

SIDON SETS IN ALGEBRAIC GEOMETRY

ARTHUR FOREY, JAVIER FRESÁN, AND EMMANUEL KOWALSKI

ABSTRACT. We report new examples of Sidon sets in abelian groups arising from generalized jacobians of curves, and discuss some of their properties with respect to size and structure.

1. INTRODUCTION

Let A be an abelian group. A subset S of A is called a *Sidon set* if S does not contain non-trivial additive quadruples; that is, if any solution $(x_1, x_2, x_3, x_4) \in S^4$ of the equation

$$x_1 + x_2 = x_3 + x_4 \tag{1}$$

satisfies $x_1 \in \{x_3, x_4\}$ (see, e.g., [6, § 1]). In other words, up to transposition an element of A is in at most one way the sum of two elements of S .

We will explain how to construct a range of new examples of Sidon sets using the theory of commutative algebraic groups. In fact, we sometimes most naturally obtain a slight variant: given an element a of A , we say that a subset S of A is a *symmetric Sidon set with center a* if $S = a - S$ and the solutions to equation (1) satisfy $x_1 \in \{x_3, x_4\}$ or $x_2 = a - x_1$ (we will explain in Remark 2 that the center is unique if S is not empty). Choosing (arbitrarily) one element of $\{x, a - x\}$ as x varies over elements of S with $2x \neq a$ leads to a Sidon set of size about $|S|/2$ if S is finite and A is without 2-torsion, but there is usually no natural choice.

Theorem 1. *Let k be a field and let C be a smooth projective geometrically connected curve of genus g over k . Let \mathfrak{m} be an effective divisor on C and $J_{\mathfrak{m}}$ the associated generalized jacobian, which is a commutative algebraic group of dimension $g + \max(\deg(\mathfrak{m}) - 1, 0)$. Let δ be a divisor of degree 1 on C whose support does not intersect that of \mathfrak{m} . Let $s: C - \mathfrak{m} \rightarrow J_{\mathfrak{m}}$ be the morphism induced by the map $x \mapsto (x) - \delta$ on divisors.*

If $\dim(J_{\mathfrak{m}}) \geq 2$, then $s((C - \mathfrak{m})(k))$ is either a Sidon set or a symmetric Sidon set in $J_{\mathfrak{m}}(k)$.

If, moreover, $(C - \mathfrak{m})(k)$ is non-empty, then it is a symmetric Sidon set if and only if one of the following conditions hold:

- (1) $g = 1$ and $\deg(\mathfrak{m}) = 2$; in this case, writing $\mathfrak{m} = (p) + (q)$ (where p and q are not necessarily k -points of C , but the divisor \mathfrak{m} is assumed to be defined over k), the center of $s((C - \mathfrak{m})(k))$ is the common value of $s(x) + s(p + q - x)$ for any $x \in (C - \mathfrak{m})(k)$.
- (2) $g \geq 2$, the curve C is hyperelliptic, and either $\deg(\mathfrak{m}) \leq 1$ or $\mathfrak{m} = (p) + (i(p))$ for some $p \in C$, where i is the hyperelliptic involution on C . In both of these cases, the center of $s((C - \mathfrak{m})(k))$ is the common value of $s(x) + s(i(x))$ for any $x \in (C - \mathfrak{m})(k)$.

A concrete description of the abelian groups $J_{\mathfrak{m}}(k)$ will be presented in Section 2.

2010 *Mathematics Subject Classification.* 14H40, 14L10, 05B10, 11B30.

Key words and phrases. Sidon set, symmetric Sidon set, algebraic curve, generalized jacobian.

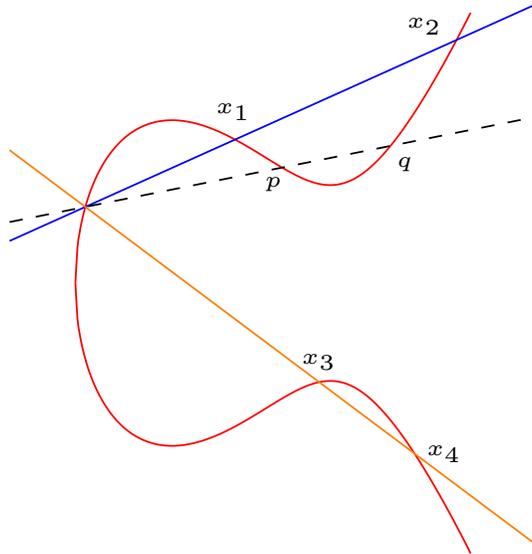


FIGURE 1. A non-trivial additive quadruple for $J_{(p)+(q)}$

Figure 1 illustrates the symmetric Sidon set obtained from a curve C of genus 1, viewed as a plane cubic curve, and a divisor $\mathbf{m} = (p) + (q)$ supported on two distinct k -points. It displays a configuration of points $(x_1, \dots, x_4) \in C(k) - \{p, q\}$ such that $(s(x_1), \dots, s(x_4))$ is a non-trivial additive quadruple in $J_{\mathbf{m}}(k)$.

The case $\mathbf{m} = 0$ of Theorem 1 was known to N. Katz (see Section 5).

Before proving Theorem 1, we will recall the definitions of the generalized jacobians, and comment on these examples of Sidon sets in comparison with the current literature. We also briefly survey some surprising applications of Sidon sets in algebraic geometry.

Remark 2. (1) It is possible that S be both a Sidon set and a symmetric Sidon set, but this only happens if S is empty or if $S = \{x, a - x\}$ for some a and x in A .

(2) Let $S \subset A$ be a non-empty symmetric Sidon set. We claim that its center is unique. Indeed, this is straightforward to check if S is of the form $\{x, a - x\}$. Otherwise, S is not a Sidon set, so that there exist elements $x_1, \dots, x_4 \in S$ such that $x_1 + x_2 = x_3 + x_4$ and $x_1 \notin \{x_3, x_4\}$. Then *any* center a is equal to $x_1 + x_2$, and hence all centers are equal.

Notation. Given complex-valued functions f and g defined on a set S , we write $f \ll g$ if there exists a real number $C \geq 0$ (which is then called an “implicit constant”) such that the inequality $|f(s)| \leq Cg(s)$ holds for all $s \in S$.

Acknowledgments. We thank K. Soundararajan for pointing out to us the terminology “Sidon sets”, and S. Eberhard and F. Manners for sharing with us their work [6] on dense Sidon sets. We also thank C. Bortolotto for pointing out a small slip when passing from symmetric Sidon sets to Sidon sets. We thank very warmly the referee, whose highly perceptive report was a model of the kind. During the preparation of this work, A.F. was supported by the SNF Ambizione grant PZ00P2_193354 and J.F. was partially supported by the grant ANR-18-CE40-0017 of the Agence Nationale de la Recherche.

2. GENERALIZED JACOBIANS

In this preliminary section, we briefly recall the group structure on the set of points of generalized jacobians (see Serre's book [20] for a complete account of the theory, in particular for the further structure of algebraic group that they carry).

Let k be an algebraically closed field. Let C be a smooth projective geometrically connected algebraic curve over k . The group $\text{Div}(C)$ of *divisors* on C is the free abelian group with basis given by the k -points of C ; we denote by (p) the basis element corresponding to $p \in C(k)$.

The *degree* $\deg(D)$ of a divisor $D = \sum n_p(p)$ is the sum $\sum n_p$ of the coefficients in its expression as a \mathbf{Z} -linear combination of the basis elements (p) . One views $\text{Div}(C)$ as an ordered abelian group, with $D \geq 0$ if and only if all coefficients are non-negative integers (in which case D is called an *effective* divisor). The *support* $|D|$ of a divisor D is the set of $p \in C(k)$ such that n_p is non-zero, and two divisors are said to be *coprime* if they have disjoint supports. We write $C - D$ for the open subvariety of C obtained by removing $|D|$.

If $f: C \rightarrow \mathbf{P}^1$ is a non-constant function, the divisor $\text{div}(f)$ of f is defined to be the sum of $p \in C(k)$ such that $f(p) = 0$, with multiplicity, minus the sum of $p \in C(k)$ such that $f(p) = \infty$, with multiplicity. It is a standard fact that $\deg(\text{div}(f)) = 0$.

