Qualified Difference Sets

A thesis presented in partial fulfilment of the requirements for the degree of
Doctor of Philosophy
in
Mathematics
at Massey University, Albany,
New Zealand.

by

Kevin Byard
2009

Abstract

Qualified difference sets are a class of combinatorial configuration. The sets are related to the residue difference sets that were first discussed in detail in 1953 by Emma Lehmer. Qualified difference sets consist of a set of residues modulo an integer v and they possess attractive properties that suggest potential applications in areas such as image formation, signal processing and aperture synthesis. This thesis outlines the theory behind qualified difference sets and gives conditions for the existence and nonexistence of these sets in various cases.

A special case of the qualified difference sets is the qualified *residue* difference sets. These consist of the set of nth power residues of certain types of prime. Necessary and sufficient conditions for the existence of qualified residue difference sets are derived and the precise conditions for the existence of these sets are given for $n = 2$, 4 and 6. Qualified residue difference sets are proved nonexistent for $n = 8$, 10, 12, 14 and 18.

A generalisation of the qualified residue difference sets is introduced. These are the qualified difference sets composed of unions of cyclotomic classes. A cyclotomic class is defined for an integer power n and the results of an exhaustive computer search are presented for $n = 4$, 6, 8, 10 and 12. Two new families of qualified difference set were discovered in the case $n = 8$ and some isolated systems were discovered for $n = 6$, 10 and 12.

An explanation of how qualified difference sets may be implemented in physical applications is given and potential applications are discussed.

Acknowledgements

This thesis has been made possible with the help of many individuals.

Firstly I would like to thank my supervisor, Dr Shaun Cooper, who has provided excellent support in this work. I greatly appreciate his decision to accept my initial research proposal. He has always been very generous with his time and I am also thankful for his patient attention to my many enquiries. I have also learned much from him, not only in the field of mathematics, but also in the many and varied facets of mathematical research at the academic level. Thanks are also due to my co-supervisor, Dr Kevin Broughan, who has similarly provided much academic support in the form of collaborative work and also fielded many of my questions on number theory. I would also like to thank Professor Ron Evans, a man I hope one day to meet. Through the modern-day medium of e-mail he has acted as a virtual third supervisor, not only answering some difficult questions but also suggesting our collaboration on an article. I thank him, not only for his extraordinary insight, but also his good humour.

Thanks are also due to Dr Derek Jennings for his collaboration in much of the early work of this thesis, to Professor Joseph Muskat for his help regarding the cyclotomic constants of order fourteen, and to David Culliford for his helpful assistance with my first successful publication since commencing formal study into this work. Also deserving of a mention are Drs Joanne Mann and Sharleen Harper, fellow students with whom I have shared not only an office, but also many ideas, resources and laughs. I also acknowledge the generous financial support of NZIAS at Massey University as well as the IT staff who have always provided fast and efficient technical support.

In such a work there are many people who provide support that, though non-academic, is no less important. Above all of these I thank Vicki, my partner and the mother of my son Shaun. She has demonstrated remarkable patience during my studies and she is one of those rare individuals who not only understands a mathematician's need to do their mathematics, but allows them the time and space to do it. Thank you Vicki, you are one of a kind. I also thank Flossy, who has often provided much needed distraction during the hard work. Finally, I thank my Mum, Dad and sister Tracey, who have been as supportive during this work as they always have.

This one's for me.

Contents

List of Figures

List of Tables

Chapter 1

Overview

Qualified difference sets (QDS) are a class of combinatorial configurations that are related to the normal residue difference sets (RDS) that were first discussed in detail by Lehmer [47, pp. 425-430]. If zero is included as an element in the QDS, we have modified qualified difference sets (MQDS), which are similarly related to the modified residue difference sets (MRDS), also discussed by Lehmer [47, pp. 431-432]. All four classes of set possess similarly attractive properties that suggest potential applications in areas such as image formation, signal processing and aperture synthesis.

Different applications require different parameters of these sets. For example, high energy astronomy uses an image formation technique called coded aperture imaging [23, 29], whereby radiation from a high energy source passes through holes in an aperture made of opaque material and lands on a position sensitive radiation detector. The transparency of any aperture (i.e. the ratio of the total area of holes to the entire aperture area) depends on the parameters of the set from which the aperture is generated. For most high energy telescopes, apertures of 50% transparency have been used [56, 69, 70], although other transparencies have been proposed to aid physical construction of the aperture [15, 33]. Accorsi et al. have investigated the use of the coded aperture technique in medical imaging, concluding that in certain circumstances a lower transparency aperture is the best compromise between instrument sensitivity and practical construction constraints [1].

The rationale behind this thesis is to introduce QDS and MQDS and hence increase the range of parameters available for use in physical applications. In it we discuss QDS and MQDS, including their existence and applications. In Chapter 2 we relate QDS and MQDS to RDS and MRDS respectively, giving some necessary definitions. We present a historical discussion of the RDS and MRDS and we discuss the current research position of these sets. We also outline some of the necessary theory of cyclotomy required in many of the proofs in the thesis. In Chapter 3 we discuss the special cases of the qualified residue difference sets (QRDS) and similar sets that include the zero element called the modified qualified residue difference sets (MQRDS). Using cyclotomy with respect to the integer power n, we present necessary and sufficient conditions for the existence of both

types of set. In Chapter 4 we provide precise conditions for the existence of both QRDS and MQRDS for $n = 2$, 4 and 6, and in Chapter 5 we prove the nonexistence of both types of set for $n = 8$, 10, 12, 14 and 18.

In Chapter 6 we discuss QDS and MQDS that are created from the unions of cyclotomic classes. We provide necessary definitions and discuss the existence of such sets for the values $n = 4$, 6, 8, 10 and 12.

In Chapter 7 we discuss the possible applications of QDS and MQDS and in Chapter 8 we summarise the thesis and the findings in it.

Some of the results in this thesis have been published elsewhere as follows: Sections 3.2, 4.2, 4.3 and 4.4 are in [40], [41] and [17]; Section 5.2 is in [17]; Section 5.3 is in [18]; Section 5.4 is in [19]; Sections 5.5 and 5.6 are in [21]; Chapter 6 is in [20].

Chapter 2

Difference Sets and Qualified Difference Sets

2.1 Difference Sets

Difference sets are a class of combinatorial configurations. Each difference set is associated with three main parameters, v, k, λ, and for this reason they are sometimes also referred to as (v, k, λ) difference sets. In the case when v is an odd prime we will use the symbol p instead of v. First we require the following preliminary definition.

Definition 2.1 *Let N be a positive integer. We define the sets $\mathbb{Z}_N$ and $\mathbb{Z}_N^+$ as follows:*

$$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\} \tag{2.1}$$

$$\mathbb{Z}_N^+ = \mathbb{Z}_N - \{0\} = \{1, 2, \ldots, N-1\}. \tag{2.2}$$

Then the set $\mathbb{Z}_N$ is a group under addition modulo N. The set $\mathbb{Z}_N^+$ is not a group under addition modulo N, but it is a group under multiplication modulo N if and only if N is prime.

Difference sets are defined as follows.

Definition 2.2 *Let v, k and λ be positive integers. A (v, k, λ) difference set $D = \{a_1, a_2, a_3, \ldots, a_k\}$ is a set of k residues modulo v, such that for each $d \in \mathbb{Z}_v^+$ the congruence*

$$a_i - a_j \equiv d \pmod{v} \qquad\qquad 1 \leq i, j \leq k,\ (i \neq j)$$

has exactly λ solution pairs $a_i, a_j \in D$. The integer v is called the modulus, k is called the size and λ is called the multiplicity of the set D.

There is evidently a relationship between the parameters v, k and λ of a difference set that arises due to the *incidences* of occurrence of each non-zero difference. As an immediate

consequence of Definition 2.2 we obtain the following equation, which we refer to as the *incidence relation* for a given difference set:

$$k(k-1) = \lambda(v-1). \tag{2.3}$$

This arises from the fact that there are $k(k-1)$ non-zero differences and each non-zero difference occurs exactly λ times. An example is the $(15, 7, 3)$ difference set given by:

$$D_{15} = \{1, 2, 3, 5, 6, 9, 11\} \pmod{15}.$$

Each non-zero difference modulo 15 occurs three times, for example the difference 5 arises from $6-1$, $11-6$ and $1-11 \pmod{15}$. Therefore $\lambda = 3$. Note that the values $(v, k, \lambda) = (15, 7, 3)$ satisfy (2.3). Note also that the condition in Equation (2.3) does not guarantee the existence of a difference set. For example, the parameters $(v, k, \lambda) = (16, 6, 2)$ satisfy (2.3) but do not give rise to a difference set.

There are a number of obvious difference sets that are generally of little interest. These are discussed by Baumert [8, pp. 1-2] and include the following;

1. The empty set: $D = \{\}$; $k = \lambda = 0$.
2. All single element sets: $D = \{i\}$; $0 \leq i \leq v-1$, $k = 1$, $\lambda = 0$.
3. The complete set of residues modulo v: $D = \{0, 1, 2, \ldots, v-1\}$; $v = k = \lambda$.
4. The complete set of residues modulo v, minus the element i: $D = \{0, 1, 2, \ldots, i-1, i+1, \ldots, v-1\}$; $0 \leq i \leq v-1$, $k = v-1$, $\lambda = v-2$.

These are called *trivial* difference sets and are often either ignored or treated as only limiting cases. From the incidence relation (2.3), trivial difference sets arise if and only if the quantity $k - \lambda$ equals either zero or unity. Therefore if a (v, k, λ) difference set exists then it is non-trivial if and only if

$$k - \lambda \geq 2. \tag{2.4}$$

In many discussions about difference sets in the literature, the assumption in Equation (2.4) is often made implicitly. The definitive work on difference sets is the book by Baumert [8] although other works of note include papers by Hall [36] and Baumert [7].

A subclass of (v, k, λ) difference sets are the *nth power residue difference sets* (RDS). In 1953, Lehmer presented a detailed discussion of RDS [47]. A RDS of order n is defined as follows.

Definition 2.3 *Let n and k be positive integers and suppose $p = nk + 1$ is prime. Let $D = \{r_1, r_2, r_3, \ldots, r_k\}$ be the set of nth power residues of p. The set D is called an nth power residue difference set with k elements, RDS for short, if, when we form all the $k(k-1)$ non-zero differences*

$$r_i - r_j \pmod{p} \qquad 1 \leq i, j \leq k, \ (i \neq j) \tag{2.5}$$

we obtain every element of $\mathbb{Z}_p^+$ exactly λ times. The prime p is called the modulus, k is called the size and λ is called the multiplicity, of the set D.

Note from the earlier discussion on trivial difference sets that a non-trivial RDS also requires n to be greater than unity. An example of a non trivial RDS is the following.

Example 2.4 *The parameters $n = 4$, $k = 9$ yield a fourth power RDS with nine elements. For $p = nk + 1 = 37$ is prime the incidence relation (2.3) implies $\lambda = 2$. Indeed, for the set*

$$\begin{aligned} D &= \{a \in \mathbb{Z}_{37}^+ : a = x^4 \text{ for some } x \in \mathbb{Z}_{37}^+\} \\ &= \{1, 7, 9, 10, 12, 16, 26, 33, 34\}, \end{aligned}$$

each non-zero difference occurs $\lambda = 2$ times.

An example of a set of parameters n, p, k, λ that obey the incidence relation (2.3) but do not yield a RDS is as follows.

Example 2.5 *The parameters $n = 4$, $k = 13$ do not yield a fourth power RDS with 13 elements.*
For $p = nk + 1 = 53$ is prime the incidence relation (2.3) would imply $\lambda = 3$. But, for the set

$$\begin{aligned} D &= \{a \in \mathbb{Z}_{53}^+ : a = x^4 \text{ for some } x \in \mathbb{Z}_{53}^+\} \\ &= \{1, 10, 13, 15, 16, 24, 28, 36, 42, 44, 46, 47, 49\} \end{aligned}$$

the difference 1 occurs twice ($16 - 15$ and $47 - 46$) while the difference 2 occurs four times ($15 - 13$, $44 - 42$, $46 - 44$ and $49 - 47$). Therefore, the differences do not occur the same number of times and hence there is no difference set in this case.

Chowla demonstrated that a fourth power RDS exists if and only if k is an odd square [24].

In her article, Lehmer also points out that similar sets exist if zero is counted as a residue [47, p. 431]. These are called *nth power modified residue difference sets*, by virtue of the modification introduced by the inclusion of the zero element. The definition of a modified residue difference set is as follows.

Definition 2.6 *Let n and k be positive integers and suppose $p = nk + 1$ is prime. Let $D^* = \{r_0, r_1, r_2, \ldots, r_k\}$ be the set of nth power residues of p where $r_0 = 0$. The set D^* is called an nth power modified residue difference set with $k + 1$ elements, MRDS for short, if, when we form all the $k(k + 1)$ non-zero differences*

$$r_i - r_j \pmod{p} \qquad 0 \leq i, j \leq k, \ (i \neq j) \tag{2.6}$$

we obtain every element of $\mathbb{Z}_p^+$ exactly λ times. The prime p is called the modulus, k is called the size and λ is called the multiplicity of the set D^*.

In this case the parameters have the following incidence relation:

$$k(k + 1) = \lambda(v - 1). \tag{2.7}$$

An example of a non trivial MRDS is the following.

Example 2.7 *The parameters $n = 4$, $k = 3$ yield a fourth power MRDS with four elements.*
For $p = nk + 1 = 13$ is prime the incidence relation (2.7) implies $\lambda = 1$. Indeed, for the set

$$\begin{aligned} D &= \{a \in \mathbb{Z}_{13}^{+} : a = x^4 \text{ for some } x \in \mathbb{Z}_{13}^{+}\} \cup \{0\} \\ &= \{0, 1, 3, 9\}, \end{aligned}$$

each non-zero difference occurs exactly once, so $\lambda = 1$.

2.2 Existence of RDS and MRDS

RDS and MRDS are subclasses of difference sets, of which there has been much study and research. These sets have come in for special attention, mainly as a result of their ease of construction. The definitive work on RDS and MRDS is by Lehmer [47] although the article by Storer also gives extensive results on both types of set via the theory of cyclotomy [60], and Berndt, Evans and Williams provide alternative proofs of many of the associated theorems using Gauss sums [10, Chapter 5]. We present the known results as a series of theorems.

Theorem 2.8 (Lehmer [47]) *There exist no nth power RDS or MRDS for odd values of n.*

Lehmer provides a full proof of the nonexistence of RDS for odd n. She attributes the nonexistence condition for MRDS to Hall without a clear citation, although a proof is given by Baumert [8, Theorem 5.17]. Therefore for RDS and MRDS we are restricted to studying cases when n is even.

Theorem 2.9 (Paley [55]) *RDS for $n = 2$ exist if and only if $p = 4x - 1$ is a prime and x is a positive integer.*

Theorem 2.10 (Baumert [8]) *MRDS do not exist for $n = 2$.*

Theorem 2.11 (Chowla [24]) *RDS for $n = 4$ exist if and only if $p = 4x^2 + 1$ is a prime and x is an odd integer.*

Chowla proved Theorem 2.11 using results of cyclotomy from Bachmann [2]. Lehmer generalised the results in Theorems 2.9, 2.10 and 2.11, and outlined the necessary and sufficient conditions for the existence of both RDS and MRDS [47, Theorems III and III']. She was therefore able to prove further results. Again she attributes the following theorem for a MRDS with $n = 4$ to Hall without citation.

Theorem 2.12 (Lehmer [47]) *MRDS for $n = 4$ exist if and only if $p = 4x^2 + 9$ is a prime and x is an odd integer.*

In the case $n = 6$ Lehmer proved the following

Theorem 2.13 (Lehmer [47]) *RDS and MRDS for $n = 6$ are nonexistent.*

and for $n = 8$ she proved the following

Theorem 2.14 (Lehmer [47]) *RDS for $n = 8$ exist if and only if p is a prime of the form $p = 8x^2 + 1 = 64y^2 + 9$ where x and y are both odd integers. MRDS for $n = 8$ exist if and only if p is a prime of the form $p = 8x^2 + 49 = 64y^2 + 441$ where x is an odd integer and y is an even integer.*

In her paper the final result for MRDS in Theorem 2.14 is incorrectly quoted [47, p. 432]. Correctly quoted results for MRDS with $n = 8$ are provided by Storer [60, p. 81, Theorem 19'], Baumert [8, p. 124] and Berndt et al. [10, p. 179, Theorem 5.3.6(b)].

For higher values of n no further RDS or MRDS have yet been found. For $n = 10$, Lehmer proved the nonexistence of RDS for the case when 2 is a 5th power residue of the prime modulus p [47, p. 430]. The final existence question for $n = 10$ for both RDS and MRDS was solved by Whiteman.

Theorem 2.15 (Whiteman [67]) *RDS and MRDS for $n = 10$ are nonexistent.*

We also have the following theorems

Theorem 2.16 (Whiteman [68]) *RDS and MRDS for $n = 12$ are nonexistent.*

Theorem 2.17 (Muskat [52]) *RDS and MRDS for $n = 14$ are nonexistent.*

In the case $n = 16$ Whiteman used cyclotomy to provide a partial solution by proving that both RDS and MRDS are nonexistent if 2 is an octic (8th power) residue of p [66]. The full proof for $n = 16$ was completed by Evans using Gauss sums [26].

Theorem 2.18 (Evans [26]) *RDS and MRDS for $n = 16$ are nonexistent.*

We also have a full solution in the following case.

Theorem 2.19 (Baumert and Fredricksen [5]) *RDS and MRDS for $n = 18$ are nonexistent.*

For $n = 20$ Muskat and Whiteman proved the nonexistence of both RDS and MRDS when 5 is a biquadratic residue of p [53]. The final solution was provided by Evans.

Theorem 2.20 (Evans [28]) *RDS and MRDS for $n = 20$ are nonexistent.*

For $n = 22$ and $n = 24$ partial solutions exist.

Theorem 2.21 (Muskat [52]) *RDS and MRDS for $n = 22$ are nonexistent if 2 is an eleventh power residue of p.*

Theorem 2.21 is a special case of the following neat theorem of Muskat.

Theorem 2.22 (Muskat [52]) *There exist no nth power RDS or MRDS when* $n \equiv 6 \pmod 8$ *and* 2 *is an* $(n/2)$*th power residue of* p*.*

Theorem 2.23 (Evans [27]) *For* $n = 24$ *RDS and MRDS do not exist if either* 2 *is a cubic residue of* p *or if* 3 *is a biquadratic residue of* p*.*

In a separate article Berndt and Evans claim that the remaining cases for $n = 24$ could '... undoubtedly be settled using the formula for G_{24} [the Gauss sums of order 24] ...' but they concede that the calculations would appear to be very laborious [9, p. 350].

In an interesting recent incident, Ott published an article claiming to prove that the order n of RDS and MRDS must be a power of 2 [54, Theorem 1]. However, Ott's result was subsequently refuted by Yuan and Yahui [72].

Summaries of the existence conditions for RDS and MRDS are given in Tables 2.1 and 2.2 respectively.

n	RDS exist if and only if	Conditions	References
2	$p = 4x - 1$	x integer	Paley [55]
4	$p = 4x^2 + 1$	x odd	Chowla [24]
6	Nonexistent		Lehmer [47]
8	$p = 8x^2 + 1 = 64y^2 + 9$	x, y odd integers	Lehmer [47]
10	Nonexistent		Lehmer [47], Whiteman [67]
12	Nonexistent		Whiteman [68]
14	Nonexistent		Muskat [52]
16	Nonexistent		Whiteman [66], Evans [26]
18	Nonexistent		Baumert & Fredricksen [5]
20	Nonexistent		Evans [28]
22	Nonexistent	2 is 11th power residue of p	Muskat [52]
24	Nonexistent	2 is cubic residue or 3 is biquadratic residue of p	Evans [27]

Table 2.1: Parameters for the existence of RDS.

n	MRDS exist if and only if	Conditions	References
2	Nonexistent		Baumert [8]
4	$p = 4x^2 + 9$	x odd	Lehmer [47]
6	Nonexistent		Lehmer [47]
8	$p = 8x^2 + 49 = 64y^2 + 441$	x odd, y even	Lehmer [47]
10	Nonexistent		Whiteman [67]
12	Nonexistent		Whiteman [68]
14	Nonexistent		Muskat [52]
16	Nonexistent		Whiteman [66], Evans [26]
18	Nonexistent		Baumert & Fredricksen [5]
20	Nonexistent		Evans [28]
22	Nonexistent	2 is 11th power residue of p	Muskat [52]
24	Nonexistent	2 is cubic residue or 3 is biquadratic residue of p	Evans [27]

Table 2.2: Parameters for the existence of MRDS.

2.3 Qualified Difference Sets

In this thesis an extension to the RDS and MRDS is introduced in the form of two new types of set. These we call *qualified difference sets* and *modified qualified difference sets*. We define the qualified difference sets as follows.

Definition 2.24 *Let k be a positive integer and $R = \{r_1, r_2, r_3, \ldots, r_k\} \subset \mathbb{Z}_v^+$ be a k-element set of distinct non-zero residues modulo an integer v. We call R a qualified difference set, QDS for short, if there exists some non-zero integer m, $0 < m < v$, which is such that*

1. $$mr_j \notin R, \quad 1 \leq j \leq k \tag{2.8}$$

2. *if we form all the k^2 non-zero differences*

$$r_i - mr_j \pmod{v} \tag{2.9}$$

we obtain every element of $\mathbb{Z}_v^+$ exactly λ times and we do not obtain zero. The integer v is called the modulus, k is called the size and λ is the multiplicity of the set R. We call m a qualifier of R.

Note that the condition $mr_j \notin R$ implies that $m = 1$ is not a qualifier, since we would then obtain exactly k zero differences, whereas Definition 2.24 specifies that the differences must

all be non-zero. If zero is counted as a residue, we can obtain *modified qualified difference sets*, by virtue of the modification introduced by the inclusion of the zero element. We define these sets as follows.

Definition 2.25 *Let $R = \{r_1, r_2, r_3, \ldots, r_k\} \subset \mathbb{Z}_v^+$ be a k-element set of distinct non-zero residues modulo an integer v. Let $r_0 = 0$ and define $R^* = R \cup \{r_0\}$. We call R^* a modified qualified difference set, MQDS for short, if there exists some non-zero integer m, $0 < m < v$, which is such that*

1.

$$mr_j \notin R, \quad 0 \leq j \leq k \tag{2.10}$$

2. if we form all the $(k+1)^2$ non-zero differences

$$r_i - mr_j \pmod{v} \tag{2.11}$$

we obtain every element of $\mathbb{Z}_v^+$ exactly λ times and zero exactly once. The integer v is called the modulus, k is called the size and λ is the multiplicity of the set R^*. We call m a qualifier of R^*.

Note the single occurrence of the zero difference for a MQDS. This results from the point that from (2.11) we have firstly $r_0 - mr_0 = 0$ (giving the single zero difference) and secondly $mr_j \notin R$, which means that another zero difference cannot occur. As above, $m = 1$ cannot be a qualifier, since we would then obtain exactly $k+1$ zero differences, whereas Definition 2.25 specifies that the zero difference occurs exactly once.

As for difference sets, the parameters of QDS and MQDS are related by an incidence relation. This is given by the following lemma.

Lemma 2.26 *For a QDS of k elements and modulus v we have the following incidence relation*

$$k^2 = \lambda(v-1) \tag{2.12}$$

and for a MQDS of $k+1$ elements and modulus v we have the incidence relation

$$(k+1)^2 = 1 + \lambda(v-1). \tag{2.13}$$

Proof. For a QDS of k elements there are k^2 possible non-zero differences, and each non-zero difference modulo v occurs exactly λ times, giving (2.12). For a MQDS, there are $k+1$ elements (including zero), and hence $(k+1)^2$ possible differences. The zero difference occurs exactly once and each non-zero difference modulo v occurs exactly λ times, giving (2.13). □

The following lemma is presented to avoid ambiguity in Chapter 5 (Lemma 5.2).

		r_j			
		1	4	13	16
	1	16	10	9	3
r_i	4	2	13	12	6
	13	11	5	4	15
	16	14	8	7	1

Table 2.3: Table showing $r_i - 2r_j \pmod{17}$.

Lemma 2.27 *If $R = \{r_1, r_2, \ldots, r_k\}$ is a QDS then $R^* = R \cup \{0\}$ is not a MQDS and if $R^* = R \cup \{0\}$ is a MQDS then R is not a QDS.*

Proof. If R is a QDS and R^* is a MQDS then by Equations (2.12) and (2.13) we obtain $k = 0$, which contradicts that k is a positive integer. □

When the modulus v is odd the following lemmas apply for QDS and MQDS.

Lemma 2.28 *For all QDS and MQDS, if the modulus v is odd, then k must be even.*

Proof. This is immediate from Lemma 2.26. □

The simplest QDS and MQDS are those composed of the nth power residues of certain types of prime p, and having analogous properties to the RDS and MRDS respectively. These are called *qualified residue difference sets* and *modified qualified residue difference sets*, the word 'residue' being incorporated to notify that the sets are composed of nth power residues. The QRDS are defined for modulus p as follows.

Definition 2.29 *Let n and k be positive integers and suppose $p = nk+1$ is an odd prime. Let $R = \{r_1, r_2, r_3, \ldots, r_k\}$ be the k-element set of non-zero nth power residues of p. We call R an nth power qualified residue difference set with k elements, QRDS for short, if R is a QDS.*

An example of a QRDS is the following.

Example 2.30 *The parameters $n = 4$, $k = 4$ and $p = nk + 1 = 17$ yield a QRDS. The complete list of possible qualifiers is $m = 2$, 8, 9 and 15.*
For $p = 17$ is prime, the incidence relation (2.12) implies $\lambda = 1$. We obtain the set

$$\begin{aligned} R &= \{r \in \mathbb{Z}_{17}^+ : r = x^4 \text{ for some } x \in \mathbb{Z}_{17}^+\} \\ &= \{1, 4, 13, 16\}. \end{aligned}$$

Since we use this example in Section 7.4, we show the resulting differences in detail. Using the qualifier $m = 2$ we use (2.9) to obtain the results in Table 2.3, modulo 17. Note from Table 2.3 that each non-zero difference modulo 17 occurs exactly once, giving $\lambda = 1$, and

the zero difference does not occur. The list of possible values of m arises due to the fact that all the qualifiers are those integers that are in residue class $n/2$, namely those integers that are $(n/2)$th power residues that are not nth power residues [21, Theorems 2.1 and 2.2]. Thus, 2, 8, 9 and 15 are the squares which are not fourth powers in $\mathbb{Z}_{17}^+$.

If zero is counted as an nth power residue we obtain modified qualified residue difference sets. We define these sets as follows.

Definition 2.31 *Let k be a positive integer and $R = \{r_1, r_2, r_3, \ldots, r_k\}$ be the set of nth power residues of an odd prime $p = nk + 1$. Let R^* be the $k+1$-element set $R^* = \{r_0, r_1, r_2, \ldots, r_k\} = R \cup \{0\}$ where $r_0 = 0$. We call R^* an nth power modified qualified residue difference set, MQRDS for short, if R^* is a MQDS.*

We now give an example of a MQRDS.

