BARKER SEQUENCES AND DIFFERENCE SETS

Autor(en): **Eliahou, Shalom / Kervaire, Michel**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **38 (1992)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-59496

L'Enseignement Mathématique, t. 38 (1992), p. 345-382

BARKER SEQUENCES AND DIFFERENCE SETS

by Shalom ELIAHOU and Michel KERVAIRE

INTRODUCTION

This paper deals with binary sequences $A = (a_1, \ldots, a_l)$, i.e. $a_i = \pm 1$ for $i = 1, \ldots, l$, and classical coefficients associated with them, the aperiodic and periodic correlation coefficients. The *aperiodic correlation coefficients* of A are defined as

$$c_j(A) = \sum_{i=1}^{l-j} a_i a_{i+j}\,, \qquad \text{for} \quad j = 1, \ldots, l-1\,,$$

and the *periodic correlation coefficients* of A as

$$\gamma_j(A) = \sum_{i=1}^{l} a_i a_{i+j}, \qquad \text{for} \quad j = 1, \ldots, l-1\,,$$

where the indices are read modulo l, i.e. $a_r = a_{r-l}$ if $r \geqslant l+1$.

It is well-known that $\gamma_j = c_j + c_{l-j}$ for $j = 1, \ldots, l-1$.

There are many interesting and difficult problems concerned with the existence of binary sequences whose correlation coefficients (or *correlations,* for short) are subject to various conditions. We will examine here three classical situations.

(1) One may require the *periodic* correlations γ_j to be constant, i.e.

$$\gamma_1 = \gamma_2 = \ldots = \gamma_{l-1} = \gamma\,.$$

We will see below that binary sequences satisfying this condition are equivalent to the classical notion of cyclic difference sets.

(2) In addition to the condition above, one may furthermore impose the constant γ to be small, i.e. $\gamma = 0$, or $\gamma = 1$, or $\gamma = -1$. We will call such

The authors gratefully acknowledge partial support from the Fonds National Suisse de la Recherche Scientifique during the preparation of this paper.

sequences *periodic Barker sequences*. Periodic Barker sequences with $\gamma = 0$ are equivalent to circulant Hadamard matrices. We will not follow the link with Hadamard matrices any further here.

(3) Without any condition on the periodic correlations, one may require the *aperiodic* correlations to be small, i.e.

$$c_j \in \{0, 1, -1\} \quad \text{for} \quad j = 1, \ldots, l-1 .$$

Such sequences are known as *Barker sequences*. They were invented by Barker [Bar] in connection with radar theory. Note that we cannot impose the c_j to be constant, since $c_j \equiv l - j \bmod 2$.

Barker sequences of *odd length* have been classified in 1961 by Storer and Turyn [ST]. Their lengths are bounded by 13. In the *even length* case, a longstanding conjecture states that the only such sequences are of length 2 or 4. It is known since Turyn [T2] that if the length of a Barker sequence is even and greater than 4, then it must be at least 12 100. We will show in Section 3 that this lower bound can be improved to 1 898 884, thanks to a recent result on Golay pairs and Barker sequences [EKS], and an observation in [JL].

Here is a summary of the content of this paper. In Section 0, we prove that Barker sequences of length greater than 2 are in fact *periodic* Barker sequences (i.e., (3) $\Rightarrow$ (2)), an elementary and well known fact. It is sometimes asserted in the literature that the converse holds as well. This is not true, and clarifying the situation was one of our motivations to write this survey. Another motivation was our exploration of the existence question of periodic Barker sequences for an extensive range of possible lengths. This work is summarized in Tables I and II at the end of the paper.

In Section 1, we show that binary sequences with constant periodic correlations (condition (1)) are equivalent to cyclic difference sets. We then recall the main results concerning these difference sets.

Section 2 deals with condition (2), that is, *periodic* Barker sequences. We examine the cases $\gamma = 0, 1$ and -1 separately. In the case $\gamma = 0$, it is widely believed that the only possible length is $l = 4$. We recall a theorem of Turyn stating that l must be of the form $l = 4N^2$, where N is an odd integer. Further results of Turyn imply that N must necessarily be greater than or equal to 55. In the case $\gamma = 1$, there is only one known example. The case $\gamma = -1$, in contrast, provides many interesting classical examples. In that case we make explicit the complete classification of $(4n - 1, 2n - 1, n - 1)$ cyclic difference sets up to $n = 100$. (See Sections 4 and 5, and Tables I and II.)

In Section 3, we show that there exists no aperiodic Barker sequence of length divisible by $2p$, when p is a prime number congruent to 3 mod 4.

Finally, in Section 4 and 5, we give several examples of the use of the Multiplier Theorem.

0. Preliminaries

In this section, we establish the simple relationship between periodic and aperiodic correlation coefficients, and show that every Barker sequence of length greater than 2 is also a *periodic* Barker sequence.

Lemma. *Let* $A = (a_1, \ldots, a_l)$ *be a binary sequence. Then*

$$\gamma_j(A) = c_j(A) + c_{l-j}(A)$$

for all $j = 1, \ldots, l-1$.

Proof. We have

$$\gamma_j(A) = \sum_{i=1}^{l} a_i a_{i+j} = \sum_{i=1}^{l-j} a_i a_{i+j} + \sum_{i=l-j+1}^{l} a_i a_{i+j}$$

$$= c_j(A) + \sum_{i=l-j+1}^{l} a_{i+j-l} a_i = c_j(A) + c_{l-j}(A)\,,$$

as claimed. □

For the next result, we will use, as other papers on binary sequences do, the simple observation that

$$ab \equiv a + b - 1 \bmod 4$$

for all $a, b \in \{+1, -1\}$.

Proposition 2. *Let* $A = (a_1, \ldots, a_l)$ *be a Barker sequence, with* $l \geqslant 3$. *Then* A *is also a periodic Barker sequence.*

Proof. We have to prove that $\gamma_j = \gamma_j(A)$ is independent of $j = 1, \ldots, l-1$, and equal to 0 or ± 1. First of all, we have (with $c_j = c_j(A)$)

$$c_j = \begin{cases} 0 & \text{if} \quad l-j \text{ is even} \\ \pm 1 & \text{if} \quad l-j \text{ is odd} \end{cases} \tag{1}$$

for all $j = 1, \ldots, l-1$.

This follows from the obvious congruence $c_j \equiv l - j \bmod 2$, and the fact that $c_j \in \{-1, 0, +1\}$, for all $j = 1, \ldots, l-1$.

Now, applying the relation $ab \equiv a + b - 1 \bmod 4$ for any $a, b = \pm 1$, we have

$$c_j = \sum_{i=1}^{l-j} a_i a_{i+j} \equiv \sum_{i=1}^{l-j} (a_i + a_{i+j}) - (l-j) \bmod 4 \tag{2}$$

for $j = 1, \ldots, l-1$.

Comparing the above congruences for two successive values of j, we obtain

$$c_j - c_{j+1} \equiv a_{l-j} + a_{j+1} - 1 \bmod 4\,, \tag{3}$$

for $j = 1, \ldots, l-2$.

Changing j to $l - j - 1$ leaves the right-hand-side unchanged. Therefore, we have

$$c_j - c_{j+1} \equiv c_{l-j-1} - c_{l-j} \bmod 4\,, \tag{4}$$

for $j = 1, \ldots, l-2$. Since $|c_j - c_{j+1}| \leqslant 1$ for all j by (1), we have in fact an equality:

$$c_j - c_{j+1} = c_{l-j-1} - c_{l-j}$$

for $j = 1, \ldots, l-2$. Using Lemma 1, it follows that

$$\gamma_j = \gamma_{j+1}$$

for all $j = 1, \ldots, l-2$, and thus γ_j is independent of j, as claimed.

Now $|\gamma_j| = |c_j + c_{l-j}| \leqslant 2$, and equality can occur only if $c_j = c_{l-j} = \pm 1$, which by (1) implies in particular that j must be odd. But this is impossible, because γ_j is independent of j. Therefore $|\gamma_j| \leqslant 1$, as claimed. □

1. Difference sets

In this section, we show that the notion of a binary sequence with constant periodic correlations is equivalent to that of a difference set on a cyclic group. We then recall basic results concerning these difference sets.

Definition. A *difference set D on a group G* is a subset $D \subset G$ such that the cardinality of the intersection

$$D \cap g \cdot D$$

is independent of g for $g \in G \backslash \{e\}$. Here, $gD = \{gx \mid x \in D\}$ is the translate of D by the element $g \in G$, and e is the neutral element of G.

It is traditional to denote by v the cardinality of G, by k the cardinality of D and by λ the cardinality of the intersection $D \cap gD$:

$$v = |G|, \quad k = |D|, \quad \lambda = |D \cap gD|.$$

The difference set D in G is then said to have *parameters* (v, k, λ). It is also traditional to denote by n the difference $k - \lambda$.

Observe that if $D \subset G$ is a difference set, then so is $D' = G \backslash D$. Thus we can and will always assume that $k = |D| \leqslant \frac{1}{2}v$.

Note that if $D \subset G$ is a difference set, the collection of *right translates* of D, including D itself, viz.

$$\mathscr{B} = \{Dg \mid g \in G\}$$

constitutes a *symmetric block design* on G. This means that each element of G is contained in exactly k blocks (recall $k = |D|$), and every pair of (distinct) elements of G belongs to precisely λ blocks.

Indeed, if $g \in G$, let $g_x = x^{-1}g$; then

$$g \in Dg_x \quad \text{if and only if} \quad x \in D$$

and therefore the correspondence $x \mapsto Dg_x$ provides a bijection between D and the set of blocks containing g.

If $g_1, g_2 \in G$ is a pair of distinct elements of G, set $g_x = x^{-1}g_1$. Then,

$$g_1, g_2 \in Dg_x \quad \text{if and only if} \quad x \in D \cap g_1 g_2^{-1} D$$

and the assignment $x \mapsto Dg_x$ establishes a bijection between $D \cap g_1 g_2^{-1} D$ of cardinality λ and the set of blocks Dg containing the pair g_1, g_2.

PROPOSITION. *There is a bijection between the set of binary sequences* $A = (a_1, \ldots, a_v)$ *with constant periodic correlation* γ, *i.e.*

$$\gamma = \sum_{i \bmod v} a_i \cdot a_{i+j}$$

for $j = 1, \ldots, v - 1$, *and difference sets* D *on the cyclic group* $G = \mathbf{Z}/v\mathbf{Z}$ *of order* v *with parameters* (v, k, λ), *where* $\lambda = k - (v - \gamma)/4$. *The set* D *associated to the sequence* A *is given by* $D = \{i \mid a_i = -1\}$.

Remark. In particular, if there is a binary sequence of length v with constant periodic correlation γ, then one must have $v \equiv \gamma \bmod 4$, and γ is given by

$$\gamma = v - 4n,$$

where, as above, $n = k - \lambda$.

