Journal of Integer Sequences, Vol. 27 (2024),
Article 24.1.2

# Constructing Thick $B_h$-Sets

Kevin O'Bryant
City University of New York
The Graduate Center and The College of Staten Island
2800 Victory Boulevard, 1S215
Staten Island, NY 10314
USA
kevin.obryant@csi.cuny.edu

**Abstract**

A subset $\mathcal{A}$ of a commutative semigroup $X$ is called a $B_h$-set in $X$ if the only solutions to

$$a_1 + \cdots + a_h = b_1 + \cdots + b_h, \qquad a_i, b_i \in \mathcal{A}$$

are the trivial solutions $\{a_1, \ldots, a_h\} = \{b_1, \ldots, b_h\}$ (as multisets). With $h = 2$ and $X = \mathbb{Z}$, these sets are also known as Sidon sets, Golomb rulers, and Babcock sets. In this work, we generalize constructions of Bose-Chowla and Singer and give the resultant bounds on the diameter of a $k$ element $B_h$-set in $\mathbb{Z}$ for $h = 3, k \le 28$ and $h = 4, k \le 16$. We conclude with a list of open problems.

## 1 Introduction

A subset $\mathcal{A}$ of a commutative semigroup $X$ is called a $B_h$-set in $X$ if the only solutions to

$$a_1 + \cdots + a_h = b_1 + \cdots + b_h, \qquad a_i, b_i \in \mathcal{A}$$

are the trivial solutions $\{a_1, \ldots, a_h\} = \{b_1, \ldots, b_h\}$ (as multisets). With $h = 2$ and $X = \mathbb{Z}$, these sets are also known as Sidon sets, Golomb rulers, and Babcock sets. For an extensive bibliography of related mathematics literature we direct the reader to [14]. The purpose of this work is to give new parameterized constructions of $B_h$-sets for $h \ge 3$, and to give criteria on the parameters for these sets to be affinely inequivalent.

One application of $B_h$-sets in $\mathbb{Z}$ is in electrical engineering; this literature starts in Babcock [1] and continues for dozens of articles in IEEE journals not covered by Math Sci-Net. Specifically, a nonlinear amplifier for channel frequencies $a_1, a_2, a_3, \dots$ produces "ghost" signals at frequencies of the form $a_1 + a_2, a_1 + a_2 - a_3$, and so on. The strongest relevant ghosts are at $a_1 + a_2 - a_3$ (third-order intermodulation) and $a_1 + a_2 + a_3 - a_4 - a_5$ (fifth-order intermodulation). Thus, the set of frequencies should avoid equations of the sort $a_4 = a_1 + a_2 - a_3$ and $a_6 = a_1 + a_2 + a_3 - a_4 - a_5$. That is, to avoid third-order intermodulation, the channels should form a $B_2$-set, and to avoid fifth-order intermodulation, the channels should be a $B_3$-set.

The first published usage of the "$B_h$" terminology that we have found is in the introduction of the famous Erdős & Turán paper [8], where they state "Such sequences, called $B_2$ sequences by Sidon, occur in the theory of Fourier series." Singer [17] had already constructed thick finite $B_h$-sets in 1939, and Bose gave a different thick finite construction of $B_2$-sets in [3], which was generalized to $B_h$-sets by Bose & Chowla in [4]. The constructions given in this work subsume those of Singer and Bose & Chowla.

**Definition 1.** For an integer $h \geq 2$ and a prime power $q$, set $M = q^h - 1$. For a generator $\theta$ of the multiplicative group $\mathbb{F}_{q^h}^\times$, and $b \in \mathbb{Z}/(q^h - 1)\mathbb{Z}$ for which $\theta^b$ has algebraic degree $h$ over $\mathbb{F}_q$, we define the set

$$\textsc{BoseCh}_h(q, b) \coloneqq \left\{ a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = \theta^b + v, \quad v \in \mathbb{F}_q \right\}.$$

**Definition 2.** For an integer $h \geq 2$, a prime power $q$, set $M = \frac{q^{h+1}-1}{q-1}$. For a generator $\theta$ of the multiplicative group $\mathbb{F}_{q^{h+1}}^\times$, and $b \in \mathbb{Z}/M\mathbb{Z}$ for which $\theta^b$ has algebraic degree $h+1$, we define the set

$$\textsc{Singer}_h(q, b) \coloneqq \left\{ a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = u\theta^b + v, \quad u, v \in \mathbb{F}_q \right\}.$$

We comment that it may seem that the modulus should be $q^{h+1} - 1$. However, for any $a$ with $\theta^a = u\theta^b + v$, one also has $\theta^{a+(q^{h+1}-1)/(q-1)} = u_1\theta^b + v_1$, where $u_1, v_1$ are in $\mathbb{F}_q$ because all of $u, v, \theta^{(q^{h+1}-1)/(q-1)}$ are in $\mathbb{F}_q$.

A cautious reader will object that the choice of the generator impacts the right side of these definitions, and so should be included in the notation $\textsc{BoseCh}_h(q, b)$ and $\textsc{Singer}_h(q, b)$. While the choice of $\theta$ does matter, we will eventually show that it does not matter in a meaningful way. To avoid this technicality, we set $\theta$ in the above definitions to be a root of the Conway polynomial [11] that generates the appropriate field. The only facts about Conway polynomials that we will use is that for each prime power $q = p^e$, the Conway polynomial $C_{p,e}(x) \in \mathbb{F}_p[x]$ is uniquely defined, irreducible, and

$$\mathbb{F}_p[x]/C_{p,e}(x) \cong \mathbb{F}_q, \qquad \langle \theta \rangle = \mathbb{F}_q^\times.$$

There are additional properties that make Conway polynomials a computationally pleasant approach to working in finite fields, particularly concerning subfields, and Luebeck [12] has provided an extensive database. The specific presentation of the finite fields is not relevant to the theory in this work, and is only useful if one wants to compare explicit computations.

The $b = 1$ cases of the following theorem are exactly the constructions of Bose-Chowla and Singer. The first sentence of Theorem 3 is Observation #1 in [9].

