Bull. Aust. Math. Soc. **80** (2009), 147–158
doi:10.1017/S0004972709000161

QUALIFIED DIFFERENCE SETS FROM UNIONS OF CYCLOTOMIC CLASSES

KEVIN BYARD✉ and KEVIN BROUGHAN

(Received 8 October 2008)

Abstract

Qualified difference sets (QDS) composed of unions of cyclotomic classes are discussed. An exhaustive computer search for such QDS and modified QDS that also possess the zero residue has been conducted for all powers $n = 4, 6, 8$ and 10. Two new families were discovered in the case $n = 8$ and some new isolated systems were discovered for $n = 6$ and $n = 10$.

2000 *Mathematics subject classification*: primary 05B10; secondary 11A15, 11T22.
Keywords and phrases: qualified residue difference sets, difference sets, cyclotomy.

1. Introduction

We define a qualified difference set (QDS) as follows.

DEFINITION 1.1. Let $R = \{r_1, r_2, r_3, \ldots, r_k\}$ be a k-element set of distinct nonzero residues modulo an integer v. We call R a *qualified difference set* (QDS) if there exists some nonzero integer $m \notin R$ which is such that if we form all the nonzero differences

$$r_i - mr_j \pmod{v}, \qquad 1 \le i, j \le k \tag{1.1}$$

we obtain every positive integer less than or equal to $v - 1$ exactly λ times. We call m a *qualifier* of multiplicity λ for the set R.

If zero is counted as a residue, then further such sets are possible. These are called *modified qualified difference sets*, (MQDS) by virtue of the modification introduced by the inclusion of the zero element. We define these sets as follows.

DEFINITION 1.2. Let $R^* = \{r_0, r_1, r_2, \ldots, r_k\}$ be a $(k + 1)$-element set of residues of an integer v, where $r_0 = 0$. We call R^* a modified qualified difference set (MQDS) if there exists some nonzero integer $m \notin R^*$ which is such that if we form all the differences

$$r_i - mr_j \pmod{v}, \qquad 0 \le i, j \le k \tag{1.2}$$

we obtain every positive integer less than or equal to $v - 1$ exactly λ times and zero exactly once. We call m a *qualifier* of multiplicity λ for the set R^*.

When QDS and MQDS are generated from nth-power residues of a prime $v = p = nk + 1$ with n a positive integer, we obtain the special cases of qualified residue difference sets (QRDS) and modified qualified residue difference sets (MQRDS) respectively. These sets were introduced by Jennings and Byard [10, 11].

QDS and MQDS have similar properties to the residue difference sets and modified residue difference sets respectively, which were discussed in detail in 1953 by Lehmer [13]. All four classes of set possess similarly attractive properties. In particular when mapped onto a binary (0, 1) array, they possess a two-valued correlation function (see Equations (A.1)–(A.3) in the appendix). This property suggests potential applications in areas such as image formation [4, 5, 17], signal processing [15] and aperture synthesis [12].

In his subsequent extensive survey, Hall [7] extended the notion of 'residue difference sets' and discovered a new family of difference set that can be created from a union of sixth-power *cyclotomic classes*, where we define the nth-power cyclotomic class $C(c_i)$ for the prime p, by

$$C(c_i) \equiv \{g^{un+c_i} \pmod p) \mid 0 \le u \le f - 1\} \tag{1.3}$$

where $p = nf + 1$ and g is a primitive root of p. Hall discovered that the union of those sixth-power cyclotomic classes with indices congruent to 0, 1 and 3 modulo 6 form a difference set when p is of the form $p = 4\alpha^2 + 27$ (integer α), for an appropriate choice of primitive root g, such that $\mathrm{ind}_g 3 = 1$. In this paper we demonstrate the existence of QDS and MQDS that are similarly composed of unions of cyclotomic classes. These sets are defined as follows.

Definition 1.3. Let $p = nf + 1$ be a prime and $k = tf$. Let $C = \{c_1, c_2, \ldots, c_t\}$ be a set of t residue classes that are all distinct modulo n. Now let R be the k-element set consisting of the union of nth-power cyclotomic classes derived from the set C as

$$R = \{r_i \mid 1 \le i \le k\} = C(c_1) \cup C(c_2) \cup \cdots \cup C(c_t) \tag{1.4}$$

and let R^* be the $(k + 1)$-element set, defined by

$$R^* = \{r_i \mid 0 \le i \le k\} = R \cup \{0\}, \quad r_0 = 0 \tag{1.5}$$

where $C(c_i)$ is defined by congruence (1.3). Then R is a QDS if, for a suitable choice of qualifier m, the conditions in Definition 1.1 are satisfied, and R^* is a MQDS if, for a suitable choice of qualifier m, the conditions of Definition 1.2 are satisfied.