Fix an effective divisor $\mathbf{m} = \sum n_p(p)$ on C , called a *modulus*. Let $\text{Div}_{0,\mathbf{m}}(C)$ be the subgroup of $\text{Div}(C)$ consisting of divisors of degree 0 which are coprime to \mathbf{m} . This contains a subgroup $P_{\mathbf{m}}(C)$ whose elements are the divisors of non-constant functions f satisfying $v_p(f - 1) \geq n_p$ for every p in the support of \mathbf{m} with multiplicity $n_p \geq 1$, where v_p is the valuation at p (order of zero or pole at p). In particular, the divisor of such a function is coprime to \mathbf{m} .

The group of k -points of the *generalized jacobian* associated to C and \mathbf{m} is then defined as

$$J_{\mathbf{m}}(k) = \text{Div}_{0,\mathbf{m}}(C)/P_{\mathbf{m}}(C).$$

The special case of the trivial modulus $\mathbf{m} = 0$ is particularly important: the corresponding quotient is the group of k -points of the classical jacobian variety J of C , which is an abelian variety over k ; its dimension is the *genus* g of C . In general, $J_{\mathbf{m}}(k)$ is the group of k -points of a commutative algebraic group $J_{\mathbf{m}}$ of dimension $g + \max(\deg(\mathbf{m}) - 1, 0)$ over k (see [20, V.1.3 and V.1.6]). It fits into an extension

$$0 \longrightarrow \left(\prod_{p \in |\mathbf{m}|} U_p/U_p^{(n_p)} \right) / \Delta \longrightarrow J_{\mathbf{m}}(k) \longrightarrow J(k) \longrightarrow 0, \quad (2)$$

where U_p denotes the multiplicative group of functions that do not vanish at p (units), $U_p^{(n_p)}$ the subgroup of those satisfying $v_p(f - 1) \geq n_p$, and Δ the diagonal subgroup of non-zero constant functions $(\lambda, \dots, \lambda)$. According to [20, V.3.15 and V.3.16], each group $U_p/U_p^{(n_p)}$ is isomorphic to $k^\times \times k^{n_p-1}$ if k has characteristic zero, and to $k^\times \times \prod W_{r_i}(k)$ if k has positive characteristic ℓ , where the product runs over integers $1 \leq i \leq n_p - 1$ coprime to ℓ and $W_{r_i}(k)$ are the ℓ -typical Witt vectors of length the smallest integer r_i satisfying $\ell^{r_i} \geq n_p/i$.

Remark 3. The formula for the dimension of the generalized jacobian shows that the condition $\dim(J_{\mathbf{m}}) \geq 2$ of Theorem 1 only excludes the cases where $g = 0$ and $\deg(\mathbf{m}) \leq 2$ or $g = 1$ and $\deg(\mathbf{m}) \leq 1$. The corresponding generalized jacobians are as follows:

- If $g = 0$ and $\deg(\mathbf{m}) \leq 1$, then C is the projective line and $J_{\mathbf{m}}$ is the trivial group.

- If $g = 0$ and $\deg(\mathbf{m}) = 2$, then C is the projective line and $J_{\mathbf{m}}$ is either the additive group (if \mathbf{m} is a single point with multiplicity 2) or the multiplicative group over k (if \mathbf{m} consists of two points).
- If $g = 1$ and $\deg(\mathbf{m}) \leq 1$, then C can be identified with an elliptic curve after fixing an origin, and $J_{\mathbf{m}}$ is isomorphic to this elliptic curve.

We have now described the groups appearing in Theorem 1 when k is algebraically closed. If k is only perfect (e.g. a finite field), we can define $J_{\mathbf{m}}(k)$ by Galois descent. Namely, we fix an algebraic closure \bar{k} of k , and consider the action of the absolute Galois group $\text{Gal}(\bar{k}/k)$ on $C(\bar{k})$, which extends by linearity to an action on the group $\text{Div}(C_{\bar{k}})$ of divisors over \bar{k} . We define the group $\text{Div}(C)$ of divisors over k as the fixed points under this action. Given a modulus \mathbf{m} on C , i.e., an effective divisor over k , the subgroups $\text{Div}_{0,\mathbf{m}}(C_{\bar{k}})$ and $P_{\mathbf{m}}(C_{\bar{k}})$ are stable under the action of $\text{Gal}(\bar{k}/k)$, hence an induced action on the quotient $J_{\mathbf{m}}(\bar{k})$. The group $J_{\mathbf{m}}(k)$ is then the subgroup of $J_{\mathbf{m}}(\bar{k})$ consisting of the fixed points under the Galois group. The most interesting case from the point of view of classical Sidon set theory is that of finite field k , in which the above construction amounts to considering fixed points under the Frobenius automorphism $x \mapsto x^{|k|}$ of \bar{k} . Then $J_{\mathbf{m}}(k)$ is a finite group.

Remark 4. Examples of divisors over k include, of course, linear combinations of k -points of C , but a k -divisor of C is *not necessarily* of this form. For instance, for $C = \mathbf{P}^1$ and a non-zero polynomial $f \in k[X]$, the divisor of f is always a k -divisor on C , although in general not all roots of f belong to k . This simple remark will play a role in the next section.

3. ALGEBRAIC SIDON SETS OVER FINITE FIELDS

A classical problem in additive combinatorics is to construct large Sidon subsets of finite groups. Thus, while it is enough to prove Theorem 1 for algebraically closed fields, we are particularly interested in the case where k is finite, and hence $J_{\mathbf{m}}(k)$ is a finite group. We therefore investigate the size and apparent structure of the finite Sidon sets we have constructed, assuming that k is a finite field with a fixed algebraic closure \bar{k} .

Given a curve C of genus g and a modulus \mathbf{m} over k satisfying $g + \max(\deg(\mathbf{m}) - 1, 0) \geq 2$, the morphism $s: C - \mathbf{m} \rightarrow J_{\mathbf{m}}$ is an embedding, so that Theorem 1 provides a Sidon set or a symmetric Sidon set $S = s((C - \mathbf{m})(k))$ of size $|(C - \mathbf{m})(k)|$ in the abelian group $A = J_{\mathbf{m}}(k)$. On the one hand, from the Hasse–Weil bound on the number of points of curves over finite fields [22], one gets the estimate

$$|k| - 2g\sqrt{|k|} + 1 - \deg(\mathbf{m}) \leq |S| \leq |k| + 2g\sqrt{|k|} + 1.$$

On the other hand, the extension structure (2) of $J_{\mathbf{m}}(k)$ along with the Riemann hypothesis for abelian varieties and tori over finite fields, in the form of the estimates

$$(\sqrt{|k|} - 1)^{2g} \leq |J(k)| \leq (\sqrt{|k|} + 1)^{2g}, \quad (|k| - 1)^d \leq |T(k)| \leq (|k| + 1)^d$$

for a d -dimensional torus T (see e.g. [18, Thm. 19.1] and [2, Prop. 3.3.5]), yield

$$(|k| - 1)^{\max(\deg(\mathbf{m}) - 1, 0)} (\sqrt{|k|} - 1)^{2g} \leq |A| \leq (\sqrt{|k|} + 1)^{2g} (|k| + 1)^{\max(\deg(\mathbf{m}) - 1, 0)}.$$

Thus, when $|k|$ is large, the set S has size about $|A|^{1/\dim(J_{\mathbf{m}})}$. The densest sets will therefore appear when $\dim(J_{\mathbf{m}}) = 2$. This happens in the following cases:

- (1) $g = 0$ and $\deg(\mathbf{m}) = 3$;
- (2) $g = 1$ and $\deg(\mathbf{m}) = 2$;
- (3) $g = 2$ and $\deg(\mathbf{m}) \leq 1$.

Note that in the second and third cases, Theorem 1 also states that we obtain a *symmetric* Sidon set, and not a Sidon set (because any curve of genus 2 is hyperelliptic [17, Prop. 4.9]), so that we get from this construction Sidon sets of size about $\sqrt{|A|}/2$ by “desymmetrizing” (using the fact that the size of the 2-torsion group of $J_{\mathbf{m}}(k)$ is bounded by 2^4 in all these cases).

We consider these three cases in turn.

(1) For $g = 0$ and $\deg(\mathbf{m}) = 3$, the curve C is isomorphic to \mathbf{P}^1 (since any non-degenerate quadratic form in three variables has a non-trivial zero by the Chevalley–Warning theorem; this would not necessarily be true over an arbitrary field). We can restrict our attention to a few special cases of \mathbf{m} using the action of the automorphism group $\mathbf{PGL}_2(k)$ on $C(k)$, which induces an action on the group of k -divisors preserving multiplicities.