Example 2.32 *The parameters $n = 2$, $k = 2$ and $p = nk + 1 = 5$ yield a MQRDS. The complete list of possible qualifiers is $m = 2$ and 3, as these are the integers that are in residue class $n/2$ [21, Theorems 2.1 and 2.2].*

For $p = 5$ is prime, the incidence relation (2.13) implies $\lambda = 2$. We obtain the set

$$\begin{aligned} R^* &= \{r \in \mathbb{Z}_5^+ : r = x^2 \text{ for some } x \in \mathbb{Z}_5^+\} \cup \{0\} \\ &= \{0, 1, 4\}. \end{aligned}$$

Using $m = 2$ or $m = 3$ with (2.11) we obtain every non-zero difference modulo 5 exactly twice, giving $\lambda = 2$ and zero occurs exactly once.

In all cases so far discovered of RDS, MRDS, QRDS and MQRDS, the modulus v of each type of configuration is an odd prime p. Storer investigated the case when the modulus of a RDS or MRDS is a power of an odd prime (p^α). He states that for $n = 4, 6, 8$ we must have $\alpha = 1$ and hence a prime modulus [60, Theorem 20, p. 82]. He gives a specific proof for the case $n = 4$, which he attributes jointly to Lebesgue [46] and a rediscovery by Hall [37], and he ascribes the proof for $n = 6$ to W.H. Mills, without citing a reference. He provides no proof for $n = 8$.

In the remainder of this thesis, the modulus $v = p$ is always an odd prime.

2.4 Cyclotomy

The proofs in this thesis make extensive use of cyclotomy and cyclotomic number theory. Therefore we present a brief discussion of cyclotomy in this section. Firstly we require a definition of a *primitive root*.

Definition 2.33 *Let p be an odd prime. The integer g is a primitive root of p if g is a generator for the multiplicative group $\mathbb{Z}_p^+$, that is, $\{g^u : u \in \mathbb{Z}_p^+\} = \mathbb{Z}_p^+$.*

Note here that $\mathbb{Z}_p^+$ is a cyclic group with respect to multiplication and so the existence of a primitive root g as a generator is guaranteed [39, p. 40-41]. Now, let n and k be positive integers and suppose we have

$$p = nk + 1 \tag{2.14}$$

where p is an odd prime. Let g be a primitive root of p. We now define the terms *residue class* and *index*. The index is also called the *discrete logarithm*.

Definition 2.34 *Let p be an odd prime which satisfies (2.14) and let g be a primitive root of p. The integer $N \in \mathbb{Z}_p^+$ is said to be in residue class i with respect to g for the given values of p and n if the following congruence holds for some integer u:*

$$N \equiv g^{un+i} \pmod{p}. \tag{2.15}$$

We call the quantity $un + i$ in (2.15) the index of N, referred to as ind N, or the discrete logarithm of n with respect to the base g. Therefore

$$g^{\,ind\ N} \equiv N \pmod{p}. \tag{2.16}$$

We also define the *cyclotomic constant of order n*.

Definition 2.35 *Let n and k be positive integers such that $p = nk + 1$ is an odd prime. Let g be a primitive root of p. The cyclotomic constant (i, j) of order n denotes the number of members of the residue class i which are followed by a member of the residue class j, that is the number of solutions to the congruence*

$$g^{un+i} + 1 \equiv g^{vn+j} \pmod{p} \tag{2.17}$$

where $0 \leq i, j \leq n-1$ and $0 \leq u, v \leq k-1$.

See Dickson [25] for an in-depth study of the properties of cyclotomic constants. The following results, also due to Dickson [25, pp. 392-394], are required too:

$$(i, j) = (-i, j - i) \tag{2.18}$$

$$(i, j) = (j, i) \text{ if } k \text{ is even} \tag{2.19}$$

$$\sum_{j=0}^{n-1} (i, j) = \begin{cases} k-1 & \text{if } k \text{ is even and } i = 0, \text{ or if } k \text{ is odd and } i = n/2 \\ k & \text{otherwise} \end{cases} \tag{2.20}$$

$$(i, j) = (i + \gamma_1 n, j + \gamma_2 n) \tag{2.21}$$

for all integers γ_1 and γ_2. We also require the following lemma.

Lemma 2.36 *Let n and k be positive integers such that $p = nk + 1$ is prime. Now let $N \in \mathbb{Z}_p^+$ be an integer and define $\bar{N}$ such that $N\bar{N} \equiv 1 \pmod{p}$. If N is in residue class $n - i$ with respect to the primitive root g then $\bar{N}$ is in residue class i with respect to g.*

Proof. Let N_1 and N_2 be integers and suppose they are in residue classes i_1 and i_2, respectively. From Definition 2.34 we see that the product N_1N_2 is in residue class $i_1 + i_2 \pmod{n}$. The claimed result now follows on taking $N_1 = N$, $N_2 = \bar{N}$ and using the fact that the integer 1 is in residue class zero. □

Apart from Dickson, cyclotomic constants have been investigated by many authors, including Lehmer [48], Whiteman [67, 68], Muskat [52] and Baumert and Fredricksen [5, 6]. Those cyclotomic constants used in this thesis are given in Appendix A.

Chapter 3

Qualified Residue Difference Sets

3.1 Introduction

In this chapter we discuss in detail QRDS and MQRDS. We establish the necessary and sufficient conditions for the existence of QRDS and MQRDS in Section 3.2. We then give a few basic properties of QRDS and MQRDS in Section 3.3.

3.2 Necessary and Sufficient Conditions for the Existence of QRDS and MQRDS

In this section we establish the necessary and sufficient conditions for the existence of QRDS and MQRDS. Throughout this section, n and k will denote positive integers and $p = nk + 1$ is assumed to be prime. Let R be a QRDS (if one exists) with modulus $v = p$ having k elements and multiplicity λ, where λ is given by the incidence relation (2.12). Also, let R^* be a MQRDS (if one exists) with modulus $v = p$ having $k + 1$ elements and multiplicity λ, where λ is given by the incidence relation (2.13).

Lemma 3.1 *For the QRDS R, we have*

$$p = \lambda n^2 + 1 \text{ and } \lambda = k/n. \tag{3.1}$$

For the MQRDS R^*, we have

$$p = \lambda n^2 - 2n + 1 \text{ and } \lambda = (k+2)/n. \tag{3.2}$$

Proof. From Equation (2.12) $k^2 = \lambda(p-1) = \lambda nk$, so $k = \lambda n$. □

Lemma 3.2 *For all QRDS of prime modulus and all MQRDS of prime modulus, k must be even.*

Proof. By definition the modulus p is odd. Therefore, k must be even by Lemma 2.28. □

We now have the required information to outline the necessary and sufficient conditions for QRDS and MQRDS to exist. The following theorem applies to QRDS.

Theorem 3.3 *Let g be a primitive root of p. Suppose the integer $m \in \mathbb{Z}_p^+$ belongs to residue class $n - \sigma$ with respect to g for some integer σ, $0 \leq \sigma \leq n-1$. Then m is a qualifier of the QRDS R if and only if the cyclotomic constants obey the relations*

$$(s, \sigma) = (\sigma, s) = \lambda = k/n \tag{3.3}$$

for $s = 0, 1, \ldots, (n-1)$.

Proof. Let R be a QRDS of modulus $p = nk + 1$ and multiplicity λ. Suppose that m is a qualifier of R, belonging to the residue class $n - \sigma$, $0 \leq \sigma \leq n-1$. For each $t = 1, 2, \ldots, p-1$ the congruence

$$r_i - m r_j \equiv t \pmod{p} : \ 1 \leq i, j \leq k \tag{3.4}$$

has exactly λ solutions. Multiplying (3.4) through by $\bar{m}\bar{r}_j$, where $m\bar{m} \equiv 1 \pmod{p}$ and $r_j \bar{r}_j \equiv 1 \pmod{p}$, and rearranging gives

$$\bar{m} t \bar{r}_j + 1 \equiv \bar{m} r_i \bar{r}_j \pmod{p}. \tag{3.5}$$

Since m belongs to residue class $n-\sigma$, $\bar{m}$ belongs to residue class σ by Lemma 2.36. Also, r_j is in residue class zero, as is $\bar{r}_j$ by Lemma 2.36. Therefore $\bar{m} t \bar{r}_j \equiv g^{u_1 n + \sigma + s + 0} \pmod{p}$ for some integer u_1 and so $\bar{m} t \bar{r}_j$ belongs to residue class $\sigma + s$, where s is the residue class of t. Also $\bar{m} r_i \bar{r}_j \equiv g^{u_2 n + \sigma + 0 + 0} \pmod{p}$ for some integer u_2 and so $\bar{m} r_i \bar{r}_j$ belongs to residue class σ. Now t takes on any value from 1 to $p-1$ and (3.5) always has λ solutions. Therefore using Definition 2.35 we have

$$(\sigma + s, \sigma) = \lambda \text{ for } s = 0, 1, \ldots, (n-1)$$

and so by periodicity modulo n (see Equation (2.21)), Lemma 3.2 and (2.19) for k even we have

$$(s, \sigma) = (\sigma, s) = \lambda \text{ for } s = 0, 1, \ldots, (n-1). \tag{3.6}$$

Eliminating p from $p = nk + 1$ and Equation (2.12) gives $\lambda = k/n$ to complete Equation (3.3). Therefore we have shown the necessity of the condition in Theorem 3.3. We now need to prove that it is sufficient.

Suppose that the (s, σ) are all equal for a given $\sigma \neq 0$, then we have

$$(s, \sigma) = \sum_{i=0}^{n-1} (i, \sigma)/n. \tag{3.7}$$

Since by Lemma 3.2 k must be even, then using (2.19) and (2.20), and noting that $\sigma \neq 0$ gives

$$\sum_{i=0}^{n-1}(i,\sigma) = \sum_{i=0}^{n-1}(\sigma,i) = k. \tag{3.8}$$

Therefore we have, from (3.7), (3.8) and (3.1), $(s,\sigma) = \lambda$ for all s. Therefore (3.5) and hence (3.4) has exactly k/n solutions for all t. Thus, using a qualifier m which is in residue class $n-\sigma$ will yield a QRDS. Hence the condition is sufficient and Theorem 3.3 is proved. □

The following theorem gives a necessary and sufficient condition for a MQRDS to exist.

Theorem 3.4 *Let g be a primitive root of p. Suppose the integer $m \in \mathbb{Z}_p^+$ belongs to residue class $n-\sigma$ with respect to g for some integer σ, $0 \leq \sigma \leq n-1$. Then m is a qualifier of the MQRDS R^* if and only if the cyclotomic constants obey the relations*

$$1 + (0,\sigma) = 1 + (\sigma,0) = 1 + (\sigma,\sigma) = (s,\sigma) = (\sigma,s) = \lambda = (k+2)/n \tag{3.9}$$

for $s = 1, 2, \ldots, (n-1)$, $s \neq \sigma$.

Proof. Let R^* be a MQRDS of modulus $p = nk+1$ and multiplicity λ. Suppose that m is a qualifier of R^*, belonging to the residue class $n-\sigma$, $0 \leq \sigma \leq n-1$. For each $t = 1, 2, \ldots, p-1$ the congruence

$$r_i - mr_j \equiv t \pmod{p} : \ 0 \leq i,j \leq k \tag{3.10}$$

has exactly λ solutions. Congruence (3.10) has only one solution when $t = 0$ i.e. when $i = j = 0$. For $i \neq 0$ and $j \neq 0$ we begin by following the same procedure as for the proof of Theorem 3.3. We multiply (3.10) through by $\bar{m}\bar{r}_j$ (where $m\bar{m} \equiv 1 \pmod{p}$ and $r_j\bar{r}_j \equiv 1 \pmod{p}$) and rearrange to give the congruence in (3.5). As above, $\bar{m}$ belongs to residue class σ, $\bar{m}t\bar{r}_j$ belongs to residue class $\sigma + s$, where s is the residue class of t, and $\bar{m}r_i\bar{r}_j$ belongs to residue class σ. The remaining non-zero differences are of the following form

$$r_i - m.0 \equiv t \pmod{p} \quad (i \neq 0,\ j = 0) \tag{3.11}$$

$$0 - mr_j \equiv t \pmod{p} \quad (i = 0,\ j \neq 0). \tag{3.12}$$

Now, by the hypothesis of Theorem 3.4, Congruence (3.10) has exactly λ solutions for each non-zero value of t. If $i \neq 0$ and $j \neq 0$ then all λ solutions arise as a result of (3.5) and in these cases we follow the reasoning for the QRDS case (Equations (3.5) to (3.6)) and obtain $(s,\sigma) = \lambda$ for those values of t (in residue class s) not generated by Equation (3.11) or (3.12). If one of the differences t does arise as a result of the zero residue r_0 we have a solution to either (3.11) or (3.12). Firstly, if $j = 0$ we obtain $t \equiv r_i$ from Equation (3.11) and so t belongs to residue class zero and hence we have a solution to (3.11) when $s = 0$. Secondly, if $i = 0$ we obtain $t \equiv (-1)mr_j$ and so t belongs to residue $\tau + n - \sigma$ where τ is the residue class of -1. Now g is a primitive root of p and so $-1 \equiv g^{(p-1)/2}$

(mod p). However, because $p = nk + 1$ we have $(p-1)/2 = nk/2$ and, since k is even by Lemma 3.2, we have $(p-1)/2 = \beta n$ for some integer β and so $-1 \equiv g^{\beta n}$ which means that the residue class of -1 is zero. Therefore t belongs to residue class $n - \sigma$ and we have a solution to (3.12) when $s = n - \sigma$ (note: it is not possible for both of Equations (3.11) and (3.12) to be satisfied simultaneously, since this would mean that $t \equiv r_i \equiv -mr_j$. But r_i belongs to residue class zero and $-mr_j$ belongs to residue class σ, a contradiction since $\sigma \neq 0$). Therefore, since R^* is a MQRDS of multiplicity λ, we have

$$(s + \sigma, \sigma) = \begin{cases} \lambda - 1 \text{ if } s = 0 \text{ or } s = n - \sigma \\ \lambda \text{ otherwise} \end{cases} \tag{3.13}$$

which by periodicity gives

$$(s, \sigma) = \begin{cases} \lambda - 1 \text{ if } s = \sigma \text{ or } s = 0 \\ \lambda \text{ otherwise} \end{cases} . \tag{3.14}$$

Finally, Lemma 3.2 and Equations (2.19) and (3.2) combine to complete Equation (3.9). This proves that the conditions are necessary. We now show that they are sufficient.

Suppose for a given $\sigma \neq 0$ we have

$$1 + (0, \sigma) = 1 + (\sigma, \sigma) = (s, \sigma),\ s = 1, 2, \ldots, n-1,\ s \neq \sigma$$

then

$$n(s, \sigma) = 2 + \sum_{i=0}^{n-1} (i, \sigma). \tag{3.15}$$

Now, k is even and $\sigma \neq 0$. Therefore, by Lemma 3.2 and Equations (2.19) and (2.20) we obtain

$$n(s, \sigma) = k + 2. \tag{3.16}$$

Now eliminating p from $p = nk + 1$ and Equations (3.16) and (2.13) gives (3.9). Thus, using a qualifier m which is in residue class σ will yield a MQRDS. This completes the proof of Theorem 3.4. □

Note that for both QRDS and MQRDS the qualifier m belongs to residue class $n - \sigma$. We therefore give the following general definition that applies to all QDS and MQDS that are generated using index classes.

Definition 3.5 *Let $p = nk+1$ be an odd prime and let g be a primitive root of p. Suppose $R_{n,p}$ is a QDS or MQDS of order n and modulus p, generated using index classes with base g. There is an integer $m \in \mathbb{Z}_p^+$ whose residue class with respect to g is $n - \sigma$. The quantity σ is called a definer of the set $R_{n,p}$.*

The analysis above indicates that the definer $\sigma \neq 0$. In the case of QRDS and MQRDS, further developments by Byard, Evans and Van Veen have limited the conditions for the definer. In 2006 the author proved that if σ is a definer for a QRDS or MQRDS then $-\sigma$ is also a definer [17, Theorem 3.3], thus limiting the need to check only for values $\sigma \leq n/2$.

However, in 2009 the definer was calculated precisely by Byard, Evans and Van Veen as follows:

$$\sigma = n/2 \tag{3.17}$$

[21, Theorem 2.1]. We therefore modify Theorems 3.3 and 3.4 accordingly to give the following existence theorems for QRDS and MQRDS.

Theorem 3.6 *A QRDS exists for the prime modulus $p = nk + 1$ if and only if the cyclotomic constants*

$$(s, n/2) = (n/2, s) = \lambda = k/n \tag{3.18}$$

for $0 \leq s < n/2$ and λ is the multiplicity of the QRDS. The qualifiers $m \in \mathbb{Z}_p^+$ are precisely all integers that are in residue class $n/2$ with respect to the primitive root g.

Proof. Combining (3.17) with (3.3) gives (3.18). However, the range of values for s is shortened as follows. Using (2.18) and (2.19) with the cyclotomic constant $(i, n/2)$ gives

$$(i, n/2) = (i + n/2, n/2). \tag{3.19}$$

Thus we only need consider values of $s < n/2$. This completes the proof of Theorem 3.6. □

Theorem 3.7 *A MQRDS exists for the prime modulus $p = nk + 1$ if and only if*

$$1 + (0, n/2) = 1 + (n/2, 0) = (s, n/2) = (n/2, s) = \lambda = (k + 2)/n \tag{3.20}$$

for $0 < s < n/2$, and λ is the multiplicity of the MQRDS. The qualifiers $m \in \mathbb{Z}_p^+$ are precisely all integers that are in residue class $n/2$ with respect to the primitive root g.

Proof. Combining (3.17) with Theorem 3.4 and (3.19) proves the theorem. □

Chapters 4 and 5 address the existence question for QRDS and MQRDS for even values of n up to $n = 18$ excluding $n = 16$. The proofs of nonexistence for $n = 16$ and $n = 20$ are presented in [21]. In all cases cyclotomy is used extensively and the relevant cyclotomic constants are given in Appendix A.

3.3 Some Properties of QRDS and MQRDS

QRDS and MQRDS have many properties. We prove some of these here. In this section we let R be a QRDS and R^* be a MQRDS.

Lemma 3.8 *All QRDS R and MQRDS R^* are symmetric, i.e. if $r \in R$, then $p - r \in R$, and if $r \in R^*$, then $p - r \in R^*$.*

Proof. Let r be a non-zero nth power residue of the prime p. Therefore $r \in R$ and $r \in R^*$. Also $r^{(p-1)/n} \equiv 1 \pmod{p}$ which by $p = nk + 1$ means that $r^k \equiv 1 \pmod{p}$. However, since k is even by Lemma 2.28 then $(-r)^k \equiv 1 \pmod{p}$. Therefore $-r$ must also be a residue and hence $p - r \in R$ and $p - r \in R^*$. □

Corollary 3.9 *$-1 \in R$ and $-1 \in R^*$*

Proof. As 1 is always an nth power residue then, by Lemma 3.8, -1 must also be a residue and hence must be in both R and R^*. □

Lemma 3.10 *If m is a qualifier of a QRDS or MQRDS then $p - m$ is also a qualifier.*

Proof. Let m be a qualifier of a QRDS or MQRDS of modulus p and order n. By Theorem 3.6 or Theorem 3.7 respectively, m is in residue class $n/2$. Therefore $m \equiv g^{un+n/2} \pmod{p}$ for some integer u. But -1 is in residue class zero by Corollary 3.9, so $-m \equiv g^{vn+n/2} \pmod{p}$ for some integer v. Therefore $-m$ is in residue class $n/2$ and is hence a qualifier. □

The following lemma makes easier the task of finding a qualifier, m, in certain circumstances.

Lemma 3.11 *If the multiplicity λ of a QRDS is odd or the multiplicity λ of a MQRDS is even, 2 and $p - 2$ are in residue class $n/2$, and can hence be used as qualifiers.*

Proof. Lehmer proved that the cyclotomic constant $(0, j)$ is odd or even according as 2 belongs to residue class j or not [47, Lemma I]. For a QRDS, using (3.18) gives $(0, n/2) = \lambda$, so if λ is odd then 2 belongs to residue class $n/2$ and can hence be used as a qualifier. Also, by Lemma 3.10 $p-2$ must also be a qualifier. For a MQRDS, using Equation (3.20) gives $1 + (0, n/2) = \lambda$. Therefore if λ is even then $(0, n/2)$ is odd and so 2 belongs to residue class $n/2$ and can hence be used as a qualifier. Also, by Lemma 3.10 $p - 2$ must also be a qualifier. □

Chapter 4

Existence of QRDS and MQRDS for $n = 2, 4$ and 6

4.1 Introduction

In this chapter we prove that QRDS and MQRDS exist for all orders $n = 2, 4$ and 6 and we determine precisely the conditions for which both types of set exist for these values of n. We use the theorems of cyclotomy derived by Dickson [25]. The proofs run along similar lines to those used by Lehmer [47] in her generalisation of RDS and MRDS. Originally the case of a RDS for $n = 2$ was discovered in a different guise by Paley [55] and Chowla proved the existence of RDS for $n = 4$ [24] using results from Bachmann [2]. Lehmer extended the analysis to include MRDS and she also proved that there do not exist RDS or MRDS for $n = 6$. The proof of existence of QRDS and MQRDS for $n = 6$ in Section 4.4 is therefore an interesting contrast to Lehmer's result.

For a QRDS to exist we need to determine conditions which satisfy Equation (3.18). For a MQRDS to exist we need to determine conditions which satisfy Equation (3.20).

4.2 Existence for $n = 2$

In this section we prove the following:

Theorem 4.1 *QRDS and MQRDS exist for $n = 2$ and prime modulus p if and only if $p = 4\alpha + 1$ where α is a positive integer.*

Proof. Since $p = nk + 1$ then for $n = 2$ we have

$$p = 2k + 1. \tag{4.1}$$

To determine the necessary and sufficient conditions for a QRDS to exist we also need to satisfy Equation (3.18) for $n = 2$. Therefore we need to demonstrate that

$$(0, 1) = \lambda = k/2. \tag{4.2}$$

Using the relevant cyclotomic constant equation for $n = 2$ and k even from Section A.1 of the Appendix we have

$$(0, 1) = (p - 1)/4. \tag{4.3}$$

Now, combining Equations (4.2), (4.3) and (4.1) combine to give no further restriction on p beyond $p = 4\lambda + 1$ which is satisfied (as per Equation (3.1)).

For a MQRDS to exist we need to satisfy Equation (3.20). Therefore we need to demonstrate that

$$1 + (0, 1) = \lambda = (k + 2)/2. \tag{4.4}$$

Here, combining Equations (4.4), (4.3) and (4.1) gives $p = 4\lambda - 3$ which is also satisfied (as per Equation (3.2)).

In both cases we have $p = 4\alpha + 1$ for integer α. This completes the proof of Theorem 4.1. □

4.3 Existence for $n = 4$

In this section we prove the following:

Theorem 4.2 *If $n = 4$ and p is an odd prime a QRDS exists if and only if $p = 16\alpha^2 + 1$ and a MQRDS exists if and only if $p = 16\alpha^2 + 9$ where α is an integer in each case.*

Proof. Since $p = nk + 1$ then for $n = 4$ we have

$$p = 4k + 1 \tag{4.5}$$

and the cyclotomic constants are given in terms of the quadratic partition

$$p = x^2 + 4y^2 \tag{4.6}$$

where x and y are integers and $x \equiv 1 \pmod 4$ (Section A.2).

By (3.1) and (3.18), a necessary condition for the existence of a QRDS is

$$(0, 2) = (p - 1)/16. \tag{4.7}$$

Also, from Section A.2 we have

$$16(0, 2) = p - 3 + 2x. \tag{4.8}$$

Equations (4.7) and (4.8) combine to give $x = 1$. Hence, from (4.6) we must have $p = 1 + 4y^2$, and since $p \equiv 1 \pmod{16}$ by (3.1), then y must be even and so $p = 16\alpha^2 + 1$.

For the converse, assume $p = 16\alpha^2 + 1$ is prime. Following Theorem 3.6 and Equation (3.1) it is enough to show

$$(0, 2) = (1, 2) = (p - 1)/16. \tag{4.9}$$

From Section A.2 we have

$$16(1, 2) = p + 1 - 2x. \tag{4.10}$$

Now $p = 16\alpha^2 + 1$ and so by (4.6) $x = 1$ since the representations of p as the sum of two squares is unique up to order and sign. Now, Equations (4.8) and (4.10) combine to give (4.9) so the converse is proved.

By (3.2) and (3.20), a necessary condition for the existence of a MQRDS is

$$1 + (0, 2) = (p + 7)/16. \tag{4.11}$$

Now (4.8) and (4.11) give $p - 3 + 2x = p + 7 - 16$ and hence $x = -3$. Therefore, by (4.6) $p = 9 + 4y^2$. From (3.2) $p = 16\lambda - 7$ and so $p \equiv 9 \pmod{16}$, which means y must be even. Therefore $p = 16\alpha^2 + 9$ for integer α.

For the converse, assume we have a prime $p = 16\alpha^2 + 9$. Following Theorem 3.7 and (3.2) it is enough to show

$$1 + (0, 2) = (1, 2) = (p + 7)/16. \tag{4.12}$$

Because $p = 16\alpha^2 + 9$ then, since $x \equiv 1 \pmod 4$ and by uniqueness, we have $x = -3$. Using this value of x with the cyclotomic constant Equations (4.8) and (4.10) gives (4.12) and so the converse is proved. This completes the proof of Theorem 4.2. □

4.4 Existence for $n = 6$

In this section we prove the following:

Theorem 4.3 *If $n = 6$ and p is an odd prime QRDS exist if and only if $p = 108\alpha^2 + 1$ and MQRDS exist if and only if $p = 108\alpha^2 + 25$ where α is an integer in each case.*

Proof. Since $p = nk + 1$ then for $n = 6$ we have

$$p = 6k + 1 \tag{4.13}$$

and the cyclotomic constants are given in terms of the quadratic partition

$$p = A^2 + 3B^2 \tag{4.14}$$

where A and B are integers and $A \equiv 1 \pmod 6$ if k is even and $A \equiv 4 \pmod 6$ if k is odd [25, pp. 408-410]. Clearly $B \neq 0$ in (4.14) since p is prime. Furthermore, we need to consider separately the three cases when $\operatorname{ind} 2 \equiv 0$, 1 or 2 $\pmod 3$ where $\operatorname{ind} a$ is defined in Definition 2.34 for a primitive root g of p.

By (3.18) and (3.20), a necessary condition for the existence of either a QRDS or MQRDS respectively is

$$(1, 3) = (2, 3). \tag{4.15}$$

When $\operatorname{ind} 2 \equiv 1 \pmod 3$, (4.15) and the equations in Section A.3 give $p + 1 - 2A - 6B = p + 1 - 2A + 12B$. Therefore $B = 0$ which is impossible by (4.14). When $\operatorname{ind} 2 \equiv 2$

(mod 3), (4.15) and the equations in Section A.3 give $p+1-2A-12B = p+1-2A+6B$. Again we obtain $B = 0$ and hence a nonexistence condition for both types of set.