We call $\gamma = v - 4n$ the *correlation* of the cyclic difference set D with parameters (v, k, λ).

In the proposition we must momentarily relax our convention $|D| \leqslant |G|/2$.

Proof. Let $G = \mathbf{Z}/v\mathbf{Z}$. We will represent the elements of G by $\{1, 2, \ldots, v\}$. Suppose $A = (a_1, \ldots, a_v)$ is a binary sequence and $\gamma = \sum_{i=1}^{v} a_i a_{i+j}$ is independent of j for $j = 1, \ldots, v-1$. To A we associate the subset

$$D = \{i \mid a_i = -1\} \subset G .$$

Set $k = |D|$. We claim that

$$\lambda = |D \cap (j + D)| = k - (v - \gamma)/4$$

for all $j \neq 0$. Indeed, we have

$$\gamma = \sum_{i=1}^{v} a_i a_{i+j} = |D' \cap (j + D')| + |D \cap (j + D)| - |D \cap (j + D')| - |D' \cap (j + D)|,$$

where $D' = G \setminus D$.

Now, we have

(1) $|D \cap (j + D)| + |D \cap (j + D')| = k$

(2) $|D \cap (j + D)| + |D' \cap (j + D)| = k$

(3) $|D' \cap (j + D')| + |D \cap (j + D')| = v - k$

(4) $|D' \cap (j + D')| + |D' \cap (j + D)| = v - k$

from which we conclude (by comparing (1) and (2)):

$$|D \cap (j + D')| = |D' \cap (j + D)| = k - \lambda$$

and (by substracting (3) from (1)):

$$|D \cap (j + D)| - |D' \cap (j + D')| = 2k - v .$$

Comparing this with

$$\gamma = |D \cap (j + D)| + |D' \cap (j + D')| - 2(k - \lambda) ,$$

we get the desired relation

$$2\lambda = 2k - v + \gamma + 2(k - \lambda) .$$

Conversely, if $D \subset \mathbf{Z}/v\mathbf{Z}$ is a cyclic difference set, then viewing D as a subset of $\{1, \ldots, v\}$, define $a_i = +1$ if $i \notin D$ and $a_i = -1$ if $i \in D$. The periodic correlations $\gamma = \sum_{i \bmod v} a_i a_{i+j}$ $(j = 1, \ldots, v-1)$ are independent of j and have the common value $\gamma = v - 4n$.

Equivalently, we may recast the proof as follows: write

$$D(z) = \sum_{d \in D} z^d \in \mathbf{Z}[z]/(z^v - 1)$$

if $D \subset \mathbf{Z}/v\mathbf{Z}$. We see that D is a difference set with parameters (v, k, λ) if and only if

$$D(z)D(z^{-1}) = n + \lambda T\,, \tag{1}$$

where $n = k - \lambda$ and $T = 1 + z + \cdots + z^{v-1}$. Now, $A(z) = \sum_{i=1}^{v} a_i z^{i-1}$ has constant periodic correlation γ if and only if

$$A(z)A(z^{-1}) = v + \gamma(T - 1) \quad \text{in} \quad \mathbf{Z}[z]/(z^v - 1) \tag{2}$$

If $D \subset \mathbf{Z}/v\mathbf{Z}$ is the set of exponents of the monomials z^i occurring with coefficient -1 in $A(z)$, then $A(z) = T - 2D(z)$, where $D(z) = \sum_{d \in D} z^d$ as above.

An easy calculation, using $T(z^{-1}) = T(z)$ and $z \cdot T(z) = T(z)$, shows that (2) is equivalent to

$$D(z)D(z^{-1}) = \frac{v - \gamma}{4} + \left(k - \frac{v - \gamma}{4}\right) T$$

and therefore (2) is equivalent to D being a cyclic difference set with parameters (v, k, λ), where $\lambda = k - \dfrac{v - \gamma}{4}$. □

Note that a difference set on a group G could equivalently be defined as a subset D of a $G-$set E such that

(1) $|E| = |G|$,

(2) G acts transitively on E, i.e. E affords the regular representation of G, and

(3) $\lambda = |D \cap gD|$ is independent of g for $g \in G \backslash \{1\}$.

We shall sometimes use this presentation in the sequel.

Several necessary conditions must be satisfied by a given triple (v, k, λ) to be realized as the parameters of some difference set. These well known conditions are recalled below. We refer to [L] for more details.

First of all, the triple (v, k, λ) must satisfy the equation

$$k(k - 1) = \lambda(v - 1)\,.$$

This follows easily from the definition of a symmetric block design. Next, we have:

(1) if v is even, then $n = k - \lambda$ must be a square (Schützenberger);

(2) if v is odd, the equation

$$nX^2 + (-1)^{\frac{1}{2}(v-1)} \lambda Y^2 = Z^2$$

must have a solution $(X, Y, Z) \neq (0, 0, 0)$ in integers (Chowla-Ryser) .

A deeper condition on the parameters of a difference set in an *abelian group* is provided by the following result. First we need a

Definition. A prime number p is said to be *semi-primitive* modulo the positive integer w if there is some integer f for which the equation

$$p^f \equiv -1 \mod w$$

holds. A number m is said to be *semi-primitive* modulo w if all its prime factors are. Finally, the number m is said to be *self-conjugate* modulo w, if m is semi-primitive modulo w', where w' denotes the largest divisor of w which is prime to m.

SEMI-PRIMITIVITY THEOREM. *Suppose that there exists a* (v, k, λ)-*difference set in an abelian group* G. *Let* p *be any prime divisor of* $n = k - \lambda$. *Then* p *is not semi-primitive modulo the exponent* $e(G)$ *of* G.

Furthermore, if p *divides the square-free part of* n, *then there is no divisor* $w > 1$ *of* $v = |G|$ *for which* p *is semi-primitive mod* w.

(See [L], Theorem 4.5, page 134.)

Another very useful theorem of R. Turyn is:

TURYN'S INEQUALITY. *Assume a non-trivial* (v, k, λ) *difference set in a* cyclic group *exists. Let* $m > 1$ *be an integer such that* m^2 *divides* $n = k - \lambda$ *and such that* m *is self-conjugate modulo* w *for some divisor* $w > 1$ *of* v. *If* $\gcd(m, w) = 1$ *then* $m \leqslant v/w$. *If* $\gcd(m, w) > 1$ *then*

$$m \leqslant 2^{r-1} v/w ,$$

where r *is the number of distinct prime factors of* $\gcd(m, w)$.

(See [T1]; in the special case $r = 1$, see also [Y] and [R].)

We now turn to one of the *multiplier theorems,* which sometimes describes a difference set as a union of orbits under multiplication by a certain integer. First a

Definition. Let G be a finite abelian group and D a difference set on G. The integer m is a *multiplier* for D if m is prime to $v = |G|$, and if the isomorphism $m: G \to G$ induced by multiplication by m, permutes the translates $a + D$ $(a \in G)$ of D.

Thus, m is a multiplier if $(m, v) = 1$, and if $m \cdot D = a + D$ for some $a \in G$.

We will also need the following result:

PROPOSITION. *Let m be a multiplier of a difference set D in an abelian group G. Then some translate $D' = a + D$ $(a \in G)$ of D, is fixed under multiplication by m, i.e. $m \cdot D' = D'$.*

This follows at once from a more general result, stating that an automorphism of a symmetric block design fixes as many points as blocks. (See [L], Theorem 3.1, page 78.) In our context, the multiplication by m in G fixes 0, hence it must fix at least one translate of D.

As a consequence, if an abelian difference set D admits a multiplier m, we may very well suppose that D is fixed under multiplication by m, and thus, that D is a *union of orbits under multiplication by m.*

The multiplier theorem below tells us how to find multipliers of abelian difference sets.

MULTIPLIER THEOREM. *Let D be a (v, k, λ) difference set in an abelian group G. Let n_1 be a divisor of $n = k - \lambda$ such that $n_1 > \lambda$. Suppose m is an integer satisfying*

(1) $\gcd(m, v) = 1$;

(2) *for every prime divisor p of n_1, m is a power of p modulo the exponent e of G.*

Then, m is a multiplier of the difference set D.

In Section 4, we will use this theorem to exclude the existence of periodic Barker sequences of various lengths.

2. PERIODIC BARKER SEQUENCES

This section deals with periodic Barker sequences, i.e. binary sequences whose periodic correlations γ_j are constant and equal to $\gamma \in \{0, 1, -1\}$.

Case $\gamma = 0$. In this case, the parameters (v, k, λ) and $n = k - \lambda$ of the associated cyclic difference set (see Section 1) satisfy:

$$n = N^2, \quad v = 4N^2, \quad k = 2N^2 - N, \quad \lambda = N^2 - N.$$

These follow respectively from Schützenberger's theorem for v even, the relations $v - 4n = \gamma$, $k(k-1) = \lambda(v-1)$, and our assumption $k \leqslant v/2$.

We will now prove a theorem of R. Turyn [T1], stating that N must necessarily be odd. (See also [Bau].)

THEOREM 1. *Let D be a cyclic difference set with parameters $v = 4N^2, k = 2N^2 - N$ and $\lambda = N^2 - N$. Then N is odd.*

For the proof, we will need the following two lemmas.

LEMMA 1. *Let $\eta = \eta_r$ be a primitive 2^r-th root of unity $(r > 0)$. Let $\theta \in \mathbf{Z}[\eta]$ satisfy*

$$\theta\bar{\theta} \equiv 0 \bmod (2)^{2s}, \quad (s > 0)$$

where $\bar{}$ denotes complex conjugation. Then

$$\theta \equiv 0 \bmod (2)^s.$$

Proof. In $\mathbf{Z}[\eta]$, the ideal (2) is a power of the prime ideal $P = (1 - \eta)$, and clearly $P = \bar{P}$. We have $(2) = P^k$, say.

Suppose $\theta \in P^m$ where m is maximal. Then $\theta\bar{\theta} \in P^{2m}$, and $2m$ is also maximal. But $\theta\bar{\theta} \in (2)^{2s} = P^{2sk}$, which implies $2m \geqslant 2sk$, i.e. $m \geqslant sk$, and hence $\theta \in (2)^s$, as claimed. □

On the level of group rings, there is a similar result, albeit necessarily weaker. For $i > 0$, we will use the following notation:

(1) η_i is a primitive 2^i-th root of unity;

(2) Γ_i is the multiplicative cyclic group of order 2^i with generator x_i;

(3) $\rho: \mathbf{Z}\Gamma_i \to \mathbf{Z}[\eta_i]$ is the map induced by $\rho(x_i) = \eta_i$;

(4) $\nu_j: \mathbf{Z}\Gamma_i \to \mathbf{Z}\Gamma_{i-j}$ is the map induced by $\nu_j(x_i) = x_{i-j}$ $(j < i)$.

