Ohio State University Mathematical Research Institute Publications 10

Ohio State University
Mathematical Research Institute Publications

1 Topology '90, *B. Apanasov*, *W. D. Neumann*, *A. W. Reid*, *L. Siebenmann* (Eds.)
2 The Arithmetic of Function Fields, *D. Goss*, *D. R. Hayes*, *M. I. Rosen* (Eds.)
3 Geometric Group Theory, *R. Charney*, *M. Davis*, *M. Shapiro* (Eds.)
4 Groups, Difference Sets, and the Monster, *K. T. Arasu*, *J. F. Dillon*, *K. Harada*, *S. Sehgal*, *R. Solomon* (Eds.)
5 Convergence in Ergodic Theory and Probability, *V. Bergelson*, *P. March, J. Rosenblatt* (Eds.)
6 Representation Theory of Finite Groups, *R. Solomon* (Ed.)
7 The Monster and Lie Algebras, *J. Ferrar*, *K. Harada* (Eds.)
8 Groups and Computation III, *W. M. Kantor*, *Á. Seress* (Eds.)
9 Complex Analysis and Geometry, *J. D. McNeal* (Ed.)

Codes and Designs

Proceedings of a conference honoring
Professor Dijen K. Ray-Chaudhuri
on the occasion of his 65th birthday

The Ohio State University
May 18–21, 2000

Editors

K. T. Arasu
Á. Seress

Walter de Gruyter · Berlin · New York 2002

Editors

K. T. Arasu
Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA

Ákos Seress
Department of Mathematics, The Ohio State University, Columbus, OH 43210-1174, USA

Series Editors

Gregory R. Baker
Department of Mathematics, The Ohio State University, Columbus, OH 43210-1174, USA

Karl Rubin
Department of Mathematics, Stanford University, Stanford, CA 94305-2125, USA

Walter D. Neumann
Department of Mathematics, Columbia University, New York, NY 10027, USA

Mathematics Subject Classification 2000: 05−06; 94−06

♾ Printed on acid-free paper which falls within the guidelines of the ANSI to ensure permanence and durability.

Library of Congress Cataloging-in-Publication Data

Codes and designs : proceedings of a conference honoring Professor Dijen K. Ray-Chaudhuri on the occasion of his 65th birthday, The Ohio State University, May 18−21, 2000 / editors, K. T. Arasu, Á. Seress.
p. cm. − (Ohio State University Mathematical Research Institute publications ; vol. 10)
ISBN 3 11 017396 4 (acid-free-paper)
I. Arasu, K. T., 1954− II. Seress, Ákos, 1958− III. Ohio State University Mathematical Research Institute publications ; 10.
2002023667

Die Deutsche Bibliothek − Cataloging-in-Publication Data

Codes and designs : proceedings of a Conference Honoring Professor Dijen K. Ray-Chaudhuri on the Occasion of His 65th Birthday, the Ohio State University, May 18−21, 2000 / ed. K. T. Arasu ; Á. Seress. − Berlin ; New York : de Gruyter, 2002
(Ohio State University Mathematical Research Institute publications ; 10)
ISBN 3-11-017396-4

Printed in Germany.
Cover design: Thomas Bonnie, Hamburg.
Typeset using the authors' T_EX files: I. Zimmermann, Freiburg.
Printing and binding: Hubert & Co. GmbH & Co. KG, Göttingen.

Preface

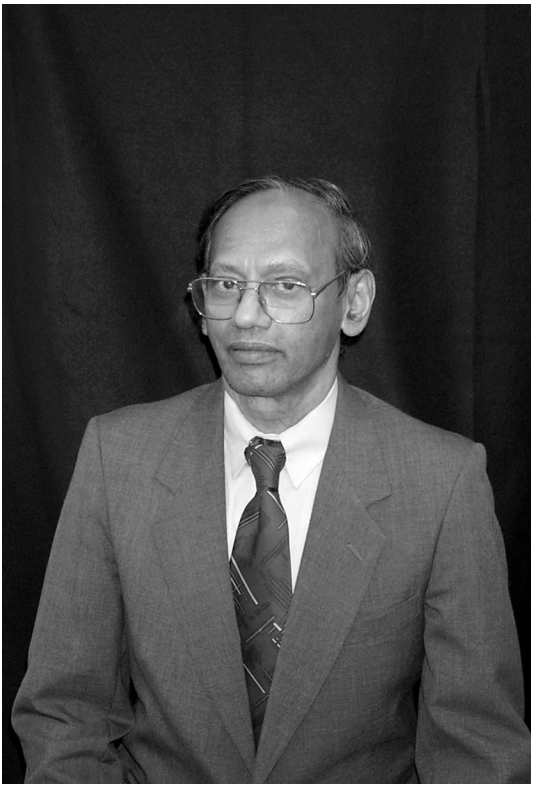
Following an initiative of the late Professor Hans Zassenhaus in 1965, the Departments of Mathematics at the The Ohio State University and Denison University have been holding conferences in Combinatorics, Group Theory, and Ring Theory. Initially, these meetings have been held annually, and later biannually; in the year 2000, the 25th meeting of this series was conducted. These conferences have primarily attracted mathematicians from institutions in Ohio and nearby states, but there have been many participants from other parts of the country, as well as from abroad. There are usually twenty to thirty invited 20-minute talks given in each of the three main areas. However, at the last conference, held during May 18–21, 2000 on the Ohio State main campus in Columbus, there was a special addition to the Combinatorics program in tribute to the 65th birthday of Dijen Ray-Chaudhuri. The Dijen 65 part of the conference consisted of fourteen 40-minute lectures by either former students of Dijen or other mathematicians with strong personal and professional ties with him. The topics ranged from Coding Theory, Design Theory, Geometry and Optimization to Graph Theory, reflecting the wide range of areas to which Professor Ray-Chaudhuri has made substantial contributions during his exemplary career.

The banquet to celebrate his 65th birthday included remarks made by Professors R.M. Wilson, Jeff Kahn, Thomas Dowling, and Dr. John F. Dillon. The highlight of this party was the presentation of the Euler medal to Professor Ray-Chaudhuri for his life-long achievements and contributions to Combinatorics. This medal was presented to him by Professor Ralph Stanton on behalf of the Institute of Combinatorics and Applications.

We are indebted to Professor Thomas Dowling for his invaluable help with the organization of the combinatorics part of the conference, and to the referees of this volume for their conscientious work. We are very grateful for the generous support of the Mathematical Research Institute of The Ohio State University and the National Security Agency.

K. T. Arasu
Ákos Seress

Table of contents



Dijen Ray-Chaudhuri

Highlights of Dijen Ray-Chaudhuri's research

Ákos Seress

Dijen Ray-Chaudhuri, in over 80 published papers, books, and monographs, has worked on a broad range of problems in combinatorics that arose in the theory of error-correcting codes, graph theory, design theory, difference sets, geometry, information retrieval, and combinatorial optimization. His first major contribution appeared in his Ph.D. thesis **[1]**, where he constructed the 2-error-correcting version of the codes which later became known as BCH codes. The name BCH stands for Bose and Chaudhuri, since Dijen constructed the d-error-correcting version of these codes with his advisor R. Bose **[2]**, and for Hocquenguem, who independently discovered the same codes. BCH codes are the first major application of algebra in coding theory, and are considered of fundamental importance in the subject. Books in the area (for example, Algebraic Theory of Coding by Berlekamp, and Theory of Error-Correcting Codes by MacWilliams and Sloane) devote at least a chapter to BCH codes.

Another fundamental result is Dijen's joint work with R. Wilson **[18]**, on a theory of recursive construction of designs. These constructions led to the solution of a century-old problem on the existence of Steiner systems, known also as the Kirkman School Girl Problem. Later, Dijen extended the scope of these investigations. He proved (with N. Singhi) **[47]** the λ-large existence theorem for designs in projective spaces and affine spaces, and (with E. Schram) **[54]** he constructed designs and large sets of designs in vector spaces, using the theory of quadratic forms. Popular scientific articles about BCH codes and the Kirkman School Girl Problem appeared in the Scientific American and in the Encyclopedia Britannica.

Besides these fundamental results, Dijen's work opened up new areas of research in other branches of combinatorics. His early paper **[4]** on minimally redundant systems of Boolean functions has a significant follow-up in the Russian electrical engineering community, while another early paper **[9]** on the connection of association schemes with finite projective spaces and designs is the basis of research on association schemes in China.

Another highlight is Dijen's work with A. Sprague **[33]** and E. Brickel **[42]**, on the characterization of graphs and association schemes arising from the intersection properties of flats of finite projective spaces, affine spaces, and attenuated spaces. These results are deep, and they attracted the attention of finite geometers.

In **[39]**, Dijen with R. Roth developed a theory of nonassociative commutative Moufang loops of exponent 3 and nilpotence class 2, arising from Hall triple systems. This theory was used to construct new Hall triple systems, which are also perfect

Codes and Designs
Ohio State Univ. Math. Res. Inst. Publ. 10

matroid designs. The seminal paper **[41]**, with S. B. Rao and N. M. Singhi, develops a structure theory for imprimitive association schemes. The paper **[57]**, with N. M. Singhi and G. R. Vijayakumar is a continuation of Dijen's interest in the spectral characterization of line graphs **[12]**, and uses root lattices and root systems for the classification of signed graphs with least eigenvalue at least -2. Earlier work with A. J. Hoffman **[10]**, **[11]** gives spectral characterization of line graphs of symmetric designs and affine planes.

Dijen also contributed to extremal set theory. His most important results are an algorithm for the computation of the covering number of a hypergraph **[6]**, a bound for the size of set systems with pairwise intersections of prescribed sizes (with R. Wilson) **[24]**, and the generalization of this result to polynomial semilattices (with T. Zhu and J. Qian) **[58]**, **[69]**.

