Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 38 (1992)
Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: BARKER SEQUENCES AND DIFFERENCE SETS
Autor: Eliahou, Shalom / Kervaire, Michel
Kapitel: 4. The use of the Multiplier Theorem
DOI: https://doi.org/10.5169/seals-59496

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 24.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

The remaining candidates are listed below, together with an indication in parenthesis showing that each one (except 505) is excluded by Theorem 2 in Section 2: if N has a prime factor p such that $p^f \equiv -1 \bmod N'$, where N' is the largest divisor of N relatively prime to p, then there is no (periodic) Barker sequence of length $4N^2$.

REMAINING CANDIDATES (excluded by Theorem 2, except $N = 505$.)

N		N	
$65 = 5 \cdot 13$	$(5^2 \equiv -1 \bmod 13)$	$425 = 5^2 \cdot 17$	$(5^8 \equiv -1 \bmod 17)$
$85 = 5 \cdot 17$	$(17^2 \equiv -1 \bmod 5)$	$445 = 5 \cdot 89$	$(89 \equiv -1 \bmod 5)$
$145 = 5 \cdot 29$	$(29 \equiv -1 \bmod 5)$	$481 = 13 \cdot 37$	$(37^6 \equiv -1 \bmod 13)$
$185 = 5 \cdot 37$	$(37^2 \equiv -1 \bmod 5)$	$485 = 5 \cdot 97$	$(97^2 \equiv -1 \bmod 5)$
$205 = 5 \cdot 41$	$(5^{10} \equiv -1 \bmod 41)$	$493 = 17 \cdot 29$	$(17^2 \equiv -1 \bmod 29)$
$221 = 13 \cdot 17$	$(13^2 \equiv -1 \bmod 17)$	$505 = 5 \cdot 101$	
$265 = 5 \cdot 53$	$(53^2 \equiv -1 \bmod 5)$	$533 = 13 \cdot 43$	$(43^3 \equiv -1 \bmod 13)$
$305 = 5 \cdot 61$	$(5^{15} \equiv -1 \bmod 61)$	$545 = 5 \cdot 109$	$(109 \equiv -1 \bmod 5)$
$325 = 5^2 \cdot 13$	$(5^2 \equiv -1 \bmod 13)$	$565 = 5 \cdot 113$	$(113^2 \equiv -1 \bmod 5)$
$365 = 5 \cdot 73$	$(73^2 \equiv -1 \bmod 5)$	$629 = 17 \cdot 37$	$(37^8 \equiv -1 \bmod 17)$
$377 = 13 \cdot 29$	$(13^7 \equiv -1 \bmod 29)$	$685 = 5 \cdot 137$	$(137^2 \equiv -1 \bmod 5)$

The case $N = 505 = 5 \cdot 101$ cannot be excluded by Theorem 2, because $101 \equiv 1 \bmod 5$ and $5^{25} \equiv 1 \bmod 101$. However, 505 can still be excluded by Turyn's Inequality, as observed in [JL]: choosing $p = 101$ and $w = 2 \cdot 101^2$, so that p is trivially semi-primitive modulo w, we would have

$$p \leqslant \frac{v}{w} = 2 \cdot 5^2 = 50 ,$$

a contradiction to the assumed existence of a Barker sequence of length $4 \cdot 505^2$.

The first open case is thus $N = 689 = 13 \cdot 53$. We have $53 \equiv 1 \bmod 13$ and $13^{13} \equiv 1 \bmod 53$, so that neither 53 is semi-primitive mod 13, nor 13 is semi-primitive mod 53. The next open case is $N = 793 = 13 \cdot 61$.

4. THE USE OF THE MULTIPLIER THEOREM

In this section we give the details of some (typical) non-existence proofs needed to establish the tables, using the multiplier theorem.

Recall that if D is a cyclic difference set with parameters (v, k, λ), and if $n = k - \lambda$ is greater than λ, then the group of multipliers of D contains the intersection M in $(\mathbf{Z}/v\mathbf{Z})^*$ of the subgroups generated by $l_1, \ldots, l_r$, where $l_1, \ldots, l_r$ are the prime factors of n.

(1) *Parameters* ($v = 181, k = 81, \lambda = 36$), *Table I with* $t = 9$.

