SAKARYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ DERGİSİ

Sakarya University Journal of Science
SAUJS

e-ISSN 2147-835X Period Bimonthly Founded 1997 Publisher Sakarya University
http://www.saujs.sakarya.edu.tr/

Title: An Existing Problem for Symmetric Design: Bruck Ryser Chowla Theorem

Authors: Emek DEMİRCİ AKARSU, Safiye ÖZTÜRK

Recieved: 2021-07-06 00:00:00

Accepted: 2022-02-10 00:00:00

Article Type: Research Article

Volume: 26
Issue: 2
Month: April
Year: 2022
Pages: 241-248

How to cite
Emek DEMİRCİ AKARSU, Safiye ÖZTÜRK; (2022), An Existing Problem for Symmetric Design: Bruck Ryser Chowla Theorem. Sakarya University Journal of Science, 26(2), 241-248, DOI: 10.16984/saufenbilder.962817
Access link
https://dergipark.org.tr/tr/journal/1115/issue/69580/962817

Sakarya University Journal of Science 26(2), 241-248, 2022

An Existing Problem for Symmetric Design: Bruck Ryser Chowla Theorem

Emek DEMİRCİ AKARSU*[1], Safiye ÖZTÜRK[1]

Abstract

Symetric designs are interesting objects of combinatorics, and have some relations with coding theory, difference sets, geometry and finite group theory. They have applications on statistics and design experiments. In the present paper we study an existing problem for symmetric design due to Bruck, Ryser and Chowla and write an algorithm by using their theorem called BRC Theorem.

Keywords: Symmetric design, difference sets, Bruck Ryser Chowla Theorem

1. INTRODUCTION

Definition 1. Let $\mathcal{P}$ be the set of points and $\mathcal{B}$ be the set of blocks. An *incidence structure* is a triple $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ such that $\mathcal{P} \cap \mathcal{B} = \emptyset$ and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$ is an *incidence relation* between $\mathcal{P}$ and $\mathcal{B}$. For $p \in \mathcal{P}$ and $B \in \mathcal{B}$ $(p, B) \in \mathcal{I}$ mean p and B are *incidence* [1]. For instance; $\mathcal{P}$ can be the point set and $\mathcal{B}$ can be the block set in the Euclidean plane.

Let $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ be incidence structure, $\mathcal{P} = (p_1, p_2, \dots, p_v)$ point set and $\mathcal{B} = (B_1, B_2, \dots, B_k)$ be the block set. An i*ncidence matrix* M is defined as finite incidence structure where p_i represents points, B_j represents blocks and $m_{ij} \in M$ such that

$$m_{ij} = \begin{cases} 1 & \text{if } p_i \in B_j, \\ 0 & \text{otherwise.} \end{cases}$$

A symmetric (v, k, λ) design is an incidence structure $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ for $0 < k < v$ the following statements hold [2].

(i) There are v points ($|\mathcal{P}| = v$)

(ii) There are v blocks ($|\mathcal{B}| = v$)

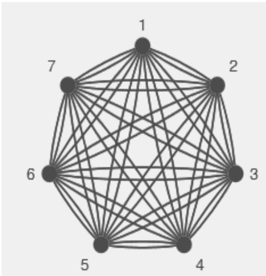
(iii) Each point and each block are incident with k blocks and k points respectively.

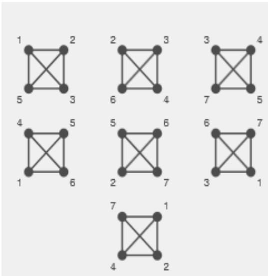
(iv) Each pair of points and each pair of blocks are incident with λ blocks and λ points respectively.

If $\lambda = 0$ and $\lambda = k - 1$, they are called trivial symmetric designs.

Example 2. The set $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ has a subset $D = \{1, 2, 3, 5\}$ with four elements, if we take shifts of all the elements of D then blocks are as follows.

* Corresponding author: emek.akarsu@erdogan.edu.tr
[1] Recep Tayyip Erdoğan University, Faculty of Science and Literature, Department of Mathematics
E-mail: k.ozturk245@gmail.com
ORCID: https://orcid.org/0000-0003-4769-0830, https://orcid.org/0000-0002-6494-6175





The definiton of design theory is combinatorial however there are strong connections to algebra, geometry and has applications to statistics and coding theory. Symetric designs play a key role in construction of differences sets in finite groups.

