The apparent structure of dense Sidon sets

Sean Eberhard[*]
Mathematical Sciences Research Centre
Queen's University Belfast
Belfast, UK
s.eberhard@qub.ac.uk

Freddie Manners[†]
Department of Mathematics
University of California, San Diego
La Jolla, California, U.S.A.
fmanners@ucsd.edu

Submitted: Apr 15, 2022; Accepted: Dec 5, 2022; Published: Feb 24, 2023

Abstract

The correspondence between perfect difference sets and transitive projective planes is well-known. We observe that all known dense (i.e., close to square-root size) Sidon subsets of abelian groups come from projective planes through a similar construction. We classify the Sidon sets arising in this manner from desarguesian planes and find essentially no new examples. There are many further examples arising from nondesarguesian planes.

We conjecture that all dense Sidon sets arise from finite projective planes in this way. If true, this implies that all abelian groups of most orders do not have dense Sidon subsets. In particular if σ_n denotes the size of the largest Sidon subset of $\mathbf{Z}/n\mathbf{Z}$, this implies $\liminf_{n\to\infty} \sigma_n/n^{1/2} < 1$.

We also give a brief bestiary of somewhat smaller Sidon sets with a variety of algebraic origins, and for some of them provide an overarching pattern.

Mathematics Subject Classifications: 05B10,11B13

1 Dense Sidon sets

Let G be an abelian group. A *Sidon set* (or B_2 *set*) is a subset $S \subset G$ such that

$$x + y = z + w \implies \{x, y\} = \{z, w\} \qquad (x, y, z, w \in S).$$

We call a solution (x, y, z, w) to $x + y = z + w$ an *additive quadruple*, and a *trivial additive quadruple* if $\{x, y\} = \{z, w\}$, so a Sidon set is a set all of whose additive quadruples are trivial. We call S a *perfect difference set* if moreover $S - S = G$.

[*] SE has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 803711) and from the Royal Society.

[†] FM is supported by a 2022 Sloan Research Fellowship.

Sidon sets are interesting in additive combinatorics for being extremely unstructured: they have maximum doubling constant and minimum additive energy (see [TV10, Chapter 2] for the definitions of these terms). It is curious therefore that all known Sidon sets which are nearly as large as possible appear to be rather structured in some other way (while for instance Sidon sets constructed randomly or greedily have much smaller size). As Ruzsa put it, "somehow all known constructions of dense Sidon sets involve the primes" ([Ruz99, Section 11]).

Let S be a Sidon set in an abelian group G of order n. Since the differences $x - y$ with $x \neq y$ are all distinct and nontrivial, we must have $|S|(|S|-1) \leqslant n-1$, or $|S|^2 - |S| + 1 \leqslant n$. Call S *dense* if $|S| \geqslant (1 - o(1))n^{1/2}$. The following are the best-known examples of dense Sidon sets.

Construction 1 (Erdős–Turán [ET41])**.** We give this example first, slightly out of chronological order, because it is the simplest to describe and understand. Let K be a finite field. Assume $\operatorname{char} K \neq 2$. Let $G = K^2$. Let S be the parabola

$$S = \{(x, x^2) : x \in K\}.$$

It is a simple exercise to check the Sidon property. Suppose

$$(x, x^2), (y, y^2), (z, z^2), (w, w^2)$$

form an additive quadruple. Then

$$\begin{aligned} x + y &= z + w \\ x^2 + y^2 &= z^2 + w^2. \end{aligned}$$

Hence

$$2xy = (x+y)^2 - (x^2 + y^2) = (z+w)^2 - (z^2 + w^2) = 2zw.$$

Since $\operatorname{char} K \neq 2$, $xy = zw$. Hence the polynomials $(t - x)(t - y)$ and $(t - z)(t - w)$ are equal, so $\{x, y\} = \{z, w\}$.

Parameters: $|G| = q^2$ and $|S| = q$, where $q = |K|$.

Construction 2 (Singer [Sin38])**.** Let K be a finite field and let L be an extension of K of degree 3. Let $G = L^\times / K^\times$. Let H be a K-plane in L, say

$$H = \{x \in L : \operatorname{tr} x = 0\}.$$

Let $S = (H \cap L^\times)/K^\times$.

To check the Sidon property, suppose $x, y, z, w \in S$ form an additive quadruple. Let $\widetilde{x}, \widetilde{y}, \widetilde{z}, \widetilde{w}$ be lifts to $L^\times$. Then $\widetilde{x}\widetilde{y}\widetilde{z}^{-1}\widetilde{w}^{-1} \in K^\times$. Let

$$H' = \widetilde{x}\widetilde{z}^{-1} H = \widetilde{w}\widetilde{y}^{-1} H.$$

Note that H and H' both contain both $\widetilde{x}$ and $\widetilde{w}$. Hence either $H = H'$ or $\widetilde{x}/\widetilde{w} \in K^\times$. In other words, either $x = z$ or $x = w$, as required.

Parameters: $|G| = q^2 + q + 1$ and $|S| = q + 1$, where $q = |K|$ (S is a perfect difference set).

Construction 3 (Bose [Bos42])**.** Let K be a finite field and let L be an extension of K of degree 2. Let $G = L^\times$. Let H be a K-line in L, let $u \in L \setminus H$, and let $S = u + H$.

The verification of the Sidon property is much as in Construction 2.

Parameters: $|G| = q^2 - 1$ and $|S| = q$, where $q = |K|$.

Construction 4 (Spence: see Ganley [Gan77], Ruzsa [Ruz93, Theorem 4.4])**.** Let K be a finite field, let $G = K^\times \times K$, and let $S = \{(x, x) : x \in K^\times\}$.

If $(x, x), (y, y), (z, z), (w, w)$ form an additive quadruple then $x+y = z+w$ and $xy = zw$, so $\{x, y\} = \{z, w\}$, as in Construction 1.

Parameters: $|G| = q(q - 1)$ and $|S| = q - 1$, where $q = |K|$.

Construction 5 (Hughes [Hug55], Cilleruelo [Cil12, Example 3])**.** Let K be a finite field, let $G = K^\times \times K^\times$, and let $S = \{(x, y) : x, y \neq 0, x + y = 1\}$.

Suppose $(x, 1 - x), (y, 1 - y), (z, 1 - z), (w, 1 - w)$ form an additive quadruple. Then

$$\begin{aligned} xy &= zw \\ (1 - x)(1 - y) &= (1 - z)(1 - w). \end{aligned}$$

We deduce $x + y = z + w$, and it follows that $\{x, y\} = \{z, w\}$ as in Constructions 1 and 4.

Parameters: $|G| = (q - 1)^2$ and $|S| = q - 2$, where $q = |K|$.

In the literature there is particular emphasis on Sidon sets in cyclic groups, since those may be used to define Sidon sets in $\mathbf{Z}$. The groups in Constructions 2 and 3 are cyclic, the groups in Constructions 1 and 5 are not, and the group in Construction 4 is cyclic if and only if q is prime. In this paper we are equally interested in all abelian groups.

Our first main observation is that the five constructions presented above are not as varied as they appear. In fact there is a correspondence with the largest abelian subgroups of $\mathrm{PGL}_3(K)$. The correspondence associates to each abelian subgroup $G \leqslant \mathrm{PGL}_3(K)$ the Sidon set given as the point-line stabilizer

$$S = \{g \in G : p^g \in \ell\},$$

for some point p and line ℓ in the projective plane $\mathbf{P}^2(K)$ such that the stabilizers G_p and G_ℓ are trivial. There are essentially no further examples in this correspondence. All this is covered in Section 2 and Section 3.