**Theorem 3.** *If $h, q, b$ are in the domain of* BoseCh*, then* $\text{BoseCh}_h(q, b)$ *is a $B_h$ set in $\mathbb{Z}/(q^h - 1)\mathbb{Z}$ with $q$ distinct elements.*

*If $h, q, b$ are in the domain of* Singer*, then* $\text{Singer}_h(q, b)$ *is a $B_h$ set in $\mathbb{Z}/(\frac{q^{h+1}-1}{q-1}\mathbb{Z})$ with $q + 1$ distinct elements.*

We say that sets $\mathcal{A}_1, \mathcal{A}_2 \in \mathbb{Z}/M\mathbb{Z}$ are affinely equivalent, writing $\mathcal{A}_1 \sim \mathcal{A}_2$, if there is some $d$ relatively prime to $M$ and some $s$ with $\mathcal{A}_2 = \{da + s : a \in \mathcal{A}_1\}$. Clearly, if $\mathcal{A}_1$ is a $B_h$ set in $\mathbb{Z}/M\mathbb{Z}$ and $\mathcal{A}_1 \sim \mathcal{A}_2$, then $\mathcal{A}_2$ is also a $B_h$ set in $\mathbb{Z}/M\mathbb{Z}$. We use the notation $d * \mathcal{A} := \{da : a \in \mathcal{A}\}$ and $\mathcal{A} + s := \{a + s : a \in \mathcal{A}\}$ to denote dilations and translations of sets.

We identify when the $B_h$-sets given in Theorem 3 are affinely equivalent in the following theorem.

**Theorem 4.** *Suppose that $h, q = p^r, b$ and $h, q, e$ are in the domain of* BoseCh*. If*

*(i)* $b \equiv e \pmod{\frac{q^h-1}{q-1}}$*, or*

*(ii)* $\theta^b - \theta^e \in \mathbb{F}_q$*, or*

*(iii)* $b \equiv p^i e \pmod{q^h - 1}$ *for some integer $i$,*

*then* $\text{BoseCh}_h(q, b) \sim \text{BoseCh}_h(q, e)$*.*

*Suppose that $h, q, b$ and $h, q, e$ are in the domain of* Singer*. If*

*(iv)* $b \equiv e \pmod{\frac{q^{h+1}-1}{q-1}}$*, or*

*(v)* $b \equiv p^i e \pmod{q^{h+1} - 1}$ *for some integer $i$, where $p$ is the prime that divides $q$, or*

*(vi)* $\theta^b - \theta^e \in \mathbb{F}_q$*, or*

*(vii)* $r\theta^b + t\theta^{e+b} + w\theta^e \in \mathbb{F}_q$ *for some $r, t, w \in \mathbb{F}_q$, and $r, t$ are not both 0,*

*then $Singer_h(q, b) \sim$* $\text{Singer}_h(q, e)$*.*

One sad consequence is that for $h = 2$ and any allowed $q, b, e$, we have $\text{BoseCh}_2(q, b) \sim \text{BoseCh}_2(q, e)$. That is, we do not produce any new (up to affine equivalence) Sidon sets. However, $\text{BoseCh}_3(5, 1) \not\sim \text{BoseCh}_3(5, 4)$ and for $h > 2$ and most (but not all) prime powers $q$ we generate previously unknown $B_h$-sets.

In the number theory literature, the thickness of a $B_h$-set $\mathcal{A}$ is sometimes measured by a lower bound on the cardinality $|\mathcal{A}|$ in terms of the diameter $\max \mathcal{A} - \min \mathcal{A}$, while in recreational, computational, and engineering literature it is more common to see an upper bound on the diameter in terms of cardinality. To serve all audiences, we define both $R_h(n)$ as the maximum possible cardinality of a $B_h$-set contained in $[1, n]$, and $R_h^{-1}(k)$ be the smallest $n$ such that there is a $B_h$-set with $k$ elements contained in $[1, n]$.

Sequence A227358 from the *On-Line Encyclopedia of Integer Sequences* (OEIS) gives the minimum diameter of $B_3$-sets with up to 10 elements. We are not aware of any such computation for $h > 3$. As comparison, we have also computed the smallest diameters achievable by any subset of any shift of dilations of $\textsc{BoseCh}_3(q,b)$, $\textsc{BoseCh}_4(q,b)$, $\textsc{Singer}_3(q,b)$, and $\textsc{Singer}_4(q,b)$ for all $b$ and small $q$ (projected from $\mathbb{Z}/M\mathbb{Z}$ to $\mathbb{Z}$ in the obvious way). In my opinion, this data suggests that the BoseCh and Singer constructions are not close to optimal for $h > 2$, in contrast to the apparent situation for $h = 2$.

The lower bound on $R_h(n)$ and upper bound on $R_h^{-1}(k)$ implied by our constructions is not better than that achieved by Singer's construction alone. Nevertheless, we give several statements using up-to-date results on the distribution of primes, as these results are frequently misstated in the literature.

**Theorem 5.**

*(a) For all $n \in \mathbb{Z}$, we have $R_h(n) \geq n^{1/h} - 2^{44} n^{154/(155h)}$ and $R_h^{-1}(k) \leq k^h + 3^{155h} k^{h-1/155}$.*

*(b) If $k, n \geq e^{e^{34}}$, we have $R_h(n) \geq n^{1/h} - 7n^{2/(3h)}$ and $R_h^{-1}(k) \leq k^h + (3k)^{h-1/3}$.*

*(c) If $k, n$ are sufficiently large, then $R_h(n) \geq n^{1/h} - n^{21/(40h)}$ and $R_h^{-1}(k) \leq k^h + 2^h k^{h-19/40}$.*

*(d) If the Riemann Hypothesis holds, then*

$$R_h^{-1}(k) < k^h + \log(20k) k^{h-1/2} + 2k^{h-1} \log^{2h}(20k), \quad R_h(n) \geq n^{1/h} - \left(7 + \tfrac{\log n}{h}\right) n^{1/(2h)}.$$

# 2 Two explicit examples

## 2.1 A BoseCh example.

Let $h = 3$ and $q = 11$; we first compute the various $\textsc{BoseCh}_3(11,b)$, and will then give $\textsc{Singer}_3(11,b)$.

The Conway polynomial for $11^3$ is $C_{11,3}(x) = 9 + 2x + x^3 \in \mathbb{F}_{11}[x]$. We have $\mathbb{F}_{q^3} \cong \mathbb{F}_q[x]/C_{11,3}(x)$, and $\theta$ (whose minimal polynomial is $C_{11,3}(x)$) generates the multiplicative group.

Our first task is to find a suitably small set of candidates for $b$. From Theorem 4(i), we only need to consider values between 1 and $\frac{q^h-1}{q-1} = 133$, inclusive. As the $\mathbb{F}_{q^3}$ has only $\mathbb{F}_q$ as a subfield, only $b = 133$ has $\theta^b$ having algebraic degree less than 3. Further, by Theorem 4(ii) each $b$ is equivalent to $11b$ and $11^2 b$. These equivalences combine to give additional equivalences, e.g., $\textsc{BoseCh}_3(11,3) \sim \textsc{BoseCh}_3(11, 11^2 \cdot 3) \sim \textsc{BoseCh}_3(11,97)$. The second condition given in Theorem 4 is much harder to use, as it requires arithmetic inside the field. For instance,

$$\theta^{21} - \theta^1 = (\theta^3)^7 - \theta = (-9 - 2\theta)^7 - \theta = 2^7(1-\theta)^7 - \theta = \cdots = 3 \in \mathbb{F}_{11},$$

and so $\textsc{BoseCh}_3(11,1) \sim \textsc{BoseCh}_3(11,21)$. With some computerized labor, we find that each $b$ value is equivalent to one of 1, 2, 4, 6. We have used the Conway polynomial representation, but any finite field representation will lead to four equivalence classes for $b$, but not necessarily these as the smallest representatives of each class.