The purpose of this article is to describe the results of an exhaustive search for QDS and MQDS created from the unions of cyclotomic classes for the cases $n = 4$, 6, 8 and 10.

2. Residue classes and cyclotomic constants

Let $p = nf + 1$ be a prime and g a primitive root of p. An integer N is said to be in *residue class* i if the following congruence holds for some integer u:

$$N \equiv g^{un+i} \pmod{p}. \tag{2.1}$$

The *cyclotomic constant* (i, j) denotes the number of solutions to the congruence

$$g^{un+i} + 1 \equiv g^{vn+j} \pmod{p} \tag{2.2}$$

where $0 \leq i, j \leq n - 1$ and $0 \leq u, v \leq f - 1$. The following further results, due to Dickson [6], are required too:

$$(i, j) = (i + \gamma_1 n, j + \gamma_2 n) \tag{2.3}$$

where γ_1 and γ_2 are integers,

$$(i, j) = (n - i, j - i) = (-i, j - i) \quad \text{for all } f, \tag{2.4}$$

$$(i, j) = (j, i) \quad \text{if } f \text{ is even}. \tag{2.5}$$

3. Theory

In order to investigate whether QDS and MQDS can be generated from unions of cyclotomic classes, it is necessary to determine how often the nonzero differences occur between the elements of sets of different cyclotomic classes. This can be done as follows, using an approach similar to that adopted by Hall [7] and a further search for residue difference sets or order $n = 10$ conducted by Hayashi [9]. Following (1.1), consider the congruence

$$Y - mX \equiv d \pmod{p} \tag{3.1}$$

where Y is in residue class j, X is in residue class i, m is in residue class $\sigma \neq 0$ and d is in residue class s. Using these conditions, we get

$$g^{An+j} - g^{Bn+i+\sigma} \equiv g^{\kappa n+s} \pmod{p}$$

where A, B and κ are integers. Multiplying this congruence by $g^{-\kappa n-s}$ and rearranging gives

$$g^{B'n+i+\sigma-s} + 1 \equiv g^{A'n+j-s} \pmod{p} \tag{3.2}$$

where A' and B' are also integers. Now by the cyclotomic constant Equation (2.2), we see that congruence (3.2), and hence congruence (3.1), has $(i + \sigma - s, j - s)$ solutions. This enables us to calculate how often each difference d arises from congruence (3.1), which is derived from different nth-power cyclotomic classes. For the set of residue classes $C = \{c_1, c_2, \ldots, c_t\}$, the general equation for the number $N(s)$ of times the difference d in residue class s occurs is given by

$$N(s) = \sum_{i \in C} \sum_{j \in C} (i + \sigma - s, j - s). \tag{3.3}$$

Note by (2.3) that $N(s+\gamma n) = N(s)$ for integer γ. As there are $n-1$ residue classes, then there are at most $n-1$ different values for $N(s)$, although in practice some of the values of $N(s)$ will repeat for different values of s. If conditions can be determined that make each value of $N(s)$ equal, then a QDS will result. If no such conditions exist, there will be no corresponding QDS.

In the case of a MQDS, the residue 0 is added to the union of cyclotomic classes. Here we denote the set of residue classes by $C = \{c_1, c_2, \ldots, c_t\}_0$. In this case we need to consider the two additional differences:

$$Y - 0 \equiv d \pmod{p}, \tag{3.4}$$

$$0 - mX \equiv d \pmod{p}. \tag{3.5}$$

For congruence (3.4) we have $Y \equiv d$ and so d, which is in residue class s, also is in residue class j. Therefore $j = s$ and hence $s \in C$. This means that we need to add 1 to the summation $N(s)$ in (3.3) if $s \in C$. Congruence (3.5) is a little more complicated. Here we have $(-1)(mX) \equiv d$ and mX is in residue class $\sigma + i$. Now

$$(-1) \equiv g^{(p-1)/2} \equiv g^{nf/2} \equiv \begin{cases} g^{n(f/2)} & \text{if } f \text{ is even,} \\ g^{n(f-1)/2+n/2} & \text{if } f \text{ is odd.} \end{cases} \tag{3.6}$$