James Singer is the first person who studied difference sets by relating to topics with finite projective geometry [4]. Then the first construction of blok designs was given by [5]. In the beginning of 40's, this study became more systematic with Halls's work [6]. Levi stressed in his work that there is a close relation between finite projective geometry and affin geometry [5,7,8,9] they used equivalent matrices for these geometries in their work [8, 10, 11] in their study the theory of Bruck Ryser Chowla for (v, k, λ) parameters was given for the existence of symmetric design. In their first paper for $\lambda = 1$ the theorem was proven and this result was extended to any positive λ in the second paper. [12] was explained more simple proof of the theorem. Later so many writers worked on the related subjects [1, 12, 13, 14, 15], etc.

Difference sets link design theory to group theory because a group acts regularly on the points and the blocks of a symmetric design with the condition the group includes a difference set. Most of the examples of difference sets obtain from theory of numbers for examples squares, twin prime numbers etc. A detailed work on the difference sets and cyclotomy is given in [18].

Definition 3. Let G be a finite group with $|G| = v$. Let $\emptyset \neq D = \{d_1, d_2, \ldots, d_k,\} \subseteq G$ be composed of k elements of the remaining classes in the $modulo\ v$. For $d_i, d_j \in D$, $d_i \neq d_j$ and $\alpha \in G$, $\alpha \not\equiv 1_G (\mathrm{mod}\ v)$, congruence

$$d_i - d_j \equiv \alpha (\mathrm{mod}\ v)$$

contains exactly λ pairs of solutions (d_i, d_j). Multiset of differences is expressed as follows:

$$\Delta = \{d_i - d_j |\ d_i, d_j \in D,\ d_i \neq d_j\}.$$

The parameter system (v, k, λ) in this structure expresses the difference set $D \subseteq G$. If G is a multiplicative group, difference set congruence $d_i d_j^{-1} \equiv \alpha (\mathrm{mod}\ v)$ has exactly λ solution pairs (d_i, d_j) with $d_i, d_j \in D$ and $d_i \neq d_j$. Hence the multiset is $\Delta = \left\{d_i d_j^{-1} \middle|\ d_i, d_j \in D,\ d_i \neq d_j\right\}$ [1].

Notice that every difference set is a symmetric block design with a point set $\{0, 1, 2, \ldots, v-1\}$ and a block set $\{D, D+1, \ldots, D+(v-1)\}$ [13]. The most important and fundemental question of difference set is the existence problem. Does a given group have a difference set? Or can we create a difference set? To find an answer to these questions, first neccessary condition is counting of parameters of a (v, k, λ) difference set which leads the equation $k\,(k-1) = \lambda\,(v-1)$.

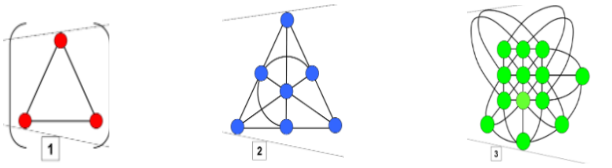
Another answer of the question mentioned above is Bruck- Ryser- Chowla (BRC) theorem. This theorem explains when a (v, k, λ) symmetric design does not exist, hence a (v, k, λ) difference set does not. The proof of this theorem uses incidence matrix M of the design.

2. MAIN RESULTS

Bruck-Ryser-Chowla Theorem is one of most important methods determining if a particular difference set cannot exist providing the conditons 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 affects the existence of a symetric design. Bruck Ryser Chowla theory was first proven for $\lambda = 1$ [8], the writers after extend the result for any positive λ [8, 11].

$$(v, k, \lambda) = (n^2 + n + 1, n + 1, 1)$$

symmetric design is called a projective spaces where parameter n is the degree of projective spaces. BRC theorem is used to investigate the question of existence of projective spaces with degree of non prime power n. For $n \equiv 1,2(mod\ 4)$ and $x, y \in \mathbb{Z}$ we have $n = x^2 + y^2$. The following designs are example of projective planes for degree *n=1*, *n=2* and *n=3* [16].



Theorem 4. (*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 $v \equiv 1(mod\ 4)$

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

[8,12].

If the BRC statements become to be false for a certain set of parameters, then those parameters do not satisfy a difference set. However if the above criteria is 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 eplore its existence.

The proof of the theorem for the case number one is straigtforward but the other case needs matrices equivalence and some arguments from linear algebra and number thoery. One can see a simplest proof of the paper in the paper of [12].