Dijen gave over hundred invited lectures at various institutions. The most important ones are a 45-minute address at the International Congress of Mathematics in 1970, and an hour-long invited talk at the Combined Winter Meeting of the AMS and MAA in 1973. He received a Senior US Scientist Award of the Alexander von Humboldt Foundation, the Distinguished Senior Research Award of The Ohio State University, and the Euler Medal of the Institute for Combinatorics and its Applications **[76]**.

Last, but not least, we have to mention Dijen's enormous contribution to the development of young researchers. So far, he has been the advisor of 31 Ph.D. students. In the order of graduation, they are R. M. Wilson, B. T. Datta, A. P. Sprague, K. S. Vijayan, A. H. Chan, K. Chang, D. Nemzer, J. LeFever, H.-P. Ko, J. Kahn, R. Roth, R. Games, E. Brickell, A. Moon, K. T. Arasu, Á. Seress, D. Miklós, E. J. Schram, J. J. Kim, L. Narayani, H.-M. Shaw, T. Zhu, X. Wu, Q. Xiang, H. Mohácsy, K. Liu, T. Blackford, J. Qian, I. Siap, G. Yeh, and A. Nabavi. Among these, there are two Pólya Prize winners, an Associate Director of the Rényi Institute of the Hungarian Academy of Sciences, over ten professors at universities all over the world, and several hold leadership positions in industry.

References

[1] D. K. Ray-Chaudhuri, On the application of the geometry of quadrics to the construction of partially balanced incomplete block designs and error-correcting codes, The Institute of Statistics, Univ. North Carolina, Chapel Hill, NC Mimeo Series 230, 1959.

[2] R. C. Bose and D. K. Ray-Chaudhuri, On a class of binary error-correcting group codes, Inform. and Control 3 (1960), 68–79.

[3] R. C. Bose and D. K. Ray-Chaudhuri, Further results on error correcting binary group codes, Inform. and Control 3 (1960), 279–290.

[4] D. K. Ray-Chaudhuri, On the construction of minimally redundant reliable system designs, Bell Systems Technical Journal 40 (1961), 595–611.

[5] D. K. Ray-Chaudhuri, Some results on quadrics in finite projective geometry based on Galois fields, Canad. J. Math. 14 (1962), 129–138.

[6] D. K. Ray-Chaudhuri, An algorithm for the minimum cover of an abstract complex, Canad. J. Math. 15 (1963), 11–24.

[7] D. K. Ray-Chaudhuri, Application of the geometry of quadrics for constructing PBIB designs, Ann. Math. Statist. 33 (1962), 1175–1186.

[8] D. K. Ray-Chaudhuri, On some connections between balanced incomplete block designs and minimum covers, in: Coll. Internat. Du'Centre National de la Recherche Sci. 110, le Plan D'experiences, Paris, August 29–September 6, 1961, 129–136.

[9] D. K. Ray-Chaudhuri, Some configurations in finite projective spaces and partially balanced incomplete block designs, Canad. J. Math. 17 (1965), 114–123.

[10] A. J. Hoffman and D. K. Ray-Chaudhuri, On the line graph of a finite affine plane, Canad. J. Math. 17 (1965), 687–694.

[11] A. J. Hoffman and D. K. Ray-Chaudhuri, On the line graph of a symmetric balanced incomplete block design, Trans. Amer. Math. Soc. 116 (1965), 238–252.

[12] D. K. Ray-Chaudhuri, Characterization of line graphs, J. Combin. Theory 3 (1967), 201–214.

[13] G. C. Chow and D. K. Ray-Chaudhuri, An alternative proof of Hannan's theorem on canonical correlation and multiple equation systems, Econometrica 35 (1967), 139–142.

[14] D. K. Ray-Chaudhuri, Combinatorial information retrieval systems for files, SIAM J. Appl. Math. 16 (1968), 973–992.

[15] C. T. Abraham, S. P. Ghosh and D. K. Ray-Chaudhuri, File organization schemes based on finite geometries, Inform. and Control 12 (1968), 143–163.

[16] D. K. Ray-Chaudhuri, On some connections between graph theory and experimental designs and some recent existence results, in: Graph Theory Appl. (Proc. Adv. Sem., Math. Research Center, Univ. of Wisconsin, Madison, WI, 1969), Academic Press, New York 1970, 149–166.

[17] D. K. Ray-Chaudhuri and R. M. Wilson, On the existence of resolvable balanced incomplete block designs, in: Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, AB, 1969), Gordon and Breach, New York 1970, 331–341.

[18] D. K. Ray-Chaudhuri and R. M. Wilson, Solution of Kirkman's schoolgirl problem, in: Combinatorics (Univ. California, Los Angeles, CA, 1968), Proc. Sympos. Pure Math. XIX, Amer. Math. Soc., Providence, R.I., 1971, 187–203.

[19] H. Hanani, D. K. Ray-Chaudhuri and R. M. Wilson, On resolvable designs, Discrete Math. 3 (1972), 343–357.

[20] D. K. Ray-Chaudhuri, Recent developments on combinatorial designs, in: Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3, Gauthier-Villars, Paris 1971, 223–227.

[21] D. K. Ray-Chaudhuri and R. M. Wilson, The existence of resolvable block designs, in: Survey of combinatorial theory (Proc. Internat. Sympos., Colorado State Univ., Fort Collins, CO, 1971), North-Holland, Amsterdam 1973, 361–375.

[22] C. Berge and D. K. Ray-Chaudhuri (editors), Hypergraph Seminar, Proceedings of the First Working Seminar on Hypergraphs, The Ohio State University, August 16 – September 9, 1972. Lecture Notes in Math. 411, Springer-Verlag, Berlin, New York 1974.

[23] H. B. Mann and D. K. Ray-Chaudhuri, Lectures on error correcting codes, The University of Arizona Department of Mathematics Lecture Note Series, University of Arizona, Tucson, AZ, 1974.

[24] D. K. Ray-Chaudhuri and R. M. Wilson, On t-designs, Osaka J. Math. 12 (1975), 737–744.

[25] D. K. Ray-Chaudhuri, Uniqueness of association schemes, in: Colloquio Internazionale sulle Teorie Combinatorie (Rome, 1973), Tomo II, Atti dei Convegni Lincei 17, Accad. Naz. Lincei, Rome 1976, 465–479.

[26] D. K. Ray-Chaudhuri and A. P. Sprague, Characterization of projective incidence structures, Geom. Dedicata 5 (1976), 361–376.

[27] D. K. Ray-Chaudhuri and N. M. Singhi, A characterization of the line-hyperplane design of a projective space and some extremal theorems for matroid designs, in: Number theory and algebra, Academic Press, New York 1977, 289–301.

[28] D. K. Ray-Chaudhuri, Combinatorial characterization theorems for geometric incidence structures, in: Combinatorial surveys (Proc. Sixth British Combinatorial Conf., Royal Holloway Coll., Egham, 1977), Academic Press, London 1977, 87–116.

[29] D. K. Ray-Chaudhuri, Some characterization theorems for graphs and incidence structures, in: Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II, Colloq. Math. Soc. János Bolyai 18, North-Holland, Amsterdam, New York 1978, 821–842.

[30] D. K. Ray-Chaudhuri (editor), Relations between combinatorics and other parts of mathematics, The Ohio State University, March 20–23, 1978, Proc. Sympos. Pure Math. XXXIV, Amer. Math. Soc., Providence, RI, 1979.

[31] A. H. Chan and D. K. Ray-Chaudhuri, Characterization of "linegraph of an affine space", J. Combin. Theory Ser. A 26 (1979), 48–64.

[32] A. H. Chan and D. K. Ray-Chaudhuri, Embedding of a pseudoresidual design into a Möbius plane, J. Combin. Theory Ser. A 32 (1982), 73–98.

[33] D. K. Ray-Chaudhuri and A. P. Sprague, A combinatorial characterization of attenuated spaces, Utilitas Math. 15 (1979), 3–29.

[34] H.-P. Ko and D. K. Ray-Chaudhuri, Group divisible difference sets and families from s-flats of finite geometries, Proceedings of the Tenth Southeastern Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic Univ., 1979, Congr. Numer. 24 (1979), 601–627.

[35] D. K. Ray-Chaudhuri, Affine triple systems, in: Combinatorics and graph theory (Calcutta, 1980), Lecture Notes in Math. 885, Springer-Verlag, Berlin, New York 1981, 60–69.

[36] D. K. Ray-Chaudhuri and S. S. Rappaport, Sampled multiserver queues with general arrivals and deterministic service time, Proc. IEE-E 127 (1980), 88–92.

[37] H.-P. Ko and D. K. Ray-Chaudhuri, Multiplier theorems, J. Combin. Theory Ser. A 30 (1981), 134–157.

[38] H.-P. Ko and D. K. Ray-Chaudhuri, Intersection theorems for group divisible difference sets, Discrete Math. 39 (1982), 37–58.

[39] R. Roth and D. K. Ray-Chaudhuri, Hall triple systems and commutative Moufang exponent 3 loops: the case of nilpotence class 2, J. Combin. Theory Ser. A 36 (1984), 129–162.

[40] D. K. Ray-Chaudhuri, Group divisible difference sets, in: Enumeration and design (Waterloo, Ont., 1982), Academic Press, Toronto, ON, 1984, 271–283.

[41] S. B. Rao, D. K. Ray-Chaudhuri and N. M. Singhi, On imprimitive association-schemes, in: Combinatorics and applications (Calcutta, 1982), Indian Statist. Inst., Calcutta 1984, 273–291.

