Erciyes Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
Cilt 39, Sayı 2, 2023

Erciyes University
Journal of Institute of Science and Technology
Volume 39, Issue 2, 2023

Difference Sets from Quadratic Residues

Emek Demirci Akarsu[*1], **Yasin Yılmaz**[*2]

[*1] Recep Tayyip Erdoğan Üniversitesi Fen Edebiyat Fakültesi Matematik, RİZE
[*2] Recep Tayyip Erdoğan Üniversitesi Fen Edebiyat Fakültesi Matematik, RİZE

(Alınış / Received: 10.05.2023, Kabul / Accepted: 16.08.2023, Online Yayınlanma / Published Online: 31.08.2023)

Keywords
Difference sets,
Quadratic residues,
QRCM Algorithm

Abstract: Difference sets are significant algebraic objects that intersect a collection of sub-areas of mathematics, such as field theory, combinatorics, number theory, and coding theory. They also have lots of application areas in other fields. The essential part of the subject is how to construct difference sets. This article proposes a new method, i.e., the Quadratic Residue Classes Method (QRCM), which produces difference sets by quadratic residue classes, and applies it to fields. The results show that QRCM successfully determines whether the quadratic residue class for a field is a difference set.

Kuadratik Rezidülerden Fark Kümesi Elde Etme

Anahtar Kelimeler
Fark Kümeleri,
Kuadratik Rezidüler,
QRCM Algoritması

Öz: Fark kümeleri cisim teorisi, kombinatorik, sayılar teorisi ve kodlama teorisi gibi matematiğin alt alanlarıyla kesişen önemli cebirsel ifadelerdir. Diğer alanlarda da birçok uygulama alanına sahiptirler. Fark kümelerinin nasıl oluşturulacağı konunun en önemli kısmıdır. Bu makale, kuadratik sınıflar tarafından fark kümeleri üreten ve bunu cisimlere uygulayan yeni bir yöntem, yani Kuadratik Rezidü Sınıfları Yöntemi (QRCM)ni önermektedir. Sonuçlar, QRCM'nin bir cisim için ikinci dereceden kuadratik rezidü sınıflarının bir fark kümesi olup olmadığını başarıyla belirlediğini göstermektedir.

*Corresponding Author, email: emek.akarsu@erdogan.edu.tr

1. Introduction

The concept of difference sets, a particular case of symmetric design, was first proposed by Singer in 1938 [1]. Later in 1940, Hall enriched the work on difference sets. As a result of the studies on the difference sets, the subject is branched into families of difference sets, such as almost difference sets, partial difference sets, etc. [2-5]. Since it is divided into branches and can be integrated into numerous application areas, coding and encryption, and interpretation of astronomical events [6], it has been a source of interest for many scientists until today.

Difference sets are a combinatorial structure in plenty of applications. Godsil and Roy [7] mentioned that the difference sets were used in quantum computing. In addition, Assmus and Key [8] examined the analysis applications of design on algebraic coding. For a difference set to exist, that structure must have a symmetrical design. On this symmetrical design entity, Bruck and Ryser proved the Bruck-Ryser - Chowla Theorem for symmetrical design with parameters $(v, k,)$ [10]. This theorem, which was first proven for $\neq 1$, was later generalized for the case of positive numbers [11]. The first author also discusses the problem of difference sets and symmetric designs [10, 11]. The relation between quadratic residues and difference sets goes back to Lehmer [14, 15]. She proved that the class formed by quadratic residues on a field was a difference set. On top of these studies, McFarland showed that there was a family of difference sets on nonresidue classes too [16, 17]. Families of difference sets and for more details, see [18].

It is also known that difference sets have a good auto-correlation property. Explaining the formal duality of the Kerdock and Preparata codes is one of the outstanding results in applied algebra in the last few years [9]. The finding of several sets of four-phase sequences on $\mathbb{Z}_4$ with correlation qualities better than the best binary sequences is connected to this outcome. Furthermore, certain sets in cyclic groups' difference sets have qualities that are strongly connected to the correlation properties of sequences.