Example 5. Let us take parameter $(76, 25, 8)$. When v even, n should be perfect square. $v = 76$, $k = 25$ and $\lambda = 8$ provide $\lambda(v-1) = k(k-1)$ condition. According to Bruck Ryser Chowla Theory, since $v = 76$ is even, $n = k - \lambda$ must be perfect square in order to get a symmetric design. However, $n = 25 - 8 = 13$ is not a perfect square, there is no symmetric design with this parameter. Therefore, there is no difference set with the parameter $(76, 25, 8)$.

MATLAB applications of Linear diophantine equation

This code lists the solution triple for linear diophantine equation provided by BRC theorem. Besides, how many solutions there can be for the result is also given. This is only a sample size of the solution space.

```
function BRC_linear(v,n,l)

if (mod(v,2)==0)

   error('given value v is even. BRC holds.')

end

devir=0;

for i=1:1000

    for j=1:1000

      x=sqrt((n*i^2)+(-1)^((v-1)/2)*(l*j^2));

      if ((x^2)>0 && mod(x,1)==0)


disp(fprintf('(x,y,z)=(%1.0f,%1.0f,%1.0f)',x,i,j))

         devir=devir+1;

      end

    end

end

disp(fprintf(' For those parameters there are %1.0f triple solutions', devir))

end
```

The following result is a possible $(v,k,\lambda) = (67,14,2)$ difference set with $\lambda = 2, n = 12$ in group $\mathbb{Z}_{67}$. Because there are too many solutions to write of (1817) outputs, they are not given here totally.

```
>> BRC_linear(67,12,2)

(x,y,z)= (2,1,2)

(x,y,z)= (4,2,4)

(x,y,z)= (10,3,2)

(x,y,z)= (6,3,6)

(x,y,z)= (8,4,8)

(x,y,z)= (10,5,10)

(x,y,z)= (20,6,4)
```

…………

```
(x,y,z)= (3310,993,662)

(x,y,z)= (3448,996,88)

(x,y,z)= (3320,996,664)

(x,y,z)= (3284,998,764)

(x,y,z)= (3330,999,666)

(x,y,z)= (3182,999,962)

With this paramaters there are 1817 triplet solutions.
```

The non symmetric design solution triple for $\mathbb{Z}_{67}$ is the following example. Here we have $v = 67$, $\lambda = 7$, $n = 15$, with this possible parameter $(v,k,\lambda) = (67,22,7)$ is not a difference set.

```
>>BRC_lineer(67,15,7)

With this parameters there are 0 triplet solutions.
```

The following result is a possible $(v,k,\lambda) = (73,9,1) -$ difference set in $\mathbb{Z}_{73}$ with $\lambda = 1, n = 8$. For other k and λ values, other possible difference sets of the group $\mathbb{Z}_{73}$ can be tested. The entire output is not shown here because there are too many solutions.

```
>>BRC_linear(73,8,1)

(x,y,z)=(273,91,91)

(x,y,z)=(387,91,289)

(x,y,z)=(663,91,611)

(x,y,z)=(276,92,92)

(x,y,z)=(414,92,322)

(x,y,z)=(561,92,497)

(x,y,z)=(759,92,713)
```

…………

```
(x,y,z)=(2988,996,996)

(x,y,z)=(2991,997,997)

(x,y,z)=(2994,998,998)

(x,y,z)=(2827,999,89)

(x,y,z)=(2997,999,999)

(x,y,z)=(2850,1000,350)

(x,y,z)=(3000,1000,1000)

With these parameters there are 3038 triplet solutions.
```

The following outputs are for the potential difference sets with parameters $(v,k,\lambda) = (91,10,1)$.

```
>> BRC_linear(91,9,1)

(x,y,z)=(12,5,9)

(x,y,z)=(9,5,12)

(x,y,z)=(24,10,18)

(x,y,z)=(18,10,24)

(x,y,z)=(36,13,15)
```

(x,y,z)=(15,13,36)

(x,y,z)=(36,15,27)

(x,y,z)=(2835,977,744)

(x,y,z)=(2880,984,648)

(x,y,z)=(2925,985,420)

(x,y,z)=(2850,986,792)

(x,y,z)=(2808,986,930)

(x,y,z)=(2835,999,972)

(x,y,z)=(2880,1000,840)

With these parameters we have 919 triplet solutions.

The non symmetric design solution triple for $\mathbb{Z}_{91}$ is $(v,k,\lambda)=(91,36,14)$ parameters, hence it is not a difference set.

```
>> BRC_linear(91,22,14)
```

With these parameters there are 0 triplet solutions.