We then compute inside the field using Definition 1 that

$$\begin{aligned}
\textsc{BoseCh}_3(11,1) &= \{1,21,65,100,111,238,324,523,535,1137,1214\},\\
\textsc{BoseCh}_3(11,2) &= \{2,16,132,237,330,338,389,419,764,1174,1254\},\\
\textsc{BoseCh}_3(11,4) &= \{4,56,116,174,354,626,782,905,979,1147,1183\}, \text{ and}\\
\textsc{BoseCh}_3(11,6) &= \{6,152,261,295,311,352,367,891,1092,1113,1228\}.
\end{aligned}$$

By Theorem 3, these four sets are $B_3$-sets in $\mathbb{Z}/1330\mathbb{Z}$, and by direct computation we can verify that no two are affinely equivalent. We are not aware of any affine equivalences that are not dictated by Theorem 4.

By directly examining all sets affinely equivalent to these, we notice that

$$167 * \textsc{BoseCh}_3(11,6) + 330 = \{1,2,27,167,385,397,439,444,484,586,594\}$$

has a particularly small diameter. Consequently $R_3(594) \geq 11$ and $R_3^{-1}(11) \leq 594$.

## 2.2 A Singer example.

We now compute $\textsc{Singer}_3(11,b)$. The Conway polynomial for $11^4$ is $C_{11,4}(x) = 2 + 10x + 8x^2 + x^4 \in \mathbb{F}_{11}[x]$.

Our first task is find a suitably small set of candidates for $b$. From Theorem 4(iv), we only need to consider values between 1 and $\frac{q^{h+1}-1}{q-1} = 1464$. We require $\theta^b$ to have algebraic degree $h+1 = 4$, and that reduces the number of $b$ values to 1452. Including Theorem 4(v) reduces the number of possible inequivalent $b$ values to 366. Theorem 4(vi) is significantly more computationally intensive, but reduces the number of inequivalent to $b$ values to at most 36. Using Theorem 4(vii) is *much* more time-consuming. With the additional assumptions that $r = 0, t = 1$, we find that each $b$ is equivalent to one of 1, 2, 3, 6, 8 or 14. We have the $B_3$-sets in $\mathbb{Z}/1464\mathbb{Z}$:

$$\begin{aligned}
\textsc{Singer}_3(11,1) &= \{1,418,502,679,846,1050,1164,1187,1285,1319,1339,1464\}\\
\textsc{Singer}_3(11,2) &= \{2,273,377,432,500,665,674,887,908,1192,1257,1464\}\\
\textsc{Singer}_3(11,3) &= \{3,201,309,425,664,700,876,1061,1105,1239,1357,1464\}\\
\textsc{Singer}_3(11,6) &= \{6,76,388,593,702,734,950,1147,1208,1440,1457,1464\}\\
\textsc{Singer}_3(11,8) &= \{8,128,582,624,739,774,841,922,1143,1311,1369,1464\}\\
\textsc{Singer}_3(11,14) &= \{14,40,85,492,529,621,683,722,940,969,1151,1464\}
\end{aligned}$$

By direct computation, no two of these are affinely equivalent. We are not aware of any affine equivalences that are not dictated by Theorem 4.

We further find, after some computation, that

$$481 * \textsc{Singer}_3(11,1) + 102 = \{1,4,36,72,89,102,229,379,583,592,629,738\}.$$

Thus, $R_3(738) \geq 12$ and $R_3^{-1}(12) \leq 738$. Moreover,

$$653 * \textsc{Singer}_3(11, 2) + 564 = \{1, 22, 31, 81, 92, 108, 225, 406, 564, 568, 592, 793\}.$$

Thus, dropping the last element, we find that $R_3(592) \geq 11$ and $R_3^{-1}(11) \leq 592$. This is slightly better than the bound from $\textsc{BoseCh}_h(11, b)$ sets.

# 3 Generalized Bose-Chowla sets

Fix an integer $h \geq 2$ and a prime power $q$, and set $M \coloneqq q^h - 1$. Let $\tau$ be a multiplicative generator of $\mathbb{F}_{q^h}^\times$ (not necessarily in line with the Conway polynomial). Take $\beta \in \mathbb{F}_{q^h}$ with algebraic degree $h$. We define $S_h$ as follows:

$$S_h(\tau, \beta) \coloneqq \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \tau^a = \beta + v, \quad v \in \mathbb{F}_q\}.$$

Further, let $\alpha_1, \alpha_2, \ldots, \alpha_h$ be a basis for $\mathbb{F}_{q^h}$ over $\mathbb{F}_q$ as a vector space, with $\alpha_1 = 1$ and $\alpha_2 = \beta$.

As $1, \beta, \ldots, \alpha_h$ is a basis, each $x' \in \mathbb{F}_q$ corresponds to a distinct $x \in \mathbb{Z}/M\mathbb{Z}$ by the equation $\theta^x = 1 \cdot x' + 1 \cdot \beta + \sum_{i=3}^h 0 \cdot \alpha_i$, so that $S_h(\tau, \beta)$ has exactly $q$ elements.

Consider $k \in \mathbb{Z}/M\mathbb{Z}$, and suppose that $a_1, \ldots, a_h, b_1, \ldots, b_h \in S_h(\tau, \beta)$ satisfy

$$k = a_1 + \cdots + a_h \equiv b_1 + \cdots + b_h \pmod{M}.$$

As $\tau$ has multiplicative order $q^h - 1 = M$, we have

$$\tau^k = \tau^{a_1 + \cdots + a_h} = \prod_{i=1}^h \tau^{a_i} = \prod_{i=1}^h (\beta + a_i')$$

for some $a_i' \in \mathbb{F}_q$. In the same manner,

$$\tau^k = \prod_{i=1}^h (\beta + b_i').$$

Now define polynomials $f, g \in \mathbb{F}_q[x]$ by

$$f(x) = \prod_{i=1}^h (x + a_i'), \qquad g(x) = \prod_{i=1}^h (x + b_i').$$

Then $\beta$ (which has algebraic degree $h$) is a root of $f(x) - g(x)$ (which has degree at most $h - 1$), from which we learn that $f(x) - g(x)$ is identically 0, i.e., $f(x) = g(x)$. We have unique factorization over finite fields, so that

$$\{a_1', \ldots, a_h'\} = \{b_1', \ldots, b_h'\}$$

as multisets. As noted above, that $\alpha_1, \dots, \alpha_h$ is a basis implies that $a_i', b_i' \in \mathbb{F}_q$ uniquely define $a_i, b_i$ in $\mathbb{Z}/M\mathbb{Z}$, and consequently

$$\{a_1, \dots, a_h\} = \{b_1, \dots, b_h\}$$

as multisets. That is, $S_h(\tau, \beta)$ is a $B_h$-set in $\mathbb{Z}/M\mathbb{Z}$.