Here, $n = 3^2 \cdot 5$, and since $5 \equiv 3^6 \bmod 181$, the multiplier theorem says that if an abelian difference set exists with these parameters, then 5 is a multiplier. The orbits of the multiplication by 5 in $\mathbf{Z}/181\mathbf{Z}$ are $\{0\}$ and 12 orbits of cardinality 15, e.g.

$$\{1, 5, 25, 125, 82, 48, 59, 114, 27, 135, 132, 117, 42, 29, 145\}.$$

(Note that 181 is a prime number.) No subset of $G = \mathbf{Z}/181\mathbf{Z}$ of cardinality $k = 81$ may thus be a union of orbits.

(2) *Parameters* ($v = 4901, k = 2401, \lambda = 1176$), *Table I with* $t = 49$.

Here, $n = 5^2 \cdot 7^2$. We have $25 = 5^2 \equiv 7^6 \bmod 4901$. Therefore, if an abelian difference set exists, $m = 25$ must be a multiplier. Writing the group $G = \mathbf{Z}/4901\mathbf{Z}$ as $G = \mathbf{Z}/13^2\mathbf{Z} \times \mathbf{Z}/29\mathbf{Z}$, with group operation $(a, b) \cdot (a', b') = (a + a', b + b')$, the orbits under multiplication by $m = 25$ are

$$\begin{aligned}
E &= \{(0,0)\} \\
U_i &= \{(13i, 0), (-13i, 0)\} \quad i = 1, 2, 3, 4, 5, 6 \\
V_j &= \{(j,0), (25j,0), (118j,0), (77j,0), (66j,0), (129j,0), (14j,0), (12j,0), \\
&\quad (131j,0), (64j,0), (79j,0), (116j,0), (27j,0), (-j,0), \ldots\} \\
&\quad j = 1, \ldots, 6, \text{ each } V_j \text{ of cardinality } 26. \\
X &= \{(0,1), (0,25), (0,16), (0,23), (0,24), (0,20), (0,7)\} \\
Y &= \{(0,2), (0,21), (0,3), (0,17), (0,19), (0,11), (0,14)\} \\
\bar{X} &= \{(0, -x) \mid (0,x) \in X\} \\
\bar{Y} &= \{(0, -y) \mid (0,y) \in Y\}
\end{aligned}$$

each of cardinality 7.

There are moreover, the 24 orbits $U_i \cdot X$, $U_i \cdot \bar{X}$, $U_i \cdot Y$, $U_i \cdot \bar{Y}$ of cardinality 14, where

$$A \cdot B = \{a \cdot b \mid a \in A, b \in B\}.$$

Finally, there are 24 orbits $V_i \cdot X$, $V_i \cdot \bar{X}$, $V_i \cdot Y$, $V_i \cdot \bar{Y}$ of cardinality 182. Contrary to the preceding example, there are many ways of writing the cardinality 2401 of a putative difference set D as a sum of numbers taken from the set of orbit cardinalities.

To ease calculations, we view a subset $S \subset G$ as the element $\sum_{s \in S} s$ in the integral group ring. Note that, with this convention, the product $S \cdot T$ in $\mathbf{Z}G$ coincides with the element of $\mathbf{Z}G$ associated with the product set

$S \cdot T = \{s \cdot t \mid s \in S, t \in T\}$. A difference set D, if it exists with the above parameters, can be written as

$$D = C + AX + BY + P\bar{X} + Q\bar{Y}$$

where C, as well as A, B, P, Q, is of the form

$$C = \alpha E + \sum_{i=1}^{6} \beta_i U_i + \sum_{j=1}^{6} \gamma_j V_j$$

with coefficients $\alpha, \beta_1, \ldots, \beta_6, \gamma_1, \ldots, \gamma_6$ all equal to 0 or 1.