Many construction methods have been developed for difference sets, which have been extensively studied. One of these methods is quadratic residues. This study simulates an algorithm which we call by Quadratic Residue Classes Method (QRCM), by utilizing MATLAB R2022a and a laptop with Intel(R) Core (TM) i5 – 5200U, a 2.20Hz processor, and 4 GB of installed memory.

2. Material and Method

This section provides some of the basic definitions and properties used to be the following sections.

2.1. Difference Sets

This section presents the concept of difference sets [18] by considering the notations used in this paper.

Definition 2.1. [18] Let $(G,*)$ be a group of order v, D be a subset of G with k elements, "e" be the unit element of G, and $\lambda \in \mathbb{Z}^+$. If for all $g \in G \setminus \{e\}$, $\left|\{(d_i, d_j) : \exists d_i, d_j \in D,\ d_i \neq d_j \text{ and } d_i d_j^{-1} = g\}\right| = \lambda$, then D is called a (v, k, λ)-difference set over G.

Example 2.2. The set $D = \{0, 1, 5, 8, 10\}$ is a (11, 5,2)-difference set over the additive group $\mathbb{Z}_{11}$. Table 1 shows the generation of the elements of $Z_{11}\backslash\{0\}$ obtained by using those of D under a frequency condition.

Table 1. Obtaining elements of $Z_{11}\backslash\{0\}$ using those of D under a frequency condition

$\mathbb{Z}_{11}/\{0\}$	λ = 2	
1	1 – 0	4 – 3
2	10 – 8	1 – 10
3	8 – 5	0 – 8
4	5 – 1	1 – 8
5	10 – 5	5 – 0
6	5 – 10	0 – 5
7	8 – 1	1 – 5
8	8 – 0	5 – 8
9	10 – 1	8 – 10
10	0 – 1	10 – 0

Theorem 2.3. [18] Let G be an abelian group and D be a (v, k, λ)-difference set over G, then

$$(v - 1)\lambda = k(k - 1).$$

The existence of this theorem does not always show that the structure is a difference set. For example, although this theorem is satisfied in (111,11,1)-parameter projective space, it does not constitute a difference set. Let D be a subset of G be a (v, k, λ)-difference set. When translating of D by the elements of G, i.e., for $g \in G$, gD $(g + D)$ and Dg $(D + g)$ according to a multiplicative (additive) group, is also a (v, k, λ)-difference set.

2.2. Quadratic Residues

We, in this subsection, define a quadratic residue, an integer a that is a square modulo p, and give the concept and properties of quadratic residues. The work of the study of quadratic residues goes back to Euler, Legendre, and Gauss. The question in their mind is when an integer a is a perfect square modulo a prime p. Modular square root problems are extensively related to quadratic residues with many application areas in cryptography, such as an interactive protocol demonstrating that a person has some secret information.

Definition 2.4. [19] Let p be an odd prime and $a \in \mathbb{Z}$ such that $(p, a) = 1$. If there is a solution to the congruent $x^2 \equiv a \ (mod\ p)$, then a is a quadratic residue in modulo p. If there is no solution in modulo p, then it is called the non-quadratic residue.

Lemma 2.5. [19] Let p be an odd prime and a be an integer not divisible by p. Then, the congruence $x^2 \equiv a(mod\ p)$ has either no solutions or exactly two incongruent solutions modulo p.

Lemma 2.5. heads to the main theorems about residues.

Theorem 2.6. [19] If p is an odd prime, then the number of quadratic residues of p is $(p - 1)/2$.

The following theorem also known as Paley difference sets is the main theorem of the article, which give rise to the relation between quadratic residues and difference sets with certain parameters.

Theorem 2.7. [19] (*Paley difference sets)* Let $p \in \mathbb{P}$ and $m \in \mathbb{N}$ such that $p^m \equiv 3 \ (mod\ 4)$ be the power of an odd prime. Let G be the group of the finite field $GF(p^m)$ and $D \subset G$ be the sets of non-zero squares in $GF(p^m)$. Then, D is a $\left(P^m, \frac{p^m-1}{2}, \frac{p^m-3}{4}\right)$ – difference set.

