathbb{F}_{q^s}$ of $\mathbb{F}_{q^m}$ contain all the roots of $A(x)$. Then each root of $A(x)$ has the same multiplicity, which is either 1 or a power of q, and the roots form an affine subspace of $\mathbb{F}_{q^s}$, regarded as a vector space over $\mathbb{F}_q$. Reciprocally, let T be an affine subspace of $\mathbb{F}_{q^m}$, considered as a vector space over $\mathbb{F}_q$. Then for any nonnegative integer k, the polynomial*

$$A(x) = \prod_{\beta \in T} (x - \beta)^{q^k}$$

is an affine q-polynomial over $\mathbb{F}_{q^m}$.

REMARK 2.3. The polynomial $f(x) = x^q - x + \beta$ in Bose's construction is an affine q-polynomial over $\mathbb{F}_{q^2}$, so it defines an affine line in $\mathbb{F}_{q^2}$.

In this paper, we are interested in the special case $L(x) = x^q + ax$ defined over $\mathbb{F}_{q^2}$. If L splits completely over $\mathbb{F}_{q^2}$, then its roots have multiplicity one and form a vector space of dimension one over $\mathbb{F}_q$, that is to say a line, denoted by $\mathcal{L}$. Let $\mathcal{A}$ be the affine line associated to the affine q-polynomial $A(x) = x^q + ax + b$, when it splits completely over $\mathbb{F}_{q^2}$.

Consider a line $\mathcal{L} \subset \mathbb{F}_{q^2}$, that is, $\mathcal{L} = \mathrm{Gen}(\theta) := \{a\theta : a \in \mathbb{F}_q\}$ for some nonzero $\theta \in \mathbb{F}_{q^2}$. Then for every $\delta \in \mathbb{F}_{q^2} \setminus \mathcal{L}$, the set $\mathcal{A} := \mathcal{L} + \delta$ is an affine line. Fix once and for all a primitive element γ in $\mathbb{F}_{q^2}^{\times}$.

Before stating and proving our main result, we require the following simple lemma.

LEMMA 2.4 [4, page 323]. *If $\alpha_1, \alpha_2, \alpha_3$ and $\alpha_4 \in \mathbb{F}_q$ are distinct, then the relations*

$$\alpha_1\alpha_2 = \alpha_3\alpha_4, \quad \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 \tag{2.1}$$

cannot hold simultaneously. In other words, any solution $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \in \mathbb{F}_q^4$ of (2.1) satisfies $\alpha_1 \in \{\alpha_3, \alpha_4\}$.

https://doi.org/10.1017/S0004972722000752 Published online by Cambridge University Press

THEOREM 2.5. *Let γ be a primitive element in $\mathbb{F}_{q^2}^{\times}$ and let $\theta, \delta \in \mathbb{F}_{q^2}^{\times}$ be such that $\delta \notin \mathcal{L} = \mathrm{Gen}(\theta)$. Then the set*

$$\mathcal{S} := \mathrm{Log}_{\gamma}(\mathcal{A}) = \{\mathrm{Log}_{\gamma}(\alpha\theta + \delta) \mid \alpha \in \mathbb{F}_q\},$$

where $\mathcal{A} := \mathcal{L} + \delta$, is a Sidon set modulo $q^2 - 1$.

PROOF. Let a_1, a_2, a_3, a_4 be any four different elements in $\mathcal{S}$ such that $a_1 + a_2 = a_3 + a_4$. Since the sum is taken modulo $q^2 - 1$ and γ is primitive, the powers of γ^i are different for $1 \le i \le q^2 - 1$ and $\gamma^{a_1} \cdot \gamma^{a_2} = \gamma^{a_3} \cdot \gamma^{a_4}$.