For the case ind $2 \equiv 0 \pmod 3$ (i.e. 2 is a cubic residue of p) we consider QRDS and MQRDS separately. For a QRDS a necessary condition from (3.18) is that we have $(0,3) = (1,3)$. This gives $p - 5 + 4A = p + 1 - 2A$ (Section A.3) and hence $A = 1$. Therefore, from (4.14) we have $p = 1+3B^2$, which combines with (3.1) to give $B^2 = 12\lambda$. Therefore λ must be of the form $\lambda = 3\alpha^2$ where α is an integer and so we have

$$p = 108\alpha^2 + 1. \tag{4.16}$$

To prove the converse, assume we have a prime of the form in (4.16). Following Theorem 3.6 and (3.1) it is enough to show

$$(0,3) = (1,3) = (2,3) = (p-1)/36. \tag{4.17}$$

From Section A.3 we have

$$(1,3) = (2,3). \tag{4.18}$$

Now, since $p = 108\alpha^2 + 1$ then, combining with (4.14) and using the uniqueness of the representation of primes of the form $A^2 + 3B^2$ (see Lemma 3.0.1 from Berndt et al. [10, p. 101]) we obtain $A = 1$. In this case we have from Section A.3

$$(0,3) = (1,3) = (p-1)/36. \tag{4.19}$$

Now (4.18) and (4.19) combine to give (4.17) and so the converse is proved.

For a MQRDS when $2 \equiv 0 \pmod 3$, a necessary condition for existence is that we have $1 + (0,3) = (1,3)$ (Equation (3.20)). Imposing this restriction and using the cyclotomic constants from Section A.3 gives $36+p-5+4A = p+1-2A$ and hence $A = -5$. Combining this result with (4.14) gives $p = 25 + 3B^2$, which along with (3.2) gives $B^2 = 12(\lambda - 1)$. Therefore $\lambda - 1$ must be of the form $3\alpha^2$ and hence $B^2 = 36\alpha^2$ where α is an integer. Therefore substituting the given values of A and B into (4.14) gives

$$p = 108\alpha^2 + 25. \tag{4.20}$$

For the converse, assume we have a prime of the form given in (4.20). It is sufficient from Theorem 3.7 and (3.2) to show that

$$1 + (0,3) = (1,3) = (2,3) = (p+11)/36. \tag{4.21}$$

Here, (4.18) applies as for the QRDS case. Since we now have $p = 108\alpha^2 + 25$ then, combining with (4.14) and by uniqueness we obtain $A = -5$. Therefore we obtain from Section A.3

$$1 + (0,3) = (1,3) = (p+11)/36. \tag{4.22}$$

Now (4.18) and (4.22) combine to give (4.21) and so the converse is proved. This completes the proof of Theorem 4.3. □

Chapter 5

Nonexistence of QRDS for Higher Values of n

5.1 Introduction

In this chapter we will give detailed proofs for the nonexistence of QRDS and MQRDS for orders $n = 8$, 10, 12, 14 and 18. Each subsequent section of the chapter deals with one of these individual values of n. Nonexistence for odd values of n and for $n = 16$ and $n = 20$ are given in [21, Theorems 2.1, 5.1 and 7.1]. Using cyclotomy we prove the nonexistence of both types of set by demonstrating that the necessary conditions of Theorems 3.6 and 3.7 are not satisfied in each case. To simplify the analysis we now combine Equations (3.18) and (3.20) from these two theorems. We begin with a definition and a lemma.

Definition 5.1 *Let n and k be positive integers such that $p = nk+1$ is an odd prime. Let R be the k-element set of non-zero nth power residues modulo p. Suppose that either R is a QRDS or $R^* = R \cup \{0\}$ is a MQRDS (both cannot occur due to Lemma 2.27). Define*

$$\epsilon = \epsilon(R) = \begin{cases} 0 \text{ if } R \text{ is a QRDS} \\ 1 \text{ if } R^* \text{ is a MQRDS}, \end{cases} \tag{5.1}$$

and

$$\nu = n\epsilon - 1. \tag{5.2}$$

Lemma 5.2 *Let n and k be positive integers such that $p = nk + 1$ is an odd prime. Let R be the k-element set of non-zero nth power residues modulo p. Let $R^* = R \cup \{0\}$. If either R is a QRDS or R^* is a MQRDS then*

$$n^2(0, n/2) = p - \nu^2 \tag{5.3}$$

and

$$n^2(s, n/2) = p + 2\nu + 1 \quad \text{for all } s \in \mathbb{N} \text{ satisfying } s < n/2. \tag{5.4}$$

Proof. Firstly, consider the case $s = 0$ in Theorem 3.6 and also Theorem 3.7. Then for a QRDS, combining (3.18) with (3.1) gives

$$n^2(0, n/2) = p - 1 \tag{5.5}$$

and for a MQRDS combining (3.20) with (3.2) gives $n^2(0, n/2) = p + 2n - 1 - n^2$ and hence

$$n^2(0, n/2) = p - (n-1)^2. \tag{5.6}$$

Combining Equations (5.1), (5.5) and (5.6) gives in either case $n^2(0, n/2) = p - (n\epsilon - 1)^2$ and hence by (5.2) we obtain (5.3).

Secondly, using Equations (3.18) and (3.1) for a QRDS with $s \neq 0$ we have

$$n^2(s, n/2) = p - 1 \qquad 0 < s < n/2 \tag{5.7}$$

and from Equations (3.20) and (3.2) for a MQRDS we have

$$n^2(s, n/2) = p + 2n - 1 \qquad 0 < s < n/2. \tag{5.8}$$

The difference between the right hand sides of Equations (5.7) and (5.8) is $2n$. Therefore, employing (5.1) gives in either case $n^2(s, n/2) = p + 2n\epsilon - 1$, which with (5.2) gives (5.4). This completes the proof of Lemma 5.2. □

In a complete proof that involves the use of cyclotomic constants, it is necessary to take account of the additional individual conditions that arise due to the peculiarities of each value of n. For example, in the cases $n = 8, 10$ and 12, these are the $(n/2)$th power character of the integer 2. In each case, the specific requirements are outlined and the analysis is completed accordingly. Also, all literary sources for the cyclotomic constants are referenced and the relevant cyclotomic constants are given in Appendix A.

5.2 Nonexistence for $n = 8$

In this section we have $p = 8k + 1$ from (2.14) and we prove the following theorem.

Theorem 5.3 *QRDS and MQRDS do not exist for* 8*th powers.*

To prove Theorem 5.3 we require the cyclotomic constants for $n = 8$. These have been calculated using Dickson's results 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) [48]. Since we have $p = 8k + 1$ and, by Lemma 3.2, k is even for all QRDS and MQRDS, we require her list for $p = 16\alpha + 1$ [48, p. 116]. The cyclotomic constants used in this section are given in Section A.4.

Theorem 5.3 is proved by demonstrating that Equation (5.4) is not satisfied for $n = 8$. Here we need to investigate the following two cases: (a) 2 is a biquadratic (4th power) residue of p, (b) 2 is biquadratic nonresidue of p. We then apply the resulting condition

to the following further condition, stipulated by Dickson [25, p. 410, Theorem 11], that for $n = 8$ the cyclotomic constants depend on the following quadratic partitions:

$$p = x^2 + 4y^2 \text{ and } p = a^2 + 2b^2 \tag{5.9}$$

where $x \equiv a \equiv 1 \pmod 4$ and x, y, a and b are all integers.

Proof of Theorem 5.3. Case 1: If 2 is a biquadratic residue of p then for Equation (5.4) to be satisfied, a necessary condition is that the cyclotomic constants $(1, 4) = (2, 4)$. Using the equations in Section A.4 we get

$$p + 1 + 2x - 4a = p + 1 - 2x.$$

This gives $x = a$ which, using Equation (5.9) gives $2y^2 = b^2$. However, because $\sqrt{2}$ is irrational, the only integer solution of this last equation is $y = b = 0$. Using this result with Equation (5.9) gives $p = x^2$, which is impossible since p must be prime. Therefore 2 cannot be a biquadratic residue of p if $n = 8$.

Case 2: If 2 is a biquadratic nonresidue of p, setting $(1, 4) = (3, 4)$ $(= (1, 5))$ by (5.4) gives

$$p + 1 + 2x - 4a + 16y = p + 1 + 2x - 4a - 16y$$

which gives $16y = -16y$ and therefore $y = 0$. However, substituting this into Equation (5.9) also gives the contradiction $p = x^2$. Therefore 2 cannot be a biquadratic nonresidue either. The nonexistence of QRDS and MQRDS for 8th powers is established and so Theorem 5.3 is proved. □

5.3 Nonexistence for $n = 10$

In this section $p = 10k + 1$ and we prove the following theorem.

Theorem 5.4 *QRDS and MQRDS do not exist for* 10*th powers.*

To prove Theorem 5.4 we require the cyclotomic constants for $n = 10$. Following work by Dickson [25] and Bruck [12], Whiteman has presented a complete solution for these cyclotomic constants which he presents as a set of tables [67, pp. 107-109]. These are given in terms of the prime p and the integers x, u, v, w, which must all satisfy the following diophantine equations:

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2 \tag{5.10}$$

$$xw = v^2 - 4uv - u^2 \tag{5.11}$$

where $x \equiv 1 \pmod 5$ [67, p. 95]. The cyclotomic constants relevant to this section are given in Section A.5.

Proof of Theorem 5.4. Let g be a primitive root of p. We consider three cases, depending on the value of ind 2 modulo 5.

Case 1: ind $2 \equiv 0 \pmod 5$. For Equation (5.4) to be satisfied, a necessary condition is that we have $(1,5) = (2,5)$. Therefore, using Whiteman's results (Section A.5), we obtain $2p + 2 + x + 25w = 2p + 2 + x - 25w$, giving $w = 0$. Therefore by Equation (5.11) we have $v^2 - 4uv - u^2 = 0$, giving $v = u(2 \pm \sqrt{5})$. The only integer solution of this last equation is $u = v = 0$. Substituting these values for u, v and w into (5.10) and rearranging gives $p = (x/4)^2$, a contradiction. Therefore there exist no QRDS or MQRDS if ind $2 \equiv 0 \pmod 5$.

Case 2: ind $2 \equiv 1 \pmod 5$. Setting $(1,5) = (2,5)$ gives $2(2p + 2 + x + 50v + 25w) = 4p + 4 - 23x + 50u - 25w$, giving

$$x + 4v + 3w = 2u \tag{5.12}$$

and setting $(2,5) = (3,5)$ (which, from Dickson [25, p. 415], is equivalent to setting $(2,5) = (2,7)$) gives $4p + 4 - 23x + 50u - 25w = 2(2p + 2 + x - 25u - 25v)$, giving

$$x + w = 4u + 2v. \tag{5.13}$$

Eliminating w from Equations (5.12) and (5.13) gives $u+v = x/5$, a result that contradicts at least one of the conditions that u and v must both be integers and $x \equiv 1 \pmod 5$. Therefore there exist no QRDS or MQRDS if ind $2 \equiv 1 \pmod 5$.

Case 3: ind $2 \equiv 2, 3$ or $4 \pmod 5$. Let g_c be any primitive root of p other than g itself. Then $g_c \equiv g^t \pmod p$ for some integer t prime to $p-1$. Therefore any of the cases ind $2 \equiv 2, 3, 4 \pmod 5$ may be transformed into the case ind $2 \equiv 1 \pmod 5$ by making an appropriate choice of the primitive root. Therefore there exist no QRDS or MQRDS if ind $2 \equiv 2, 3$ or $4 \pmod 5$. The nonexistence of QRDS and MQRDS for 10th powers is established and so Theorem 5.4 is proved. □

5.4 Nonexistence for $n = 12$

In this section $p = 12k + 1$ and we prove the following theorem.

Theorem 5.5 *QRDS and MQRDS do not exist for* 12*th powers.*

To prove Theorem 5.5 we require the cyclotomic constants for $n = 12$. Following the groundwork of Dickson [25, pp. 417-424], Whiteman has calculated a complete solution for these cyclotomic constants, which he presents as a set of tables in his article [68, pp. 69-73]. Because of Equations (2.18) and (2.19) there are various equalities between the constants, which Whiteman also lists [68, p. 69, Table III]. The cyclotomic constants depend 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 $p = 12k + 1$, and a variable c which is equal to the ratio of Jacobi sums as follows:

$$\begin{gathered} \beta = \exp(2\pi i/12) \text{ is a primitive 12th root of unity} \\ \psi(\beta^\gamma, \beta^\delta) = \sum_{a+b \equiv 1 \pmod p} \beta^{(\gamma \text{ ind } a) + (\delta \text{ ind } b)} \\ c = \psi(\beta^3, \beta)/\psi(\beta^5, \beta) \end{gathered} \tag{5.14}$$

(see [68, Equations (2.3) and (5.7)]). Since $p = 12k + 1$ then $(3/p) = 1$ (where $(3/p)$ is the Legendre symbol for quadratic residues - see for example [42, pp. 131-132]) and so ind 3 must be even [68, p. 64]. Therefore we have ind $3 \equiv 0$ or 2 (mod 4). Since k is even we have $(2/p) = 1$ and so ind 2 must also be even (see [68, p. 64]). Therefore we have ind $2 \equiv 0, 2$ or 4 (mod 6). Furthermore, Whiteman demonstrated that for $n = 12$, c is actually a fourth root of unity and can thus take on values of 1, -1, β^3 or $-\beta^3$ [68, pp. 64-65]. He went on to prove that $c = \pm 1$ if k is even and ind $3 \equiv 0$ (mod 4), and that $c = \pm\beta^3$ if k is even and ind $3 \equiv 2$ (mod 4) [68, p. 65]. Thus, we have to deal with twelve cases in total. These are listed in Table 5.1.

The first six cases in Table 5.1 are covered by Whiteman's tables. Because for all QRDS and MQRDS k is even, we require Whiteman's Tables 1,3,4,7,9 and 10. The parameters ind 2, ind 3 and c for each of these tables required in the analysis of this section are summarised in Table 5.1. The remaining six cases are dealt with at the end of the section

ind 2 (mod 6)	ind 3 (mod 4)	c	Table from Whiteman [68]
2	2	β^3	Table 1
2	0	1	Table 3
2	0	-1	Table 4
0	2	β^3	Table 7
0	0	1	Table 9
0	0	-1	Table 10
0	2	$-\beta^3$	
2	2	$-\beta^3$	
4	0	1	
4	0	-1	
4	2	β^3	
4	2	$-\beta^3$	

Table 5.1: Parameters for the cyclotomic constants of order 12 for even k.

(Cases 7 and 8).

For $n = 12$ the cyclotomic constants depend on the following quadratic partitions:

$$p = x^2 + 4y^2 \text{ and } p = A^2 + 3B^2 \tag{5.15}$$

where $x \equiv 1$ (mod 4), $A \equiv 1$ (mod 6) and x, y, A and B are all integers [25, p. 417]. We prove Theorem 5.5 by demonstrating that in all cases the cyclotomic constants do not simultaneously satisfy Equations (5.4) and (5.15). Those cyclotomic constants required for this section are given in Section A.6.

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

Lemma 5.6 *If $B = 0$ then QRDS and MQRDS are nonexistent.*

Proof. If $B = 0$, then by (5.15) we have the contradiction $p = A^2$. □

Lemma 5.7 *If $x = \pm A$ then QRDS and MQRDS are nonexistent.*

Proof. If $x = \pm A$ then by (5.15) we have $y = B\sqrt{3}/2$. The only integer solution of this last equation is $y = B = 0$, which by Lemma 5.6 gives a nonexistence condition for QRDS and MQRDS. □

Proof of Theorem 5.5. Case 1: ind $2 \equiv 2 \pmod 6$, ind $3 \equiv 2 \pmod 4$, $c = \beta^3$, Table 1 from Whiteman [68, p. 70]. For Equation (5.4) to be satisfied, a necessary condition is that the cyclotomic constants $(4, 6) = (5, 6)$. From [68, Table III] this is equivalent to setting $(2, 8) = (1, 7)$, giving $p+1+2A+12B+8y = p+1+8A-12B+6x+8y$ and hence

$$4B = x + A. \tag{5.16}$$

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

$$2B + A + x = 0. \tag{5.17}$$

Combining Equations (5.16) and (5.17) gives $B = 0$ and so, by Lemma 5.6, a nonexistence condition results for both QRDS and MQRDS.

Case 2: ind $2 \equiv 2 \pmod 6$, ind $3 \equiv 0 \pmod 4$, $c = 1$, Table 3. Setting $(1, 6) = (3, 6)$ gives $p + 1 + 6A - 8x = p + 1 - 6A + 4x$, giving $x = A$ and hence by Lemma 5.7, a nonexistence condition.

Case 3: ind $2 \equiv 2 \pmod 6$, ind $3 \equiv 0 \pmod 4$, $c = -1$, Table 4. $(3, 6) = (4, 6)$ (i.e. $(3, 6) = (2, 8)$ from [68, Table III]) gives $p + 1 + 10A - 12x = p + 1 + 6A + 8x$ giving

$$A = 5x \tag{5.18}$$

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

$$8B + x = A. \tag{5.19}$$

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

$$7x + A = 6B. \tag{5.20}$$

Combining Equations (5.18), (5.19) and (5.20) gives $B = 0$ and hence, by Lemma 5.6, a nonexistence condition.

Case 4: ind $2 \equiv 0 \pmod 6$, ind $3 \equiv 2 \pmod 4$, $c = \beta^3$, Table 7. Note that from [68, Table III] $(5, 6) = (1, 7)$. Whiteman proved that when k is even and ind $2 \equiv 0 \pmod 6$ then the cyclotomic constant (i, j) can be replaced by $(5i, 5j)$ except that B is replaced by $-B$ [68, pp. 71-73]. We denote this new cyclotomic constant by $(5i, 5j)_{-B}$. Therefore we have here $(1, 7) = (5, 35)_{-B}$ which taken modulo 12 equals $(5, 11)_{-B}$ which in turn by

Whiteman [68, Table III] equals $(1,6)_{-B}$. Setting $(1,6) = (5,6)$ is therefore 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 5.6, a nonexistence condition.

Case 5: ind $2 \equiv 0 \pmod 6$, ind $3 \equiv 0 \pmod 4$, $c = 1$, Table 9. Setting $(1,6) = (2,6)$ gives $p + 1 + 6A - 8x = p + 1 - 2A$, giving $x = A$ and by Lemma 5.7, a nonexistence condition.

Case 6: ind $2 \equiv 0 \pmod 6$, ind $3 \equiv 0 \pmod 4$, $c = -1$, Table 10. Setting $(1,6) = (2,6)$ gives $p + 1 - 2A + 24B = p + 1 + 6A + 24B + 8x$, giving $x = -A$ and by Lemma 5.7, a nonexistence condition.

Case 7: ind $3 \equiv 2 \pmod 4$ (two subcases) (a) ind $2 \equiv 2 \pmod 6$, $c = -\beta^3$, (b) ind $2 \equiv 0 \pmod 6$, $c = -\beta^3$. Whiteman demonstrated that when k is even and ind $3 \equiv 2 \pmod 4$, if the cyclotomic constant (i,j) is replaced by $(7i,7j)$ then y and c change sign while ind 2 and ind 3 are unaltered [68, pp. 70-71]. We denote this new cyclotomic constant by $(7i,7j)_{-y}$. Therefore we replace $(i,6)$ by $(7i,42)_{-y} = (7i,6)_{-y}$. Thus the argument for $c = -\beta^3$ is the same as the corresponding argument for $c = \beta^3$ except that y is replaced by $-y$. Thus subcase (a) reduces to Case 1 and subcase (b) reduces to Case 4, both yielding a nonexistence condition.

Case 8: ind $2 \equiv 4 \pmod 6$ (four subcases) (a) ind $3 \equiv 0 \pmod 4$, $c = 1$, (b) ind $3 \equiv 0 \pmod 4$, $c = -1$, (c) ind $3 \equiv 2 \pmod 4$, $c = \beta^3$, (d) ind $3 \equiv 2 \pmod 4$, $c = -\beta^3$. Whiteman demonstrated that for k odd or even if the cyclotomic constant (i,j) is replaced by $(5i,5j)$ then B and ind 2 change sign while ind 3 and c are unaltered [68, p. 70]. We denote this new cyclotomic constant by $(5i,5j)_{-B}$. Therefore we replace $(i,6)$ by $(5i,30)_{-B} = (5i,6)_{-B}$. Thus subcase (a) reduces to Case 2, subcase (b) reduces to Case 3, subcase (c) reduces to Case 1 and subcase (d) reduces to subcase (a) of Case 7, in each case giving a nonexistence condition.

As a nonexistence condition has been obtained in all cases then the nonexistence of QRDS and MQRDS for 12th powers is established and so Theorem 5.5 is proved. □

5.5 Nonexistence for $n = 14$

In this section $p = 14k + 1$ and we prove the following theorem.

Theorem 5.8 *QRDS and MQRDS do not exist for* 14*th powers.*

To prove Theorem 5.8 we require the cyclotomic constants for $n = 14$. These have been calculated by Muskat [52] and are given as linear combinations of the integer parameters p, T, U and C_i $(0 \le i \le 6)$ relative to a fixed primitive root g. The quantities T, U and p satisfy the following quadratic partition

$$p = T^2 + 7U^2 \tag{5.21}$$

where $T \equiv 1 \pmod 7$ [52, p. 264 and 270]. To determine the condition for the C_i we proceed as follows. We define the quantity S as:

$$S = \sum_{i=0}^{6} C_i \zeta_7^i \qquad \zeta_7 = \exp(2\pi i/7) \tag{5.22}$$

where

$$\sum_{i=0}^{6} C_i = p - 2 \tag{5.23}$$

[52, p. 264, Equation (2.5)]. If we denote the complex conjugate of S by $\bar{S}$ then, since S is a Jacobi sum, the values C_i must satisfy the following

$$p = S\bar{S} = |S|^2. \tag{5.24}$$

Combining (5.22) and (5.24) and expanding we have

$$\begin{aligned} p &= \sum_{i=0}^{6} C_i \zeta_7^i \sum_{j=0}^{6} C_j \zeta_7^{-j} \\ &= \zeta_7^0 \sum_{i=0}^{6} C_i C_i + \zeta_7^1 \sum_{i=0}^{6} C_i C_{i+1} + \zeta_7^2 \sum_{i=0}^{6} C_i C_{i+2} + \zeta_7^3 \sum_{i=0}^{6} C_i C_{i+3} \\ &+ \zeta_7^4 \sum_{i=0}^{6} C_i C_{i+4} + \zeta_7^5 \sum_{i=0}^{6} C_i C_{i+5} + \zeta_7^6 \sum_{i=0}^{6} C_i C_{i+6} \\ &= \zeta_7^0 h_0 + \zeta_7^1 h_1 + \zeta_7^2 h_2 + \zeta_7^3 h_3 + \zeta_7^4 h_4 + \zeta_7^5 h_5 + \zeta_7^6 h_6 \end{aligned} \tag{5.25}$$

where

$$h_j = \sum_{i=0}^{6} C_i C_{i+j} \tag{5.26}$$

and where all subscripts in (5.25) and (5.26) are viewed modulo 7. Comparing coefficients in powers of ζ_7 in (5.25) and using (5.26) gives the following

$$h_1 = h_2 = h_3 = h_4 = h_5 = h_6 = h_0 - p = 0. \tag{5.27}$$

To prove Theorem 5.8 we need to consider the two cases when $\text{ind } 2 \equiv 0 \pmod 7$ and $\text{ind } 2 \not\equiv 0 \pmod 7$. Here, the case $\text{ind } 2 \not\equiv 0 \pmod 7$ is the simpler to deal with. This is where we begin.

Proof of Theorem 5.8. Case 1: $\text{ind } 2 \not\equiv 0 \pmod 7$. In this case in order to cater for the different possible values of ind 2 simultaneously Muskat has adopted the following approach [52, p. 271]. Letting

$$\begin{aligned} m &= \text{ind } 2 \pmod 7 & 1 \le m \le 6 \\ M &\equiv m \pmod 7 & M \text{ odd} \end{aligned} \tag{5.28}$$

we represent the cyclotomic constants by the following generalised form

$$(iM, jM) \tag{5.29}$$

and we replace the C_i by the generalised C_{im} in the evaluation of the cyclotomic constants [52, pp. 277-278]. (Note incidentally that Muskat quotes the second congruence in (5.28) incorrectly in his article [52, p. 271]). From (5.28) we therefore have the following values for the parameters m and M: $m = M = 1$; $m = 2, M = 9$; $m = M = 3$; $m = 4, M = 11$; $m = M = 5$; $m = 6, M = 13$.

Therefore combining (5.4) with (5.29) and noting that M is odd, for a QRDS or MQRDS to exist we need to satisfy

$$196(sM, 7) = p + 2\nu + 1 \qquad 1 \leq s \leq 6. \tag{5.30}$$

For ease of notation we adopt the symbol $A_i = C_{im}$. Therefore Equation (5.26) is replaced with

$$H_j = \sum_{i=0}^{6} A_i A_{i+j}. \tag{5.31}$$

and (5.27) is replaced with

$$H_1 = H_2 = H_3 = H_4 = H_5 = H_6 = H_0 - p = 0. \tag{5.32}$$

Solving (5.30) for $1 \leq s \leq 6$ and rearranging, we obtain the following

$$\begin{aligned}
14A_1 &= 2p - 4 + T - 17U - \nu \\
14A_2 &= 2p - 4 + T + 15U - \nu \\
14A_3 &= 2p - 4 + T - 9U - \nu \\
14A_4 &= 2p - 4 + T - 5U - \nu \\
14A_5 &= 2p - 4 - 6T + 6U + 6\nu \\
14A_6 &= 2p - 4 + T + 3U - \nu
\end{aligned} \tag{5.33}$$

and using (5.23) with (5.33) gives

$$14A_0 = 2p - 4 + T + 7U - \nu. \tag{5.34}$$

Now, inputting the A_i values into (5.31) gives

$$\begin{aligned}
28H_1 &= -16p + 16 + 4p^2 - T^2 + 2TU + 2T\nu - 65U^2 - 2U\nu - \nu^2 \\
28H_2 &= -16p + 16 + 4p^2 - T^2 + 2TU + 2T\nu + 15U^2 - 2U\nu - \nu^2.
\end{aligned} \tag{5.35}$$

Now, combining (5.32) and (5.35) gives $U = 0$. This, with (5.21), yields $p = T^2$ which is impossible.