LEMMA 2. *Let $\theta \in \mathbf{Z}[\eta_r]$ $(r > 0)$ satisfy*

$$\theta\bar{\theta} \equiv 0 \bmod (2)^{2s}, \quad (0 < s \leqslant r)$$

and let $\alpha \in \mathbf{Z}\Gamma_r$ be any element such that $\rho(\alpha) = \theta$. Then

$$\nu_s(\alpha) \equiv 0 \bmod (2)^s$$

in $\mathbf{Z}\Gamma_{r-s}$.

Proof. By induction on s.

(1) Case $s = 1$. Let us write α as

$$\alpha = \sum_{i=0}^{2^r-1} \alpha_i x_r^i .$$

Then

$$\theta = \rho(\alpha) = \sum_{i=0}^{2^{r-1}-1} (\alpha_i - \alpha_{i+2^{r-1}})\eta_r^i ,$$

since $\eta_r^{2^{r-1}} = -1$. Furthermore, the powers η_r^k with $0 \leqslant k \leqslant 2^{r-1} - 1$ form a $\mathbf{Z}$-basis of $\mathbf{Z}[\eta_r]$. By Lemma 1, we have $\theta \equiv 0 \bmod (2)$, and therefore

$$(*) \qquad \alpha_i \equiv \alpha_{i+2^{r-1}} \mod (2)$$

for all $i = 0, \ldots, 2^{r-1} - 1$.

On the other hand,

$$\nu_1(\alpha) = \sum_{i=0}^{2^{r-1}-1} (\alpha_i + \alpha_{i+2^{r-1}})x_{r-1}^i ,$$

and (*) implies that $\nu_1(\alpha) \equiv 0 \bmod (2)$ in $\mathbf{Z}\Gamma_{r-1}$, as claimed.

(2) Case $s > 1$. By (1) above, we have $\nu_1(\alpha) \equiv 0 \bmod (2)$ in $\mathbf{Z}\Gamma_{r-1}$. Thus we have $\nu_1(\alpha) = 2\beta$ in $\mathbf{Z}\Gamma_{r-1}$. Now $\rho(\beta) = \frac{1}{2}\rho(\alpha)$, so that

$$\rho(\beta)\overline{\rho(\beta)} \equiv 0 \mod (2)^{2(s-1)}$$

in $\mathbf{Z}[\eta_{r-1}]$. By the induction hypothesis, we have $\nu_{s-1}(\beta) \equiv 0 \bmod (2)^{s-1}$ in $\mathbf{Z}\Gamma_{r-s}$, and therefore $\nu_s(\alpha) \equiv 0 \bmod (2)^s$ in $\mathbf{Z}\Gamma_{r-s}$. □

Proof of the Theorem. Let $D \subset \mathbf{Z}/v\mathbf{Z} = C_v$ denote a difference set with parameters $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$. Identifying $\mathbf{Z}C_v$ with $\mathbf{Z}[x]/(x^v - 1)$, we will denote by $\theta(x)$ the element $\theta(x) = \sum_{d \in D} x^d \in \mathbf{Z}C_v$. We have by hypothesis,

$$(1) \qquad \theta(x)\theta(x^{-1}) = N^2 + \lambda(1 + x + \cdots + x^{v-1}) .$$

Given any element z in some ring A, we will denote by $\theta(z)$ the image of $\theta(x)$ under the map $\phi: \mathbf{Z}C_v \to A$ induced by $x \mapsto z$.

Let us write $N = 2^t N_1$ with N_1 odd. Thus, $w = 2^{2t+2}$ is the highest power of 2 dividing $v = 4N^2$. Let Γ_i denote, as above, the cyclic group of order 2^i with generator x_i.

If η is a primitive 2^{2t+2}-th root of unity, we have $\theta(\eta) \cdot \overline{\theta(\eta)} = N^2 \equiv 0 \mod (2)^{2t}$. Hence, Lemma 2 implies $\theta(x_{t+2}) \equiv 0 \mod (2)^t$ in $\mathbf{Z}\Gamma_{t+2}$. Denoting x_{t+2} by y, we thus have

$$\theta(y) = 2^t \theta_1(y) ,$$

for some $\theta_1(y) \in \mathbf{Z}\Gamma_{t+2}$.

Now, a direct computation yields

$$\theta_1(y)\overline{\theta_1(y)} = N_1^2 + N_1^3(N-1)\,(1 + y + \cdots + y^{2^{t+2}-1}) ,$$

so that the constant term (i.e., the coefficient of $1 = y^0$) of $\theta_1(y)\overline{\theta_1(y)}$ is equal to $N_1^2 + N_1^3(N-1)$. On the other hand, write $\theta_1(y)$ as

$$\theta_1(y) = \sum_{i=0}^{2^{t+2}-1} d_i y^i$$

in $\mathbf{Z}\Gamma_{t+2}$. In this notation, the constant term of $\theta_1(y)\overline{\theta_1(y)}$ is equal to $\sum d_i^2$, so that

$$N_1^2 + N_1^3(N-1) = \sum d_i^2 .$$

Now, $\sum d_i^2 \equiv (\sum d_i)^2 \mod 2$, and

$$(\sum d_i)^2 = \theta_1(1)^2 = N_1^2 + N_1^3(N-1)2^{t+2} .$$

Thus,

$$N_1^2 + N_1^3(N-1) \equiv N_1^2 + N_1^3(N-1)2^{t+2} \mod 2 ,$$

which implies $N \equiv 1 \mod 2$, as claimed. □

Another very strong restriction on the parameter N is provided by the following easy consequence of Turyn's Inequality, Section 1.

THEOREM 2. *Let N be an odd integer. If N has a prime factor p which is self-conjugate modulo N, then there is no periodic Barker sequence of length $l = 4N^2$.*

Recall that, by definition, p is self-conjugate modulo N if and only if there is a positive integer f such that $p^f \equiv -1 \mod N'$, where N' is the largest divisor of N which is relatively prime to p.

Proof. In the notation of Turyn's Inequality, take $v = 4N^2$ of course, $m = p$, and $w = v/2 = 2N^2$. Thus $v/w = 2$ and r, the number of distinct prime factors of $\gcd(m, w) = p$ is equal to 1 here.

Let now N' denote the largest divisor of N which is relatively prime to p. By hypothesis, there is a positive integer f such that $p^f \equiv -1 \bmod N'$. Since N' and p are odd, we also have $p^{N'f} \equiv -1 \bmod 2N'^2$. Therefore p is self-conjugate modulo $2N^2 = w$, because $2N'^2$ is the largest divisor of $2N^2$ which is relatively prime to p. If a periodic Barker sequence of length $4N^2$ existed, Turyn's Inequality would then imply

$$p = m \leqslant 2^{r-1}v/w = 2 ,$$

contrary to the fact that p divides N. □

An immediate corollary is that N cannot be a prime or a prime power. R. Turyn used his inequality to show that there exists no periodic Barker sequence of length $l = 4N^2$ with $1 < N < 55$. (The case $N = 39$ required a special argument.) See [T2].

As an example, suppose that $N = p^\lambda \cdot q^\mu$, where both p, q are prime and $\equiv 3 \bmod 4$. The hypothesis of Theorem 2 is then satisfied, i.e. either p or q is self-conjugate modulo N.

This follows from quadratic reciprocity, which implies that either $p^{\frac{q-1}{2}} \equiv -1 \bmod q$, or $q^{\frac{p-1}{2}} \equiv -1 \bmod p$.

More generally, suppose that $N = p^\lambda \cdot q^\mu \cdot N_1$, where p, q are as above, and where N_1 is coprime to p, q, and satisfies furthermore $N_1^2 < \min(p, q)$. Then there are no periodic Barker sequences of length $4N^2$. This follows from Turyn's Inequality, by choosing $w = 4p^{2\lambda}q^{2\mu}$, and $m = p$ or q, according as to wether p is self-conjugate modulo q, or q is self-conjugate modulo p.

(As observed by J. Jedwab, it even suffices to have $N_1^2 < \min(p^\lambda, q^\mu)$, taking $m = p^\lambda$ or q^μ, as the case may be.)

Case $\gamma = 1$. In this case, the parameters (v, k, λ) and $n = k - \lambda$ satisfy

$$\begin{aligned} v &= 2t(t+1) + 1 \\ k &= t^2 \\ \lambda &= \frac{1}{2}t(t-1) \\ \text{and} \quad n &= \frac{1}{2}t(t+1) , \end{aligned}$$

for some positive integer t. Indeed, $v = 4n + 1$ (since $v - \gamma = 4n$ for a periodic Barker sequence with correlation γ), and the symmetric block design relation $k(k-1) = \lambda(v-1)$ yields $k = (k - 2\lambda)^2$. Setting $t = k - 2\lambda$, we find the parametrization above. Since the parameter values are the same for $-t$ and $t-1$, we may assume $t \geqslant 1$. (Recall also our convention $k \leqslant \frac{1}{2}v$.) Observe that the Chowla-Ryser condition is here always satisfied: the triple $X = 1$, $Y = 1$ and $Z = t$ is a nontrivial integral solution to the equation $nX^2 + (-1)^{\frac{1}{2}(v-1)}\lambda Y^2 = Z^2$. The case $t = 1$ is trivial: $\lambda = 0$. It does however correspond to the Barker sequence $1, 1, 1, -1, 1$. For $t = 2$, we have the parameter values $(13, 4, 1)$ and the essentially unique cyclic difference set

$$D = \{0, 1, 3, 9\} .$$

More geometrically, we can describe this difference set using the projective plane $\mathbf{P}^2(\mathbf{F}_3)$ over the field $\mathbf{F}_3$ with 3 elements which possesses an automorphism, the Singer automorphism of order 13. Viewing $E = \mathbf{P}^2(\mathbf{F}_3)$ as a G-set with G cyclic of order 13, the difference set $D \subset E$ is then given by any line $\mathbf{P}^1(\mathbf{F}_3) \subset \mathbf{P}^2(\mathbf{F}_3)$. The Singer automorphism is best described by taking the orbits of the $\mathbf{F}_3^*$-action on $\mathbf{F}_{27}$. The map $S: \mathbf{P}^2(\mathbf{F}_3) \to \mathbf{P}^2(\mathbf{F}_3)$ then corresponds to the multiplication by a generator α of the cyclic group $\mathbf{F}_{27}^*$. (See [L], page 125.)

We will prove that there is no other cyclic difference set with parameters $\left(2t(t+1), t^2, \frac{1}{2}t(t-1)\right)$ for $t \leqslant 100$, except perhaps for $t = 50$, where the existence of a cyclic difference set with parameters $(5101, 2500, 1225)$ still remains unsettled. We only know that 191 is a multiplier if such a difference set exists.