Lemma 5. *The action of $\mathbf{PGL}_2(k)$ on effective k -divisors of degree 3 on \mathbf{P}^1 has five orbits, represented by*

$$\begin{aligned} \mathbf{m}_1 &= (0) + (1) + (\infty), & \mathbf{m}_2 &= (0) + 2(\infty), & \mathbf{m}_3 &= 3(\infty), \\ \mathbf{m}_4 &= (a) + (b) + (c), & \mathbf{m}_5 &= (\alpha) + (\beta) + (\infty), \end{aligned}$$

where a, b, c are the roots of an irreducible monic cubic polynomial $f_3 \in k[X]$, and α, β are the roots of an irreducible monic quadratic polynomial $f_2 \in k[X]$.

Proof. Since $\mathbf{PGL}_2(k)$ acts 3-transitively on $\mathbf{P}^1(k)$, the orbits of the divisors \mathbf{m}_1 , \mathbf{m}_2 and \mathbf{m}_3 are, respectively, the divisors whose support is contained in $\mathbf{P}^1(k)$ and consists of three distinct points, two points, or a single point.

Now let \mathbf{m} be an effective k -divisor of degree 3 such that at least one point x of the support of \mathbf{m} does not belong to $\mathbf{P}^1(k)$. Since, for any such x , all its Galois conjugates are also in the support with the same multiplicity (because \mathbf{m} is Galois-invariant), we see that x must generate either the extension k_3 of degree 3 of k in \bar{k} , or the extension k_2 of degree 2.

In the former case, \mathbf{m} is equal to $(x) + (x^{|k|}) + (x^{|k|^2})$. But there exists $\gamma \in \mathbf{PGL}_2(k)$ such that $\gamma(x) = a$ (because $\mathbf{GL}_2(k)$ acts on $k_3 - k$ with stabilizers given by the center, so acts transitively since $|\mathbf{GL}_2(k)| = |k^\times| |k_3 - k|$) and then $\gamma(\mathbf{m}) = \mathbf{m}_4$ since the Frobenius commutes with γ .

Finally, if x generates the quadratic extension k_2 , then \mathbf{m} is of the form $(x) + (x^{|k|}) + (y)$ for some $y \in \mathbf{P}^1(k)$, and from the transitivity of the action of $\mathbf{PGL}_2(k)$ on $\mathbf{P}^1(k)$ and that of $\mathbf{GL}_2(k)$ on k_2 one sees that \mathbf{m} and \mathbf{m}_5 lie in the same orbit. \square

We obtain this way five Sidon sets $S_i \subset A_i = J_{\mathbf{m}_i}(k)$ for $1 \leq i \leq 5$, of sizes

$$|S_1| = |k| - 2, \quad |S_2| = |k| - 1, \quad |S_3| = |k|, \quad |S_4| = |k| + 1, \quad |S_5| = |k|.$$

Moreover, one can easily check that there are isomorphisms of abelian groups

$$\begin{aligned} A_1 &\simeq (k^\times)^2, & A_2 &\simeq k^\times \times k, \\ A_3 &\simeq k^2, & \text{if } k &\text{ has characteristic } \geq 3 \\ A_3 &\simeq W_2(k), & \text{if } k &\text{ has characteristic } 2, \\ A_4 &\simeq k_3^\times/k^\times, & A_5 &\simeq k_2^\times, \end{aligned}$$

where k_3 and k_2 are respectively the cubic and quadratic extensions of k inside \bar{k} and $W_2(k)$ is the group of Witt vectors of length 2 (which in characteristic 2 is a non-trivial extension of k by k ; see [20, V.16]). The groups A_4 and A_5 appear as the groups of k -points of the 2-dimensional non-split k -tori $J_{\mathfrak{m}_4} \simeq \text{Res}_{k_3/k}(\mathbf{G}_m)/\mathbf{G}_m$ and $J_{\mathfrak{m}_5} \simeq \text{Res}_{k_2/k}(\mathbf{G}_m)$.

It is not difficult to see further that S_1, S_2, S_3 can be identified, respectively, with

$$\begin{aligned} S_1 &= \{(x, 1-x) \in (k^\times)^2 \mid x \in k^\times, x \neq 1\}, \\ S_2 &= \{(x, x) \in k^\times \times k \mid x \in k^\times\}, \\ S_3 &= \{(x, x^2) \in k^2 \mid x \in k\}, \text{ if } k \text{ has characteristic } \geq 3 \end{aligned}$$

(see [7, Rem. 9.13 (2)]). These are very classical examples of Sidon sets; they appear in the paper [6] of Eberhard and Manners as Constructions 5, 4 and 1, respectively, and are due to Erdős–Turán, Spence and Hugues (with S_2 also discovered independently by Ruzsa and S_3 by Cilleruelo). One can also check that S_4 and S_5 correspond to Constructions 2 and 3 of loc. cit., which are due to Singer and Bose, respectively.

All these are Sidon sets of size approximately $\sqrt{|A|}$. Thus, we recover “uniformly” the five main examples of dense Sidon sets discussed by Eberhard and Manners. This construction appears to be very different from their own uniform interpretation, where the groups A_i arise as maximal abelian subgroups of $\mathbf{PGL}_3(k)$ and the Sidon sets take the form

$$S = \{g \in A \mid p \in g(\ell)\}$$

for some line ℓ and some point p in $\mathbf{P}^2(k)$ (see [6, §2-3]).

(2) For $g = 1$, we have a curve of genus 1. It is classical that, over a finite field, such a curve always has a k -rational point, and one can take this as origin to view the curve as an elliptic curve. In particular, the set $C(k)$ is then also a finite abelian group. The general structure of the generalized jacobians from (2) specializes in this case to a short exact sequence

$$0 \rightarrow B \rightarrow J_{\mathfrak{m}}(k) \rightarrow C(k) \rightarrow 0,$$

where the abelian group B is given by:

$$\begin{aligned} B &= k \text{ if } \mathfrak{m} = 2(p) \text{ for some } p \in C(k), \\ B &= k^\times \text{ if } \mathfrak{m} = (p) + (q) \text{ for some } p \neq q \text{ in } C(k), \\ B &= k_2^\times/k^\times \text{ if } \mathfrak{m} = (p) + (q) \text{ for some Galois-conjugate } p \neq q \text{ in } C(k_2). \end{aligned}$$

Since $|k| - 1 \leq |B| \leq |k| + 1$ (and $J_{\mathfrak{m}}(k)$ has at most 8 points of 2-torsion), the desymmetrized Sidon sets have size about $\sqrt{|A|}/2$.

(3) For $g = 2$ and $\deg(\mathfrak{m}) \leq 1$, the generalized jacobians are all isomorphic to the classical jacobian of C , and again we obtain Sidon sets of size about $\sqrt{|A|}/2$.

All these examples are rather dense Sidon sets. Cases (2) and (3) are seemingly of a different type than previous examples, which is of interest in the context of the existing speculation that “sufficiently large” Sidon sets in finite abelian groups should have some kind of algebraic structure (see e.g. the blog post [9] of T. Gowers, and the comments there). As already mentioned, Eberhard and Manners [6] have classified in a uniform way all known examples of Sidon sets S with $|S| \sim \sqrt{|A|}$ using finite projective planes. Our constructions show that there is a much wider variety of examples of Sidon sets of size $\sqrt{|A|}/2$ than previously reported, and exhibit the following features which, to the best of our knowledge, were previously unknown:

- Any classification of Sidon sets of size at least $\sqrt{|A|}/2$ will have to be sophisticated enough to account for jacobians of curves of genus 2 as well as generalized jacobians of dimension 2 coming from elliptic curves;
- There are natural “continuous” families of Sidon sets of size about $\sqrt{|A|}/2$, up to “isomorphism”. Namely, we note that the space of hyperelliptic curves of genus 2 over a given field k , up to isomorphism, is three-dimensional; the space of elliptic curves is one-dimensional, each giving rise to a one-parameter family of generalized jacobians (for $\mathbf{m} = 2(p)$, it is not difficult to see that all generalized jacobians are isomorphic as p varies, and for $\mathbf{m} = (p) + (q)$, one can check that $J_{(p)+(q)}$ is isomorphic to $J_{(0)+(q-p)}$). Although one might object that maybe distinct curves (as geometric objects) would give rise to “isomorphic” finite Sidon sets, this is certainly not the case, at least in a naive sense (e.g. because many different finite abelian groups arise as $J(k)$ for the jacobian J of a curve of genus 2 and a fixed large finite field k).
- All our examples are obtained as the intersection of an *infinite* Sidon set, namely

$$s((C - \mathbf{m})(\bar{k})) \subset J_{\mathbf{m}}(\bar{k}),$$

with the finite subgroup $J_{\mathbf{m}}(k)$. (Note that this applies also to examples where the modulus is not defined over k ; for instance, this happens for the sets S_4 and S_5 above, in which case this feature is not apparent from the classical constructions of Bose and Singer, or those of Eberhard–Manners.)

