Věroslav Jurák

Conjugate cyclic (v, k, λ)-configurations

Časopis pro pěstování matematiky, Vol. 105 (1980), No. 1, 31--40

Persistent URL: `http://dml.cz/dmlcz/118045`

Časopis pro pěstování matematiky, roč. 105 (1980), Praha

CONJUGATE CYCLIC (v, k, λ)-CONFIGURATIONS*)

VĚROSLAV JURÁK, Poděbrady

(Received July 6, 1977)

I. BASIC DEFINITIONS AND THEOREMS

Definition 1. Let $\mathscr{X} = \{x_0, x_1, \ldots, x_{v-1}\}$ be a set of distinct integers modulo v and $B_0, B_1, \ldots, B_{b-1}$ a system $\mathscr{B}$ of distinct subsets (blocks) of $\mathscr{X}$. If the system $\mathscr{B}$ satisfies the following axioms:

(I) $|B_i| = k$ $(i = 0, 1, \ldots, b - 1)$,

(II) each pair of distinct elements of $\mathscr{X}$ occurs together in exactly λ distinct sets of $\mathscr{B}$,

(III) the integers v, k, λ satisfy the inequalities $0 < \lambda, k < v - 1$,

then $\mathscr{B}$ is called a (b, v, r, k, λ)-*configuration*. (As in [1].)

For the (b, v, r, k, λ)-configurations we have the following theorems:

(IV) each element of $\mathscr{X}$ occurs in exactly r sets of $\mathscr{B}$,

(V) $bk = vr$,

(VI) $r(k - 1) = \lambda(v - 1)$,

(VII) $b \geqq v$ $(\Rightarrow r \geqq k)$.

(The proofs are in [1].)

Definition 2. Let $\mathscr{X} = \{x_0, x_1, \ldots, x_{v-1}\}$ be a set of distinct integers modulo v and $B_0, B_1, \ldots, B_{v-1}$ a system $\mathscr{B}$ of distinct subsets (blocks) of $\mathscr{X}$. If the system $\mathscr{B}$ satisfies the following axioms:

(1) $|B_i| = k$ $(i = 0, 1, \ldots, v - 1)$,

(2) $|B_i \cap B_j| = \lambda,\ i \neq j,\ (i, j = 0, 1, \ldots, v - 1)$,

(3) the integers v, k, λ satisfy the inequalities $0 < \lambda < k < v - 1$,

*) The author had presented this result in another form at the Conference on Graph Theory — Smolenice (Czechoslovakia), March 1976.

then $\mathscr{B}$ is called a (v, k, λ)-*configuration*. (As in [1].) The system $\mathscr{B}$ is also called the (v, k, λ)-*configuration* $(\mathscr{X}, \mathscr{B})$. We note that any (v, k, λ)-configuration is in fact a (v, v, k, k, λ)-configuration. (See [1].)

Definition 3. Two (v, k, λ)-configurations $(\mathscr{X}, \mathscr{B})$, $(\mathscr{X}, \mathscr{B}')$ are said *to be identical* if and only if $\mathscr{B} = \mathscr{B}'$, and we write $(\mathscr{X}, \mathscr{B}) = (\mathscr{X}, \mathscr{B}')$.

Proposition 1. *Given a (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$, there exists no $(v + 1, v, k, k, \lambda)$-configuration $(\mathscr{X}, \mathscr{B}^*)$ such that $\mathscr{B}^* = \mathscr{B} \cup B$ where $B \subset \mathscr{X}$, $B \neq B_i \in \mathscr{B}$ $(i = 0, 1, \ldots, v - 1)$ and $|B| = k$.*

Proof. From Theorem (V) we get

$$(v + 1)\, k = vk$$

and this implies $k = 0$; a contradiction with Axiom (3).

Definition 4. An isomorphism α of a (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$ is a permutation of $\mathscr{X}$ such that if $x \in \mathscr{X}$ and $B \in \mathscr{B}$, then

$$x \in B \Leftrightarrow \alpha(x) \in \alpha(B)\,.$$

(As in [2].) If $\alpha(\mathscr{B}) = \mathscr{B}$, then the isomorphism α is called an *automorphism of the (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$*.