These non-existence claims are obtained by using the semi-primitivity and multiplier theorems of Section 1. Table I at the end of the paper indicates in each case which of these two results was used. When relevant, the semi-primitivity theorem is very easy to use. In our case, where the parameters are of the form $(v, k, \lambda) = \left(2t(t+1) + 1, t^2, \frac{1}{2}t(t-1)\right)$, there is one further simplification; the semi-primitivity theorem implies the non-existence of a cyclic difference set with n even, in the following two instances:

(1) $v = 2t(t+1) + 1$ is a prime power

(2) $n = k - \lambda = \frac{1}{2}t(t-1)$ is square-free.

(Unfortunately, this simplified criterion does not apply for n odd.) Indeed, since $v = 4n + 1$, we have

$$4n \equiv -1 \mod v ,$$

so that one of the primes dividing $4n$ must be of even order in the group of units $(\mathbf{Z}/v\mathbf{Z})^*$.

If n is even, then $4n$ and n are divisible by the same primes and one of the primes dividing n must be of even order modulo v. Let p, say, be a prime divisor of n and let $2f$ be its order in $(\mathbf{Z}/v\mathbf{Z})^*$.

If v is a prime power, the group $(\mathbf{Z}/v\mathbf{Z})^*$ is cyclic (yes, v is odd) and $p^f \equiv -1 \mod v$. The semi-primitivity theorem applies. If v is not a prime power, there is a prime power divisor w of v such that p is of even order, $2f'$ say, in $(\mathbf{Z}/w\mathbf{Z})^*$. Again, $(\mathbf{Z}/w\mathbf{Z})^*$ being cyclic, this implies $p^{f'} \equiv -1 \mod w$, and the semi-primitivity theorem applies. In the range $3 \leqslant t \leqslant 100$, the semi-primitivity theorem takes care of all the cases, except the values $t = 9, 49, 50$ and 82. (See Table I.)

In contrast, applying the multiplier theorem may require quite lengthy computations on the structure of multiplier orbits. The cases $t = 9$, $t = 82$ (easy) and $t = 49$ (harder) are treated in Section 4 using the multiplier theorem.

Case $\gamma = -1$. The symmetric block design equation $k(k-1) = \lambda(v-1)$ in this case yields the parameter values $(v, k, \lambda) = (4n-1, 2n-1, n-1)$, where $n = k - \lambda$ as usual. Recall that we are assuming $k \leqslant \frac{1}{2}v$, without loss of generality.

Again the Chowla-Ryser equation $nX^2 + (-1)^{\frac{1}{2}(v-1)}\lambda Y^2 = Z^2$ is non-trivially solvable in integers: $X = 1$, $Y = 1$, $Z = 1$.

However, here the situation is quite different from the one in case $\gamma = 1$. There are well known families of cyclic difference sets with parameters of the form $(4n-1, 2n-1, n-1)$.

(1) *Quadratic residues.*

Suppose $v = 4n - 1 = p$ is a prime. Let $D \subset \mathbf{Z}/p\mathbf{Z}$ be the set of non-zero quadratic residues mod p. Then,

$$k = |D| = \frac{1}{2}(p-1) = 2n - 1$$

and D is a difference set with $\lambda = (p-3)/4 = n - 1$. We shall denote this difference set by $QR(p)$.

(2) *Projective spaces.*

Let $E = \mathbf{P}^d(\mathbf{F}_2)$ be the projective d-space over the field with two elements $\mathbf{F}_2$. Of course, $|E| = 2^{d+1} - 1$. The hyperplanes in E form a symmetric block design with parameters

$$(2^{d+1} - 1, 2^d - 1, 2^{d-1} - 1) .$$

The Singer automorphism exhibits this design as a cyclic design on the cyclic group of order $v = 2^{d+1} - 1$. We use $\mathbf{P}^d(\mathbf{F}_2)$ as a notation for this cyclic difference set.

(3) *Gordon-Mills-Welch difference sets.*

Other difference sets with the same parameters as projective spaces have been discovered by B. Gordon, W. H. Mills and L. R. Welch. (See [GMW].) They appear in Table II under the label *GMW*. We give some details of their construction in Section 5.

(4) *Twin primes cyclic difference sets.*

If p and q are twin primes, $q = p + 2$, there is a difference set on $\mathbf{Z}/pq\mathbf{Z} = \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$ with parameters $\left(pq, \frac{1}{2}(pq-1), \frac{1}{4}(pq-3)\right)$ and which we shall denote by $TP(p, q)$.

The set $D \subset \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$ is defined by

$$D = (\mathbf{Z}/p\mathbf{Z} \times \{0\}) \cup (S_p \times S_q) \cup (N_p \times N_q) ,$$

where S_p and N_p denote the (non-zero) squares and non-squares mod p respectively, and similarly for S_q and N_q.

(5) *Marshall Hall cyclic difference sets.*

If v is a prime number of the form $v = 4x^2 + 27$ where x is an integer, there is a cyclic difference set with parameters $\left(v, \frac{v-1}{2}, \frac{v-3}{4}\right)$ [H], page 170. We will denote this difference set by $MH(v)$. In Table II, they occur for the values $n = 56$ and $n = 71$ of the parameter n.

In Table II, we settle the existence question for a cyclic difference set with parameters $(4n - 1, 2n - 1, n - 1)$ for $n = 2, \ldots, 100$.

It turns out that the cyclic difference sets with parameters (7, 3, 1) provided by $\mathbf{P}^2(\mathbf{F}_2)$ and $QR(7)$ are isomorphic. In the two other cases of Table II where $4n - 1$ is a prime p of the form $p = 2^d - 1$ (that is, $n = 8$ and 32), $\mathbf{P}^{d-1}(\mathbf{F}_2)$ and $QR(p)$ are non-isomorphic difference sets. (According to [BF], there actually are 6 distinct examples for $n = 32$.)

In the fourth column of Table II, we have indicated the known existing cyclic difference sets or the relevant prime power exhibiting non-existence by the semi-primitivity theorem of Section 1. The values of the parameter n left out by these two classes are $n = 7, 25, 28, 37, 43, 44, 49, 52, 61, 67, 72, 75, 76, 86, 97, 99$ and 100. We have reached a non-existence conclusion in these cases by using the multiplier theorem of Section 1. The required calculations being quite lengthy, it is impossible to expose them all. Instead, Section 4 contains some typical examples of application of this theorem.

3. Barker sequences

Recall that a Barker sequence is a binary sequence $A = (a_1, \ldots, a_l)$ such that the aperiodic correlations $c_j(A) = \sum_{i=1}^{l-j} a_i a_{i+j}$ belong to $\{-1, 0, 1\}$ for all $j = 1, \ldots, l-1$.

The set of Barker sequences of a given length is preserved by the following transformations:

$$A \mapsto \alpha A, \text{ where } (\alpha A)_i = -a_i$$

$$A \mapsto \beta A, \text{ where } (\beta A)_i = (-1)^i a_i$$

$$A \mapsto \gamma A, \text{ where } (\gamma A)_i = a_{l-i+1},$$

with $l = \text{length}(A)$.

The group of transformations of Barker sequences generated by α, β and γ is the elementary abelian 2-group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ of rank 3 if l is odd, and is the non-abelian dihedral 2-group of order 8 with presentation

$$D_8 = <\alpha, \beta, \gamma: \alpha^2 = \beta^2 = \gamma^2 = 1, \alpha\beta = \beta\alpha, \alpha\gamma = \gamma\alpha, \gamma\beta\gamma = \alpha\beta>$$

for l even. Note that in this case, D_8 is also generated by $\rho = \beta\gamma$ and γ with presentation

$$D_8 = <\rho, \gamma: \rho^4 = \gamma^2 = 1, \gamma\rho\gamma = \rho^{-1}> .$$

Case of odd length. The complete list of Barker sequences of odd length was established by R. Turyn and J. Storer, [ST] and reads as follows (in lengths $\geqslant 3$):

$$(1, 1, -1)$$

$$(1, 1, 1, -1, 1)$$

$$(1, 1, 1, -1, -1, 1, -1)$$

$$(1, 1, 1, -1, -1, -1, 1, -1, -1, 1, -1)$$

$$(1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1) .$$

The list is complete up to the transformations α, β and γ given above. The orbit of each Barker sequence in the above Turyn-Storer list under this transformation group consists of 4 sequences.

Case of even length. The situation here is completely different. The only known examples are

$$(1, 1) \quad \text{and} \quad (1, 1, 1, -1) ,$$

again up to modifications by the above transformations α, β and γ. Note that the sequence $(1, 1, 1, -1)$ gives rise to 8 sequences under this transformation group.

It is widely believed that these are the only Barker sequences of even length. We will show that this is true up to length 1 898 884.

We know from Section 1 that a Barker sequence of even length ($\geqslant 4$) is also a periodic Barker sequence with correlation $\gamma = 0$, and we know from Section 2 that the length l must be of the form $l = 4N^2$ with N odd, if $l \geqslant 4$. We also know from Section 2 that if N is an odd integer with a prime factor p such that p is self-conjugate modulo N, then there is no (periodic) Barker sequence of length $4N^2$. In other words, N is excluded if, for p as above, there is some positive integer f such that $p^f \equiv -1 \bmod N'$, where N' is the largest divisor of N which is relatively prime to p. An immediate consequence is that N cannot be a prime or a prime power. R. Turyn used the above theorem to show that, if there exists a (periodic) Barker sequence of length $l = 4N^2$ with $N > 1$, then necessarily $N \geqslant 55$. With the following result of [EKS], this bound can be improved to $N \geqslant 689$, but only for true (i.e. aperiodic) Barker sequences.

THEOREM. *Let l be an even integer having a prime factor $p \equiv 3 \bmod 4$. Then there is no Barker sequence of length l.*

For the proof, we will need the following

LEMMA. *Let $f(z), g(z) \in \mathbf{F}_p[z, z^{-1}]$ be non-zero elements satisfying*

$$f(z) f(z^{-1}) + g(z) g(z^{-1}) = 0 .$$

Then either $p = 2$ or $p \equiv 1 \bmod 4$.