Therefore if f is even, then -1 is in residue class 0. In this case, by Equation (3.5), d, which is in residue class s, is also in residue class $\sigma + i + 0$ (that is the residue class of $-mX$). Therefore $i = s - \sigma$ and so we must add 1 to the summation for $N(s)$ in Equation (3.3) if $s - \sigma \in C$. If f is odd, then by (3.6) -1 is in residue class $n/2$. Here, by (3.5), d, which is in residue class s, is also in residue class $\sigma + i + n/2$. Therefore, $i = s - \sigma - n/2$ and so we must add 1 to the summation for $N(s)$ in Equation (3.3) if $s - \sigma - n/2 \in C$.

Equation (3.3) has been applied to the cases $n = 4$, 6, 8 and 10 to determine if any QDS or MQDS composed of unions of cyclotomic classes exist. In each case, an exhaustive computer search has been completed for the range $1 \le \sigma \le n-1$, for f odd and f even (note that $\sigma = 0$ corresponds to difference sets, which is not the subject of this study).

An important type of equivalence between the sets is the concept of ‘complementary’ sets. This is a familiar notion in the study of difference sets (see, for example, Baumert [2, pp. 2–3]) and the same applies to QDS and MQDS. If R is a QDS, then the set $R^* = \{Z_p\} - \{R\}$ is a MQDS which is the complement of R, that has the same qualifier m. Stated differently, if C is the set of residue classes that give a QDS, then $C^* = \{Z_n\} - \{C\}$ is the set of residue classes that, with the residue zero, gives the corresponding complementary MQDS. The detailed analysis of this point is given in the appendix. Because of this equivalence, it is only necessary to analyse cases where $t \le n/2$.

For each value of n, there are many other equivalent cases that arise due to the following two isomorphisms. Firstly, assume that $C = \{c_1, c_2, \ldots, c_t\}$ is a set of residue classes that produces a QDS. Therefore, congruence (3.1) and (3.3) lead to values of $N(s)$ that are equal for all s. Now consider the set $C' = \{c_1 + q, c_2 + q, \ldots, c_t + q\}$ for some integer q. Using Equation (3.3) the summation $N(s)$ for the set C' is as follows:

$$\begin{aligned} N(s) &= \sum_{i \in C'} \sum_{j \in C'} (i + \sigma - s, j - s) \\ &= \sum_{i \in C} \sum_{j \in C} (i + q + \sigma - s, j + q - s) \\ &= \sum_{i \in C} \sum_{j \in C} (i + \sigma - [s - q], j - [s - q]) \\ &= N(s - q). \end{aligned} \tag{3.7}$$

Now, since each value of $N(s)$ is equal for C then the same values for $N(s - q)$ will result for the set C'. Therefore, if $C = \{c_1, c_2, \ldots, c_t\}$ is a set of residue classes that gives a QDS, then the set $C' = \{c_1 + q, c_2 + q, \ldots, c_t + q\}$ will also give an isomorphic QDS. In the case of MQDS, R^*, the same argument applies. If $C = \{c_1, c_2, \ldots, c_t\}_0$ is a set of residue classes that produces a MQDS then $C^* = \{Z_n\} - \{C\}$ will give a complementary QDS.

Secondly assume that $C = \{c_1, c_2, \ldots, c_t\}$ is a set of residue classes that, using the primitive root g, gives a QDS. Choose one of these classes, say c, and let $C(c)$ be the corresponding cyclotomic class. Therefore, by congruence (1.3) we have

$$C(c) \equiv \{g^{un+c} (\text{mod } p) \mid 0 \leq u \leq f - 1\}. \tag{3.8}$$

Now, let g_1 be another primitive root of p, where

$$g_1^z \equiv g \pmod p \tag{3.9}$$

where z must be prime to $p - 1 = nf$. Substituting this into (3.8) gives

$$C(c) \equiv \{g_1^{zun+zc}\} \equiv \{g_1^{zc} (g_1^n)^{uz} (\text{mod } p) \mid 0 \leq u \leq f - 1\}. \tag{3.10}$$

Now, because the integers $u : 0 \leq u \leq f - 1$ form a complete residue system modulo f, then because z is prime to f (which is the case, since z must be prime to nf), the integers $uz : 0 \leq u \leq f - 1$ also form the same reduced residue system. Therefore, congruence (3.10) becomes

$$C(c) \equiv \{g_1^{zc} (g_1^n)^u\} \equiv \{g_1^{un+zc} (\text{mod } p) \mid 0 \leq u \leq f - 1\}. \tag{3.11}$$

Comparing (3.8) with (3.11) shows that a QDS derived from $C = \{c_1, c_2, \ldots, c_t\}$ and primitive root g will be the same as that derived from $C = \{zc_1, zc_2, \ldots, zc_t\}$ and primitive root g_1 where $g_1^z \equiv g \pmod p$. In the case of a MQDS, the same argument evidently applies.