[42] E. Brickel and D. K. Ray-Chaudhuri, Characterization of incidence structures of intervals of affine geometries, Mitt. Math. Sem. Giessen 166 (1984), 17–34.

[43] K. T. Arasu and D. K. Ray-Chaudhuri, Divisible quotient lists and their multipliers, in: Combinatorics, Graph theory and Computing (Proceedings of the sixteenth Southeastern international conference on combinatorics, graph theory and computing, Boca Raton, FL, 1985) Congr. Numer. 49 (1985), 321–338.

[44] K. T. Arasu and D. K. Ray-Chaudhuri, Multiplier theorem for a difference list, Ars Combin. 22 (1986), 119–137.

[45] D. K. Ray-Chaudhuri and N. M. Singhi, On existence of t-designs with large v and λ, SIAM J. Discrete Math. 1 (1988), 98–104.

[46] D. K. Ray-Chaudhuri and N. M. Singhi, On existence and number of orthogonal arrays, J. Combin. Theory Ser. A 47 (1988), 28–36; Corrigendum: J. Combin. Theory Ser. A 66 (1994), 327–328.

[47] D. K. Ray-Chaudhuri and N. M. Singhi, q-analogues of t-designs and their existence, Linear Algebra Appl. 114/115 (1989), 57–68.

[48] K. T. Arasu and D. K. Ray-Chaudhuri, Affine difference sets and their homomorphic images, Mitt. Math. Sem. Giessen 192 (1989), 71–78.

[49] D. K. Ray-Chaudhuri (editor), Coding theory and design theory. Part I. Coding theory, IMA Vol. Math. Appl. 20, Springer-Verlag, New York 1990.

[50] D. K. Ray-Chaudhuri (editor), Coding theory and design theory. Part I. Design theory, IMA Vol. Math. Appl. 21, Springer-Verlag, New York 1990.

[51] M. Deza, D. K. Ray-Chaudhuri and N. M. Singhi, Positive independence and enumeration of codes with a given distance pattern, in: Coding theory and design theory, Part I, IMA Vol. Math. Appl. 20, Springer-Verlag, New York 1990, 93–101.

[52] D. K. Ray-Chaudhuri, editor, Combinatorial mathematics and applications, Sankhyā Ser. A 54 (1992), special issue dedicated to the memory of R. C. Bose.

[53] D. K. Ray-Chaudhuri and N. M. Singhi, Some recent results on t-designs, Sankhyā Ser. A 54 (1992), special issue (Combinatorial mathematics and applications, Calcutta, 1988), 383–391.

[54] D. K. Ray-Chaudhuri and E. J. Schram, Designs on vector spaces constructed using quadratic forms, Geom. Dedicata 42 (1992), 1–42.

[55] D. K. Ray-Chaudhuri and T. Zhu, A recursive method for construction of designs, Discrete Math. 106/107 (1992), A collection of contributions in honour of Jack van Lint, 399–406.

[56] D. K. Ray-Chaudhuri and N. M. Singhi (editors), Prof. R. C. Bose Memorial Issue, J. Combin. Inform. System Sci. 17 (1992), 1–2.

[57] D. K. Ray-Chaudhuri, N. M. Singhi and G. R. Vijayakumar, Signed graphs having least eigenvalue around -2, J. Combin. Inform. System Sci. 17 (1992), 148–165.

[58] D. K. Ray-Chaudhuri and T. Zhu, s-intersection families and tight designs, in: Coding theory, design theory, group theory (Burlington, VT, 1990), Wiley-Interscience Publishers, New York 1993, 67–75.

[59] K. T. Arasu, D. K. Ray-Chaudhuri and N. M. Singhi, Simple designs, J. Combin. Inform. System Sci. 18 (1993), 130–135.

[60] D. K. Ray-Chaudhuri, N. M. Singhi, S. Sanyal, and P. S. Subramanian, Theory and design of t-unidirectional error-correcting and d-unidirectional error-detecting code, IEEE Trans. Comput. 43 (1994), 1221–1226.

[61] D. K. Ray-Chaudhuri and E. J. Schram, A large set of designs on vector spaces, J. Number Theory 47 (1994), 247–272.

[62] D. K. Ray-Chaudhuri and H.-M. Shaw, A greedy algorithm for maximum multicommodity flows on dominance networks, J. Combin. Inform. System Sci. 20 (1995), 161–171.

[63] D. K. Ray-Chaudhuri and X. Wu, Abelianizations of non-abelian difference sets, J. Combin. Inform. System Sci. 20 (1995), 173–195.

[64] D. K. Ray-Chaudhuri, Vector space designs, in: The CRC Handbook of Combinatorial Designs (Colbourn, Charles J. et al., eds.), CRC Press Ser. Discrete Math. Appl., CRC Press, Boca Raton, FL, 1996, 492–496.

[65] D. K. Ray-Chaudhuri and Q. Xiang, Constructions of partial difference sets and relative difference sets using Galois rings, Des. Codes Cryptogr. 8 (1996), special issue dedicated to Hanfried Lenz, 215–227.

[66] Y. Q. Chen, D. K. Ray-Chaudhuri and Q. Xiang, Constructions of partial difference sets and relative difference sets using Galois rings. II, J. Combin. Theory Ser. A 76 (1996), 179–196.

[67] D. K. Ray-Chaudhuri and T. Zhu, Orthogonal arrays and ordered designs, J. Statist. Plann. Inference 58 (1997), 177–183.

[68] D. K. Ray-Chaudhuri and Q. Xiang, New necessary conditions for abelian Hadamard difference sets, J. Statist. Plann. Inference 62 (1997), 69–79.

[69] J. Qian and D. K. Ray-Chaudhuri, Frankl-Füredi type inequalities for polynomial semilattices, Electron. J. Combin. 4 (1997), no. 1, Research Paper 28, 15 pp. (electronic).

[70] J. Qian and D. K. Ray-Chaudhuri, Combinatorial inequalities for quasi polynomial semilattices, Recent advances in interdisciplinary mathematics, Portland, ME, 1997, J. Combin. Inform. System Sci. 25 (2000), 59–76.

[71] I. Siap, N. Aydin, and D. K. Ray-Chaudhuri, New ternary quasi-cyclic codes with better minimum distances, IEEE Trans. Inform. Theory 46 (2000), 1554–1558.

[72] T. Blackford and D. K. Ray-Chaudhuri, A transform approach to permutation groups of cyclic codes over Galois rings, IEEE Trans. Inform. Theory 46 (2000), 2350–2358.

[73] I. Siap and D. K. Ray-Chaudhuri, New linear codes over $\mathbf{F_3}$ and $\mathbf{F_5}$ and improvements on bounds, Des. Codes Cryptogr. 21 (2000), special issue dedicated to Dr. Jaap Seidel on the occasion of his 80th birthday (Oisterwijk, 1999), 223–233.

[74] J. Qian and D. K. Ray-Chaudhuri, On mod-p Alon-Babai-Suzuki inequality, J. Algebraic Combin. 12 (2000), 85–93.

[75] I. Siap and D. K. Ray-Chaudhuri, On r-fold complete weight enumerators of r linear codes, in: Algebra and its applications (Athens, OH, 1999), Contemp. Math. 259, Amer. Math. Soc., Providence, RI, 2000, 501–513.

[76] The 1999 Euler, Hall, and Kirkman medals, Bull. Inst. Combin. Appl. 30 (2000), 7–9.

[77] I. Siap, N. Aydin, and D. K. Ray-Chaudhuri, New 1-generator quasi-twisted codes over GF(5), in: Codes and association schemes (Piscataway, NJ, 1999), DIMACS Ser. Discrete Math. Theoret. Comput. Sci. 56, Amer. Math. Soc., Providence, RI, 2001, 265–275.

[78] H. Mohácsy and D. K. Ray-Chaudhuri, A construction for infinite families of Steiner 3-designs, J. Combin. Theory Ser. A 94 (2001), 127–141.

[79] J. Qian and D. K. Ray-Chaudhuri, Extremal case of Frankl-Ray-Chaudhuri-Wilson inequality, J. Statist. Plann. Inference 95 (2001), special issue on design combinatorics: in honor of S. S. Shrikhande, 293–306.

[80] H. Mohácsy and D. K. Ray-Chaudhuri, Candelabra systems and t-designs, J. Statist. Plann. Inference, to appear.

[81] H. Mohácsy and D. K. Ray-Chaudhuri, A construction for group-divisible t-designs with strength $t \geq 2$ and index 1, J. Statist. Plann. Inference, to appear.

[82] N. Aydin, D. K. Ray-Chaudhuri and I. Siap, The structure of 1-generator quasi-twisted codes and improvements on bounds, Des. Codes Cryptogr., to appear.

Á. Seress
Department of Mathematics
The Ohio State University
Columbus, OH 43210-1174, U.S.A.
akos@math.ohio-state.edu

On the p-ranks of GMW difference sets

K. T. Arasu, Henk D. L. Hollmann, Kevin Player, and Qing Xiang *

Abstract. We determine the p-ranks of the classical GMW difference sets (p even or odd). In the p odd case, this solves an open problem mentioned in **[4]**, p. 461 and **[15]**, p. 84. We also compute the 2-ranks of some non-classical GMW difference sets arising from monomial hyperovals.

2000 Mathematics Subject Classification: primary 05B10; secondary 11L05.

1. Introduction

Let G be a finite (multiplicative) group of order v. A k-element subset D of G is called a (v, k, λ) *difference set* in G if the list of "differences" $d_1 d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$, represents each nonidentity element in G exactly λ times.