On the other hand, the correspondence is valid for arbitrary finite projective planes, desarguesian[1] or not. The plane should have a large abelian group of automorphisms, playing the role of $G \leqslant \mathrm{PGL}_3(K)$ in the desarguesian case, which significantly constrains the projective planes to be considered. Nevertheless, many further examples arise in this way; see Section 4.

Conversely, the correspondence also shows that any dense Sidon set gives rise to an object that is "almost" a projective plane. We cannot show, but it is natural to conjecture, that these objects are always true projective planes with some points and lines missing,

[1] A projective plane is called *desarguesian* if it satisfies Desargues's theorem. Desarguesian finite projective planes are exactly those of the form $\mathbf{P}^2(K)$ for some finite field K.

meaning that all dense Sidon sets are obtained from projective planes. We will state some precise conjectures of this form in Section 5.

Assuming this conjecture, known results on projective planes having large abelian automorphism groups (specifically, the Dembowski–Piper classification) limits which abelian groups G could possibly admit dense Sidon sets $S \subseteq G$. In particular, the conjecture would imply that $\liminf_{n\to\infty} \max\bigl\{|S| \colon S \subseteq \mathbf{Z}/n\mathbf{Z} \text{ Sidon}\bigr\}/n^{1/2} < 1$.

Even Sidon sets which are significantly smaller than $(1 - o(1))n^{1/2}$, e.g., by a constant factor or a power of $\log n$, seem to be rather structured, although the situation is less rigid. In Section 6 we gather some apparently varied existing constructions, and show—similarly to the dense case above—that many of them fit a common pattern. We also use this general pattern to generate new examples.

1.1 Notation

We adopt the group-theoretic conventions that, for a group G acting on a set X and $g \in G$, $x \in X$, x^g denotes the action of g on x and G_x denotes the stabilizer of x in G. We will also use standard big O and little o notation occasionally (as we have done already), as well as the Vinogradov notation $X \ll Y$ to mean $X = O(Y)$.

2 The correspondence

An *incidence structure* $\mathcal{L}$ is abstractly just a triple (P, L, I) of sets such that $I \subset P \times L$ (this is also the abstract definition of a bipartite graph). Conventionally we call the elements of P *points*, the elements of L *lines*, and the elements of I *incidences*. We say that $p \in P$ and $\ell \in L$ are *incident* if $(p, \ell) \in I$, and we may write $p \in \ell$. We freely use further geometric language: we say ℓ and ℓ' intersect if there is a point p incident to both of them, we say p and p' are joined by a line if there is a line incident to both of them, etc. The following definitions, of increasing specialization, are standard.

1. An incidence structure $\mathcal{L}$ is a *partial linear space* if any two distinct points are incident with at most one line. (Equivalently, the bipartite graph defined by $I \subset P \times L$ contains no C_4.)
2. A partial linear space $\mathcal{L}$ is
   (a) a *linear space* if any two points are joined by a line,
   (b) a *dual linear space*[2] if any two lines intersect.
3. A partial linear space which is both a linear space and a dual linear space is a *projective plane*.

[2] sometimes a *semiplane* or a *partial projective plane*

A *collineation* or *morphism* ϕ between incidence structures $\mathcal{L} = (P, L, I)$ and $\mathcal{L}' = (P', L', I')$ is a pair of maps $P \to P'$ and $L \to L'$ (both denoted ϕ) such that

$$p \in \ell \implies p^\phi \in \ell^\phi.$$

As usual, an *isomorphism* is a morphism with an inverse morphism. We write $\operatorname{Aut} \mathcal{L}$ for the group of automorphisms of $\mathcal{L}$.

Now let G be an abelian group. The following proposition articulates a basic equivalence between Sidon sets $S \subset G$ and partial linear spaces $\mathcal{L}$ with a regular G-action.

Proposition 2.1. *Suppose $\mathcal{L}$ is a partial linear space and G is an abelian subgroup of $\operatorname{Aut} \mathcal{L}$ such that the action of G is regular on both points and lines. Then for any point p and line ℓ, the set*

$$S = \{g \in G : p^g \in \ell\}$$

is a Sidon set in G.

Conversely, suppose G is an abelian group and $S \subset G$. The development $\operatorname{dev}(S)$ *of S is the incidence structure (P, L, I) with $P = L = G$ and*

$$I = \{(p, \ell) \in G^2 : p - \ell \in S\}.$$

The incidence structure $\operatorname{dev}(S)$ *is a partial linear space if (and only if) S is a Sidon set. Every point is contained in $|S|$ lines and every line contains $|S|$ points, and G acts regularly on both points and lines.*

Proof. For the first part, suppose $x, y, z, w \in S$ and $xz^{-1} = wy^{-1}$. Let

$$q = p^{xz^{-1}} = p^{wy^{-1}}.$$

Then

$$p, q \in \ell^{z^{-1}}, \ell^{y^{-1}}.$$

Since $\mathcal{L}$ is a partial linear space, this implies $p = q$ or $\ell^{z^{-1}} = \ell^{y^{-1}}$. Since the action is regular, this implies $x = z$ or $y = z$. Hence S is a Sidon set, as claimed.

For the second part, let $\mathcal{L} = \operatorname{dev}(S)$, and suppose $p_1, p_2 \in \ell_1, \ell_2$. Then $p_1 - \ell_1, p_1 - \ell_2, p_2 - \ell_1, p_2 - \ell_2 \in S$. Since

$$(p_1 - \ell_1) + (p_2 - \ell_2) = (p_1 - \ell_2) + (p_2 - \ell_1),$$

the Sidon condition implies that $p_1 = p_2$ or $\ell_1 = \ell_2$. Hence $\mathcal{L}$ is a partial linear space. The further claims are clear. □

Remark 2.2. The dual $\mathcal{L}^*$ of an incidence structure $\mathcal{L}$ is the incidence structure (L, P, I^*), where $I^* = \{(\ell, p) : (p, \ell) \in I\}$. An incidence structure $\mathcal{L}$ is *self-dual* if $\mathcal{L} \cong \mathcal{L}^*$. The development $\operatorname{dev}(S)$ of a set $S \subset G$ is always self-dual: the dual incidence set is $\operatorname{dev}(-S)$, and the maps $P \to L^*$, $x \mapsto -x$ and $L \to P^*$, $x \mapsto -x$ define an isomorphism.

Remark 2.3. Proposition 2.1 is well-established in the design theory literature in the extreme case of perfect difference sets and projective planes, but less well-known in the general case. The reason is more cultural than mathematical: design theorists are not interested in Sidon sets beyond the cases of difference sets and relative difference sets, while additive-combinatorialists are interested in quite sparse Sidon sets (anything above cube-root density, usually in $\{1, \dots, n\}$) and the development $\operatorname{dev}(S)$ is less interesting in that case.

Recall that for any projective plane $\mathcal{P}$ there is a positive integer q, called the *order* of $\mathcal{P}$, such that there are $q^2 + q + 1$ points, $q^2 + q + 1$ lines, and the incidence graph is $(q + 1)$-regular.

Corollary 2.4. *Let $\mathcal{P}$ be a projective plane of order q, and let G be an abelian subgroup of $\operatorname{Aut} \mathcal{P}$. Let p be a point and ℓ a line such that $G_p = G_\ell = 1$, and suppose ℓ contains d points of $P \setminus Gp$. Then $S = \{g \in G : p^g \in \ell\}$ is a Sidon set of size $q + 1 - d$, and*

$$d \leqslant (q + 1)\left(\frac{q^2 + q + 1}{|G|} - 1\right). \tag{2.1}$$

Proof. A partial linear space with a regular G-action is obtained by restricting to the orbits of p and ℓ, so the fact that S is a Sidon set follows from Proposition 2.1. Since ℓ contains $q + 1 - d$ points of Gp and the action of G on Gp is regular, it is clear that $|S| = q + 1 - d$. We must prove the bound on d.