Example 2.8. In the group $(\mathbb{Z}_7, +)$, a subset $D = \{1, 2, 4\}$ of $\mathbb{Z}_7$ is a difference set. This difference set is a $(7, (7 - 1)/2, (7 - 3)/4)$ -Paley difference set for $q = 7$.

Theorem 2.9. [15] Let $p \in \mathbb{P}$ and x be an odd integer such that $p = 4x^2 + 1$, and $G = \mathbb{Z}_p$. Then, the set of the fourth power of every non-zero element of G is a difference set.

Example 2.10. Let us take $x = 3$ and $p = 4.3^2 + 1 = 37$ as the form of an odd prime in the group $\mathbb{Z}_{37}$. Then, the set $D = \{1, 2, 7, 9, 10, 12, 16, 26, 33, 34\}$ of the fourth powers is a difference set with parameters $(37, 9, 2)$.

Theorem 2.11. [15] Let $p \in \mathbb{P}$ and x be an odd integer such that $p = 4x^2 + 9$, and $G = \mathbb{Z}_p$. Then, the set of the fourth power of every non-zero element of G is a difference set.

Example 2.12. Let p be prime as in the form of $p = 4.1^4 + 9 = 13$ with $x = 1$ in the group $\mathbb{Z}_{13}$. Then, the subset $D = \{0, 1, 3, 9\}$ of the set of the fourth power of non-zero elements of $\mathbb{Z}_{13}$with parameters $(13, 4, 1)$ is a difference set.

3. Result

Here, it was checked whether the class obtained from the quadratic residues on the field $GF(q)$ on the MATLAB constituted a difference set with parameters $\left(r, \frac{r-1}{2}, \frac{r-3}{4}\right)$. The method and its flowchart are as follows:

We are now ready to give the algorithm.

3.1. Difference Set Algorithm Obtained from Quadratic Residue Class

Step 1. Determine the size of the field $GF(q)$.

Step 2. Construct a vector consisting of the quadratic residue class of the field

$$(x_i)^2 \equiv 1 \ (mod\ q). \tag{1}$$

Step 3. Figure out the number of elements of the quadratic residue class (k) on the field $GF(q)$

$$k = \frac{q-1}{2} \tag{2}$$

Step 4. A separate k^2 vector is obtained by taking the differences between each pair of points in the quadratic class $[x_i]_{1\times k}$ where $i = 1, 2, 3, \ldots, k$.

Step 5. A new vector of size $k^2 - k$ is created by taking the differences between the elements of the quadratic residue class in the vector. For $\forall\ i, j = 1, 2, 3, \ldots, k$ and $i \neq j$, the following

$$[\boldsymbol{x_i} - \boldsymbol{x_j}]_{\boldsymbol{1\times k^2-k}} \tag{3}$$

where $(x_i - x_j\,) \in GF(q)$, is obtained.

Step 6. A new vector is obtained by sorting the vector obtained in Step 5 from smallest to largest and reparametrizing it. For $= \frac{k(k-1)}{q-1} = \frac{q-3}{4}$, the following

$$\left[v_{s+\lambda(t-1)}\right]_{1\times k^2-k} \tag{4}$$

where $s = 1,2, \ldots, \lambda$ and $t = 1, 2, 3, \ldots, q-1$, is obtained.

Thus, it is seen how many times each element is repeated.

Step 7. For all $s = 1,2, \ldots, \lambda$ and $t = 1, 2, 3, \ldots, q-1$ the number of repetitions in Step 6 satisfies the condition $v_{s+\lambda(t-1)} = t$. In other words, if each element repeats λ times, then this structure is the difference set with the parameters $(r, (r-1)/2, (r-3)/4)$.

Step 8. If the repeats in Step 6 are unequal, it does not form a difference set.

The algorithm's flowchart is given in Figure 1 below.