The results below are given up to equivalence, either by complementary sets or isomorphism. A major positive result was revealed in the case $n = 8$, This, therefore, is where we begin.

4. Results for $n = 8$

In this section we prove the following theorem.

THEOREM 4.1. *Qualified difference sets created from the union of eighth-power cyclotomic classes $C = \{0, 1\}$ exist for all primes of the form $p = 64z^4 + 128z^3 + 144z^2 + 80z + 17$ and $p = 64z^4 + 48z^2 + 1$ where z is an integer. All other unions of eighth-power cyclotomic classes are isomorphic to either of these cases or to previously known QDS, MQDS or residue difference sets.*

PROOF. For the case $n = 8$, we need to consider the additional condition of whether 2 is either a biquadratic (that is fourth-power) residue or a biquadratic nonresidue of p. In order to demonstrate the computational methods used, a detailed analysis follows, for the case when f is even, $t = 2$, $C = \{0, 1\}$, $\sigma = 4$ and 2 is a biquadratic nonresidue of p.

For $C = \{0, 1\}$ and $\sigma = 4$, Equation (3.3), along with Equations (2.3), (2.4) and (2.5), gives the following condition for the number of differences $N(s)$:

$$\begin{aligned} s = 0: &\quad N(0) = (4, 0) + (4, 1) + (5, 0) + (5, 1), \\ s = 1: &\quad N(1) = (3, 7) + (3, 0) + (4, 7) + (4, 0), \\ s = 2: &\quad N(2) = (2, 6) + (2, 7) + (3, 6) + (3, 7), \\ s = 3: &\quad N(3) = (1, 5) + (1, 6) + (2, 5) + (2, 6). \end{aligned} \tag{4.1}$$

In this case the values for $s = 4, 5, 6, 7$ repeat those for $s = 0, 1, 2, 3$. Following Dickson's work [6, Theorem 11], Berndt *et al.* demonstrated that the cyclotomic constants for $n = 8$ are determined uniquely by the quadratic partition

$$p = a_4^2 + b_4^2 = a_8^2 + 2b_8^2 \tag{4.2}$$

where, for our case $p = 8f + 1$, we have

$$a_4 \equiv -1 \pmod 4, \qquad b_4 \equiv a_4 g^{(p-1)/4} \pmod p \tag{4.3}$$

[3, p. 78], and

$$a_8 \equiv -1 \pmod 4, \qquad 2b_8 \equiv a_8(g^f + g^{3f}) \pmod p \tag{4.4}$$

[3, p. 109] where a_4, b_4, a_8 and b_8 are integers in the nomenclature of Berndt *et al.* The actual cyclotomic constants for $n = 8$ have been calculated, using Dickson's results [6], by Lehmer, who lists them in the appendix of her paper for the cases $p = 16\alpha + 1$ and $p = 16\alpha + 9$ (integer α) [14]. Since we now have $p = 8f + 1$ and f is even, we require her list for $p = 16\alpha + 1$ [14, p. 116]. Substituting these cyclotomic constants for the case when 2 is a biquadratic nonresidue of p into Equations (4.1) gives

$$\begin{aligned} s = 0: &\quad 64N(0) = 4p - 12 + 4a_4 + 4a_8, \\ s = 1: &\quad 64N(1) = 4p - 12 + 4a_4 + 4a_8, \\ s = 2: &\quad 64N(2) = 4p + 4 - 4a_4 - 4a_8 + 8b_4 - 16b_8, \\ s = 3: &\quad 64N(3) = 4p + 4 - 4a_4 - 4a_8 + 16b_8 - 8b_4. \end{aligned} \tag{4.5}$$

