CURVES IN THEIR JACOBIAN ARE SIDON SETS

ARTHUR FOREY AND EMMANUEL KOWALSKI

Abstract. We report new examples of Sidon sets in abelian groups arising from algebraic geometry.

Let A be an abelian group. A *Sidon set* S in A is a subset such that any solution $(x_1, x_2, x_3, x_4) \in \mathrm{S}^4$ of the equation

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

satisfies $x_1 \in \{x_3, x_4\}$, i.e., any $x \in \mathrm{A}$ is in at most one way (up to transposition) the sum of two elements of S.

We construct some natural examples of Sidon sets in certain abelian groups, arising from algebraic geometry. In some cases, we obtain a slight variant: we say that a set S in A is a *symmetric Sidon set* if there exists $a \in \mathrm{A}$ such that $\mathrm{S} = a - \mathrm{S}$ and the solutions to the equation above satisfy either $x_1 \in \{x_3, x_4\}$ or $x_2 = a - x_1$.

Proposition 1 (Diagonal). *Let k be a field. The diagonal subset*

$$\mathrm{S} = \{(x, x) \mid x \in k^\times\}$$

is a Sidon set in $k^\times \times k$.

Proof. For elements $(x_i, x_i) \in k^\times \times k$ for $1 \leqslant i \leqslant 4$, the equation (1) becomes

$$\begin{cases} x_1x_2 = x_3x_4 \\ x_1 + x_2 = x_3 + x_4. \end{cases}$$

Thus x_1 is a solution of the polynomial equation $(\mathrm{X} - x_3)(\mathrm{X} - x_4) = 0$, and hence $x_1 \in \{x_3, x_4\}$. ∎

Proposition 2 (Curves in their jacobians). *Let k be a field and let C be a smooth projective geometrically connected curve of genus $g \geqslant 2$ over k. Let A be the jacobian of C. Assume that there is a k-rational point $0_{\mathrm{C}} \in \mathrm{C}(k)$, and let $\iota\colon \mathrm{C} \to \mathrm{A}$ be the closed immersion induced by the map $x \mapsto (x) - (0_{\mathrm{C}})$.*

1. *If C is not hyperelliptic, then $\iota(\mathrm{C}(k))$ is a Sidon set in $\mathrm{A}(k)$.*
2. *If C is hyperelliptic, with hyperelliptic involution i, then $\iota(\mathrm{C}(k))$ is a symmetric Sidon set in $\mathrm{A}(k)$.*

Proof. Let x_1, x_2, x_3, x_4 be points in $\mathrm{C}(k)$ such that

$$\iota(x_1) + \iota(x_2) = \iota(x_3) + \iota(x_4).$$

A. F. and E. K. are partially supported by the DFG-SNF lead agency program grant 200020L_175755.

If $x_1 \notin \{x_3, x_4\}$, this implies the existence of a rational function on C with zeros $\{x_1, x_2\}$ and poles $\{x_3, x_4\}$, which corresponds to a morphism $f\colon \mathrm{C} \to \mathbf{P}^1$ of degree at most 2. This is not possible unless C is hyperelliptic (see [6, Def. 7.4.7]), proving (1).

On the other hand, if C is hyperelliptic, then since there exists on C a unique morphism to $\mathbf{P}^1$ of degree 2, up to automorphisms (see, e.g., [6, Rem. 7.4.30]), it follows that the hyperelliptic involution exchanges the points on the fibers of f, which means that we have $x_2 = i(x_1)$ and $x_4 = i(x_3)$. Conversely, for any x_1 and x_2, there exists a function f with divisor $(x_1) + (i(x_1)) - (x_2) - (i(x_2))$, so that the equation above holds. In particular, the element $\iota(x) + \iota(i(x))$ in $\mathrm{A}(k)$ is independent of $x \in \mathrm{C}(k)$. If we denote it by a, then we have $a - \iota(x) = \iota(i(x))$ for all x, hence $a - \iota(\mathrm{C}(k)) = \iota(\mathrm{C}(k))$, and we conclude that $\iota(\mathrm{C}(k))$ is a symmetric Sidon set. ☐

Remark 3. If k is algebraically closed, then the group $\mathrm{A}(k)$ can be described concretely as follows: we have $\mathrm{A}(k) = \mathrm{D}_0/\mathrm{P}$, where

– denoting by D the free abelian group generated by formal integral linear combinations of elements of $\mathrm{C}(k)$, the group D_0 is the subgroup such that the sum of the coefficients is equal to 0;
– P is the subgroup of D_0 formed by looking at non-zero rational functions f on C and taking the combination of the sum of the zeros of f, with multiplicity, minus the sum of the poles, with multiplicity.

If k is a finite field, with some algebraic closure $\bar{k}$, then there is a natural action of the Frobenius automorphism of k on $\mathrm{A}(\bar{k})$, and A is the set of fixed points of this action.

If C is a hyperelliptic curve, and the characteristic of k is not 2, then it can be represented by an equation $y^2 = f(x)$ for some polynomial f of degree $2g+1$ or $2g+2$, together with one or two points at infinity, one of which can be taken as the rational point $0_{\mathrm{C}} \in \mathrm{C}(k)$ if $\deg(f) = 2g+1$ or (for instance) if f is monic (see [6, Prop. 4.24]).

