A Construction of Modular Generalized Sidon Sets

Charles C.Y. Lam* and Alan C.H. Ling†

Abstract

A Sidon set S is a set of integers where the number of solutions to any integer $k = k_1 + k_2$ with $k_1, k_2 \in S$ is at most $g = 2$. If $g \geq 3$, the set S is a generalised Sidon set. We consider the Sidon sets modulo n, where the solutions to addition of elements are considered under a given modulus. In this note, we give a construction of a generalised Sidon set modulo n from any known Sidon set.

1 Introduction

Let S be a set of integers, we are interested in the number of distinct solutions to

$$s_1 + s_2 = s_3 + s_4$$

where $s_1, s_2, s_3, s_4 \in S$, such that $\{s_1, s_2\} \neq \{s_3, s_4\}$.

Sidon's Problem can be stated as follows. Given a set $S \subset \mathbb{Z}$, define

$$\begin{aligned} ||S^{*h}||_\infty &= ||S * S * \cdots * S||_\infty \\ &= \max_{k \in \mathbb{Z}} |\{(s_1, s_2, \ldots, s_h) : s_i \in S, s_1 + s_2 + \cdots + s_h = k\}|. \quad (1) \end{aligned}$$

If $||S^{*2}||_\infty \leq 2$, then S is called a Sidon set. For any $n \in \mathbb{Z}^+$, let $[n] = \{1, 2, 3, \ldots n\}$. We are interested in constructions of sets $S \subseteq [n]$ such that $||S^{*2}||_\infty \leq g$.

In order to study the mathematics of Sidon sets, we consider the following, according to Martin and O'Bryant [7]. Define

$$R(g, n) = \max_S \{|S| : S \subseteq [n], ||S^{*2}||_\infty \leq g\}.$$

*Department of Mathematics, California State University, Bakersfield, Bakersfield, California 93311, USA, e-mail:clam@csub.edu

†Department of Computer Science, University of Vermont, Burlington, Vermont 05405, USA, e-mail:aling@emba.uvm.edu

Note that $R(2,n)$ measures the largest possible size of a subset of $[n]$ that is a Sidon set. In the process in proving certain bounds, the following is considered. Define

$$C(g,n) = \max_S\{|S| : S \subseteq \mathbb{Z}/(n), ||S^{*2}||_\infty \leq g\}.$$

It is believed that the study of Sidon sets requires the understanding of Sidon sets mod n. In particular, a result from Martin and O'Bryant [7] is listed as follows.

Proposition 1 *Let g, f, x, y be positive integers, then*

$$R(gf, xy) \geq R\left(gf, xy + 1 - \lceil \frac{y}{C(f,y)} \rceil\right) \geq R(g,x)C(f,y).$$

The above result was used to provide lower bounds for the quantity

$$\underline{\rho}(g) = \liminf_{n\to\infty} \frac{R(g,n)}{\sqrt{gn}}.$$

The precise asymptotics for $\underline{\rho}(g)$ are known only for $g = 2, 3$. Lower bounds of $\underline{\rho}(g)$ are investigated in [7, 6, 3]. Some upper bounds of $\underline{\rho}(g)$ are also investigated in [5].

In this note, we look at a construction of generalised Sidon sets modulo n from known Sidon sets. The construction method gives rise to inequalities stemming from several known Sidon sets which may be applicable for analysis of Sidon sets. In addition, these new constructions may give rise to possible constructions of new designs.

2 Construction

Let A be a Sidon set modulo kn on $[kn]$. Let $A_i = \{x \in A \mid (i-1)n + 1 \leq x \leq in\}$, where $1 \leq i \leq k$, so that $A = A_1 \dot\cup A_2 \dot\cup \cdots \dot\cup A_k$, the disjoint union of $A_1, A_2, \ldots, A_k$. We construct corresponding S_i's as follows: let $S_1 = \{x \bmod n \mid x \in A_1\}$; for $2 \leq j \leq k$, let $S_j = \{x \bmod n \mid x \in A_j\} \setminus \cup_{i=1}^{j-1} S_i$. It will turn out that all S_i's are disjoint. Consider the set

$$S = S_1 \dot\cup S_2 \dot\cup \cdots \dot\cup S_k.$$

Theorem 1 *Using the above construction,*

$$||S * S||_\infty \leq 2k,$$

under addition modulo n.

Proof: Let $J \in \mathbb{Z} \cap [n]$ be a constant. For $1 \leq i, j \leq k$, $i + j \equiv J \pmod{k}$, consider $||S_i * S_j||_\infty$, as in equation (1), where

$$||S_i * S_j||_\infty = \max_{k \in \mathbb{Z}} |\{(s_1, s_2) : s_1 \in S_i, s_2 \in S_j, s_1 + s_2 = k\}|. \qquad (2)$$

We will show that

$$\sum_{(i,j) \in [k]^2, i+j \equiv J \pmod{k}} ||S_i * S_j||_\infty \leq 2,$$

when the sum $s_1 + s_2$ in equation (2) is taken modulo n.

