#A31 INTEGERS 9 (2009), 401-410

TWELFTH POWER QUALIFIED RESIDUE DIFFERENCE SETS

Kevin Byard
Institute of Information and Mathematical Sciences, Massey University, Albany, North Shore, Auckland, New Zealand
k.byard@massey.ac.nz

Received: 5/16/08, Revised: 2/24/09, Accepted: 3/5/09

Abstract

Qualified residue difference sets of power n are known to exist for $n = 2, 4, 6$, as do similar sets that include the zero element, while both classes of set are known to be nonexistent for $n = 8$ and $n = 10$. Both classes of set are proved nonexistent for $n = 12$.

Keywords: Qualified residue difference sets, difference sets, cyclotomy.

1. Introduction

Qualified residue difference sets are a class of combinatorial configuration, first introduced by Jennings and Byard [6]. These sets are defined as follows.

Definition 1 Let $R = \{r_1, r_2, r_3, \ldots, r_k\}$ be the k-element set of non-zero nth power residues of an odd prime $p = nk + 1$. We call R a *qualified residue difference set* (QRDS) if there exists some non-zero integer $m \notin R$ which is such that if we form all the non-zero differences

$$r_i - mr_j \pmod{p}, \qquad 1 \leq i, j \leq k,$$

we obtain every positive integer $\leq p - 1$ exactly λ times. We call m a *qualifier* of multiplicity λ for the set R.

If zero is counted as a residue we can obtain further qualified residue difference sets. These were also discussed by Jennings and Byard but in a separate paper [7]. These sets are called *modified qualified residue difference sets*, (MQRDS) by virtue of the modification introduced by the inclusion of the zero element. MQRDS are defined as follows.

Definition 2 Let $R^* = \{r_0, r_1, r_2, \ldots, r_k\}$ be the $(k + 1)$-element set of nth power residues of an odd prime $p = nk + 1$, where $r_0 = 0$. We call R^* a modified qualified residue difference set (MQRDS) if there exists some non-zero integer $m \notin R^*$ which is such that if we form all the differences

$$r_i - mr_j \pmod{p}, \qquad 0 \leq i, j \leq k,$$

we obtain every positive integer $\leq p - 1$ exactly λ times and zero exactly once. We call m a *qualifier* of multiplicity λ for the set R^*.

Note in the case of a MQRDS that the integer k is the number of non-zero elements of R^*.

QRDS and MQRDS are related to the normal residue difference sets and modified residue difference sets that were first discussed in detail by Lehmer [9]. All four classes of sets possess similarly attractive properties that suggest potential applications in areas such as image formation [1, 4, 11] signal processing [10] and aperture synthesis [8].

QRDS and MQRDS exist for the cases $n = 2, 4, 6$ [6, 7, 2], while both classes of set are nonexistent for $n = 8$ [2] and $n = 10$ [3]. The purpose of this report is to extend this analysis to $n = 12$ and prove the following theorem:

Theorem 3 *Qualified residue difference sets and modified qualified residue difference sets do not exist for 12th powers.*

2. Preliminary Discussion

In order to study QRDS and MQRDS efficiently, cyclotomy provides a very useful tool. We therefore give a brief outline of the main points of cyclotomy and its link with QRDS and MQRDS.

Let $p = nk + 1$ 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 a:

$$N \equiv g^{an+i} \pmod{p}$$

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

$$g^{an+i} + 1 \equiv g^{bn+j} \pmod{p}$$

where $0 \leq i, j \leq n-1$ and $0 \leq a, b \leq k-1$. See Dickson [5] for an in-depth study of the properties of cyclotomic constants. For both QRDS and MQRDS, the integer k must be even [2, Lemma 3.1], and so for these configurations the following condition, also due to Dickson, always applies [5, p. 394]:

$$(i, j) = (j, i) \text{ if } k \text{ is even.} \tag{1}$$

Let $\sigma \neq 0$ be an integer. We call σ a *definer* if the qualifier m of a QRDS or MQRDS is in residue class $n - \sigma$ [6, 7]. The author has shown that if $n - \sigma$ is a definer, then σ is also a definer [2, Theorem 3.3]. Therefore a qualifier, m, will also belong to residue class σ. Jennings and Byard have also proved the following two existence conditions. Firstly a necessary and sufficient condition for a QRDS to exist is