Since the γ^{a_i} terms are different elements of $\mathbb{F}_{q^2}$ and by construction also belong to $\mathcal{A}$, there exist distinct $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}_q$ such that $(\alpha_1\theta + \delta)(\alpha_2\theta + \delta) = (\alpha_3\theta + \delta)(\alpha_4\theta + \delta)$, that is,

$$\alpha_1\alpha_2\theta^2 + (\alpha_1 + \alpha_2)\theta\delta + \delta^2 = \alpha_3\alpha_4\theta^2 + (\alpha_3 + \alpha_4)\theta\delta + \delta^2. \tag{2.2}$$

Equation (2.2) is equivalent to

$$(\alpha_1\alpha_2 - \alpha_3\alpha_4)\theta = (\alpha_3 + \alpha_4 - \alpha_1 - \alpha_2)\delta.$$

By Lemma 2.4, the expressions $\alpha_1\alpha_2 - \alpha_3\alpha_4$ and $\alpha_3 + \alpha_4 - \alpha_1 - \alpha_2$ are not zero simultaneously, so we can write

$$\delta = \frac{b}{a}\theta, \tag{2.3}$$

where $b = \alpha_1\alpha_2 - \alpha_3\alpha_4$ and $a = \alpha_3 + \alpha_4 - \alpha_1 - \alpha_2$. Since $b/a \in \mathbb{F}_q$, (2.3) implies $\delta \in \mathrm{Gen}(\theta)$, which contradicts our hypothesis and proves our claim. □

REMARK 2.6. Let us consider the linearised polynomial $f(x) = x^q - x$, which decomposes completely in $\mathbb{F}_{q^2}$. Its roots are all the elements of $\mathbb{F}_q$, so the affine polynomial $g(x) = f(x - a)$ is also reducible and

$$f(x - a) = x^q - a^q - (x - a) = x^q - x - (a^q + a).$$

Setting $\beta = a^q + a$, a straightforward calculation shows that β has trace 0 and we get Bose's construction as a particular case.

EXAMPLE 2.7. Let us consider $q = p = 5$. The polynomial $p(x) = x^2 + 4x + 2$ is primitive over $\mathbb{F}_5$. Let γ be a root of $p(x)$, so that γ is a primitive element. The polynomial $A(x) = x^5 + \gamma^{16}x + \gamma^{14}$ splits completely over $\mathbb{F}_{5^2}$ with roots $\{\gamma^4, \gamma^6, \gamma^{11}, \gamma^{14}, \gamma^{15}\}$, so the set $\mathcal{S} := \{4, 6, 11, 14, 15\}$ is a Sidon set modulo 24.

3. Linearised polynomials and Sidon arrays

In this section, we define new objects which we have called *Sidon arrays*. We first make some further remarks on the linearised polynomials that appear in the construction of Sidon sets in the previous section. We need the following lemma giving conditions for the polynomial $x^q + ax$ to factorise completely over $\mathbb{F}_{q^2}$.

https://doi.org/10.1017/S0004972722000752 Published online by Cambridge University Press

LEMMA 3.1 (see [6, Theorem 2.24 and Exercise 2.14]). *The polynomial* $L(x) = x^q + ax$ *in* $\mathbb{F}_{q^2}[x]$ *splits completely over* $\mathbb{F}_{q^2}$ *if and only if there exists* $\beta \in \mathbb{F}_{q^2}$ *such that* $a = \beta^{q-1}$.

Using Lemma 3.1 and since $f(x) = b^{-q}\mathrm{Tr}(bx) = \prod_{i=1}^{q}(x - b^{-1}\lambda_i)$, the roots of f can be written as $\beta\lambda_j$ for β a $(q+1)$th root of unity and λ_j ranging over all trace zero elements in $\mathbb{F}_{q^2}$.

REMARK 3.2. The roots of a q-polynomial of the form $x^q + ax$ form a vector subspace of dimension one over $\mathbb{F}_q$ and therefore an additive normal subgroup $\mathcal{G}_a$ of $\mathbb{F}_{q^2}$ with q elements. Thus, $\mathbb{F}_{q^2}$ is the union of q different classes, that is,

$$\mathbb{F}_{q^2} = \bigcup_{i=1}^{q}(c_i + \mathcal{G}_a)$$

with the convention that $c_1 = 0$ corresponds to the class of $\mathcal{G}_a$.