Case 2: ind $2 \equiv 0 \pmod 7$. We solve (5.4) for $1 \leq s \leq 6$ and rearrange to obtain the following

$$\begin{aligned}
14C_1 &= 4p - 8 + 2T - 2\nu - 14C_6 \\
14C_2 &= 4p - 8 + 2T - 2\nu - 14C_5 \\
14C_3 &= 6p - 12 + 3T - 14U - 3\nu - 14C_5 - 14C_6 \\
14C_4 &= -2p + 4 - T + 14U + \nu + 14C_5 + 14C_6.
\end{aligned} \tag{5.36}$$

For ease of notation we write

$$y = (2p - 4 + T - \nu)/7, \qquad C_5 = r, \qquad C_6 = s \tag{5.37}$$

which, with (5.36) gives

$$\begin{aligned} C_1 &= y - s, & C_2 &= y - r, \\ C_3 &= 3y/2 - U - r - s, & C_4 &= -y/2 + U + r + s. \end{aligned} \tag{5.38}$$

Combining (5.38) with (5.23) gives

$$C_0 = p - 2 - 3y. \tag{5.39}$$

Substituting the values for the C_i from (5.38) and (5.39) into (5.26) gives the following values for h_0, h_1, h_2 and h_3:

$$\begin{aligned} h_0 &= 4 + p^2 - 4p - 6py + 12y + 4r^2 + 4s^2 + 27y^2/2 - 6sy - 6ry - 4Uy \\ &\quad +4rU + 2U^2 + 4sU + 4rs \\ h_1 &= -2y + r^2 - s^2 + py - 5y^2/4 - 2ry + Uy - U^2 - 2sU + 2rs \\ h_2 &= -2y - 2r^2 + s^2 + py - 2y^2 - sy + 2ry - 2rU + 2sU \\ h_3 &= -2y - r^2 - 2s^2 + py - 7y^2/2 + 4sy + 3ry + Uy - 2sU - 4rs. \end{aligned} \tag{5.40}$$

We eliminate the s^2 term from the equations in (5.40) by using (5.27) and setting $3h_1 - h_2 - 2h_3 = 0$ to give

$$3h_1 - h_2 - 2h_3 = 7r^2 + 21y^2/4 - 14ry + Uy - 3U^2 - 4sU + 14rs - 7sy + 2rU = 0. \tag{5.41}$$

Rearranging (5.41) gives the following equation for s:

$$s = (28r^2 + 21y^2 + 8rU - 56ry + 4Uy - 12U^2)/(28y + 16U - 56r). \tag{5.42}$$

Now, if the denominator in (5.42) were zero, we would have $r = y/2 + 2U/7$ which, substituting into (5.41) would yield $3h_1 - h_2 - 2h_3 = -13U^2/7 = 0$ and hence $U = 0$. Thus by (5.21) we would obtain the impossible result $p = T^2$. Therefore we must have $r \neq y/2 + 2U/7$, i.e.

$$r = y/2 - Uw, \qquad w \neq -2/7 \tag{5.43}$$

where w must be rational, due to the fact that y is rational and r and U must be integers (see (5.37) and (5.21)). Now, by (5.27) we have $h_1 - h_3 = 0$ and hence from (5.40)

$$2r^2 + s^2 + 9y^2/4 - 5ry - 4sy - U^2 + 6rs = 0. \tag{5.44}$$

Substituting for s and r from (5.42) and (5.43) into (5.44) and factorising we obtain

$$\frac{7U^2(3w - 1)(7w^3 - 7w^2 - 7w - 1)}{4(7w + 2)^2} = 0. \tag{5.45}$$

Now, since condition (5.21) means that U cannot be zero, we have either $7w^3 - 7w^2 - 7w - 1 = 0$ or $3w - 1 = 0$. However, the cubic polynomial in w cannot have any rational solutions

for the following reason. Assume that $7w^3 - 7w^2 - 7w - 1 = 0$ and that $w = a/b$ for some integers a and b, with $\gcd(a, b) = 1$. Therefore we have $7(a/b)^3 - 7(a/b)^2 - 7(a/b) - 1 = 0$, which multiplying through by b^3 gives

$$7a^3 - 7a^2b - 7ab^2 - b^3 = 0. \tag{5.46}$$

Now, the integer a must have a prime factor e. Therefore e must divide each term in Equation (5.46) and hence $e|b^3$ which contradicts the condition $\gcd(a, b) = 1$. Therefore we must have $3w - 1 = 0$ and hence

$$w = 1/3. \tag{5.47}$$

Thus by (5.43) we have

$$r = y/2 - U/3 \tag{5.48}$$

and substituting for r from (5.48) into (5.42) gives

$$s = y/2 - U/3. \tag{5.49}$$

Now, by Equation (5.27) we have

$$h_0 - h_1 - p = 0 \tag{5.50}$$

which by (5.40) gives

$$\begin{aligned} 4 + p^2 - 5p - 7py + 14y + 3r^2 + 5s^2 + 59y^2/4 \\ -6sy - 4ry - 5Uy + 4rU + 3U^2 + 6sU + 2rs \quad = 0. \end{aligned} \tag{5.51}$$

Substituting for r and s from (5.48) and (5.49) into (5.51) gives

$$4 + p^2 - 5p - 7py + 14y + 49y^2/4 + 7U^2/9 = 0 \tag{5.52}$$

and hence, on eliminating y from (5.37) we have

$$0 = -p + T^2/4 - T\nu/2 + \nu^2 + 7U^2/9. \tag{5.53}$$

Substituting for p from (5.21) into (5.53) and rearranging gives

$$27T^2 + 224U^2 + 18T\nu - 9\nu^2 = 0. \tag{5.54}$$

Solving (5.54) for T gives

$$9T = -3\nu \pm 2\sqrt{9\nu^2 - 168U^2}. \tag{5.55}$$

Now, by (5.1) and (5.2) ν can only take on the values -1 or 13. But $U \neq 0$, so if $\nu = -1$ the discriminant $9\nu - 168U^2$ is negative and (5.55) has no real solutions. If $\nu = 13$ we obtain from (5.55) $U^2 = 9$. Therefore we have $T = -5$ which contradicts the condition $T \equiv 1 \pmod 7$ from (5.21). Theorem 5.8 is proved. □

5.6 Nonexistence for $n = 18$

In this section $p = 18k + 1$ and we prove the following theorem.

Theorem 5.9 *QRDS and MQRDS do not exist for* 18*th powers.*

To prove Theorem 5.9 we require the cyclotomic constants for $n = 18$. These have been calculated by Baumert and Fredricksen [5, 6] and those cyclotomic constants relevant to the analysis in this section are given in Section A.8. The cyclotomic constants are given in terms of the integer parameters L, M, and C_i $(0 \leq i \leq 5)$ relative to a fixed primitive root g, and we let ind 2 and ind 3 denote the indices of 2 and 3, respectively, with respect to g. The quantities L, M and p satisfy the following equation

$$4p = L^2 + 27M^2 \tag{5.56}$$

where $L \equiv 7 \pmod 9$ [5, p. 208 and Equation (5.3)] and we define the quantity S as follows:

$$S = \sum_{i=0}^{5} C_i \zeta_9^i \qquad \zeta_9 = \exp(2\pi i/9). \tag{5.57}$$

If we denote the complex conjugate of S by $\bar{S}$ then, since S is a Jacobi sum, we have

$$S\bar{S} = |S|^2 = p \tag{5.58}$$

[5, p. 209]. Noting that $\zeta_9^6 + \zeta_9^3 + 1 = 0$ then, if we combine Equations (5.57) and (5.58), we obtain the following equations when the coefficients of the powers ζ_9 are compared:

$$\begin{aligned}
\zeta_9^0: \quad p = {} & C_0^2 + C_1^2 + C_2^2 + C_3^2 + C_4^2 + C_5^2 - C_0C_3 - C_1C_4 - C_2C_5 && (5.59)\\
\zeta_9^1: \quad 0 = {} & C_0C_1 + C_1C_2 + C_2C_3 + C_3C_4 + C_4C_5 - C_0C_2 - C_1C_3 \\
& -C_2C_4 - C_3C_5 && (5.60)\\
\zeta_9^2: \quad 0 = {} & C_0C_2 + C_1C_3 + C_2C_4 + C_3C_5 - C_0C_1 - C_1C_2 - C_2C_3 \\
& -C_3C_4 - C_4C_5 && (5.61)\\
\zeta_9^4: \quad 0 = {} & C_0C_4 + C_1C_5 - C_0C_2 - C_1C_3 - C_2C_4 - C_3C_5 + C_0C_5 && (5.62)\\
\zeta_9^5: \quad 0 = {} & C_0C_5 - C_0C_1 - C_1C_2 - C_2C_3 - C_3C_4 - C_4C_5 + C_0C_4 \\
& +C_1C_5 && (5.63)
\end{aligned}$$

(note that the terms in ζ_9^3 cancel to give a coefficient of zero).

For $n = 18$ the cyclotomic constants are split into 54 separate cases, determined by the nine values of ind 2 (mod 9) and the six values of ind 3 (mod 6) [5, p. 212]. However, Baumert and Fredricksen demonstrated that due to restrictions imposed by the quadratic character of 3 and by suitably changing the primitive root, all possibilities can be derived from just eight separate cases [5, pp. 212-215]. These are:
(a) ind $2 \equiv 0 \pmod 9$, ind $3 \equiv 0 \pmod 3$
(b) ind $2 \equiv 0 \pmod 9$, ind $3 \equiv 1 \pmod 3$

(c) ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 0 \pmod 3$
(d) ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 1 \pmod 3$
(e) ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 2 \pmod 3$
(f) ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 0 \pmod 3$
(g) ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 1 \pmod 3$
(h) ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 2 \pmod 3$.
We apply Equation (5.4) to each of these cases in turn to prove Theorem 5.9.

Proof of Theorem 5.9. Case 1: ind $2 \equiv 0 \pmod 9$, ind $3 \equiv 0 \pmod 3$. Setting $(1, 9) = (4, 9)$ as per Equation (5.4) gives $18C_1 - 18C_4 - 18C_5 = -18C_2 + 18C_4 + 18C_5$ and hence

$$C_1 + C_2 = 2C_4 + 2C_5. \tag{5.64}$$

Also, setting $(1, 9) = (2, 9)$ and simplifying gives

$$2C_1 = C_2 + C_4 + C_5. \tag{5.65}$$

Combining Equations (5.64) and (5.65) gives

$$C_1 = C_2 = C_4 + C_5. \tag{5.66}$$

Setting $(3, 9) = (6, 9)$ (where $(6, 9) = (3, 12)$ on using (2.18) and (2.19) we obtain

$$C_3 = M. \tag{5.67}$$

We now substitute for C_1, C_2 and C_3 from (5.66) and (5.67) into Equations (5.61) and (5.62) to give respectively

$$\begin{aligned} C_5^2 + 2C_4C_5 + MC_4 - MC_5 &= 0 \\ C_5^2 - C_4^2 - MC_4 - 2MC_5 &= 0. \end{aligned} \tag{5.68}$$

Eliminating C_4 from Equations (5.68) gives

$$C_5^3 - 3C_5M^2 - M^3 = 0. \tag{5.69}$$

Now, Equation (5.69) is of the form $x^3 - 3x - 1 = 0$ with $x = C_5/M$, which has no rational solutions. Therefore $M = C_5 = 0$ which, from (5.56) gives $4p = L^2$ and hence a contradiction.

Case 2: ind $2 \equiv 0 \pmod 9$, ind $3 \equiv 1 \pmod 3$. By (5.4), setting $(2, 9) = (7, 9)$ $(= (2, 11))$ and simplifying gives

$$2C_4 + C_5 = 0. \tag{5.70}$$

Also, setting $(1, 9) = (5, 9)$ $(= (4, 13))$ gives

$$C_1 + C_2 = 4C_4 \tag{5.71}$$

and setting $(1, 9) = (8, 9)$ $(= (1, 10))$ gives

$$C_2 = C_5 + 2C_1. \tag{5.72}$$

Combining Equations (5.70), (5.71) and (5.72) gives

$$C_1 = C_2 = 2C_4 = -C_5. \tag{5.73}$$

Setting $(2, 9) = (8, 9)$ $(= (1, 10))$ gives

$$4C_1 + C_2 + C_4 + C_5 = 0 \tag{5.74}$$

which, substituting for C_1, C_2 and C_5 from (5.73) gives

$$C_1 = C_2 = C_4 = C_5 = 0. \tag{5.75}$$

Now, setting $(3, 9) = (2, 9)$ gives

$$M = -C_3 \tag{5.76}$$

and setting $324(1, 9) = p + 1 + 2\nu$ from (5.4) gives

$$L = 2\nu. \tag{5.77}$$

The formula $324(6, 9) = p + 1 + 2\nu$, with (5.76) and (5.77) gives $p + 1 + L = p + 1 - 8L + 18C_0 + 9M$ and hence with (5.77) we get

$$M = 2(\nu - C_0). \tag{5.78}$$

Combining (5.75), (5.59) and (5.76) gives $p = C_0^2 + M^2 + MC_0$ and hence, by (5.78) we obtain

$$p = 3C_0^2 + 4\nu^2 - 6C_0\nu. \tag{5.79}$$

Eliminating M and L from (5.56), (5.77) and (5.78) gives

$$p = 27C_0^2 - 54C_0\nu + 28\nu^2. \tag{5.80}$$

Since Equations (5.79) and (5.80) are equal, we obtain $C_0^2 - 2C_0\nu + \nu^2 = (C_0 - \nu)^2 = 0$ and therefore $C_0 = \nu$, which, by (5.78), gives $M = 0$ and by (5.56) the contradiction $4p = L^2$.

Case 3: ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 0 \pmod 3$. Setting $(3, 9) = (6, 9)$ $(= (3, 12))$ and simplifying gives

$$-2C_1 + 3C_2 + 3C_3 + 2C_4 - 4C_5 = 0. \tag{5.81}$$

Also, setting $(1, 9) = (7, 9)$ $(= 2, 11))$ gives

$$5C_1 - 5C_4 + 4C_5 = 0 \tag{5.82}$$

and $(7, 9) = (4, 9)$ gives

$$C_1 - C_4 - C_5 = 0. \tag{5.83}$$

Combining Equations (5.81), (5.82) and (5.83) we have

$$C_5 = 0, \qquad C_1 = C_4, \qquad C_2 = -C_3. \tag{5.84}$$

Substituting for C_1, C_2 and C_5 from (5.84) into (5.63) gives $C_3^2 = 0$ and hence with (5.84) we get

$$C_3 = C_2 = 0. \tag{5.85}$$

Combining Equations (5.62), (5.84) and (5.85) gives

$$C_0 C_4 = 0 \tag{5.86}$$

and so at least one of C_0 or C_4 must be zero. Also, combining (5.84) and (5.85) with (5.59) gives

$$p = C_0^2 + C_4^2. \tag{5.87}$$

Combining (5.86) and (5.87) gives either $p = C_0^2$, $p = C_4^2$ or $p = 0$, all of which are contradictions.

Case 4: ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 1 \pmod 3$. Setting $(3, 9) = (6, 9)$ $(= (3, 12))$ we have

$$-2C_1 + C_2 + 3C_3 + 2C_4 = 0 \tag{5.88}$$

and setting $(4, 9) = (7, 9)$ $(= (2, 11))$ gives

$$-2C_1 + C_2 + 2C_4 = 0. \tag{5.89}$$

From (5.88) and (5.89) we obtain

$$C_3 = 0. \tag{5.90}$$

Since $(1, 9) = (7, 9)$, we have

$$5C_1 + 2C_2 = 5C_4. \tag{5.91}$$

Combining (5.89) and (5.91) gives

$$C_1 = C_4, \qquad C_2 = 0. \tag{5.92}$$

Now, using Equation (5.4), $p + 2\nu + 1 = 324(4, 9)$ and hence $2p + 4\nu + 2 = 648(4, 9)$. Therefore, using the formula for the cyclotomic constant $(4, 9)$ we obtain $2p + 4\nu + 2 = 2p + 2 + 2L + 18M + 36C_0 + 18C_1 - 36C_2 - 36C_3 - 18C_4$ and hence, employing (5.90) and (5.92), we have

$$L + 9M + 18C_0 = 2\nu. \tag{5.93}$$

We now set $(5, 9) = (8, 9)$ (i.e. $(4, 13) = (1, 10)$) to give $L+3M-2C_0-2C_1+C_2+C_3+2C_4 = 0$ which, using (5.90) and (5.92) gives

$$L + 3M - 2C_0 = 0. \tag{5.94}$$

Eliminating C_0 from (5.93) and (5.94) gives

$$5L + 18M = \nu. \tag{5.95}$$

Now, using (5.4) and adding the formulae for $(2,9)$, $(8,9)$ $(= (1,10))$ and $(5,9)$ $(= (4,13))$ we have $6p + 12\nu + 6 = 6p + 6 - 21L - 27M + 108C_3$ and hence by (5.90) we have

$$7L + 9M + 4\nu = 0. \tag{5.96}$$

Eliminating L from (5.95) and (5.96), we obtain $\nu = 3M$, which contradicts (5.2).

Case 5: ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 2 \pmod 3$. Using Equation (5.4) for the cyclotomic constants $(1,9)$, $(2,9)$, $(3,9)$, $(5,9)$ $(= (4,13))$, $(6,9)$ $(= (3,12))$, $(7,9)$ $(= (2,11))$ and $(8,9)$ $(= (1,10))$ gives

$$\begin{aligned}
(1,9): &\quad 4\nu = 2L + 18M - 36C_0\\
(2,9): &\quad 4\nu = -L + 45M - 12C_0 - 12C_1 + 6C_2 + 6C_3 + 24C_4 + 24C_5\\
(3,9): &\quad 4\nu = 5L - 9M - 6C_0 - 24C_1 - 24C_2 + 48C_3 + 12C_4 - 6C_5\\
(5,9): &\quad 4\nu = -19L - 9M + 78C_0 + 24C_1 - 30C_2 - 66C_3 - 12C_4 + 6C_5\\
(6,9): &\quad 4\nu = 5L - 9M - 6C_0 + 12C_1 - 6C_2 - 6C_3 - 24C_4 + 30C_5\\
(7,9): &\quad 4\nu = 2L + 18M - 36C_0 + 18C_1 + 36C_2 - 18C_4 - 36C_5\\
(8,9): &\quad 4\nu = -L - 63M + 42C_0 - 12C_1 + 24C_2 - 48C_3 - 12C_4 - 30C_5.
\end{aligned} \tag{5.97}$$

Solving the set of equations for each C_i and M in (5.97) gives the follwing

$$\begin{gathered}
C_2 = C_3 = C_5 = -C_0 = -(\nu + L)/9, \qquad C_1 = C_4 = (L - 8\nu)/9\\
M = (4\nu + L)/9.
\end{gathered} \tag{5.98}$$

By (5.98) and (5.60) we have $C_2^2 = 0$, giving $L = -\nu$ and hence from (5.98) $M = \nu/3$, which contradicts (5.2) for integer M.

Case 6: ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 0 \pmod 3$. Setting $(1,9) = (5,9)$ $(= (4,13))$ we obtain

$$C_1 = C_2 \tag{5.99}$$

and setting $(1,9) = (7,9)$ $(= (2,11))$ gives $2C_1 + 2C_5 = C_2 + C_4$ which, with (5.99) gives

$$C_1 + 2C_5 = C_4. \tag{5.100}$$

Also, since $(2,9) = (8,9)$ $(= (1,10))$ then we have $5C_1 + 5C_2 - C_4 - C_5 = 0$ which, with (5.99) and (5.100) gives

$$C_5 = 3C_4/7, \qquad C_1 = C_4/7. \tag{5.101}$$

Now, since by $(1,9) = (8,9)$ we have $6C_1 - C_2 - 5C_4 + 4C_5 = 0$. Therefore employing (5.99) and (5.101) gives

$$C_1 = C_2 = C_4 = C_5 = 0. \tag{5.102}$$

Finally, since $(3,9) = (4,9)$ we obtain $M = C_2 + C_4$ which by (5.102) gives $M = 0$. Therefore, substituting $M = 0$ into (5.56) yields the contradiction $4p = L^2$.

Case 7: ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 1 \pmod 3$. Setting $(2,9) = (5,9)$ $(= (4,13))$ we obtain

$$C_1 + C_5 = 0 \tag{5.103}$$

and setting $(5, 9) = (8, 9)$ (i.e. $(4, 13) = (1, 10)$) gives

$$C_2 + C_4 = 0. \tag{5.104}$$

Now, setting $(1, 9) = (4, 9)$ gives $-C_1 + 2C_2 - 4C_4 - C_5 = 0$ and hence with (5.103) and (5.104) we have

$$C_2 = C_4 = 0. \tag{5.105}$$

Setting $(1, 9) = (2, 9)$ gives $3C_1 - 4C_4 + C_5 = 0$, which combined with (5.103) and (5.105) gives

$$C_1 = C_5 = 0. \tag{5.106}$$

Using (5.4) with the cyclotomic constant $(1, 9)$ we have

$$2p + 4\nu + 2 = 2p + 2 + 2L + 18C_1 + 18C_2 - 54C_4 - 18C_5$$

which with (5.105) and (5.106) gives

$$L = 2\nu. \tag{5.107}$$

Similarly using the formula for $(3, 9)$ gives $2p + 4\nu + 2 = 2p + 2 - 16L + 36C_0 + 36C_3$ and hence by (5.107) we have

$$\nu = C_0 + C_3. \tag{5.108}$$

Using the formula for $(6, 9)$ $(= 3, 12))$ we have $2p + 4\nu + 2 = 2p + 2 + 2L - 54M - 54C_0$ and hence from (5.107)

$$C_0 = -M. \tag{5.109}$$

Thus by (5.108) and (5.109) we obtain

$$C_3 = \nu + M. \tag{5.110}$$

Combining Equations (5.105), (5.106), (5.109) and (5.110) with (5.59) gives $p = M^2 + (\nu + M)^2 + M(\nu + M)$ and hence

$$p = 3M^2 + 3\nu M + \nu^2. \tag{5.111}$$

Eliminating p from Equations (5.56) and (5.111) gives $L^2 + 15M^2 = 12\nu M + 4\nu^2$ which, upon employing (5.107) gives

$$5M^2 = 4\nu M. \tag{5.112}$$

Therefore we obtain from (5.112) either $M = 0$ which with (5.56) leads to the contradiction $4p = L^2$, or $M = 4\nu/5$ which contradicts (5.2) for integer M.

Case 8: ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 2 \pmod 3$. Using (5.4) with the cyclotomic constants $(1, 9)$, $(2, 9)$ and $(8, 9)$ $(= (1, 10))$ and summing gives $6(p+2\nu+1) = 6p+6+6L$ and hence

$$L = 2\nu. \tag{5.113}$$

Also, calculating the formula for $(3, 9)$ with (5.4) gives $2p + 4\nu + 2 = 2p + 2 + 2L - 54M$ and hence

$$4\nu = 2L - 54M. \tag{5.114}$$

Combining (5.113) and (5.114) gives $M = 0$ which, in view of (5.56) gives the contradiction $4p = L^2$.

As we have reached contradictions in all cases the proof of Theorem 5.9 is complete.

□

Chapter 6

Qualified Difference Sets from Unions of Cyclotomic Classes

6.1 Introduction

In this chapter we describe a cyclotomic extension of the QRDS and MQRDS to produce new QDS and MQDS. The new sets are created from the unions of two or more smaller sets of integers modulo certain types of prime p, which are themselves generated using as a basis the theory of cyclotomy with respect to the integer order n (see Section 2.4). We first present a preliminary discussion in Section 6.2, where we introduce a few definitions and a necessary lemma. We then present the theoretical considerations of the chapter in Section 6.3. A description of the results obtained is given in Section 6.4 and the results themselves for $n = 4, 6, 8, 10$ and 12 are presented in Sections 6.5 to 6.8. As will be seen, some new isolated systems were discovered for the cases $n = 6, 10$ and 12 (Sections 6.6, 6.7 and 6.8 respectively), and two new entire families of QDS were discovered in the case $n = 8$ (Section 6.5).

6.2 Preliminary Discussion

The QDS and MQDS have similar properties to the RDS and MRDS respectively, which were discussed in detail in 1953 by Lehmer [47]. In his subsequent extensive survey, Hall extended the notion of 'residue difference sets' and discovered a new family of difference set that can be created from a union of 6th power *cyclotomic classes* [36, Theorem 2.2]. We define the *nth power cyclotomic class* $C(c_i)$ as follows.

Definition 6.1 *Let*

$$p = nf + 1 \tag{6.1}$$

be an odd prime, with n and f being positive integers, and let g be a primitive root of p. The nth power cyclotomic class $C(c_i)$ is given by the set of integers derived from the

congruence

$$C(c_i) = \{g^{un+c_i} \pmod p : 0 \leq u \leq f-1\}. \tag{6.2}$$

Note that $C(c_i) = C(c_i + \gamma n)$ for integer γ. Hall discovered that if $n = 6$ and if a primitive root g of p is chosen such that $\text{ind}_g\ 3 = 1$ then the union of cyclotomic classes $C(0) \cup C(1) \cup C(3)$ forms a difference set for all prime moduli of the form $p = 4\alpha^2 + 27$ (integer α). For example, let $\alpha = 1$ giving $p = 31$ and $f = 5$. Noting that $g = 3$ is a primitive root of $p = 31$ satisfying $\text{ind}_g\ 3 = 1$ and using this value of g in (6.2) gives the following cyclotomic classes:

$$\begin{aligned} C(0) &= \{1, 2, 4, 8, 16\} \\ C(1) &= \{3, 6, 12, 17, 24\} \\ C(3) &= \{15, 23, 27, 29, 30\}. \end{aligned}$$

Now, the union of these cyclotomic classes gives the set

$$R = \{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\}$$

which upon inspection can be shown to be a $(31, 15, 7)$ difference set as per Definition 2.2.

Hayashi later extended Hall's theorem, noting that if a primitive root g is chosen such that $\text{ind}_g\ 3 = 2$ then the union of cyclotomic classes $C(0) \cup C(2) \cup C(3)$ also forms a difference set for all $p = 4\alpha^2 + 27$ (integer α) [38, p. 73].

In this chapter we demonstrate the existence of QDS and MQDS that are similarly composed of unions of cyclotomic classes. These sets are defined as follows.

Definition 6.2 *Let $p = nf + 1$ be a prime and $k = tf$ where k and t are positive integers. Let $E = \{c_1, c_2, \ldots, c_t\}$ 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 E as follows:*

$$R = \{r_i : 1 \leq i \leq k\} = C(c_1) \cup C(c_2) \cup \ldots \cup C(c_t) \tag{6.3}$$

where $C(c_i)$ is defined by (6.2). If a set R of the form of the set in (6.3) is a QDS then we call it a QDS composed of a union of cyclotomic classes. Now let R^* be the $k+1$-element set consisting of the union of nth power cyclotomic classes, together with the residue zero, derived from the set E as follows:

$$R^* = \{r_i : 0 \leq i \leq k\} = C(c_1) \cup C(c_2) \cup \ldots \cup C(c_t) \cup \{0\}, \quad r_0 = 0 \tag{6.4}$$

where $C(c_i)$ is defined by (6.2). If a set R^* of the form of the set in (6.4) is a MQDS then we call it a MQDS composed of a union of cyclotomic classes.

Note that if we set $t = 1$ in Definition 6.2, we obtain the special cases of QDS and MQDS from a single cyclotomic class, which are the QRDS and MQRDS respectively, as discussed in Chapters 3, 4 and 5. Since we have $k = tf$ then we have a slight modification to Equations (3.1) and (3.2) to give the following lemma.