$$(s, \sigma) = \lambda \quad (s = 0, 1, \ldots, n-1) \tag{2}$$

[6, Theorem 3]. Secondly, a necessary and sufficient condition for a MQRDS to exist is

$$1 + (0, \sigma) = 1 + (\sigma, \sigma) = (s, \sigma) = \lambda \quad (s = 1, 2, \ldots, n-1,\ s \neq \sigma) \tag{3}$$

[7, Theorem 3].

3. Cyclotomy When $n = 12$

To prove Theorem 3 we require the cyclotomic constants for $n = 12$. Following work by Dickson [5], Whiteman has calculated a complete solution for these cyclotomic constants, which he presents in a set of tables in his article [12, p. 69-73]. There are various equalities between the cyclotomic constants of order 12, which Whiteman also lists [12, p.69, Table III], and in particular the condition $(i, j) = (j, i)$ when k is even, as is always the case for QRDS and MQRDS [2, Lemma 3.1].

The tables give results depending on the parity of k, the values of ind $3 \pmod 4$ and ind $2 \pmod 6$ with respect to the primitive root g and prime p (where ind a is defined by $g^{\text{ ind } a} \equiv a \pmod p$), and a variable c which is equal to the ratio of Jacobi sums: $c = \psi(\beta^3, \beta)/\psi(\beta^5, \beta)$ where $\beta = \exp(2\pi i/12)$ is a primitive 12th root of unity [12, p. 64] and $\psi(\beta^\gamma, \beta^\delta) = \sum_{a+b \equiv 1 \pmod p} \beta^{(\gamma \text{ ind } a\ +\delta \text{ ind } b)}$. Whiteman demonstrated that for $n = 12$, c is actually a fourth root of unity and can thus take on values of 1, -1 or β^3. Because for all QRDS and MQRDS k is even, we require from Whiteman tables 1,3,4,7,9 and 10. The parameters ind 2, ind 3 and c for each of Whiteman's tables required in the current analysis are summarised in Table 1.

Table number from Whiteman [12]	ind $3 \pmod 4$	ind $2 \pmod 6$	c
1	2	2	β^3
3	0	2	1
4	0	2	-1
7	2	0	β^3
9	0	0	1
10	0	0	-1

Table 1: Parameters for Whiteman's tables of cyclotomic constants for even k

4. Proof of Theorem 3

The existence of either a QRDS or a MQRDS depends upon the existence of a definer σ ($\neq 0$) for the set that satisfies equation (2) or (3) respectively. If no values of σ satisfy these equations for a given n then nth power QRDS and MQRDS are nonexistent. Here we prove Theorem 3 by demonstrating that no value of σ exists to satisfy equation (2) or (3) for $n = 12$.

The author has shown that if σ is a definer then $-\sigma \equiv n - \sigma \pmod{n}$ is also a definer [2, Theorem 3.3]. Therefore for $n = 12$, it is only necessary to test for $\sigma = 1, 2, 3, 4, 5, 6$. For each of these values of σ a condition is determined from each of Whiteman's tables. We then apply the resulting condition to the following further condition, stipulated by Dickson [5, Theorem 12], that for $n = 12$ the cyclotomic constants depend on the following quadratic partitions:

$$p = x^2 + 4y^2 \text{ and } p = A^2 + 3B^2 \qquad x \equiv 1 \pmod 4,\ A \equiv 1 \pmod 6 \tag{4}$$

where x, y, A, B are all integers.

In the analysis which follows the results $y = 0$ or $B = 0$ or $x = \pm A$ occur frequently. In such cases, the following two lemmas apply.