By Theorem 2.2, the q elements of a class $c_i + \mathcal{G}_a$ are the roots of an affine polynomial of the form $f(x) = x^q + ax + b$. Since c_i belongs to at least one line, there is a linearised polynomial $L(x)$ that has c_i as one of its roots. By the description given above for the roots of $L(x)$, we can also characterise the roots of the affine polynomial $f(x)$ as $\theta\lambda + \beta\mathcal{G}_0$, where $\mathcal{G}_0$ is the additive subgroup in $\mathbb{F}_{q^2}$ of trace zero elements, β and θ are $(q+1)$th roots of unity and $\lambda \in \mathcal{G}_0$ is such that $\theta\lambda \notin \beta\mathcal{G}_0$.

By Remark 3.2, the elements of $\mathbb{F}_{q^2}$ can be organised in a $q \times q$ matrix $\mathcal{S}$ such that the ith row is the class $(c_i + \mathcal{G}_a)$. Recall that the elements of $\mathcal{G}_a$ are of the form $\beta\lambda_j$, where β is a $(q+1)$th root of unity and λ_j ranges over all trace zero elements in $\mathbb{F}_{q^2}$. So the entries of $\mathcal{S}$ are $s_{i,j} = c_i + \beta\lambda_j$.

DEFINITION 3.3. A Sidon array of order q is a matrix of order $q \times q$ whose entries are all integers in the interval $[0, q^2 - 1]$ such that any row or column other than the first row and first column is a Sidon set modulo $q^2 - 1$.

From the comments and Remark 3.2, Sidon arrays of order q exist and they can be constructed as indicated above.

EXAMPLE 3.4. Let us consider $q = p = 5$. The polynomial $p(x) = x^2 + 4x + 2$ is primitive over $\mathbb{F}_5$ with root γ. Take $a = \gamma^{16}$. Then $\mathcal{G}_a = \{0, \gamma^{19}\gamma, \gamma^7, \gamma^{13}\}$ is the set of roots of $f(x) = x^5 + \gamma^{16}x$. The elements of $\mathbb{F}_{q^2}$ can be organised as in Table 1.

Taking logarithms, with the convention $\mathrm{Log}_\gamma(0) = 24$, gives Table 2.

It can be verified that the table meets the conditions for a Sidon array. In fact, the second row corresponds to the set obtained in Example 2.7, as logarithms of the roots of the polynomial $A(x) = x^5 + \gamma^{16}x + \gamma^{14}$.

Sidon arrays are a refinement of the partitions in the case $h = 2$ introduced by Gilberto *et al.* [5]. They proved the following theorem.

THEOREM 3.5 [5]. *There is a partition of* $\mathbb{Z}_{q^h}$ *into* B_d *sets modulo* $q^h - 1$ *where* d *runs through the divisors of* h.

https://doi.org/10.1017/S0004972722000752 Published online by Cambridge University Press

TABLE 1. A Sidon array modulo 25 before taking logarithms.

0	γ^{19}	γ	γ^{7}	γ^{13}
γ^{11}	γ^{15}	γ^{14}	γ^{6}	γ^{4}
γ^{17}	γ^{10}	γ^{21}	γ^{20}	γ^{12}
γ^{23}	γ^{18}	γ^{16}	γ^{3}	γ^{2}
γ^{5}	γ^{8}	γ^{0}	γ^{22}	γ^{9}

TABLE 2. A Sidon array modulo 25.

24	19	1	7	13
11	15	14	6	4
17	10	21	20	12
23	18	16	3	2
5	8	0	22	9

In our case, taking $h = 2$, we have a partition of $\mathbb{Z}_{q^2}$ modulo $q^2 - 1$ as B_2 sets, that is, Sidon sets.

