

Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.

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 n th 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

1	Overview	1
2	Difference Sets and Qualified Difference Sets	3
2.1	Difference Sets	3
2.2	Existence of RDS and MRDS	6
2.3	Qualified Difference Sets	9
2.4	Cyclotomy	12
3	Qualified Residue Difference Sets	15
3.1	Introduction	15
3.2	Necessary and Sufficient Conditions for the Existence of QRDS and MQRDS	15
3.3	Some Properties of QRDS and MQRDS	19
4	Existence of QRDS and MQRDS for $n = 2, 4$ and 6	21
4.1	Introduction	21
4.2	Existence for $n = 2$	21
4.3	Existence for $n = 4$	22
4.4	Existence for $n = 6$	23
5	Nonexistence of QRDS for Higher Values of n	25
5.1	Introduction	25
5.2	Nonexistence for $n = 8$	26
5.3	Nonexistence for $n = 10$	27
5.4	Nonexistence for $n = 12$	28
5.5	Nonexistence for $n = 14$	31
5.6	Nonexistence for $n = 18$	36
6	Qualified Difference Sets from Unions of Cyclotomic Classes	43
6.1	Introduction	43
6.2	Preliminary Discussion	43
6.3	Theory	45
6.4	Results	48
6.5	Results for $n = 8$	48

6.6	Results for $n = 4$ and $n = 6$	54
6.7	Results for $n = 10$	56
6.8	Results for $n = 12$	59
7	Applications of Qualified Difference Sets	63
7.1	Introduction	63
7.2	Example of a Practical Application	64
7.3	Theoretical Outline	66
7.4	Numerical Example	69
7.5	Potential Applications of QDS	69
8	Summary and Conclusions	73
A	Cyclotomic Constants	75
A.1	Cyclotomic Constants for $n = 2$	75
A.2	Cyclotomic Constants for $n = 4$	75
A.3	Cyclotomic Constants for $n = 6$	75
A.4	Cyclotomic Constants for $n = 8$	76
A.5	Cyclotomic Constants for $n = 10$	77
A.6	Cyclotomic Constants for $n = 12$	78
A.7	Cyclotomic Constants for $n = 14$	79
A.8	Cyclotomic Constants for $n = 18$	80
B	Complementary QDS	83
	Bibliography	85

List of Figures

- 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. 65
- 7.2 Cross-correlation function for a QRDS with $n = 4$, $p = 17$, $k = 4$ and $\lambda = 1$. 69

List of Tables

2.1	Parameters for the existence of RDS.	8
2.2	Parameters for the existence of MRDS.	9
2.3	Table showing $r_i - 2r_j \pmod{17}$	11
5.1	Parameters for the cyclotomic constants of order 12 for even k	29
6.1	List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n = 8$	54
6.2	List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n = 4$ and $n = 6$	57
6.3	List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n = 10$	60
6.4	List of parameters of QDS and MQDS composed of unions of cyclotomic classes for $n = 12$	61