Proof. Since $\mathbf{F}_p[z, z^{-1}]$ is a unique factorization domain, we may suppose that $f(z)$, $g(z)$ are coprime, by clearing any common factor. But then, the equation implies that $f(z)$ divides $g(z^{-1})$. We may thus write

$$g(z^{-1}) = h(z) f(z) , \quad g(z) = h(z^{-1}) f(z^{-1})$$

for some $h(z) \in \mathbf{F}_p[z, z^{-1}]$. Substituting these expressions for $g(z)$ and $g(z^{-1})$ and clearing the common factor $f(z)f(z^{-1})$ in the resulting equation, we obtain

$$1 + h(z)h(z^{-1}) = 0 .$$

Letting $z = 1$, this gives $-1 = h(1)^2$ in $\mathbf{F}_p$, and therefore p is not congruent to 3 mod 4. □

Proof of the Theorem. Let $A = (a_1, \ldots, a_l)$ be a Barker sequence of even length l, and consider the two polynomials

$$F(z) = \sum_{i=1}^{l} a_i z^{i-1} \quad \text{and} \quad G(z) = F(-z) = \sum_{i=1}^{l} (-1)^{i-1} a_i z^{i-1} .$$

CLAIM: *Then,* (F, G) *is a Golay pair, i.e.*

$$F(z)F(z^{-1}) + G(z)G(z^{-1}) = 2l \quad \text{in } \mathbf{Z}[z, z^{-1}] .$$

Indeed, the constant term of $F(z)F(z^{-1}) + G(z)G(z^{-1})$ is equal to $2\sum a_i^2 = 2l$. On the other hand, for $j > 0$, the coefficient of $z^j + z^{-j}$ in $F(z)F(z^{-1}) + G(z)G(z^{-1})$ is equal to

$$\sum_{i=1}^{l-j} (a_i a_{i+j} + (-1)^j a_i a_{i+j}) ,$$

which is zero if j is odd, and is equal to $2c_j(A)$ if j is even. But $c_j(A) = 0$ if j is even and positive, since $c_j(A)$ belongs to $\{-1, 0, 1\}$ by hypothesis, and $c_j \equiv j \bmod 2$. Therefore, $F(z)F(z^{-1}) + G(z)G(z^{-1}) = 2l$ in $\mathbf{Z}[z, z^{-1}]$, as claimed.

Reducing the above equation modulo p, we obtain two non-zero elements $f(z), g(z)$ in $\mathbf{F}_p[z, z^{-1}]$ satisfying

$$f(z)f(z^{-1}) + g(z)g(z^{-1}) = 0 .$$

By the lemma above, we conclude that p cannot be congruent to 3 mod 4. □

APPLICATION. *There is no Barker sequence of length* $l = 4N^2$, *if* $1 < N < 689$. *In particular, there is no Barker sequence of even length greater than* 4 *and less than 1 898 884.*

Of course, it suffices to consider only those $N < 689$ which are odd, are not a prime or a prime power, and have no factor congruent to 3 mod 4. Since the square root of 689 is smaller than 26, every such N must have a prime factor equal to 5, 13 or 17.

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

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

$$U_i = \{(13i, 0), (-13i, 0)\} \quad i = 1, 2, 3, 4, 5, 6$$

$$V_j = \{(j,0), (25j,0), (118j,0), (77j,0), (66j,0), (129j,0), (14j,0), (12j,0), (131j,0), (64j,0), (79j,0), (116j,0), (27j,0), (-j,0), \ldots\}$$
$$j = 1, \ldots, 6, \text{ each } V_j \text{ of cardinality } 26.$$

$$X = \{(0,1), (0,25), (0,16), (0,23), (0,24), (0,20), (0,7)\}$$

$$Y = \{(0,2), (0,21), (0,3), (0,17), (0,19), (0,11), (0,14)\}$$

$$\bar{X} = \{(0, -x) \mid (0,x) \in X\}$$

$$\bar{Y} = \{(0, -y) \mid (0,y) \in Y\}$$

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

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

and

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

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 $p \equiv 3 \bmod 4$ implies $z \equiv 2 \bmod 4$, 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}. □

(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 $4 = 2^2 \equiv 5^8 \bmod 399$, 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 $k = 199 \equiv 1 \bmod 3$, 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

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

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

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

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

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.

The case $n = 36$, also leads by machine enumeration to the single difference set $TP(11, 13)$ of twin-prime type with parameters $(143 = 11 \cdot 13, 71, 35)$.

The only other values of $n(\leqslant 100)$ for which $v = 4n - 1$ is *not* a prime and a Hadamard cyclic difference set with parameters $(4n - 1, 2n - 1, n - 1)$ does exist are powers of 2. The examples for $n = 2, 4$ and 8 are easily seen to be unique.

For $n = 16$, there are 2 isomorphism classes of Hadamard difference sets with parameters $(63, 31, 15)$: Both have multiplier $m = 2$, and denoting by X_a the orbit of a under multiplication by 2 in $\mathbf{Z}/63\mathbf{Z}$, they are

$$D_0 = 1 + X_{-25} + X_{-9} + X_1 + X_3 + X_7 + X_9 ,$$

which is isomorphic to $\mathbf{P}^5(\mathbf{F}_2)$, and

$$D_1 = 1 + X_{-9} + X_{-1} + X_1 + X_3 + X_9 + X_{25} ,$$

which is of type *GMW*.

The difference sets D_0 and D_1 are not isomorphic, even as block designs, as can be seen by computing the cardinalities of the intersection of triples of blocks of D_1, giving the enumerating polynomial

$$10584t^6 + 19656t^7 + 3528t^8 + 5880t^9 + 63t^{15} ,$$

in contrast to $39060t^7 + 651t^{15}$ for $\mathbf{P}^5(\mathbf{F}_2)$. (The coefficient of t^i being the multiplicity of triple intersections of cardinality i.)

For $n = 32$, L. Baumert and H. Fredricksen have found that there are exactly 6 non-isomorphic examples. (See [BF].) Three of these, $QR(127)$, $\mathbf{P}^6(\mathbf{F}_2)$ and $MH(127)$ are members of the classical families.

For $n = 64$, we have found that there exist exactly 4 examples (up to isomorphism). One of them is $\mathbf{P}^7(\mathbf{F}_2)$, another one is of type *GMW*. The other two seem to be new.

All 4 of them have multiplier 2, which is of order 8 modulo $v = 255$. They all contain the union U of the multiplier orbits of length < 8, viz.

$$U = \{0\} + \{85, -85\} + \{51, 102, -51, -102\} + \{17, 34, 68, -119\} + \{-17, -34, -68, 119\} .$$

Denoting by $(a_1, \ldots, a_{14})$ the union $\sum_{i=1}^{14} X_{a_i}$ of the orbits

$$X_a = \{a, 2a, \ldots, 2^7 a\} ,$$

the 4 examples are of the form $D_i = U + V_i$, where

$V_0 = (-19, -9, -7, -1, 1, 3, 7, 13, 19, 23, 25, 27, 37, 45)$,

$V_1 = (-43, -27, -25, -13, -9, -5, -3, 7, 11, 13, 19, 23, 27, 43)$,

$V_2 = (-43, -27, -23, -13, -11, -3, 1, 3, 7, 13, 15, 25, 37, 43)$,

$V_3 = (-43, -23, -21, -11, -7, -3, 7, 9, 11, 15, 19, 25, 37, 43)$.

The difference sets D_2 and D_3 appear to be exotic. D_0 is isomorphic to $\mathbf{P}^7(\mathbf{F}_2)$. Finally, D_1 is of type *GMW,* and can be constructed as follows.

Let $L = \mathbf{F}_{256}$ be the extension of degree 8 over $F = \mathbf{F}_2$. We will use the trace $Tr = Tr_{L/F}: L \to F$ given by $Tr(\gamma) = \sum_{i=0}^{7} \gamma^{2^i}$. The extension L/F is defined by the irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1 \in \mathbf{F}[x]$. The multiplicative group $\mathbf{F}_{256}^*$ is generated by any root α of this polynomial. The Hall polynomial $D_0(x)$ of D_0 is then given by

$$D_0(x) = \sum_{i=0}^{254} d_i x^i \in \mathbf{Z}[x]/(x^{255} - 1) ,$$

where

$$d_i = \begin{cases} 0 & \text{if } Tr(\alpha^i) \neq 0 \\ 1 & \text{if } Tr(\alpha^i) = 0 . \end{cases}$$

Thus a block of the difference set is the hyperplane $\ker(Tr) \subset \mathbf{F}_{256} = \mathbf{F}_2^8$.

Under the identification

$$\mathbf{Z}/255\mathbf{Z} \to \mathbf{F}_{256}^*$$

given by $i \mapsto \alpha^i$, the multiplication by 2 in $\mathbf{Z}/255\mathbf{Z}$ becomes the Frobenius automorphism in the extension $\mathbf{F}_{256}/\mathbf{F}_2$. The block $\ker(Tr)$ is a union of orbits under the action of the multiplier.

In order to construct D_1, the example of type *GMW*, we need the intermediate extension $K = \mathbf{F}_{16}$, $F \subset K \subset L$. Set $\beta = \alpha^{17}$, a generator of $K^* = \mathbf{F}_{16}^*$. Denote by $tr = tr_{K/F}: K \to F$ the trace.

Consider the complementary polynomial $D_0'(x) = T - D_0(x)$, where $T = \sum_{i=0}^{254} x^i \in \mathbf{Z}[x]/(x^{255} - 1)$. The crucial point is to observe that $D_0'(x)$ splits as

$$D_0'(x) = \Omega(x) \cdot \theta_0(x^{17}) \in \mathbf{Z}[x]/(x^{255} - 1) ,$$

where $\theta_0(y) = \sum_{j=0}^{14} a_j y^j$ with

$$a_j = \begin{cases} 0 & \text{if } tr(\beta^j) = 0 \\ 1 & \text{if } tr(\beta^j) \neq 0 , \end{cases}$$

and $\Omega(x) = x^7 + x^{14} + \cdots + x^{246}$. Here,

$$\theta_0(y) = y + y^2 + y^3 + y^4 + y^6 + y^8 + y^9 + y^{12} .$$

Now define

$$D_1'(x) = \Omega(x) \cdot \theta_1(x^{17}) ,$$

where $\theta_1(y) = \theta_0(y^{-1})$. Then $D_1(x) = T - D_1'(x)$ is the Hall polynomial of the difference set D_1.