An intriguing comparison suggests itself with infinite Sidon sets of integers, which are known to be *less* dense in segments than the densest finite Sidon sets of integers. Indeed, a result of Erdős states that

$$\liminf_{n \rightarrow +\infty} \frac{(\log N)^{1/2}}{N^{1/2}} |\{n \in S \mid 0 \leq n \leq N\}| < +\infty$$

for any Sidon set $S \subset \mathbf{Z}$ (see, e.g., [10, p. 89, Th. 8]). The referee pointed out that the proof leads to a precise upper-bound $\leq \sqrt{40}$.

4. SOME FINITE ABELIAN GROUPS WITH LARGE SIDON SETS

Babai and Sós [1, Th. 4.2] considered the problem of finding “large” Sidon subsets in arbitrary finite abelian groups. It should be noted before stating their results that they use a slightly different definition of Sidon sets (see [1, Def. 1.1]), which also allows for solutions of (1) with $x_1 = x_2$ and $x_3 = x_4$, which are not trivial in the sense of our definition unless also $x_1 = x_3$. (In other words, a Sidon set can contain distinct elements x_1, x_3 satisfying $2x_1 = 2x_3$.) This definition coincides with ours if A has trivial 2-torsion but not in general:

for instance, a vector space over \mathbf{F}_2 does not contain Sidon sets of size ≥ 2 with our definition. Babai and Sós proved (using a probabilistic argument) that any finite abelian group A contains a set S with their property such that $|S| \gg |A|^{1/3}$; as far as we know, this remains the best general lower bound. Our results lead to new families of finite abelian groups A in which Sidon sets S with $|S| \gg |A|^{1/2}$ are known to exist.

Proposition 6. *Let $j \geq 1$ be an integer and $(n_i)_{1 \leq i \leq j+1}$ a finite sequence of integers ≥ 2 . Suppose that there exist a prime number p and an integer n coprime to p such that*

$$\begin{aligned} p &\leq n_i \text{ for } 1 \leq i \leq j, & n &\leq n_{j+1}, \\ |p^j + 1 - n| &\leq 2p^{j/2}. \end{aligned}$$

Then there exists a Sidon set

$$S \subset A = \prod_{1 \leq i \leq j+1} \mathbf{Z}/n_i\mathbf{Z}$$

such that $|S| \gg (p/2)^j$, where the implicit constant is absolute.

Roughly speaking, this means that if we have a prime number p and integers j and n with n of size about p^j , then a finite abelian group A which is “close to” the group

$$(\mathbf{Z}/p\mathbf{Z})^j \times \mathbf{Z}/n\mathbf{Z} \tag{3}$$

(in some sense) contains a Sidon set of size $\gg |A|^{1/2}$. By contrast, the results of Babai and Sós [1, Prop. 5.3] give such a lower bound for groups “close to”

$$(\mathbf{Z}/p\mathbf{Z})^j.$$

For groups like (3), the bound of Babai and Sós is of size $|A|^{1/4}$, which is therefore worse than the general probabilistic lower bound $|A|^{1/3}$.

Proof of Proposition 6. The argument is similar to the proof of [1, Prop. 5.3]. Let k be a field with p^j elements. Pick an elliptic curve E over k such that $E(k)$ is cyclic of order n (which is possible, by independent work of Ruck [19] and Volloch [21]), set $\tilde{E} = E - \{0_E\}$ and consider the generalized jacobian $E^\sharp = J_{2(0_E)}$. Choose a k -rational divisor of degree 1 to define the embedding $s: \tilde{E} \rightarrow E^\sharp$. We also fix a group isomorphism

$$E^\sharp(k) \rightarrow (\mathbf{Z}/p\mathbf{Z})^j \times \mathbf{Z}/n\mathbf{Z}$$

(which exists since there is an exact sequence

$$0 \rightarrow k \rightarrow E^\sharp(k) \rightarrow E(k) \simeq \mathbf{Z}/n\mathbf{Z} \rightarrow 0,$$

and the assumption that $n = |E(k)|$ is coprime to p implies that this exact sequence is split). We denote by $t: \tilde{E}(k) \rightarrow (\mathbf{Z}/p\mathbf{Z})^j \times \mathbf{Z}/n\mathbf{Z}$ the composition of s and such an isomorphism. The image $t(\tilde{E}(k))$ is a symmetric Sidon set of size $n - 1$ by Theorem 1.

For any integer $q \geq 1$ and any $x \in \mathbf{Z}/q\mathbf{Z}$, we denote by \dot{x} the integer such that $0 \leq \dot{x} \leq q-1$ and $x \equiv \dot{x} \pmod{q}$. By an *interval* in $\mathbf{Z}/q\mathbf{Z}$, we mean the image modulo q of an interval $\{a, a+1, \dots, b\}$, where $0 \leq a \leq b \leq q-1$; the integer a is called the *origin* of the interval.

By the pigeon-hole principle, there is a choice of intervals I_i for $1 \leq i \leq j$ (resp. I) with $I_i \subset \mathbf{Z}/p\mathbf{Z}$ for $1 \leq i \leq j$ (resp. $I \subset \mathbf{Z}/n\mathbf{Z}$) and $|I_i| = \lfloor p/2 \rfloor$ (resp. $|I| = \lfloor n/2 \rfloor$), so that

$$|t(\tilde{E}(k)) \cap X| \geq \frac{|\tilde{E}(k)|}{2^{j+1}},$$

where we denote $X = I_1 \times \cdots \times I_j \times I$.

(We note in passing that a fairly simple appeal to the Riemann hypothesis over finite fields and discrete Fourier analysis on $E^\sharp(k)$ shows that this will be valid for all choices of intervals of this size, provided p is large enough and the constant $2^{-(j+1)}$ is replaced, say, by $2^{-(j+2)}$.)

Let α_j (resp. α) be the origin of I_j (resp. of I). Define an injective map

$$\varphi: (\mathbf{Z}/p\mathbf{Z})^j \times \mathbf{Z}/n\mathbf{Z} \rightarrow \mathbf{Z}^{j+1}$$

by the assignment $(a_1 + p\mathbf{Z}, \dots, a_j + p\mathbf{Z}, a + n\mathbf{Z}) \mapsto (\hat{a}_1 - \alpha_1, \dots, \hat{a}_j - \alpha_j, \hat{a} - \alpha)$. The restriction of φ to X is a *Freiman isomorphism* of order 2 (i.e., for x_1, \dots, x_4 in X , we have $x_1 + x_2 = x_3 + x_4$ if and only if $\varphi(x_1) + \varphi(x_2) = \varphi(x_3) + \varphi(x_4)$).

In addition, by the assumptions $p \leq n_i$ and $n \leq n_{j+1}$, as well as the condition on the intervals, the image of $E^\sharp(k)$ by φ (resp. the image of X by φ) is contained in the set

$$\begin{aligned} & \{0, \dots, p-1\}^j \times \{0, \dots, n-1\}, \\ & \text{(resp. } \{0, \dots, \lfloor p/2 \rfloor\}^j \times \{0, \dots, \lfloor n/2 \rfloor\}). \end{aligned}$$

In particular, the restriction of the canonical projection $\pi: \mathbf{Z}^{j+1} \rightarrow A$ to the image of φ is injective, and the restriction of π to X is also a Freiman isomorphism of order 2.

Thus, we have a Freiman isomorphism $\pi \circ \varphi$ of order 2 from X to A , and since $t(\tilde{E}(k))$ is a symmetric Sidon set in $(\mathbf{Z}/p\mathbf{Z})^j \times \mathbf{Z}/n\mathbf{Z}$, we conclude that the set

$$(\pi \circ \varphi)(t(\tilde{E}(k)) \cap X) \subset A$$

is a symmetric Sidon set in A of size $\gg |\tilde{E}(k)| \gg (p/2)^j$, where the implicit constant is absolute. Since $E^\sharp(k)$ is cyclic, the size of its 2-torsion subgroup is at most 2, so this symmetric Sidon set contains a Sidon set of size $\gg \frac{1}{2}|\tilde{E}(k)| \gg (p/2)^j$ where the implicit constant is absolute. \square

5. APPLICATIONS OF SIDON SETS IN ALGEBRAIC AND ARITHMETIC GEOMETRY

In this short section, we briefly recall some of the applications of Sidon sets (even in cases where they are not very dense) in arithmetic geometry.