As in Section 1, D is a difference set if and only if

$$D\bar{D} = 1225 + 1176 \cdot \left(1 + \sum_{i=1}^{6} U_i + \sum_{j=1}^{6} V_j\right) \cdot (1 + X + \bar{X} + Y + \bar{Y}) .$$

Now, writing $G = G_1 \times G_2$ as above, $G_1 = \mathbf{Z}/13^2\mathbf{Z}$, $G_2 = \mathbf{Z}/29\mathbf{Z}$, let $\pi : \mathbf{Z}G \to \mathbf{Z}G_1$ be the projection on the group ring of G_1. We have $\pi X = \pi\bar{X} = \pi Y = \pi\bar{Y} = 7$, and reducing modulo 7,

$$\pi(D\bar{D}) = C\bar{C} = 0 \text{ in } \mathbf{F}_7 G_1 .$$

The involution of $\mathbf{Z}G$, sending (a, b) to $\overline{(a, b)} = (-a, -b)$, is the identity on U_i, V_j:

$$\bar{U}_i = U_i, \qquad \bar{V}_j = V_j .$$

Therefore $\bar{C} = C$ and $C^2 = 0$ in $\mathbf{F}_7 G_1$. However, $\mathbf{F}_7 G_1$, where G_1 is of order 13^2, prime to 7, is a semi-simple algebra and does not contain any nilpotent element. It follows that $C = 0$ in $\mathbf{F}_7 G_1$. Since the coefficients of $C = \alpha E + \sum_{i=1}^{6} \beta_i U_i + \sum_{j=1}^{6} \gamma_i V_j$ are all 0 or 1, this implies $C = 0$ in $\mathbf{Z}G_1$, i.e.

$$D = AX + BY + P\bar{X} + Q\bar{Y} ,$$

and $\pi D = 7 \cdot S$ with

$$S = r + \sum_{i=1}^{6} s_i U_i + \sum_{j=1}^{6} t_j V_j ,$$

where $S = A + B + P + Q$. Thus, all coefficients $r, s_1, \ldots, s_6, t_1, \ldots, t_6$ are non-negative integers $\leqslant 4$.

Again $\pi(D\bar{D}) = 1225 + 1176 \cdot (1 + \sum U_i + \sum V_j) \cdot 29$. Therefore,

$$S^2 = 25 + 696 \cdot \left(1 + \sum_{i=1}^{6} U_i + \sum_{j=1}^{6} V_j\right) .$$

With our (abuse of) notation, we set $G_1 = 1 + \sum U_i + \sum V_j$. Then, $G_1^2 = 169 \cdot G_1$. Thus, we see that

$$S = \pm (5 + 2G_1)$$

are solutions of $S^2 = 25 + 696 \cdot G_1$. We claim that there is no other. This will clearly finish the non-existence proof since $r \leqslant 4$. Note the decomposition

$$\mathbf{Q}G_1 = \mathbf{Q} \times \mathbf{Q}(\zeta_{13}) \times \mathbf{Q}(\zeta_{169})$$

of the algebra $\mathbf{Q}G_1$ as a product of fields, where ζ_{13} is a primitive 13-th root of unity, and ζ_{169} a primitive 169-th root of unity.

The element $G_1 = \sum_{k=0}^{168} z^k \in \mathbf{Z}G_1$ corresponds on the right hand side to $(169, 0, 0)$ since ζ_{13} and ζ_{169} are roots of the polynomial $\sum_{k=0}^{168} X^k$. It follows that $S^2 = (343^2, 5^2, 5^2)$. Hence, any solution $Z \in \mathbf{Z}G_1$ of the equation $Z^2 = 25 + 696G_1$ must correspond to $(\pm 343, \pm 5, \pm 5)$. Changing Z to $-Z$, we can assume $Z = (343, \pm 5, \pm 5)$. Now, the diagrams

$$\begin{array}{ccc} \mathbf{Z}G_1 & \rightarrow & \mathbf{Z}[\zeta_{13}] \\ \downarrow & & \downarrow \\ \mathbf{Z} & \rightarrow & \mathbf{F}_{13} \end{array}$$

and

$$\begin{array}{ccc} \mathbf{Z}G_1 & \rightarrow & \mathbf{Z}[\zeta_{169}] \\ \downarrow & & \downarrow \\ \mathbf{Z} & \rightarrow & \mathbf{F}_{13} \end{array}$$

where the right vertical arrows send ζ_{13}, resp. ζ_{169} to $1 \in \mathbf{F}_{13}$, are commutative. Since 5 is not congruent to -5 modulo 13, and 343 maps to $+5 \in \mathbf{F}_{13}$, we see that $Z = (343, 5, 5) = S$.