4. Discussion and Conclusion

This study presents difference sets and quadratic residues, and discusses the connection between quadratic residues and difference sets. Moreover, the paper provides the results and running times for constructing difference sets provided by the QRCM algorithm. The results show that the quadratic residue class for a field is a difference set. The table below gives the program's running time for the MATLAB R2022a application for difference sets constructed from quadratic residues.

Table 2. Running time of the QRCM algorithm

$(\boldsymbol{v}, \boldsymbol{k}, \boldsymbol{l})$	**Running time**
(11,5, 2)	0.001086
(19,9,4)	0.007533
(23,11,5)	0.007545
(31,11,7)	0.016996
(43,21,10)	0.02141
(47,23,11)	0.026246
(59,29,14)	0.029884
(67,33,16)	0.029931
(71,35,17)	0.036807
(79,39,19)	0.038065
(83,41,20)	0.047412
(103,51,25)	0.055755
(107,53,26)	0.058593

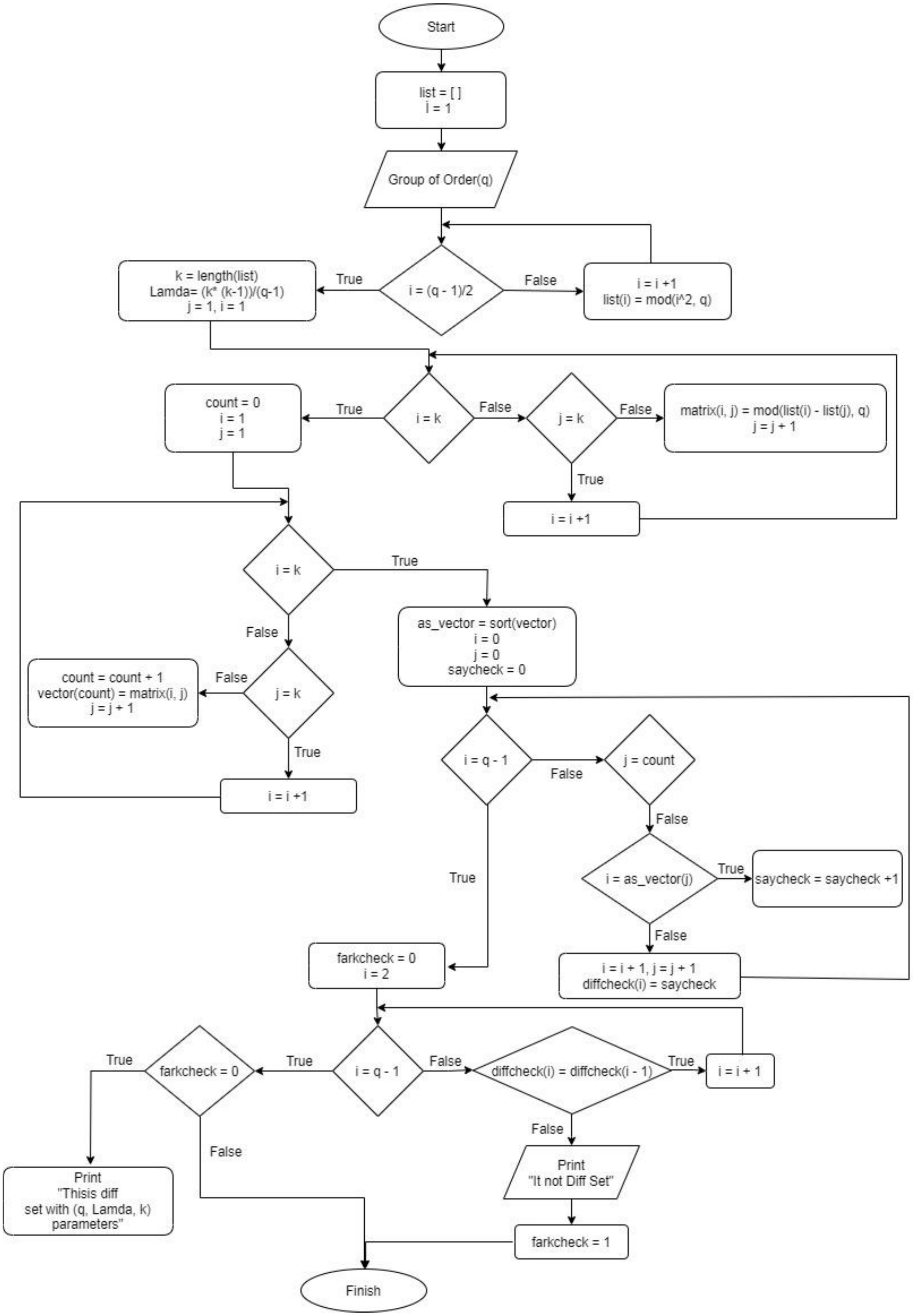

Figure 1. The Algorithm's Flowchart

We have seen that a difference set is a nontrivial specialization of symmetric design [11,13]. They give rise to several new combinatorial objects. Their properties are remarkably similar to those of the difference sets. A computer search for difference sets with small parameters has been conducted using these results.

Acknowledgment

All the authors contributed equally to this work. They all read and approved the last version of the manuscript. This work was derived from the second author's master's thesis supervised by the first author.

References

[1] J. Singer, *A Theorem in Finite Projective Geometry and Some Applications to Number Theory,* Transactions of the American Mathematical Society 43(3) (1938), 377-385.

[2] M. Hall, *Cyclic Projective Planes,* Duke Mathematical Journal 14(4) (1947), 1079-1090.

[3] M. Hall, H. J. Ryser, *Cyclic Incidence Matrices,* Canadian Journal of Mathematics 3(1951), 495-502.

[4] M. Hall, The Theory of Groups, California Institute of Technology, New York, 1959.