(1) In work of Katz (see, e.g., [12, Th. 2.8.1 and Th. 7.9.6]), the assumption that the critical values of a polynomial, or the set of parameters of a hypergeometric differential equation, form a Sidon set or a symmetric Sidon set in the additive group \mathbf{C} lead to computations of certain monodromy groups or differential Galois groups; here, even sets of 3 elements give non-trivial results, and such computations in turn have a number of important implications (see, for instance, [8] and [16] for recent examples).

(2) The fact that the sets in Theorem 1 are Sidon sets or symmetric Sidon sets leads by our work [7, Ch. 7 and §9.3] to equidistribution results for exponential sums over finite fields parameterized by characters of the groups $J_m(k)$. The (symmetric) Sidon property allows us to compute the so-called fourth moment of the relevant tannakian group which

controls the distribution properties of the sums, and to almost determine it by means of Larsen’s alternative [14]. We emphasize again here that symmetric Sidon sets arise just as naturally as Sidon sets, and that the size of the sets is not particularly relevant. In the special case $\mathbf{m} = 0$, this was already used by Katz in 2010 to answer a question of Tsimerman (unpublished, but see [7, Th. 12.1]).

(3) In another paper of Katz [13], it is shown how to use Larsen’s alternative to prove some of the key statements in Deligne’s second proof [5] of the Riemann hypothesis over finite fields. The crucial moment computation (performed in cohomological form in [13, p. 120, Step 5]) relies ultimately (but implicitly) on the fact that the parabola (x, x^2) in k^2 is a Sidon set in odd characteristic. As we pointed out above, this is the case of the curve $C = \mathbf{P}^1$ and the modulus $\mathbf{m} = 3(\infty)$ of Theorem 1.

6. PROOFS

We will now prove Theorem 1. We first notice that we may reduce to the case where the field k is algebraically closed. Indeed, let \bar{k} be an algebraic closure of k , and let S be a subset of $J_{\mathbf{m}}(k)$. By definition, S is a Sidon set in $J_{\mathbf{m}}(k)$ if and only if it is one in $J_{\mathbf{m}}(\bar{k})$. Similarly, if S is a symmetric Sidon set in $J_{\mathbf{m}}(k)$ with center $a \in J_{\mathbf{m}}(k)$, then it is one in $J_{\mathbf{m}}(\bar{k})$, with the same center. But also, suppose that S is a symmetric Sidon set in $J_{\mathbf{m}}(\bar{k})$ with center $a \in J_{\mathbf{m}}(\bar{k})$. Then either S is empty, or we can find x and y in S (maybe equal) such that $x = a - y$, hence $a = x + y \in J_{\mathbf{m}}(k)$, and it follows that S is a symmetric Sidon set in $J_{\mathbf{m}}(k)$ in all cases.

Thus we assume that k is algebraically closed and $\dim(J_{\mathbf{m}}) \geq 2$.

We recall that if $\mathbf{m} \geq \mathbf{m}' \geq 0$ and δ is a divisor of degree 1 with support disjoint from that of \mathbf{m} , then there is a commutative diagram

$$\begin{array}{ccc} J_{\mathbf{m}} & \xrightarrow{f} & J_{\mathbf{m}'} \\ \uparrow s & & \uparrow s \\ C - \mathbf{m} & \xrightarrow{i} & C - \mathbf{m}' \end{array}$$

where i is the inclusion and f is a group homomorphism (see [20, V.3.12, Prop. 6]). This implies that if $s((C - \mathbf{m}')(k))$ is a Sidon set in $J_{\mathbf{m}'}(k)$, then so is $s((C - \mathbf{m})(k))$ in $J_{\mathbf{m}}(k)$.

This means that we can reduce the proof of Theorem 1 to the following cases:

- (1) $g = 0$ and $\deg(\mathbf{m}) = 3$ (obtaining Sidon sets);
- (2) $g = 1$ and $\deg(\mathbf{m}) = 2$ (obtaining symmetric Sidon sets);
- (3) $g = 1$ and $\deg(\mathbf{m}) \geq 3$ (obtaining Sidon sets);
- (4) $g \geq 2$, $\mathbf{m} = 0$ and C not hyperelliptic (obtaining Sidon sets);
- (5) $g \geq 2$ and C hyperelliptic (obtaining either Sidon sets or symmetric Sidon sets).

Case (1). This corresponds to the three “classical” Sidon sets discussed in Section 3, but it is also straightforward to show that we obtain Sidon sets directly from the definition.

Thanks to the action of $\mathbf{PGL}_2(k)$ on $\mathbf{P}^1(k)$, it suffices to handle the cases $\mathbf{m} = 3(\infty)$, $\mathbf{m} = 2(\infty) + (0)$ and $\mathbf{m} = (\infty) + (0) + (1)$. In any case, let x_1, \dots, x_4 be points of $(\mathbf{P}^1 - \mathbf{m})(k)$ satisfying $s(x_1) + s(x_2) = s(x_3) + s(x_4)$, and assume that $x_1 \notin \{x_3, x_4\}$. There is a unique rational function $\varphi: \mathbf{P}^1 \rightarrow \mathbf{P}^1$ such that $\varphi(\infty) = 1$ which vanishes at x_1 and x_2 and has

poles at x_3 and x_4 , namely

$$\varphi = \frac{(X - x_1)(X - x_2)}{(X - x_3)(X - x_4)}.$$

Thus the Sidon equation holds if and only if the divisor of φ belongs to $P_{\mathbf{m}}(\mathbf{P}^1)$. Now:

- (1) If $\mathbf{m} = 3(\infty)$, we need $v_{\infty}(\varphi - 1) \geq 3$, which is impossible because φ has degree 2.
- (2) If $\mathbf{m} = 2(\infty) + (0)$, we need $(x_1x_2)/(x_3x_4) = \varphi(0) = 1$ and $v_{\infty}(\varphi - 1) \geq 2$; using the uniformizer $Z = 1/X$ at infinity, the last condition is seen to be equivalent to $x_1 + x_2 = x_3 + x_4$. But the two equations $x_1x_2 = x_3x_4$ and $x_1 + x_2 = x_3 + x_4$ imply that $\{x_1, x_2\} = \{x_3, x_4\}$, both sets being the roots of the same polynomial of degree 2.
- (3) If $\mathbf{m} = (\infty) + (0) + (1)$, we need the equalities $(x_1x_2)/(x_3x_4) = \varphi(0) = 1$ and $(1 - x_1)(1 - x_2)/((1 - x_3)(1 - x_4)) = \varphi(1) = 1$ to hold, and expanding we see that these two conditions are equivalent to $x_1x_2 = x_3x_4$ and $x_1 + x_2 = x_3 + x_4$ again, so we obtain once more $\{x_1, x_2\} = \{x_3, x_4\}$.

This concludes the proof of the first case. □

For case (2), recall that the group law of an elliptic curve $E \subset \mathbf{P}^2$ with neutral element 0_E is characterized by the condition that if ℓ is a line in \mathbf{P}^2 , then the sum of the intersection points of ℓ and E (with multiplicity) is equal to 0_E . We will use the following.

Lemma 7. *Let E be an elliptic curve over k with $\tilde{E} = E - \{0_E\}$ given by a Weierstrass equation*

$$y^2 + a_1xy + a_3y = f(x), \quad f \in k[X], \quad \deg(f) = 3, \quad f \text{ squarefree.}$$

Let (x_1, \dots, x_4) be points of $\tilde{E}(k)$ such that $x_1 + x_2 = x_3 + x_4$. Then the line in the affine plane joining x_1 to x_2 , or by convention the tangent line to the curve at x_1 if $x_1 = x_2$, is parallel to the line joining x_3 to x_4 , with the same convention, if and only if either $\{x_1, x_2\} = \{x_3, x_4\}$, or $x_2 = -x_1$. If the two lines are equal, then $\{x_1, x_2\} = \{x_3, x_4\}$.

Proof. If $x_2 = -x_1$, then $x_4 = -x_3$, so that the two lines meet at the point at infinity, and hence are parallel in the affine plane.