(3) *Parameters* ($v = 13613$, $k = 6724$, $\lambda = 3321$), *Table I with* $t = 82$.

This case is as simple as case (1). Indeed, $n = 3403 = 41 \cdot 83$. Since $41 \equiv 83^3 \bmod 13613$, it follows from the multiplier theorem that if a cyclic difference set D with parameters (13613, 6724, 3321) existed, then 41 would be a multiplier, and D could be taken to be a union of orbits under multiplication by 41 on the cyclic group $\mathbf{Z}/13613\mathbf{Z}$.

The order of 41 modulo 13613 is 3403, and beside the one-point orbit $\{0\}$, there are 4 orbits X, iX, i^2X, i^3X each of cardinality 3403, where

$$X = \{1, 41, 1681, \ldots, 13281\}$$

and i is a square root of -1 mod 13613, e.g. $i = 165$. Note that 13613 is a prime number.

However, 6724 is not of the form $n_0 + 3403n_1$ with $n_0 = 0$ or 1 and $0 \leqslant n_1 \leqslant 4$. No difference set can therefore have the above parameters.

(4), (5), (6) *Parameters* $(v, k, \lambda) = (3^3, 13, 6)$, $(3^5, 121, 60)$ *and* $(7^3, 171, 85)$ *of Table II, with* $n = 7, 61$ *and* 86 *respectively.*

More generally, we will consider the case

$$(v, k, \lambda) = \left(p^{2t+1}, \frac{p^{2t+1} - 1}{2}, \frac{p^{2t+1} - 3}{4}\right),$$

where p is a prime $\equiv 3$ mod 4.

We have $n = k - \lambda = \dfrac{p^{2t+1} + 1}{4}$. Let $l_1, \ldots, l_r$ be the primes dividing n. The group of multipliers for a putative difference set D with the above parameters contains the intersection M in $(\mathbf{Z}/v\mathbf{Z})^*$ of the subgroups generated by $l_1, \ldots, l_r$. Since $(\mathbf{Z}/v\mathbf{Z})^*$ is cyclic, M is the unique subgroup of $(\mathbf{Z}/v\mathbf{Z})^*$ whose order is the greatest common divisor of the orders $q_1, \ldots, q_r$ of $l_1, \ldots, l_r$ in $(\mathbf{Z}/v\mathbf{Z})^*$. We will now assume that the orders $q_1, \ldots, q_r$ of the prime factors $l_1, \ldots, l_r$ of $n = k - \lambda$ in $(\mathbf{Z}/v\mathbf{Z})^*$ are all divisible by p^{t+1}.

THEOREM. *There is no cyclic difference set with parameters*

$$(v, k, \lambda) = \left(p^{2t+1}, \frac{p^{2t+1} - 1}{2}, \frac{p^{2t+1} - 3}{4}\right),$$

where p *is a prime* $\equiv 3$ mod 4, *provided that the orders* $q_1, \ldots, q_r$ *of the prime factors* $l_1, \ldots, l_r$ *of* $n = k - \lambda$ *in* $(\mathbf{Z}/v\mathbf{Z})^*$ *are all divisible by* p^{t+1}.

Note that the hypotheses of the theorem above are satisfied for the three examples we have in mind. (Cases $n = 7, 61$ and 86 in Table II.)

(1) $n = 7: p = 3, t = 1$, and 7 is of order 3^2 modulo 27;

(2) $n = 61: p = 3, t = 2$, and 61 is of order 3^4 modulo 243;

(3) $n = 86: p = 7, t = 1$, and 2 is of order $3 \cdot 7^2$ modulo 343, 43 is of order 7^2 modulo 343.

As expected, the hypothesis on the orders of the prime factors of n is not satisfied in general. It fails for instance for $p = 11$, $t = 1$: here $n = \dfrac{11^3 + 1}{4} = 333 = 3^2 \cdot 37$ and whereas 37 is of order $5 \cdot 11^2$ modulo 11^3, 3 is only of order $5 \cdot 11$ modulo 11^3.

However, failure of the hypothesis seems fairly rare: the next example with $t = 1$ occurs for $p = 3511$. Note that 3511 is special for another reason: it satisfies the congruence $2^{p-1} \equiv 1 \bmod p^2$, the only other known solution being the famous $p = 1093$. Such prime numbers are known in the literature as Wieferich prime numbers.