Definition 5. A (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$ is called *cyclic* if there exists its automorphism α such that

$$\alpha : i \mapsto i + 1 \pmod v \quad \text{for each} \quad i \in \mathscr{X}$$

and the system $\mathscr{B}$ is denoted so that

$$B_i \mapsto B_{i+1}\,, \quad i + 1 \pmod v \quad \text{for each} \quad B_i \in \mathscr{B}\,.$$

(As in [2].)

Proposition 2. *For a given integer j define a mapping α of the given cyclic (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$ onto $(\mathscr{X}, \mathscr{B})$ by*

$$\alpha : i \mapsto i + j \pmod v \quad \text{for each} \quad i \in \mathscr{X}\,, \quad \text{and}$$

$$B_i \mapsto B_{i+j}\,, \quad i + j \pmod v \quad \text{for each} \quad B_i \in \mathscr{B}\,.$$

Then α is an automorphism of $(\mathscr{X}, \mathscr{B})$.

Proof. This Proposition follows from a composition of automorphisms from Definition 5.

Definition 6. A set $D = \{a_1, a_2, \ldots, a_k\}$ of integers modulo v is called a (v, k, λ)-*difference set*, if for each $d \not\equiv 0 \pmod v$ there are exactly λ distinct ordered pairs (a_i, a_j), where $a_i, a_j \in D$, such that $a_i - a_j \equiv d \pmod v$. (As in [2].)

Theorem 1. *A set $D = \{a_1, a_2, \ldots, a_k\}$ of integers modulo v is a (v, k, λ)-difference set if and only if a system of v sets $B_p = \{a_1 + p, a_2 + p, \ldots, a_k + p\}$ modulo v $(p = 0, 1, \ldots, v - 1)$ is a cyclic (v, k, λ)-configuration.* (Cf. the proof in [2].) *Hence $B_0 = D$ and each set B_p is a (v, k, λ)-difference set.*

We shall use the (v, k, λ)-configuration $(\mathcal{X}, \mathcal{B})$ where the system $\mathcal{B} = \{B_p\}$ $(p = 0, 1, \ldots, v - 1)$ is the system of sets from Theorem 1, and its isomorphism α which is given by the following definition:

$$\alpha : x \mapsto v - x \pmod v \quad \text{for each} \quad x \in \mathcal{X} .$$

Theorem 1 implies

$$B_p = \{a_1 + p, a_2 + p, \ldots, a_k + p\} \pmod v \ (p = 0, 1, \ldots, v - 1) .$$

Let p be a fixed integer. Then to each $d \not\equiv 0 \pmod v$ there exist exactly λ distinct ordered pairs $(a_i + p, a_j + p)$ where $a_i + p, a_j + p \in B_p$ such that

$$(a_i + p) - (a_j + p) = a_i - a_j \equiv d \pmod v .$$

We get

$$\alpha(B_p) = \{v - (a_1 + p), v - (a_2 + p), \ldots, v - (a_k + p)\} \pmod v$$
$$(p = 0, 1, \ldots, v - 1) .$$

Let p be a fixed integer. Then to each $d \not\equiv 0 \pmod v$ there exist exactly λ distinct ordered pairs $(v - (a_j + p), v - (a_i + p))$ where $v - (a_j + p)$, $v - (a_i + p) \in \alpha(B_p)$ such that

$$(v - (a_j + p)) - (v - (a_i + p)) = a_i - a_j \equiv d \pmod v .$$

The foregoing remarks yield

Proposition 3. *Let a set $D = \{a_1, a_2, \ldots, a_k\}$ of integers modulo v be a (v, k, λ)-difference set. Given a fixed integer p, then the set*

$$\alpha(B_p) = \{v - (a_1 + p), v - (a_2 + p), \ldots, v - (a_k + p)\} \pmod v$$

is a (v, k, λ)-difference set. The system of sets

$$\overline{\mathcal{B}} = \{\alpha(B_p)\} \quad (p = 0, 1, \ldots, v - 1)$$

is a cyclic (v, k, λ)-configuration.