[5] M. Hall, *A Survey of Difference Sets,* Proceedings of the American Mathematical Society 7(6) (1956), 975-986.

[6] E. Demirci Akarsu, T. Navdar Günay. *Twin Prime Difference Set and Its Application on a Coded Mask*, Discrete Mathematics, Algorithms and Applications (2022), DOI:10.1142/S1793830922501427, In Press.

[7] C. Godsil, A. Roy. *Equiangular lines, mutually unbiased bases, and spin models*, European Journal of Combinatorics 30 (2009), 246-162.

[8] E. F. Assmus, J. D. Key. Designs and Their Codes, Cambridge University Press, Cambridge, 1992.

[9] C. Ding, Codes from Difference Sets, Singapore: World Scientific, 2014.

[10] S. Chowla, H.J. Ryser, *Combinatorial Problems*, Canadian Journal of Mathematics 2 (1950), 93-99.

[11] H. J. Ryser, *The Existence of Symmetric Block Designs,* Journal of Combinatorial Theory A 32(1) (1982), 103-105.

[12] E. Demirci Akarsu, S. Öztürk, *An Existing Problem for Symmetric Design: Bruck Ryser Chowla Theorem*, Sakarya University Journal of Science 26 (2) (2022), 241-248.

[13] E. Demirci Akarsu, S. Öztürk, *The Existence Problem of Difference Sets*, Gümüşhane University Journal of Science and Technology, 12 (3) (2022), 917-922.

[14] E. Lehmer, *On the Number of Solutions of $u^k + D \equiv w^2$ (mod p),* Pacific Journal of Mathematics 5 (1955), 103 – 118.

[15] E. Lehmer, *On Residue Difference Sets,* Canadian Journal of Mathematics 5 (1953), 425-432.

[16] R. L. McFarland, *A Family of Difference Sets in Noncyclic Groups*, Journal of Combinatorial Theory A, 15(1) (1973), 1-10.

[17] R. L. McFarland, B. F. Rice, *Translates and Multipliers of Abelian Difference Sets,* Proceedings of American Mathematical Society 68 (1978), 375-379.

[18] E. H. Moore, H. S. Pollatsek, Difference Sets: Connecting Algebra, Combinatorics, and Geometry, Providence, RI: American Mathematical Society, 2013.

[19] K. H. Rosen, Elementary Number Theory and its Applications, 5th Edition, Pearson Addison Wesley, USA (2005).