Conversely, we assume that $x_2 \neq -x_1$ (and hence $x_4 \neq -x_3$). By the geometric description of the group law, the condition $x_1 + x_2 = x_3 + x_4$ means that the two lines indicated meet in the *affine* plane at the point $-(x_1 + x_2) = -(x_3 + x_4) \neq 0_E$. Since the lines are parallel, they are equal. Then this common line ℓ satisfies

$$\ell \cap \tilde{E}(k) = \{x_1, x_2, -(x_1 + x_2)\} = \{x_3, x_4, -(x_3 + x_4)\}.$$

This implies $x_1 \in \{x_3, x_4\}$. Indeed, otherwise we would have $x_1 = -(x_3 + x_4) = -(x_1 + x_2)$, so that $\ell \cap \tilde{E}(k) = \{x_1, x_2\}$ and hence $x_3 \in \{x_1, x_2\}$, which yields a contradiction. □

Case (2). Let p and q be points of $C(k)$ (not necessarily distinct) such that $\mathbf{m} = (p) + (q)$, and let s denote an immersion $x \mapsto (x) - \delta$ from $C - \{p, q\}$ to $J_{\mathbf{m}}$. Taking q as the origin of the group law, we can view C as an elliptic curve, which we denote by E and view as a smooth plane cubic curve.

Let x_1, \dots, x_4 in $E - \{p, q\}$ be solutions of $s(x_1) + s(x_2) = s(x_3) + s(x_4)$. We denote by L_{12} (resp. L_{34}) the line in the projective plane passing through x_1 and x_2 , or the tangent line

to E at x_1 if $x_1 = x_2$ (resp. the line in the projective plane passing through x_3 and x_4 , or the tangent line to E at x_3 if $x_3 = x_4$).

If $L_{12} = L_{34}$ then we deduce from Lemma 7 that $\{x_1, x_2\} = \{x_3, x_4\}$. We assume that this is not the case. Let r be the intersection point of L_{12} and L_{34} . Since the assumption implies that $x_1 + x_2 = x_3 + x_4$, the description of the group law implies that r lies in $E(k)$. We denote by \mathbf{P}_r^1 the space of projective lines in \mathbf{P}^2 passing through r ; it is an algebraic curve, isomorphic to \mathbf{P}^1 , and we identify it with \mathbf{P}^1 in such a way that $L_{12} = 0$ and $L_{34} = \infty$.

Now define a map $E - \{r\} \rightarrow \mathbf{P}_r^1$ by sending x to the line joining r and x . This is an algebraic map and can be extended to a morphism $\varphi: E \rightarrow \mathbf{P}_r^1 = \mathbf{P}^1$ such that $\varphi(r)$ is the tangent line to E at r .

We claim that $\varphi^{-1}(0) = \varphi^{-1}(L_{12}) = \{x_1, x_2\}$ and $\varphi^{-1}(\infty) = \varphi^{-1}(L_{34}) = \{x_3, x_4\}$. Indeed, the equality $\varphi(x_1) = \varphi(x_2) = L_{12}$ holds by definition, and the only other $x \in E$ that may map to L_{12} is $x = r$. But $\varphi(r) = L_{12}$ means that the tangent line at r passes through x_1 and through x_2 . Since E is a cubic, this is only possible if $x_1 = x_2$, and then if also $x_1 = x_2 = r$.

The function $\varphi: E \rightarrow \mathbf{P}^1$ has divisor $(x_1) + (x_2) - (x_3) - (x_4)$. In particular, $\varphi(p)$ and $\varphi(q)$ are in k^\times . The definition of $J_{\mathbf{m}}$ shows that the equation $s(x_1) + s(x_2) = s(x_3) + s(x_4)$ is valid if and only if

- $p \neq q$ and $\varphi(p) = \varphi(q)$;
- or $p = q$ and p is a zero of order ≥ 2 of $\varphi(p)^{-1}\varphi - 1$.

If $p \neq q$ then the condition $\varphi(p) = \varphi(q)$ means that the line joining r to p is the same as the line joining r to q , with the usual tangent convention if $r = p$ or $r = q$. This means that r, p, q are on the same line, so that $r + p + q = 0$, hence $x_1 + x_2 = x_3 + x_4 = -r = p + q$. Conversely, the equality $\varphi(p) = \varphi(q)$ holds if $x_1 + x_2 = p + q = x_3 + x_4$.

If $p = q$, a moment's thought (or the crutch of writing down equations) shows that the condition that p is a zero of order ≥ 2 of $\varphi(p)^{-1}\varphi - 1$ is valid if and only if the line joining p and r is the tangent line to E at r . This translates to $2p + r = 0$, and hence to $x_1 + x_2 = x_3 + x_4 = 2p$.

Since the conditions above are equivalent with $s(x_1) + s(x_2) = s(x_3) + s(x_4)$, this concludes the proof of Case (2). \square

Case (3). Let x_1, x_2, x_3, x_4 be k -points of $C - \mathbf{m}$ satisfying $s(x_1) + s(x_2) = s(x_3) + s(x_4)$ and $x_1 \notin \{x_3, x_4\}$. For any effective divisor $\mathbf{m}' = (p) + (q)$ of degree 2 such that $\mathbf{m} \geq \mathbf{m}'$, projecting to $J_{\mathbf{m}'}$ and applying case (2), we see that $x_1 + x_2 = x_3 + x_4 = p + q$. Varying p and q among k -points in the support of \mathbf{m} , we see that \mathbf{m} is of the form $\mathbf{m} = d(p)$ for some point $p \in E(k)$ and $d \geq 3$. The Sidon equation then holds if and only if the unique function φ with divisor $(x_1) + (x_2) - (x_3) - (x_4)$ with $\varphi(p) = 1$ is such that $\varphi - 1$ vanishes to order $\geq d$ at p . Since φ has degree ≤ 2 , this is not possible. Thus, $s((C - \mathbf{m})(k))$ is a Sidon set. \square

Case (4). Here C has genus ≥ 2 , the modulus \mathbf{m} is trivial and C is not hyperelliptic. Let x_1, x_2, x_3, x_4 be points in $C(k)$ such that $s(x_1) + s(x_2) = s(x_3) + s(x_4)$. If $x_1 \notin \{x_3, x_4\}$, this implies the existence of a rational function on C with set of zeros $\{x_1, x_2\}$ and set of poles $\{x_3, x_4\}$, which corresponds to a morphism $f: C \rightarrow \mathbf{P}^1$ of degree at most 2. By definition, this is not possible unless C is hyperelliptic (see, e.g., [17, Def. 7.4.7]), hence the result. \square

Case (5). Finally, we assume that C has genus ≥ 2 and is hyperelliptic.

We first assume that $\mathbf{m} = 0$. Let x_1, x_2, x_3, x_4 be points in $\mathbf{C}(k)$ such that $s(x_1) + s(x_2) = s(x_3) + s(x_4)$ and $x_1 \notin \{x_3, x_4\}$. As in the previous case, this implies the existence of a rational function on \mathbf{C} with set of zeros $\{x_1, x_2\}$ and set of poles $\{x_3, x_4\}$, which corresponds to a morphism $f: \mathbf{C} \rightarrow \mathbf{P}^1$ of degree at most 2. Since there exists on \mathbf{C} a unique morphism to \mathbf{P}^1 of degree 2, up to automorphisms (see, e.g., [17, Rem. 7.4.30]), the hyperelliptic involution i exchanges the points on the fibers of f , whence $x_2 = i(x_1)$ and $x_4 = i(x_3)$.

Conversely, for any x_1 and x_3 , a function φ with divisor $(x_1) + (i(x_1)) - (x_3) - (i(x_3))$ is given by $\varphi = \sigma \circ \pi$, where π is the quotient $\mathbf{C} \rightarrow \mathbf{C}/i$ modulo the hyperelliptic involution and $\sigma: \mathbf{C}/i \rightarrow \mathbf{P}^1$ is an isomorphism which maps $\pi(x_1) = \pi(i(x_1))$ to 0 and $\pi(x_3) = \pi(i(x_3))$ to ∞ . This implies that $s(x_1) + s(i(x_1)) = s(x_3) + s(i(x_3))$ holds in $\mathbf{J}(k)$. In particular, the element $s(x) + s(i(x))$ in $\mathbf{J}(k)$ is independent of $x \in \mathbf{C}(k)$. If we denote it by a , then we have $a - s(x) = s(i(x))$ for all x , so that $s(\mathbf{C}(k))$ is a symmetric Sidon set with center a .