We say that two (v, k, λ) difference sets D_1 and D_2 in an abelian group G are *equivalent* if there exists an automorphism α of G and an element $g \in G$ such that $\alpha(D_1) = D_2 g$. In particular, if G is cyclic, then D_1 and D_2 are equivalent if there exists an integer t, $\gcd(t, v) = 1$, such that $D_1^{(t)} = D_2 g$ for some $g \in G$, where $D_1^{(t)} = \{d^t \mid d \in D_1\}$.

Singer **[17]** discovered a large class of difference sets which are related to finite projective geometry. These difference sets have parameters

$$v = \frac{q^d - 1}{q - 1}, \qquad k = \frac{q^{d-1} - 1}{q - 1}, \qquad \lambda = \frac{q^{d-2} - 1}{q - 1} \tag{1}$$

where $d \geq 3$, and they exist whenever q is a prime power.

In this paper, difference sets with parameters (1), or the complementary parameters $v = (q^d - 1)/(q - 1)$, $k = q^{d-1}$, $\lambda = q^{d-2}(q - 1)$ are called difference sets with *classical* parameters. In ([**2**], p. 143), it is mentioned that on one hand, Singer **[17]** conjectured that there is only one equivalence class of difference sets with parameters (1) if $d = 3$ (i.e., $\lambda = 1$); on the other hand, the largest known class of multiple inequivalent difference sets also have classical parameters. While little progress has

*K. T. Arasu's research is supported by NSF grant CCR-9814106 and by NSA grant 904-01-1-0041. Kevin Player was partially supported by an REU grant from the NSF. Q. Xiang was supported by NSA grant 904-01-1-006.

been made on the Singer conjecture above, there has been a great deal of research on constructing inequivalent difference sets with classical parameters, especially when $q = 2$. For a survey of recent work in this area, we refer the reader to **[20]**.

The first infinite series of examples of mutually inequivalent difference sets with parameters $\left(\frac{q^m-1}{q-1}, q^{m-1}, q^{m-2}(q-1)\right)$ is due to Gordon, Mills and Welch **[8]**. These difference sets will be called *GMW difference sets*, and the symmetric designs developed from these difference sets are called *GMW designs*. When $q = 2$, the 2-ranks of the so-called *classical* GMW difference sets (see Section 2 for definition) were computed by Scholtz and Welch **[16]** in terms of the linear spans of their characteristic sequences. However, the p-ranks of the classical GMW difference sets in the case $q \neq 2$ are not known (cf. **[4]**, p. 461, **[15]**, p. 84). In this paper, we compute the p-ranks of the classical GMW difference sets. We also compute the 2-ranks of some non-classical GMW difference sets from monomial hyperovals. The methods used here to compute the p-ranks are essentially the same as those in **[7]**, but the details are more complicated because of the recursive nature of GMW difference sets. We first show that the character sums of the GMW difference sets under consideration are related to Gauss or Jacobi sums, then we use Stickelberger's theorem on the prime ideal factorization of Gauss sums to reduce the problem of computing the p-ranks to certain counting problems. The counting problems are then solved either in a straightforward manner or with the help of the so-called transfer matrix method.

It should be noted that the p-ranks of GMW difference sets usually cannot distinguish GMW designs because very often inequivalent GMW difference sets have the same p-ranks (see, for example, Corollary 3.7). The difficult problem whether inequivalent GMW difference sets lead to nonisomorphic GMW designs is recently solved by Kantor **[11]** using group theory.

2. Preliminaries

We first recall a construction of Singer difference sets. Let $\mathbb{F}_{q^d}$ be the finite field with q^d elements, where $q = p^s$, p is a prime, $d \geq 3$, and let Tr be the trace from $\mathbb{F}_{q^d}$ to $\mathbb{F}_q$. We may take a system L of coset representatives of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^d}^*$ such that Tr maps L into $\{0, 1\}$. Write $L = L_0 \cup L_1$, where

$$L_0 = \{x \in L \mid \mathrm{Tr}(x) = 0\}, \quad L_1 = \{x \in L \mid \mathrm{Tr}(x) = 1\}. \tag{2}$$

Theorem 2.1. *With the above notation, L_0 is a $\left(\frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}, \frac{q^{d-2}-1}{q-1}\right)$ difference set in the quotient group $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$, and L_1 is a $\left(\frac{q^d-1}{q-1}, q^{d-1}, q^{d-2}(q-1)\right)$ difference set in $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$.*

Proofs of Theorem 2.1 of course can be found in many places. For our later use, we mention a proof by Yamamoto **[22]** (see also **[7]**), in which it is shown that the

character values of L_0 and L_1 are related to Gauss sums. More precisely, let χ be a nontrivial multiplicative character of $\mathbb{F}_{q^d}$ whose restriction to $\mathbb{F}_q^*$ is trivial. Then

$$\chi(L_0) = g(\chi)/q, \text{ and } \chi(L_1) = -g(\chi)/q, \tag{3}$$

where $g(\chi)$ is the Gauss sum defined over $\mathbb{F}_{q^d}$, i.e.,

$$g(\chi) = \sum_{a \in \mathbb{F}_{q^d}^*} \chi(a) \xi_p^{\mathrm{Tr}_{q^d/p}(a)},$$

here ξ_p is a fixed complex primitive pth root of unity and $\mathrm{Tr}_{q^d/p}$ is the absolute trace from $\mathbb{F}_{q^d}$ to $\mathbb{F}_p$, the field of p elements.

Now we proceed to discuss the GMW construction. Let $m = d \cdot e$, where $d > 2$, $e > 1$ are integers, and let q be a prime power. We define

$$R' = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q^d}(x) = 1\},$$

where Tr_{q^m/q^d} is the trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^d}$. Let $\mu : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ be the canonical epimorphism, and let $R = \mu(R')$. Using the terminology of relative difference sets (see, for example **[15]**, p. 13), the set R' is a $\left(\frac{q^m-1}{q^d-1}, q^d - 1, q^{d(e-1)}, q^{d(e-2)}\right)$ relative difference set in $\mathbb{F}_{q^m}^*$ relative to $\mathbb{F}_{q^d}^*$, and R is a

$$\left(\frac{q^m-1}{q^d-1}, \frac{q^d-1}{q-1}, q^{d(e-1)}, q^{d(e-2)}(q-1)\right)$$

relative difference set in $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ relative to $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$. We state the following theorem of Gordon, Mills and Welch.

Theorem 2.2 (**[8]**). *If Δ is any $\left(\frac{q^d-1}{q-1}, q^{d-1}, q^{d-2}(q-1)\right)$ difference set in $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$, then $D = \Delta R$ is a $\left(\frac{q^m-1}{q-1}, q^{m-1}, q^{m-2}(q-1)\right)$ difference set in $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$, with the above definition of R. Moreover, if Δ' is another $\left(\frac{q^d-1}{q-1}, q^{d-1}, q^{d-2}(q-1)\right)$ difference set in $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$, then the two cyclic difference sets $D = \Delta R$ and $D' = \Delta' R$ are equivalent if and only if Δ' is a translate of Δ.*

In Theorem 2.2, if one uses the difference sets $L_1^{(r)} = \{x^r \mid x \in L_1\}$ as Δ, where $\gcd(r, \frac{q^d-1}{q-1}) = 1$, and L_1 is the same as in Theorem 2.1, then the resulting difference sets $D = L_1^{(r)} R$ are called *classical* GMW difference sets. If we assume furthermore that $q = 2$ so that $R = R' = \{x \in \mathbb{F}_{2^m} \mid \mathrm{Tr}_{2^m/2^d}(x) = 1\}$, then the characteristic sequence of $D = L_1^{(r)} R$ in $\mathbb{F}_{2^m}$ is given by $\{\mathrm{Tr}_{2^d/2}\left([\mathrm{Tr}_{2^m/2^d}(\alpha^i)]^{1/r}\right)\}_{0 \le i \le 2^m-2}$. This sequence is called a binary *GMW sequence* in **[16]**. The linear spans of GMW sequences (i.e., the 2-ranks of classical GMW difference sets with $q = 2$) are computed in **[16]**. Antweiler and Bömer **[1]** consider sequences defined over $\mathbb{F}_p$ in a way analogous to the definition of GMW sequences, and computed their linear spans. We

note that the sequences they considered apparently are different from the characteristic sequences of the GMW difference sets when $q \neq 2$ (cf. **[15]**, p. 84). It therefore remains a problem to compute the p-ranks of GMW difference sets for general p. We will solve this problem in Section 3.

We emphasize that in Theorem 2.2, the choice of the $\left(\frac{q^d-1}{q-1}, q^{d-1}, q^{d-2}(q-1)\right)$ difference set Δ in $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$ is completely arbitrary. When $q = 2$, and Δ is not of the form $L_1^{(r)}$ for any r relatively prime to $2^d - 1$, the characteristic sequences of the GMW difference sets ΔR are studied in **[14]** and **[6]**.

We now define the p-rank of a difference set. Let G be a (multiplicative) abelian group of order v, and let D be a (v, k, λ) difference set in G. Then $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is a (v, k, λ) symmetric design with a regular automorphism group G, where the set $\mathcal{P}$ of *points* of $\mathcal{D}$ is G, and where the set $\mathcal{B}$ of *blocks* of $\mathcal{D}$ is $\{gD \mid g \in G\}$. This design is usually called the *development* of D. The incidence matrix of $\mathcal{D}$ is the matrix A whose rows are indexed by the blocks B of $\mathcal{D}$ and whose columns are indexed by the points g of $\mathcal{D}$, where the entry $A_{B,g}$ in row B and column g is 1 if $g \in B$, and 0 otherwise.