It is easy to see the validity of the following two propositions:

Proposition 4. *Let a_i, a_j, p, v be integers. Then*

$$v - a_i \equiv a_j + p \pmod v \Leftrightarrow a_i + a_j \equiv v - p \pmod v .$$

Proposition 5. *Let p be an integer and let $\mathscr{X} = \{x_0, x_1, \ldots, x_{v-1}\}$ be a set of distinct integers modulo v. Then the congruence*

$$(*) \qquad v - x \equiv x + p \pmod v$$

has at most one solution from $\mathscr{X}$ for v odd and at most two solutions from $\mathscr{X}$ for v even.

These facts are important for the formulation of suppositions in the following considerations.

II. OBSERVATIONS FOR v ODD

Now, we shall prove the following

Lemma 1. *Let v be an odd integer and let the set $D = \{a_1, a_2, \ldots, a_k\}$ of integers modulo v be a (v, k, λ)-difference set. We have here a cyclic (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$ with the system $\mathscr{B} = \{B_p\}$ $(p = 0, 1, \ldots, v-1)$ where $B_p = \{a_1 + p, a_2 + p, \ldots, a_k + p\}$. If we define an isomorphism of $(\mathscr{X}, \mathscr{B})$ as follows:*

$$\alpha : x \mapsto v - x \pmod v \quad \text{for each of} \quad x \in X\,,$$

then $B_p \neq \alpha(B_0)$ for all $p = 0, 1, \ldots, v-1$.

Proof. To prove this lemma we consider four cases.

1. Let k be an odd integer. Let each $a_i \in B_0$ satisfy the condition $a_i + a_i \equiv \equiv v - p \pmod v$. Next, let the elements of B_0 be suitably denoted so that

$$a_{2r-1} + a_{2r} \equiv v - p \pmod v\,,$$

where $r = 1, 2, \ldots, (k-1)/2$. Hence we get that

$$v - a_{2r-1} \equiv a_{2r} + p \pmod v$$

and also

$$v - a_{2r} \equiv a_{2r-1} + p \pmod v\,,$$

where $r = 1, 2, \ldots, (k-1)/2$. Then $\alpha(B_0)$ and B_p have $k - 1$ elements in common. Since

$$a_k + a_k \not\equiv v - p \pmod v$$

(cf. the suppositions and Proposition 5), it follows that

$$v - a_k \not\equiv a_k + p \pmod v\,.$$

That is, $B_p \neq \alpha(B_0)$.

2. Let again k be an odd integer. Let the elements of B_0 be suitably denoted so that

$$a_1 + a_1 \equiv v - p \pmod v$$

and

(a) $$a_{2r} + a_{2r+1} \equiv v - p \pmod{v}$$

for all $r = 1, 2, \ldots, (k - 1)/2$. Hence and from Proposition 4 it follows that $B_p = \alpha(B_0)$.

2_1. Now, let also λ be an odd integer. The number of congruences (a) is $(k - 1)/2$, the number of differences $a_{2r} - a_{2r+1}, a_{2r+1} - a_{2r}$, $(r = 1, 2, \ldots, (k - 1)/2)$ is $k - 1$ and in view of Axiom (3) it is $k - 1 < v - 2$. Hence there exists at least one number $d \not\equiv 0 \pmod{v}$ for which

$$a_{2r} - a_{2r+1}, a_{2r+1} - a_{2r} \not\equiv d \pmod{v}$$

for all $r = 1, 2, \ldots, (k - 1)/2$. Then it is possible that there exists a convenient $s = 1, 2, \ldots, (k - 1)/2$ such that

$$\text{either} \quad a_{2s} - a_1 \equiv d \pmod{v} \quad \text{or} \quad a_1 - a_{2s} \equiv d \pmod{v}.$$

This s fulfils

$$a_{2s} + a_{2s+1} \equiv v - p \pmod{v}.$$

Hence in the first case we have in fact also

$$a_1 - a_{2s+1} \equiv d \pmod{v}$$

and in the second case also

$$a_{2s+1} - a_1 \equiv d \pmod{v}.$$

Then to d in the first case there exist two pairs $(a_{2s}, a_1), (a_1, a_{2s+1})$ satisfying

$$a_{2s} - a_1, a_1 - a_{2s+1} \equiv d \pmod{v}$$

and in the second case there exist two pairs $(a_1, a_{2s}), (a_{2s+1}, a_1)$, satisfying

$$a_1 - a_{2s}, a_{2s+1} - a_1 \equiv d \pmod{v}.$$

For each a_t, $t = 2, 3, \ldots, k$, $t \neq 2s$, it is

$$\text{either} \quad a_t - a_1 \not\equiv d \pmod{v} \quad \text{or} \quad a_1 - a_t \not\equiv d \pmod{v}.$$

