GUFBD / *GUJS* (2022) 12(3): 917-922
DOI: 10.17714/gumusfenbil.1105985 Araştırma Makalesi / *Research Article*

The existence problem of difference sets

Fark kümelerinin varlık problemi

Emek DEMIRCI AKARSU*[1, a], Safiye ÖZTÜRK[b]
[1]*Department of Mathematics, Recep Tayyip Erdoğan University, 53100, Rize*

• Geliş tarihi / *Received*: 19.04.2022 • Düzeltilerek geliş tarihi / *Received in revised form*: 17.06.2022 • Kabul tarihi / *Accepted*: 26.06.2022

Abstract
The existence problem of difference sets in a group becomes more interesting since the applications of difference sets on real life problems become more common. There are several construction methods for difference sets: the relation among parameters, nonexistence of difference sets (Bruck Ryser Chowla Theorem), multipliers etc. A similar problem for symmetric designs along with an investigation of Bruck Ryser Chowla theorem has been discussed by the writers (Sakarya University Journal of Science). In this paper, we study the existence problem of difference sets in a more general concept by using difference sets parameters, BRC Theorem, and an algorithm written in MATLAB.

Keywords: Algorithm in MATLAB, Bruck Ryser Chowla theorem, Difference sets

Öz
Fark kümelerinin gerçek hayat problemlerine uygulamaları arttıkça, bir grup üzerinde tanımlanan fark kümelerinin varlık problemi daha ilgi çekici hale gelmiştir. Fark kümelerinin birçok oluşturma metodu vardır: parametreler arası ilişkiler, fark kümelerinin var olmama teoremi (Bruck Ryser Chowla Teoremi), çarpanlar vb. Simetrik tasarım için benzer bir problem yine Bruck Ryser Chowla Teoremi'nin araştırılmasıyla yazarlar tarafından çalışılmıştır (Sakarya Üniversitesi Bilim Dergisi). Bu makalede fark kümelerinin varlık problemini; fark kümelerinin parametrelerini, BRC Teoremini ve MATLAB'da yazılmış bir algoritmayı kullanarak daha genel bir açıyla inceliyoruz.

Anahtar kelimeler*: MATLAB algoritma, Bruck Ryser Chowla teoremi, Fark kümeleri.*

[*a] Emek DEMİRCİ AKARSU; emek.akarsu@erdogan.edu.tr, Tel: (0464) 223 61 26, orcid.org/0000-0003-4769-0830
[b] orcid.org/0000-0002-6494-6175

1. Introduction
1. Giriş

Difference sets are algebraic constructions that bridge group theory, geometry and combinatorics. The definition of difference sets is combinatorial; however, there are strong connections to algebra especially in finite groups. Their applications vary from coding theory to statistics, from physics to computer sciences, and from engineering to communications. In the late 30's, Singer introduced the first class of difference sets (Singer, 1939), and the study of difference sets became common with discovering the concept of multipliers of difference sets (Hall) (Hall, 1947). Then difference sets in general groups were studied in 1955 (by Bruck) (Bruck, 1955). There is a relation between difference sets and finite sequences (Golomb) (Golomb, 1999), when the existence of a difference set on a cyclic group means there exists a particular periodic sequence with optimal autocorrelation properties. Formal definition of a difference set is as follows;

Definition 1.1. Let D be a k-element subset of a group G of order v. If the multiset Δ formed by $d_i, d_j \in D$ and $d_i * d_j^{-1}$ contains each of the non-identity elements of G exactly λ times, then this subset D is called a (v, k, λ) difference set in group G. Since the groups used in creating the difference set are usually additive groups, the definition can be given as follows: Let G be a finite group and $|G| = v$. Let $\emptyset \neq D \subseteq G$ it consists of k elements of the remaining classes in modulo v with $D = \{d_1, d_2, \ldots, d_k\}$, $|D| = k$. for every $d_i, d_j \in D$, $d_i \neq d_j$ and $\alpha \in G$, $\alpha \not\equiv 1_G \pmod v$, congruence $d_i - d_j \equiv \alpha \pmod v$ contains exactly λ times (d_i, d_j) solution pairs. The multiset in here is defined by $\Delta = \{d_i - d_j |\, d_i, d_j \in D,\ d_i \neq d_j\}$. The (v, k, λ) parameter system in this structure will give $D \subseteq G$ difference set. If the group G is multiplicative, then difference set congruence $d_i d_j^{-1} \equiv \alpha \pmod v$ contains exactly λ times (d_i, d_j) solution pairs. The multiset is this time defined accordingly $\Delta = \left\{d_i d_j^{-1} \middle|\, d_i, d_j \in D,\ d_i \neq d_j\right\}$ (Lander, 1983).

Even though difference sets can be seen similar to a subgroup however they have opposite structure. The differences of elements of a subgroup include in whole subgroup since it has closure property while difference sets have elements of differences spanned uniformly inside the original group.