The behaviour of the orders of the prime factors of $n = \dfrac{p^{2t+1}+1}{4}$ in $(\mathbf{Z}/p^{2t+1}\mathbf{Z})^*$ is probably a difficult question.

Proof of the Theorem. The hypothesis on the orders $q_1, \ldots, q_r$ means that $m = 1 + p^t$, which generates the subgroup of order p^{t+1} in $(\mathbf{Z}/p^{2t+1}\mathbf{Z})^*$, is contained in all the subgroups $< l_1 >, \ldots, < l_r >$ of $(\mathbf{Z}/p^{2t+1}\mathbf{Z})^*$, and thus is a multiplier of any candidate difference set $D \subset \mathbf{Z}/p^{2t+1}\mathbf{Z}$ with the above parameters.

What are the orbits of multiplication by $m = 1 + p^t$ in the ring $\mathbf{Z}/p^{2t+1}\mathbf{Z}$? If $a_i = i \cdot p^{t+1}$, then $a \cdot m \equiv a \bmod p^{2t+1}$. Hence, there are p^t fixed points $a_0 = 0, a_1, \ldots, a_{p^t-1}$.

More generally, if $a_{i,j} = ip^{t-j+1}$ with $1 \leqslant i \leqslant p^t - 1$ and $\gcd(i,p) = 1$, $j = 1, \ldots, t+1$, then $a_{i,j}$ produces an orbit $\{a_{i,j}m^\nu\}_{\nu = 0, \ldots, p^j - 1}$ of length p^j. Here, we use the formula

$$(1 + p^t)^{p^s} \equiv 1 + p^{t+s} \mod (p^{t+s+1})$$

easily proved (for p odd) by induction on s, and which implies that m has (multiplicative) order p^j modulo p^{t+j}.

The orbits $A_{i,j}$ of $a_{i,j}$ with $i \in \mathbf{Z}/p^t\mathbf{Z}$ for $j = 0$ $(a_{i,0} = a_i)$, and $i \in (\mathbf{Z}/p^t\mathbf{Z})^*$ for $j = 1, \ldots, t+1$ are easily verified to be disjoint. Together, they sweep out

$$p^t + \sum_{j=1}^{t+1} (p-1)p^{t-1}\, p^j = p^{2t+1}$$

elements of the group $\mathbf{Z}/p^{2t+1}\mathbf{Z}$. Hence, $A_{i,j}$ with $i \in \mathbf{Z}/p^t\mathbf{Z}$ for $j = 0$ $(a_{i,0} = a_i)$, and $i \in (\mathbf{Z}/p^t\mathbf{Z})^*$ for $j = 1, \ldots, t+1$ is the complete collection of orbits under multiplication by $m = 1 + p^t$ in $\mathbf{Z}/p^{2t+1}\mathbf{Z}$. At this point, it may be more convenient to write the group ring of $\mathbf{Z}/p^{2t+1}\mathbf{Z}$ as $\mathbf{Z}[x]/(x^{p^{2t+1}} - 1)$. Identifying a subset $A \subset \mathbf{Z}/p^{2t+1}\mathbf{Z}$ with the sum of the corresponding elements $\sum_{a \in A} a$ in the group ring, the orbits $A_{i,j}$ can then be written as

$$A_{i,j} = \sum_{\nu=0}^{p^j - 1} x^{ip^{t-j+1}m^\nu}.$$

If a difference set D with the above parameters exists, it must be of the form

$$D = \sum_{i \in S_0} x^{ip^{t+1}} + \sum_{j=1}^{t+1} \sum_{i \in S_j} A_{i,j}$$

where $S_0 \subset \mathbf{Z}/p^t\mathbf{Z}$ and $S_j \subset (\mathbf{Z}/p^t\mathbf{Z})^*$ for $j = 1, \ldots, t+1$. Now, let $\pi : \mathbf{Z}[x]/(x^{p^{2t+1}} - 1) \to \mathbf{Z}[y]/(y^p - 1)$ be the projection of the group ring of $\mathbf{Z}/p^{2t+1}\mathbf{Z}$ onto the group ring of the cyclic group of order p. We have $\pi(x) = y$ and

$$\pi A_{i,j} = p^i \quad \text{for} \quad j = 0, 1, \ldots, t$$
$$\pi A_{i,t+1} = p^{t+1} \cdot y^i \quad \text{for} \quad i \in (\mathbf{Z}/p^t\mathbf{Z})^* .$$

It follows that

$$\pi D = s_0 + ps_1 + \cdots + p^t s_t + p^{t+1} \left(\sum_{i \in S_{t+1}} y^i \right),$$

where $s_j = \mathrm{Card}(S_j)$.