(Note that in her paper, Lehmer instead uses the symbols x, y, a, b, where $x = -a_4$, $a = -a_8$, $2y = b_4$ and $b = b_8$.) Now, if all values $N(s)$ are equal then a QDS will result. Putting this restriction on the equations in (4.5) gives

$$\begin{aligned} b_4 &= 2b_8, \\ a_4 + a_8 &= 2. \end{aligned} \tag{4.6}$$

Combining (4.6) and (4.2), and setting $x = -a_4$ and $2y = b_4$ for ease of notation, gives

$$\begin{aligned} p &= x^2 + 8x + 8 \quad x \equiv 1 \pmod 4, \\ y^2 &= 2 + 2x \end{aligned} \tag{4.7}$$

and hence $p = 64z^4 + 128z^3 + 144z^2 + 80z + 17$ as in the statement of Theorem 4.1. Now, under the conditions in Equation (4.2), 2 is always a biquadratic nonresidue of p of the form in Equation (4.7) by the following analysis. Equation (4.7) gives $y^2 = 2(x + 1)$, but since $x \equiv 1 \pmod 4$ then we have $y^2 = 4(2\eta + 1)$ where $2\eta + 1$ must be an odd square. Substituting this into Equation (4.2) means that $p = x^2 + [4(2\eta + 1)]^2$, and so, since the representation of $p = 8f + 1 \equiv 1 \pmod 4$ as the sum of two squares is unique up to order and sign, p cannot be represented in the form $p = x^2 + 64\eta_1^2$ for integer η_1. Therefore 2 must be a biquadratic nonresidue of p by a known theorem on biquadratic reciprocity (see, for example, Mollin [16, Corollary 5.71]) and as a result we shall always obtain values for $N(s)$ as given by the equations in (4.5). The sequence of primes of this form starts $p = 17, 433, 2801, 10\,193, 60\,017, \ldots$.

The values of those primitive roots that can be used to generate the QDS are determined by the condition $b_4 = 2b_8$ from (4.6). Substituting the values of b_4 and b_8 from (4.3) and (4.4) into (4.6) and rearranging gives

$$a_8\mu^2 - a_4\mu + a_8 \equiv 0 \pmod p \tag{4.8}$$

where $\mu = g^f$. This quadratic congruence for μ can be demonstrated to give

$$(2a_8\mu - a_4)^2 \equiv a_4^2 - 4a_8^2 \pmod p. \tag{4.9}$$

Congruence (4.9) reduces to a simple calculation of the squares $(2a_8\mu - a_4)^2$, which can then be used to calculate the values of $\mu = g^f$ that lead to the condition $b_4 = 2b_8$, and hence those primitive roots g that give QDS for $n = 8$, $\sigma = 4$, $C = \{0, 1\}$ and $p = x^2 + 8x + 8$ ($x \equiv 1 \pmod 4$). For the converse, assume that we have a prime of the form given in (4.7). We can write $p = (x + 2)^2 + 2y^2$ and so, by uniqueness and (4.2), $b^2 = y^2$ and so $(x + 2)^2 = a^2$, where $a = -a_8$. Therefore $x + 2 = \pm a$, which combined with the condition $x \equiv a \equiv 1 \pmod 4$ means that $x + a = -2$ and so the second of the equations in (4.6) is satisfied. Now since $x + a + 2 = 0$, we have $a = -(x + 2)$ so we can write

$$x^2 - 4a^2 = -[x^2 + 2(x^2 + 8x + 8)] = -(x^2 + 2p) \equiv -x^2 \pmod p. \tag{4.10}$$

However, $(-1/p) = 1$ where $(-1/p)$ is the Legendre symbol, since $p \equiv 1 \pmod 4$. Combining this with (4.10) means that $x^2 - 4a^2$ (that is $a_4^2 - 4a_8^2$) is a square modulo p and so congruence (4.9) always has a solution and so there is always a QDS of the current form under the conditions in (4.7).