Lemma 6.3 *For a QDS composed of t cyclotomic classes we have*

$$p = \lambda(n/t)^2 + 1 \tag{6.5}$$

and for a MQDS composed of t cyclotomic classes we have

$$p = \lambda(n/t)^2 - 2(n/t) + 1. \tag{6.6}$$

Proof. For a QDS of k elements we have Equation (2.12). Substituting $k = tf$ into (2.12) and eliminating the parameter f using (6.1) gives (6.5). For a MQDS of $k + 1$ elements (including zero), we have Equation (2.13). Substituting $k = tf$ into (2.13) and combining with (6.1) gives (6.6). □

Motivated by Hall's discovery, Hayashi undertook an exhaustive computer search for all the possible difference sets composed of unions of cyclotomic classes for the case $n = 10$ [38]. Although his project failed to uncover any new difference sets, his approach re-established some known results and also provides a very useful technique in this chapter to search for QDS and MQDS composed of unions of cyclotomic classes as defined in Definition 6.2. It should be noted here that Baumert has demonstrated the nonexistence of any new residue difference sets from unions of cyclotomic classes in the case $n = 4$ [8, pp. 128-129].

The purpose of this chapter is to describe the results of an exhaustive search for QDS and MQDS created from the unions of cyclotomic classes for the cases $n = 4, 6, 8, 10$ and 12. Two new families were discovered in the case $n = 8$ and some new isolated systems were discovered for $n = 6, 10$ and 12.

6.3 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 non-zero differences occur between the elements of sets of different cyclotomic classes. This can be done as follows, using a similar approach to that adopted by Hall [36] and Hayashi [38] in their analyses. Following (2.9), consider the congruence

$$Y - mX \equiv d \pmod{p} \tag{6.7}$$

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

$$g^{B'n+i+\sigma-s} + 1 \equiv g^{A'n+j-s} \pmod{p} \tag{6.8}$$

where A' and B' are also integers. Now by the cyclotomic constant equation (2.17), we see that Congruence (6.8), and hence Congruence (6.7), has $(i + \sigma - s, j - s)$ solutions. This enables us to calculate how often each difference d arises from Congruence (6.7), and hence how often each difference arises from sets of integers composed of unions of cyclotomic classes. For the set of residue classes $E = \{c_1, c_2, \ldots, c_t\}$, the general equation for the number $N(s)$ of times the difference d in residue class s occurs is given by

$$N(s) = \sum_{i \in E} \sum_{j \in E} (i + \sigma - s, j - s). \tag{6.9}$$

Note by Equation (2.21) 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. In this case we need to consider the two additional differences:

$$Y - 0 \equiv d \pmod{p} \tag{6.10}$$

$$0 - mX \equiv d \pmod{p}. \tag{6.11}$$

For Congruence (6.10) we have $Y \equiv d \pmod{p}$ and so d, which is in residue class s, also is in residue class j. Therefore $j = s$ and hence $s \in E$. This means that we need to add 1 to the summation $N(s)$ in Equation (6.9) if $s \in E$. Congruence (6.11) is a little more complicated. Here we have $(-1)(mX) \equiv d \pmod{p}$ and mX is in residue class $\sigma + i$. Now, since g is a primitive root of p

$$(-1) \equiv g^{(p-1)/2} \equiv g^{nf/2} \equiv \begin{cases} g^{n(f/2)} & \text{if } f \text{ is even} \\ g^{n(f-1)/2+n/2} & \text{if } f \text{ is odd.} \end{cases} \tag{6.12}$$

Therefore if f is even, then -1 is in residue class 0. In this case, by (6.11), d, which is in residue class s, is also in residue class $\sigma + i + 0$ (i.e. the residue class of $-mX$). Therefore $i = s - \sigma$ and so we must add 1 to the summation for $N(s)$ in Equation (6.9) if $s - \sigma \in E$. If f is odd, then by Equation (6.12) -1 is in residue class $n/2$. Here, by (6.11), 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 (6.9) if $s - \sigma - n/2 \in E$.

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 [8, pp. 2-3]) and the same applies to QDS and MQDS. If R is a QDS, then the set $R^* = \mathbb{Z}_p - R$ is a MQDS which is the complement of R, that has the same qualifier m. Stated differently, if E is the set of residue classes that gives a QDS, then $E^* = \mathbb{Z}_n - E$ is the set of residue classes that, with the residue zero, gives the corresponding complementary MQDS. In the case of a MQDS, R^*, the same argument applies. If $E = \{c_1, c_2, \ldots, c_t\}$ is a set of residue

classes, together with the residue zero, that produces a MQDS R^* then $E^* = \mathbb{Z}_n - E$ will give rise to a complementary QDS. The detailed analysis of this point is given in Appendix B. Because of this equivalence, it is only necessary to analyse cases where $t \leq n/2$.

For each value of n, there are many other equivalent cases that arise due to the following two isomorphisms. Firstly, assume that $E = \{c_1, c_2, \ldots, c_t\}$ is a set of residue classes that produces a QDS. Therefore, Congruence (6.7) and Equation (6.9) lead to values of $N(s)$ that are equal for all s. Now consider the set $E' = \{c_1 + q, c_2 + q, \ldots, c_t + q\}$ for some integer q. Using Equation (6.9) the summation $N(s)$ for the set E' is as follows:

$$\begin{aligned} N(s) &= \sum_{i \in E'} \sum_{j \in E'} (i + \sigma - s, j - s) \\ &= \sum_{i \in E} \sum_{j \in E} (i + q + \sigma - s, j + q - s) \\ &= \sum_{i \in E} \sum_{j \in E} (i + \sigma - [s - q], j - [s - q]) \\ &= N(s - q). \end{aligned} \tag{6.13}$$

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

Secondly assume that $E = \{c_1, c_2, \ldots, c_t\}$ 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 Equation (6.2) we have

$$C(c) = \{g^{un+c} \pmod p : 0 \leq u \leq f - 1\}. \tag{6.14}$$

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

$$g_1^z \equiv g \pmod p \tag{6.15}$$

where z must be prime to $p - 1 = nf$. Substituting this into (6.14) gives

$$C(c) = \{g_1^{zun+zc}\} = \{g_1^{zc}(g_1^n)^{uz} \pmod p : 0 \leq u \leq f - 1\}. \tag{6.16}$$

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 (6.16) becomes

$$C(c) = \{g_1^{zc}(g_1^n)^u\} = \{g_1^{un+zc} \pmod p : 0 \leq u \leq f - 1\}. \tag{6.17}$$

Comparing (6.14) with (6.17) shows that a QDS derived from $E = \{c_1, c_2, \ldots, c_t\}$ and primitive root g will be the same as that derived from $E = \{zc_1, zc_2, \ldots, zc_t\}$ and primitive root g_1 where $g_1^z \equiv g \pmod{p}$. In the case of a MQDS, the same argument evidently applies.

6.4 Results

Equation (6.9) has been applied to the cases $n = 4, 6, 8, 10$ and 12 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 $1 \leq \sigma \leq n-1$, for f odd and f even (note that $\sigma = 0$ corresponds to difference sets, which is not the subject of this chapter). Also, in any exhaustive analysis, one must take account of the additional individual conditions for each value of n, such as the $(n/2)$th power character of 2, for example. This has also been done and each such condition, where necessary, is addressed in the relevant section below.

The results below are given up to equivalence, either by complementary sets or isomorphism (see Section 6.3). A major positive result was revealed in the case $n = 8$, This, therefore, is where we begin.

6.5 Results for $n = 8$

In this section we prove the following theorem.

Theorem 6.4 *Qualified difference sets created from the union of 8th power cyclotomic classes $C(0) \cup C(1)$ exist for all primes of the form $p = 64z^4 + 128z^3 + 144z^2 + 80z + 17$ or $p = 64z^4 + 48z^2 + 1$ where z is an integer in each case. All other unions of 8th 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 (i.e. 4th power) residue or a biquadratic nonresidue of p. In order to demonstrate the computational methods used in this chapter, a detailed analysis follows, whereby we generate a QDS for the case when f is even, $t = 2$, $R = C(0) \cup C(1)$, $\sigma = 4$ and 2 is a biquadratic nonresidue of p.

For $R = C(0) \cup C(1)$ we have $E = \{0, 1\}$. Using this with $\sigma = 4$ and using Definition 6.2, along with Equations (6.9) and (2.21), gives the following condition for the number of differences $N(s)$:

$$\begin{aligned} s = 0: &\quad N(0) = (4,0) + (4,1) + (5,0) + (5,1) \\ s = 1: &\quad N(1) = (3,7) + (3,0) + (4,7) + (4,0) \\ s = 2: &\quad N(2) = (2,6) + (2,7) + (3,6) + (3,7) \\ s = 3: &\quad N(3) = (1,5) + (1,6) + (2,5) + (2,6). \end{aligned} \tag{6.18}$$

In this case the values for $s = 4, 5, 6, 7$ repeat those for $s = 0, 1, 2, 3$ respectively. Following Dickson's work [25, p. 410, Theorem 11], Berndt et al. demonstrated that the cyclotomic constants for $n = 8$ are determined uniquely by

$$p = a_4^2 + b_4^2 = a_8^2 + 2b_8^2 \tag{6.19}$$

where a_4, b_4, a_8 and b_8 are integers (see also Equation (5.9)) and for the case $p = 8f + 1$:

$$a_4 \equiv -(2/p) \equiv -1 \pmod 4, \qquad b_4 \equiv a_4 g^{(p-1)/4} \pmod p \tag{6.20}$$

[10, p. 78], and

$$a_8 \equiv -1 \pmod 4, \qquad 2b_8 \equiv a_8(g^f + g^{3f}) \pmod p \tag{6.21}$$

[10, p. 109]. The cyclotomic constants for $n = 8$ have been calculated by Lehmer [48] and are given in Section A.4. Substituting these cyclotomic constants for the case when 2 is a biquadratic nonresidue of p into Equations (6.18) gives:

$$\begin{aligned}
s = 0: &\quad 64N(0) = 4p - 12 + 4a_4 + 4a_8 \\
s = 1: &\quad 64N(1) = 4p - 12 + 4a_4 + 4a_8 \\
s = 2: &\quad 64N(2) = 4p + 4 - 4a_4 - 4a_8 + 8b_4 - 16b_8 \\
s = 3: &\quad 64N(3) = 4p + 4 - 4a_4 - 4a_8 + 16b_8 - 8b_4.
\end{aligned} \tag{6.22}$$

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 (6.22) gives:

$$\begin{aligned}
b_4 &= 2b_8 \\
a_4 + a_8 &= 2.
\end{aligned} \tag{6.23}$$

Combining Equations (6.23) and (6.19), and setting $x = -a_4$ and $2y = b_4$ for ease of notation, gives

$$\begin{aligned}
p &= x^2 + 8x + 8 \qquad\qquad x \equiv 1 \pmod 4 \\
y^2 &= 2 + 2x.
\end{aligned} \tag{6.24}$$

Now, since $x \equiv 1 \pmod 4$ then $y^2 = 2 + 2x$ is of the form $y^2 = 4l^2$, where l is an odd integer, and so $x = 2l^2 - 1$, l odd. Thus, $x = 8z^2 + 8z + 1$ for integer z which, using (6.24), gives

$$p = 64z^4 + 128z^3 + 144z^2 + 80z + 17 \tag{6.25}$$

where z is an integer, as in the statement of Theorem 6.4. Now, under the conditions in Equation (6.19), 2 is always a biquadratic nonresidue of p of the form in Equation (6.24) by the following analysis. Equation (6.24) 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 (6.24) 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, [51, Corollary 5.71]) and as a result we will always obtain values for $N(s)$ as given by the equations in (6.22). The condition in (6.25) appears strict, but there are fifty primes of this form $\leq 10^{11}$ and eighty primes $\leq 10^{12}$. The sequence begins $p = 17, 433, 2801, 10193, 60017, \ldots$. Since the polynomial (6.25) is irreducible over the integers it is expected that there would be an infinite number of primes of this form but this would be very difficult to establish, as is the case even for polynomials of degree two.

The values of those primitive roots that can be used to generate the QDS are determined by the condition $b_4 = 2b_8$ from Equation (6.23). Substituting for b_4 and b_8 from (6.20) and (6.21) into the first equation in (6.23) and rearranging gives

$$a_8\mu^2 - a_4\mu + a_8 \equiv 0 \pmod p \tag{6.26}$$

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

$$(2a_8\mu - a_4)^2 \equiv a_4^2 - 4a_8^2 \pmod p. \tag{6.27}$$

Congruence (6.27) 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 $n = 8$, $\sigma = 4$, $R = C(0) \cup C(1)$ 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 Equation (6.24). We can write $p = x^2 + 4x + 4 + 4x + 4 = (x + 2)^2 + 2y^2$ and so, by uniqueness with (6.19) we have $b^2 = y^2$ 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 (6.23) is satisfied. Now since $x + a + 2 = 0$, we have $a = -(x + 2)$ so we can write

$$x^2 - 4a^2 = -[x^2 + 2(x^2 + 8x + 8)] = -(x^2 + 2p) \equiv -x^2 \pmod p. \tag{6.28}$$

However $(-1/p) = 1$, where $(-1/p)$ is the Legendre symbol, since $p \equiv 1 \pmod 4$. Combining this with (6.28) means that $x^2 - 4a^2$ is a square modulo p and so Congruence (6.27) always has a solution and so there is always a QDS of the current form under the conditions in (6.24).

An example of a QDS of the form in (6.24) is as follows.

Example 6.5 *The parameters $n = 8$, $f = 2$, $t = 2$, $R = C(0) \cup C(1)$ and $k = tf = 4$, yield a QDS of modulus $p = 17$ and multiplicity $\lambda = 1$.*

This particular QDS has 4 elements. The parameters satisfy (6.25) for $z = 0$ and also (6.24) for the case $x = -a_4 = 1$ which, in turn by Equation (6.23), gives $a_8 = 3$. We now need to determine a primitive root g that will generate the corresponding QDS, the full

set of primitive roots of the prime 17 being $3, 5, 6, 7, 10, 11, 12$ and 14. Using Congruence (6.27) we have

$$(6\mu + 1)^2 \equiv 16 \pmod{17} \tag{6.29}$$

where $\mu = g^f = g^2$. The integers congruent to 16 modulo 17 that give squares of the form $(6g^2+1)^2$ are $3025, 47089, 528528$ and 1385329. These give values of $g = 3, 6, 11$ and 14 respectively, any of which can be used to generate a QDS with the given parameters. Using Equation (6.2) with $g = 3$, we have

$$C(c_1) = \{g^{un+c_1} : 0 \le u \le f-1\} = \{3^{8u+0} : 0 \le u \le 1\} = \{3^0, 3^8\} \equiv \{1, 16\} \pmod{17}$$
$$C(c_2) = \{g^{un+c_2} : 0 \le u \le f-1\} = \{3^{8u+1} : 0 \le u \le 1\} = \{3^1, 3^9\} \equiv \{3, 14\} \pmod{17}$$

the union of which gives the set $R = \{1, 3, 14, 16\} \pmod{17}$. We now need to choose a qualifier, m, that is in residue class $\sigma = 4$. Therefore, $m \equiv g^{un+\sigma} \equiv 3^{8u+4} \pmod{17}$, which gives $m = 4$ or $m = 13$. Using $m = 4$ we get the set $mR = \{4, 12, 56, 64\} \equiv \{4, 12, 5, 13\}$. Therefore we have

$$\begin{aligned} R &= \{1, 3, 14, 16\} \pmod{17} \\ mR &= \{4, 5, 12, 13\} \pmod{17}. \end{aligned} \tag{6.30}$$

Note that using the qualifier $m = 13$ gives rise to the same set of integers as mR in (6.30), but in a different order. It can be readily seen that taking all 16 differences $R - mR \pmod{17}$ between the elements of the sets in (6.30) gives the integers $1, 2, \ldots, 16$ exactly once each. Therefore R is a QDS with multiplicity $\lambda = 1$, which agrees with Equation (2.12). Note in this example, that the corresponding complementary MQDS R^* is given by $R^* = \{0, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15\}$ which can be generated by $R^* = C(2) \cup C(3) \cup C(4) \cup C(5) \cup C(6) \cup C(7) \cup \{0\}$.

The second family of QDS in Theorem 6.4 arises when 2 is a biquadratic residue of p. Using (6.18) for this case gives the following:

$$\begin{aligned} s = 0: &\quad 64N(0) = 4p - 12 - 4a_4 - 4a_8 + 8b_4 - 16b_8 \\ s = 1: &\quad 64N(1) = 4p - 12 - 4a_4 - 4a_8 - 8b_4 + 16b_8 \\ s = 2: &\quad 64N(2) = 4p + 4 + 4a_4 + 4a_8 \\ s = 3: &\quad 64N(3) = 4p + 4 + 4a_4 + 4a_8. \end{aligned} \tag{6.31}$$

Equalising all the values of $N(s)$ in (6.31) gives:

$$\begin{aligned} b_4 &= 2b_8 \\ a_4 + a_8 &= -2. \end{aligned} \tag{6.32}$$

Combining (6.32) and (6.19) gives here

$$\begin{aligned} p &= x^2 - 8x + 8 \qquad\qquad x \equiv 1 \pmod{4} \\ y^2 &= 2 - 2x. \end{aligned} \tag{6.33}$$

Now, since $x \equiv 1 \pmod{4}$ then $y^2 = 2 - 2x$ is of the form $y^2 = 16z^2$, where z is an integer, and so $x = 1 - 8z^2$. Thus using (6.33) this gives

$$p = 64z^4 + 48z^2 + 1 \tag{6.34}$$

where z is an integer, as in the statement of Theorem 6.4. Under the conditions in Equation (6.19), 2 is always a biquadratic residue of p of the form in Equation (6.33) as follows. Equation (6.33) gives $y^2 = 2(1 - x)$, but since $x \equiv 1 \pmod 4$ then we have $y^2 = 16\eta_2^2$ where η_2 must be an integer. Substituting this into (6.33) gives $p = x^2 + 64\eta_2^2$. This means that p is always of the correct form for 2 to be a biquadratic residue of p by the same biquadratic reciprocity theorem as referenced above [51, Corollary 5.71]. Therefore we will always obtain values for $N(s)$ as given by the equations in (6.31). Again, proof of the infinitude of primes of the form in (6.34) would be extremely difficult but an infinite number would be expected. There are fifty seven primes of the form $\leq 10^{11}$ and eighty five $\leq 10^{12}$, the sequence beginning $p = 113, 1217, 41201, 84673, 644801 \ldots$.

To calculate the required primitive roots in this case, firstly note that from (6.32) $b_4 = 2b_8$. Therefore using (6.20) and (6.21) similarly gives (6.26) and hence (6.27) as in the case when 2 is a biquadratic nonresidue of p. Therefore the primitive roots g are calculated exactly in the same manner as in the earlier case, but here with the different values of a_4 and a_8, as derived from the second equation in (6.32).

For the converse, assume that we have a prime of the form given in Equation (6.33). We can write $p = x^2 - 4x + 4 - 4x + 4 = (x - 2)^2 + 2y^2$ and so, by uniqueness with (6.19) we have $b^2 = y^2$ 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 (6.32) is satisfied. Now since $a = 2 - x$ we can write

$$x^2 - 4a^2 = -[x^2 + 2(x^2 - 8x + 8)] = -(x^2 + 2p) \equiv -x^2 \pmod p. \tag{6.35}$$

As above, $(-1/p) = 1$, which with (6.35) means that $x^2 - 4a^2$ is a square modulo p and so Congruence (6.27) always has a solution in this case. The proof of Theorem 6.4 is complete. □

An example of a QDS of the form in (6.33) is as follows.

Example 6.6 *The parameters $n = 8$, $f = 14$, $t = 2$, $R = C(0) \cup C(1)$ and $k = tf = 28$, yield a QDS of modulus $p = 113$ and multiplicity $\lambda = 7$.*

The QDS has 28 elements. Firstly we note that the parameters satisfy (6.32), (6.33) and (6.34), where $z = 1$, $x = -a_4 = -7$ and $a = -a_8 = 9$. We now need to calculate a suitable primitive root g that will be used to generate the QDS. Using (6.27) we have $(-18\mu - 7)^2 \equiv 64 \pmod{113}$ and hence

$$(18\mu + 7)^2 \equiv 64 \pmod{113} \tag{6.36}$$

where $\mu = g^f = g^{14}$. Solving (6.36) gives the following list of suitable values of primitive root: $g = 10$, 38, 39, 43, 47, 54, 59, 66, 70, 74, 75 and 103. Using $g = 10$, we employ (6.2)

to give

$$\begin{aligned} C(0) &= \{10^0, 10^8, 10^{16}, \ldots, 10^{104}\} \\ &\equiv \{1, 4, 7, 16, 28, 30, 49, 64, 83, 85, 97, 106, 109, 112\} \pmod{113} \\ C(1) &= \{10^1, 10^9, 10^{17}, \ldots, 10^{105}\} \\ &\equiv \{10, 38, 39, 40, 43, 47, 54, 59, 66, 70, 73, 74, 75, 103\} \pmod{113} \end{aligned}$$

which by (6.3) gives

$$\begin{aligned} R = \{&1, 4, 7, 10, 16, 28, 30, 38, 39, 40, 43, 47, 49, 54, 59, \\ &64, 66, 70, 73, 74, 75, 83, 85, 97, 103, 106, 109, 112\}. \end{aligned} \tag{6.37}$$

To choose a qualifier, m, that is in residue class $\sigma = 4$ we use $m \equiv g^{un+\sigma} \equiv 10^{8u+4} \pmod{113}$, which gives us any of the values $m = 2$, 8, 14, 15, 32, 53, 56, 57, 60, 81, 98, 99, 105, or 111. Using $m = 2$ with (6.37) we obtain the set

$$\begin{aligned} mR = \{&2, 5, 8, 14, 15, 19, 20, 27, 32, 33, 35, 37, 53, 56, 57, \\ &60, 76, 78, 80, 81, 86, 93, 94, 98, 99, 105, 108, 111\}. \end{aligned} \tag{6.38}$$

Taking all 784 differences $R - mR \pmod{113}$ between the elements of the sets in (6.37) and (6.38) gives the integers $1, 2, \ldots, 112$ exactly seven times each. Therefore R is a QDS with multiplicity $\lambda = 7$, which agrees with Equation (2.12).

Many of the other possible combinations of residue classes give non-integer and/or zero values for a_4, b_4, a_8 or b_8 and hence no QDS or MQDS. However, a particularly interesting instance of nonexistence occurs in the case of a MQDS when $R^* = C(0) \cup C(1) \cup \{0\}$ and $\sigma = 4$ (and hence a complementary QDS with $R = C(2) \cup C(3) \cup C(4) \cup C(5) \cup C(6) \cup C(7)$ and $\sigma = 4$). Here we have $E = \{0, 1\}$. Again we use Equation (6.9). However, since we are dealing with MQDS we need to add 1 to the summations for $N(0)$, $N(1)$, $N(4)$ and $N(5)$ as per the reasoning surrounding Congruences (6.10) and (6.11) in Section 6.3. Now, equalising all the equations for $N(s)$ gives the following conditions

$$\begin{aligned} &b_4 = 2b_8 \\ &a_4 + a_8 = \quad 6 \quad \text{if 2 is a biquadratic residue of } p \\ &a_4 + a_8 = -6 \quad \text{if 2 is a biquadratic nonresidue of } p. \end{aligned} \tag{6.39}$$

Combining this with (6.19), and setting $x = -a_4$, $2y = b_4$ gives

$$\begin{aligned} &y^2 = 18 + 6x; p = x^2 + 24x + 72 \text{ if 2 is a biquadratic residue of } p \\ &y^2 = 18 - 6x; p = x^2 - 24x + 72 \text{ if 2 is a biquadratic nonresidue of } p. \end{aligned} \tag{6.40}$$

Here, there is no family of MQDS for the following reason. Because $3|(18 \pm 6x)$ then, since $18 \pm 6x$ is a square by (6.40), $9|(18 \pm 6x)$. But $9|18$ so therefore $9| \pm 6x$ which means that $3| \pm x$. Hence $9|(x^2 \pm 24x + 72)$ and so any p of the form given in (6.40) is a multiple of 9 and hence cannot be prime.

For brevity, the rest of the results for $n = 8$ are given without the detailed computational proofs. Some of these are simply redefinitions of known QRDS or MQRDS.

For example the set $R = C(0) \cup C(2) \cup C(4) \cup C(6)$ with $\sigma = 1$, 3, 5 or 7 simply gives a QRDS for $n = 2$ (see Section 4.2). Note, however, the difference in the form of the prime modulus of these two isomorphic cases. A QRDS generated purely from the 2nd powers (i.e. $n = 2$) has a prime modulus of the form $p = 4\alpha + 1$ for integer α. However, when a QDS is generated using $n = 8$ and $t = 4$ there is a further restriction on the form of the prime modulus due to the higher value of n. Here, combining the conditions in Theorem 4.1 with $p = 8f + 1$ gives $p = 8\alpha + 1$ for integer α. This is shown in Table 6.1. Similar modifications in the prime moduli occur for other values of n (see Tables 6.2, 6.3 and 6.4).

Except for isomorphisms of either the above described examples or of those already known, the computer calculations revealed no further QDS. For example, the QDS for $R = C(0) \cup C(3)$ and $n = 8$ was found, but this is simply isomorphic to $R = C(0) \cup C(1)$ with $n = 8$, as described in Section 6.3 above. The list of QDS and MQDS discovered for $n = 8$ is given in Table 6.1. For each case in the table, except for $R = C(0) \cup C(1)$, any primitive root g can be used to generate the set.

f	Set	p	σ	Comments
even	$C(0) \cup C(1)$	$x^2 + 8x + 8$ $x \equiv 1 \pmod 4$ $2 + 2x$ is square	4	New family of QDS; g determined by (6.26)
even	$C(0) \cup C(1)$	$x^2 - 8x + 8$ $x \equiv 1 \pmod 4$ $2 - 2x$ is square	4	New family of QDS; g determined by (6.26)
even	$C(0) \cup C(4)$	$16\alpha^2 + 1$ integer α	2, 6	Isomorphic to QRDS with $n = 4$
odd	$C(0) \cup C(4) \cup \{0\}$	$16\alpha^2 + 9$ integer α	2, 6	Isomorphic to MQRDS with $n = 4$
even or odd	$C(0) \cup C(2) \cup C(4)$ $\cup C(6)$	$8\alpha + 1$ integer α	1, 3, 5, 7	Isomorphic to QRDS with $n = 2$
even or odd	$C(0) \cup C(2) \cup C(4)$ $\cup C(6) \cup \{0\}$	$8\alpha + 1$ integer α	1, 3, 5, 7	Isomorphic to MQRDS with $n = 2$

Table 6.1: List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n = 8$.

6.6 Results for $n = 4$ and $n = 6$

In this section we have the following theorem.