Consider the bipartite incidence graph between $P \setminus Gp$ and $G\ell$. The degree of each vertex in $G\ell$ is d, while the degree of each vertex in $P \setminus Gp$ is at most $q+1$, so by counting edges we have

$$d|G| \leqslant (q + 1)(q^2 + q + 1 - |G|).$$

Rearranging gives (2.1). □

Note that Corollary 2.4 guarantees a dense Sidon set if and only if $|G| = (1 - o(1))(q^2 + q + 1)$. In other words, almost all the points of $\mathcal{P}$ must be in a single G-orbit and the same for the lines. We will see that this is a harsh restriction.

3 Desarguesian constructions

The desarguesian projective plane $\mathbf{P}^2(K)$ over the finite field K is defined by taking the points and lines to be the lines and planes, respectively, in the three-dimensional vector space K^3, with incidence defined naturally. In this section we establish that the five constructions of Sidon sets listed in the introduction arise from Corollary 2.4 applied to $\mathbf{P}^2(K)$ and the maximal abelian subgroups of $\mathrm{PGL}_3(K)$.[3] No further examples arise in this way (apart from a variant of Construction 1 in even characteristic).

[3] It was previously observed by Tait and Timmons [TT16] that the Cayley graph of the Bose Sidon set (Construction 3) is a large subset of an "orthogonal polarity graph", i.e., $\mathbf{P}^2(K)$ with the points and lines identified by a self-duality. This is essentially a special case of this general correspondence. In unpublished work, Timmons made similar observations about the Erdős–Turán and Spence examples (Constructions 1 and 4) (Michael Tait, personal communication).

Proposition 3.1. *Let K be the finite field $\mathbf{F}_q$. Let $Z \cong K^\times$ be the center of $\mathrm{GL}_3(K)$. The maximal abelian subgroups of $\mathrm{PGL}_3(K) = \mathrm{GL}_3(K)/Z$, are, up to conjugacy:*

(i) identifying K^3 with the field $L = \mathbf{F}_{q^3}$, the cyclic group $L^\times/K^\times$;

(ii) identifying K^3 with $L \times K$ where $L = \mathbf{F}_{q^2}$, the group $L^\times K^\times/K^\times$;

(iii) the group $(K^\times)^3/Z \cong (K^\times)^2$ of diagonal matrices mod Z;

(iv)

$$\left\{ \begin{pmatrix} r & a & 0 \\ 0 & r & 0 \\ 0 & 0 & 1 \end{pmatrix} : r \in K^\times,\ a \in K \right\} Z/Z \cong K^\times \times K;$$

(v)

$$\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} : a, b \in K \right\} Z/Z \cong \begin{cases} K^2 & : q \text{ odd}, \\ C_4^d & : q = 2^d; \end{cases}$$

(vi)

$$\left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} : a, b \in K \right\} Z/Z \cong K^2;$$

(vii)

$$\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a, b \in K \right\} Z/Z \cong K^2,$$

(viii) (only if $q \equiv 1 \pmod 3$) the group $\langle g, h\rangle Z/Z \cong C_3 \times C_3$, where

$$g = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \qquad h = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

where $\omega \in K$ is a primitive cube root of unity;

(ix) (only if $q \equiv 1 \pmod 3$) identifying K^3 with $L = \mathbf{F}_{q^3}$, the group

$$\langle (K^\times)^{1/3}, \mathrm{Frob}_q \rangle K^\times/K^\times \cong C_3 \times C_3,$$

where Frob_q is the $x \mapsto x^q$ automorphism of L/K.

Proof. It is equivalent to classify maximal subgroups $G \leqslant \mathrm{GL}_3(K)$ such that $Z \leqslant G$ and $G' \leqslant Z$.

First suppose $G' = 1$. Let $g \in G$. If $h \in G$ then h preserves the generalized eigenspaces of g over $\bar{K}$, the algebraic closure of K. If g has an eigenvalue of degree 3 then we are in case *(i)*, while if g has an eigenvalue of degree 2 then we are in case *(ii)*. Hence we may assume all eigenvalues of all $g \in G$ are in K.

Let m be maximum number of distinct eigenvalues of any $g \in G$, so $m \in \{1, 2, 3\}$. If $m = 3$ then we are in case *(iii)*. Suppose $m = 2$. Then some $g \in G$ has two distinct eigenvalues, one with algebraic multiplicity 2, so G preserves a decomposion of the form $K^3 = U \oplus W$ where $\dim U = 2$ and $\dim W = 1$. By maximality, G is the direct product of its projections to $\mathrm{GL}(U) \cong \mathrm{GL}_2(K)$ and $\mathrm{GL}(W) \cong K^\times$. In the $\mathrm{GL}_2(K)$ factor, each element must have the form scalar × unipotent, so we can assume G is upper-triangular.[4] This is case *(iv)*.

Hence assume $m = 1$, so all $g \in G$ have the form scalar × unipotent, and again we may choose a basis in which G is upper-triangular. Since G is maximal, $G = ZU$ for some unipotent subgroup

$$U \leqslant \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}.$$

Since U is abelian, we must have

$$U = \left\{ \begin{pmatrix} 1 & tx_0 & z \\ 0 & 1 & ty_0 \\ 0 & 0 & 1 \end{pmatrix} : t, z \in K \right\} \qquad (x_0, y_0 \in K).$$

By conjugating by a diagonal matrix can assume $x_0, y_0 \in \{0, 1\}$, and by maximality $(x_0, y_0) \in \{(1, 1), (0, 1), (1, 0)\}$, giving cases *(v)*, *(vi)*, and *(vii)*, respectively.

Now suppose G' is a nontrivial subgroup of Z. Pick $g, h \in G$ such that $[g, h]$ is some nontrivial scalar $\omega \in K$. Then h permutes the generalized eigenspaces of g and the eigenvalues according to $\lambda \mapsto \omega\lambda$, so we must have $\omega^3 = 1$ and g has eigenvalues $\lambda, \omega\lambda, \omega^2\lambda$ for some $\lambda \in \bar{K}$. The determinant of g is λ^3, so $\lambda \in (K^\times)^{1/3}$. Similarly, h has eigenvalues $\mu, \omega\mu, \omega^2\mu$ for some $\mu \in (K^\times)^{1/3}$.

We claim that $G = \langle g, h\rangle Z$. Suppose $x \in G$. Then $[x, g], [x, h] \in Z$, so $[x, g] = \omega^i$ and $[x, h] = \omega^j$ for some $i, j \in \{0, 1, 2\}$. Let $y = xg^{-j}h^i$. Then $[y, g] = [y, h] = 1$. But the centralizer of $\{g, h\}$ is Z, so $y \in Z$, so $x \in \langle g, h\rangle Z$.

Suppose $\lambda, \mu \in K$. By replacing g and h with g/λ and h/μ we may assume $\lambda = \mu = 1$. Then $g^3 = h^3 = 1$, and there is a basis in which g and h have the form stated in case *(viii)*.

Alternatively suppose one of λ and μ is not in K, say λ. By replacing h with hg or hg^2 we may assume $\mu \in K$, and then by replacing h with h/μ we may assume $\mu = 1$ and hence $h^3 = 1$. Since λ has degree 3 over K, we may identify K^3 with $L = \mathbf{F}_{q^3}$ in such a way that g is multiplication by λ. Since h is an $\mathbf{F}_q$-linear map which sends $\lambda \mapsto \omega\lambda \mapsto \omega^2\lambda \mapsto \lambda$, it must be Frob_q or Frob_q^2. Hence we get case *(ix)*. □

Remark 3.2. The subgroup structure of $\mathrm{PSL}_3(\mathbf{F}_q)$ was completely determined by Mitchell and Hartley in the early 20th century: see the survey by King [Kin05, Section 2.2]. The

[4] Unipotent subgroups can be upper-triangularized: see [Weh73, Corollary 1.21]. Alternatively, it is elementary that commuting sets of matrices can be upper-triangularized (over any field containing all their eigenvalues), by finding a common eigenvector e_1 and using induction on the quotient by $\langle e_1\rangle$.

theorem above is essentially a special case of those classical results (apart from the wrinkle to do with PGL vs PSL).