One of the main and simplest theorems of construction of difference set is stated below.

Theorem 1.1. Let D be a (v, k, λ)-difference set, with $D \subset G$. In this case, there is a $k(k-1) = \lambda(v-1)$ relationship between the parameters. Then $n = k^2 - \lambda v$ (Schützenberger, 1949). n is defined as the size of difference sets here.

Many difference sets can be constructed by exploiting combinatorial properties and algebraic structures. Some obvious examples of difference sets follow immediately from their definition. For example, any set with one item and the empty set are simple difference sets with $\lambda = 0$, whereas the whole group G itself is also a difference set for $\lambda = v$. These examples are simple facts of the difference set construction and are usually negligible. It is also known that the complement of a difference set is a difference set. The proof of the theorem exploits the need of the group ring $Z[G]$. Group ring structure, defined as the polynomials with integer coefficients whose variables are the group elements, they are used working on the properties of difference sets and their construction methods.

In a cyclic group, its automorphisms and translation properties employing a difference set outcomes in another difference set (Baumert, 1971).

In addition to these certain trivial results, many more challenging construction approaches have been studied while difference sets theory has advanced. Yet, the most sophisticated investigation in the field is still unsolved: For any given group G, can we figure out if the group G has a difference set? If it does, how might it be constructed?

In this paper, an existence problem for a difference set is investigated. One of the main tools of showing existence is Bruck Ryser and Chowla Theorem. By means of this theorem, the example of difference sets and non-difference sets of for suitable parameters for symmetric designs and later for difference sets are given by the codes written on MATLAB.

In this study, the existence problem of a difference set in a group is examined by exploiting Bruck Ryser Chowla Theorem. Nonexistence examples of difference sets are eliminated by codes written in MATLAB. Known difference sets with appropriate parameters in the literature are listed by using MATLAB codes (Lehmer, 1953). Some difference sets results when v is odd are listed by Bruck Ryser

Chowla Theorem. An algorithm for construction difference sets in the main program is given and all the examples of symmetric designs till $v = 60$ are obtained. How many suitable (v, k, λ) parameters with the condition $k(k-1) = \lambda(v-1)$ are for possible difference sets are found and listed? In our work, in general, a simplifier way of determining difference sets is shown (Öztürk, 2020).

2. Existence problem

2. Varlık problemi

Bruck-Ryser-Chowla Theorem is one of the most important methods of determining if a particular difference set cannot exist providing the conditions for (v, k, λ) symmetric designs (non)- existence. This theorem also restricts the parameters of a difference set and explains how the solutions of a linear diophantine equation affect the existence of a symmetric design. After Bruck Ryser Chowla theory was first proven for $\lambda = 1$ (Bruck & Ryser, 1949), the writers have extended the result for any positive λ (Bruck & Ryser, 1949; Chowla & Ryser, 1950).

In below, parameter $n = k - \lambda$ is called the order of symmetric design.

Theorem 2.1. (*Bruck-Ryser-Chowla Theorem*) *Let* G be a group with degree v and (v, k, λ) symmetric design exists;

- If v is even, then n is a perfect square.
- If v is odd, Diophantine equation $x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2$ has a nonzero solution in integers x, y, z.

Linear diophantine equation can also be rephrased when $v \equiv 3(mod\ 4)$ or $v \equiv 1(mod\ 4)$

$$x^2 = \begin{cases} \text{If } v \equiv 3(mod\ 4), & ny^2 - \lambda z^2 \\ \text{If } v \equiv 1(mod\ 4), & ny^2 + \lambda z^2. \end{cases}$$

(Bruck & Ryser, 1949; Chowla & Ryser, 1950; Ryser, 1982).

If the BRC statements become false for a certain set of parameters, then those parameters do not satisfy a difference set. However, if the above criteria are true, we say a difference set may be possible. In addition to that, it is safe to presume difference set exists whereas other tools must be used to explore its existence.

2.1. An algorithm for existence of difference sets

2.1. Fark kümelerinin varlığı için algoritma

With this algorithm we will determine whether a given parameter construct a symmetric design or not and therefore a difference set.

- A group with order v is given
- Test that v is a prime number
- If v is not a prime, the prime factors of v are computed.
- Possible (v, k, λ) parameters are calculated.
- New difference sets are determined by using the complement of difference sets.

Let $\lambda = \{1,2,3, \dots, (v-2)\}$ and $k = \frac{1+\sqrt{1+4\lambda(v-1)}}{2}$

- Special parameter $n = k - \lambda$ is calculated.
- The BRC (Bruck- Ryser- Chowla) is used (Legendre Theorem is also used when needed)
- p is found if n is a prime power such that $n = p^m$, for $m \in \mathbb{Z}$ (Morrice, 2015).