The *p-ary code* of D, denoted $\mathcal{C}_p(D)$, is defined to be the row space of A over $\mathbb{F}_p$, the field of p elements. This code is also the p-ary code of $\mathcal{D}$, denoted by $\mathcal{C}_p(\mathcal{D})$. The $\mathbb{F}_p$-dimension of $\mathcal{C}_p(D)$ is usually called the *p-rank* of the difference set D. It is well known that $\mathcal{C}_p(D)$ is of interest only if $p \mid (k - \lambda)$ (see **[5]**). So from now on, we always assume that $p \mid (k - \lambda)$.

In our computation of p-ranks of the GMW difference sets, we will take the well known approach described by the following lemma.

Lemma 2.3. *Let G be an Abelian group of order v and exponent v^*, let p be a prime not dividing v^*, and let $\mathfrak{p}$ be a prime ideal above p in $\mathbb{Z}[\xi_{v^*}]$. Let D be a (v, k, λ) difference set in G. Then the p-rank of D is equal to the number of complex characters χ of G with $\chi(D) \not\equiv 0 \pmod{\mathfrak{p}}$*

For a proof of this lemma, we refer the reader to **[12]**, and (**[4]**, p. 465).

We will also need Stickelberger's result (Theorem 2.4 below) on the prime ideal factorization of Gauss sums. We first introduce some notation.

Let p be a prime, $q = p^s$, and let ξ_{q-1} be a complex primitive $(q-1)$th root of unity. Fix any prime ideal $\mathfrak{p}$ in $\mathbb{Z}[\xi_{q-1}]$ lying over p. Then $\mathbb{Z}[\xi_{q-1}]/\mathfrak{p}$ is a finite field of order q, which we identify with $\mathbb{F}_q$. Let $\omega_{\mathfrak{p}}$ be the Teichmüller character on $\mathbb{F}_q$, i.e., an isomorphism

$$\omega_{\mathfrak{p}} : \mathbb{F}_q^* \to \left\{1, \xi_{q-1}, \xi_{q-1}^2, \ldots, \xi_{q-1}^{q-2}\right\}$$

satisfying

$$\omega_{\mathfrak{p}}(\alpha) \pmod{\mathfrak{p}} = \alpha, \tag{4}$$

for all α in $\mathbb{F}_q^*$. The Teichmüller character $\omega_{\mathfrak{p}}$ has order $q - 1$; hence it generates all multiplicative characters of $\mathbb{F}_q$.

Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Z}[\xi_{q-1}, \xi_p]$ lying above $\mathfrak{p}$. For an integer a, let

$$s(a) = v_{\mathfrak{P}}(g(\omega_{\mathfrak{p}}^{-a})),$$

where $v_{\mathfrak{P}}$ is the $\mathfrak{P}$-adic valuation. Thus $\mathfrak{P}^{s(a)} \mid\mid g(\omega_{\mathfrak{p}}^{-a})$. The following evaluation of $s(a)$ is due to Stickelberger (see **[3]**, p. 344, **[19]**, p. 96).

Theorem 2.4. *Let p be a prime, and $q = p^s$. For an integer a not divisible by $q-1$, let $a_0 + a_1 p + a_2 p^2 + \cdots + a_{s-1} p^{s-1}$, $0 \le a_i \le p-1$, be the p-adic expansion of the reduction of a modulo $q-1$. Then*

$$s(a) = a_0 + a_1 + \cdots + a_{s-1},$$

that is, $s(a)$ is the sum of the p-adic digits of the reduction of a modulo $q-1$.

As an easy application of Stickelberger's theorem, we prove the following lemma.

Lemma 2.5. *Let $q = p^s$, and let $d > 2$ be an integer. For any integer a not divisible by $q^d - 1$, let $s(a)$ be the sum of p-adic digits of the reduction of a modulo $q^d - 1$. Then $s((q-1)b) \ge (p-1)s$, for all integers b, $0 < b < (q^d - 1)/(q-1)$.*

Proof. For $\mathfrak{p}$ a prime ideal in $\mathbb{Z}[\xi_{q^d-1}]$ lying over p, let $\omega_{\mathfrak{p}}$ be the Teichmüller character on $\mathbb{F}_{q^d}$ and let $\chi = \omega_{\mathfrak{p}}^{-(q-1)}$. Then χ is a generator of the character group of $\mathbb{F}_{q^d}^*/\mathbb{F}_q^*$. By (3), we know that for each b, $0 < b < \frac{q^d-1}{q-1}$,

$$q \cdot \chi^b(L_0) = g(\chi^b), \tag{5}$$

where L_0 is defined as in (2).

Let $\mathfrak{P}$ be the prime ideal of $\mathbb{Z}[\xi_{q^d-1}, \xi_p]$ lying above $\mathfrak{p}$. By Theorem 2.4, we have

$$\mathfrak{P}^{s((q-1)b)} \mid\mid g(\chi^b).$$

Also it is clear that $\mathfrak{P}^{(p-1)s} \mid\mid q$. Since $\chi^b(L_0)$ is an algebraic integer, we see from (5) that $s((q-1)b) \ge (p-1)s$. This completes the proof. □

Remark. This lemma can of course be proven in an elementary way. We give the above proof to show application of Theorem 2.4. We will later prove a strengthening of Lemma 2.5 in a completely elementary manner in Section 3.

As a final preparation, we calculate the character value of the set R defined before the statement of Theorem 2.2. We note that this calculation is essentially an Eisenstein sum computation (**[3]**, p. 389, 400) (see also **[22]**, **[21]**).

We first recall the definition of R. Let $m = d \cdot e$, where $d > 2$, $e > 1$ are integers, $R' = \{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{q^m/q^d}(x) = 1\}$, here Tr_{q^m/q^d} is the trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^d}$. Let $\mu : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ be the canonical epimorphism. As before, we define $R = \mu(R')$. Let χ be a nontrivial character of $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$. Our goal here is to compute $\chi(R) := \sum_{x \in R} \chi(x)$.

Since $R = \mu(R')$, we see that $\chi(R) = \chi \circ \mu(R')$. Let $\eta = \chi \circ \mu$. Then η is a multiplicative character of $\mathbb{F}_{q^m}^*$, whose restriction to $\mathbb{F}_q^*$ is trivial.

By the definition of Gauss sums over $\mathbb{F}_{q^m}$, we have

$$g(\eta) = \sum_{y \in \mathbb{F}_{q^m}^*} \eta(y)\, \xi_p^{\mathrm{Tr}_{q^m/p}(y)}.$$

Let L' be a system of coset representatives of $\mathbb{F}_{q^d}^*$ in $\mathbb{F}_{q^m}^*$ such that $\{\mathrm{Tr}_{q^m/q^d}(x) \mid x \in L'\} = \{0, 1\}$. Define $L_0' = \{x \in L' \mid \mathrm{Tr}_{q^m/q^d}(x) = 0\}$, and $L_1' = \{x \in L' \mid \mathrm{Tr}_{q^m/q^d}(x) = 1\}$. Then

$$\begin{aligned} g(\eta) &= \sum_{x \in L'} \eta(x) \sum_{a \in \mathbb{F}_{q^d}^*} \eta(a)\, \xi_p^{\mathrm{Tr}_{q^d/p}\left(a\mathrm{Tr}_{q^m/q^d}(x)\right)} \\ &= \sum_{x \in L_0'} \eta(x) \sum_{a \in \mathbb{F}_{q^d}^*} \eta(a) + \sum_{x \in L_1'} \eta(x) \sum_{a \in \mathbb{F}_{q^d}^*} \eta(a)\, \xi_p^{\mathrm{Tr}_{q^d/p}(a)} \end{aligned}$$

Therefore, if $\eta\big|_{\mathbb{F}_{q^d}^*} = 1$, then

$$g(\eta) = -q^d\, \eta(L_1');$$

and if $\eta\big|_{\mathbb{F}_{q^d}^*} \neq 1$, then $\sum_{a \in \mathbb{F}_{q^d}^*} \eta(a) = 0$, hence

$$g(\eta) = \eta(L_1') \cdot g_1(\eta_1),$$

where $\eta_1 = \eta\big|_{\mathbb{F}_{q^d}^*}$ (the restriction of η to $\mathbb{F}_{q^d}$), and $g_1(\eta_1)$ is the Gauss sum over $\mathbb{F}_{q^d}$ with respect to the character η_1.

Noting that $L_1' = R'$, we have

$$\eta(R') = \chi(R) = \begin{cases} -\frac{1}{q^d}\, g(\eta)\,, & \text{if} \quad \eta\big|_{\mathbb{F}_{q^d}^*} = 1\,, \\ \frac{g(\eta)}{g_1(\eta_1)}\,, & \text{if} \quad \eta\big|_{\mathbb{F}_{q^d}^*} \neq 1\,. \end{cases} \tag{6}$$

We will use this evaluation of $\chi(R)$ in later sections.

3. The p-ranks of the classical GMW difference sets

Let $m = d \cdot e$, where $d > 2, e > 1$ are integers. Let R be defined as in Section 2. Let L_1 be defined as in (2.1), and let r be an integer such that $\gcd\left(r, \frac{q^d-1}{q-1}\right) = 1$. Then Theorem 2.2 tells us that the set $D := L_1^{(r)} R$ is a $\left(\frac{q^m-1}{q-1}, q^{m-1}, q^{m-2}(q-1)\right)$ difference set in $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$, and such a difference set is called a classical GMW difference

set. In this section, we compute the p-ranks of the classical GMW difference sets. We will maintain the notation in Section 2.

We begin with a lemma which reduces the computation of p-ranks of the classical GMW difference sets to a combinatorial counting problem.