MATLAB Application of BRC Theorem

This code is the application of the second condition of BRC Theorem. The possible solutions of the equation $x^2=ny^2+(-1)^{\frac{v-1}{2}}\lambda z^2$ are analayzed. That controls integers values from 1 to 1000 for y and z values. If the program results 0 output, that means there is no symmetric design. However, if the result is 1 it can be a symmetric design. When the result is 1, the existence of symmetric design should be checked by other tools.

```
function s = brc_odd(v,k,lam)
s = 0;
n = k-lam;
tic
for y= 1:1000
  for z= 1:1000
     x= sqrt((n*y^2)+((-1)^((v-1)/2))*lam*z^2);
     if floor(x)==x && x^2>0
        s = 1;
toc
        return
     end
  end
end
```

The following are the resuts of both solutions and non solutions.

```
>> brc_odd (27,13,16)        ans = 0
>> brc_odd (34,12,4)         ans = 0
>> brc_odd (46,10,2)         ans = 0
>> brc_odd (92,14,2)         ans = 0
>> brc_odd (172,19,2)        ans = 0
>> brc_odd (115,19,4)        ans = 0
>> brc_odd (117,29,7)        ans = 0
>> brc_odd (119,59,7)        ans = 0
>> brc_odd (125,32,8)        ans = 0
>> brc_odd (67,12,2)         ans = 0
>> brc_odd (137,17,2)        ans = 0
>> brc_odd (103,18,3)        ans = 0
>> brc_odd (53,13,3)         ans = 0
>> brc_odd (43,15,5)         ans = 0
>> brc_odd (77,20,5)         ans = 0
>> brc_odd (157,40,10)       ans = 0
>> brc_odd (171,85,41)       ans = 0
```

```
>> brc_odd (173,44,11)        ans = 0
>> brc_odd (181,45,11)        ans = 0
>> brc_odd (185,24,3)         ans = 0
>> brc_odd (187,31,5)         ans = 0
>> brc_odd (193,129,82)       ans = 0
>> brc_odd (6271,210,7)       ans = 1
>> brc_odd (2591,260,26)      ans = 1
```

```
>> brc_odd (5167,288,16)      ans = 1
>> brc_odd (5167,820,130)     ans = 0
>> brc_odd (5167,1107,237)    ans = 0
>> brc_odd (5167,1477,422)    ans = 0
>> brc_odd (5167,1764,602)    ans = 0
>> brc_odd (5167,2296,1020)   ans = 1
>> brc_odd (5167,2583,1291)   ans = 1
```

Table 1 The average working time for the number of solutions parameters (v,k,λ) according to (x,y,z)

(v,n,λ)	Function	The number of solutions	Average working time of the programme
(67,12,2)	BRC (v,n,l)	1817	0,22 second
(67,15,7)	BRC (v,n,l)	0	0,10 second
(73,8,1)	BRC (v,n,l)	3038	0,29 second
(91,9,1)	BRC (v,n,l)	919	0,15 second
(91,22,14)	BRC (v,n,l)	0	1,15 second

Table 2 Average working time for $(\mathrm{v},\mathrm{k},\lambda)$ parameters

(v,k,λ)	Function	1&0	Average working time of the programme
(43,15,5)	brc_odd (v,k,lam)	0	0,1 second
(53,13,3)	brc_odd($v,k,lam)$	0	0,1 second
(67,12,2)	brc_odd (v,k,lam)	0	0,1 second
(77,20,5)	brc_odd (v,k,lam)	0	0,1 second
(103,18,3)	brc_odd (v,k,lam)	0	0,1 second
(115,19,4)	brc_odd (v,k,lam)	0	0,1 second
(117,29,7)	brc_odd (v,k,lam)	0	0,2 second
(119,59,7)	brc_odd(v,k,lam)	0	0,2 second
(125,32,8)	brc_odd(v,k,lam)	0	0,2 second
(137,17,2)	brc_odd(v,k,lam)	0	0,2 second
(157,40,10)	brc_odd(v,k,lam)	0	0,2 second
(171,85,41)	brc_odd(v,k,lam)	0	0,2 second
(173,44,11)	brc_odd(v,k,lam)	0	0,2 second
(181,45,11)	brc_odd(v,k,lam)	0	0,2 second
(185,24,3)	brc_odd(v,k,lam)	0	0,2 second
(187,31,5)	brc_odd(v,k,lam)	0	0,2 second
(193,129,82)	brc_odd(v,k,lam)	0	0,2 second
(2591,260,26)	brc_odd(v,k,lam)	1	0,3 second
(5167,288,16)	brc_odd(v,k,lam)	1	0,5 second
(5167,2296,1020)	brc_odd(v,k,lam)	1	0,5 second
(5167,2583,1291)	brc_odd(v,k,lam)	1	0,5 second
(5167,1477,422)	brc_odd(v,k,lam)	0	0,5 second
(5167,1764,602)	brc_odd(v,k,lam)	0	0,5 second

Acknowledgments

The work has been done mostly in here come from Öztürk's thesis under supervision of the first author [17]. The authors would like to thank the anonymous referees for necessary comments which have improved the presentation of the paper.