Lemma 4 *If $y = 0$ or $B = 0$ then QRDS and MQRDS are nonexistent.*

Proof. If $y = 0$ or $B = 0$, then by equation 4 we have $p = x^2$ or $p = A^2$ respectively, both of which are contradictions, since p must be prime. Therefore if $y = 0$ or $B = 0$ there exist no QRDS or MQRDS. □

Lemma 5 *If $x = \pm A$ then QRDS and MQRDS are nonexistent.*

Proof. If $x = \pm A$ then $x^2 = A^2$ and by equation 4 we have $4y^2 = 3B^2$, giving $y = B\sqrt{3}/2$. Now, because $\sqrt{3}$ is irrational, the only integer solution of this last equation is $y = B = 0$, which by Lemma 4 gives a nonexistence condition for QRDS and MQRDS. □

The following subsections present an analysis for each value of σ using each of Whiteman's tables given in Table 1, to establish the nonexistence of QRDS and MQRDS. To simplify the analysis, cyclotomic constants are chosen which can be conveniently applied to both equations (2) and (3) and hence which test for QRDS and MQRDS simultaneously. This is achieved by ensuring that only cyclotomic constants (i, j) that meet the criteria $i \neq 0$, $j \neq 0$ and $i \neq j$ are used in the analysis.

4.1. $\sigma = 1$

(a) Table 1 from Whiteman [12, p.70]. For either equation (2) or (3) to be satisfied (and hence for the existence of QRDS or MQRDS respectively to be possible), a necessary condition is that the cyclotomic constants $(3, 1) = (6, 1)$ (which for even k, is the same as setting $(1, 3) = (1, 6)$). Therefore, using Whiteman's results, we get $p + 1 + 2A - 24B + 8y = p + 1 + 2A + 12B + 8y$. Therefore $B = 0$ and, by Lemma 4, a nonexistence condition results for both QRDS and MQRDS.

(b) Table 3. Setting $(3, 1) = (6, 1)$ (i.e. $(1, 3) = (1, 6)$) gives $p + 1 - 6A + 4x = p + 1 + 6A - 8x$, giving $x = A$ and hence by Lemma 5 a nonexistence condition.

(c) Table 4. $(5,1) = (10,1)$ gives $p+1+4A+12B-6x-24y = p+1+4A+12B-6x+24y$, giving $y = 0$ and by Lemma 4, a nonexistence condition.

(d) Table 7. $(3,1) = (6,1)$ gives $p+1+2A-24B+8y = p+1+2A+12B+8y$, giving $B = 0$ and by Lemma 4, a nonexistence condition.

(e) Table 9. $(2,1) = (3,1)$ gives $p+1+6A-8x = p+1-6A+4x$, giving $x = A$ and by Lemma 5, a nonexistence condition.

(f) Table 10. $(3,1) = (4,1)$ gives $p+1-2A-12B-24y = p+1-2A-12B+24y$, giving $y = 0$ and by Lemma 4, a nonexistence condition.

As the nonexistence of 12th power QRDS and MQRDS has been established for each of the relevant tables from Whiteman's paper, then σ cannot equal 1.

4.2. $\sigma = 2$

(a) Table 1. $(4,2) = (9,2)$ gives $p+1+8A-12B+6x+8y = p+1+8A+24B+6x+8y$, giving $B = 0$ and, by Lemma 4, a nonexistence condition.

(b) Table 3. Setting $(4,2) = (6,2)$ gives $p+1+4A-12B-6x = p+1-8A-12B+6x$, giving $x = A$ and hence by Lemma 5 a nonexistence condition.

(c) Table 4. Whiteman proved that when k is even and ind $3 \equiv 0 \pmod 4$ then the cyclotomic constant (i,j) can be replaced by $(7i,7j)$ except that y is replaced by $-y$ [12, p.71]. We denote this new cyclotomic constant by $(7i,7j)_{-y}$. Therefore we have here $(5,2) = (2,5) = (14,35)_{-y}$ which taken modulo 12 equals $(2,11)_{-y}$ which in turn by Whiteman [12, Table III] equals $(1,3)_{-y}$. Also $(11,2) = (1,3)$. Setting $(5,2) = (11,2)$ is therefore the same as setting $(1,3)_{-y} = (1,3)$. Therefore $p+1-2A-12B+24y = p+1-2A-12B-24y$, giving $y = 0$ and by Lemma 4, a nonexistence condition.