We can take $\tau$ to be $\theta$, the generator provided in the Conway polynomial representation of $\mathbb{F}_{q^h}$, and note that $\beta = \theta^b$ for some $b \in \mathbb{Z}/M\mathbb{Z}$, so that $S_h(\tau, \beta) = \textsc{BoseCh}_h(\theta, b)$. We have proven the claims in Theorem 3 concerning $\textsc{BoseCh}_h(q, b)$ sets.

Before proceeding into the proof of Theorem 4 as it pertains to $\textsc{BoseCh}$ sets, we spend a few words noting some tempting generalizations that aren't really meaningful generalizations. First, fix any basis $\alpha_1, \dots, \alpha_h$ of $\mathbb{F}_{q^h}$ over $\mathbb{F}_q$, and any constants $c_1, \dots, c_{h-1} \in \mathbb{F}_q$, not all 0 and with $(c_1\alpha_1 + \cdots + c_{h-1}\alpha_{h-1})\alpha_h^{-1}$ having degree $h$. Then the set

$$\{a \in \mathbb{Z}/M\mathbb{Z}\colon \tau^a = c_1\alpha_1 + \cdots + c_{h-1}\alpha_{h-1} + v\alpha_h, v \in \mathbb{F}_q\}$$

is a $B_h$-set with $q$ elements. By details we spare the reader, each such set is affinely equivalent to $\textsc{BoseCh}_h(q, b)$ for some integer $b$. Second, we note that if $\tau$ is also a generator of the multiplicative group of $\mathbb{F}_{q^h}$, then $S_h(\tau, \beta) \sim S_h(\theta, \beta)$. Specifically, $\tau = \theta^t$ for some $t$, and since $\tau$ is a generator, $\gcd(t, M) = 1$; let $t^{-1}$ be the inverse of $t$ modulo $m$. Then

$$\begin{aligned} S_h(\tau, \beta) &\coloneqq \{a \in \mathbb{Z}/M\mathbb{Z} : \tau^a = \beta + v, \quad v \in \mathbb{F}_q\} \\ &= \{a \in \mathbb{Z}/M\mathbb{Z} : \theta^{ta} = \beta + v, \quad v \in \mathbb{F}_q\} = t^{-1} * S_h(\theta, \beta). \end{aligned}$$

We now turn to the task of determining when

$$\textsc{BoseCh}_h(q, b) \sim \textsc{BoseCh}_h(q, e).$$

First, suppose that $b \equiv e \pmod{\frac{q^h-1}{q-1}}$. Then for some integer $x$ we have $b = e + x\frac{q^h-1}{q-1}$ and $\theta^b = \theta^e\theta^{x(q^h-1)/(q-1)} = w\theta^e$, and $w = (\theta^{(q^h-1)/(q-1)})^x \in \mathbb{F}_q$ because $\theta^{(q^h-1)/(q-1)}$ is in $\mathbb{F}_q$. We have

$$\begin{aligned} \textsc{BoseCh}_h(q, b) &\coloneqq \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = \theta^b + v, \quad v \in \mathbb{F}_q\right\} \\ &= \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = w\theta^e + v, \quad v \in \mathbb{F}_q\} \\ &= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^{a - x(q^h-1)/(q-1)} = \theta^e + vw^{-1}, \quad v \in \mathbb{F}_q\right\} \\ &= x\tfrac{q^h-1}{q-1} + \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = \theta^e + v, \quad v \in \mathbb{F}_q\} \\ &= x\tfrac{q^h-1}{q-1} + \textsc{BoseCh}_h(q, e). \end{aligned}$$

Thus, $\textsc{BoseCh}_h(q, b) \sim \textsc{BoseCh}_h(q, e)$.

Now, suppose that $pb \equiv e \pmod{M}$, where $p$ is the characteristic of the field $\mathbb{F}_{q^h}$. The map $u \mapsto u^p$, the Frobenius automorphism, is a bijection and satisfies $(u + v)^p = u^p + v^p$ for any $u, v \in \mathbb{F}_{q^h}$. We have

$$\begin{aligned}\textsc{BoseCh}_h(q,b) &:= \big\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = \theta^b + v, \quad v \in \mathbb{F}_q\big\} \\ &= \big\{a \in \mathbb{Z}/M\mathbb{Z} : \quad (\theta^a)^p = (\theta^b + v)^p, \quad v \in \mathbb{F}_q\big\} \\ &= \big\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^{ap} = \theta^{pb} + v^p, \quad v \in \mathbb{F}_q\big\} \\ &= p^{-1} * \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^{ap} = \theta^e + v, \quad v \in \mathbb{F}_q\} \\ &= p^{-1} * \textsc{BoseCh}_h(q,e).\end{aligned}$$

It follows that if $b \equiv p^i e \pmod M$ for any $i$, then $\textsc{BoseCh}_h(q,b) \sim \textsc{BoseCh}_h(q,e)$.

Now suppose that $w := \theta^e - \theta^b \in \mathbb{F}_q$. Then

$$\begin{aligned}\textsc{BoseCh}_h(q,b) &:= \big\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = \theta^b + v, \quad v \in \mathbb{F}_q\big\} \\ &= \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = \theta^e - w + v, \quad v \in \mathbb{F}_q\} \\ &= \textsc{BoseCh}_h(q,e).\end{aligned}$$

Thus, $S_h(q,\theta,\theta^b) \sim S_h(q,\theta,\theta^e)$.

This concludes the proof of all of the claims regarding BoseCh sets made in Theorems 3 and 4.

# 4 Generalized Singer sets

Fix an integer $h \geq 2$ and a prime power $q$, and set $M := (q^{h+1} - 1)/(q-1)$. Let $\tau$ be a multiplicative generator $\mathbb{F}_{q^{h+1}}^\times$. Suppose further that $\beta$ has algebraic degree $h+1$. We define $S_h$ as follows:

$$S_h(\tau,\beta) := \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \tau^a = u\beta + v, \quad u, v \in \mathbb{F}_q\}.$$

Further, let $\alpha_1, \alpha_2, \ldots, \alpha_h$ be a basis for $\mathbb{F}_{q^h}$ over $\mathbb{F}_q$ as a vector space, with $\alpha_1 = 1$ and $\alpha_2 = \beta$. Note that $\tau^M \in \mathbb{F}_q$, as is $\tau^{kM}$ for any integer $k$.