A similar analysis for the case when 2 is a biquadratic residue of p leads to another family of QDS. Here we have

$$\begin{aligned} b_4 &= 2b_8, \\ a_4 + a_8 &= -2 \end{aligned} \tag{4.11}$$

which, it can be proved, gives a QDS for all primes of the form

$$\begin{aligned} p &= x^2 - 8x + 8, \quad x \equiv 1 \pmod 4, \\ y^2 &= 2 - 2x \end{aligned} \tag{4.12}$$

and hence $p = 64z^4 + 48z^2 + 1$ as in the statement of Theorem 4.1. Because $b_4 = 2b_8$ from (4.11), the primitive root g is calculated exactly in the same manner as for when 2 is a biquadratic nonresidue, using (4.9). In this case the sequence of primes starts $p = 113, 1217, 41\,201, 84\,673, 644\,801 \ldots$. The proof of Theorem 4.1 is complete. □

The well known conjectures of Hardy and Littlewood [8] and their vast generalization by Bateman and Horn [1] can be used to estimate the number of primes of the form

$$p = f(z) = 64z^4 + 128z^3 + 144z^2 + 80z + 17 \quad \text{or} \quad p = 64z^4 + 48z^2 + 1$$

which occur in the statement of Theorem 4.1 above. In the case of the first polynomial $f(z)$ the conjecture takes the following explicit form:

$$Q(x) = \#\{n \le x \mid f(n) \text{ is prime}\},$$

$$Q(x) \sim C_f/4 \int_2^x \frac{\mathrm{d}t}{\log t} \quad \text{where}$$

$$C_f = \prod_{p \equiv 1 \pmod 8} \left(1 - \frac{1}{p}\right)\left(1 - \frac{4}{p}\right) \cdot \prod_{p \not\equiv 1 \pmod 8} \left(1 - \frac{1}{p}\right).$$

An evaluation of $C_f/4$ using 10 000 primes gave a value 1.337 92. A more complete set of evaluations is listed in Table 1.

Note that we have used the property, derived heuristically, that $f(z)$ has four solutions modulo a prime p if and only if $p \equiv 1 \pmod 8$.

When we made an explicit count of the number of prime values $p = f(n)$ up to $n = 10^5$ and divided this by the number predicted by Bateman–Horn we obtained the ratio 0.901, showing a degree of feasibility for the conjecture in this case. A set of four evaluations is listed in Table 1.

For brevity, the rest of the results for $n = 8$ are given without the detailed computational proofs. As noted in Theorem 4.1 some of these are simply redefinitions of known QDS or MQDS. The list of QDS discovered for $n = 8$ is given in Table 2. For each case in the table, except for $C = \{0, 1\}$, any primitive root g can be used to generate the set.

TABLE 1. Evaluation of Bateman–Horn predictions for primes of the form $p = 64z^4 + 128z^3 + 144z^2 + 80z + 17$.

Primes	Coefficient	x	Actual/Bateman–Horn
10 000	1.337 92	99 997	0.901 38
11 000	1.338 66	99 998	0.901 37
12 000	1.339 17	99 999	0.901 36
13 000	1.338 85	100 000	0.901 35

TABLE 2. List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n = 8$.

f	C	p	σ	Comments
Even	$\{0, 1\}$	$x^2 + 8x + 8$ $x \equiv 1 \pmod 4$ $y^2 = 2 + 2x$	4	New family of QDS; g determined by (4.8)
Even	$\{0, 1\}$	$x^2 - 8x + 8$ $x \equiv 1 \pmod 4$ $y^2 = 2 - 2x$	4	New family of QDS; g determined by (4.8)
Even or odd	$\{0, 4\}$	$16\alpha^2 + 1$ integer α	2, 6	Isomorphic to QRDS with $n = 4$
Even or odd	$\{0, 4\}_0$	$16\alpha^2 + 9$ integer α	2, 6	Isomorphic to MQRDS with $n = 4$
Even or odd	$\{0, 2, 4, 6\}$	$8\alpha + 1$ integer α	1, 3, 5, 7	Isomorphic to QRDS with $n = 2$
Even or odd	$\{0, 2, 4, 6\}_0$	$8\alpha + 1$ integer α	1, 3, 5, 7	Isomorphic to MQRDS with $n = 2$

5. Results for $n = 4$, $n = 6$ and $n = 10$

An exhaustive computer search for QDS created from unions of cyclotomic classes was also completed for $n = 4$, 6 and 10. The results are discussed in this section. For $n = 4$ and $n = 6$ the following theorem applies.

THEOREM 5.1. *A modified difference set created from the unions of sixth-power cyclotomic classes $C = \{0, 1\}_0$ exists for $p = 13$. All other unions of fourth-power and sixth-power cyclotomic classes are isomorphic to previously known QDS, MQDS or residue difference sets.*

The results for the cases $n = 4$ and $n = 6$ are given in Table 3.

In the case $n = 10$ we have the following theorem.