Lemma 3.1. *Let $D = L_1^{(r)} R$ be the difference set in $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ defined above. Let $q = p^s$, where p is a prime. Then the p-rank of D is equal to the cardinality of the set*

$$\mathcal{B} = \Big\{ a \mid 0 < a < \frac{q^m-1}{q-1},\ (q^d-1) \nmid (q-1)a\,, \\ s_1(a(q-1)r) + s((q-1)a) - s_1((q-1)a) = (p-1)s \Big\},$$

where $s(x)$ is the sum of the p-adic digits of the reduction of x modulo q^m-1, and $s_1(x)$ is the sum of the p-adic digits of the reduction of x modulo q^d-1.

Proof. For $\mathfrak{P}$ a prime ideal in $\mathbb{Z}[\xi_{q^m-1}]$ lying over p, let $\omega_{\mathfrak{P}}$ be the Teichmüller character on $\mathbb{F}_{q^m}$. Then $\omega_{\mathfrak{P}}^{-(q-1)}$ is a generator of the character group of $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$, hence any nontrivial character of $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ takes the form $\omega_{\mathfrak{P}}^{-a(q-1)}$, $0 < a < \frac{q^m-1}{q-1}$.

So let $\chi = \omega_{\mathfrak{P}}^{-a(q-1)}$ be an arbitrary nontrivial character of $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$, where $0 < a < \frac{q^m-1}{q-1}$. Let $\eta = \chi \circ \mu$, where $\mu : \mathbb{F}_{q^m}^* \to \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ is the natural epimorphism. Since χ is trivial on $\mathbb{F}_q^*$, we have

$$\eta(x) = \chi \circ \mu(x) = \chi(\bar{x}) = \chi(x)\,,$$

for any $x \in \mathbb{F}_{q^m}^*$.

We now compute the character value $\chi(D) := \sum_{x \in D} \chi(x)$. The computations are naturally divided into two cases.

Case 1. $\chi\big|_{\mathbb{F}_{q^d}^*} = 1$. By (6), we have

$$\begin{aligned} \chi(D) &= \chi\big|_{\mathbb{F}_{q^d}^*}(L_1^{(r)}) \cdot \chi(R) \\ &= -\frac{1}{q}\, g(\chi) \end{aligned}$$

Case 2. $\chi\big|_{\mathbb{F}_{q^d}^*} \neq 1$. Using the character value of L_1 and (6), we see that

$$\begin{aligned} \chi(D) &= \chi\big|_{\mathbb{F}_{q^d}^*}\big(L_1^{(r)}\big) \cdot \chi(R) \\ &= -\frac{1}{q}\, g_1\big(\omega_{\mathfrak{p}}^{-a(q-1)r}\big) \cdot \frac{g\big(\omega_{\mathfrak{P}}^{-(q-1)a}\big)}{g_1\big(\omega_{\mathfrak{p}}^{-(q-1)a}\big)}\,, \end{aligned}$$

where $g_1(\phi)$ is the Gauss sum over $\mathbb{F}_{q^d}$ with respect to the multiplicative character ϕ of $\mathbb{F}_{q^d}$. Note that here we have used the fact that $\omega_{\mathfrak{P}}\big|_{\mathbb{F}^*_{q^d}} = \omega_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal in $\mathbb{Z}[\xi_{q^d-1}]$ lying above p. To simplify notation, in what follows, we will omit the index $\mathfrak{P}$ in the character $\omega_{\mathfrak{P}}$ if there is no confusion.

By Lemma 2.3, the p-rank of D is equal to the number of χ, where $\chi = \omega^{-a(q-1)}$, $0 < a < (q^m-1)/(q-1)$, such that $\chi(D) \pmod{\mathfrak{P}} \neq 0$. Let $\tilde{\mathfrak{P}}$ be the prime of $\mathbb{Z}[\xi_{q^m-1}, \xi_p]$ lying above $\mathfrak{P}$. Since $\tilde{\mathfrak{P}} \mid \chi(D)$ if and only if $\mathfrak{P} \mid \chi(D)$, the p-rank of D is equal to the number of χ such that $\tilde{\mathfrak{P}} \nmid \chi(D)$.

Corresponding to the above two cases, we have the following.

Case 1′. $\omega^{-a(q-1)}\big|_{\mathbb{F}^*_{q^d}} = 1$ (i.e., $(q^d-1) \mid (q-1)a$). By the computation in Case 1, we have

$$\omega^{-a(q-1)}(D) = -\frac{1}{p^s}\, g(\omega^{-(q-1)a}).$$

By Theorem 2.4, we have

$$v_{\tilde{\mathfrak{P}}}(g(\omega^{-(q-1)a})) = s((q-1)a),$$

where $s(x)$ is the p-ary weight of $x \pmod{q^m-1}$.

Also it is clear that

$$v_{\tilde{\mathfrak{P}}}(p^s) = (p-1)s.$$

Therefore in this case, the number of a, $0 < a < \frac{q^m-1}{q-1}$, such that

$$\omega^{-a(q-1)}(D) \not\equiv 0 \pmod{\tilde{\mathfrak{P}}},$$

is equal to

$$\#\Big\{a \mid 0 < a < \frac{q^m-1}{q-1},\ (q^d-1) \mid (q-1)a,\ s((q-1)a) = (p-1)s\Big\}.$$

Let us denote this cardinality by A. We will show that $A = 0$ later on.

Case 2′. $\omega^{-a(q-1)}\big|_{\mathbb{F}^*_{q^d}} \neq 1$ (i.e., $(q^d-1) \nmid (q-1)a$). By our computation in Case 2, we have

$$\omega^{-a(q-1)}(D) = -\frac{1}{q}\, g_1\big(\omega_{\mathfrak{p}}^{-a(q-1)r}\big)\, \frac{g\big(\omega_{\mathfrak{P}}^{-(q-1)a}\big)}{g_1\big(\omega_{\mathfrak{p}}^{-(q-1)a}\big)}.$$

So in this case the number of a, $0 < a < \frac{q^m-1}{q-1}$, such that

$$\omega^{-a(q-1)}(D) \not\equiv 0 \pmod{\tilde{\mathfrak{P}}},$$

is equal to

$$\#\Big\{a \mid 0 < a < \frac{q^m-1}{q-1},\ (q^d-1) \nmid (q-1)a\,,\\ s_1(a(q-1)r) + s((q-1)a) - s_1((q-1)a) = (p-1)s\Big\}$$

where $s_1(x)$ is the p-ary weight of $x \pmod{q^d-1}$. Let us denote this cardinality by B.

We now prove that $A = 0$. Set $x = (q-1)a$, we need to count the number of x, $0 < x < q^m - 1$, $(q^d-1) \mid x$, $s(x) = (p-1)s$. Since $(q^d-1) \mid x$, $q = p^s$, we may write $x = (p^{sd}-1)b$ for some integer b. Since $d > 2$, by Lemma 2.5, we have

$$s((p^{sd}-1)b) \geq (p-1)sd > (p-1)s.$$

So it is impossible to have $s(x) = (p-1)s$. Hence $A = 0$. This shows that Case $1'$ does not contribute to the p-rank of D at all, therefore the p-rank of D is equal to B, the cardinality of the set defined in the statement of the lemma. The proof is now complete. □

We now proceed to solve the counting problem. First we prove two lemmas.

Lemma 3.2. *Let $q = p^s$ be a prime power, $m = de$, where $d > 2$, and $e > 1$ are integers. Let X be an integer not divisible by $q^d - 1$, $0 < X < q^m - 1$, and let $s(X)$, $s_1(X)$ be the p-weight of the reduction of X modulo $q^m - 1$ and $q^d - 1$ respectively. Then*

$$s(X) - s_1(X) = (p-1)\alpha,$$

for some integer $\alpha \geq 0$.

Proof. We write

$$X = \sum_{i=0}^{e-1} X_i q^{di},$$

where

$$X_i = \sum_{j=0}^{ds-1} X_{ij} p^j$$

with $0 \leq X_{ij} \leq p-1$.

We will use $x = \sum_{j=0}^{ds-1} x_j p^j$, $0 \leq x_j \leq p-1$, to denote the reduction of $X \pmod{q^d-1}$. So $0 \leq x \leq q^d - 1$ and $x \equiv X \bmod q^d - 1$. By add-with-carry

algorithm, there are nonnegative carries c_j, $j = 0, 1, \ldots, ds - 1$ such that

$$pc_j + x_j = \sum_{i=0}^{e-1} X_{ij} + c_{j-1},$$

holds for all $j = 0, 1, \ldots, ds - 1$. Here $c_{-1} = c_{ds-1}$. This implies that

$$(p-1)\sum_j c_j + \sum_j x_j = \sum_j \sum_i X_{ij},$$

that is, $(p-1)\alpha + s_1(X) = s(X)$, where $\alpha = \sum_j c_j$. □

We now give a completely elementary proof of Lemma 2.5. In fact, we will prove a strengthening of the lemma. We first introduce some notation.

Let $b \geq 2$ be any integer. Define $\mathbb{Z}_{\geq 0} = \{0, 1, \ldots\}$. For any index set $I \subseteq \mathbb{Z}_{\geq 0}$, let $\mathcal{R}(I)$ be the collection of all sequences $x = (x_i)_{i \in I}$ with x_i nonnegative integer for all $i \in I$ and $x_i = 0$ for all but finitely many i. For convenience, we define $0 \in \mathcal{R}(I)$ as the sequence x with $x_i = 0$ for all $i \in I$. Also, we write $\mathcal{R}$ and $\mathcal{R}_m$ to denote $\mathcal{R}(\mathbb{Z}_{\geq 0})$ and $\mathcal{R}(\{0, 1, \ldots, m-1\})$, respectively. For each $x \in \mathcal{R}(I)$, we associate its *numerical value*

$$\nu(x) = \sum_{i \in I} x_i b^i$$

and its b-ary *weight*

$$s_b(x) = \sum_{i \in I} x_i.$$

Note that if $I = \mathbb{Z}_{\geq 0} = \{0, 1, \ldots\}$ and the x_i are the b-ary digits of a number, then the numerical value of the sequence is just the number itself and the weight of the sequence is just the weight of the number. With these definitions, we have the following.