We first argue that $S_h(\tau,\beta)$ has $q+1$ distinct elements. As $1, \beta, \alpha_3, \ldots, \alpha_h$ is a basis, for each $u, v \in \mathbb{F}_q$, not both 0, there is a unique $a$ in $[1, q^{h+1} - 1]$ with $\tau^a = u + v\beta$. That is, there are $q^2 - 1$ such $a$. For each particular $a$, there is also a solution (with different $u, v$) with $a + kM$ for any integer $k$, as

$$\tau^{a+kM} = \tau^{kM}\big(u\beta + v\big) = (wu)\beta + (wv),$$

where $w = \tau^{kM} \in \mathbb{F}_q$, and so $wu, wv \in \mathbb{F}_q$. Thus, the $q^2 - 1$ solutions with $1 \leq a \leq q^{h+1} - 1$ fall into congruence classes modulo $M$. Each congruence class modulo $M$ has $q-1$ elements in $1 \leq a \leq q^{h+1} - 1$, so that $S_h(\tau,\beta)$ consists of $(q^2-1)/(q-1) = q+1$ distinct elements.

We now prove that $S_h(\tau,\beta)$ is a $B_h$-set in $\mathbb{Z}/M\mathbb{Z}$. Define functions $u, v \colon S_h(\tau,\beta) \to \mathbb{F}_q$ by

$$\tau^k = u(k)\beta + v(k).$$

Note that $u(M) = 0$ since $\tau^M \in \mathbb{F}_q$. Clearly the pair $(u(k), v(k))$ uniquely determines $k \in S_h(\tau, \beta)$. But more surprisingly, the value $-v(k)u(k)^{-1}$ (possibly undefined) uniquely determines $k \in S_h(\tau, \beta)$, as we now explain. Suppose $-v(k)u(k)^{-1}$ is undefined, whence $u(k) = 0$. Then $\tau^k = v(k) \in \mathbb{F}_q$, so that $k \equiv 0 \pmod{M}$. Since $S_h(\tau, \beta) \subseteq \mathbb{Z}/M/ZZ$, we must have $k = M$. Otherwise, $w \coloneqq -v(k)u(k)^{-1}$ is defined, whence $wu(k) = v(k)$. This means that $\tau^k = u(k)\beta + wu(k)$. We know $\beta$ and $w$, and therefore know the value $y \in [1, q^{h+1} - 1]$ with $\tau^y = \beta + w$. Since $u(k) \in \mathbb{F}_q$, we have $y \equiv k \pmod{M}$, whence there is a unique candidate for $k$ in $[1, M]$.

Now suppose that

$$a_1 + \cdots + a_h \equiv b_1 + \cdots + b_h \pmod{M}, \tag{1}$$

with $a_i, b_i \in S_h(\tau, \beta)$, and we must show that

$$\{a_1, \ldots, a_h\} = \{b_1, \ldots, b_h\} \tag{2}$$

as multisets. From line (1), there is an integer $x$ with

$$a_1 + \cdots + a_h = kM + b_1 + \cdots + b_h.$$

Let $w = \tau^{kM} \in \mathbb{F}_q$. We then have, using that $a_i, b_i \in S_h(\tau, \beta)$,

$$\begin{aligned}
\prod_{i=1}^{h} \big(u(a_i)\beta + v(a_i)\big) &= \prod_{i=1}^{h} \tau^{a_i} \\
&= \tau^{\sum_{i=1}^{h} a_i} \\
&= \tau^{xM + \sum_{i=1}^{h} b_i} \\
&= w \prod_{i=1}^{h} \tau^{b_i} \\
&= w \prod_{i=1}^{h} \big(u(b_i)\beta + v(b_i)\big).
\end{aligned}$$

We define the polynomials (each with degree at most $h$) in $\mathbb{F}_q[x]$

$$f(x) \coloneqq \prod_{i=1}^{h} \big(u(a_i)x + v(a_i)\big), \qquad g(x) \coloneqq \prod_{i=1}^{h} \big(u(b_i)x + v(b_i)\big).$$

Then $\beta$, which by hypothesis has degree $h + 1$, is a root of the polynomial $f(x) - wg(x)$, which has degree at most $h$. Thus $f(x) = wg(x)$, and $f, g$ must have the same roots in the same multiplicities. That is, the multisets are equal

$$\left\{-v(a_i)u(a_i)^{-1} \colon 1 \le i \le h\right\} = \left\{-v(b_i)u(b_i)^{-1} \colon 1 \le i \le h\right\},$$

including the number of occurrences of undefined elements. As noted above, the value of $-v(a_i)u(a_i)^{-1}$ uniquely determines $a_i$, so that the multiset equality

$$\{a_1, \dots, a_h\} = \{b_1, \dots, b_h\}$$

holds.

We can take $\tau$ to be $\theta$, the generator provided in the Conway polynomial representation, and we can locate $b \in \mathbb{Z}/M\mathbb{Z}$ so that $\beta = \theta^b$, and then $S_h(\tau, \beta) = \textsc{Singer}_h(\theta, b)$. We have proven the claims in Theorem 3 concerning $\textsc{Singer}_h(q, b)$ sets.

Before proceeding into the proof of Theorem 4 as it pertains to $\textsc{Singer}$ sets, we note that as with $\textsc{BoseCh}$ sets, neither the completion of $1, \beta$ into a basis (which we do not elaborate upon) nor the particular choice of generator actually matters, up to affine equivalence, which we now elaborate. Suppose $\tau = \theta^k, \beta = \theta^b$. Then

$$\begin{aligned} S_h(\tau, \beta) &:= \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \tau^a = u\beta + v, \quad u, v \in \mathbb{F}_q\} \\ &= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^{ka} = u\theta^b + v, \quad u, v \in \mathbb{F}_q\right\} = k^{-1} * \textsc{Singer}_h(q, b). \end{aligned}$$

Thus, we have lost nothing by defining $\textsc{Singer}_h(q, b)$ with respect to a specific generator.