TABLE 3. List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n=4$ and $n=6$.

n	f	C	p	σ	Comments
4	Even or odd	$\{0, 2\}$	$4\alpha+1$ integer α	1, 3	Isomorphic to QRDS with $n=2$
4	Even or odd	$\{0, 2\}_0$	$4\alpha+1$ integer α	1, 3	Isomorphic to MQRDS with $n=2$
6	Even	$\{0, 1\}_0$	13	3	Single case
6	Even	$\{0, 2, 4\}$	$12\alpha+1$ integer α	1, 3, 5	Isomorphic to QRDS with $n=2$
6	Even	$\{0, 2, 4\}_0$	$12\alpha+1$ integer α	1, 3, 5	Isomorphic to MQRDS with $n=2$
6	Odd	$\{0, 2, 4\}$	$12\alpha+3$ integer α	2, 4	Isomorphic to residue difference set with $n=2$
6	Odd	$\{0, 2, 4\}_0$	$12\alpha+3$ integer α	2, 4	Isomorphic to modified residue difference set with $n=2$

THEOREM 5.2. *Modified residue difference sets created from the unions of tenth-power cyclotomic classes $C=\{0, 2\}_0$ and $C=\{0, 1, 2, 6\}_0$ exist for $p=41$. All other unions of tenth-power cyclotomic classes are isomorphic to previously known QDS, MQDS or residue difference sets.*

The investigation for $n=10$ revealed similar results to $n=6$ and are shown in Table 4. In addition to previously known systems, we have two single cases of MQDS for $n=10$, $p=41$, $f=4$ and $\sigma=5$, namely $t=2$, $C=\{0, 2\}_0$, and $t=4$, $C=\{0, 1, 2, 6\}_0$. In the configuration for $t=4$ any primitive root can be used to generate the MQDS. In the case $t=2$, however, the choice of primitive root is important. In the case $C=\{0, 2\}_0$ we need to use a primitive root g such that $\text{ind}_g 2 \equiv 1$ or 4 (mod 5).

6. Summary

This article describes an exhaustive search for QDS and MQDS composed of unions of cyclotomic classes for powers $n=4$, 6, 8 and 10. For each value of n studied, some cases were discovered that are simply equivalent to known systems, including QRDS, MQRDS and difference sets. In the case $n=4$, no new systems were found. However, there were positive new results for $n=6$, 8 and 10. In the case $n=6$ an isolated system for $p=13$ was found, and for $n=10$, two MQDS, both for $p=41$ were discovered, one consisting of a union of two cyclotomic classes and another of

TABLE 4. List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n = 10$.

f	C	p	σ	Comments
Even	$\{0, 2\}_0$	41	5	Single case with g chosen such that $\mathrm{ind}_g 2 \equiv 1$ or $4 \pmod 5$
Even	$\{0, 1, 2, 6\}_0$	41	5	Single case
Even	$\{0, 2, 4, 6, 8\}$	$20\alpha + 1$ integer α	1, 3, 5, 7, 9	Isomorphic to QRDS with $n = 2$
Even	$\{0, 2, 4, 6, 8\}_0$	$20\alpha + 1$ integer α	1, 3, 5, 7, 9	Isomorphic to MQRDS with $n = 2$
Odd	$\{0, 2, 4, 6, 8\}$	$20\alpha + 3$ integer α	2, 4, 6, 8	Isomorphic to residue difference set with $n = 2$
Odd	$\{0, 2, 4, 6, 8\}_0$	$20\alpha + 3$ integer α	2, 4, 6, 8	Isomorphic to modified residue difference set with $n = 2$

four cyclotomic classes. In the two-class case, the choice of $\mathrm{ind}_g 2$ is important. In the case $n = 8$, two entire families of QDS were discovered, the first for all primes of the form $p = 64z^4 + 128z^3 + 144z^2 + 80z + 17$ and the second for all primes of the form $p = 64z^4 + 48z^2 + 1$ where z is an integer in each case.

Acknowledgements

The authors would like to thank Dr Shaun Cooper and Professor Ron Evans for their help with this article.