First, assume that there exists S_i, S_j, S_l, S_m, where i, j, l, m are not necessarily distinct, and that $(t_1, t_2) \in S_i \times S_j$, $(t_3, t_4) \in S_l \times S_m$, where $i + j \equiv l + m \pmod{k}$, and $(t_1, t_2) \neq (t_3, t_4)$, such that

$$t_1 + t_2 \equiv t_3 + t_4 \pmod{n}.$$

Then,

$$t_1 + (i-1)n + t_2 + (j-1)n \equiv t_3 + (l-1)n + t_4 + (m-1)n \pmod{kn}.$$

Since $t_1 + (i-1)n \in A_1$, $t_2 + (j-1)n \in A_2$, $t_3 + (l-1)n \in A_3$, and $t_4 + (m-1)n \in A_4$, contradicting the hypothesis that A is a Sidon set modulo kn.

Since there are k equivalence classes modulo k,

$$||S^{*2}||_\infty \leq 2k,$$

under addition modulo n. □

Corollary 1 *Using the same construction, if $A \subseteq [kn]$ is a generalised Sidon set such that under addition modulo kn,*

$$||A * A||_\infty \leq 2t,$$

then, using the same construction as above, we have

$$||S * S||_\infty \leq 2tk,$$

under addition modulo n.

3 Applications

In this section, we look at three different constructions of Sidon sets and use them to induce inequalities about generalised Sidon sets modulo n.

3.1 Bose's construction

Let q be any prime power, and θ to be a generator of $\mathbb{F}_{q^2}$, $k \in \mathbb{F}_q$. Let

$$\text{Bose}(q, \theta, k) = \{a \in [q^2 - 1] \mid \theta^a - k\theta \in \mathbb{F}_q\}.$$

Then if $k \neq 0$, $\text{Bose}(q, \theta, k)$ is a Sidon set [1] of size q. It is also a Sidon set modulo $q^2 - 1$.

It is known also from [1] that in $\text{Bose}(q, \theta, k)$, there does not exist two distinct elements where the difference is a multiple of $q + 1$ modulo $q^2 - 1$. Hence, using our construction from the previous section, let $q^2 - 1 = kn$ where $n = t(q + 1)$. Then, the collapsed set S still has size q. We arrive at the following result.

Theorem 2 *If q is a prime power, and $q^2 - 1 = kt(q + 1)$, where $k, t \in \mathbb{Z}$, then*

$$C(2k, \frac{q^2 - 1}{k}) \geq q.$$

As an example, we choose $q = 31$. Then the set

$$\begin{aligned} A = \{&16, 20, 53, 140, 178, 195, 198, 203, 238, 280, 311, 324, 347, 415, 441, \\ &510, 520, 521, 677, 711, 726, 765, 787, 849, 858, 865, 877, 879, 906, \\ &924, 930\} \end{aligned}$$

is a Sidon set mod 960.

Since $960 = 5 \cdot 192$, dividing A into five parts, we get

$$\begin{aligned} T_5 = \{&3, 6, 11, 16, 19, 20, 31, 46, 53, 57, 81, 88, 90, 97, 101, 109, 111, 119, \\ &126, 132, 135, 136, 137, 138, 140, 150, 155, 156, 162, 178, 189\}. \end{aligned}$$

Note that $||T_5 * T_5||_\infty = 10$, under addition modulo 192.

We can divide the set into more parts, however, the inequality may not be tight. For example, $960 = 10 \cdot 96$, we divide A into 10 parts and get

$$\begin{aligned} T_{10} = \{&1, 3, 5, 6, 11, 13, 15, 16, 19, 20, 23, 30, 31, 36, 39, 40, 41, 42, 44, 46, \\ &53, 54, 57, 59, 60, 66, 81, 82, 88, 90, 93\} \end{aligned}$$

while $||T_{10} * T_{10}||_\infty = 14$, under addition modulo 96.

3.2 Ruzsa's construction

Let p be a prime. Let θ be a generator of the multiplicative group $\mathbb{F}_p^*$. For $1 \leq i < p$, let $a_{t,i}$ be the congruence class modulo $p^2 - p$ defined by

$$a_{t,i} \equiv t \pmod{p - 1} \text{ and } a_{t,i} \equiv i\theta^t \pmod{p}.$$

Define

$$\text{Ruzsa}(p, \theta, k) = \{a_{t,k} \mid 1 \leq t < p\} \subseteq \mathbb{Z}/(p^2 - p).$$

According to [8], $\text{Ruzsa}(p, \theta, k)$ is a Sidon set. Note that $|\text{Ruzsa}(p, \theta, k)| = p - 1$.