If there exists no s with the above properties, then there are necessarily such $m, n = 1, 2, \ldots, (k - 1)/2$, where $m \neq n$, that either the equivalence

$$a_{2m} - a_{2n} \equiv d \pmod{v} \Leftrightarrow a_{2n+1} - a_{2m+1} \equiv d \pmod{v}$$

or

$$a_{2m} - a_{2n+1} \equiv d \pmod{v} \Leftrightarrow a_{2n} - a_{2m+1} \equiv d \pmod{v}$$

holds. This means that to d there exist either two pairs $(a_{2m}, a_{2n}), (a_{2n+1}, a_{2m+1})$ satisfying

$$a_{2m} - a_{2n}, a_{2n+1} - a_{2m+1} \equiv d \pmod{v}$$

or two pairs (a_{2m}, a_{2n+1}), (a_{2n}, a_{2m+1}) satisfying

$$a_{2m} - a_{2n+1}, a_{2n} - a_{2m+1} \equiv d \pmod{v}.$$

Altogether, we have that the number of pairs (a_i, a_j) with $a_i, a_j \in B_0$ such that

$$a_i - a_j \equiv d \pmod{v},$$

is even; a contradiction with λ odd, Hence $B_p \neq \alpha(B_0)$.

2_2. Now, let λ be an even integer. By congruences (a) we have

$$a_{2r} - a_{2r+1} \equiv 2a_{2r} - v + p \pmod{v}, \quad a_{2r+1} - a_{2r} \equiv 2a_{2r+1} - v + p \pmod{v}$$

Since all elements of B_0 are different, the same holds for all numbers $2a_{2r} - v + p$, $2a_{2r+1} - v + p \pmod{v}$ for all $r = 1, 2, \ldots, (k-1)/2$. None of these numbers are congruent with $0 \pmod{v}$ by the assumption and Proposition 5. Then to some $d \not\equiv 0 \pmod{v}$ there exists a convenient $r = 1, 2, \ldots, (k-1)/2$ such that the congruence

$$a_{2r} - a_{2r+1} \equiv d \pmod{v}$$

holds. To complete the proof we use the same argument as in 2_1 of this, proof, now with this d. However, now the number of pairs (a_i, a_j) with $a_i, a_j \in B_0$ such that

$$a_i - a_j \equiv d \pmod{v}$$

is even or zero. Hence we conclude that the number of these pairs (a_i, a_j) is odd; a contradiction with the assumption that it is even. Thus $B_p \neq \alpha(B_0)$.

3. Let k be an even integer. Let each $a_i \in B_0$ satisfy the condition $a_i + a_i \not\equiv v - p \pmod{v}$. Next, let the elements of B_0 be suitably denoted so that

$$\text{(b)} \qquad a_{2r-1} + a_{2r} \equiv v - p \pmod{v},$$

where $r = 1, 2, \ldots, k/2$. Hence and from Proposition 4 it follows that $B_p = \alpha(B_0)$.

3_1. Let us consider the integer λ to be odd. The number of congruences (b) is $k/2$, the number of differences $a_{2r} - a_{2r-1}$, $a_{2r-1} - a_{2r}$ $(r = 1, 2, \ldots, k/2)$ is k and in view of Axiom (3) it is $k < v - 1$. Hence there exists at least one number $d \not\equiv 0 \pmod{v}$ for which

$$a_{2r} - a_{2r-1}, a_{2r-1} - a_{2r} \not\equiv d \pmod{v}$$

for all $r = 1, 2, \ldots, k/2$. Then there are necessarily such $s, t = 1, 2, \ldots, k/2$, where $s \neq t$, that either the equivalence

$$a_{2s} - a_{2t} \equiv d \pmod{v} \Leftrightarrow a_{2t-1} - a_{2s-1} \equiv d \pmod{v},$$