Funding

The authors received no financial support for the research, autorship or publication of this study.

The Declaration of Conflict of Interest/ Common Interest

No conflict of interest or common interest has been declared by the authors.

The Declaration of Ethics Committee Approval

The authors declares that this document does not require an ethics committee approval or any special permission.

The Declaration of Research and Publication Ethics

The authors of the paper declares that she complies with the scientific, ethical and quotation rules of SAUJS in all processes of the paper and that she does not make any falsification on the data collected. In addition, she declares that Sakarya University Journal of Science and its editorial board have no responsibility for any ethical violations that may be encountered, and that this study has not been evaluated in any academic publication environment other than Sakarya University Journal of Science.

REFERENCES

[1] E.S. Lander, "Symmetric Designs an Algebraic Approach," Volume 74 of London Mathematical Society, Lecture Note Series. Cambridge University, pp. 3-40, 1983.

[2] M. Hall Jr and H.J. Ryser, "Cyclic incidence matrices," Canadian Journal of Mathematics, vol. 3, pp. 495-502, 1951.

[3] D. Peifer, "Difference Set Transfers," Northfield Undergraduate Mathematics Symposium, 29 Ekim, 3-4. 2013

[4] J. Singer, "A theorem in finite projective geometry and some applications to number theory," Transactions of the American Mathematical Society, vol. 43, no. 3, pp. 377-385, 1938.

[5] R.C. Bose and K.R. Nair, "Partially balanced incomplete block designs," Sankhya: The Indian Journal of Statistics, vol. 4, no. 3, pp. 337-372, 1939.

[6] M. Hall Jr, "Cyclic projective planes," Duke Mathematical Journal, vol. 14, no. 4, pp. 1079-1090, 1947.

[7] F.W. Levi, "Groups in which the commutator operation satisfies certain algebraic conditions," The Journal of the Indian Mathematical Society, vol. 6, pp. 87-97. 1942.

[8] R.H. Bruck and H.J. Ryser, "The non existence of certain finite projective planes," Canadian Journal of Mathematics, vol. 1, no. 1, pp. 88-93, 1949.

[9] M.P. Schützenberger, "A Nonexistence Theorem for Infinite family of symmetrical block designs," Annals of Human Genetics, vol. 14, no. 1, pp. 286-287, 1949.

[10] P. Dembowski, "Finite geometries," Mathematics Subject Classification (1991): 51E, vol. 44, 1997.

[11] S. Chowla and H. J. Ryser, "Combinatorial problems," Canadian Journal of Mathe matics, vol. 2, pp. 93-99, 1950.

[12] H.J. Ryser, "The existence of symmetric block designs," Journal of Combinatorial Theory A, vol. 32, no. 1, pp. 103-105, 1982.

[13] L.D. Baumert, “Cyclic Difference Sets,” California Institute of Technology Pasadane, vol. 172, pp. 1-9, 1971.

[14] D. Raghavarao, “Constructions and Combinatorial Problems in Design of Experiments,” John Wiley, Newyork, 1971.

[15] R.E. Kibler, “A summary of noncyclic difference sets k<20,” Journal of Combinatorial Theory A, vol. 25, no. 1, pp. 62-67, 1978.

[16] P. J. Cameron and J. H. Lint, “Desings, Graps, Codes and their Links www.maa.org/programs/maa-awards/writing-awards/the-search-for-finite-projective-plane-of-order-10,” Cambridge University Press, 1991.

[17] S. Öztürk, “Fark kümelerinin varlık problemi ve Bruck Ryser Chowla Teoremi,” Yüksek Lisan Tezi, Recep Tayyip Erdoğan Üniversitesi Fen Bilimleri Enstitüsü, Rize, 2020.

[18] E. Demirci Akarsu, “Almost Difference Sets and Cyclotomy,” in Academic Studies in Science and Mathematics. Izmir, Turkey: Platanus Duvar Publishing, ch. 10, pp. 143–159, 2021.