These propositions apply to any field k. We now specialize to finite fields k. In the case of Proposition 1, we obtain a Sidon set of size $|k| - 1$ in the group $k^\times \times k$, which is a cyclic group of order $|k|(|k|-1)$. In fact, these finite Sidon sets are "the same" as those described by Ruzsa [7, Th. 4.4] using a primitive root in $k^\times$; S. Eberhard has pointed out to us that they appear previously in a paper of Ganley [3, p. 323], who attributes the example to E. Spence.

In the case of Proposition 2, we obtain a Sidon set (or a symmetric Sidon set) $\mathrm{S} = \iota(\mathrm{C}(k))$ of size $|\mathrm{C}(k)|$ that satisfies

$$|k| - 2g\sqrt{|k|} + 1 \leqslant |\mathrm{S}| \leqslant |k| + 2g\sqrt{|k|} + 1$$

in the group $\mathrm{A} = \mathrm{A}(k)$ which satisfies

$$(\sqrt{|k|} - 1)^{2g} \leqslant |\mathrm{A}| \leqslant (\sqrt{|k|} + 1)^{2g}$$

(all these estimates follow from Weil's proof of the Riemann Hypothesis for curves over finite fields). Thus, S has size about $|\mathrm{A}|^{1/g}$.

Since there is most interest in the literature in large Sidon sets, we consider the case $g = 2$. Note that the curve C is then automatically hyperelliptic (see, e.g., [6, Prop. 4.9]), so that

$\iota(\mathrm{C}(k))$ is not a Sidon set, but keeping only one element in any pair $\{x, i(x)\}$, we obtain a Sidon set of size about $\frac{1}{2}|\mathrm{A}|^{1/2}$.

Suppose still that $g = 2$. If S has (close to) maximal size $|\mathrm{S}| = q + (4-\varepsilon)\sqrt{q} + 1$, then we get

$$|\mathrm{S}| \geqslant |\mathrm{A}|^{1/2} + (2-\varepsilon)|\mathrm{A}|^{1/4} - 2.$$

It may be interesting to note that the right-hand side is of the same shape as the upper bound $\mathrm{N}^{1/2} + \mathrm{N}^{1/4} + 1$ (essentially first proved by Erdős–Turán) for the size of a Sidon set in $\{1, \ldots, \mathrm{N}\}$.

Remark 4. (1) There has been some speculation (see the blog post [4] of T. Gowers, and the comments there) that "large" Sidon sets in $\{1, \ldots, \mathrm{N}\}$ might have some kind of algebraic structure. Since there are many hyperelliptic curves over finite fields (the space of parameters is of dimension 3), and these not infrequently have $\mathrm{A}(k)$ cyclic (see for instance the heuristic in [1]), Proposition 2 shows that such an algebraic structure must be sophisticated enough, in the range of sets of size $\alpha\sqrt{\mathrm{N}}$ for some fixed $\alpha \geqslant 1/2$, to account for jacobians of curves of genus 2 over finite fields.

(2) The fact that the sets in Propositions 1 and 2 are Sidon sets (or symmetric Sidon sets) appears naturally, and plays a key role, in our work [2, §7] in the study of the distribution of exponential sums over finite fields parameterized by characters of the groups $k^\times \times k$ or $\mathrm{A}(k)$; the (symmetric) Sidon property allows us to compute the so-called fourth moment of the relevant (tannakian) monodromy group $\mathbf{G}$, and to (almost) determine it by means of the Larsen Alternative [5].

(3) The content of Proposition 2, if not the terminology, was apparently first noticed by N. Katz (unpublished).

References

[1] W. Castryck, A. Folsom, H. Hubrechts, and A. Sutherland: *The probability that the number of points on the Jacobian of a genus 2 curve is prime*, Proc. London Math. Soc. 104 (2012), 1235–1270.

[2] A. Forey, J. Fresán, and E. Kowalski: *Generic vanishing, tannakian categories, and equidistribution*, in preparation.

[3] M.J. Ganley: *Direct product difference sets*, Journal Combinat. Theory A 23 (1977), 321–332.

[4] T. Gowers: *What are dense sidon subsets of $\{1, 2 \ldots, n\}$ like?*, blog post, https://gowers.wordpress.com/2012/07/13/what-are-dense-sidon-subsets-of-12-n-like/.

[5] N. M. Katz: *Larsen's alternative, moments, and the monodromy of Lefschetz pencils*, in *Contributions to automorphic forms, geometry, and number theory*, Johns Hopkins Univ. Press, Baltimore, MD, 2004, 521–560.

[6] Q. Liu: *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics 6, Oxford University Press, 2002.

[7] Imre Z. Ruzsa: *Solving a linear equation in a set of integers, I*, Acta Arith. 65 (1993), 259–282.

(A. Forey) D-MATH, ETH Zürich, Rämistrasse 101, CH-8092 Zürich, Switzerland

Email address: arthur.forey@math.ethz.ch

(E. Kowalski) D-MATH, ETH Zürich, Rämistrasse 101, CH-8092 Zürich, Switzerland

Email address: kowalski@math.ethz.ch