A *Golomb ruler* G_k of order k is an ordered set of k integers $(a_1, a_2, \ldots, a_k)$ such that $0 \le a_1 < a_2 < \cdots < a_k$ and all the differences $\{a_i - a_j \mid 1 \le j < i \le k\}$ are distinct. A (v, k)-*modular Golomb ruler* is an ordered set of k integers $(a_1, a_2, \ldots, a_k)$ such that $0 \le a_1 < a_2 < \cdots < a_k$ and all the differences $\{a_i - a_j \mid 1 \le j < i \le k,\ i \ne j\}$ are distinct and nonzero modulo v.

Sidon sets are widely used in the construction of Golomb rulers and modular Golomb rulers (see [2, 3, 8]). In this context, *disjoint Golomb rulers* (see [11]) are similar to Sidon arrays. This is another reason for our interest in Sidon arrays, since they could have similar properties and applications as disjoint Golomb Rulers.

4. Linear recurrences and fast construction of Sidon sets

We begin this section with the definition and properties of recurrence relations, which we need for our applications. For more details, see [6, Ch. 6].

DEFINITION 4.1. Let $k \in \mathbb{N}$. A sequence $s_0, s_1, \ldots$ of elements of $\mathbb{F}_q$ is called a linear recurring sequence of order k in $\mathbb{F}_q$ if there are elements $a, a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_q$ such that

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_0 s_n + a. \tag{4.1}$$

The terms $s_0, s_1, \ldots, s_{k-1}$ determining the sequence are called *initial values*. Equation (4.1) is called a *linear recurrence relation of order k*. If $a = 0$ it is called *homogeneous*, otherwise it is called *nonhomogeneous*. The vector $(s_n, s_{n+1}, \ldots, s_{n+k-1})$

https://doi.org/10.1017/S0004972722000752 Published online by Cambridge University Press

is called an nth state vector; in particular, $(s_0, s_1, \ldots, s_{k-1})$ is called an initial state vector. Linear recurring sequences in $\mathbb{F}_q$ are eventually periodic. More precisely, we have the following result.

THEOREM 4.2 (see [6, page 194]). *If $s_0, s_1, \ldots$ is a linear recurring sequence in a finite field satisfying the linear recurrence relation (4.1) and if the coefficient a_0 is nonzero, then the sequence $s_0, s_1, \ldots$ is periodic.*

Suppose that the affine polynomial $f(x) = x^q + ax + b$ factorises as a product of linear polynomials over $\mathbb{F}_{q^2}$, so its roots lie on an affine line and therefore their discrete logarithms form a Sidon set modulo $q^2 - 1$. As remarked above, $f(x) = \beta^{-q}\mathrm{Tr}(\beta x + \alpha)$ for some nonzero $\beta, \alpha \in \mathbb{F}_{q^2}$. So if θ is a root of $f(x)$, then it is also a root of $\mathrm{Tr}(\beta x + \alpha)$. We will use this fact to give a fast construction of Sidon sets without the need to take discrete logarithms.

Fix a primitive element γ of $\mathbb{F}_{q^2}$ and define the sequence $s_i := \mathrm{Tr}(\beta\gamma^i + \alpha) \in \mathbb{F}_q$. By the properties of the trace polynomial, it is easy to prove that the sequence s_i is periodic with period $q^2 - 1$ and therefore a linear recurring sequence of order k in $\mathbb{F}_q$ for some k. The next theorem follows from the above discussion and the construction in Section 2.

THEOREM 4.3. *Let s_i be the sequence defined above. Then the set $\mathcal{S}$ defined by $\mathcal{S} := \{i \pmod{q^2 - 1} \mid s_i = 0\}$ is a Sidon set modulo $q^2 - 1$.*

Although the definition of the set does not involve discrete logarithms, there is still the problem of evaluating the trace polynomial and calculating all the powers of the primitive element γ. Using the fact that the sequence is recurrent, we can reduce our problem to calculate only the initial values of the recurrence, with the rest reduced to arithmetic on $\mathbb{F}_q$.