(d) Table 7. $(1,2) = (6,2)$ gives $p+1+2A+8y = p+1+2A+12B+8y$, giving $B = 0$ and by Lemma 4, a nonexistence condition.

(e) Table 9. $(1,2) = (4,2)$ gives $p+1+6A-8x = p+1-2A$, giving $x = A$ and by Lemma 5, a nonexistence condition.

(f) Table 10. $(4,2) = (6,2)$ gives $p+1+6A+8x = p+1+6A+24B+8x$, giving $B = 0$ and by Lemma 4, a nonexistence condition.

Therefore σ cannot equal 2.

4.3. $\sigma = 3$

(a) Table 1. $(1,3) = (6,3)$ gives $p+1+2A-24B+8y = p+1+2A-16y$, giving

$$y = B \tag{5}$$

and $(2,3) = (10,3)$, which from Whiteman [12] is the same as $(1,10) = (2,5)$ gives $p+1-4A-12B-6x-16y = p+1-10A+12B-12x-16y$, giving

$$A + x = 4B. \tag{6}$$

Also, $(5,3) = (11,3)$, which from Whiteman is the same as $(2,9) = (1,4)$ gives $p+1+8A+24B+6x+8y = p+1-4A+12B-6x+32y$, giving

$$A + x + B = 2y. \tag{7}$$

Combining equations (5), (6) and (7) gives the result $B = 0$ and hence, by Lemma 4, a nonexistence condition.

(b) Table 3. $(1,3) = (2,3)$ (i.e. $(1,3) = (1,10)$) gives $p+1-6A+4x = p+1-2x$, giving $x = A$ and hence by Lemma 5 a nonexistence condition.

(c) Table 4. $(6,3) = (11,3)$ (i.e. $(3,6) = (1,4)$) gives $p+1+10A-12x = p+1-8A+6x$, giving $x = A$ and hence by Lemma 5 a nonexistence condition.

(d) Table 7. Whiteman proved that when ind $2 \equiv 0 \pmod 6$ then the cyclotomic constant (i,j) can be replaced by $(5i,5j)$ except that B is replaced by $-B$ [12, p.71-73]. We denote this new cyclotomic constant by $(5i,5j)_{-B}$. Therefore we have here $(7,3) = (35,15)_{-B}$ which taken modulo 12 equals $(11,3)_{-B}$ which in turn by Whiteman [12, Table III] equals $(1,4)_{-B}$. Setting $(1,3) = (7,3)$ is therefore the same as setting $(1,3) = (1,4)_{-B}$. Therefore $p+1+2A-24B+8y = p+1+2A+8y$, giving $B = 0$ and by Lemma 4, a nonexistence condition.

(e) Table 9. $(1,3) = (6,3)$ gives $p+1-6A+4x = p+1-2x$, giving $x = A$ and by Lemma 5, a nonexistence condition.

(f) Table 10. Setting $(1,3) = (11,3)$ is, from Whiteman [12, Table III], the same as setting $(1,3) = (1,4)$, or $(3,1) = (4,1)$, as for the case $\sigma = 1$, which was proved to give a nonexistence condition.

Therefore σ cannot equal 3.

4.4. $\sigma = 4$

(a) Table 1. $(5,4) = (11,4)$ (i.e. $(1,8) = (1,5)$) gives $p+1+8A+12B+6x-16y = p+1-8A+12B+6x$ giving

$$y = A \tag{8}$$

and $(5,4) = (6,4)$ (i.e. $(1,8) = (2,8)$) gives $p+1+8A+12B+6x-16y = p+1+2A+12B+8y$, giving

$$A + x = 4y. \tag{9}$$

Also, $(6,4) = (8,4)$ (i.e. $(2,8) = (4,8)$) gives $p+1+2A+12B+8y = p+1+16A+12B-18x-24y$, giving

$$9x + 16y = 7A. \tag{10}$$

Combining equations (8), (9) and (10) gives the result $y = 0$ and hence, by Lemma 4, a nonexistence condition.

(b) Table 3. $(2,4) = (10,4)$ is, from Whiteman, the same as setting $(2,4) = (2,6)$, or $(4,2) = (6,2)$, as for the case $\sigma = 2$, which was proved to give a nonexistence condition.