Now suppose that $b \equiv e \pmod{M}$, whence $b = e + kM$ for some integer $k$ and

$$\theta^b = \theta^e \theta^{kM} = w\theta^e$$

for some $0 \neq w \in \mathbb{F}_q$. We have

$$\begin{aligned} \textsc{Singer}_h(q, b) &:= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = u\theta^b + v, \quad u, v \in \mathbb{F}_q\right\} \\ &= \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = uw\theta^e + v, \quad u, v \in \mathbb{F}_q\} = \textsc{Singer}_h(q, e). \end{aligned}$$

Recall that the Frobenius automorphism $u \mapsto u^p$, where $p$ is the characteristic of $\mathbb{F}_{q^h}$ fixes each element of $\mathbb{F}_q$, and satisfies the "children's binomial theorem": $(u + v)^p = u^p + v^p$ for all $u, v \in \mathbb{F}_{q^h}$. Suppose that $e \equiv pb \pmod{M}$. Then

$$\begin{aligned} \textsc{Singer}_h(q, b) &:= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = u\theta^b + v, \quad u, v \in \mathbb{F}_q\right\} \\ &= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^{ap} = u^p\theta^{bp} + v^p, \quad u, v \in \mathbb{F}_q\right\} \\ &= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^{ap} = u\theta^{bp} + v, \quad u, v \in \mathbb{F}_q\right\} \\ &= p^{-1} * \textsc{Singer}_h(q, bp). \end{aligned}$$

It follows that if $b \equiv p^i e \pmod{q^{h+1} - 1}$ for some integer $i$, then $\textsc{Singer}_h(q, b) \sim \textsc{Singer}_h(q, e)$.

While Theorem 4(vi) is a special case of Theorem 4(vii), we provide a separate proof of the easier (vi) as it is independently useful in computations. Suppose that $w := \theta^e - \theta^b \in \mathbb{F}_q$. Then

$$\begin{aligned} \textsc{Singer}_h(q, b) &:= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = u\theta^b + v, \quad u, v \in \mathbb{F}_q\right\} \\ &= \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = u(\theta^e - w) + v, \quad u, v \in \mathbb{F}_q\} \\ &= \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = u\theta^e + v - uw, \quad u, v \in \mathbb{F}_q\} \\ &= \textsc{Singer}_h(q, e). \end{aligned}$$

We now address Theorem 4(vii). Suppose that $r, t, w, s \in \mathbb{F}_q$, and at least one of $r, t$ is nonzero, and

$$r\theta^b + t\theta^{e+b} + w\theta^e = s.$$

Then $(r + t\theta^e)\theta^b = s - w\theta^e$. Since $1, \theta^e$ are linearly independent over $\mathbb{F}_q$ and at least one of $r, t$ is nonzero, we know that $r + t\theta^e$ is nonzero, say $\theta^k = r + t\theta^e$. We have

$$\begin{aligned}
\textsc{Singer}_h(q, b) &\coloneqq \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = u\theta^b + v, \quad u, v \in \mathbb{F}_q\right\} \\
&= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^k\theta^a = (r + t\theta^e)(u\theta^b + v), \quad u, v \in \mathbb{F}_q\right\} \\
&= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^k\theta^a = rv + u(r + t\theta^e)\theta^b + vt\theta^e, \quad u, v \in \mathbb{F}_q\right\} \\
&= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^k\theta^a = rv + u(s - w\theta^e) + vt\theta^e, \quad u, v \in \mathbb{F}_q\right\} \\
&= \left\{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^k\theta^a = rv + us + (vt - uw)\theta^e, \quad u, v \in \mathbb{F}_q\right\} \\
&= -k + \{a \in \mathbb{Z}/M\mathbb{Z} : \quad \theta^a = u'\theta^e + v', \quad u', v' \in \mathbb{F}_q\}. \\
&= -k + \textsc{Singer}_h(q, e).
\end{aligned}$$

The equality of the last line relies upon the nonsingularness of the equations $u' = rv + us, v' = rt - uw$, which follows from $\theta^b$ being outside $\mathbb{F}_q$ and the equation $(r + t\theta^e)\theta_b = s - w\theta^e$

This concludes the proof of all of the claims regarding Singer sets made in Theorems 3 and 4.

# 5 Lower bounds on $R_h(n)$ and upper bounds on $R_h^{-1}(k)$

Computing $R_2^{-1}(k)$ is an old game already [18]. Babcock [1] computed by hand for $k \leq 10$ (his value of $R_2^{-1}(10)$ is incorrect). More recently, the OGR Project [6] has computed $R_2^{-1}(28) = 585$; the computation took 8.5 years on thousands of machines. We refer the reader to the Wikipedia page for Golomb rulers [19] for $R_2^{-1}(k)$ for $k \leq 28$ and for the sets that are optimal.

Another massive computation for $R_2^{-1}(k)$ was carried out by Dogon & Rokicki [16]. With several clever optimizations, they computed the bound achieved by all subsets of all sets affinely equivalent to $\textsc{BoseCh}_2(q, 1)$ and $\textsc{Singer}_2(q, 1)$ for all $q \leq 40\,000$. In this section, we report on a similar computation, much smaller in scale, for $h = 3$ and $h = 4$.

The asymptotic growth of $R_h(n)$ (respectively, $R_h^{-1}(k)$) is not known for $h > 2$. The best lower bounds on $R_h(n)$ (upper bounds on $R_h^{-1}(k)$) arise from the construction of Singer [17]. Our generalization produces many more such sets, but they are of roughly the same size. Nevertheless, we feel it would be a contribution to the literature to record the resulting bounds under several hypotheses.

Clearly, $R_h^{-1}(1) = 1$, $R_h^{-1}(2) = 2$, and $R_h^{-1}(3) = \max\{1, 2, h + 2\} = h + 2$. We therefore restrict our attention to $k \geq 4$ and $n \geq h + 3$.

By "Bose $B_h$-set", we mean any affine image of $\textsc{BoseCh}_h(q, \theta, b)$ for any $q, \theta, b$ in the domain of $\textsc{BoseCh}_h$. By "Singer $B_h$-set", we mean any affine image of $\textsc{Singer}_h(q, b)$ for any $q, \theta, b$ in the domain of $\textsc{Singer}_h$.

While Singer $B_h$-sets are slightly thicker than Bose $B_h$-sets, it is easier to work with Bose sets. First, if $q$ is a prime power, then $\textsc{BoseCh}_h(q,1)$ is a set with $q$ elements modulo $q^h-1$. Thus, $R_h(q^h-1)\geq q$ and $R_h^{-1}(q)\leq q^h-1$. Consequently, if $k\leq q$ then $R_h^{-1}(k)\leq R_h^{-1}(q)<q^h$. The difficulty is now reduced to locating a prime power greater than $k$, but not too much greater.

We will state results that work for every $k$, for $k>k_0$ with explicit $k_0$, and for $k$ sufficiently large assuming the Riemann Hypothesis. The bounds are either impracticably bad for small $k$, or only apply for impracticably large $k$, or use an impracticably difficult hypothesis. Except for $h=2$, we do not believe that the main terms reported below even have the "correct" coefficient. We start with the most explicit unconditional result.