Theorem 6.7 *A MQDS created from the union of 6th power cyclotomic classes* $R^* = C(0) \cup C(1) \cup \{0\}$ *exists for* $p = 13$. *Any primitive root* g *can be used to generate the*

MQDS. All other unions of 4th power and 6th power cyclotomic classes are isomorphic to previously known QDS, MQDS or residue difference sets.

Proof. For the first statement of Theorem 6.7 we have $n = 6$. We use $\sigma = 3$. Now, since $R^* = C(0) \cup C(1) \cup \{0\}$ (i.e. $E = \{0, 1\}$) we will be dealing with MQDS, as indicated by the presence of the zero element. We now employ (6.9) but because of the zero residue, we need to modify the sums in (6.9) according to the reasoning surrounding (6.10) and (6.11) described in Section 6.3. Namely, we need to add 1 to the summation $N(s)$ in the cases when $s \in E$ and $s - \sigma \in E$ (i.e. $s - 3 \in E$). Thus we need to add 1 to $N(0)$, $N(1)$, $N(3)$ and $N(4)$. Therefore from (6.9) we have

$$\begin{aligned} s = 0: &\quad N(0) = (3,0) + (3,1) + (4,0) + (4,1) + 1 \\ s = 1: &\quad N(1) = (2,5) + (2,0) + (3,5) + (3,0) + 1 \\ s = 2: &\quad N(2) = (1,4) + (1,5) + (2,4) + (2,5) \end{aligned} \tag{6.41}$$

with the values for $s = 3, 4, 5$ repeating those for $s = 0, 1, 2$ respectively. The cases that yield positive results are when f is even and ind $2 \equiv 1 \pmod 3$ or ind $2 \equiv 2 \pmod 3$.

Firstly when ind $2 \equiv 1 \pmod 3$ we use the cyclotomic constants from Section A.3 with (6.41) to give

$$\begin{aligned} s = 0: &\quad 36N(0) = 4p + 28 - 8A \\ s = 1: &\quad 36N(1) = 4p + 28 + 4A - 6B \\ s = 2: &\quad 36N(2) = 4p + 4 + 4A + 6B \end{aligned} \tag{6.42}$$

where the integers A and B are given in terms of the quadratic partition in (4.14). Equalising these values of $N(s)$ gives $A = 1$ and $B = 2$, which combining with (4.14) gives

$$p = 13. \tag{6.43}$$

Secondly when ind $2 \equiv 2 \pmod 3$ we obtain from (6.41)

$$\begin{aligned} s = 0: &\quad 36N(0) = 4p + 28 + 4A + 6B \\ s = 1: &\quad 36N(1) = 4p + 28 - 8A \\ s = 2: &\quad 36N(2) = 4p + 4 + 4A - 6B. \end{aligned} \tag{6.44}$$

Equalising the $N(s)$ values here gives $A = 1$ and $B = -2$, which with (4.14) similarly gives (6.43). Since we obtain the same result for both cases of ind 2 considered, it follows that we have a MQDS when 2 is not a cubic residue of p, which is the case for $p = 13$. (Incidentally, the case when 2 is a cubic residue of p leads to the result $B = 0$ upon using (6.41) with $N(0) = N(1)$, and hence by (4.14) the contradiction $p = A^2$). Because of this, any of the four primitive roots of $p = 13$ (i.e. $2, 6, 7$ and 11) can be used to generate the MQDS. This completes the proof of the first statement of Theorem 6.7.

We now generate the above MQDS for $p = 13$ using $g = 2$. Since $n = 6$, $p = 13$, $f = 2$, $k = tf = 4$ and $R^* = C(0) \cup C(1) \cup \{0\}$, then using these parameters with (6.4) and (6.2) gives

$$R^* = \{0, 2^0, 2^6, 2^1, 2^7\} = \{0, 1, 64, 2, 128\} \equiv \{0, 1, 12, 2, 11\} \pmod{13}$$

giving

$$R^* = \{0, 1, 2, 11, 12\}.$$

Using the qualifier $m = 8$ (which is in residue class $\sigma = 3$ with respect to the primitive root $g = 2$) we see that Congruence (2.11) for the set R^* has exactly 2 solutions for each non-zero difference modulo 13 and the zero difference occurs exactly once. Therefore R^* constitutes a MQDS of multiplicity $\lambda = 2$.

The second statement of Theorem 6.7 asserts that the above MQDS is the only new set for $n = 4$ or $n = 6$. All other sets are equivalent to previously known systems. The full results for the cases $n = 4$ and $n = 6$ are given in Table 6.2. As can be seen from the table, the only results for existing QDS and MQDS for $n = 4$ are simply equivalent to known systems for $n = 2$. For the case $n = 6$, the remainder of the cases for f even are equivalent to known QRDS and MQRDS with $n = 2$ but with a modified form of p, similar to the case for $n = 8$ described above (compare with Section 4.2). In the cases for f odd we obtain systems that are equivalent to both RDS and complementary RDS for $n = 2$. The RDS here have a modification to the modulus compared to that discussed by Paley [55] and Lehmer [47, p. 428]. Here we have $p = 12\alpha + 7$. This modification arises due to the combination of the conditions $p = 4x - 1$ from Theorem 2.9 and $p = 6f + 1$. This is given in Table 6.2. The proof of Theorem 6.7 is complete. □

6.7 Results for $n = 10$

In this section we have the following theorem.

Theorem 6.8 *A MQDS created from the union of* 10*th power cyclotomic classes* $R^* = C(0) \cup C(2) \cup \{0\}$ *exists for* $p = 41$. *In this case the primitive root* g *to generate the MQDS must be chosen such that* $ind_g 2 \equiv 1$ *or* $4 \pmod 5$. *A MQDS created from the union of* 10*th power cyclotomic classes* $R^* = C(0) \cup C(1) \cup C(2) \cup C(6) \cup \{0\}$ *exists for* $p = 41$. *In this case any primitive root can be chosen to generate the MQDS. All other unions of* 10*th power cyclotomic classes are isomorphic to previously known QDS, MQDS or residue difference sets.*

Proof. We begin by proving the first MQDS case in Theorem 6.8. The procedure runs along the same lines as those in the proofs of Theorems 6.4 and 6.7 above. Therefore we omit some routine steps during the proof and we also refer the reader to the cyclotomic constants in the paper of Whiteman [67] when necessary, rather than give them explicitly in the appendices.

For $R^* = C(0) \cup C(2) \cup \{0\}$ we use (6.9) with f even, $\sigma = 5$ and note that we need to add 1 to the summations for $N(0)$, $N(2)$, $N(5)$ and $N(7)$ (see the reasoning in Section 6.3). Using the cyclotomic constant equations for the case when ind $2 \equiv 1 \pmod 5$ from

n	f	Set	p	σ	Comments
4	even	$C(0) \cup C(2)$	$8\alpha + 1$ integer α	$1, 3$	Isomorphic to QRDS with $n = 2$
4	odd	$C(0) \cup C(2)$	$4\alpha + 1$ α odd	$1, 3$	Isomorphic to QRDS with $n = 2$
4	even	$C(0) \cup C(2) \cup \{0\}$	$8\alpha + 1$ integer α	$1, 3$	Isomorphic to MQRDS with $n = 2$
4	odd	$C(0) \cup C(2) \cup \{0\}$	$4\alpha + 1$ α odd	$1, 3$	Isomorphic to MQRDS with $n = 2$
6	2	$C(0) \cup C(1) \cup \{0\}$	13	3	Single case, all g
6	even	$C(0) \cup C(2) \cup C(4)$	$12\alpha + 1$ integer α	$1, 3, 5$	Isomorphic to QRDS with $n = 2$
6	even	$C(0) \cup C(2) \cup C(4)$ $\cup\{0\}$	$12\alpha + 1$ integer α	$1, 3, 5$	Isomorphic to MQRDS with $n = 2$
6	odd	$C(0) \cup C(2) \cup C(4)$	$12\alpha + 7$ integer α	$2, 4$	Isomorphic to RDS with $n = 2$
6	odd	$C(0) \cup C(2) \cup C(4)$ $\cup\{0\}$	$12\alpha + 7$ integer α	$2, 4$	Isomorphic to complementary RDS with $n = 2$

Table 6.2: List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n = 4$ and $n = 6$.

[67, p. 108] we therefore obtain

$$\begin{aligned}
s = 0: &\quad 400N(0) = 16p + 336 + 13x + 100u - 50v - 75w \\
s = 1: &\quad 400N(1) = 16p + 16 + 8x - 50u + 50v - 50w \\
s = 2: &\quad 400N(2) = 16p + 336 - 12x + 100u - 100v \\
s = 3: &\quad 400N(3) = 16p + 16 + 8x - 50u + 50v - 50w \\
s = 4: &\quad 400N(4) = 16p + 16 - 17x - 100u + 50v + 175w
\end{aligned} \tag{6.45}$$

where the values for $s = 5, 6, 7, 8, 9$ repeat those for $s = 0, 1, 2, 3, 4$ respectively. If we equalise all the values of $N(s)$ in (6.45) we get $x = -9$, $u = 0$, $v = 3$ and $w = -1$, which satisfy (5.11). Substituting these values into (5.10) gives $p = 41$ which is prime. Whiteman demonstrated that the cyclotomic constants in the cases ind $2 \equiv 2$, 3 or 4 (mod 5) can be derived from the case ind $2 \equiv 1$ (mod 5), but with some transformation of the values of u, v and w [67, p. 107]. Using this, along with the cyclotomic constant

equations for the case when ind $2 \equiv 4 \pmod 5$ [67, p. 108] with $\sigma = 5$ gives

$$\begin{aligned} s = 0: &\quad 400N(0) = 16p + 336 - 12x - 100u + 100v \\ s = 1: &\quad 400N(1) = 16p + 16 + 8x + 50u - 50v - 50w \\ s = 2: &\quad 400N(2) = 16p + 336 + 13x - 100u + 50v - 75w \\ s = 3: &\quad 400N(3) = 16p + 16 - 17x + 100u - 50v + 175w \\ s = 4: &\quad 400N(4) = 16p + 16 + 8x + 50u - 50v - 50w. \end{aligned} \tag{6.46}$$

Again the values for $s = 5, 6, 7, 8, 9$ repeat those for $s = 0, 1, 2, 3, 4$ respectively. Here, equalising the values of $N(s)$ gives $x = -9$, $u = 0$, $v = -3$ and $w = -1$. These values satisfy (5.11) and hence by (5.10) once again give $p = 41$. Therefore we can generate a MQDS for $n = 10$ and $R^* = C(0) \cup C(2) \cup \{0\}$ for $p = 41$, provided we choose a primitive root g such that $\text{ind}_g 2 \equiv 1$ or $4 \pmod 5$. The cases ind $2 \equiv 0, 2$ or $3 \pmod 5$ do not give a MQDS here. We now give an example of a MQDS using ind $2 \equiv 1 \pmod 5$.

Example 6.9 *The parameters $n = 10$, $f = 4$, $t = 2$, $R = C(0) \cup C(1) \cup \{0\}$ and $k = tf = 8$, yield a MQDS of modulus $p = 41$ and multiplicity $\lambda = 2$ when the primitive root $g = 6$ is used.*

Note firstly in Example 6.9 that the choice of $g = 6$ is consistent, since $\text{ind}_6 2 = 26 \equiv 1 \pmod 5$. We now use the parameters in Example 6.9 to generate the set R^* using Equations (6.2) and (6.4). We also choose the qualifier $m \equiv g^\sigma \equiv 6^5 \equiv 27 \pmod{41}$. We therefore obtain the following sets

$$\begin{aligned} R^* &= \{0, 1, 4, 5, 9, 32, 36, 37, 40\} \\ mR^* &= \{0, 3, 12, 14, 15, 26, 27, 29, 38\}. \end{aligned} \tag{6.47}$$

Inspection of the differences $R^* - mR^*$ between the elements of the two sets in (6.47) reveals that each non zero difference modulo 41 occurs exactly twice and the zero difference occurs exactly once. Thus R^* is a MQDS with multiplicity $\lambda = 2$.

If we wish to generate the isomorphic MQDS $R^* = C(0) \cup C(2z) \cup \{0\}$ where z is prime to $p - 1 = nf$, we use the primitive root g_1 given by Equation (6.15) and use the isomorphism described in Section 6.3 (Equations (6.14) to (6.17)). Note here that the form of $\text{ind}_{g_1} 2$ changes as follows. Let $I = \text{ind}_g 2$ and $I_1 = \text{ind}_{g_1} 2$. We have $g^I \equiv g_1^{I_1} \equiv 2 \pmod p$ which, by Congruence (6.15), gives $g_1^{zI} \equiv g_1^{I_1} \pmod p$ and hence $zI \equiv I_1 \pmod{p-1}$. Therefore $\text{ind}_{g_1} 2 \equiv z \, \text{ind}_g 2 \pmod{p-1}$. As an example the set $R^* = C(0) \cup C(2z) \cup \{0\} = C(0) \cup C(4) \cup \{0\}$ $(= C(0) \cup C(14) \cup \{0\})$ can be generated by using $z = 7$ (note: $z = 2$ will not give a result since 2 is not prime to $f = 4$). Using Equation (6.15) gives $g_1 = 30$, and $\text{ind}_{30} 2 \equiv 7 \, \text{ind}_6 2 \equiv 7(26) \pmod{40}$ giving $\text{ind}_{30} 2 = 22 \equiv 2 \pmod 5$. Applying (6.4), along with $m \equiv g_1^\sigma \pmod p$, $\sigma = 5$, gives the same sets as given in (6.47) and hence a MQDS.

To prove the second MQDS case in Theorem 6.7 we use (6.9) for the set $R^* = C(0) \cup C(1) \cup C(2) \cup C(6) \cup \{0\}$ with f even and $\sigma = 5$. Here we need to add 1 to the summations for $N(0)$, $N(2)$, $N(5)$ and $N(7)$, and we need to add 2 to the summations for $N(1)$, $N(6)$

(since for $s = 1$ and $s = 6$ we note that both $s \in E$ and $s - \sigma \in E$, from Section 6.3). Using the cyclotomic constant equations for the case when ind $2 \equiv 1 \pmod 5$ from [67, p. 108] we obtain

$$\begin{aligned} s = 0: &\quad 400N(0) = 64p + 224 - 3x + 100u - 50v - 75w \\ s = 1: &\quad 400N(1) = 64p + 464 + 32x - 50u + 50v + 150w \\ s = 2: &\quad 400N(2) = 64p + 224 - 28x + 100u - 100v \\ s = 3: &\quad 400N(3) = 64p - 16 + 12x + 150u + 50v - 150w \\ s = 4: &\quad 400N(4) = 64p - 16 - 13x - 300u + 50v + 75w. \end{aligned} \tag{6.48}$$

The values for $s = 5, 6, 7, 8, 9$ repeat those for $s = 0, 1, 2, 3, 4$ respectively. If we equalise the values of $N(s)$ we obtain $x = -9$, $u = 0$, $v = 3$, $w = -1$, satisfying (5.11) and yielding $p = 41$ after substitution into (5.10).

As noted above, Whiteman demonstrated that the cyclotomic constants in the cases ind $2 \equiv 2$, 3 or 4 (mod 5) can be derived from the case ind $2 \equiv 1 \pmod 5$, but with some transformation of the values of u, v and w [67, p. 107] . When we apply Equation (6.9) and use the cyclotomic constants for these values of ind 2 along with the relevant transformation in u, v and w we obtain the following results:

$$\begin{aligned} \text{ind } 2 \equiv 2 \pmod 5: &\quad x = -9,\ u = 3,\ v = 0,\ w = 1 \\ \text{ind } 3 \equiv 2 \pmod 5: &\quad x = -9,\ u = -3,\ v = 0,\ w = 1 \\ \text{ind } 4 \equiv 2 \pmod 5: &\quad x = -9,\ u = 0,\ v = -3,\ w = -1. \end{aligned}$$

In each case the parameters satisfy (5.11) and after substitution into (5.10) give $p = 41$. Note finally that for $p = 41$, the case ind $2 \equiv 0 \pmod 5$ is not possible and so there is obviously no set in this case. Thus, there is a MQDS for $p = 41$ and $R^* = C(0) \cup C(1) \cup C(2) \cup C(6) \cup \{0\}$ with $\sigma = 5$ for all primitive roots of 41.

The remainder of the investigation for $n = 10$ revealed similar results to $n = 6$ and are shown in Table 6.3. Here we also have, for f even, some QDS and MQDS that are equivalent to known QRDS and MQRDS for $n = 2$ respectively with slight modifications in the moduli p similar to those discussed in Section 6.5, and for f odd, QDS and MQDS that are equivalent to RDS and complementary RDS for $n = 2$ respectively, with similar modifications in p to those discussed in Section 6.6. The proof of Theorem 6.8 is complete. □

6.8 Results for $n = 12$

In this section we have the following theorem.

Theorem 6.10 *A MQDS created from the union of* 12*th power cyclotomic classes* $R^* = C(0) \cup C(1) \cup C(5) \cup \{0\}$ *exists for* $p = 73$*. The primitive root* g *to generate the MQDS must be chosen such that* $ind_g 2 \equiv 2$ *or* $4 \pmod 6$*,* $ind_g 3 \equiv 2 \pmod 4$ *and the parameter* $c = \beta^3$ *in (5.14). All other unions of* 12*th power cyclotomic classes are isomorphic to previously known QDS, MQDS or residue difference sets.*

f	Set	p	σ	Comments
4	$C(0) \cup C(2) \cup \{0\}$	41	5	Single case with g chosen such that $\text{ind}_g 2 \equiv 1$ or 4 (mod 5)
4	$C(0) \cup C(1) \cup C(2) \cup C(6) \cup \{0\}$	41	5	Single case, all g
even	$C(0) \cup C(2) \cup C(4) \cup C(6) \cup C(8)$	$20\alpha + 1$ integer α	1, 3, 5, 7, 9	Isomorphic to QRDS with $n = 2$
even	$C(0) \cup C(2) \cup C(4) \cup C(6) \cup C(8) \cup \{0\}$	$20\alpha + 1$ integer α	1, 3, 5, 7, 9	Isomorphic to MQRDS with $n = 2$
odd	$C(0) \cup C(2) \cup C(4) \cup C(6) \cup C(8)$	$20\alpha + 11$ integer α	2, 4, 6, 8	Isomorphic to RDS with $n = 2$
odd	$C(0) \cup C(2) \cup C(4) \cup C(6) \cup C(8) \cup \{0\}$	$20\alpha + 11$ integer α	2, 4, 6, 8	Isomorphic to complementary RDS with $n = 2$

Table 6.3: List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n = 10$.

Proof. For $R^* = C(0) \cup C(1) \cup C(5) \cup \{0\}$, we use $\sigma = 6$ with f even, and choose a primitive root g such that the parameter c in (5.14) is equal to β^3 and ind $3 \equiv 2 \pmod 4$. Along with these parameters, a MQDS exists for the two cases ind $2 \equiv 2 \pmod 6$ and ind $2 \equiv 4 \pmod 6$. Again, we refer the reader to the work of Whiteman for the necessary cyclotomic constants [68]. In both cases we use the cyclotomic constants from Table 1 of Whiteman's article [68, p. 70]. For the case ind $2 \equiv 2 \pmod 6$ we use Whiteman's Table 1 as given. For the case ind $2 \equiv 4 \pmod 6$ we use the same table, but replace the cyclotomic constant (i, j) with $(5i, 5j)_{-B}$, and change the sign of B [68, pp. 70-73]. Here the change in sign of B has no effect on the existence condition for the MQDS, which is the same for both values of ind 2. We present the case when ind $2 \equiv 2 \pmod 6$. We use (6.9) with f even and $\sigma = 6$. Note therefore that we need to add 1 to the summations for $N(0)$, $N(1)$, $N(5)$, $N(6)$, $N(7)$ and $N(11)$ for a MQDS (see Section 6.3). Using (6.9) and the relevant cyclotomic constants from [68, Table 1] we obtain

$$\begin{aligned}
s = 0: &\quad 144N(0) = 9p + 117 - 30x + 8y + 16A - 24B \\
s = 1: &\quad 144N(1) = 9p + 117 + 18x \\
s = 2: &\quad 144N(2) = 9p + 9 + 6x + 8y - 8A \\
s = 3: &\quad 144N(3) = 9p + 9 - 18x + 24y - 24B \\
s = 4: &\quad 144N(4) = 9p + 9 + 6x - 16y - 8A + 24B \\
s = 5: &\quad 144N(5) = 9p + 117 + 18x - 24y + 24B.
\end{aligned} \tag{6.49}$$

The values for $s = 6, 7, 8, 9, 10, 11$ repeat those for $s = 0, 1, 2, 3, 4, 5$ respectively. Equalising the values of $N(s)$ in (6.49) gives $y = B$, $y = A + 9$ and $x = -3$, which with (5.15) gives the result $p = 73$ which is prime. For $p = 73$ with $c = \beta^3$, ind $3 \equiv 2 \pmod 4$ and ind

$2 \equiv 2 \pmod 6$, we have the following possible list of primitive roots: $g = 5$, 28, 33, 40, 45 and 68. We now generate the MQDS using $g = 5$. The qualifier m must be in residue class $\sigma = 6$, and hence we can choose from $m = 3$, 24, 27, 46, 49 or 70. Using $m = 3$ with $R^* = C(0) \cup C(1) \cup C(5) \cup \{0\}$, (6.2) and (6.4) we have

$$\begin{aligned} R^* &= \{0, 1, 5, 8, 9, 14, 20, 28, 33, 34, 39, 40, 45, 53, 59, 64, 65, 68, 72\} \\ mR^* &= \{0, 3, 11, 13, 15, 24, 26, 27, 29, 31, 42, 44, 46, 47, 49, 58, 60, 62, 70\}. \end{aligned} \tag{6.50}$$

Here, inspection of the differences $R^* - mR^*$ between the elements of the two sets in (6.50) reveals that each non zero difference modulo 73 occurs exactly five times and the zero difference occurs exactly once. Therefore R^* is a MQDS with multiplicity $\lambda = 5$.

The remainder of the results for the investigation for $n = 12$ are shown in Table 6.4. Like the case $n = 10$ we have a lot of cases which correspond to previously known systems of QRDS, MQRDS, RDS or MRDS. The proof of Theorem 6.10 is complete. □

f	Set	p	σ	criteria for g	Comments
even	$C(0) \cup C(6)$	$108\alpha^2 + 1$ α even	$3, 9$	ind $2 \equiv 0 \pmod 6$	Isomorphic to QRDS for $n = 6$
odd	$C(0) \cup C(6)$	$108\alpha^2 + 1$ α odd	$3, 9$	ind $2 \equiv 3 \pmod 6$	Isomorphic to QRDS for $n = 6$
even	$C(0) \cup C(6) \cup \{0\}$	$108\alpha^2 + 25$ α even	$3, 9$	ind $2 \equiv 0 \pmod 6$	Isomorphic to MQRDS for $n = 6$
odd	$C(0) \cup C(6) \cup \{0\}$	$108\alpha^2 + 25$ α odd	$3, 9$	ind $2 \equiv 3 \pmod 6$	Isomorphic to MQRDS for $n = 6$
even	$C(0) \cup C(4) \cup C(8)$	$36\alpha^2 + 1$ α even	$2, 6, 10$	any	Isomorphic to QRDS for $n = 4$
odd	$C(0) \cup C(4) \cup C(8)$	$36\alpha^2 + 1$ α odd	$4, 8$	any	Isomorphic to RDS for $n = 4$
even	$C(0) \cup C(4) \cup C(8)$ $\cup\{0\}$	$4\alpha^2 + 9$ $\alpha \equiv 2$ or $4 \pmod 6$	$2, 6, 10$	any	Isomorphic to MQRDS for $n = 4$
odd	$C(0) \cup C(4) \cup C(8)$ $\cup\{0\}$	$4\alpha^2 + 9$ $\alpha \equiv 1$ or $5 \pmod 6$	$4, 8$	any	Isomorphic to MRDS for $n = 4$
6	$C(0) \cup C(1) \cup C(5)$ $\cup\{0\}$	73	6	$c = \beta^3$ from (5.14) ind $2 \equiv 2$ or $4 \pmod 6$ ind $3 \equiv 2 \pmod 4$	Single case
1	$C(0) \cup C(1) \cup C(6)$ $\cup C(7) \cup \{0\}$	13	$3, 9$	ind $2 \equiv 1$ or $5 \pmod 6$	Isomorphic to single case of MQDS for $n = 6$
even	$C(0) \cup C(2) \cup C(4)$ $\cup C(6) \cup C(8) \cup C(10)$	$24\alpha + 1$ integer α	$1, 3, 5,$ $7, 9, 11$	any	Isomorphic to QRDS for $n = 2$
odd	$C(0) \cup C(2) \cup C(4)$ $\cup C(6) \cup C(8) \cup C(10)$	$24\alpha + 13$ integer α	$1, 3, 5,$ $7, 9, 11$	any	Isomorphic to QRDS for $n = 2$
even	$C(0) \cup C(2) \cup C(4)$ $\cup C(6) \cup C(8) \cup C(10)$ $\cup\{0\}$	$24\alpha + 1$ integer α	$1, 3, 5,$ $7, 9, 11$	any	Isomorphic to MQRDS for $n = 2$
odd	$C(0) \cup C(2) \cup C(4)$ $\cup C(6) \cup C(8) \cup C(10)$ $\cup\{0\}$	$24\alpha + 13$ integer α	$1, 3, 5,$ $7, 9, 11$	any	Isomorphic to MQRDS for $n = 2$

Table 6.4: List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n = 12$.

Chapter 7

Applications of Qualified Difference Sets

7.1 Introduction

In this chapter we discuss the potential uses of QDS and MQDS in physical applications. Like the difference sets, QDS and MQDS possess similarly attractive properties that suggest potential applications in many areas. One such application, explained in detail below, is coded aperture imaging. In this application a sheet of opaque material, called the *aperture*, which has open elements, or 'holes', in it is placed between an energy source and a position sensitive radiation detector. The source casts a shadow of the aperture onto the detector and the source distribution is determined by the nature of the shadow. The distribution of holes in the aperture can be generated from difference sets, QDS or MQDS, as well as other systems. Here the parameter v represents the total number of elements in the aperture and k represents the number of holes. Therefore, the transparency of the aperture is given by k/v. In astronomical applications, the transparency used is typically 0.5. [56, 69, 70]. This value of k/v allows a large number of photons to pass through the aperture and hence provides a high sensitivity to weak energy sources. However, other values of k/v are often desirable. For example an aperture having such a high proportion of holes will be structurally weak and so smaller transparencies are sometimes considered to prevent disintegration of the aperture [1, 15, 33]. Other applications, such as aperture synthesis, require extremely low values of k/v [44]. While RDS and MRDS can be used, the values of v and k related to these sets are restricted to certain conditions, as outlined in Section 2.2. As a result, only certain values of k/v are available. The introduction of QDS and MQDS, which have different conditions for v and k, allow a greater freedom of choice of systems to use.