It is known also from [8] that in $\text{Ruzsa}(p, \theta, k)$, there does not exist two elements where the difference is a multiple of p or $p - 1$ modulo $p^2 - p$. Hence, using our construction from the previous section, if we choose k such that $(p^2 - p)/k$ is a multiple of p or $p - 1$, then, the collapsed set S still has size $p - 1$.

Suppose $p^2 - p = (p - 1)tk$, since p is a prime, either $t = 1$ or $k = 1$. If $t = 1$, we have $S = \mathbb{Z}_{p-1}$. If $k = 1$, then $S = \text{Ruzsa}(p, \theta, k)$. In either case, we arrive at the trivial result. Otherwise, we arrive at the following result.

Theorem 3 *If p is a prime, let $p^2 - p = ptk$. Then*

$$C(2k, \frac{p^2 - p}{k}) \geq p - 1.$$

3.3 Singer's construction

Using the notations in [9, 4, 2, 7], let q be any prime power, and let θ be a generator of the multiplicative group of $\mathbb{F}_{q^3}$. For each $k \in \mathbb{F}_q$, let

$$T(k) = \{0\} \cup \{a \in [q^3 - 1] \mid \theta^a - k\theta \in \mathbb{F}_q\}.$$

Define $\text{Singer}(q, \theta, k)$ to be the congruence classes modulo $q^2 + q + 1$ that intersect $T(k)$. Then $\text{Singer}(q, \theta, k)$ is a Sidon set. Note that $|T(k)| = q + 1$.

It is also known that in $\text{Singer}(q, \theta, k)$, there is exactly one pair of distinct elements that give a difference of any $s \in \mathbb{Z}/(q^2 + q + 1)$. Applying the construction from the previous section, for any $k \in \mathbb{Z}$ such that $q^2 + q + 1 = kn$, exactly one element is duplicated when we take $S = A \bmod n$. Hence, we have shown the following.

Theorem 4 *If q is a power of a prime, and $q^2 + q + 1 = kn$, then*

$$C(2k, \frac{q^2 + q + 1}{k}) \geq q.$$

4 Conclusion

The following are proved in [7]. Let q be a prime power.

- If q is a prime, then $C(2k^2, q^2 - q) \geq k(q - 1)$;
- $C(2k^2, q^2 - 1) \geq kq$;

- $C(2k^2, q^2+q+1) \geq kq+1$.

In this note, we have proved the following. Let q be a prime power.

- If q is a prime, and $q \not| k$, then $C(2k, \frac{q^2-q}{k}) \geq q-1$;
- If $k|q-1$, then $C(2k, \frac{q^2-1}{k}) \geq q$;
- If $k|q^2+q+1$, then $C(2k, \frac{q^2+q+1}{k}) \geq q$.

Our result differs in that we restrict $||S^{*2}|| \leq 2k$ instead of $2k^2$ in the inequalities derived. Though, in the application to the limits of $\underline{\rho}$ in [7], only the case $k=1$ was applied, thus the results for the bounds of $\underline{\rho}$ are not changed.

For any $k \in \mathbb{Z}$, our results apply when $k|p^2-p$, $k|q-1$ or $k|q^2+q+1$. In particular, let p be a prime and consider the congruence

$$p^n \equiv 1 \pmod{k}.$$

Note that by the Euler-Fermat Theorem, if $\gcd(k,p)=1$, then $p^{t\phi(k)} \equiv 1 \pmod{k}$ for all $t \in \mathbb{Z}$. Hence, for each prime p, there are infinitely many cases where $q=p^n$ and $k|q-1$ so that Theorem 2 can be applied.

In our results, the bounds are tight when the number of divisors is small, as seen in our example. Further research is needed to determine the behaviour of bounds when number of divisors is high.

References

[1] R.C. Bose, An Affine Analogue of Singer's Theorem, J. Indian Math. Soc. (N.S.), 6:1-15 (1942)

[2] C.J. Colbourn, J.H. Dinitz, CRC Handbook of Combinatorial Designs, CRC Press, 1996.

[3] J. Cilleruelo, I. Ruzsa and C. Trujillo. Upper and lower bounds for finite $B_h[g]$ sequences, $g > 1$. To Appear.

[4] R.C. Bose and S. Chowla. Theorems in the addictive theory of numbers. Comment. Math. Helv., 37:1962/1963, 141-147.

[5] B. Green. The number of squares and $B_h[g]$ sets. Acta Arithmetica, 100(4):365-390, 2001.

[6] L. Habsieger and A. Plagne. Ensembles $B_2[2]$: l'étau se resserre. Preprint.

[7] Greg Martin, Kevin O'Bryant: Constructions of generalized Sidon sets, J. Comb. Theory, Ser. A 113(4): 591-607 (2006)

[8] Imre Z. Ruzsa. Sumsets of Sidon sets. Acta Arith., 77(4):353-359, 1996.

[9] James Singer. A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc., 43(3):377-385, 1938.