The fact that D_0, D_1, D_2 and D_3 are not isomorphic, even as block designs, can again be seen by determining the cardinalities of all triple intersections of blocks, for each D_i. Denoting by P_i the corresponding enumerating polynomial of triple intersections for D_i, we have

$$P_0 = 2720340t^{31} + 10795t^{63}$$

$$P_1 = 979200t^{29} + 823140t^{31} + 734400t^{33} + 183600t^{35} + 10200t^{39} + 595t^{63}$$

$$P_2 = 9180t^{25} + 8160t^{26} + 45900t^{27} + 163200t^{28} + 342720t^{29} + 514080t^{30} + 518160t^{31} + 465120t^{32} + 358020t^{33} + 179520t^{34} + 81090t^{35} + 18360t^{36} + 18360t^{37} + 6120t^{38} + 3145t^{39}$$

$$P_3 = 4080t^{25} + 14280t^{26} + 40800t^{27} + 142800t^{28} + 385560t^{29} + 403920t^{30} + 692580t^{31} + 424320t^{32} + 352920t^{33} + 128520t^{34} + 79050t^{35} + 32640t^{36} + 9180t^{37} + 12240t^{38} + 7225t^{39} + 1020t^{45} .$$

TABLE I

Case $\gamma = +1$:
Non-existence of a cyclic difference set with parameters $(2t(t+1)+1, t^2, \frac{1}{2}t(t-1))$ *for* $3 \leqslant t \leqslant 100$.
(The case $t = 50$ is still undecided.)

t	(v, k, λ)	$n = k - \lambda$	reason for non-existence
3	$(5^2, 9, 3)$	$2 \cdot 3$	$2^2 \equiv -1 \bmod 5$
4	(41, 16, 6)	$2 \cdot 5$	$5^{10} \equiv -1 \bmod 41$
5	(61, 25, 10)	$3 \cdot 5$	$3^5 \equiv -1 \bmod 61$
6	$(5 \cdot 17, 36, 15)$	$3 \cdot 7$	$3^2 \equiv -1 \bmod 5$
7	(113, 49, 21)	$2^2 \cdot 7$	$7^7 \equiv -1 \bmod 113$
8	$(5 \cdot 29, 64, 28)$	$2^2 \cdot 3^2$	$2^{14} \equiv -1 \bmod 145$
9	(181, 81, 36)	$3^2 \cdot 5$	$5 \equiv 3^6 \bmod 181$ would be multiplier
10	$(13 \cdot 17, 100, 45)$	$5 \cdot 11$	$5^2 \equiv -1 \bmod 13$
11	$(5 \cdot 53, 121, 55)$	$2 \cdot 3 \cdot 11$	$2^2 \equiv -1 \bmod 5$
12	$(3 \cdot 13, 144, 66)$	$2 \cdot 3 \cdot 13$	$2^{78} \equiv -1 \bmod 313$
13	$(5 \cdot 73, 169, 78)$	$7 \cdot 13$	$7^2 \equiv -1 \bmod 5$
14	(421, 196, 91)	$3 \cdot 5 \cdot 7$	$5^{105} \equiv -1 \bmod 421$

TABLE I *(continued)*

t	(v, k, λ)	$n = k - \lambda$	reason for non-existence
15	$(13 \cdot 37, 225, 105)$	$2^3 \cdot 3 \cdot 5$	$5^2 \equiv -1 \bmod 13$
16	$(5 \cdot 109, 256, 120)$	$2^3 \cdot 17$	$17^2 \equiv -1 \bmod 5$
17	(613, 289,136)	$3^2 \cdot 17$	$17^{51} \equiv -1 \bmod 613$
18	$(5 \cdot 137, 324, 153)$	$3^2 \cdot 19$	$19 \equiv -1 \bmod 5$
19	(761, 361, 171)	$2 \cdot 5 \cdot 19$	$2^{190} \equiv -1 \bmod 761$
20	$(29^2, 400, 190)$	$2 \cdot 3 \cdot 5 \cdot 7$	$2^{14} \equiv -1 \bmod 29$
21	$(5^2 \cdot 37, 441, 210)$	$3 \cdot 7 \cdot 11$	$3^2 \equiv -1 \bmod 5$
22	(1013, 484, 231)	$11 \cdot 23$	$11^{23} \equiv -1 \bmod 1013$
23	$(5 \cdot 13 \cdot 17, 529, 253)$	$2^2 \cdot 3 \cdot 23$	$3^2 \equiv -1 \bmod 5$
24	(1201, 576, 276)	$2^2 \cdot 3 \cdot 5^2$	$3^{150} \equiv -1 \bmod 1201$
25	(1301, 625, 300)	$5^2 \cdot 13$	$5^{325} \equiv -1 \bmod 1301$
26	$(5 \cdot 281, 676, 325)$	$3^3 \cdot 13$	$13^2 \equiv -1 \bmod 5$
27	$(17 \cdot 89, 729, 351)$	$2 \cdot 3^3 \cdot 7$	$2^4 \equiv -1 \bmod 17$
28	$(5^3 \cdot 13, 784, 378)$	$2 \cdot 7 \cdot 9$	$2^2 \equiv -1 \bmod 5$
29	(1741, 841, 406)	$3 \cdot 5 \cdot 29$	$3^{435} \equiv -1 \bmod 1741$
30	(1861, 900, 435)	$3 \cdot 5 \cdot 31$	$3^{155} \equiv -1 \bmod 1861$
31	$(5 \cdot 397, 961, 465)$	$2^4 \cdot 31$	$2^{22} \equiv -1 \bmod 1985$
32	(2113, 1024, 496)	$2^4 \cdot 3 \cdot 11$	$3^{528} \equiv -1 \bmod 2113$
33	$(5 \cdot 449, 1089, 528)$	$3 \cdot 11 \cdot 17$	$3^2 \equiv -1 \bmod 5$
34	(2381, 1156, 561)	$5 \cdot 7 \cdot 17$	$5^{119} \equiv -1 \bmod 2381$
35	(2521, 1225, 595)	$2 \cdot 3^2 \cdot 5 \cdot 7$	$2^{630} \equiv -1 \bmod 2521$
36	$(5 \cdot 13 \cdot 41, 1296, 630)$	$2 \cdot 3^2 \cdot 37$	$2^2 \equiv -1 \bmod 5$
37	$(29 \cdot 97, 1369, 666)$	$19 \cdot 37$	$19^{14} \equiv -1 \bmod 29$
38	$(5 \cdot 593, 1444, 703)$	$3 \cdot 13 \cdot 19$	$3^2 \equiv -1 \bmod 5$
39	(3121, 1521, 741)	$2^2 \cdot 3 \cdot 5 \cdot 13$	$2^{78} \equiv -1 \bmod 3121$
40	$(17 \cdot 193, 1600, 780)$	$2^2 \cdot 5 \cdot 41$	$5^8 \equiv -1 \bmod 17$
41	$(5 \cdot 13 \cdot 53, 1681, 820)$	$3 \cdot 7 \cdot 41$	$3^2 \equiv -1 \bmod 5$
42	(3613, 1764, 861)	$3 \cdot 7 \cdot 43$	$3^{903} \equiv -1 \bmod 3613$
43	$(5 \cdot 757, 1849, 903)$	$2 \cdot 11 \cdot 43$	$2^2 \equiv -1 \bmod 5$
44	$(17 \cdot 233, 1936, 946)$	$2 \cdot 3^2 \cdot 5 \cdot 11$	$2^4 \equiv -1 \bmod 17$
45	$(41 \cdot 101, 2025, 990)$	$3^2 \cdot 5 \cdot 23$	$5^{10} \equiv -1 \bmod 41$
46	$(5^2 \cdot 173, 2116, 1035)$	$23 \cdot 47$	$23^2 \equiv -1 \bmod 5$
47	(4513, 2209, 1081)	$2^3 \cdot 3 \cdot 47$	$3^{188} \equiv -1 \bmod 4513$
48	$(5 \cdot 941, 2304, 1128)$	$2^3 \cdot 3 \cdot 7^2$	$3^2 \equiv -1 \bmod 5$
49	$(13^2 \cdot 29, 2401, 1176)$	$5^2 \cdot 7^2$	$5^2 \equiv 7^6 \bmod 4901$ would be multipli
50	(5101, 2500, 1225)	$3 \cdot 5^2 \cdot 17$	existence unsettled
51	$(5 \cdot 1061, 2601, 1275)$	$2 \cdot 3 \cdot 13 \cdot 17$	$2^2 \equiv -1 \bmod 5$
52	$(37 \cdot 149, 2704, 1326)$	$2 \cdot 13 \cdot 53$	$2^{18} \equiv -1 \bmod 37$
53	$(5^2 \cdot 229, 2809, 1378)$	$3^3 \cdot 53$	$53^2 \equiv -1 \bmod 5$
54	$(13 \cdot 457, 2916, 1431)$	$3^3 \cdot 5 \cdot 11$	$5^2 \equiv -1 \bmod 13$
55	$(61 \cdot 101, 3025, 1485)$	$2^2 \cdot 5 \cdot 7 \cdot 11$	$5^{15} \equiv -1 \bmod 61$
56	$(5 \cdot 1277, 3136, 1540)$	$2^2 \cdot 3 \cdot 7 \cdot 19$	$3^2 \equiv -1 \bmod 5$
57	$(17 \cdot 389, 3249, 1596)$	$3 \cdot 19 \cdot 29$	$3^8 \equiv -1 \bmod 17$