Generally, maximal subgroups of classical groups are classified by a famous theorem of Aschbacher [Asc84]. However, maximal abelian subgroups are usually *not* maximal subgroups.

Via Corollary 2.4, the subgroups *(i)–(v)* give precisely the five constructions from the introduction (not in that order). Let us recover, for example, Construction 1. The subgroup *(v)* is

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix} : a, b \in K \right\} Z/Z \cong \begin{cases} K^2 & : q \text{ odd}, \\ C_4^d & : q = 2^d. \end{cases}$$

In Corollary 2.4 take $p = (0:0:1)$ and $\ell = \{(X:Y:Z) : X = 0\}$. Then the point–line stabilizer $\{g \in G : p^g \in \ell\}$ is the subgroup defined by $b = 0$. If q is odd, an isomorphism between K^2 and G is given by

$$(x, y) \mapsto \begin{pmatrix} 1 & x & y + x(x-1)/2 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence a Sidon subset of K^2 is defined by $y + x(x-1)/2 = 0$, which is indeed equivalent to Construction 1 up to a change of coordinates. If q is even, we find a Sidon subset of C_4^d of size 2^d. An analogous derivation of the other constructions is left as amusement for the reader.

The four other cases *(vi)–(ix)* of Proposition 3.1 are unproductive from the point of view of Corollary 2.4. Indeed, (*vi*) has no large line orbit while (*vii*) has no large point orbit, and the other cases are simply too small.

While the previous proposition classifies maximal abelian subgroups of $\mathrm{PGL}_3(K)$, the fundamental theorem of projective geometry asserts that the full collineation group $\operatorname{Aut} \mathbf{P}^2(K)$ is the projective *semilinear* group

$$\mathrm{P\Gamma L}_3(K) \cong \mathrm{PGL}_3(K) \rtimes \mathrm{Gal}(K),$$

where $\mathrm{Gal}(K)$ is the Galois group of K over the prime subfield $\mathbf{F}_p$. There are many further maximal abelian subgroups of $\mathrm{P\Gamma L}_3(K)$ not contained in $\mathrm{PGL}_3(K)$, but the following proposition establishes that, like the cases *(vi)–(ix)* of Proposition 3.1, they are not useful for Corollary 2.4.

Proposition 3.3. *Let G be an abelian subgroup of $\mathrm{P\Gamma L}_3(K)$ not contained in $\mathrm{PGL}_3(K)$. Then $|G| \ll q$.*

The proof of this proposition is somewhat off-topic so is placed in Appendix A.

4 Nondesarguesian constructions

We now consider Sidon sets coming from nondesarguesian planes. Although a dizzying variety of nondesarguesian projective planes are known (see [Wei07] or [JJB07]), the existence of a large abelian group of collineations cuts down the possibilities considerably, as established by a fundamental classification theorem of Dembowski and Piper [DP67]. Since we will rely on this theory in the next section, we now briefly summarize what is known and conjectured in this area.

Let G be an abelian (or, more generally, quasiregular) collineation group of a projective plane $\mathcal{P}$ of order q, and assume $|G| > \frac{1}{2}(q^2+q+1)$. Let t be the number of point orbits. It is possible to show that t is also the number of line orbits. Let F be the incidence structure consisting of the fixed points and the fixed lines. The Dembowski–Piper classification asserts that one of the following holds (the labelling of the cases is standard):

(a) $|G| = q^2+q+1$, $t=1$, and F is empty. In this case G is transitive.

(b) $|G| = q^2$, $t=3$, and F is a flag, i.e., an incident point-line pair.

(c) $|G| = q^2$, $t=q+2$, and F is either a line and all its points or dually a point and all its lines.

(d) $|G| = q^2-1$, $t=3$, and F is an antiflag, i.e., a nonincident point-line pair.

(e) $|G| = q^2-q^{1/2}$, $t=2$, and F is empty. In this case one point orbit and one line orbit form a subplane of order $q^{1/2}$.

(f) $|G| = q(q-1)$, $t=5$, and F consists of two points u, v, the line ℓ through u and v, and another line $\ell' \neq \ell$ through v.

(g) $|G| = (q-1)^2$, $t=7$, and F consits of the vertices and sides of a triangle.

(We have omitted a case included in [DP67] that was later shown not to arise in [GM75].)

It is conjectured[5] that all nondesarguesian planes in the Dembowski–Piper classification are type (b) (see Zhou [Zho13, Section 1.9]), and the prime power conjecture for type (b) planes is known [BJS02], so from now on assume $q=p^d$ for some prime p and $d \geqslant 1$. In even characteristic we must have $G = C_4^d$: see [Zho13]. In odd characteristic, all known examples have the following special form.

A *planar function* (often called a *perfect nonlinear function* or *bent function* in computer science literature), introduced by Dembowski and Ostrom [DO68], is a function $\phi : \mathbf{F}_q \to \mathbf{F}_q$ such that $x \mapsto \phi(x+h)-\phi(x)$ is a bijection for each $h \neq 0$. For any planar function ϕ the graph

$$S = \{(x,\phi(x)) : x \in \mathbf{F}_q\} \subset \mathbf{F}_q^2$$

is a Sidon set of size q with $\mathbf{F}_q^2 \setminus (S-S) = \{0\} \times \mathbf{F}_q \setminus \{0\}$.

[5] This is an amalgamation of several conjectures, including in particular the well-known conjecture that all cyclic projective planes are desarguesian.

If ϕ is quadratic then we get Construction 1. All planar functions over prime fields are quadratic [Glu90, RS89, Hir89], but over general finite fields many nonquadratic examples are known. Monomial examples include

$$\begin{aligned} \phi(x) &= x^{p^\alpha+1} && (q = p^d, d/(\alpha, d) \text{ odd}), \\ \phi(x) &= x^{(3^\alpha+1)/2} && (q = 3^d, (\alpha, 2d) = 1). \end{aligned}$$

The latter example was a breakthrough discovery of Coulter and Matthews [CM97]. There is a conjecture that these are in fact the only monomial examples: see Zieve [Zie15] for progress on this conjecture.

All known examples of planar functions besides the Coulter–Matthews functions have the generalized quadratic form (sometimes called a Dembowski–Ostrom polynomial)

$$\phi(x) = \sum_{i,j=0}^{d-1} a_{ij} x^{p^i+p^j}. \tag{4.1}$$

It is easily proved that ϕ is planar function if and only if the polarization

$$\beta(x, y) = \phi(x + y) - \phi(x) - \phi(y) = \sum_{i,j=0}^{d-1} a_{ij}(x^{p^i} y^{p^j} + x^{p^j} y^{p^i})$$

is nondegenerate in the sense that

$$\beta(x, y) = 0 \implies x = 0 \text{ or } y = 0. \tag{4.2}$$

For example, following [CM97, Theorem 3.4], consider $q = 3^d$, d odd, and

$$\phi(x) = x^{10} \pm x^6 - x^2.$$

The polarization is

$$\beta(x, y) = xy^9 + x^9y \mp x^3y^3 + xy = xy((x^4 + y^4)^2 + (x^2y^2 \pm 1)^2).$$

Since $a^2 + b^2 = 0$ implies $a = b = 0$ in K, the second factor is never zero, so β is nondegenerate and ϕ is a planar function.