Let $N = s_0 + ps_1 + \cdots + p^t s_t$ and $a_\mu = \mathrm{Card}\{i \mid i \in S_{t+1}, i \equiv \mu \bmod p\}$, then

$$\pi D = N + p^{t+1} Y,$$

with $Y = \sum_{\mu=1}^{p-1} a_\mu y^\mu$. (Note that a_0 is indeed 0 as $S_{t+1} \subset (\mathbf{Z}/p^t\mathbf{Z})^*$.) Therefore $\pi(D\bar{D}) = \pi(D)\overline{\pi(D)}$ has the form

$$\pi(D\bar{D}) = N^2 + Np^{t+1} \sum_{\mu=1}^{p-1} a_\mu (y^\mu + y^{-\mu}) + p^{2t+2} Y\bar{Y} .$$

On the other hand the condition for D being a difference set yields, after applying π,

$$\pi(D\bar{D}) = \frac{p^{2t+1}+1}{4} + \frac{p^{2t+1}-3}{4} p^{2t} \left(\sum_{\mu=0}^{p-1} y^\mu \right) .$$

We will reach a contradiction by comparing the constant terms (coefficient of 1 in $\mathbf{Z}[y]/(y^p - 1)$) in the two expressions for $\pi(D\bar{D})$:

$$N^2 + p^{2t+2} \sum_{\mu=1}^{p-1} a_\mu^2 = \frac{p^{2t+1}+1}{4} + \frac{p^{2t+1}-3}{4} p^{2t} .$$

Note that $k = \mathrm{Card}(D) = N + p^{t+1} s_{t+1}$, where $s_{t+1} = \mathrm{Card}(S_{t+1})$, and hence $N = \dfrac{p^{2t+1}-1}{2} - p^{t+1} s_{t+1}$. Substituting this in the above equation,

we get

$$4s_{t+1} \equiv 3p^{t-1}(p-1) \mod p^{t+1} .$$

Writing $4s_{t+1} = 3p^{t-1}(p-1) + z \cdot p^{t+1}$ for $z \in \mathbf{Z}$, we observe that $p \equiv 3 \mod 4$ implies $z \equiv 2 \mod 4$, and so $2p^{t+1} \leqslant |z \cdot p^{t+1}|$. But, $s_{t+1} = \mathrm{Card}(S_{t+1}) \leqslant p^{t-1}(p-1)$, since $S_{t+1} \subset (\mathbf{Z}/p^t\mathbf{Z})^*$. It follows that

$$|z \cdot p^{t+1}| \leqslant |4s_{t+1} - 3p^{t-1}(p-1)| \leqslant 3p^{t-1}(p-1) < 2p^{t+1} \leqslant |z \cdot p^{t+1}| .$$

We have reached the desired contradiction, i.e. no cyclic difference set with parameters $\left(p^{2t+1}, \dfrac{p^{2t+1}-1}{2}, \dfrac{p^{2t+1}-3}{4}\right)$ exists if the orders of the prime factors of $n = \dfrac{p^{2t+1}+1}{4}$ in $(\mathbf{Z}/p^{2t+1}\mathbf{Z})^*$ are all divisible by p^{t+1}. $\square$

(7) *Parameters* ($v = 399, k = 199, \lambda = 99$), *Table II.* This is the last item in Table II, corresponding to $n = k - \lambda = 100$.

Since $4 = 2^2 \equiv 5^8 \mod 399$, it follows that 4 must be a multiplier of any abelian difference set D with the above parameters.