Now assume that \mathbf{m} has degree ≥ 2 . If x_1, \dots, x_4 are such that $s(x_1) + s(x_2) = s(x_3) + s(x_4)$ and $x_1 \notin \{x_3, x_4\}$, then by comparing with $\mathbf{m}' = 0$, we deduce that we must have $x_2 = i(x_1)$ and $x_4 = i(x_3)$. Consider the function $\varphi = \sigma \circ \pi$ described previously. The Sidon equation in $\mathbf{J}_{\mathbf{m}}$ requires that for all p in the support of \mathbf{m} , the value of $\varphi(p)$ is the same, which can only be the case if \mathbf{m} has degree 2 since φ itself has degree 2. As a first consequence, this means that the image of \mathbf{C} is a Sidon set if $\deg(\mathbf{m}) \geq 3$.

On the other hand, if $\mathbf{m} = (p) + (q)$, then $\varphi(p) = \varphi(q)$ if and only if $q = i(p)$. Thus the image of s is again a Sidon set if this is not the case. Finally, if \mathbf{m} is of this form, then we do have $\varphi(p) = \varphi(i(p))$ (resp. $\varphi - \varphi(p)$ has a zero of order 2 at p , if $p = i(p)$), so the image of s is then a symmetric Sidon set, with center the common value of $s(x) + s(i(x))$ for any $x \in \mathbf{C} - \{p\}$. \square

7. THE UNIVERSAL VECTOR EXTENSION OF AN ELLIPTIC CURVE

In the special case where the curve \mathbf{C} is an elliptic curve \mathbf{E} , with origin $0_{\mathbf{E}}$, and the modulus \mathbf{m} is $2(0_{\mathbf{E}})$, the generalized jacobian $\mathbf{E}^{\sharp} = \mathbf{J}_{2(0_{\mathbf{E}})}$ is also classically known through other interpretations, related to its identification with the so-called *universal vector extension* of \mathbf{E} (see Coleman's paper [3, Prop. 1.2] for this relation). We now present, for the sake of variety, two proofs of Theorem 1 in this case, using these alternative descriptions.

Analytic proof over the complex numbers. We use an explicit description by Katz [11, App. C] of the universal extension and the morphism s (another concrete discussion by Corvaja, Masser and Zannier can be found in [4, §3]), which applies when $k = \mathbf{C}$.

Let $\Lambda \subset \mathbf{C}$ be a lattice so that $\mathbf{E}(\mathbf{C}) \simeq \mathbf{C}/\Lambda$. Let \wp denote the Weierstrass function for Λ and ζ the Weierstrass zeta function (so that $\zeta' = -\wp$; see, e.g. [23, Ch. 20] for the classical theory of elliptic functions). Define a group homomorphism $\eta: \Lambda \rightarrow \mathbf{C}$ by setting

$$\eta(\ell) = \int_p^{p+\ell} \wp(z) dz = \zeta(p) - \zeta(p + \ell)$$

where p is any point in $\mathbf{C} - \Lambda$ and the integration path avoids Λ . Let $\Lambda^{\sharp} \subset \mathbf{C}^2$ be the subgroup of elements of the form $(\ell, -\eta(\ell))$ for $\ell \in \Lambda$.

Katz [11, p. 300–301] shows that there is an isomorphism of complex Lie groups

$$\mathbf{E}^{\sharp}(\mathbf{C}) \simeq \mathbf{C}^2/\Lambda^{\sharp}$$

which is compatible with the projection to $E(\mathbf{C}) \simeq \mathbf{C}/\Lambda$. Under this identification, the embedding $s: \tilde{E}(\mathbf{C}) = (\mathbf{C}/\Lambda) - \{0\} \rightarrow E^\sharp(\mathbf{C}) = \mathbf{C}^2/\Lambda^\sharp$ is given by the formula

$$s(\alpha) = (\alpha, \zeta(\alpha)) \bmod \Lambda^\sharp$$

(see [11, Th. C.6 (2)]).

Now let $\alpha_1, \dots, \alpha_4 \in \tilde{E}(\mathbf{C})$ satisfy

$$s(\alpha_1) + s(\alpha_2) = s(\alpha_3) + s(\alpha_4).$$

There exist representatives $(\alpha_i, \zeta(\alpha_i)) \in \mathbf{C}^2$ of $s(\alpha_i)$ such that the equation $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$ holds in \mathbf{C} . Then these representatives necessarily also satisfy

$$\zeta(\alpha_1) + \zeta(\alpha_2) = \zeta(\alpha_3) + \zeta(\alpha_4).$$

Let $x_i = (\wp(\alpha_i), \wp'(\alpha_i)) = (a_i, b_i) \in \mathbf{C}^2$ be the points in $E(\mathbf{C})$ corresponding to $\alpha_i \in \mathbf{C}/\Lambda$.

Let us first suppose that $\alpha_1 \neq \alpha_2$ and $\alpha_3 \neq \alpha_4$. By a classical formula (see [11, p. 304], citing Whittaker and Watson [23, p. 451, ex. 2]), we have

$$\zeta(\alpha_i) + \zeta(\alpha_j) = \zeta(\alpha_i + \alpha_j) + \frac{1}{2} \frac{\wp'(\alpha_i) - \wp'(\alpha_j)}{\wp(\alpha_i) - \wp(\alpha_j)},$$

so the equation becomes

$$\frac{\wp'(\alpha_1) - \wp'(\alpha_2)}{\wp(\alpha_1) - \wp(\alpha_2)} = \frac{\wp'(\alpha_3) - \wp'(\alpha_4)}{\wp(\alpha_3) - \wp(\alpha_4)},$$

or in other words

$$\frac{b_1 - b_2}{a_1 - a_2} = \frac{b_3 - b_4}{a_3 - a_4},$$

or equivalently the line joining x_1 to x_2 is parallel to the line joining x_3 to x_4 . We can then apply Lemma 7.

In the remaining cases where $\alpha_1 = \alpha_2$ (or $\alpha_3 = \alpha_4$) we argue as before with points $\alpha'_2 \neq \alpha_1$ (or $\alpha'_4 \neq \alpha_3$) converging to α_2 (or α_4) and deduce that the same condition as above holds where the slopes of the line joining α_1 to α_2 is replaced where needed by the slopes of the tangent line at α_1 (and similarly with α_3 and α_4). \square

We have yet another argument in characteristic ≥ 5 using the interpretation of E^\sharp in terms of connections and differentials of the third kind.

Proof with connections. We assume that k is algebraically closed of characteristic ≥ 5 . As explained by Katz [15], the points of E^\sharp can be interpreted as isomorphism classes of pairs (\mathcal{L}, ∇) consisting of a line bundle \mathcal{L} on E and a connection $\nabla: \mathcal{L} \rightarrow \mathcal{L} \otimes \Omega_E^1$.

Since the characteristic is at least 5, we can describe an immersion $\tilde{E} \rightarrow E^\sharp$ in that case as follows (see, for instance, [15, Lemma 2.1] or [11, C.2, C.3]). First, view E as a plane cubic curve in short Weierstrass form $Y^2 = f(X)$, and for $x = (a, b) \in \tilde{E}$, let

$$\omega_x = \frac{1}{2} \frac{Y + b}{X - a} \frac{dX}{Y}$$

(this is a meromorphic differential 1-form ω_x on E which has only simple poles at x and 0, with residue 1 at x and residue -1 at 0; classically, these are called “differentials of the third

kind" on E). We then define $s(x) = (\mathcal{L}_x, \nabla_x)$, where $\mathcal{L}_x = \mathcal{O}((x) - (0))$ and the connection ∇_x is defined for a local section ξ of \mathcal{L}_x by

$$\nabla_x(\xi) = d\xi - \xi\omega_x.$$

(which is easily checked to be well-defined).

Let again x_1, \dots, x_4 be elements of $\tilde{E}(k)$ such that $s(x_1) + s(x_2) = s(x_3) + s(x_4)$ holds. The points $s(x_1) + s(x_2)$ and $s(x_3) + s(x_4)$ are, respectively, the isomorphism classes of $(\mathcal{L}_{12}, \nabla_{12})$ and $(\mathcal{L}_{34}, \nabla_{34})$, with the notation

$$\mathcal{L}_{ij} = \mathcal{O}((x_i) + (x_j) - 2(0_E)), \quad \nabla_{ij}(\xi) = d\xi - \xi(\omega_{x_i} + \omega_{x_j}).$$

The equation implies as in the previous proof that $x_1 + x_2 = x_3 + x_4$, so that there exists a non-zero rational function $\varphi: E \rightarrow \mathbf{P}^1$ with divisor $(x_1) + (x_2) - (x_3) - (x_4)$. Multiplication by $1/\varphi$ is then an isomorphism $\mathcal{L}_{12} \rightarrow \mathcal{L}_{34}$, and there is no other isomorphism up to multiplication by a non-zero constant.