Appendix A. Complementary QDS

Consider a QDS R composed of the union of cyclotomic classes derived from $C = \{c_1, c_2, \ldots\}$. Let $A(i)$ be a binary (0, 1) array, defined such that

$$\begin{aligned} A(i) &= 1 \quad \text{if } i \in R, \\ A(i) &= 0 \quad \text{if } i \notin R. \end{aligned} \tag{A.1}$$

Now define another binary (0, 1) array, $G(j)$ such that

$$\begin{aligned} G(j) &= 1 \quad \text{if } j \in mR, \\ G(j) &= 0 \quad \text{if } j \notin mR. \end{aligned} \tag{A.2}$$

By the properties of a QDS we have

$$\sum_{i=0}^{p-1} A(i)G(i + j) = \begin{cases} N_0 & \text{if } j \equiv 0 \pmod p, \\ \lambda & \text{if } j \not\equiv 0 \pmod p) \end{cases} \tag{A.3}$$

where N_0 is the number of zero differences and λ is the number of nonzero differences between the elements of the sets R and mR. (This two-valued correlation function is useful in applications such as image formation [4, 5, 17] signal processing [15] and aperture synthesis [12].) Now, if we let R^* be the complement of R, we now have $R^* = \{Z_p\} - \{R\}$, composed of the residue classes $C^* = \{Z_n\} - \{C\}$ with the residue zero. Here the corresponding sets $A^*(i)$ and $G^*(j)$ are simply obtained by replacing zeroes for ones in (A.1) and (A.2), and *vice versa*. It can be readily seen that this transformation has the effect of simply altering the values of the double summation in (A.3) to give, say, N_0^* and λ^*. Therefore, we now have a MQDS R^*, which is simply the complement of the original QDS, R.

References

[1] P. T. Bateman and R. A. Horn, 'A heuristic asymptotic formula concerning the distribution of prime numbers', *Math. Comp.* **16** (1962), 363–367.

[2] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, 182 (Springer, New York, 1971).

[3] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Canad. Math. Soc. Ser. Monogr. Adv. Texts series, 21 (Wiley, New York, Toronto, 1998).

[4] K. Byard, 'Synthesis of binary arrays with perfect correlation properties – coded aperture imaging', *Nucl. Instrum. Methods Phys. Res. A* **336** (1993), 262–268.

[5] E. Caroli, J. B. Stephen, G. Di Cocco, L. Natalucci and A. Spizzichino, 'Coded aperture imaging in x- and gamma-ray astronomy', *Space Sci. Rev.* **45** (1987), 349–403.

[6] L. E. Dickson, 'Cyclotomy, higher congruences and Waring's problem', *Amer. J. Math.* **57** (1935), 391–424.

[7] M. Hall Jr, 'A survey of difference sets', *Proc. Amer. Math. Soc.* **7** (1956), 975–986.

[8] G. H. Hardy and J. E. Littlewood, 'Some problems of 'Partitio numerorum'; III: on the expression of a number as a sum of primes', *Acta Math.* **44** (1923), 1–70.

[9] H. S. Hayashi, 'Computer investigation of difference sets', *Math. Comp.* **19** (1965), 73–78.

[10] D. Jennings and K. Byard, 'An extension for residue difference sets', *Discrete Math.* **167/168** (1997), 405–410.

[11] ———, 'Qualified residue difference sets with zero', *Discrete Math.* **181** (1998), 283–288.

[12] W. K. Klemperer, 'Very large array configurations for the observation of rapidly varying sources', *Astron. Astrophys. Suppl.* **15** (1974), 449–451.

[13] E. Lehmer, 'On residue difference sets', *Canad. J. Math.* **5** (1953), 425–432.

[14] ———, 'On the number of solutions of $u^k + D \equiv w^2 (\mathrm{mod}\, p)$', *Pacific J. Math.* **5** (1955), 103–118.

[15] H. D. Luke, L. Bomer and M. Antweiler, 'Perfect binary arrays', *Signal Process.* **17** (1989), 69–80.

[16] R. A. Mollin, *Algebraic Number Theory* (Chapman and Hall/CRC, London, 1999).

[17] W. L. Rogers, K. F. Koral, R. Mayans, P. F. Leonard, J. H. Thrall, T. J. Brady and J. W. Keyes, 'Coded aperture imaging of the heart', *J. Nucl. Med.* **21** (1980), 371–378.

KEVIN BYARD, Institute of Information and Mathematical Sciences,
Massey University, Albany, North Shore, Auckland, New Zealand
e-mail: k.byard@massey.ac.nz

KEVIN BROUGHAN, Department of Mathematics, University of Waikato,
Private Bag 3105, Hamilton, New Zealand
e-mail: kab@waikato.ac.nz