**Theorem 6** (Cully-Hugill [5])**.** *For all integers $n\geq 1$, there is a prime between $n^{155}$ and $(n+1)^{155}$.*

It follows that there is a prime between $\lceil k^{1/155}\rceil^{155}$ and $\lceil k^{1/155}+1\rceil^{155}$. As

$$\lceil k^{1/155}+1\rceil^{155h}<(k^{1/155}+2)^{155h}<k^h+3^{155h}k^{h-1/155},$$

we have the statement in the theorem below for $R_h^{-1}(k)$. Assuming that

$$k^{155}<q<(k+1)^{155}<n^{1/h}\leq(k+2)^{155}$$

and using the straightforward $k^{155}>(k+2)^{155}-2^{44}(k+1)^{154}$ yields the $R_h(n)$ result.

**Theorem 7.** *For all $k\geq 4$ and $n\geq h+3\geq 5$, we have $R_h^{-1}(k)<k^h+3^{155h}k^{h-1/155}$ and $R_h(n)\geq n^{1/h}-2^{44}n^{154/(155h)}$.*

For large $k$, we can do somewhat better.

**Theorem 8** (Cully-Hugill [5])**.** *For all integers $n>\exp(\exp(32.537))$, there is a prime between $n^3$ and $(n+1)^3$.*

Hence:

**Theorem 9.** *For all $k>e^{e^{34}}$, we have $R_h^{-1}(k)<k^h+(3k)^{h-1/3}$ and $R_h(n)>n^{1/h}-7n^{2/(3h)}$.*

The following famed result [2] is beautifully straightforward to use.

**Theorem 10** (Baker & Harman & Pintz [2])**.** *If $x$ is sufficiently large, then there is a prime in the interval $[x-x^{21/40},n]$, and in the interval $[x,x+x^{21/40}]$.*

This leads to:

**Theorem 11.** *If $k,n$ are sufficiently large, then $R_h^{-1}(k)<k^h+2^hk^{h-19/40}$ and $R_h(n)\geq n^{1/h}-n^{21/(40h)}$.*

Assuming the Riemann Hypothesis, we naturally have stronger results. The best result along these lines of which this author is aware follows [7].

**Theorem 12** (Dudek & Grenié & Loïc [7])**.** *Assuming the Riemann Hypothesis, for all $n \geq 2$, there is a prime between $n^2$ and $(n + (1 + \frac{1}{\log n})^2 \log n)^2$.*

This leads directly to the following.

**Theorem 13.** *Assume the Riemann Hypothesis, and that $k \geq 4$, $n \geq h + 3$. Then*

$$R_h^{-1}(k) < k^h + \log(20k)k^{h-1/2} + 2k^{h-1}\log^{2h}(20k), \quad R_h(n) \geq n^{1/h} - (7 + \tfrac{\log n}{h})n^{1/(2h)}.$$

# 6 Explicit computations

For $k \leq 9$, we computed the minimum-diameter $B_3$-sets in $\mathbb{Z}$ by brute force. This allowed us to find the sequence in the OEIS (A227358), where $R_3^{-1}(10)$ is also reported. These results are shown in Table 1.

| $k$ | $R_3^{-1}(k)$ | witness |
|---|---|---|
| 1 | 1 | $\{0\}$ |
| 2 | 2 | $\{0, 1\}$ |
| 3 | 5 | $\{0, 1, 4\}$ |
| 4 | 12 | $\{0, 1, 7, 11\}, \{0, 1, 8, 11\}$ |
| 5 | 24 | $\{0, 1, 15, 18, 23\}, \{0, 1, 15, 20, 23\}$ |
| 6 | 46 | $\{0, 2, 11, 26, 42, 45\}$ |
| 7 | 83 | $\{0, 1, 7, 50, 59, 78, 82\}, \{0, 2, 23, 45, 72, 79, 82\}$ |
| | | $\{0, 4, 23, 32, 75, 76, 82\}$ |
| 8 | 130 | $\{0, 2, 5, 34, 74, 107, 120, 129\}$ |
| 9 | 209 | $\{0, 1, 17, 26, 127, 138, 185, 204, 208\}$ |
| | | $\{0, 1, 18, 76, 83, 162, 188, 193, 208\}$ |
| 10 | 310 | |

Table 1: A227358, computations by John Tromo, sets and $k \leq 9$ independently computed by the author.

We have computed all translations of all dilations of all subsets of the Singer and Bose $B_3$-sets generated with small $q$ and any $b$. These results are shown in Table 2. The same computation was performed for $B_4$-sets, and those results are given in Table 3.

| $k$ | $R_3^{-1}(k)$ | from Greedy | from BoseCh | with $q$ | from Singer | with $q$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 2 | 1 | 2 |
| 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 5 | 5 | 5 | 4 | 5 | 2 |
| 4 | 12 | 14 | 12 | 5 | 14 | 3 |
| 5 | 24 | 33 | 33 | 5 | 28 | 4 |
| 6 | 46 | 72 | 73 | 11 | 57 | 5 |
| 7 | 83 | 125 | 122 | 7 | 121 | 7 |
| 8 | 130 | 219 | 202 | 8 | 157 | 7 |
| 9 | 209 | 376 | 306 | 9 | 258 | 8 |
| 10 | 310 | 573 | 493 | 11 | 365 | 9 |
| 11 | | 745 | 594 | 11 | 592 | 11 |
| 12 | | 1209 | 894 | 13 | 738 | 11 |
| 13 | | 1557 | 1044 | 13 | 1014 | 13 |
| 14 | | 2442 | 1612 | 17 | 1236 | 13 |
| 15 | | 3098 | 1874 | 17 | 1877 | 16 |
| 16 | | 4048 | 2247 | 16 | 2071 | 16 |
| 17 | | 5298 | 2537 | 17 | 2392 | 16 |
| 18 | | 6704 | 3433 | 19 | 2960 | 17 |
| 19 | | 7839 | 3821 | 19 | 3679 | 19 |
| 20 | | 10987 | 5578 | 23 | 4326 | 19 |
| 21 | | 12332 | 6060 | 23 | 5849 | 23 |
| 22 | | 15465 | 6212 | 23 | 6476 | 23 |
| 23 | | 19144 | 6997 | 23 | 7229 | 23 |
| 24 | | 24546 | 8846 | 25 | 8010 | 23 |
| 25 | | 28974 | 9624 | 25 | 8854 | 25 |
| 26 | | 34406 | 11447 | 27 | 10177 | 25 |
| 27 | | 37769 | 12088 | 27 | 12143 | 27 |
| 28 | | 45864 | 14272 | 29 | 13432 | 27 |
| 29 | | 50877 | 15544 | 29 | | |
| 30 | | 61372 | 17999 | 31 | | |

Table 2: The upper bounds on $R_3^{-1}$ that arise from Singer and Bose $B_3$-sets, and also the greedy $B_3$-set (A096772).