For a local section ξ of \mathcal{L}_{12} , we have

$$\frac{1}{\varphi} \nabla_{12}(\xi) = \frac{1}{\varphi} (d\xi - \xi(\omega_{x_1} + \omega_{x_2})),$$

while, on the other hand, we have

$$\nabla_{34}(\xi/\varphi) = d(\xi\varphi^{-1}) - \frac{\xi}{\varphi}(\omega_{x_3} + \omega_{x_4}) = \frac{d\xi}{\varphi} - \xi \frac{d\varphi}{\varphi^2} - \frac{\xi}{\varphi}(\omega_{x_3} + \omega_{x_4}).$$

The equation $s(x_1) + s(x_2) = s(x_3) + s(x_4)$ is therefore equivalent with the condition that the formula

$$\frac{1}{\varphi} (d\xi - \xi(\omega_{x_1} + \omega_{x_2})) = \frac{d\xi}{\varphi} - \xi \frac{d\varphi}{\varphi^2} - \frac{\xi}{\varphi}(\omega_{x_3} + \omega_{x_4})$$

holds for all local sections ξ . This boils down to the equality

$$\omega_{x_1} + \omega_{x_2} = \frac{d\varphi}{\varphi} + \omega_{x_3} + \omega_{x_4}$$

of meromorphic differentials on E .

From the known poles and residues of these differentials, we see that the difference of the left and right-hand sides has no poles, and hence is a constant multiple of the holomorphic differential dx/y . To determine the constant, say α , and check when it vanishes, we look close to 0_E . Using the uniformizer x/y , the properties of the ω_{x_i} show that $\alpha = 0$ if and only if $d\varphi/\varphi$ is 0 at 0_E .

Recall that we view \tilde{E} as a plane Weierstrass curve, and as before we can take $\varphi = \ell_{12}/\ell_{34}$, where $\ell_{ij} = \alpha_{ij}x + \beta_{ij}y + \gamma_{ij}$ defines the affine line joining x_i to x_j in the plane (resp. the tangent line to E at x_i if $x_i = x_j$). Thus

$$\frac{d\varphi}{\varphi} = \frac{d\ell_{12}}{\ell_{12}} - \frac{d\ell_{34}}{\ell_{34}}, \quad \frac{d\ell_{ij}}{\ell_{ij}} = \frac{\alpha_{ij}dx}{\ell_{ij}} + \frac{\beta_{ij}dy}{\ell_{ij}}.$$

Let $\pi = x/y$ be a uniformizer at 0_E . Then

$$\frac{\alpha_{ij}dx}{\ell_{ij}} = \left(\frac{\alpha_{ij}}{\beta_{ij}} + O(\pi) \right) \frac{dx}{y},$$

while dy/ℓ_{ij} has a pole at 0. Thus the contributions of these last terms must cancel, as well as those involving $O(\pi)$, and we find that

$$(\omega_{x_1} + \omega_{x_2}) - \left(\frac{d\varphi}{\varphi} + \omega_{x_3} + \omega_{x_4} \right) = \left(\frac{\alpha_{12}}{\beta_{12}} - \frac{\alpha_{34}}{\beta_{34}} \right) \frac{dx}{y}.$$

We therefore have $\alpha = 0$ if and only if $\alpha_{12}/\beta_{12} - \alpha_{34}/\beta_{34} = 0$, which once more means that the lines ℓ_{12} and ℓ_{34} are parallel, allowing us to conclude using Lemma 7. \square

8. FINAL QUESTIONS

We conclude with some natural questions arising from this work:

- (1) Are there other interesting examples of Sidon sets arising from algebraic geometry? In [7, § 12.2], we point out that a classical construction related to smooth cubic threefolds leads to a morphism s from a surface S to an abelian variety A of dimension 5 such that the equation $s(\ell_1) + s(\ell_2) = x$ admits generically either zero or six solutions for given $x \in A$.
- (2) How close are the Sidon sets that we construct from being *maximal*? In particular, can one embed one of the fairly dense examples into even larger Sidon sets?
- (3) What are the most general statements of existence of Sidon sets in “abstract” finite abelian groups that can be deduced from these constructions?

REFERENCES

- [1] L. Babai and V. T. Sós. Sidon sets in groups and induced subgraphs of Cayley graphs. *European J. Combin.*, 6(2):101–114, 1985.
- [2] R. W. Carter. *Finite groups of Lie type. Conjugacy classes and complex characters*. Wiley Classics Library. John Wiley & Sons, Ltd., Chichester, 1993.
- [3] R. F. Coleman. Vectorial extensions of Jacobians. *Ann. Inst. Fourier (Grenoble)*, 40(4):769–783, 1990.
- [4] P. Corvaja, D. Masser, and U. Zannier. Sharpening ‘Manin-Mumford’ for certain algebraic groups of dimension 2. *Enseign. Math.*, 59(3-4):225–269, 2013.
- [5] P. Deligne. La conjecture de Weil. II. *Publ. Math. Inst. Hautes Études Sci.*, (52):137–252, 1980.
- [6] S. Eberhard and F. Manners. The apparent structure of dense Sidon sets. *Electron. J. Combin.*, 30:1–33, 2023.
- [7] A. Forey, J. Fresán, and E. Kowalski. Arithmetic Fourier transforms over finite fields: generic vanishing, convolution, and equidistribution. [arXiv:2109.11961](https://arxiv.org/abs/2109.11961).
- [8] J. Fresán and P. Jossen. A non-hypergeometric E-function. *Ann. of Math. (2)*, 194(3):903–942, 2021.
- [9] T. Gowers. What are dense Sidon subsets of $\{1, 2, \dots, n\}$ like? Blog post, <https://gowers.wordpress.com/2012/07/13/what-are-dense-sidon-subsets-of-1-2-n-like/>.
- [10] H. Halberstam and F. K. Roth. *Sequences*. Springer, 1983.
- [11] N. M. Katz. The Eisenstein measure and p -adic interpolation. *Amer. J. Math.*, 99(2):238–311, 1977.
- [12] N. M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1990.
- [13] N. M. Katz. L-functions and monodromy: four lectures on Weil II. *Adv. Math.*, 160(1):81–132, 2001.
- [14] N. M. Katz. Larsen’s alternative, moments, and the monodromy of Lefschetz pencils. In *Contributions to automorphic forms, geometry, and number theory*, pages 521–560. Johns Hopkins University Press, Baltimore, MD, 2004.
- [15] N. M. Katz. Equidistribution questions for universal extensions. *Exp. Math.*, 23(4):452–464, 2014.
- [16] E. Kowalski and K. Soundararajan. Exponential sums, twisted multiplicativity, and moments. In A. Avila, M. Rassias, and Y. Sinai, editors, *Analysis at Large*, pages 299–332. Springer, 2022.

- [17] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002.
- [18] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.
- [19] H.-G. Rück. A note on elliptic curves over finite fields. *Math. Comp.*, 49(179):301–304, 1987.
- [20] J.-P. Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988.
- [21] J. F. Voloch. A note on elliptic curves over finite fields. *Bull. Soc. Math. France*, 116(4):455–458, 1988.
- [22] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*, volume 7 of *Publ. Inst. Math. Univ. Strasbourg*. Hermann & Cie, Paris, 1948.
- [23] E. T. Whittaker and G. N. Watson. *A course of modern analysis. An introduction to the general theory of infinite processes and of analytic functions: with an account of the principal transcendental functions*. Cambridge University Press, New York, 1962. Fourth edition. Reprinted.

(A. Forey) UNIV. LILLE, CNRS, UMR 8524 - LABORATOIRE PAUL PAINLEVÉ, F-59000 LILLE, FRANCE

Email address: `arthur.forey@univ-lille.fr`

(J. Fresán) CMLS, ÉCOLE POLYTECHNIQUE, F-91128 PALAISEAU CEDEX, FRANCE

Email address: `javier.fresan@polytechnique.edu`

(E. Kowalski) D-MATH, ETH ZÜRICH, RÄMISTRASSE 101, CH-8092 ZÜRICH, SWITZERLAND

Email address: `kowalski@math.ethz.ch`