TABLE I *(continued)*

t	(v,k,λ)	$n=k-\lambda$	reason for non-existence
58	$(5\cdot 37^2, 3364, 1653)$	$29\cdot 59$	$29 \equiv -1 \bmod 5$
59	$(73\cdot 97, 3481, 1711)$	$2\cdot 3\cdot 5\cdot 59$	$3^6 \equiv -1 \bmod 73$
60	$(7321, 3600, 1770)$	$2\cdot 3\cdot 5\cdot 61$	$2^{610} \equiv -1 \bmod 7321$
61	$(5\cdot 17, 3721, 1830)$	$31\cdot 61$	$31^8 \equiv -1 \bmod 17$
62	$(13\cdot 601, 3844, 1891)$	$3^2\cdot 7\cdot 31$	$7^6 \equiv -1 \bmod 13$
63	$(5\cdot 1613, 3969, 1953)$	$2^5\cdot 3^2\cdot 7$	$7^2 \equiv -1 \bmod 5$
64	$(53\cdot 157, 4096, 2016)$	$2^5\cdot 5\cdot 13$	$5^{26} \equiv -1 \bmod 53$
65	$(8581, 4225, 2080)$	$3\cdot 5\cdot 11\cdot 13$	$3^{715} \equiv -1 \bmod 8581$
66	$(5\cdot 29\cdot 61, 4356, 2145)$	$3\cdot 11\cdot 67$	$3^2 \equiv -1 \bmod 5$
67	$(13\cdot 701, 4489, 2211)$	$2\cdot 17\cdot 67$	$2^6 \equiv -1 \bmod 13$
68	$(5\cdot 1877, 4624, 2278)$	$2\cdot 3\cdot 17\cdot 23$	$2^2 \equiv -1 \bmod 5$
69	$(9661, 4761, 2346)$	$3\cdot 5\cdot 7\cdot 23$	$7^{2415} \equiv -1 \bmod 9661$
70	$(9941, 4900, 2415)$	$5\cdot 7\cdot 71$	$7^{2485} \equiv -1 \bmod 9941$
71	$(5^2\cdot 409, 5041, 2485)$	$2^2\cdot 3^2\cdot 71$	$2^{510} \equiv -1 \bmod 10225$
72	$(10513, 5184, 2556)$	$2^2\cdot 3^2\cdot 73$	$2^{1314} \equiv -1 \bmod 10513$
73	$(5\cdot 2161, 5329, 2628)$	$37\cdot 73$	$37^2 \equiv -1 \bmod 5$
74	$(17\cdot 653, 5476, 2701)$	$3\cdot 5^2\cdot 37$	$3^8 \equiv -1 \bmod 17$
75	$(13\cdot 877, 5625, 2775)$	$2\cdot 3\cdot 5^2\cdot 19$	$2^6 \equiv -1 \bmod 13$
76	$(5\cdot 2341, 5776, 2850)$	$2\cdot 7\cdot 11\cdot 19$	$2^2 \equiv -1 \bmod 5$
77	$(41\cdot 293, 5929, 2926)$	$3\cdot 7\cdot 11\cdot 13$	$3^4 \equiv -1 \bmod 41$
78	$(5^2\cdot 17\cdot 29, 6084, 3003)$	$3\cdot 13\cdot 79$	$3^2 \equiv -1 \bmod 5$
79	$(12641, 6241, 3081)$	$2^3\cdot 5\cdot 79$	$5^{1580} \equiv -1 \bmod 12641$
80	$(13\cdot 997, 6400, 3160)$	$2^3\cdot 3^4\cdot 5$	$5^2 \equiv -1 \bmod 13$
81	$(5\cdot 2657, 6561, 3240)$	$3^4\cdot 41$	$41^{332} \equiv -1 \bmod 2657$
82	$(13613, 6724, 3321)$	$41\cdot 83$	$41 \equiv 83^3 \bmod 13613$ would be multipl
83	$(5\cdot 2789, 6889, 3403)$	$2\cdot 3\cdot 7\cdot 83$	$2^2 \equiv -1 \bmod 5$
84	$(14281, 7056, 3486)$	$2\cdot 3\cdot 5\cdot 7\cdot 17$	$2^{1190} \equiv -1 \bmod 14281$
85	$(14621, 7225, 3570)$	$5\cdot 17\cdot 43$	$5^{3655} \equiv -1 \bmod 14621$
86	$(5\cdot 41\cdot 73, 7396, 3655)$	$3\cdot 29\cdot 43$	$3^2 \equiv -1 \bmod 5$
87	$(15313, 7569, 3741)$	$2^2\cdot 3\cdot 11\cdot 29$	$3^{1276} \equiv -1 \bmod 15313$
88	$(5\cdot 13\cdot 241, 7744, 3828)$	$2^2\cdot 11\cdot 89$	$89 \equiv -1 \bmod 5$
89	$(37\cdot 433, 7921, 3916)$	$3^2\cdot 5\cdot 89$	$5^{18} \equiv -1 \bmod 37$
90	$(16381, 8100, 4005)$	$3^2\cdot 5\cdot 7\cdot 13$	$13^{65} \equiv -1 \bmod 16381$
91	$(5\cdot 17\cdot 197, 8281, 4095)$	$2\cdot 7\cdot 13\cdot 23$	$2^2 \equiv -1 \bmod 5$
92	$(109\cdot 157, 8464, 4186)$	$2\cdot 3\cdot 23\cdot 31$	$2^{18} \equiv -1 \bmod 109$
93	$(5\cdot 13\cdot 269, 8649, 4278)$	$3\cdot 31\cdot 47$	$3^2 \equiv -1 \bmod 5$
94	$(53\cdot 337, 8836, 4371)$	$5\cdot 19\cdot 47$	$5^{26} \equiv -1 \bmod 53$
95	$(17\cdot 29\cdot 37, 9025, 4465)$	$2^4\cdot 3\cdot 5\cdot 19$	$3^8 \equiv -1 \bmod 17$
96	$(5^3\cdot 149, 9216, 4560)$	$2^4\cdot 3\cdot 97$	$3^2 \equiv -1 \bmod 5$
97	$(19013, 9409, 4656)$	$7^2\cdot 97$	$7^{4753} \equiv -1 \bmod 19013$
98	$(5\cdot 3881, 9604, 4753)$	$3^2\cdot 7^2\cdot 11$	$11^{97} \equiv -1 \bmod 3881$
99	$(19801, 9801, 4851)$	$2\cdot 3^2\cdot 5^2\cdot 11$	$2^{4950} \equiv -1 \bmod 19801$
100	$(20201, 10000, 4950)$	$2\cdot 5^2\cdot 101$	$2^{5050} \equiv -1 \bmod 20201$

TABLE II

Case $\gamma = -1$:

Cyclic difference sets with parameters $(4n-1, 2n-1, n-1)$, $2 \leqslant n \leqslant 100$

n	$(4n-1, 2n-1, n-1)$	exists?	examples or comment to non-existence
2	(7, 3, 1)	Yes	$\mathbf{P}^2(\mathbf{F}_2) = QR(7)$
3	(11, 5, 2)	Yes	$QR(11)$
4	$(3 \cdot 5, 7, 3)$	Yes	$TP(3, 5) = \mathbf{P}^3(\mathbf{F}_2)$
5	(19, 9, 4)	Yes	$QR(19)$
6	(23, 11, 5)	Yes	$QR(23)$
7	$(3^3, 13, 6)$	No	7 would be multiplier
8	(31, 15, 7)	Yes	$\mathbf{P}^4(\mathbf{F}_2)$ and $QR(31)$
9	$(5 \cdot 7, 17, 8)$	Yes	$TP(5, 7)$
10	$(3 \cdot 13, 19, 9)$	No	$2 \equiv -1 \bmod 3$
11	(43, 21, 10)	Yes	$QR(43)$
12	(47, 23, 11)	Yes	$QR(47)$
13	$(3 \cdot 17, 25, 12)$	No	$13^2 \equiv -1 \bmod 17$
14	$(5 \cdot 11, 27, 13)$	No	$2^2 \equiv -1 \bmod 5$
15	(59, 29, 14)	Yes	$QR(59)$
16	$(3^2 \cdot 7, 31, 15)$	Yes	$\mathbf{P}^5(\mathbf{F}_2)$ and GMW
17	(67, 33, 16)	Yes	$QR(67)$
18	(71, 35, 17)	Yes	$QR(71)$
19	$(3 \cdot 5^2, 35, 18)$	No	$19 \equiv -1 \bmod 5$
20	(79, 39, 19)	Yes	$QR(79)$
21	(83, 41, 20)	Yes	$QR(83)$
22	$(3 \cdot 29, 43, 21)$	No	$2 \equiv -1 \bmod 3$
23	$(7 \cdot 13, 45, 22)$	No	$23^3 \equiv -1 \bmod 13$
24	$(5 \cdot 19, 47, 23)$	No	$3^2 \equiv -1 \bmod 5$
25	$(3^2 \cdot 11, 49, 24)$	No	25 would be multiplier
26	(103, 51, 25)	Yes	$QR(103)$
27	(107, 53, 26)	Yes	$QR(107)$
28	$(3 \cdot 37, 55, 27)$	No	$m = 7 \equiv 2^{32}$ would be multiplier
29	$(5 \cdot 23, 57, 28)$	No	$29 \equiv -1 \bmod 5$
30	$(7 \cdot 17, 59, 29)$	No	$2^4 \equiv -1 \bmod 17$
31	$(3 \cdot 41, 61, 30)$	No	$31^5 \equiv -1 \bmod 41$
32	(127, 63, 31)	Yes	$\mathbf{P}^6(\mathbf{F}_2)$, $QR(127)$, $MH(127)$, and 3 others
33	(131, 65, 32)	Yes	$QR(131)$
34	$(3^3 \cdot 5, 67, 33)$	No	$17 \equiv -1 \bmod 3$
35	(139, 69, 34)	Yes	$QR(139)$
36	$(11 \cdot 13, 71, 35)$	Yes	$TP(11, 13)$
37	$(3 \cdot 7^2, 73, 36)$	No	37 would be multiplier
38	(151, 75, 37)	Yes	$QR(151)$
39	$(5 \cdot 31, 77, 38)$	No	$3^2 \equiv -1 \bmod 5$
40	$(3 \cdot 53, 79, 39)$	No	$5 \equiv -1 \bmod 3$

TABLE 2 *(continued)*

n	$(4n-1, 2n-1, n-1)$	exists?	examples or comment to non-existence
41	(163, 81, 40)	Yes	$QR(163)$
42	(167, 83, 41)	Yes	$QR(167)$
43	$(3^2 \cdot 19, 85, 42)$	No	43 would be multiplier
44	$(5^2 \cdot 7, 87, 43)$	No	$m = 11 \equiv 2^{56} \bmod 175$ would be multiplier
45	(179, 89, 44)	Yes	$QR(179)$
46	$(3 \cdot 61, 91, 45)$	No	$23 \equiv -1 \bmod 3$
47	$(11 \cdot 17, 93, 46)$	No	$47^2 \equiv -1 \bmod 17$
48	(191, 95, 47)	Yes	$QR(191)$
49	$(3 \cdot 5 \cdot 13, 97, 48)$	No	7 would be multiplier
50	(199, 99, 49)	Yes	$QR(199)$
51	$(7 \cdot 29, 101, 50)$	No	$3^3 \equiv -1 \bmod 7$
52	$(3^2 \cdot 23, 103, 51)$	No	13 would be multiplier
53	(211, 105, 52)	Yes	$QR(211)$
54	$(5 \cdot 43, 107, 53)$	No	$2^2 \equiv -1 \bmod 5$
55	$(3 \cdot 73, 109, 54)$	No	$5 \equiv -1 \bmod 3$
56	(223, 111, 55)	Yes	$QR(223)$ and $MH(223)$
57	(227, 113, 56)	Yes	$QR(227)$
58	$(3 \cdot 7 \cdot 11, 115, 57)$	No	$2 \equiv -1 \bmod 3$
59	$(5 \cdot 47, 117, 58)$	No	$59 \equiv -1 \bmod 5$
60	(239, 119, 59)	Yes	$QR(239)$
61	$(3^5, 121, 60)$	No	61 would be multiplier
62	$(13 \cdot 19, 123, 61)$	No	$2^6 \equiv -1 \bmod 13$
63	(251, 125, 62)	Yes	$QR(251)$
64	$(3 \cdot 5 \cdot 17, 127, 63)$	Yes	$\mathbf{P}^7(\mathbf{F}_2)$, GMW and 2 new ones
65	$(7 \cdot 37, 129, 64)$	No	$5^3 \equiv -1 \bmod 7$
66	(263, 131, 65)	Yes	$QR(263)$
67	$(3 \cdot 89, 133, 66)$	No	67 would be multiplier
68	(271, 135, 67)	Yes	$QR(271)$
69	$(5^2 \cdot 11, 137, 68)$	No	$3^2 \equiv -1 \bmod 5$
70	$(3^2 \cdot 31, 139, 69)$	No	$2 \equiv -1 \bmod 3$
71	(283, 141, 70)	Yes	$QR(283)$ and $MH(283)$
72	$(7 \cdot 41, 143, 71)$	No	$m = 9 \equiv 2^{55} \equiv 3^2 \bmod 287$ would be multiplier
73	$(3 \cdot 97, 145, 72)$	No	$73^{12} \equiv -1 \bmod 97$
74	$(5 \cdot 59, 147, 73)$	No	$2^2 \equiv -1 \bmod 5$
75	$(13 \cdot 23, 149, 74)$	No	$m = 3^3 \equiv 5^4 \bmod 299$ would be multiplier
76	$(3 \cdot 101, 151, 75)$	No	$m = 19 \equiv 2^9 \bmod 303$ would be multiplier
77	(307, 153, 76)	Yes	$QR(307)$
78	(311, 155, 77)	Yes	$QR(311)$
79	$(3^2 \cdot 5 \cdot 7, 157, 78)$	No	$79 \equiv -1 \bmod 5$
80	$(11 \cdot 29, 159, 79)$	No	$5^7 \equiv -1 \bmod 29$
81	$(17 \cdot 19, 161, 80)$	Yes	$TP(17, 19)$
82	$(3 \cdot 109, 163, 81)$	No	$2 \equiv -1 \bmod 3$