Lemma 3.3. *Let $x \in \mathcal{R} \setminus \{0\}$ satisfy $(b^s - 1) \mid \nu(x)$ for some integer $s \geq 1$. Then*

$$s_b(x) \geq (b-1)s,$$

with equality if and only if

$$\sum_{i \equiv r \pmod{s}} x_i = b - 1 \tag{7}$$

for $r = 0, 1, \ldots, s-1$. Conversely, if (7) holds, then $(b^s - 1) \mid \nu(x)$ and $s_b(x) = (b-1)s$.

Proof. Let $x = (x_i)_{i \geq 0} \in \mathcal{R} \setminus \{0\}$ satisfy the assumptions in the lemma. For $i = 0, \ldots, s-1$, write

$$x_{i,j} = x_{i+js}$$

for all $j \geq 0$ and define

$$y_i = \sum_{j \geq 0} x_{i,j}.$$

We consider $y = (y_0, \ldots, y_{s-1})$ as a member of $\mathcal{R}_s$. Note that

$$s_b(x) = \sum_{i=0}^{s-1} y_i = s_b(y). \tag{8}$$

Now modulo $b^s - 1$ we have that

$$\begin{aligned} 0 &\equiv \nu(x) \\ &= \sum_{i=0}^{s-1} \sum_{j \geq 0} x_{i,j} b^i b^{js} \\ &\equiv \sum_{i=0}^{s-1} \sum_{j \geq 0} x_{i,j} b^i \\ &= \sum_{i=0}^{s-1} y_i b^i \\ &= \nu(y) \pmod{b^s - 1}. \end{aligned}$$

For each $i = 0, 1, \ldots, s-1$ (considered modulo s), we define the transformation τ_i on sequences z from $\mathcal{R}_s$ with $z_i \geq b$ as follows. The image $z' = \tau_i(z)$ will have $z'_k = z_k$ for $k \neq i, i+1$; $z'_i = z_i - b$, and $z'_{i+1} = z_{i+1} + 1$. Note that we have that $\tau_i(z) \in \mathcal{R}_s \setminus \{0\}$, $s_b(\tau_i(z)) = s_b(z) - (b-1) < s_b(z)$, and

$$\nu(\tau_i(z)) = \begin{cases} \nu(z), & \text{if } i \neq s-1; \\ \nu(z) - (b^s - 1), & \text{if } i = s-1. \end{cases}$$

In particular, we have that $\nu(\tau_i(z)) \equiv \nu(z) \mod b^s - 1$. Now, repeatedly apply transformations τ_i to the sequence $y = (y_j)_{0 \leq j \leq s-1}$ until we obtain a sequence $y' = (y'_0, y'_1, \ldots y'_{s-1})$, where $y'_i \leq b-1$ for all $i = 0, 1, \ldots, m-1$. By the above remarks, we have that $\nu(y') \equiv \nu(y) \equiv 0 \pmod{b^s - 1}$, $y' \neq 0$, and

$$s_b(y') \leq s_b(y)$$

with equality if and only if $y_i \leq b-1$ for all i. To finish the proof, it suffices to remark that we may consider the sequence y' as the b-ary representation of the number $\nu(y')$; so $0 < \nu(y') \leq b^s - 1$ and hence $\nu(y') \equiv 0 \pmod{b^s - 1}$ implies that $y'_i = b-1$ for all i.

The converse in the lemma is evident: indeed, if the condition in the lemma holds, that is, if $y_i = b-1$ for each $i = 0, \ldots, s-1$, then $\nu(x) \equiv \nu(y) = b^s - 1 \equiv 0 \mod b^s - 1$ and $s_b(x) = s_b(y) = (b-1)s$. □

Remarks. (1) In fact, from the proof of Lemma 3.3 we see the following: if $0 < \nu(x) \equiv \nu(z) \bmod b^s - 1$ with $0 \neq z = (z_0, z_1, \ldots, z_{s-1}, 0, 0, \ldots)$ and $0 \leq z_i \leq b-1$ for all i, then we have that

$$s_b(x) \geq s_b(z)$$

with equality if and only if

$$\sum_{i \equiv r \pmod{s}} x_i = z_i$$

for all $i = 0, \ldots, s-1$. (The lemma is simply the case where $z = (b-1, b-1, \ldots, b-1, 0, 0, \ldots)$ so that $\nu(z) = b^s - 1 \equiv 0 \mod b^s - 1$.)

(2) As a consequence of this lemma, we see that if $(b^s - 1) \mid x$ and $s_b(x) = (b-1)s$, then certainly $(b^t - 1) \nmid x$ for $t > s$.

Using the notation introduced at the beginning of this section, we now have the following.

Theorem 3.4. *Let $q = p^s$, p a prime, let $m = de$, where $d > 2$, $e > 1$ are integers. Let r be an integer relatively prime to $\frac{q^d-1}{q-1}$. Then the p-rank of the difference set $D = L_1^{(r)} R$ is equal to*

$$\sum_x \prod_{j=0}^{ds-1} \binom{x_j + e - 1}{e - 1},$$

where the sum is over all $x = \sum_{j=0}^{ds-1} x_j p^j$, $0 \leq x_j \leq p-1$, such that the number $y \equiv rx \pmod{q^d - 1}$ has the form

$$y = \sum_{i=0}^{s-1} \sum_{j=0}^{d-1} y_{ij} p^i q^j$$

with $0 \leq y_{ij} \leq p-1$ and

$$\sum_{j=0}^{d-1} y_{ij} = p - 1$$

for $i = 0, \ldots, s-1$.

Proof. By Lemma 3.1, the p-rank of D is equal to B, the cardinality of the following set

$$\mathcal{B} = \{X \mid 0 < X < q^m - 1,\ (q-1) \mid X,\ (q^d - 1) \nmid X,\ s_1(Xr) + s(X) - s_1(X) = (p-1)s\},$$

where $s_1(X)$ is the p-weight of $X \pmod{q^d - 1}$.

Let $X \in \mathcal{B}$. By Lemma 3.2, we see that $s(X) - s_1(X) \geq 0$, hence $s_1(Xr) \leq (p-1)s$. Since $(q-1) \mid X$ and $X \mid Xr$, by Lemma 3.3, we have either $Xr \equiv 0 \mod q^d - 1$, or $s_1(Xr) = (p-1)s$. In the latter case, Xr is of a special form as specified in Lemma 3.3.

Let us first show that $Xr \equiv 0 \mod q^d - 1$ is impossible. Indeed, in that case we have $rX = c(q^d - 1)$, for some integer c. So with $X' = X/(q-1)$, which is an integer by our assumption on X, we have that $rX' = c(q^d - 1)/(q-1)$, that is, $rX' \equiv 0 \mod (q^d - 1)/(q-1)$. So by our assumption on r, this implies $X' \equiv 0 \mod (q^d - 1)/(q-1)$, and that implies $X \equiv 0 \bmod q^d - 1$, contradicting the assumption that $(q^d - 1) \nmid X$.

So we must have $s_1(Xr) = (p-1)s$ (with Xr of a special form). Hence $s(X) = s_1(X)$. Let x denote the integer in the range $[0, q^d - 1)$ such that $x \equiv X \mod q^d - 1$. Then $s(X) = s_1(x)$. Therefore in order compute the cardinality of $\mathcal{B}$, we must count, for each x, $0 < x < q^d - 1$, with $s_1(xr) = (p-1)s$, the number of $X \in \mathcal{B}$ such that $X \equiv x \mod q^d - 1$ and $s(X) = s_1(x)$.

We will use the same notation as in Lemma 3.2, i.e., $X = \sum_{i=0}^{e-1} X_i q^{di}$, $X_i = \sum_{j=0}^{ds-1} X_{ij} p^j$, with $0 \leq X_{ij} \leq p-1$. Given an $x = \sum_{j=0}^{ds-1} x_j p^j$, $0 \leq x_j \leq p-1$, since we want to count those $X \in \mathcal{B}$ such that $X \equiv x \mod q^d - 1$, and $s(X) = s_1(x)$, we require that

$$x_j = \sum_{i=0}^{e-1} X_{ij},$$

that is, the addition $X_0 + X_1 + \cdots + X_{e-1} \pmod{q^d - 1}$ has no carry. As before, given an x_j, there are precisely

$$\binom{x_j + e - 1}{e - 1}$$

ways to distribute the quantity x_j over the X_{ij}'s. So for each x, $0 < x < q^d - 1$, with $s_1(xr) = (p-1)s$, the number of "liftings" $X \in \mathcal{B}$ of x is $\prod_{j=0}^{ds-1} \binom{x_j+e-1}{e-1}$. Summing over these x, we get the desired formula for the p-rank of D. □

Example 3.5. We use a concrete example to illustrate the p-rank formula in Theorem 3.4. Let us take $p = 3$, $s = 1$, $d = 3$, $e = 2$, so $m = de = 6$. Let $r \equiv 1/5 \pmod{3^3 - 1}$. We have 6 choices for $y \equiv x/5 \pmod{3^3 - 1}$ such that $s_1(y) = p - 1 = 2$. Therefore we have 6 choices for x. These are $x \equiv 1 + 3^2, 1 + 3, 3 + 3^2, 2 + 2 \cdot 3, 2 \cdot 3 + 2 \cdot 3^2, 2 + 2 \cdot 3^2 \pmod{3^3 - 1}$. By Theorem 3.4, the 3-rank of $D = L_1^{(1/5)} R$ is

$$3 \cdot \binom{1+e-1}{1} \cdot \binom{0+e-1}{1} \cdot \binom{1+e-1}{1} + 3 \cdot \binom{2+e-1}{1} \cdot \binom{2+e-1}{1} \cdot \binom{0+e-1}{1} = 39.$$

This agrees with the result in the table on page 86 of **[15]**.