Writing $\mathbf{Z}/399\mathbf{Z}$ as a direct product

$$\mathbf{Z}/399\mathbf{Z} = \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/7\mathbf{Z} \times \mathbf{Z}/19\mathbf{Z} ,$$

and accordingly writing the elements of $\mathbf{Z}/399\mathbf{Z}$ as triples $g = (x, y, z)$, $x \in \mathbf{Z}/3\mathbf{Z}$, $y \in \mathbf{Z}/7\mathbf{Z}$, $z \in \mathbf{Z}/19\mathbf{Z}$, we have the following orbits of the multiplication by 4 in $\mathbf{Z}/399\mathbf{Z}$: all monomials XYZ, with $X \in \{1, U, \bar{U}\}$, $Y \in \{1, V, \bar{V}\}$, $Z \in \{1, W, \bar{W}\}$, where

$$1 = \{(0,0,0)\}$$

$$U = \{(1,0,0)\}$$

$$V = \{(0,1,0), (0,-3,0), (0,2,0)\}$$

$$W = \{(0,0,1), \ (0,0,4), \ (0,0,-3), \ (0,0,7), \ (0,0,9), \ (0,0,-2), \ (0,0,-8), \ (0,0,6), \ (0,0,5)\} ,$$

and bar denotes the conjugate, i.e. if $C \subset \mathbf{Z}/v\mathbf{Z}$, then $\bar{C} = \{-g \mid g \in C\}$.

All orbits, except $1, U, \bar{U}$ have cardinality divisible by 3. Since $k = 199 \equiv 1 \mod 3$, any putative difference set D can be assumed to contain a single one-point orbit 1, U or $\bar{U}$. Multiplying D by U or $\bar{U}$ if necessary, we may assume that

$$D = 1 + A \cdot V + B \cdot \bar{V} + P \cdot W + Q \cdot \bar{W} ,$$

where

$$A = \alpha_0 + \alpha_1 U + \alpha_2 \bar{U} , \ 0 \leqslant \alpha_i \leqslant 1 ,$$

$$B = \beta_0 + \beta_1 U + \beta_2 \bar{U} , \ 0 \leqslant \beta_i \leqslant 1 ,$$

and P, Q are polynomials in $U, \bar{U}$ and $V, \bar{V}$.

We first show that A and B must be 0. Let $a = \alpha_0 + \alpha_1 + \alpha_2$, $b = \beta_0 + \beta_1 + \beta_2$, and let $\pi: \mathbf{Z}/399\mathbf{Z} \to \mathbf{Z}/7\mathbf{Z}$ be the projection on the second factor.

We indulge in various abuses of notation: we write π for the group ring projection as well and denote πV again by V. Note that $\pi U = \pi \bar{U} = 1$, $\pi W = \pi \bar{W} = 9$. Then $\pi D \equiv 1 + aV + b\bar{V} \bmod 9$, a congruence in the group ring of $\mathbf{Z}/7\mathbf{Z}$.

Since $D\bar{D} = 100 + 99 \cdot (1 + U + \bar{U})(1 + V + \bar{V})(1 + W + \bar{W})$, the equation expressing that D is a difference set with the required parameters, we have $D\bar{D} \equiv 1 \bmod 9$.

Consequently, using

$$V\bar{V} = 3 + V + \bar{V}, \qquad V^2 = V + 2\bar{V}, \qquad \bar{V}^2 = 2V + \bar{V},$$

we get, expanding $\pi(D\bar{D}) = \pi(D)\pi(\bar{D})$, and after collecting terms,

$$3(a^2 + b^2) + (a + b + a^2 + b^2 + 3ab)(V + \bar{V}) \equiv 0 \mod 9 .$$

Thus, $a^2 + b^2 \equiv 0 \bmod 3$, and this means $a \equiv b \equiv 0 \bmod 3$. But then $a^2 + b^2 + 3ab \equiv 0 \bmod 9$, and so we must also have

$$a + b \equiv 0 \mod 9 ,$$

after looking at the coefficient of $V + \bar{V}$ in the above congruence.