(c) Table 4. $(8,4) = (10,4)$ (i.e. $(4,8) = (2,6)$) gives $p + 1 + 4A + 12B - 6x = p + 1 + 12B + 14x$, giving

$$A = 5x \tag{11}$$

and $(1,4) = (2,4)$ gives $p + 1 - 8A + 6x = p + 1 + 12A - 12B + 2x$ giving

$$3B + x = 5A. \tag{12}$$

Also note from Whiteman [12, Table III] that $(5,4)$ is equivalent to $(1,8)$ which becomes $(7,56)_{-y} = (7,8)_{-y} = (1,5)_{-y}$, and that $(9,4)$ is equivalent to $(3,7)$ which becomes $(21,49)_{-y}$, or $(9,1)_{-y}$. Therefore, setting $(5,4) = (9,4)$ is the same as setting $(1,5)_{-y} = (1,9)_{-y}$ which gives $p+1+4A+12B-6x+24y = p+1-2A-12B+24y$, giving

$$A + 4B = x. \tag{13}$$

Combining equations (11), (12) and (13) gives the result $B = 0$ and hence, by Lemma 4, a nonexistence condition.

(d) Table 7. Note from Whiteman [12, Table III] that $(6,4)$ is equivalent to $(2,8)$ which becomes $(10,40)_{-B} = (10,4)_{-B} = (2,6)_{-B}$, and that $(10,4)$ is equivalent to $(2,6)$. Therefore, setting $(6,4) = (10,4)$ is the same as setting $(2,6)_{-B} = (2,6)$ which gives $p+1+2A-12B+8y = p+1+2A+12B+8y$, giving $B = 0$ and hence by Lemma 4, a nonexistence condition.

(e) Table 9. $(1,4) = (2,4)$ gives $p+1+2A-4x = p+1-2A$, giving $x = A$ and by Lemma 5, a nonexistence condition.

(f) Table 10. $(2,4) = (8,4)$ gives $p+1+6A+8x = p+1-26A-24x$, giving $x = -A$ and by Lemma 5, a nonexistence condition.

Therefore σ cannot equal 4.

4.5. $\sigma = 5$

(a) Table 1. $(3,5) = (6,5)$ (i.e. $(2,9) = (1,7)$) gives $p+1+8A+24B+6x+8y = p+1+8A-12B+6x+8y$ giving $B = 0$ and hence, by Lemma 4, a nonexistence condition.

(b) Table 3. $(6,5) = (11,5)$ (i.e. $(1,7) = (1,6)$) gives $p+1+12A-14x = p+1+6A-8x$ giving $x = A$ and hence, by Lemma 5, a nonexistence condition.

(c) Table 4. Note that $(4,5)$ is equal to $(1,8) = (7,56)_{-y} = (7,8)_{-y} = (1,5)_{-y}$. Therefore, setting $(1,5) = (4,5)$ is the same as setting $(1,5) = (1,5)_{-y}$. Therefore $p+1+4A+12B-6x-24y = p+1+4A+12B-6x+24y$, giving $y = 0$ and hence, by Lemma 4, a nonexistence condition.

(d) Table 7. $(4,5) = (11,5)$ (i.e. $(1,8) = (1,6)$) gives $p+1+2A+8y = p+1+2A+12B+8y$, giving $B = 0$ and hence by Lemma 4, a nonexistence condition.

(e) Table 9. $(1,5) = (11,5)$ (i.e. $(1,5) = (1,6)$) gives $p+1-10A+8x = p+1+6A-8x$, giving $x = A$ and by Lemma 5, a nonexistence condition.

(f) Table 10. $(1,5) = (11,5)$ (i.e. $(1,5) = (1,6)$) gives $p+1-2A = p+1-2A+24B$, giving $B = 0$ and by Lemma 4, a nonexistence condition.

Therefore σ cannot equal 5.