TABLE II *(continued)*

n	$(4n-1, 2n-1, n-1)$	exists?	examples or comment to non-existence
83	(331, 165, 82)	Yes	$QR(331)$
84	$(5 \cdot 67, 167, 83)$	No	$3^2 \equiv -1 \bmod 5$
85	$(3 \cdot 113, 169, 84)$	No	$5 \equiv -1 \bmod 3$
86	$(7^3, 171, 85)$	No	$m = 43 \equiv 2^{144} \bmod 343$ would be multiplier
87	(347, 173, 86)	Yes	$QR(347)$
88	$(3^3 \cdot 13, 175, 87)$	No	$11 \equiv -1 \bmod 3$
89	$(5 \cdot 71, 177, 88)$	No	$89 \equiv -1 \bmod 5$
90	(359, 179, 89)	Yes	$QR(359)$
91	$(3 \cdot 11^2, 181, 90)$	No	$7^5 \equiv -1 \bmod 11$
92	(367, 183, 91)	Yes	$QR(367)$
93	$(7 \cdot 53, 185, 92)$	No	$3^3 \equiv -1 \bmod 7$
94	$(3 \cdot 5^3, 187, 93)$	No	$2 \equiv -1 \bmod 3$
95	(379, 189, 94)	Yes	$QR(379)$
96	(383, 191, 95)	Yes	$QR(383)$
97	$(3^2 \cdot 43, 193, 96)$	No	97 would be multiplier
98	$(17 \cdot 23, 195, 97)$	No	$2^4 \equiv -1 \bmod 17$
99	$(5 \cdot 79, 197, 98)$	No	$11 \equiv 3^{68} \bmod 395$ would be multiplier
100	$(3 \cdot 7 \cdot 19, 199, 99)$	No	$4 = 2^2 \equiv 5^8 \bmod 399$ would be multiplier

REFERENCES

[Bar] BARKER, R. H. Group synchronizing of binary digital systems. In *Communication Theory,* W. Jackson, Ed., London: Butterworth, 1953, pp. 273-287.

[Bau] BAUMERT, L. D. *Cyclic difference sets.* Lecture Notes in Mathematics 182, New York: Springer-Verlag, 1971.

[BF] BAUMERT, L. D. and H. FREDRICKSEN. The Cyclotomic Numbers of Order Eighteen with Applications to Difference Sets. *Math. Comp. 21* (1967), 204-219.

[EKS] ELIAHOU, S., M. KERVAIRE and B. SAFFARI. A New Restriction on the Lengths of Golay Complementary Sequences. *J. Comb. Theory., Ser. A 55* (1990), 45-59.

[GMW] GORDON, B., W. H. MILLS and L. R. WELCH. Some New Difference Sets. *Canad. J. Math. 14* (1962), 614-625.

[H] HALL, M. Jr. *Combinatorial Theory.* Wiley-Interscience, Second Edition, 1986.

[JL] JEDWAB, J. and S. LLOYD. A Note on the Nonexistence of Barker Sequences. *Designs, Codes and Cryptography 2* (1992), 93-97.

[L] LANDER, E. S. *Symmetric Designs: An Algebraic Approach.* London Math. Soc. Lecture Note Series 74, Cambridge University Press, 1983.

[R] RANKIN, R. A. Difference sets. *Acta Arithmetica 9* (1964), 161-168.
[ST] STORER, J. and R. TURYN. On binary sequences. *Proc. Amer. Math. Soc. 12* (1961), 394-399.
[T1] TURYN, R. Character sums and difference sets. *Pac. J. Math. 15* (1965), 319-346.
[T2] —— Sequences with small correlation. In *Error Correcting Codes,* H. B. Mann, Editor, Wiley, New York, 1968, pp. 195-228.
[Y] YAMAMOTO, K. Decomposition fields of difference sets. *Pacific J. Math. 13* (1963), 337-352.

(Reçu le 13 février 1992)

Shalom Eliahou
Michel Kervaire

Section de Mathématiques
Université de Genève
C.P. 240
1211 Genève 24, Switzerland

Monographies de l'Enseignement Mathématique

2. H. HADWIGER et H. DEBRUNNER, *Kombinatorische Geometrie in der Ebene*; 35 Fr. suisses.
3. J.-E. HOFMANN, *Über Jakob Bernoullis Beiträge zur Infinitesimal-Mathematik*; 20 Fr. suisses.
4. H. LEBESGUE, *Notices d'histoire des mathématiques*; 15 Fr. suisses.
5. J. BRACONNIER, *L'analyse harmonique dans les groupes abéliens*; 15 Fr. suisses.
15. K. KURATOWSKI, *Introduction à la théorie des ensembles et à la topologie*; 70 Fr. suisses, relié.

*19. W. M. SCHMIDT, *Approximation to algebraic numbers*; 70 pages, 1972; 25 Fr. suisses.

*20. J. L. LIONS, *Sur le contrôle optimal de systèmes distribués*; 45 pages, 1973; 20 Fr. suisses.

*21. F. HIRZEBRUCH, *Hilbert modular surfaces*; 103 pages, 1973; 35 Fr. suisses.

22. A. WEIL, *Essais historiques sur la théorie des nombres*; 56 pages, 1975; 24 Fr. suisses.
23. J. GUENOT et R. NARASIMHAN, *Introduction à la théorie des surfaces de Riemann*; 214 pages, 1976; 60 Fr. suisses.

*24. DAVID MUMFORD, *Stability of projective varieties*; 74 pages, 1977; 30 Fr. suisses.

*25. A. G. VITUSHKIN, *On representation of functions by means of superpositions and related topics*; 68 pages, 1978; 25 Fr. suisses.

26. TOPOLOGY AND ALGEBRA, *Proceedings of a Colloquium in Honour of B. Eckmann,* Edited by M.-A. Knus, G. Mislin and U. Stammbach; 280 pages, 1978; 55 Fr. suisses.
27. CONTRIBUTIONS TO ANALYSIS, *Papers communicated to a Symposium in Honour of A. Pfluger,* 106 pages, 1979; 30 Fr. suisses.
28. P. ERDÖS and R. L. GRAHAM, *Old and new problems and results in combinatorial number theory.* 128 pages, 1980; 43 Fr. suisses.
29. THÉORIE ERGODIQUE, *Séminaire des Plans-sur-Bex, Mars 1980*; 112 pages, 1981; 30 Fr. suisses.
30. LOGIC AND ALGORITHMIC, *An International Symposium in Honour of E. Specker*; 392 pages, 1982; 75 Fr. suisses.
31. NŒUDS, TRESSES ET SINGULARITÉS, *Séminaire des Plans-sur-Bex, Mars 1982*; 260 pages, 1983; 45 Fr. suisses.

*32. M. KASHIWARA, *Introduction to microlocal analysis*: 38 pages, 1986; 20 Fr. suisses.

*33. S. T. YAU, *Nonlinear analysis in geometry*; 56 pages, 1986; 25 Fr. suisses.

*34. V. I. ARNOLD, *Contact geometry and wave propagation*; 56 pages, 1989; 27 Fr. suisses.

*Série des Conférences de l'Union Mathématique Internationale.

Un escompte de 20% est accordé aux commandes payées d'avance et adressées à

L'Enseignement Mathématique, Case postale 240

CH-1211 GENÈVE 24 (Suisse)

(Compte de chèques postaux 12-12042 – 5)

UNIONE MATEMATICA ITALIANA

OPERE DEI GRANDI MATEMATICI ITALIANI

CESARE ARZELA' - Opere - 2 volumi - **Novità** (1992) - complessive L. 66.900

LUIGI BIANCHI - Opere - 11 volumi (in 12 tomi) - complessive L.507.700

ENRICO BOMPIANI - Opere scelte - 3 volumi - L.135.900

RENATO CACCIOPPOLI - Opere - 2 volumi - L.79.100

FELICE CASORATI - Opere - 2 volumi - L.79.100

BONAVENTURA CAVALIERI - (fuori collana) - Exercitationes Geometricae Sex (edizione anastatica da quella originale del 1647), e di Enrico Giusti: Bonaventura Cavalieri and the Theory of Indivisibles - 2 volumi indivisibili in cofanetto - L.80.400

ERNESTO CESARO - Opere scelte - 2 volumi (in 3 tomi) - L.135.900

ULISSE DINI - Opere - 5 volumi - L.246.700

LUIGI FANTAPPIE' - Opere scelte - 2 volumi - L.90.600

GUIDO FUBINI - Opere scelte - 3 volumi - L.112.900

ELIA EUGENIO LEVI - Opere - 2 volumi - L.90.600

GIANFRANCESCO MALFATTI - Opere - 2 volumi - L.90.600

PIA NALLI - Opere scelte - un volume - L.45.300

GIUSEPPE PEANO - Opere - 3 volumi - L.135.900

MARIO PIERI - Opere sui fondamenti della matematica - un volume - L.45.300

SALVATORE PINCHERLE - Opere scelte - 2 volumi - L.90.600

GREGORIO RICCI CURBASTRO - Opere - 2 volumi - L.90.600

PAOLO RUFFINI - Opere matematiche e carteggio - 2 tomi - L.79.100

GAETANO SCORZA - Opere scelte - 3 volumi - L.135.900

BENIAMINO SEGRE - Opere scelte - 2 volumi - L.106.400

CORRADO SEGRE - Opere scelte - 4 volumi - L.181.200

ANTONIO SIGNORINI - Opere scelte - un volume - L.66.900

LEONIDA TONELLI - Opere scelte - 4 volumi - L.181.200

GIUSEPPE VITALI - Opere sull'analisi reale e complessa, Carteggio - un volume - L.66.900

EDIZIONI CREMONESE - Borgo S. Croce, 17 - 50122 Firenze -
tel.055-2476371 - c.c.p. 13631502.

Ai soci dell'U.M.I. sconto del 20%