For given v, k, λ parameters, after the first condition is hold, they are tested for the BRC theorem by the algorithm itemized above.

Suitable v, k, λ, n and multipliers of difference sets are listed (Baumert & Gordon, 2004).

2.2. MATLAB application of symmetric design (or difference sets)

2.2. Simetrik tasarım (veya fark kümesi) için MATLAB uygulaması

In this section, the stages of construction of difference sets with possible parameters by means of codes are given. According to entered (v, k, λ) values, the code controls whether there is a difference set with appropriate parameters. If there is the result is 1, if not the result is 0.

```
function g = symmetricdesign(v,k,lam)
g = 0;
Z = 0:(v-1);
D = nchoosek(0:v,k);
[n_D,~]= size(D);
tic
for j=1:n_D
    Dk = D(j,:);%
    B = zeros(v,k); %initialization
    for i=1:v
       B(i,:) = Dk+(i-1);%shifting
    end
     H = (B>=v). *B-v;   %
     H(H<0)=0;
     B = (B<v). *B + H ;
% constructing vector A
A = zeros(v,v);
    for ii = 1:v
       for jj=1:v
```

```
            if ~isempty(find(Z(ii)==B(jj,:),1))
            A(jj,ii)=1;
            end
          end
      end
toc
    if A'*A == lam*ones(v)+(k-lam)*eye(v)
        g = 1;
        return
    end
%if Dk==[0 1 2]; disp(B);disp(A); disp(A'); disp(A'*A);
end
   clear B A
end
```

Table 1. For entered parameter v, calculating k and λ values for symmetric design.
Tablo 1. *Girilen v parametresi için, simetrik dizayn oluşturabilecek k ve λ değerlerinin hesaplanması*

v	k	λ	(v,k,λ)
7	3	1	(7,3,1)
11	5	2	(11,5,2)
13	4	1	(13,4,1)
15	7	3	(15,7,3)
19	9	4	(19,9,4)
21	5	1	(21,5,1)
23	11	5	(23,11,5)
31	6	1	(31,6,1)
31	15	7	(31,15,7)
35	17	8	(35,17,8)
37	9	2	(37,9,2)
43	21	10	(43,21,10)
47	23	11	(47,23,11)
59	29	14	(59,29,14)

2.3. Main programme
2.3. Ana program

This programme, first of all, checks whether or not parameters v, k, λ are convenient for difference set. Second, that controls if there are symmetric designs with these parameters or not. Third, the programme lists suitable difference sets. Since there is much of combination, MATLAB results in a long time.

```
for v = 7:2:60
   for k = 3:1:v/2
      for lam = 1:(k-1)
         s = brc_odd(v,k,lam);
         tic
         if s == 1
            g = symmetricdesign(v,k,lam);
            if g==1
                fprintf('%i %i %i\n',v,k,lam)
            toc
           end
         end
      end
   end
end
```

When the code of main programme runs, the following symmetric designs of appropriate parameters by scanning v up to 60 are obtained.

(v,k,λ)=(7,3,1),(11,5,2),(13,4,1),(15,7,3),(19,9,4),(21,5,1),(23,11,5),(31,6,1),(31,15,7),(35,17,8),(37,9,2),(43,21,10),(47,23,11), (57,8,1),(59,29,14)

2.4. MATLAB application of possible difference set parameters
2.4. Olası fark küme parametreleri için MATLAB uygulaması

This code produces results of possible difference sets by the help of the relation of set parameters. This gives the number of symmetric designs of potential (v,k,λ) parameters with $k(k-1)=\lambda(v-1)$.

```
function setparameters(v)
if(mod(v,2)==0)
    value = v/2;
else
   value = (v-1)/2;
end
sayac=0;
for k=2:value
   lam = (k*(k-1))/(v-1);
   if (mod(lam,1)==0)
   disp(fprintf('(v,k,l)=(potential set for parameters %1.0f,%1.0f,%1.0f) ',v,k,lam))
   sayac=sayac+1;
   end
end
disp(fprintf('There are %1.0f potential difference sets.',sayac))
end
```

The following complies potential set of parameters for given v with the condition $v(v-1) = \lambda(k-1)$.