The attraction of QDS and MQDS lies in the *cross-correlation function* of certain binary sequences that can be generated from the sets. Typically this cross-correlation function is similar to the Kronecker delta function, but with the restriction that it is

periodic. We thus define here a *periodic* delta function Δ_j for an integer period v, as follows:

$$\Delta_j = \begin{cases} 1 \text{ if } j \equiv 0 \pmod{v} \\ 0 \text{ otherwise.} \end{cases} \tag{7.1}$$

Notationally we call the value at $j \equiv 0 \pmod{p}$ the *peak* of the function and the region outside this peak the *sidelobes* of the function. Note that the sidelobes of Δ_j are a constant ($= 0$). This point is discussed with respect to an imaging application in Section 7.2. In Section 7.3 we present a discussion of the theory behind the implementation of QDS and MQDS in physical applications. In Section 7.4 we give a specific numerical example, in the form of a QRDS of modulus $v = 17$. Finally in Section 7.5 we discuss potential applications of QDS and MQDS.

7.2 Example of a Practical Application

We now present in detail an example of a physical application for which QDS and MQDS have a potential use.

Coded aperture imaging has become the standard technique for forming images of objects that emit X-rays and gamma-rays [23]. Because of the penetrating nature of these high-energy rays, conventional imaging techniques are not possible, since mirrors and lenses do not have any effect on the radiation. One alternative is to replace the mirror or lens with an *aperture*, which consists of a sheet of opaque material (such as lead or tungsten) that has a single pinhole to allow some radiation from the object to pass through. This aperture is placed between the object and a position sensitive radiation detector and after a period of time an inverted image of the object will form on the detector, in the manner of a standard pinhole camera. Unfortunately in many situations that involve the collection of X-rays and gamma-rays, the source intensities are typically very weak compared to the presence of background 'noise', such as radiation in the local environment, or in the form of noise in the electronics of the data collecting systems and so on. As a result the observation times using this arrangement would be prohibitively long. The situation can be remedied by allowing more of the rays from the source to reach the detector by including more pinholes in the aperture to increase its transparent area. For example in most astronomical applications the transparent area is 50% of the whole aperture. As a result we obtain many inverted images of the object on the detector in the form of a shadowgram. However, the individual images from each pinhole often overlap to the extent that the shadowgram is unrecognisable as a representation of the object being observed. We therefore need to apply a decoding algorithm to the shadowgram to form a reconstruction of the object that is hopefully as close a representation to the object as possible. The whole process is shown schematically in Figure 7.1.

Let the shadowgram be represented by the function P, the aperture by A and the

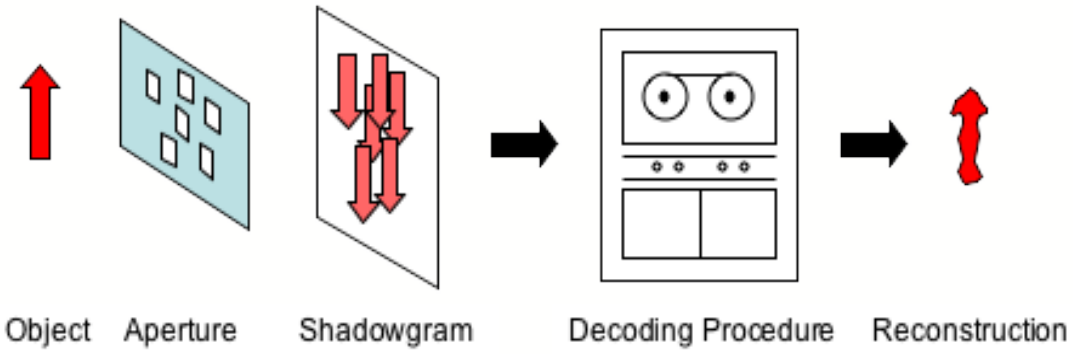

Figure 7.1: The steps involved in coded aperture imaging. Radiation from the object passes through the pinholes in the aperture and is collected by the detector to form a shadowgram. The shadowgram is decoded to form a reconstruction of the object.

object by O. For the data collection stage we have

$$P = (O * A) + N \tag{7.2}$$

where $*$ is a correlation operator and N is some noise function. We call the function for the aperture the *incidence vector*. In most practical applications the incidence vector is a binary function, as defined below.

Definition 7.1 *We call the function B a binary function if $B : \mathbb{Z}_v \to \{0, 1\}$.*

Therefore, the incidence vector A is an array of ones and zeroes where a one represents a transparent element of the aperture and a zero represents an opaque element (see also (7.5) below). A major reason for using binary functions is that their use simplifies implementation in many physical applications, or because the constraints of a given application may render the use of multiple valued functions impossible.

If we represent the *postprocessing function* by G (see also (7.7)) then for the decoding stage we have

$$\hat{O} = P * G \tag{7.3}$$

where $\hat{O}$ is the reconstructed image, with the caret $\hat{}$ being used to indicate that the quantity is an estimate. Combining (7.2) and (7.3) gives $\hat{O} = (O * A) * G + N * G$ and hence

$$\hat{O} = O * (A * G) + N * G. \tag{7.4}$$

Therefore, if G can be chosen such that $A * G$ is a delta function similar to (7.1) then from (7.4) we will have $\hat{O} = O + N * G$ and the object will thus be perfectly constructed, except for the presence of the noise term (the finer points of the mathematics behind the above reasoning can be found in [29, pp. 337-339] and [11, pp. 514-515]).

One important restriction on the function G is that it must be two-valued. We define a *two-valued* function as follows.

Definition 7.2 *A function $U : \mathbb{Z}_v \to \mathbb{R}$ is said to be two-valued if its range is $\{u_1, u_2\}$ with $u_1 \neq u_2$.*

Gottesman and Fenimore demonstrated the importance of having a two-valued postprocessing function, using $G : \mathbb{Z}_v \to \{+1, -1\}$ in their analysis. They showed that if the postprocessing function is two-valued then the imaging performance of the system is optimal in the sense that the signal to noise ratio is independent of the source structure [32, p. 4346]. This same range for the postprocessing function has been used by other authors, notably Calabro and Wolf [22], Fenimore and Cannon [29, p. 339] and Byard [16, pp. 263-264].

7.3 Theoretical Outline

In this section we outline the generic theory behind the implementation of QDS and MQDS in practical applications. Although different applications may use QDS and MQDS in slightly different ways depending on the peculiarities of each application, the fundamental idea behind the use of these sets is the same. Binary functions are generated using the QDS or MQDS and then employed accordingly, depending on the requirements and restrictions of the individual application.

Here we discuss the detailed implementation of a QDS. Because the argument for MQDS is very similar, we restrict the analysis for MQDS to a brief description below.

Let $R = \{r_1, r_2, r_3, \ldots, r_k\}$ be a QDS with k elements, modulus v, multiplicity λ and qualifier m, as given in Definition 2.24, where k, v and λ satisfy the incidence relation (2.12). Define the incidence vector $A : \mathbb{Z}_v \to \{0, 1\}$ for the set R as follows

$$A(i) = \begin{cases} 1 \text{ if } i \in R \\ 0 \text{ if } i \notin R \end{cases} \tag{7.5}$$

where $i = 0, 1, 2, \ldots, v-1$. Note that for a QDS $A(0) = 0$ since $0 \notin R$. Now construct the set $M = mR$ as follows:

$$M = mR = \{mr_1, mr_2, mr_3, \ldots, mr_k\} \pmod{v}. \tag{7.6}$$

Note from Definition 2.24 that $r_i \notin mR$ for all i since the zero difference $r_i - mr_j \pmod{v}$ does not occur. Therefore, similarly $mr_j \notin R$. Let $G : \mathbb{Z}_v \to \{g_1, g_2\}$ be the two-valued function defined by

$$G(i) = \begin{cases} g_1 = 1 - k/\lambda \text{ if } i \in mR \\ g_2 = 1 \text{ otherwise.} \end{cases} \tag{7.7}$$

We will use G for the postprocessing function of the set R. We now define the *cross-correlation function* F of A and G as follows:

Definition 7.3 *For a given incidence vector A and postprocessing function G, the cross-correlation function F of A and G is given by*

$$F(j) = \sum_{i=0}^{v-1} A(i)G(i+j) \tag{7.8}$$

where $i + j$ is taken modulo v.

In Theorem 7.5 below, we will show that the cross-correlation function of A and G defined by (7.5) and (7.7) is a delta function. Firstly we need the following lemma.

Lemma 7.4 *For $d \in \{1, 2, \ldots, v-1\}$*

$$\sum_{\substack{r_i \in R \\ r_i - d \in mR}} 1 = \lambda. \tag{7.9}$$

Proof. By the definition of a QDS (Definition 2.24) for $r_i \in R$ and $r_j \in R$ the value $r_i - d \equiv mr_j \pmod{v}$ occurs λ times for each d as $1 \leq i, j \leq k$. Thus we have $r_i - d \in mR$ when $r_i \in R$ exactly λ times and hence the lemma. □

Theorem 7.5 *For a QDS the cross-correlation function F is given by:*

$$F(j) = k\Delta_j = \begin{cases} k \text{ if } j \equiv 0 \pmod{v} \\ 0 \text{ otherwise} \end{cases} \tag{7.10}$$

where Δ_j is the delta function of (7.1).

Proof. Assume $R = \{r_1, r_2, r_3, \ldots, r_k\}$ is a QDS of k elements and modulus v. Suppose that A is the incidence vector of R given by (7.5), and let G be the postprocessing function as defined in (7.7). From (7.8) we have

$$F(-d) = \sum_{i=0}^{v-1} A(i)G(i-d) \tag{7.11}$$

with $i - d$ taken modulo v. By (7.5), $A(i)$ has a value of unity when $i \in R$ and zero otherwise. Therefore we can rewrite (7.11) as

$$F(-d) = \sum_{r_i \in R} G(r_i - d) \tag{7.12}$$

with $r_i - d$ taken modulo v. Firstly assume $d = 0$. We have from (7.12)

$$F(0) = \sum_{r_i \in R} G(r_i). \tag{7.13}$$

However, since $r_i \notin mR$ for all i then combining (7.7) with (7.13) gives

$$F(0) = kg_2 = k. \tag{7.14}$$

Secondly, assume $d \neq 0$. We can rewrite (7.12) as follows

$$F(-d) = \sum_{\substack{r_i \in R \\ r_i - d \in mR}} G(r_i - d) \quad + \sum_{\substack{r_i \in R \\ r_i - d \notin mR}} G(r_i - d). \tag{7.15}$$

Noting that there are k elements in R, we combine (7.15) with (7.7) to obtain

$$F(-d) = g_1 \sum_{\substack{r_i \in R \\ r_i - d \in mR}} 1 \; + \; g_2 \left(k - \sum_{\substack{r_i \in R \\ r_i - d \in mR}} 1 \right). \tag{7.16}$$

Now, using Lemma 7.4 with (7.16) gives $F(-d) = 0$ when $d \neq 0$. The proof of Theorem 7.5 is complete. □

Note that here we have chosen the values for the postprocessing function G in (7.7) in order to normalise the peak of F to equal the number of open elements in the aperture and to give the sidelobes a value of zero, although different values can be used if desired, such as the values of $+1$ and -1 of Gottesman and Fenimore, as mentioned above. Note also that the delta function cross-correlation function is similar to that obtained when using difference sets and $G = A$ [34, pp. 488-490]. Calabro and Wolf have also generated two-dimensional arrays with a similar property [22].

Once the functions A and G have been generated they can either be used in one or two dimensions, depending on the application. For two-dimensional applications, such as coded aperture imaging, the incidence vector A can be mosaiced onto either a rectangular or a hexagonal lattice. Some methods for doing this are outlined in [29], [30] and [32]. The author has investigated optimal mosaicing onto a square lattice [13].

The analagous analysis for MQDS reveals similar properties. Here, let R^* be a MQDS of $k+1$ elements with modulus v and multiplicity λ, calculated from Equation (2.13) (see Definition 2.25):

$$R^* = \{0, r_1, r_2, \ldots, r_k\} \pmod{v} \tag{7.17}$$

and, for a suitable value of m (Section 2.3), construct the set $M^* = mR^*$:

$$M^* = mR^* \equiv \{0, mr_1, mr_2, \ldots, mr_k\} \pmod{v}. \tag{7.18}$$

Here we define the binary incidence vector $A^*(i)$ and two-valued postprocessing function $G^*(i)$, both of length v, where $i = 0, 1, 2, \ldots, v-1$, as follows:

$$A^*(i) = \begin{cases} 1 \text{ if } i \in R^* \\ 0 \text{ if } i \notin R^* \end{cases} \tag{7.19}$$

$$G^*(i) = \begin{cases} \lambda/(\lambda - 1) \text{ if } i \in mR^*,\ i \neq 0 \\ 1 - k/(\lambda - 1) \text{ otherwise.} \end{cases} \tag{7.20}$$

In this case, the cross-correlation function F^* is also a perfect delta function, as given in the following theorem, which we present without proof.

Theorem 7.6 *For MQDS the cross-correlation function F^* is given by:*

$$F^*(j) = (k+1)\Delta_j = \begin{cases} k+1 \text{ if } j \equiv 0 \pmod{v} \\ 0 \text{ otherwise} \end{cases} \tag{7.21}$$

where Δ_j is the delta function of (7.1).

7.4 Numerical Example

The principles described in the previous section are now demonstrated by means of a numerical example. Consider Example 2.30. We have $n = 4$, $v = p = 17$, $k = 4$, $\lambda = 1$ and $R = \{1, 4, 13, 16\}$. Let $m = 2$. Then

$$M = mR = \{2, 8, 26, 32\} \equiv \{2, 8, 9, 15\} \pmod{17}. \tag{7.22}$$

So, by (7.5) we have

$$A(i) = \begin{cases} 1 \text{ if } i = 1, 4, 13, \text{ or } 16 \\ 0 \text{ otherwise} \end{cases} \tag{7.23}$$

and we use the set M to create the postprocessing function $G(i)$ as per (7.7) to give

$$G(i) = \begin{cases} -3 \text{ if } i = 2, 8, 9 \text{ or } 15 \\ 1 \text{ otherwise.} \end{cases} \tag{7.24}$$

Now, if we cross-correlate the two functions $A(i)$ and $G(i)$ from (7.23) and (7.24) by using (7.8) we obtain

$$F(j) = \sum_{i=0}^{16} A(i)G(i+j) = \begin{cases} 4 \text{ if } j \equiv 0 \pmod{17} \\ 0 \text{ otherwise} \end{cases} \tag{7.25}$$

(where $i + j$ is taken modulo 17) which agrees with (7.10).

The graph of this cross-correlation function is given in Figure 7.2. Note from (7.25) and Figure 7.2 that the cross-correlation function graph is a periodic delta function, with a peak value of $k = 4$, zero sidelobes, and a period of $p = 17$.

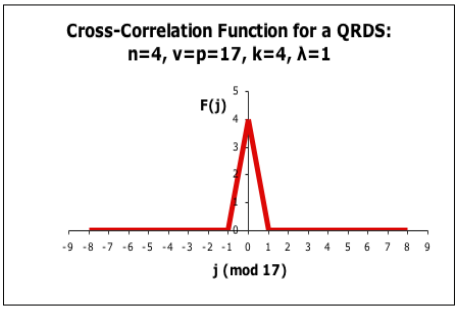

Figure 7.2: Cross-correlation function for a QRDS with $n = 4$, $p = 17$, $k = 4$ and $\lambda = 1$.

7.5 Potential Applications of QDS

In this section we discuss the possible potential applications of QDS. The most obvious application is in the field of coded aperture imaging, as described in Section 7.2. The simplest type of QDS (and MQDS) are the quadratic QRDS, i.e., $n = 2$ (see Section

4.2). These have already been proposed for coded aperture imaging by Gottesman and Fenimore, albeit in a different guise [32]. These authors refer to the resulting fully mosaiced two-dimensional aperture as a *modified uniformly redundant array* (MURA). This term was coined following their minor modification to the *uniformly redundant arrays* (URA), previously proposed for coded aperture imaging by Fenimore and Cannon [29]. Furthermore the author has demonstrated that a subset of these MURA arrays possess 90° antisymmetry, which may be useful in removing systematic background noise that may be present in a physical application [14].

To date only those QDS with $n = 2$ have been proposed for actual coded aperture applications. These include the MURAs. Therefore the results in Chapters 4 and 6 offer many new possible aperture patterns that may be of use in such applications.

Any application that employs the coded aperture technique can potentially employ QDS. To date the most commonly proposed use of coded aperture imaging is in the field of high energy astronomical imaging. The first example of a coded aperture instrument being used in a real astronomical application was in an observation of the sun in 1972 by Blake et al. [11]. The aperture used consisted of a plate of randomly positioned pinholes, as the optimum aperture systems such as URAs or those based on difference sets or QDS had yet to be developed. More recent examples of high energy telescopes that have used the coded aperture technique are the XRT [69], and SIGMA [56] experiments. A major high-energy astronomical project is the INTEGRAL mission [70], which has on board three separate coded aperture experiments: IBIS [62], SPI [63] and JEM-X [50].

A second important use of the coded aperture technique is in medical imaging. Many medical applications have made use of gamma radiation and so forming the resulting images is important in many areas of medical diagnosis [43]. Barrett investigated the use of a Fresnel zone plate in nuclear medicine imaging [4] and coded apertures have been used to form images of the thyroid [45], and heart [58]. One disadvantage of the coded aperture technique in medical imaging is the presence of image artifacts due to the near-field geometry of such systems, although recent advances have made the technique an increasingly viable possibility [1, 59].

Latterly the coded aperture technique has also been proposed as an alternative method to detect flaws in mechanical structures when normal radiographic techniques are not possible. Conventional radiography requires the radiation to pass through the structure to be analysed and for the transmitted radiation to be measured. However, if a structure is too thick to allow a sufficient amount through to be measured, or if access to both sides of the structure is impossible, then backscattering of the radiation is an alternative possibility. Thangavelu and Hussein have studied the feasibility of using the coded aperture technique for producing the resulting images [61]. Woodring et al. have discussed the possibility of using the coded aperture technique in tracking radiation contamination [71]. They propose a data collection and storage system which gives both the position and intensity information of the radiation and they present superimposed pictures of the

gamma ray coded aperture images onto video images for easy location.

Sequences and arrays generated from QDS may have applications in signal processing. To date much of the research effort invested in signal processing has been into the search for sequences that have a delta function *autocorrelation function*. The autocorrelation function is similar to the cross-correlation function in Definition 7.3 but with the restriction $G = A$. Luke has conducted a detailed search for such sequences that have a delta function autocorrelation function [49] and he presents a list of many such sequences. A lot of his sequences are many-valued [49, pp. 289-290], but unfortunately these are often either difficult or impossible to implement in practice. However, if the restriction for the postprocessing function G to be the same as the incidence vector A is relaxed, then we are more readily able to use two-valued sequences that are often easier to implement in practice, for example in an application requiring on/off states, such as the open/closed elements of a coded-aperture.

QDS may have potential uses in radar applications, where it is important to discriminate a signal from the cluttering effect of interfering signals [65], and position location using map-matching [57]. Also, time-frequency coding, which often requires binary patterns having correlation functions with minimum sidelobes may benefit from QDS [31], as may built-in testing of very large scale integration circuits, such as microprocessors [3]. In radio astronomy the earth's rotation is often used to acquire information from a large number of baselines, although this technique in not always feasible for those astronomical objects that exhibit temporal variability on timescales that are shorter than that of the earth's rotation. Klemperer proposed the idea of placing the receivers in a pattern in the form of a nonredundant array so as to sample many spatial frequencies simultaneously [44]. He also gives two possible antenna configurations, one of 12 elements and another of 24 elements, both of which he demonstrates to have a transfer function that possesses flat sidelobes out to some radius [44, p. 451]. QDS may be of use here, due to the similarly flat sidelobes of their cross-correlation functions.

Chapter 8

Summary and Conclusions

This thesis discusses qualified difference sets (QDS) and modified qualified difference sets (MQDS). Using the theory of cyclotomy with respect to the integer order n, the sets are generated modulo a prime modulus p. Both types of set are defined in Section 2.3 of Chapter 2. Special cases of these sets are the qualified residue difference sets (QRDS) and modified qualified residue difference sets (MQRDS) respectively. These sets are also defined in Section 2.3 of Chapter 2.

We prove that for $n = 2$ QRDS and MQRDS both exist for all $p = 4\alpha + 1$ where α is a positive integer. For $n = 4$, we demonstrate the existence of QRDS for all $p = 16\alpha^2 + 1$ and MQRDS for all $p = 16\alpha^2 + 9$ where α is an integer in each case. For $n = 6$ we demonstrate the existence of QRDS for all $p = 108\alpha^2 + 1$ and MQRDS for all $p = 108\alpha^2 + 25$ where α is an integer in each case. We demonstrate the nonexistence of all QRDS and MQRDS for $n = 8$, 10, 12, 14 and 18.

QDS and MQDS created from the unions of cyclotomic classes are discussed in Chapter 6. We present the results of an exhaustive search for QDS and MQDS composed of unions of cyclotomic classes for orders $n = 4$, 6, 8, 10 and 12. For each value of n studied, some cases were discovered that are simply equivalent to known systems, including QRDS, MQRDS and residue difference sets. In the case $n = 4$, no new systems were found. However, there were positive new results for the other values of n studied. In the case $n = 6$ a new isolated system for $p = 13$ was found, and for $n = 10$, two new MQDS, both for $p = 41$ were discovered, one consisting of a union of two cyclotomic classes and another of four cyclotomic classes. In the two-class case, the choice of ind 2 is important. In the case $n = 12$ a new MQDS for $p = 73$ consisting of a union of two cyclotomic classes was found. For $n = 8$, two new entire families of QDS were discovered. Both created from the union of two cyclotomic classes, one family exists for all $p = 64z^4 + 128z^3 + 144z^2 + 80z + 17$ and the other exists for all $p = 64z^4 + 48z^2 + 1$ where z is an integer in each case.

QDS and MQDS have potential uses in various physical applications, largely due to the delta function cross-correlation function of certain binary sequences that can be generated from the sets. Potential uses of QDS and MQDS are discussed in Chapter 7.

Appendix A

Cyclotomic Constants

This appendix contains those cyclotomic constants that are required in the calculations in this thesis. The cyclotomic constants are given in terms of the prime p, order n and the integer f where $p = nf + 1$. The literary source of the cyclotomic constants in each section is referenced accordingly.

A.1 Cyclotomic Constants for $n = 2$

The cyclotomic constants for $n = 2$ and prime $p = 2f + 1$ are from Dickson [25, p. 394].

f even:
$(0, 1) = (p - 1)/4$

A.2 Cyclotomic Constants for $n = 4$

The cyclotomic constants for $n = 4$ are from Dickson [25, p. 400, (48), (52)]. For $n = 4$ and prime $p = 4f + 1$ the cyclotomic constants depend on the quadratic partition

$$p = x^2 + 4y^2 \tag{A.1}$$

where x and y are integers and $x \equiv 1 \pmod 4$ [25, p. 400, (51)].

f even:
$16(0, 2) = p - 3 + 2x$
$16(1, 2) = p + 1 - 2x$

A.3 Cyclotomic Constants for $n = 6$

The cyclotomic constants for $n = 6$ are from Dickson [25, pp. 408-410]. For $n = 6$ and prime $p = 6f + 1$ the cyclotomic constants depend on the quadratic partition

$$p = A^2 + 3B^2 \tag{A.2}$$

where A and B are integers and $A \equiv 1 \pmod 6$ if f is even and $A \equiv 4 \pmod 6$ if f is odd.

f even, ind $2 \equiv 0 \pmod 3$:
$36(0,3) = p - 5 + 4A$
$36(1,3) = p + 1 - 2A$
$(2,3) = (1,3)$ [25, Equation (91)]

f even, ind $2 \equiv 1 \pmod 3$:
$36(0,2) = p - 5 + 4A - 6B$
$36(0,4) = p - 5 - 8A$
$36(1,3) = p + 1 - 2A - 6B$
$36(1,4) = p + 1 - 2A + 12B$
$36(1,5) = p + 1 - 2A - 6B$
$36(2,4) = p + 1 + 10A + 6B$
$(0,3) = (0,2)$
$(2,3) = (1,4)$
$(2,5) = (1,3)$
$(3,5) = (1,4)$

f even, ind $2 \equiv 2 \pmod 3$:
$36(0,2) = p - 5 - 8A$
$36(0,3) = p - 5 + 4A + 6B$
$36(1,3) = p + 1 - 2A - 12B$
$36(1,4) = p + 1 - 2A + 6B$
$36(2,4) = p + 1 + 10A - 6B$
$(0,4) = (0,3)$
$(1,5) = (1,2)$
$(2,3) = (1,4)$
$(2,5) = (1,3)$
$(3,5) = (1,4)$

A.4 Cyclotomic Constants for $n = 8$

The groundwork for calculating the cyclotomic constants for $n = 8$ was laid down by Dickson, who presented criteria in the form of a set of simultaneous equations for the calculation of the constants [25, pp. 410-413]. Lehmer used Dickson's results to calculate the cyclotomic constants specifically [48, pp. 115-117]. For $n = 8$ and prime $p = 8f + 1$ the cyclotomic constants depend on the quadratic partitions

$$p = x^2 + 4y^2 \text{ and } p = a^2 + 2b^2 \tag{A.3}$$

where x, y, a, b are all integers and $x \equiv a \equiv 1 \pmod 4$.

f even ($p = 16\alpha + 1$), 2 is a biquadratic residue of p:
$64(0,3) = p - 7 + 2x + 4a - 16y + 16b$
$64(0,4) = p - 7 - 2x + 8a$
$64(0,5) = p - 7 + 2x + 4a + 16y - 16b$
$64(1,4) = p + 1 + 2x - 4a$
$64(1,5) = p + 1 + 2x - 4a$
$64(1,6) = p + 1 - 6x + 4a$
$64(2,4) = p + 1 - 2x$
$64(2,5) = p + 1 + 2x - 4a$
$(2,6) = (2,4)$
$64(2,7) = p + 1 - 6x + 4a$
$(3,6) = (2,5)$
$(3,7) = (1,4)$
$(4,7) = (1,5)$

f even ($p = 16\alpha + 1$), 2 is a biquadratic nonresidue of p:
$64(0,3) = p - 7 + 2x + 4a$
$64(0,4) = p - 7 - 10x$
$64(0,5) = p - 7 + 2x + 4a$
$64(1,4) = p + 1 + 2x - 4a + 16y$
$64(1,5) = p + 1 + 2x - 4a - 16y$
$64(1,6) = p + 1 + 2x - 4a + 16b$
$64(2,5) = p + 1 - 6x + 4a$
$64(2,6) = p + 1 + 6x + 8a$
$64(2,7) = p + 1 + 2x - 4a - 16b$
$(3,4) = (1,5)$
$(3,6) = (2,5)$
$(3,7) = (1,4)$
$(4,7) = (1,5)$

A.5 Cyclotomic Constants for $n = 10$

The cyclotomic constants for $n = 10$ are from Whiteman [67, pp. 107-109]. For $n = 10$ and prime $p = 10f + 1$ the cyclotomic constants are given in terms of the following equations

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2 \tag{A.4}$$

$$xw = v^2 - 4uv - u^2 \tag{A.5}$$

where u, v, w, x are all integers and $x \equiv 1 \pmod 5$.