or

$$a_{2s} - a_{2t-1} \equiv d \pmod{v} \Leftrightarrow a_{2t} - a_{2s-1} \equiv d \pmod{v}$$

holds. This means that to d there exist either two pairs (a_{2s}, a_{2t}), (a_{2t-1}, a_{2s-1}) satisfying

$$a_{2s} - a_{2t}, a_{2t-1} - a_{2s-1} \equiv d \pmod{v}$$

or two pairs (a_{2s}, a_{2t-1}), (a_{2t}, a_{2s-1}) satisfying

$$a_{2s} - a_{2t-1},\ a_{2t} - a_{2s-1} \equiv d \pmod v .$$

Hence we conclude that for this d the number of paírs (a_i, a_j) with $a_i, a_j \in B_0$ such that

$$a_i - a_j \equiv d \pmod v$$

is even; a contradiction with λ odd. Thus $B_p \not\equiv \alpha(B_0)$.

3_2. Let λ be also an even integer. By congruences (b) we have

$$a_{2r} - a_{2r-1} \equiv 2a_{2r} - v + p \pmod v, \quad a_{2r-1} - a_{2r} \equiv 2a_{2r-1} - v + p \pmod v .$$

As in 2_2 of this proof these differences are distinct, in fact $\not\equiv 0 \pmod v$, for all $r = 1, 2, \ldots, k/2$. Then to each $d \not\equiv 0 \pmod v$ there exists a convenient $r = 1, 2, \ldots$ $\ldots, k/2$ such that the congruence

$$a_{2r-1} - a_{2r} \equiv d \pmod v$$

holds. Now we proceed with this d in the same way as in 3_1 of this proof. We have here that the number of pairs (a_i, a_j) with $a_i, a_j \in B_0$ such that

$$a_i - a_j \equiv d \pmod v$$

is even or zero. Hence we conclude that the number of these pairs (a_i, a_j) is odd; a contradiction with the assumption that λ is even. Thus $B_p \not\equiv \alpha(B_0)$.

4. Let k be an even integer. Let the elements of B_0 be denoted in a suitable way so that

$$a_1 + a_1 \equiv v - p \pmod v$$

and

$$a_{2r} + a_{2r+1} \equiv v - p \pmod v$$

for all $r = 1, 2, \ldots, (k-2)/2$. Hence and from Proposition 4 it follows that B_p and $\alpha(B_0)$ have $k - 1$ elements in common. In view of Proposition 5 the congruence $(*)$ is satisfied for precisely one element. With regard to the supposition we may assume that this occurs exactly for $x = a_1$, and thus it is

$$v - a_k \not\equiv a_k + p \pmod v .$$

Then $B_p \not\equiv \alpha(B_0)$.

This completes the proof of Lemma 1.

III. OBSERVATIONS FOR v EVEN

It is quite easy to verify

Proposition 6. *Let v be an even integer. Then the equation*

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

(*which follows from Theorem* (VI)) *is satisfied only for even* λ.

Now, we shall sketch the proof of the following

Lemma 2. *Let v be an even integer and let a set $D = \{a_1, a_2, \ldots, a_k\}$ of integers modulo v be a (v, k, λ)-difference set. We have a cyclic (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$ wtth the system $\mathscr{B} = \{B_p\}$ $(p = 0, 1, \ldots, v - 1)$ where $B_p = \{a_1 + p, a_2 + p, \ldots, a_k + p\}$. If we define an isomorphism of $(\mathscr{X}, \mathscr{B})$ as follows:*

$$\alpha : x \mapsto v - k \pmod{v} \quad \textit{for each of} \quad x \in \mathscr{X}\,,$$

then $B_p \neq \alpha(B_0)$ for all $p = 0, 1, \ldots, v - 1$.

Proof. 1. Let k be an odd integer. Let each $a_i \in B_0$ satisfy the condition $a_i + a_i \not\equiv v - p \pmod{v}$. Further, let the elements of B_0 be denoted in a suitable way so that

$$a_{2r-1} + a_{2r} \equiv v - p \pmod{v}$$

where $r = 1, 2, \ldots, (k - 1)/2$. If we proceed in the same way as in part 1 of the proof of Lemma 1 then we have also $B_p \neq \alpha(B_0)$.