Classifying planar functions of the form (4.1) is equivalent to classifying symmetric bilinear maps $\beta : \mathbf{F}_p^d \times \mathbf{F}_p^d \to \mathbf{F}_p^d$ satisfying nondegeneracy (4.2), which in turn is equivalent to classifying commutative semifields up to isotopy. See Kantor [Kan06] for a slew of examples.

5 Conjectures

Recall that a Sidon subset S of a group G of order n is called *dense* if $|S| \geqslant (1 - o(1))n^{1/2}$. The examples we know (just Constructions 1 to 5 and the examples in Section 4) point to the following conjecture.

Conjecture 5.1. Suppose S is a dense Sidon set in an abelian group G of order n. Then G acts faithfully on a projective plane $\mathcal{P}$ of size $|\mathcal{P}| = (1 + o(1))n$ in such a way that for some point p and line ℓ, $S \subset \{g \in G : p^g \in \ell\}$.

Equivalently, the development $\operatorname{dev}(S)$ may be completed to a projective plane by adding $o(|G|)$ points and lines. The following conjecture is slightly weaker.

Conjecture 5.2. Suppose S is a dense maximal Sidon set in a group G of order n. Then $T = G \setminus (S - S) \cup 0$ is the union of $O(1)$ subgroups.

For example, in Construction 5, T is the union of three subgroups. It may be that this is the worst case.

We have no idea how to approach these conjectures. Maybe they are false and we are just bad at constructing examples. We are unable to solve even the following basic cases.

Conjecture 5.3. Let $G = \mathbf{F}_p^2$. Suppose $S \subset G$ is a Sidon set of size p. Then $T = G \setminus (S - S) \cup 0$ is a subgroup of order p.

Note that if the conclusion above holds then S is a linear transformation of the graph of a function. By the results cited in Section 4, it then follows that S is a parabola. This problem was independently posed by Cilleruelo: see [CRS18, Problem 3].

Conjecture 5.4 (Michael Tait, personal communication)**.** Let p be a (sufficiently large) prime and let $G = C_{p^2+p+1}$. Suppose $S \subset G$ is a Sidon set of size p. Then S is a subset of some perfect difference set S' of size $p + 1$.

If true, however, Conjecture 5.1 places serious constraints on which abelian groups admit dense Sidon subsets, since we can import the constraints mentioned in Section 4. One concrete example is the following.

Corollary 5.5. *Suppose Conjecture 5.1 holds. Then there is a constant $\varepsilon > 0$ such that the following is true. Suppose S is a dense Sidon set in an abelian group G of order n, and suppose $|S| > (1 - \varepsilon)n^{1/2}$. Then*

$$|G| \in \{q^2 + q + 1, q^2, q^2 - 1, q^2 - q^{1/2}, q(q - 1), (q - 1)^2\}$$

for some integer $q > 1$. In particular,

$$\liminf_{n\to\infty} \max\bigl\{|S| \colon S \subseteq \mathbf{Z}/n\mathbf{Z} \text{ Sidon}\bigr\}/n^{1/2} < 1.$$

Proof. Suppose there is no such constant $\varepsilon > 0$. Then there is a sequence of abelian groups G_i of order n_i and Sidon sets $S_i \subset G_i$ such that $|S_i| \geqslant (1 - o(1))n_i^{1/2}$ and such that n_i is not of any of the given forms. Assuming Conjecture 5.1 holds, G_i acts faithfully on a projective plane $\mathcal{P}_i$ of size $|\mathcal{P}_i| = (1 + o(1))n_i$. In particular $n_i > |\mathcal{P}_i|/2$. Now the Dembowski–Piper classification gives a contradiction. □

Further refinements are possible if we also assume some of the conjectures discussed in Section 4. For example, it should be true that if G admits a dense Sidon set then either it is one of the groups appearing in Proposition 3.1, or $|G| = q^2$ for q a prime power. Extracting further consequences of this type is left to the reader.

6 Less dense Sidon sets

6.1 Background

As we have mentioned, random or greedy constructions of Sidon sets in a group of order n tend to have size only $n^{1/3}$ or so, while Sidon sets of size $(1-o(1))n^{1/2}$ appear to have very restricted structure. Between these two extremes there is a lot of variety and it is unclear what if any sort of structure should exist in general.

As in the introduction, we collect some examples of these less dense Sidon sets (both published and unpublished) and in some cases their justifications, so that we may later observe a general pattern. In accordance with Ruzsa's maxim, the constructions all involve the primes in some way.

First, Ruzsa [Ruz98] constructed an infinite Sidon set containing $n^{\sqrt{2}-1+o(1)}$ elements of $\{1,\dots,n\}$ for all n.[6] The construction starts with the observation that $\{\log p : p \text{ prime}\}$ is a Sidon set of real numbers. As observed by Cilleruelo (see Gowers [Gow12]), a finite version of the same argument produces a Sidon subset of $\{1,\dots,n\}$ of size $n^{1/2}/(\log n)^{3/2}$.

Construction A (Logarithms of primes)**.** Let $\mathcal{P}_X$ be the set of all primes $p \leqslant X$, for some parameter X to be determined. For primes $p,q,r,s \in \mathcal{P}_X$, by unique factorization if $\{p,q\} \neq \{r,s\}$ we have $pq \neq rs$, so $|pq - rs| \geqslant 1$. Since $\log x$ has derivative $1/x$ it follows that

$$|\log(pq) - \log(rs)| \geqslant X^{-2}.$$

Hence

$$|3X^2\log p + 3X^2\log q - 3X^2\log r - 3X^2\log s| \geqslant 3$$

and, defining $\lambda_p = \lfloor 3X^2 \log p\rfloor$,

$$|\lambda_p + \lambda_q - \lambda_r - \lambda_s| \geqslant 1.$$

Thus $S = \{\lambda_p : p \in \mathcal{P}_X\}$ is a Sidon set in $\{1,\dots,\lfloor 3X^2\log X\rfloor\}$. Taking X so that $3X^2\log X \sim n$, we have a Sidon set in $\{1,\dots,n\}$ of size

$$|S| = \pi(X) \sim \frac{X}{\log X} \asymp \frac{n^{1/2}}{(\log n)^{3/2}}.$$

The next simple example has not appeared much in the literature. To the best of our knowledge it was first mentioned by Cilleruelo in [Cil14].

Construction B (Primes in a quotient ring)**.** Let m be a positive integer and set $G = (\mathbf{Z}/m\mathbf{Z})^\times$. The set

$$S = \{p \bmod m : p \text{ prime},\ 1 < p \leqslant m^{1/2}\}$$

[6] Any of the finite constructions (Constructions 1 to 5) can be adapted to construction an infinite Sidon set $S \subset \mathbf{Z}$ such that $\limsup |S \cap \{1,\dots,n\}|/n^{1/2} > 0$, but constructing Sidon sets with $|S \cap \{1,\dots,n\}|$ large for *all* n is a different ball game. Despite considerable attention, the exponent $\sqrt{2}-1$ has not been improved.

is Sidon: indeed, if four primes $1 < p_1, \ldots, p_4 \leqslant m^{1/2}$ obey $p_1p_2 \equiv p_3p_4 \pmod{m}$, i.e. $m \mid (p_1p_2 - p_3p_4)$, then as $|p_1p_2 - p_3p_4| < m$ we must have $p_1p_2 = p_3p_4$ and hence $\{p_1, p_2\} = \{p_3, p_4\}$ by unique factorization. We have

$$|S| = \pi(m^{1/2}) \sim 2m^{1/2}/\log m$$

and $|G| = \phi(m)$ which is asymptotically somewhere between m and $m/\log\log m$.