In some special cases, the p-rank formula in Theorem 3.4 can be made more explicit.

Corollary 3.6. *Let $D = L_1^{(r)}R$, with $r = 1$ (or a power of p). Then the p-rank of D is $\binom{p+de-2}{de-1}^s$.*

Proof. Since $r = 1$, we have $rx = x$. By Theorem 3.4, the p-rank of D is

$$\sum_x \prod_{j=0}^{ds-1} \binom{x_j + e - 1}{e-1},$$

where the sum is over all $x = \sum_{j=0}^{ds-1} x_j p^j$, $0 \le x_j \le p-1$, with

$$x_i + x_{i+s} + x_{i+2s} + \cdots + x_{i+(d-1)s} = p - 1,$$

for $i = 0, 1, \ldots, s-1$.

The above sum is easily seen to be

$$\Big[\sum_{\substack{z_0+\cdots+z_{d-1}=p-1 \\ 0\le z_i<p}} \prod_{i=0}^{d-1} \binom{z_i + e - 1}{z_i}\Big]^s = \binom{p+de-2}{de-1}^s,$$

where the last equality is obtained by comparing coefficients of x^{p-1} in $(1-x)^{-m} = ((1-x)^{-e})^d$. This completes the proof. □

Corollary 3.6 is of course well-known, since $D = L_1 R$ is nothing but a Singer difference set.

Corollary 3.7. *Let $q = p = 2$, and $D = L_1^{(r)}R$ with $\gcd(r, 2^d - 1) = 1$. Then the 2-rank of D is $d \cdot e^{s_1(1/r)}$.*

Proof. Since $p = 2$, a solution to $s_1(rx) = p - 1 = 1$ must satisfy $rx \equiv 2^i \pmod{2^d - 1}$ for some i. Therefore $x \equiv r^{-1}2^i \pmod{2^d - 1}$. So the 2-adic expansion of $x = \sum_{j=0}^{d-1} x_j 2^j \pmod{2^d - 1}$ is just a shift of the 2-adic expansion of r^{-1}. Note that each x_j is 0 or 1, and the number of $x_j = 1$ is the binary weight $s_1(1/r)$ of $1/r \pmod{2^d - 1}$. Therefore the 2-rank of D is

$$\sum_{x_j} \prod_{i=0}^{d-1} \binom{x_j + e - 1}{x_j} = d \cdot e^{s_1(1/r)}.$$

This completes the proof. □

Corollary 3.7 was first proved by Scholtz and Welch **[16]** in terms of linear span of GMW sequences. The method they used to obtain this rank formula is completely different from ours.

Corollary 3.8. *Let $q = p$ be a prime, and $D = L_1^{(-1)}R$ (i.e., $s = 1$ and $r = -1$ in Theorem* 3.4). *Then the p-rank of D is equal to the coefficient of $x^{(p-1)(d-1)}$ in the expansion of $\left(\sum_{t=0}^{p-1}\binom{t+e-1}{e-1}x^t\right)^d$.*

Proof. We will use the same notation as in the statement of Theorem 3.4. Since $s = 1$ and $r = -1$, we have $x \equiv -y \bmod p^d - 1$, where $y = \sum_{j=0}^{d-1} y_j p^j$, and $\sum_j y_j = (p-1)$, $0 \le y_j \le (p-1)$. So in proper p-adic expansion, we have $x = \sum_{j=0}^{d-1} x_j p^j$, with $x_j = p - 1 - y_j$. By Theorem 3.4, the p-rank of D is

$$\sum_{\substack{x_0+x_1+\cdots+x_{d-1}=(p-1)(d-1)\\ 0\le x_j<p}} \prod_{j=0}^{d-1}\binom{x_j+e-1}{x_j},$$

which is the coefficient of $x^{(p-1)(d-1)}$ in the expansion of $\left(\sum_{t=0}^{p-1}\binom{t+e-1}{e-1}x^t\right)^d$. This completes the proof. □

4. The 2-ranks of some non-classical GMW difference sets

In this section, we will compute the 2-ranks of some non-classical GMW difference sets. By non-classical GMW difference sets, we mean that in the GMW construction (cf. Theorem 2.2), we choose $\Delta \ne L_1^{(r)}$, for any r relatively prime to $\frac{q^d-1}{q-1}$, where L_1 is defined in (2.1). In general, it is difficult to get *explicit* formulas for the p-ranks of non-classical GMW difference sets. In this section, we consider the case in which Δ is chosen to be equivalent to a difference set constructed from monomial hyperovals.

In **[13]**, Maschietti constructed some $(2^d - 1, 2^{d-1} - 1, 2^{d-2} - 1)$ difference sets from monomial hyperovals. His construction can be stated as follows.

Theorem 4.1. *Let $q = 2^d$, and let $f : \mathbb{F}_q \to \mathbb{F}_q$, $f(x) = x + x^h$, be a two-to-one map, where* $\gcd(h, q-1) = 1$. *Then the set $D_{d,h} = \mathrm{Im}(f)\setminus\{0\}$ is a $(q-1, q/2-1, q/4-1)$ difference set in $\mathbb{F}_q^*$. Here* $\mathrm{Im}(f)$ *stands for $\{f(x) \mid x \in \mathbb{F}_q\}$.*

The two-to-one map in the above theorem comes from monomial hyperovals

$$D(x^h) = \{(1, t, t^h) \mid t \in \mathbb{F}_{2^d}\} \cup \{(0, 0, 1), (0, 1, 0)\},$$

where h necessarily satisfies $\gcd(h, q-1) = \gcd(h-1, q-1) = 1$. (See Lemma 2.4 in **[7]**.) The known monomial hyperovals include the regular, translation, Segre,

Glynn type (I), and Glynn type (II) hyperovals (see **[7]**). It is easy to show that the regular and translation hyperovals give rise to Singer difference sets via the Maschietti construction. In **[7]**, the 2-ranks of the difference sets from the Segre and Glynn hyperovals are computed, and it is shown that these difference sets are inequivalent to previously known ones.

Let $\overline{D_{d,h}}$ be the complement of $D_{d,h}$ in $\mathbb{F}_{2^d}^*$. Then $\overline{D_{d,h}}$ is a difference set in $\mathbb{F}_{2^d}^*$ with parameters

$$v = 2^d - 1, k = 2^{d-1}, \lambda = 2^{d-2}.$$

In the GMW construction (see Theorem 2.2), if we choose $\Delta = \overline{D_{d,h}}^{(r)}$, where $\gcd(r, 2^d - 1) = 1$, what is the 2-rank of the resulting difference set $D = \Delta \cdot R$? Questions like this were raised in **[10]** (see also **[4]**, p. 461). We will investigate this problem in this section.

We note that the character values of $\overline{D_{d,h}}$ were computed in **[7]**, they are related to Jacobi sums. So as we did in the previous section, we may reduce the 2-rank computations of these difference sets to a counting problem also.

Lemma 4.2. *Let $D = \overline{D_{d,h}}^{(r)} R$ be the difference set in $\mathbb{F}_{2^m}^*$ defined above, where $\gcd(r, 2^d - 1) = 1$. Then the 2-rank of D is equal to the cardinality of the set*

$$\{a \mid 0 < a < 2^m - 1,\ (2^d - 1) \nmid a\,,\\ s(a) - s_1(a) + s_1(ar) + s_1(ar/(h-1)) - s_1(har/(h-1)) = 1\},$$

where $s(x)$ is the sum of the 2-adic digits of the reduction of x modulo $2^m - 1$, and $s_1(x)$ is the sum of the 2-adic digits of the reduction of x modulo $2^d - 1$.

Proof. The proof is similar to that of Lemma 3.1. (Actually, it is easier because $q = 2$.) For $\mathfrak{P}$ a prime ideal in $\mathbb{Z}[\xi_{2^m-1}]$ lying over 2, let $\omega_{\mathfrak{P}}$ be the Teichmüller character on $\mathbb{F}_{2^m}$. Then $\omega_{\mathfrak{P}}^{-1}$ is a generator of the character group of $\mathbb{F}_{2^m}^*$, hence any nontrivial character of $\mathbb{F}_{2^m}^*$ takes the form $\omega_{\mathfrak{P}}^{-a}$, $0 < a < 2^m - 1$.

So let $\chi = \omega_{\mathfrak{P}}^{-a}$ be an arbitrary nontrivial character of $\mathbb{F}_{2^m}^*$, where $0 < a < 2^m - 1$. We now compute the character value $\chi(D)$ of D. The computations are naturally divided into two cases.

Case 1. $\chi\big|_{\mathbb{F}_{2^d}^*} = 1$. By (6), we have

$$\begin{aligned}\chi(D) &= \chi\big|_{\mathbb{F}_{2^d}^*}(\overline{D_{d,h}}^{(r)}) \cdot \chi(R)\\ &= -\frac{1}{2}\, g(\chi)\end{aligned}$$

Case 2. $\chi\big|_{\mathbb{F}_{2^d}^*} \neq 1$. Recalling the character value of $\overline{D_{d,h}}$ from **[7]**, we have

$$\chi(\overline{D_{d,h}}) = \frac{1}{2} J\big(\omega_{\mathfrak{p}}^{-a}, \omega_{\mathfrak{p}}^{-a/(h-1)}\big),$$