Since γ is a primitive element, there exist n_0 and m_0 such that $\beta = \gamma^{n_0}$ and $\alpha = \gamma^{m_0}$. In $\mathbb{F}_q$,

$$s_i = \mathrm{Tr}(\beta\gamma^i + \alpha) = \mathrm{Tr}(\beta\gamma^i) + \mathrm{Tr}(\alpha) = \mathrm{Tr}(\gamma^{n_0}\gamma^i) + \mathrm{Tr}(\gamma^{m_0}) = t_{i+n_0} + t_{m_0},$$

where $t_i := \mathrm{Tr}(\gamma^i)$ is the sequence given by the trace. Also, t_i is periodic with period $q^2 - 1$.

Let $p(x) = x^2 - a_1 x - a_0 \in \mathbb{F}_q[x]$ be the minimal polynomial of γ. Then we have $\gamma^2 = a_1\gamma + a_0$ and multiplying by γ^i gives $\gamma^{i+2} = a_1\gamma^{i+1} + a_0\gamma^i$. Taking the trace on both sides,

$$t_{i+2} = \mathrm{Tr}(\gamma^{i+2}) = \mathrm{Tr}(a_1\gamma^{i+1} + a_0\gamma^i) = a_1\mathrm{Tr}(\gamma^{i+1}) + a_0\mathrm{Tr}(\gamma^i) = a_1 t_{i+1} + a_0 t_i. \tag{4.2}$$

That is, the recurrence has order 2 and the coefficients of the recurrence are the coefficients of the minimal polynomial $p(x)$. So we only need to find the initial values t_0 and t_1:

$$t_0 = \mathrm{Tr}(\gamma^0) = 1^q + 1 = 2, \quad t_1 = \mathrm{Tr}(\gamma) = \gamma^q + \gamma = -a_1,$$

the last equation because γ and γ^q are conjugates. Thus the sequence s_i is completely determined. However, this is not yet an effective method because if n_0 and m_0 are large,

https://doi.org/10.1017/S0004972722000752 Published online by Cambridge University Press

we need to calculate many terms of the recurrence t_i. Instead, we use the particular case $\beta = 1$, that is, we consider the sequence $s_i = \mathrm{Tr}(x + \alpha) = t_i + t_{m_0}$. Set $b = t_{m_0}$ so that $t_i = s_i - b$. Substituting this in (4.2) gives

$$\begin{aligned} s_{n+2} &= a_1(s_{n+1} - b) + a_0(s_n - b) + b \\ &= a_1 s_{n+1} + a_0 s_n + b(1 - a_1 - a_0) \\ &= a_1 s_{n+1} + a_0 s_n + bp(1). \end{aligned}$$

From this discussion, we derive the following result.

THEOREM 4.4. *Let $b \in \mathbb{F}_q$ and $f(x) = x^2 - a_1 x - a_0 \in \mathbb{F}_q[x]$ be a primitive polynomial. Define the nonhomogeneous sequence $s_{n+2} = a_1 s_{n+1} + a_0 s_n + a$ with $s_0 = 2 + b$, $s_1 = -a_1 + b$ and $a = bf(1)$. Then the set $\mathcal{S} := \{i \pmod{(q^2 - 1)} \mid s_i = 0\}$ is a Sidon set modulo $q^2 - 1$.*

The result of the previous theorem can be described algorithmically as shown in Algorithm 1.

ALGORITHM 1: `SidonSets`

Input: $b \in \mathbb{F}_q$ and $f(x) = x^2 - a_1 x - a_0 \in \mathbb{F}_q[x]$, a primitive polynomial.
Output: A set $\mathcal{S}$ which is a Sidon set modulo $q^2 - 1$ with q elements.