The following is a neat variant of Ruzsa's construction. See Maldonado [ML11, Theorem 2.2] for details.

Construction C. For each (rational) prime $p \equiv 1 \pmod 4$, factorize $p = \rho_p\bar{\rho}_p$ in $\mathbf{Z}[i]$, normalized so that $0 < \Im\rho_p < \Re\rho_p$, and let $\phi_p = \arg(\rho_p^4)/2\pi \in (0, 1/2)$. Take $S = \{\lfloor n\phi_p \rfloor : p \leqslant n^{1/2}/4\}$.

The construction achieves $|S| \gg n^{1/2}/\log n$.

The next one was related to us by Ben Green, who heard it from Ellenberg and Venkatesh.

Construction D. Assume the Generalized Riemann Hypothesis (GRH). Let $K = \mathbf{Q}(\sqrt{-D})$ and let $G = \mathrm{Cl}(K)$ be the class group. Let $S \subset G$ be a maximal set of prime ideal classes $[\mathfrak{p}]$ with $N\mathfrak{p} < D^{1/4}/2$ having no solutions to $x + y = 0$. Then

$$|G| \leqslant D^{1/2}(\log D)^{O(1)},$$
$$|S| \geqslant cD^{1/4}/\log D.$$

Indeed, for each rational prime $p < D^{1/4}/2$ which splits (but does not ramify) in K, we may add exactly one of its prime factors $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ to S, and we claim that different primes p contribute different classes. Indeed, if $p_1, p_2 < D^{1/4}$ and $\mathfrak{p}_1 \mid p_1$, $\mathfrak{p}_2 \mid p_2$ and $\mathfrak{p}_1 \sim \mathfrak{p}_2$, then $\mathfrak{p}_1\bar{\mathfrak{p}}_2$ is principal, say $(a + b\sqrt{-D})$, and of norm less than $D^{1/2}/4$, so $b = 0$, so $\mathfrak{p}_1\bar{\mathfrak{p}}_2 = (a)$. Comparing norms, we have $p_1 \mid a$, hence $\mathfrak{p}_1\bar{\mathfrak{p}}_1 = (p_1) \mid (a)$, and by unique factorization we deduce that $\mathfrak{p}_1 = \mathfrak{p}_2$.

By much the same argument we claim S is Sidon. Suppose $\mathfrak{p}_i \in S$ $(1 \leqslant i \leqslant 4)$ satisfy $\mathfrak{p}_i \mid p_i$ and $\mathfrak{p}_1\mathfrak{p}_2 \sim \mathfrak{p}_3\mathfrak{p}_4$. Then as above, $\mathfrak{p}_1\mathfrak{p}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_4 = (a)$ for some $a \in \mathbf{Z}$. Taking norms, we deduce that $p_i | a$ for each i and hence $\mathfrak{p}_i\bar{\mathfrak{p}}_i | (a)$ for each i. By unique factorization, it follows that $\mathfrak{p}_1, \mathfrak{p}_2, \bar{\mathfrak{p}}_3, \bar{\mathfrak{p}}_4$ can be arranged into two conjugate pairs. But since $\mathfrak{p} \in S \Rightarrow \bar{\mathfrak{p}} \notin S$ by construction, this implies $\{\mathfrak{p}_1, \mathfrak{p}_2\} = \{\mathfrak{p}_3, \mathfrak{p}_4\}$.

We give a variation of Construction A that is also very similar to Construction D.

Construction E. Set $K = \mathbf{Q}(\sqrt{D})$. Suppose also that K has class number 1.[7] Let $u \in \mathcal{O}_K^\times$ be a fundamental unit, and write $r = \log|u| > 0$ for the regulator. Let $M = \lceil r \rceil$.

Define $S \subset \mathbf{Z}/M\mathbf{Z}$ as follows: for each prime p, $1 < p \leqslant D^{1/4}/10$ that splits in K, factor $p = \mathfrak{p}\bar{\mathfrak{p}}$ where $\mathfrak{p} = a + b\sqrt{D}$ and $\bar{\mathfrak{p}}$ denotes the Galois conjugate $a - b\sqrt{D}$. Then

[7] It is open to show that there are infinitely many such K, even on GRH, but in practice this should occur a positive fraction of the time.

add the element $\lfloor (M/r)\log|\mathfrak{p}/\bar{\mathfrak{p}}|\rfloor \bmod M$ to S. (Note this definition is unaffected if we change $\mathfrak{p}$ by a unit.)

We claim that different p give different elements of S, as in Section D. Note that if $x = a + b\sqrt{D} \in \mathcal{O}_K$ then either $b = 0$ or $|x/\bar{x}| > D/4N(x)$ or $|x/\bar{x}| < 4N(x)/D$: indeed, if $a, b > 0$ then $|x| > \sqrt{D}/2$ and $|x/\bar{x}| = |x|^2/N(x)$, and the other cases are analogous. Hence, if $1 < p_1, p_2 \leqslant D^{1/4}/10$ and $\big|\log|\mathfrak{p}_1/\bar{\mathfrak{p}}_1| - \log|\mathfrak{p}_2/\bar{\mathfrak{p}}_2|\big| < 1$ we set $x = \mathfrak{p}_1\bar{\mathfrak{p}}_2$ and obtain a contradiction unless $x \in \mathbf{Z}$, in which case $\mathfrak{p}_1 = \mathfrak{p}_2$ by unique factorization.

The proof that S is Sidon is by extending this argument in exactly the same way as in Section D, and we omit the details.

On GRH[8], we have $r \leqslant D^{1/2}(\log D)^{O(1)}$, so S is again fairly dense.

6.2 A common generalization

We now observe that Constructions A to E can be placed into a common framework using (essentially) the notion of Hecke characters.

Let L be a number field with integers $\mathcal{O}_L$. Write $\sigma_1, \dots, \sigma_r \colon L \to \mathbf{R}$ and $\tau_1, \dots, \tau_s \colon L \to \mathbf{C}$ for its real and complex embeddings, up to isomorphism. Let $\ell : L^\times \to (\mathbf{R}^\times)^r \times (\mathbf{C}^\times)^s$ be the homomorphism defined by

$$\ell(x) = (\sigma_1(x), \dots, \sigma_r(x), \tau_1(x), \dots, \tau_s(x)).$$

Let $\mathfrak{m} \subset \mathcal{O}_L$ be an ideal. Let $I_\mathfrak{m}$ denote the abelian group of fractional ideals of L coprime to $\mathfrak{m}$, and for some parameter R let

$$\mathcal{P}_R = \big\{\mathfrak{p} \in I_\mathfrak{m} : \mathfrak{p} \text{ prime},\ N\mathfrak{p} \leqslant R\big\}.$$

For a metric abelian group H, a group homomorphism $\phi\colon I_\mathfrak{m} \to H$ is termed *admissible*[9] if there is a continuous homomorphism $\psi\colon (\mathbf{R}^\times)^r \times (\mathbf{C}^\times)^s \to H$ such that $\phi\big((x)\big) = \psi(\ell(x))$ whenever $x \in L^\times$, $x \equiv 1 \pmod{\mathfrak{m}}$, and $\sigma_i(x) > 0$ for all $i \in [r]$. Finally, let $\Lambda \subseteq H$ be a lattice (discrete co-compact subgroup) and write $[x]$ for the nearest point in Λ to $x \in H$, resolving ambiguity in some arbitrary way. Let

$$S = \{[\phi(\mathfrak{p})] : \mathfrak{p} \in \mathcal{P}_R\} \subseteq \Lambda.$$

If necessary, discard elements from S so that it contains no pair $\{x, -x\}$. Then S is a Sidon if we can show, for a particular choice of $\mathfrak{m}, R, H, \Lambda$, that

(i) $[\phi(\mathfrak{p}_1)] + [\phi(\mathfrak{p}_2)] = [\phi(\mathfrak{p}_3)] + [\phi(\mathfrak{p}_4)] \implies \phi(\mathfrak{p}_1) + \phi(\mathfrak{p}_2) = \phi(\mathfrak{p}_3) + \phi(\mathfrak{p}_4)$,

(ii) $\mathfrak{p}_1\mathfrak{p}_2 \equiv \mathfrak{p}_3\mathfrak{p}_4 \pmod{\ker\phi} \implies \mathfrak{p}_1\mathfrak{p}_2 = \mathfrak{p}_3\mathfrak{p}_4$

for all $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4 \in \mathcal{P}_R$.