Table 2. The number of potential difference sets for entered value v
Tablo 2. *Girilen v değerinin fark kümesi oluşturan* (v, k, λ) *üçlüleri*

$v = 6271$	$v = 2591$	$v = 5167$	$v = 15001$
(6271,210,7)	(2591,260,26)	(5167,288,16)	(15001,625,26)
(6271,286,13)	(2591,371,53)	(5167820,130)	(15001,5001,1667)
(6271,495,39)	(2591,630,153)	(5167,1107,237)	(15001,5625,2109)
(6271,760,92)	(2591,666,171)	(5167,1477,422)	
(6271,1045,174)	(2591,925,330)	(5167,1764,602)	
(6271,1255,251)	(2591,1036,414)	(5167,2296,1020)	
(6271,1540,378)	(2591,1295,647)	(5167,2583,1291)	
(6271,1596,406)			
(6271,1881,564)			
(6271,2091,697)			
(6271,2376,900)			
(6271,2641,1112)			
(6271,2850,1295)			
(6271,2926,1365)			
(6271,3135,1567)			

Table 3. Average working time for the number of potential difference sets for entered value v
Tablo 3. *Girilen v değerinin olası fark kümelerinin programda çalışma süreleri*

v	Function	The number of difference sets	Average working time for programme
2591	parameter (v)	7	0,17 second
5167	parameter (v)	7	0,11 second
6271	parameter (v)	15	0,65 second
15001	parameter (v)	3	0,96 second

Table 4. Average working time for the number of potential difference sets for entered value v
Tablo 4. *Girilen v değerinin fark kümesi oluşturan üçlülerinin çalışma süreleri*

(v, k, λ)	Function	1&0	Average working time for programme
(7,3,1)	symmetric (v, k, λ)	1	0,14 second
(11,5,2)	symmetric (v, k, λ)	1	0,16 second
(13,4,1)	symmetric (v, k, λ)	1	0,35 second
(15,7,3)	symmetric (v, k, λ)	1	0,45 second
(19,9,4)	symmetric (v, k, λ)	1	0,74 second
(21,5,1)	symmetric (v, k, λ)	1	1,21 second
(23,11,5)	symmetric (v, k, λ)	1	1,77 second
(31,6,1)	symmetric (v, k, λ)	1	4,45 second

Author contribution
Yazar katkısı

Emek DEMİRCİ AKARSU (%60): Conceptualization, Methodology, Supervisor, Programming, Writing - original draft, Writing - review & editing. Safiye ÖZTÜRK (%40): Conceptualization, Programming, Writing - review & editing.

Declaration of ethical code
Etik beyanı

The authors of this article declare that the materials and methods used in this study do not require any ethical committee approval and/or legal-specific permission.

Conflicts of interest
Çıkar çatışması beyanı

The authors declare that there is no conflict of interest.

References
Kaynaklar

Baumert, L. D. (1971). *Cyclic difference sets*. (Vol. 182). California Institute of Technology Pasadena CA/USA. ISBN: 978-3540053682.

Bruck, R. H., & Ryser, H. J. (1949). The nonexistence of certain finite projective planes. *Canadian Journal of Mathematics*, *1*(1), 88-93. https://doi.org/10.4153/CJM-1949-009-2

Bruck, R. H. (1955). Difference sets in a finite group, *Transactions of the American Mathematical Society*, *78*(2), 464-481. https://doi.org/10.2307/1993074

Chowla, S., & Ryser, H. J. (1950). Combinatorial problems. *Canadian Journal of Mathematics*, *2*, 93-99. https://doi.org/10.4153/CJM-1950-009-8

Demirci Akarsu E., & Öztürk, S. (2022). An existence problem for symmetric design: Bruck Ryser Chowla theorem. *Sakarya University Journal of Science*, *26*(2), 241-248, https://doi.org/10.16984/saufenbilder.962817

Golomb, S. W. (1999). Construction of signals with favorable correlation properties, in difference sets, sequences and their correlation roperties. *Kluwer Academic Publishers*, *542*(448), 159-194. https://doi.org/10.1007/978-94-011-4459-9_7

Hall Jr, M. (1947). Cyclic projective planes. *Duke Mathematical Journal*, *14*(4), https://doi.org/1079-1090. 10.1215/S0012-7094-47-01482-8

Lander, E. S. (1983). *Symmetric designs: An algebraic approach*. (Vol.74). London Mathematical Society, Lecture Note Series. Cambridge University. ISBN: 978-0-52128693-0

Lehmer, E. (1953). On residue difference sets. *Canadian Journal of Mathematics*, *5*, 425-432. https://doi.org/10.4153/CJM-1953-047-3

Morrice, R. T. (2015). *Difference sets: An investigation into the properties and criteria for existence* [Master thesis, Carleton University].

Öztürk, S. (2020). *Fark kümelerinin varlık problemi ve Bruck Ryser Chowla teoremi* [Master thesis, Institute of Science of Recep Tayyip Erdoğan University].

Ryser, H. J. (1982). The existence of symmetric block designs. *Journal of Combinatorial Theory A*, *32*(1), 103-105. https://doi.org/10.1016/0097-3165(82)90068-1

Schützenberger, M. P. (1949). A nonexistence theorem for infinite family of symmetrical block designs. *Annals of Human Genetics*, *14*(1), 286-287. https://doi.org/10.1111/j.1469-1809.1947.tb02404.x

Singer, J. (1938). A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society*, *43*(3), 377-385. https://doi.org/10.2307/1990067