1: Set the initial values $s_0 = 2 + b$, $s_1 = -a_1 + b$ and the term $a = bf(1)$ of the nonhomogeneous recurrence sequence.
2: Set $\mathcal{S} = \{\}$.
3: Calculate the remaining values of the recurrence sequence with the formula $s_{n+2} = a_1 s_{n+1} + a_0 s_n + a$ (noting that it has period $q^2 - 1$).
4: Find the integers i modulo $q^2 - 1$ such that $s_i = 0$.
5: Put the integer i of the previous step in $\mathcal{S}$.
6: Return $\mathcal{S}$.

Algorithm 1 requires calculation of $O(q^2)$ terms to form the period and the calculations being done in $\mathbb{F}_q$. In [7, Theorem 2.1], the author shows that Bose-type Sidon sets can be constructed without taking logarithms, only calculating certain powers and doing arithmetic modulo $q^2 - 1$, that is, with the same complexity. When $q = p$ with p prime, [7] also gives a fast criterion to construct primitive polynomials.

EXAMPLE 4.5. Let us consider $q = p = 5$. The polynomial $p(x) = x^2 + 4x + 2$ is irreducible over $\mathbb{F}_5$ and primitive. Taking $b = 2$, we construct the first 25 terms of the sequence $\{4, 1, 2, 4, 4, 0, 1, 0, 2, 1, 1, 3, 0, 3, 2, 0, 0, 4, 3, 4, 2, 3, 3, 1\}$ and get the set $\mathcal{S} := \{5, 7, 12, 15, 16\}$ which is a Sidon set modulo 24. This can be found by considering the polynomial $x^5 + \gamma^{20}x + \gamma^{19}$ with γ a root of $p(x)$.

https://doi.org/10.1017/S0004972722000752 Published online by Cambridge University Press

References

[1] R. C. Bose, 'An affine analogue of Singer's theorem', *J. Indian Math. Soc. (N.S.)* **6** (1942), 1–15.
[2] Y. Caicedo, C. A. Martos and C. A. Trujillo, 'g-Golomb rulers', *Rev. Integr.* **33** (2015), 161–172.
[3] A. A. Davydov, G. Faina, M. Giulietti, S. Marcugini and F. Pambianco, 'On constructions and parameters of symmetric configurations v_k', *Des. Codes Cryptogr.* **80** (2016), 125–147.
[4] M. J. Ganley, 'Direct product difference sets', *J. Combin. Theory Ser. A* **23** (1977), 321–332.
[5] G. P. Gilberto, T. S. C. Alberto and J. M. Velasquez, 'Construccion de conjuntos B_h módulo m y particiones', *Mat. E. Univ.* **XIV** (2006), 65–70.
[6] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications* (Cambridge University Press, New York, 2000).
[7] B. Lindström, 'Finding finite B_2-sequences faster', *Math. Comp.* **67** (1998), 1173–1178.
[8] C. A. Martos Ojeda, L. M. Delgado Ordoñez and C. A. Trujillo Solarte, 'B_h sets as a generalization of Golomb rulers', *IEEE Access* **9** (2021), 118042–118050.
[9] K. O'Bryant, 'A complete annotated bibliography of work related to Sidon sequences', *Electron. J. Combin.* **DS11** (2004), 39 pages.
[10] R. M. Roth, N. Raviv and I. Tamo, 'Construction of Sidon spaces with applications to coding', *IEEE Trans. Inform. Theory* **64**(6) (2018), 4412–4422.
[11] B. Xiu, C. Fan and M. Liang, 'On disjoint Golomb rulers', Preprint, 2014, arXiv:1405.4535.

CESAR ANDRADE, Departamento de Matemáticas,
Universidad del Valle, Cali, Colombia
e-mail: cesar.andrade@correounivalle.edu.co

YAMIDT BERMUDEZ, Departamento de Matemáticas,
Universidad del Valle, Cali, Colombia
e-mail: yamidt.bermudez@correounivalle.edu.co

CARLOS TRUJILLO, Departamento de Matemáticas,
Universidad del Cauca, Popayan, Colombia
e-mail: trujillo@unicauca.edu.co

https://doi.org/10.1017/S0004972722000752 Published online by Cambridge University Press