Then Constructions A to E are the following special cases (with minor modifications):

[8] More precisely, the class number formula relates $r\,|\operatorname{Cl}(K)|$ to the residue of $\zeta_K(s)$ at 1, which is controlled by GRH, and we have assumed $|\operatorname{Cl}(K)| = 1$.

[9] This condition is natural in the setting of L-functions or class field theory. Its appearance here is motivated only by the previous examples.

- in Construction A, $L = \mathbf{Q}$, $\mathfrak{m} = (1)$, $H = \mathbf{R}$, $\phi((t)) = \log|t|$, and $\Lambda = 1/(3R^2)\mathbf{Z}$;
- in Construction B, $L = \mathbf{Q}$, $\mathfrak{m} = (m)$, $H = \Lambda = (\mathbf{Z}/m\mathbf{Z})^\times$, $R = m^{1/2}$, and $\phi((x)) = |x| \bmod m$;
- in Construction C, $L = \mathbf{Q}(i)$, $\mathfrak{m} = (1)$, $H = \mathbf{R}/\mathbf{Z}$, $\phi((z)) = \arg(z^4)/2\pi$, and $\Lambda = (1/16R^2)\mathbf{Z}/\mathbf{Z}$;
- in Construction D, $L = \mathbf{Q}(\sqrt{-D})$, $\mathfrak{m} = (1)$, $H = \Lambda = \mathrm{Cl}(L)$, and ϕ the quotient map $I_1 \to \mathrm{Cl}(L)$.
- in Construction E, $L = \mathbf{Q}(\sqrt{D})$, $\mathfrak{m} = (1)$, $H = \mathbf{R}/r\mathbf{Z}$, $\Lambda = (r/M)\mathbf{Z}/r\mathbf{Z}$ and ϕ is the map $(t) \mapsto \log|t/\bar{t}|$.

Here a few "hybrid" examples:

- Let $L = \mathbf{Q}$, $\mathfrak{m} = (m)$, $H = \mathbf{R} \times (\mathbf{Z}/m\mathbf{Z})^\times$, and $\phi((x)) = (\log|x|, x \bmod m)$ and $\Lambda = (m/5R^2)\mathbf{Z} \times (\mathbf{Z}/m\mathbf{Z})^\times$. This gives a dense Sidon set by combining the arguments in Construction A and Construction B.
- Let $L = \mathbf{Q}(\sqrt{-D})$, $\mathfrak{m} = (m)$ for some positive integer m, and $H = I_\mathfrak{m}/P_\mathfrak{m}$ (the *ray class group*), where $P_\mathfrak{m} = \{(x) : x \in L^\times,\ x \bmod \mathfrak{m} = 1\}$. Let $\phi : I_\mathfrak{m} \to H$ be the quotient map and let $R = D^{1/4}m^{1/2}/2$. This gives a dense Sidon set (on GRH) by combining and extending the observations in Construction B and Construction D. (Crucially, when writing $\mathfrak{p}_1\mathfrak{p}_2\bar{\mathfrak{p}}_3\bar{\mathfrak{p}}_4 = (a + b\sqrt{-D})$, now $m \mid b$, which given $N\mathfrak{p}_i \leqslant R$ forces $b = 0$.)
- In Construction E, we can similarly augment H to $\mathbf{R}/r\mathbf{Z} \times \mathrm{Cl}(K)$ and remove the inconvenient requirement that $|\,\mathrm{Cl}(K)| = 1$.

There is a standard correspondence between Hecke characters and characters on the idèle class group, so it would be equivalent to phrase this construction in terms of idèles.

6.3 Other examples

We finish by mentioning some further examples of somewhat dense Sidon sets that do not fit the pattern stated above. A precise classification in general seems hopeless for now, though there are some suggestive analogies.

Construction F. Let K be a finite field, $\operatorname{char} K > 3$, let $G = K^2$, and let

$$S = \{(x, x^3) : x \in U\} \subseteq \mathbb{F}_p^2$$

where $U \subset K$ is some subset. One can show that S is a Sidon set if and only if U has at most one solution to $x + y = 0$, as in Construction D. The largest S can be in this construction is therefore $(q+1)/2$, where $|G| = q^2$.

Construction G. Recently Forey and Kowalski found a construction involving Jacobian varieties [FK21]. Let K be a finite field and C a (hyperelliptic) curve of genus two with a K-rational point. There is a natural map ι from C to its Jacobian variety G, which is a finite abelian group. It can be shown that $S = \iota(C(K))$ is a Sidon set up to a factor of two, similarly to the previous example. Moreover, it follows from Weil's proof of the Riemann hypothesis over finite fields that $|S| \sim |G|^{1/2}$, so we get a Sidon set of size $\sim |G|^{1/2}/2$ in A.

This is spiritually related to Construction D or Section 6.2, under the "arithmetic geometry" analogy between ideal/idèle class groups and divisor class groups.

Construction H. As noted by Gowers [Gow12], if S is a Sidon subset of $\{1, \dots, n\}$ then $S' = \{5s + \varepsilon(s) : s \in S\}$ is a Sidon subset of $\{1, \dots, 5n + 1\}$, where $\varepsilon : S \to \{-1, 0, 1\}$ is arbitrary. Thus, if S has some algebraic structure, S' will have somewhat less, and its density will be smaller only by a constant factor. As noted by Ben Green, one could also use an irrational multiplier, such as $s \mapsto \lfloor s\sqrt{2} \rfloor$.

A Proof of Proposition 3.3

Recall we wish to show that if $K = \mathbf{F}_q$ and $H \leqslant \mathrm{P\Gamma L}_3(K)$ is an abelian subgroup not contained in $\mathrm{PGL}_3(K)$ then $|H| \ll q$.

Let G be the subgroup of $\Gamma\mathrm{L}_3(K) = \mathrm{GL}_3(K) \rtimes \mathrm{Gal}(K)$ upstairs corresponding to H. Hence $Z \leqslant G$, G is not contained in $\mathrm{GL}_3(K)$, $G' \leqslant Z$, and $|G| = (q-1)|H|$. We wish to show that $|G| \ll q^2$.

Let $G_0 = G \cap \mathrm{GL}_3(K)$. Fix an element $h = g\sigma \in G$ such that $\sigma \in \mathrm{Gal}(K)$ generates the (nontrivial) image of G in the cyclic group $\mathrm{Gal}(K)$. Let $k \subset K$ denote the fixed field of σ, and write $d = [K : k]$ for the degree of K over k; equivalently, d is the order of σ in $\mathrm{Gal}(K)$. Hence, $|G| = d\,|G_0|$.

If G_0 is nonabelian, it is a subgroup of either *(viii)* or *(ix)* in Proposition 3.1, so $|G_0| \ll q$, $|G| \ll dq \leqslant q \log_p q$ and we are done. We now assume that G_0 is abelian.