f even, ind $2 \equiv 0 \pmod 5$:
$200(1,5) = 2p + 2 + x + 25w$
$200(2,5) = 2p + 2 + x - 25w$

f even, ind $2 \equiv 1 \pmod 5$:
$200(1,5) = 2p + 2 + x + 50v + 25w$
$400(2,5) = 4p + 4 - 23x + 50u - 25w$
$200(3,5) = 2p + 2 + x - 25u - 25v$

A.6 Cyclotomic Constants for $n = 12$

The cyclotomic constants for $n = 12$ are from Whiteman [68, pp. 69-73]. For $n = 12$ and prime $p = 12f + 1$ the cyclotomic constants are given in terms of the following quadratic partitions

$$p = x^2 + 4y^2 \text{ and } p = A^2 + 3B^2 \tag{A.6}$$

where x, y, A and B are integers, $x \equiv 1 \pmod 4$ and $A \equiv 1 \pmod 6$

f even, ind $2 \equiv 2 \pmod 6$, ind $3 \equiv 2 \pmod 4$, $c = \beta^3$ [68, Table 1]:
$144(1,6) = p + 1 + 2A + 12B + 8y$
$144(2,6) = p + 1 - 4A - 6x + 8y$
$144(4,6) = p + 1 + 2A + 12B + 8y$
$144(5,6) = p + 1 + 8A - 12B + 6x + 8y$

f even, ind $2 \equiv 2 \pmod 6$, ind $3 \equiv 0 \pmod 4$, $c = 1$ [68, Table 3]:
$144(1,6) = p + 1 + 6A - 8x$
$144(3,6) = p + 1 - 6A + 4x$

f even, ind $2 \equiv 2 \pmod 6$, ind $3 \equiv 0 \pmod 4$, $c = -1$ [68, Table 4]:
$144(1,6) = p + 1 - 2A + 24B$
$144(2,6) = p + 1 + 12B + 14x$
$144(3,6) = p + 1 + 10A - 12x$
$144(4,6) = p + 1 + 6A + 8x$
$144(5,6) = p + 1 + 4A - 24B - 6x$

f even, ind $2 \equiv 0 \pmod 6$, ind $3 \equiv 2 \pmod 4$, $c = \beta^3$ [68, Table 7]:
$144(1,6) = p + 1 + 2A + 12B + 8y$
$144(5,6) = p + 1 + 2A - 12B + 8y$

f even, ind $2 \equiv 0 \pmod 6$, ind $3 \equiv 0 \pmod 4$, $c = 1$ [68, Table 9]:
$144(1,6) = p + 1 + 6A - 8x$

$144(2,6) = p + 1 - 2A$

f even, ind $2 \equiv 0 \pmod 6$, ind $3 \equiv 0 \pmod 4$, $c = -1$ [68, Table 10]:
$144(1,6) = p + 1 - 2A + 24B$
$144(2,6) = p + 1 + 6A + 24B + 8x$

A.7 Cyclotomic Constants for $n = 14$

The cyclotomic constants for $n = 14$ are from Muskat [52]. For $n = 14$ and prime $p = 14f+1$ the cyclotomic constants are given in terms of the following quadratic partition

$$p = T^2 + 7U^2 \tag{A.7}$$

where T and U are integers and $T \equiv 1 \pmod 7$. We define the quantity S as follows:

$$S = \sum_{i=0}^{6} C_i \zeta_7^i \tag{A.8}$$

where $\zeta_7 = \exp(2\pi i/7)$ and the C_i are integers, such that

$$S\bar{S} = |S|^2 = p. \tag{A.9}$$

There are two sets of cyclotomic constants: (a) ind $2 \equiv 0 \pmod 7$, (b) ind $2 \not\equiv 0 \pmod 7$. In the case where ind $2 \not\equiv 0 \pmod 7$ we let $m =$ ind 2 and $M \equiv m \pmod 7$ with M odd, giving the following separate cases: $m = M = 1$; $m = 2, M = 9$; $m = M = 3$; $m = 4, M = 11$; $m = M = 5$; $m = 6, M = 13$ (see Section 5.5 and [52, p. 271]).

f even, ind $2 \equiv 0 \pmod 7$:
$196(1,7) = 5p - 7 + 2T + 14U - 14C_1 - 7C_2 - 14C_4 + 7C_5$
$196(2,7) = 5p - 7 + 2T + 14U - 14C_1 - 14C_2 + 7C_3 - 7C_4$
$196(3,7) = 5p - 7 + 2T - 14U + 7C_1 - 14C_3 - 14C_5 - 7C_6$
$196(4,7) = 5p - 7 + 2T + 14U - 7C_1 - 14C_2 - 14C_4 + 7C_6$
$196(5,7) = 5p - 7 + 2T - 14U - 7C_3 + 7C_4 - 14C_5 - 14C_6$
$196(6,7) = 5p - 7 + 2T - 14U + 7C_2 - 14C_3 - 7C_5 - 14C_6$

f even, ind $2 \not\equiv 0 \pmod 7$:
$196(M,7) = 5p - 7 + 2T + 14U + 14C_m - 14C_{3m} - 28C_{6m}$
$196(2M,7) = -44p + 91 + 2T + 14U + 49C_m + 63C_{2m} + 56C_{3m} + 49C_{4m} + 49C_{5m} + 49C_{6m}$
$196(3M,7) = 5p - 7 + 2T - 14U - 21C_m - 7C_{2m} + 14C_{3m} - 14C_{4m}$
$196(4M,7) = 5p - 7 + 2T + 14U - 14C_m - 28C_{2m} + 7C_{4m} + 7C_{6m}$
$196(5M,7) = 5p - 7 + 2T - 14U - 28C_{3m} + 7C_{4m} - 7C_{6m}$
$196(6M,7) = 5p - 7 + 2T - 14U - 7C_m - 7C_{2m} - 28C_{4m} + 14C_{6m}$

A.8 Cyclotomic Constants for $n = 18$

The cyclotomic constants for $n = 18$ are from Baumert and Fredricksen [5, 6]. For $n = 18$ and prime $p = 18f + 1$ the cyclotomic constants are given in terms of the following quadratic partition

$$4p = L^2 + 27M^2 \tag{A.10}$$

where L and M are integers and $L \equiv 7 \pmod 9$. We define the quantity S as follows:

$$S = \sum_{i=0}^{5} C_i \zeta_9^i \tag{A.11}$$

where $\zeta_9 = \exp(2\pi i/9)$ and the C_i are integers, such that

$$S\bar{S} = |S|^2 = p. \tag{A.12}$$

f even, ind $2 \equiv 0 \pmod 9$, ind $3 \equiv 0 \pmod 3$:
$648(1,9) = 2p + 2 + 2L + 18C_1 - 18C_4 - 18C_5$
$648(2,9) = 2p + 2 + 2L - 18C_1 + 18C_2$
$648(3,9) = 2p + 2 + 2L - 54M + 54C_3$
$648(4,9) = 2p + 2 + 2L - 18C_2 + 18C_4 + 18C_5$
$648(6,9) = 2p + 2 + 2L + 54M - 54C_3$

f even, ind $2 \equiv 0 \pmod 9$, ind $3 \equiv 1 \pmod 3$:
$648(1,9) = 2p + 2 + 2L - 18C_1 + 36C_2 - 18C_4 - 18C_5$
$648(2,9) = 2p + 2 + 2L - 18C_1 - 18C_2 - 36C_4$
$648(3,9) = 2p + 2 + 2L + 54M + 54C_3$
$648(5,9) = 2p + 2 + 2L - 36C_1 + 18C_2 + 54C_4 - 18C_5$
$648(6,9) = 2p + 2 - 16L + 36C_0 - 18C_3$
$648(7,9) = 2p + 2 + 2L - 18C_1 - 18C_2 + 36C_4 + 36C_5$
$648(8,9) = 2p + 2 + 2L + 54C_1 - 18C_4 + 18C_5$

f even, ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 0 \pmod 3$:
$648(1,9) = 2p + 2 + 2L + 18M + 72C_1 + 36C_3 - 72C_4 + 36C_5$
$648(3,9) = 2p + 2 + 5L - 9M - 6C_0 - 24C_1 + 12C_2 + 12C_3 + 12C_4 - 42C_5$
$648(4,9) = 2p + 2 + 2L + 18M - 54C_1 + 36C_3 + 54C_4$
$648(6,9) = 2p + 2 + 5L - 9M - 6C_0 + 12C_1 - 42C_2 - 42C_3 - 24C_4 + 30C_5$
$648(7,9) = 2p + 2 + 2L + 18M - 18C_1 + 36C_3 + 18C_4 - 36C_5$

f even, ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 1 \pmod 3$:
$648(1,9) = 2p + 2 + 2L + 18M + 36C_0 + 36C_1 + 36C_2 - 36C_3 - 36C_4$
$648(2,9) = 2p + 2 - L - 63M - 48C_0 - 12C_1 + 6C_2 + 42C_3 - 12C_4 - 12C_5$
$648(3,9) = 2p + 2 + 5L - 9M - 42C_0 - 24C_1 + 12C_2 + 48C_3 + 12C_4 - 6C_5$

$648(4,9) = 2p + 2 + 2L + 18M + 36C_0 + 18C_1 - 36C_2 - 36C_3 - 18C_4$
$648(5,9) = 2p + 2 - L + 45M + 6C_0 - 12C_1 + 6C_2 + 42C_3 + 24C_4 + 6C_5$
$648(6,9) = 2p + 2 + 5L - 9M - 42C_0 + 12C_1 - 6C_2 - 6C_3 - 24C_4 - 6C_5$
$648(7,9) = 2p + 2 + 2L + 18M + 36C_0 - 54C_1 - 36C_3 + 54C_4$
$648(8,9) = 2p + 2 - 19L - 9M + 42C_0 + 24C_1 - 12C_2 + 24C_3 - 12C_4 + 6C_5$

f even, ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 2 \pmod 3$:
$648(1,9) = 2p + 2 + 2L + 18M - 36C_0$
$648(2,9) = 2p + 2 - L + 45M - 12C_0 - 12C_1 + 6C_2 + 6C_3 + 24C_4 + 24C_5$
$648(3,9) = 2p + 2 + 5L - 9M - 6C_0 - 24C_1 - 24C_2 + 48C_3 + 12C_4 - 6C_5$
$648(5,9) = 2p + 2 - 19L - 9M + 78C_0 + 24C_1 - 30C_2 - 66C_3 - 12C_4 + 6C_5$
$648(6,9) = 2p + 2 + 5L - 9M - 6C_0 + 12C_1 - 6C_2 - 6C_3 - 24C_4 + 30C_5$
$648(7,9) = 2p + 2 + 2L + 18M - 36C_0 + 18C_1 + 36C_2 - 18C_4 - 36C_5$
$648(8,9) = 2p + 2 - L - 63M + 42C_0 - 12C_1 + 24C_2 - 48C_3 - 12C_4 - 30C_5$

f even, ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 0 \pmod 3$:
$648(1,9) = 2p + 2 + 2L + 54C_1 - 54C_2 - 54C_4 + 54C_5$
$648(2,9) = 2p + 2 + 2L + 36C_1 + 54C_2 + 18C_4 - 36C_5$
$648(3,9) = 2p + 2 + 2L + 54M$
$648(4,9) = 2p + 2 + 2L + 54C_2 + 54C_4$
$648(5,9) = 2p + 2 + 2L + 18C_1 - 18C_2 - 54C_4 + 54C_5$
$648(7,9) = 2p + 2 + 2L - 54C_1 - 54C_5$
$648(8,9) = 2p + 2 + 2L - 54C_1 - 36C_2 + 36C_4 - 18C_5$

f even, ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 1 \pmod 3$:
$648(1,9) = 2p + 2 + 2L + 18C_1 + 18C_2 - 54C_4 - 18C_5$
$648(2,9) = 2p + 2 + 2L - 36C_1 + 18C_2 + 18C_4 - 36C_5$
$648(3,9) = 2p + 2 - 16L + 36C_0 + 36C_3$
$648(4,9) = 2p + 2 + 2L + 36C_1 - 18C_2 + 18C_4$
$648(5,9) = 2p + 2 + 2L + 18C_1 + 18C_2 + 18C_4 + 18C_5$
$648(6,9) = 2p + 2 + 2L - 54M - 54C_0$
$648(8,9) = 2p + 2 + 2L + 18C_1 - 36C_2 - 36C_4 + 18C_5$

f even, ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 2 \pmod 3$:
$648(1,9) = 2p + 2 + 2L + 18C_1 - 18C_2 - 18C_4 + 18C_5$
$648(2,9) = 2p + 2 + 2L + 18C_2 + 18C_4$
$648(3,9) = 2p + 2 + 2L - 54M$
$648(8,9) = 2p + 2 + 2L - 18C_1 - 18C_5$

Appendix B

Complementary QDS

Consider a QDS R of modulus p where $R = \{r_1, r_2, r_3, \ldots, r_k\}$ is composed of the union of t cyclotomic classes derived from $E = \{c_1, c_2, \ldots, c_t\}$, and let $mR = \{mr_1, mr_2, mr_3, \ldots, mr_k\} \pmod p$ where m is a qualifier of the QDS. Now let $A(i)$ be a binary sequence, defined such that

$$A(i) = \begin{cases} 1 \text{ if } i \in R \\ 0 \text{ if } i \notin R \end{cases} \tag{B.1}$$

and define another binary sequence, $G(i)$ such that

$$G(i) = \begin{cases} 1 \text{ if } i \in mR \\ 0 \text{ if } i \notin mR \end{cases} . \tag{B.2}$$

By the properties of a QDS we have

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

where N_0 is the number of zero differences and λ is the number of non-zero differences between the elements of the sets R and mR (compare Equation (7.10)). Now, if we let R^* be the complement of R, we now have $R^* = \mathbb{Z}_p - R$, composed of the residue classes $E^* = \mathbb{Z}_n - E$ with the residue zero. Here the corresponding sets $A^*(i)$ and $G^*(j)$ are simply obtained by replacing zeroes for ones in Equations (B.1) and (B.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 Equation (B.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.

Bibliography

[1] R. Accorsi and R. Lanza, Near-Field Artifact Reduction in Planar Coded-Aperture Imaging, *J. Appl. Opt.* **40** (2001) 4697–4705.

[2] P. Bachmann, Die Lehre von der Kreistheilung, Teubner, Leipzig (1927).

[3] P.H. Bardell and W.H. McAnney, Pseudorandom Arrays for Built-In Tests, *IEEE Trans. Computers* **C-35** (1986) 653–658.

[4] H.H. Barrett, Fresnel Zone Plate Imaging in Nuclear Medicine, *J. Nucl. Med.* **13** (1972) 382–385.

[5] L.D. Baumert and H. Fredricksen, The Cyclotomic Numbers of Order Eighteen with Applications to Difference Sets, *Math. Comp.* **21** (1967) 204–219.

[6] L.D. Baumert and H. Fredricksen, The Cyclotomic Numbers of Order Eighteen, *Math. Comp. Unpublished Mathematical Tables Collection* **21**(98) (1967) 262 (Box 97–196/5, 5662986).

[7] L.D. Baumert, Difference Sets, *SIAM J. Appl. Math.* **17** (1969) 826–833.

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

[9] B.C. Berndt and R.J. Evans, Sums of Gauss, Jacobi and Jacobsthal, *J. Number Theory* **11** (1979) 349–398.

[10] B.C. Berndt, R.J. Evans and K.S. Williams, Gauss and Jacobi Sums, Can. Math. Soc., series 21, Wiley, New York, Toronto (1998).

[11] R.L. Blake, A.J. Burek, E. Fenimore and R. Puetter, Solar X-Ray Photography with Multiplex Pin-Hole Camera, *Rev. Sci. Instrum.* **45** (1974) 513–516.

[12] R.H. Bruck, Computational Aspects of Certain Combinatorial Problems, *Proc. Symp. Appl. Math.* **6** (1956) 31–43.

[13] K. Byard, An Optimised Coded Aperture Imaging System, *Nucl. Instrum. Meth. Phys. Res.* **A313** (1992) 283–289.

[14] K. Byard, Square Element Antisymmetric Coded Apertures, *Experimental Astronomy* **2** (1992) 227–232.

[15] K. Byard, On Self-Supporting Coded Aperture Arrays, *Nucl. Instrum. Meth. Phys. Res.* **A322** (1992) 97–100.

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

[17] K. Byard, On Qualified Residue Difference Sets, *Int. J. Number Theory.* **2** (2006) 591–598.

[18] K. Byard, Tenth Power Qualified Residue Difference Sets, *Int. J. Number Theory.* **5** (2009) 797–803.

[19] K. Byard, Twelfth Power Qualified Residue Difference Sets, *INTEGERS.* **9** (2009) 401–410.

[20] K. Byard and K. Broughan, Qualified Difference Sets from Unions of Cyclotomic Classes, *Bull. Australian Math. Soc.* **80** (2009) 147–158.

[21] K. Byard, R. Evans and M. Van Veen, Lam's Power Residue Addition Sets, *Advances in Applied Mathematics.* (2010) to appear.

[22] D. Calabro and J.K. Wolf, On the Synthesis of Two-Dimensional Arrays With Desirable Correlation Properties, *Inf. Control* **11** (1968) 537–560.

[23] 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.

[24] S. Chowla, A Property of Biquadratic Residues, *Proc. Nat. Acad. Sci. India* **A14** (1944) 45–46.

[25] L.E. Dickson, Cyclotomy, Higher Congruences and Waring's Problem, *Am. J. Math.* **57** (1935) 391–424.

[26] R. Evans, Bioctic Gauss Sums and Sixteenth Power Residue Difference Sets, *Acta Arith.* **38** (1980) 37–46.

[27] R. Evans, Twenty-Fourth Power Residue Difference Sets, *Math. Comp.* **40** (1983) 677–683.

[28] R. Evans, Nonexistence of Twentieth Power Residue Difference Sets, *Acta Arith.* **89** (1999) 397–402.

[29] E.E. Fenimore and T.M. Cannon, Coded Aperture Imaging with Uniformly Redundant Arrays, *Appl. Opt.* **17** (1978) 337–347.

[30] M.H. Finger and T.A. Prince, Hexagonal Uniformly Redundant Arrays for Coded Aperture Imaging, *Proc. 19th Int. Cosmic Ray Conf.* La Jolla, USA, National Aeronautics and Space Administration, Washington **3** (1985), 295–298.

[31] S.W. Golomb and H. Taylor, Two-Dimensional Synchronization Patterns for Minimum Ambiguity, *IEEE Trans. Inf. Theory* **IT-28** (1982) 600–604.

[32] S.R. Gottesman and E.E. Fenimore, New Family of Binary Arrays for Coded Aperture Imaging, *Appl. Opt.* **28** (1989) 4344–4352.

[33] S.R. Gottesman and E.J. Schneid, PNP-A New Class of Coded Aperture Arrays *IEEE Trans. Nucl. Sci.* **NS-33** (1986) 745–749.

[34] J. Gunson and B. Polychronopulos, Optimum Design of a Coded Mask X-Ray Telescope for Rocket Applications, *Mon. Not. R. Astron. Soc.* **177** (1976) 485–497.

[35] M. Hall Jr, Cyclic Projective Planes, *Duke Math. J.* **14** (1947) 1079–1090.

[36] M. Hall Jr, A Survey of Difference Sets, *Proc. Amer. Math. Soc.* **7** (1956) 975–986.

[37] M. Hall Jr, Characters and Cyclotomy, *Amer. Math. Soc., Symp. Pure Math.* **8** (1965) 31–43.

[38] H.S. Hayashi, Computer Investigation of Difference Sets, *Math. Comp.* **19** (1965) 73–78.

[39] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York (1982).

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

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

[42] G.A. Jones and J.M. Jones, Elementary Number Theory, Springer, London (1998).

[43] Yu.P. Kazachkov, D.S. Semenov and N.P. Goryacheva, Application of Coded Apertures in Medical γ-ray Cameras, *Instruments and Experimental Techniques* **50** (2007) 267–274.

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

[45] K.F. Koral, J.E. Freitas, W.L. Rogers and J.W. Keyes, Thyroid Scintigraphy with Time-Coded Aperture, *J. Nucl. Med.* **20** (1979) 345–349.

[46] M. Lebesgue, Sur L'Impossibilite, en Nombres Entiers, de l'Equation $x^m = y^2 + 1$, *Nouvelles Ann. Math.* **9** (1850) 178–181.

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

[48] E. Lehmer, On The Number of Solutions of $u^k + D \equiv w^2 \pmod{p}$, *Pacific. J. Math.* **5** (1955) 103–118.

[49] H.D. Luke, Sequences and Arrays with Perfect Periodic Correlation, *IEEE Trans. Aerosp. Electron. Systems* **24** (1988) 287–294.

[50] N. Lund, C. Budtz-Jorgensen, N.J. Westergaard, S. Brandt, I.L. Rasmussen, A. Hornstrup, C.A. Oxborrow, J. Chenevez, P.A. Jensen, S. Laursen, K.H. Andersen, P.B. Morgensen, I. Rasmussen, K. Omo, S.M. Pedersen, J. Polny, H. Andersson, T. Andersson, V. Kamarainen, O. Vilhu, J. Huovelin, S. Maisala, M. Mrawski, G. Juchnikowski, E. Costa, M. Feroci, A. Rubini, M. Rapisarda, E. Morelli, V. Carassiti, F. Frontera, C. Pelliciari, G. Loffredo, S. Martinez Nunez, V. Reglero, T. Velasco, S. Larsson, R. Svensson, A.A. Zdziarski, A. Casrto-Tirado, P. Attina, M. Goria, G. Giulianelli, F. Cordero, M. Rezazad, M. Schmidt, R. Carli, C. Gomez, P.L. Jensen, G. Sarri, A. Tiemon, A. Orr, R. Much, P. Kretschmar and H.W. Schnopper, JEM-X: The X-Ray Monitor Aboard INTEGRAL, *Astron. Astrophys.* **411** (2003) L231–L238.

[51] R.A. Mollin, Algebraic Number Theory, Chapman and Hall/CRC Boca Raton, London, New York, Washington D.C. (1999).

[52] J.B. Muskat, The Cyclotomic Numbers of Order Fourteen, *Acta Arith.* **11** (1966) 263–279.

[53] J.B. Muskat and A.L. Whiteman, The Cyclotomic Numbers of Order Twenty, *Acta Arith.* **17** (1970) 401–413.

[54] U. Ott, Sharply Flag-Transitive Projective Planes and Power Residue Difference Sets, *J. Algebra* **276** (2004) 663–673.

[55] R.E.A.C. Paley, On Orthogonal Matrices, *J. Math. and Phys.* **12** (1933) 311–320.

[56] J. Paul, P. Mandrou, J. Ballet, M. Cantin, J.P. Chabaud, B. Cordier, M. Ehanno, A. Goldwurm, A. Lambert, J. Lande, P. Laurent, F. Lebrun, J.P. Leray, B. Mena, M. Niel, J.-P. Roques, G. Rouaix, L. Salotti, P. Soueille and G. Vedrenne, SIGMA: The Hard X-Ray and Soft Gamma-Ray Telescope on Board the GRANAT Space Observatory, *Adv. Spa. Res.* **11** (1991) 289–302.

[57] I.S. Reed and R.M. Stewart, Note on the Existence of Perfect Maps, *IEEE Trans. Inf. Theory* **IT-8** (1962) 10–12.

[58] 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.

[59] D.M. Starfield, D.M. Rubin and T. Marwala, Near-Field Artifact Reduction Using Realistic Limited-Field-Of-View Coded Apertures in Planar Nuclear Medicine Imaging, *IFMBE Proc. World Cong. Med. Phys and Biomed. Eng.* **14** (2006) 1558–1561.

[60] T. Storer, Cyclotomy and Difference Sets, Markham, Chicago (1967).

[61] S. Thangavelu and M.A. Hussein, Flaw Detection by Spatially Coded Backscatter Radiography, *Appl. Radiation and Isotopes* **65** 189–198 (2006).

[62] P. Ubertini, F. Lebrun, G. Di Cocco, A. Bazzano, A.J. Bird, K. Broenstad, A. Goldwurm, G. La Rosa, C. Labanti, P. Laurent, I.F. Mirabel, E.M. Quadrini, B. Ramsay, V. Reglero, L. Sabau, B. Sacco, R. Staubert, L. Vigroux, M.C. Weisskopf and A.A. Zdziarski, IBIS: The Imager On-Board INTEGRAL, *Astron. Astrophys.* **411** (2003) L131–L139.

[63] G. Vedrenne, J.-P. Roques, V. Schonfelder, P. Mandrou, G.G. Lichti, A. von Kienlin, B. Cordier, S. Schanne, J. Knodlseder, G. Skinner, P. Jean, F. Sanchez, P. Caraveo, B. Teegarden, P. von Ballmoos, L. Bouchet, P. Paul, J. Matteson, S. Boggs, C. Wunderer, P. Leleux, G. Weidenspointer, P. Durouchoux, R. Diehl, A. Strong, M. Casse, M.A. Clair and Y Andre, SPI: The Spectrometer Aboard INTEGRAL, *Astron. Astrophys.* **411** (2003) L63–L70.

[64] T. Villela, J. Braga, F. D'Amico and U.B. Jayanthi, A MURA-Based Coded Mask Telescope, *Adv. Spa. Res.* **15** (1995) 95–98.

[65] G. Weathers and E.M. Holliday, Group-Complementary Array Coding for Radar Clutter Rejection, *IEEE Trans. Aerosp. Electron. Sys.* **AES-19** (1983) 369–379.

[66] A.L. Whiteman, The Cyclotomic Numbers of Order Sixteen, *Trans. Amer. Math. Soc.* **86** (1957) 401–413.

[67] A.L. Whiteman, The Cyclotomic Numbers of Order Ten, *Proc. Symp. Appl. Math.* **10**, American Mathematical Society, Providence, RI (1960), 95–111.

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

[69] A.P. Willmore, G.K. Skinner, C.J. Eyles and B. Ramsey, A Coded Mask Telescope for the Spacelab-2 Mission, *Nucl. Instrum. Meth. Phys. Res.* **A221** (1984) 284–287.

[70] C. Winkler, T. J.-L. Courvoisier, G. Di Cocco, N. Gehrels, A. Gimenez, S. Grebenev, W. Hermsen, J.M. Mas-Hesse, F. Lebrun, N. Lund, G.G.C. Palumbo, J. Paul, J.-P. Roques, H. Schnopper, V. Schonfelder, R. Sunyaev, B. Teegarden, P. Ubertini, G. Vedrenne and A.J. Dean, The INTEGRAL Mission, *Astron. Astrophys.* **411** (2003) L1–L6.

[71] M. Woodring, D. Beddingfield, D. Souza, G. Entine, M. Squillante, J. Christian and A. Kogan, Advanced Multi-Dimensional Imaging of Gamma-Ray Radiation, *Nucl. Instrum. Meth. Phys. Res.* **A505** (2003) 415–419.

[72] P. Yuan and H. Yahui, A Note on Power Residue Difference Sets, *J. Algebra* **291** (2005) 269–273.