4.6. $\sigma = 6$

(a) Table 1. $(4,6) = (5,6)$ (i.e. $(2,8) = (1,7)$) gives $p+1+2A+12B+8y = p+1+8A-12B+6x+8y$ giving

$$4B = x + A. \tag{14}$$

Also $(2,6) = (1,6)$ gives $p+1-4A-6x+8y = p+1+2A+12B+8y$, giving

$$2B + A + x = 0. \tag{15}$$

Combining equations (14) and (15) gives $B = 0$ and hence, by Lemma 4, a nonexistence condition.

(b) Table 3. $(1,6) = (3,6)$ gives $p+1+6A-8x = p+1-6A+4x$, giving $x = A$ and hence by Lemma 5, a nonexistence condition.

(c) Table 4. $(3,6) = (4,6)$ (i.e. $(3,6) = (2,8)$) gives $p+1+10A-12x = p+1+6A+8x$ giving

$$A = 5x \tag{16}$$

and $(1,6) = (5,6)$ (i.e. $(1,6) = (1,7)$) gives $p+1-2A+24B = p+1+4A-24B-6x$ giving

$$8B + x = A. \tag{17}$$

Also, $(2,6) = (1,6)$ gives $p+1+12B+14x = p+1-2A+24B$ giving

$$7x + A = 6B. \tag{18}$$

Combining equations (16), (17) and (18) gives $B = 0$ and hence, by Lemma 4, a nonexistence condition.

(d) Table 7. Note that $(5,6)$ is equal to $(1,7) = (5,35)_{-B} = (5,11)_{-B} = (1,6)_{-B}$. Therefore, setting $(1,6) = (5,6)$ is the same as setting $(1,6) = (1,6)_{-B}$. Therefore $p+1+2A+12B+8y = p+1+2A-12B+8y$, giving $B = 0$ and hence, by Lemma 4, a nonexistence condition.

(e) Table 9. $(1,6) = (2,6)$ gives $p+1+6A-8x = p+1-2A$, giving $x = A$ and by Lemma 5, a nonexistence condition.

(f) Table 10. $(1,6) = (2,6)$ gives $p+1-2A+24B = p+1+6A+24B+8x$, giving $x = -A$ and by Lemma 5, a nonexistence condition.

Therefore σ cannot equal 6.

As $\sigma \neq 1, 2, 3, 4, 5$ or 6 the non-existence of QRDS and MQRDS for 12th powers is established and so Theorem 3 is proved. □

Acknowledgement The author would like to thank Dr Shaun Cooper for his help during the preparation of this paper.

References

[1] K. Byard, Synthesis of Binary Arrays with Perfect Correlation Properties - Coded Aperture Imaging, *Nucl. Instrum. Meth. Phys. Res.* A336 (1993) 262-268.

[2] K. Byard, On Qualified Residue Difference Sets, *Int. J. Number Theory.* 2 (2006) 591–597.

[3] K. Byard, Tenth Power Qualified Residue Difference Sets. To Appear in *Int. J. Number Theory.*.

[4] E. Caroli, J.B. Stephen, G. Di Cocco, L. Natalucci and A. Spizzichino, Coded Aperture Imaging in X- and Gamma-Ray Astronomy, *Spa. Sci. Rev.* 45 (1987) 349-403.

[5] L.E. Dickson, Cyclotomy, Higher Congruences and Warings Problem, *Am. J. Math.* 57 (1935) 391–424.

[6] D. Jennings and K. Byard, An Extension for Residue Difference Sets, *Discrete Math.* 167/168 (1997) 405–410.

[7] D. Jennings and K. Byard, Qualified Residue Difference Sets with Zero, *Discrete Math.* 181 (1998) 283–288.

[8] W.K. Klemperer, Very Large Array Configurations for the Observation of Rapidly Varying Sources, *Astron. Astrophys. Suppl.* 15 (1974) 449-451.

[9] E. Lehmer. On Residue Difference Sets, *Can. J. Math.* 5 (1953) 425-432.

[10] H.D. Luke, L. Bomer and M. Antweiler, Perfect Binary Arrays, *Signal Processing* 17 (1989) 69-80.

[11] 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.

[12] A.L. Whiteman, The Cyclotomic Numbers of Order Twelve, *Acta Arithmetica* 6 (1960) 53–76.