Consider the function $\lambda \colon G_0 \to K^\times$ defined by $[h, a] = hah^{-1}a^{-1} = \lambda(a)I$. We observe it is a group homomorphism. Moreover,

$$\lambda(a)a = hah^{-1} = g\sigma(a)g^{-1}$$

and hence

$$\lambda(a)^3\,(\det a) = \det \sigma(a) = \sigma(\det a)$$

so $\lambda(a)^3$ has the form $\sigma(t)/t$ for some $t \in K^\times$, hence $N_{K/k}(\lambda(a)^3) = 1$. There are $|K^\times|/|k^\times|$ elements $u \in K^\times$ with $N_{K/k}(u) = 1$, so $|\lambda(G_0)| \leqslant 3|K^\times|/|k^\times|$.

Let $G_{00} = \ker \lambda \leqslant G_0$. By definition, for all $a \in G_{00}$ we have

$$\sigma(a) = g^{-1}ag. \tag{A.1}$$

Let $A_k = \mathrm{span}_k(G_{00}) \leqslant M_3(K)$ and $A_K = \mathrm{span}_K(G_{00}) \leqslant M_3(K)$. Note A_K is a commutative K-subalgebra of $M_3(K)$, and by a theorem of Schur [Sch05, Mir98][10] any commutative K-subalgebra of $M_3(K)$ has K-dimension at most 3, so $\dim_K(A_K) \leqslant 3$.

[10] Alternatively, in dimension 3, this could be extracted from Proposition 3.1 or its proof.

We claim $\dim_k(A_k) \leqslant 3$. Indeed, any $a_1, a_2, a_3, a_4 \in A_k$ must be linearly dependent over K (as they lie in A_K): say $\sum_{i=1}^4 t_i a_i = 0$ for some $t_i \in K$, not all zero. Applying (A.1),

$$\sum_{i=1}^4 \sigma(t_i)\, a_i = 0$$

and by iterating this and summing, we obtain

$$\sum_{i=1}^4 \mathrm{tr}_{K/k}(t_i)\, a_i = 0.$$

Finally, we may apply this replacing t_i with ut_i for any $u \in K$ throughout, and u may be chosen so that some $\mathrm{tr}_{K/k}(ut_i)$ is non-zero. Hence $a_1, \ldots, a_4$ are necessarily linearly dependent over k, so $\dim_k(A_k) \leqslant 3$ as claimed.

It follows that $|G_{00}| \leqslant |k|^3 - 1$ (as $0 \in A_k$). Putting everything together, we deduce

$$|G| \leqslant 3d\frac{|K^\times|}{|k^\times|}(|k|^3 - 1) = 3d(q-1)(q^{2/d} + q^{1/d} + 1).$$

When $d = 2$ this is $O(q^2)$ as claimed,[11] and for $3 \leqslant d \leqslant \log_p q$ this implies an even stronger bound.

References

[Asc84] M. Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), no. 3, 469–514. MR746539

[BJS02] A. Blokhuis, D. Jungnickel, and B. Schmidt, *Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2*, Proc. Amer. Math. Soc. **130** (2002), no. 5, 1473–1476. MR1879972

[Bos42] R. C. Bose, *An affine analogue of Singer's theorem*, J. Indian Math. Soc. (N.S.) **6** (1942), 1–15. MR6735

[Cil12] J. Cilleruelo, *Combinatorial problems in finite fields and Sidon sets*, Combinatorica **32** (2012), no. 5, 497–511. MR3004806

[Cil14] ______, *Infinite Sidon sequences*, Adv. Math. **255** (2014), 474–486.

[CM97] R. S. Coulter and R. W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. **10** (1997), no. 2, 167–184.

[CRS18] P. Candela, J. Rué, and O. Serra, *Memorial to Javier Cilleruelo: a problem list*, Integers **18** (2018), Paper No. A28, 9.

[DO68] P. Dembowski and T. G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258.

[11] In this case the above bound can be sharp, at least up to the factor of 3. For example, suppose $q = p^2$, h is Frob_{p^3}, and $G_0 = K^\times \mathbf{F}_{p^3}^\times$.

[DP67] P. Dembowski and F. Piper, *Quasiregular collineation groups of finite projective planes*, Math. Z. **99** (1967), 53–75.

[ET41] P. Erdös and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212–215.

[FK21] A. Forey and E. Kowalski, *Algebraic curves in their Jacobian are Sidon sets*, arXiv e-prints (Mar. 2021), arXiv:2103.04917.

[Gan77] M. J. Ganley, *Direct product difference sets*, J. Combinatorial Theory Ser. A **23** (1977), no. 3, 321–332.

[Glu90] D. Gluck, *A note on permutation polynomials and finite geometries*, Discrete Math. **80** (1990), no. 1, 97–100.

[GM75] M. J. Ganley and R. L. McFarland, *On quasiregular collineation groups*, Arch. Math. (Basel) **26** (1975), 327–331.

[Gow12] T. Gowers, *What are dense sidon subsets of* $\{1, \ldots, n\}$ *like?*, 2012.

[Hir89] Y. Hiramine, *A conjecture on affine planes of prime order*, J. Combin. Theory Ser. A **52** (1989), no. 1, 44–50.

[Hug55] D. R. Hughes, *Planar division neo-rings*, Trans. Amer. Math. Soc. **80** (1955), 502–527.

[JJB07] N. L. Johnson, V. Jha, and M. Biliotti, *Handbook of finite translation planes*, Pure and Applied Mathematics (Boca Raton), vol. 289, Chapman & Hall/CRC, Boca Raton, FL, 2007.

[Kan06] W. M. Kantor, *Finite semifields*, Finite geometries, groups, and computation, 2006, pp. 103–114.

[Kin05] O. H. King, *The subgroup structure of finite classical groups in terms of geometric configurations*, Surveys in combinatorics 2005, 2005, pp. 29–56.

[Mir98] M. Mirzakhani, *A simple proof of a theorem of Schur*, Amer. Math. Monthly **105** (1998), no. 3, 260–262.

[ML11] J. P. Maldonado López, *A remark on infinite Sidon sets*, Rev. Colombiana Mat. **45** (2011), no. 2, 113–127.

[RS89] L. Rónyai and T. Szőnyi, *Planar functions over finite fields*, Combinatorica **9** (1989), no. 3, 315–320.

[Ruz93] I. Z. Ruzsa, *Solving a linear equation in a set of integers. I*, Acta Arith. **65** (1993), no. 3, 259–282.

[Ruz98] ______, *An infinite Sidon sequence*, J. Number Theory **68** (1998), no. 1, 63–71.

[Ruz99] ______, *Erdős and the integers*, J. Number Theory **79** (1999), no. 1, 115–163.

[Sch05] J. Schur, *Zur Theorie der vertauschbaren Matrizen*, J. Reine Angew. Math. **130** (1905), 66–76.

[Sin38] J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), no. 3, 377–385.

[TT16] M. Tait and C. Timmons, *Orthogonal polarity graphs and Sidon sets*, J. Graph Theory **82** (2016), no. 1, 103–116.

[TV10] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2010.

[Weh73] B. A. F. Wehrfritz, *Infinite linear groups. An account of the group-theoretic properties of infinite groups of matrices*, Springer-Verlag, New York-Heidelberg, 1973.

[Wei07] C. Weibel, *Survey of non-desarguesian planes*, 2007, pp. 1294–1303.

[Zho13] Y. Zhou, *Difference sets from projective planes*, Ph.D. Thesis, 2013.

[Zie15] M. E. Zieve, *Planar functions and perfect nonlinear monomials over finite fields*, Des. Codes Cryptogr. **75** (2015), no. 1, 71–80.