| $k$ | $R_4^{-1}(k)$ | from Greedy | from BoseCh | with $q$ | from Singer | with $q$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 2 | 1 | 2 |
| 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| 3 | 6 | 6 | 6 | 3 | 6 | 2 |
| 4 | 16 | 22 | 26 | 5 | 18 | 3 |
| 5 | 42 | 56 | 89 | 5 | 71 | 5 |
| 6 | 101 | 154 | 212 | 7 | 156 | 5 |
| 7 | | 369 | 404 | 7 | 388 | 7 |
| 8 | | 857 | 959 | 8 | 693 | 7 |
| 9 | | 1425 | 1731 | 11 | 1290 | 9 |
| 10 | | 2604 | 2878 | 11 | 2345 | 9 |
| 11 | | 4968 | 4469 | 11 | 4053 | 11 |
| 12 | | 8195 | 7967 | 13 | 5174 | 11 |
| 13 | | 13664 | 9903 | 13 | 9328 | 13 |
| 14 | | 22433 | 15907 | 16 | 11348 | 13 |
| 15 | | 28170 | 20849 | 16 | | |
| 16 | | 47689 | 25397 | 16 | | |
| 17 | | 65546 | 35282 | 17 | | |
| 18 | | 96616 | 45783 | 19 | | |
| 19 | | 146249 | 58033 | 19 | | |

Table 3: The upper bounds on $R_4^{-1}$ that arise from Singer and Bose $B_4$-sets, and the greedy $B_4$-set (A365300).

# 7 Open questions

The following questions are interesting to the author, who does not know of solutions.

1. The greedy $B_2$-set is called the Mian-Chowla sequence [13], and the first terms were computed in the 1940s. I'm not aware of any computation of the greedy $B_h$ sequence for $h > 2$. I have added these sequences to the OEIS for $4 \le h \le 9$ (sequences A365300 through A365305).

2. The conditions in Theorem 4 are necessary for $\text{BoseCh}_h(q, e) \sim \text{BoseCh}_h(q, b)$; are they sufficient? Also, for Singer sets.

3. Is there a faster way to interpret Theorem 4(ii)? Theorem 4(vii) is particularly time consuming, can one assume without loss of generality that $r = 0$ and $t = 1$?

4. Does $\text{BoseCh}_2(q, 1)$ always have two elements whose difference is relatively prime to $q^2 - 1$? Equivalently, is there an affine image of $\text{BoseCh}_2(q, \theta, 1)$ that contains $\{1, 2\}$?

Is there any $m, s, q$ with

$$\{0, 1, 4, 10, 18, 23, 25\} \subseteq m * \textsc{BoseCh}_2(q, 1) + s \pmod{q^2 - 1}?$$

Halberstam & Laxton [10] considered the $m$ for which there is an $s$ with $\textsc{BoseCh}_2(q, 1) = m * \textsc{BoseCh}_2(q, 1) + s$. Can this be generalized to $h > 2$? Also for Singer sets.

5. Does the largest modular gap between consecutive elements of $\textsc{BoseCh}_2(q, 1), \textsc{Singer}_2(q, 1)$ have order $O(q)$? It seems not, even if one chooses an affine image to make the largest gap as small as possible.

6. It is obvious that affine maps preserve the $B_h$ property. The existence of Bose sets that are not affine images of each other suggests that there may be some more general arithmetic (or geometric) operation (beyond affine equivalence) that preserves the $B_h$ property in cyclic groups.

# References


[1] Wallace C. Babcock, Intermodulation interference in radio systems, *Bell System Technical Journal* **32** (1953), 63–73.

[2] R. C. Baker, G. Harman, and J. Pintz, The difference between consecutive primes. II, *Proc. London Math. Soc.* **83** (2001), 532–562.

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

[4] R. C. Bose and S. Chowla, Theorems in the additive theory of numbers, *Comment. Math. Helv.* **37** (1962/63), 141–147.

[5] Michaela Cully-Hugill, Primes between consecutive powers, *J. Number Theory* **247** (2023), 100–117.

[6] Distributed.net, Completion of OGR-28 project. A collaborative computing effort. Published electronically at https://blogs.distributed.net/2022/11/23/03/28/bovine/.

[7] Adrian W. Dudek, Loïc Grenié, and Giuseppe Molteni, Primes in explicit short intervals on RH, *Int. J. Number Theory* **12** (2016), 1391–1407.

[8] 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.

[9] Carlos Alexis Gómez Ruiz and Carlos Alberto Trujillo Solarte, Una nueva construcción de conjuntos $B_h$ modulares, *Matemáticas: Enseñanza Universitaria* **19** (2011), 53–62.

[10] H. Halberstam and R. R. Laxton, On perfect difference sets, *Quart. J. Math. Oxford Ser.* **14** (1963), 86–90.

[11] Lenwood S. Heath and Nicholas A. Loehr, New algorithms for generating Conway polynomials over finite fields, *J. Symbolic Comput.* **38** (2004), 1003–1024.

[12] Frank Lübeck, Conway polynomials for finite fields. Published electronically at `http://www.math.rwth-aachen.de/~Frank.Luebeck/data/ConwayPol/index.html`.

[13] Abdul Majid Mian and S. Chowla, On the $B_2$ sequences of Sidon, *Proc. Nat. Acad. Sci. India. Sect. A.* **14** (1944), 3–4.

[14] Kevin O'Bryant, A complete annotated bibliography of work related to Sidon sequences, *Electron. J. Combin.* **DS11** (2004), Paper # 39.

[15] OEIS Foundation Inc., The On-Line Encyclopedia of Integer Sequences, 2023. Published electronically at `https://oeis.org`.

[16] Tomas Rokicki and Gil Dogon, Larger Golomb rulers, *Gathering4Gardner 12 Exchange Book* **1** (2016), 155–166. Available at `https://www.gathering4gardner.org/g4g12gift/Rokicki_Dogon-Larger_Golomb_Rulers.pdf`.

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

[18] Oswald Veblen, Diophantine analysis: problem 132, *Amer. Math. Monthly* **13** (1906), 46. Solution by F. H. Safford appears in **13** (1906), 215.

[19] Wikipedia, Golomb ruler, 2023-12-20. `https://en.wikipedia.org/wiki/Golomb_ruler`.

---

2020 *Mathematics Subject Classification*: Primary 05B10; Secondary 11B83.
*Keywords:* $B_h$-set, Sidon set, Golomb ruler.

---

(Concerned with sequences A096772, A227358, A365300, A365301, A365302, A365303, A365304, A365305.)

---

Received August 24 2023; revised versions received August 26 2023; January 3 2024. Published in *Journal of Integer Sequences*, January 4 2024.

---

Return to Journal of Integer Sequences home page.