Since $0 \leqslant a \leqslant 3, 0 \leqslant b \leqslant 3$, this means $a = b = 0$ and therefore $A = B = 0$. Any difference set D with parameters (399, 199, 99) can therefore be assumed to have the form

$$D = 1 + P \cdot W + Q \cdot \bar{W} .$$

Plugging $D = 1 + P \cdot W + Q \cdot \bar{W}$ into the equation

$$D\bar{D} = 100 + 99(1 + U + \bar{U})(1 + V + \bar{V})(1 + W + \bar{W})$$

and using the multiplication table

$$W\bar{W} = 9 + 4(W + \bar{W}), \quad W^2 = 4W + 5\bar{W},$$

we get

$$1 + 9(P\bar{P} + Q\bar{Q}) = 100 + 99(1 + U + \bar{U})(1 + V + \bar{V})$$

$$P + \bar{Q} + 4(P\bar{P} + Q\bar{Q}) + 5\bar{P}Q + 4P\bar{Q} = 99(1 + U + \bar{U})(1 + V + \bar{V}),$$

where

$$P = p_0 + p_1 U + p_2 \bar{U} + (p_3 + p_4 U + p_5 \bar{U})V + (p_6 + p_7 U + p_8 \bar{U})\bar{V}$$

$$Q = q_0 + q_1 U + q_2 \bar{U} + (q_3 + q_4 U + q_5 \bar{U})V + (q_6 + q_7 U + q_8 \bar{U})\bar{V}$$

with $0 \leqslant p_i, q_i \leqslant 1$, for $i = 0, \ldots, 8$.

The first equation gives

$$P\bar{P} + Q\bar{Q} = 11 + 11(1 + U + \bar{U})(1 + V + \bar{V}) .$$

Substituting in the second equation, we get

$$(*) \qquad P + \bar{Q} + 5\bar{P}Q + 4P\bar{Q} = -44 + 55(1 + U + \bar{U})(1 + V + \bar{V}) .$$

Since $U\bar{U} = 1$, $U^2 = \bar{U}$ and $V\bar{V} = 3 + V + \bar{V}$, $V^2 = V + 2\bar{V}$, the constant terms in $\bar{P}Q$ and $P\bar{Q}$ are equal to $\sum_{i=0}^{2} p_i q_i + 3 \sum_{j=3}^{8} p_j q_j = c$, say. Hence, equating constant terms in the above equation (*), we must have

$$p_0 + q_0 + 9c = 11 .$$

The only solution to this equation with all p_i, q_i being 0 or 1, is $p_0 = q_0 = 1$, $p_i = q_i = 0$ for $i = 1, \ldots, 8$. This means $P = Q = 1$, contradicting (*).

5. Comments on the examples in Tables II

Difference sets with parameters $(v, k, \lambda) = (4n - 1, 2n - 1, n - 1)$ are usually called *Hadamard difference sets.* Our purpose here is to discuss the classification of these cyclic difference sets for $2 \leqslant n \leqslant 100$.

In many cases where $v = 4n - 1$ is a prime p, the quadratic residue difference set, which we denote by $QR(p)$ is unique for the given values of the parameters. This is obviously the case if the multiplier m has order $k = \frac{1}{2}(v - 1)$ in $(\mathbf{Z}/v\mathbf{Z})^*$. Indeed, in this case, there are exactly 3 orbits of multiplication by m in $\mathbf{Z}/v\mathbf{Z}$, namely $1 = \{0\}$, $M = \{1, m, m^2, \ldots, m^{k-1}\}$ and $\bar{M} = \{-1, -m, \ldots, -m^{k-1}\}$. Thus the only choice for D is $D = M$ or $D = \bar{M}$, which are isomorphic under conjugation $\sigma: \mathbf{Z}/v\mathbf{Z} \to \mathbf{Z}/v\mathbf{Z}$, $\sigma(a) = -a$.

In our Table II, this situation happens for $n = 3, 5, 6, 12, 15, 17, 18, 20, 21, 27, 33, 35, 41, 42, 45, 48, 53, 57, 60, 63, 66, 68, 77, 87, 90$ and 96.

The remaining cases where $v = 4n - 1$ is a prime p (for $2 \leqslant n \leqslant 100$) have been shown to lead to a single difference set, namely $QR(p)$, by machine enumeration of the various choices of D as a union of orbits under multiplication by a multiplier m. This includes the cases $n = 26$ (multiplier 8), $n = 38$ (multiplier 19), $n = 50$ (multiplier 5), $n = 78$ (multiplier 13), $n = 83$ (multiplier 83), and $n = 95$ (multiplier 5). By far, the most difficult case (for the machine) occurs with $n = 38$, which required the examination of 37 442 160 combinations of multiplier orbits.