2. Let k be an odd integer. Let the elements of B_0 be denoted so that

$$a_1 + a_1 \equiv v - p \pmod{v}$$

and

$$a_{2r} + a_{2r+1} \equiv v - p \pmod{v}$$

for all $r = 1, 2, \ldots, (k - 1)/2$. Now we proceed in the same way as in 2_2 of the proof of Lemma 1. Here we have that $B_p \neq \alpha(B_0)$.

3. Let k be an odd integer. Let the elements of B_0 be denoted so that

$$a_1 + a_1 \equiv v - p \pmod{v}\,,$$

$$a_2 + a_2 \equiv v - p \pmod{v}$$

and

$$a_{2r-1} + a_{2r} \equiv v - p \pmod{v}\,,$$

where $r = 2, 3, \ldots, (k - 1)/2$. Then B_p and $\alpha(B_0)$ have $k - 1$ elements in common. Since

$$a_k + a_k \not\equiv v - p \pmod{v}$$

it is

$$v - a_k \not\equiv a_k + p \pmod{v}$$

in view of Proposition 4. Hence $B_p \neq \alpha(B_0)$.

4. Let k be an even integer. Let $a_i + a_i \not\equiv v - p \pmod{v}$ for each $a_i \in B_0$. Further, let the elements of B_0 be denoted so that

$$a_{2r-1} + a_{2r} \equiv v - p \pmod{v}$$

where $r = 1, 2, \ldots, k/2$. Now we proceed in the same way as in 3_2 of the proof of Lemma 1. Here we have $B_p \neq \alpha(B_0)$.

5. Let k be an even integer. Let the elements of B_0 be denoted so that

$$a_1 + a_1 \equiv v - p \pmod{v}$$

and

$$a_{2r} + a_{2r+1} \equiv v - p \pmod{v}$$

for all $r = 1, 2, \ldots, (k-2)/2$. We proceed in this case in the same way as in 4 of the proof of Lemma 1. Here we have that $B_p \neq \alpha(B_0)$.

6. Let k be an even integer. Let the elements of B_0 be denoted so that

$$a_1 + a_1 \equiv v - p \pmod{v}, \quad a_2 + a_2 \equiv v - p \pmod{v}$$

and

$$\text{(c)} \qquad a_{2r-1} + a_{2r} \equiv v - p \pmod{v}$$

for all $r = 2, 3, \ldots, k/2$. From the congruences (c) we obtain

$$a_{2r} - a_{2r-1} \equiv 2a_{2r} - v + p \pmod{v}, \quad a_{2r-1} - a_{2r} \equiv 2a_{2r-1} - v + p \pmod{v}.$$

As in 2_2 of the proof of Lemma 1 these differences are distinct, and $\not\equiv 0 \pmod{v}$ and here even $\not\equiv v/2 \pmod{v}$ for all $r = 2, 3, \ldots, k/2$. Then to some $d \not\equiv 0, v/2 \pmod{v}$ there exists a convenient $r = 2, 3, \ldots, k/2$ such that the congruence

$$a_{2r-1} - a_{2r} \equiv d \pmod{v}$$

holds. Note that

$$a_1 - a_2,\ a_2 - a_1 \not\equiv d \pmod{v}.$$

If we proceed in the same way as in 3_1 of the proof of Lemma 1 with this d, we have again $B_p \neq \alpha(B_0)$.

This completes the proof of Lemma 2.

IV. CONCLUSION

Let, in this section, the set $D = \{a_1, a_2, \ldots, a_k\}$ of integers modulo v be a (v, k, λ)-difference set. Hence, the system $\mathscr{B} = \{B_p\}$, $p = 0, 1, \ldots, v-1$ where $B_p = \{a_1 + p, a_2 + p, \ldots, a_k + p\}$ is a cyclic (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$ and the system $\overline{\mathscr{B}} = \{\alpha(B_p)\}$, $p = 0, 1, \ldots, v-1$ where $\alpha(B_p) = \{v - (a_1 + p), v - (a_2 + p), \ldots, v - (a_k + p)\}$ is also a cyclic (v, k, λ)-configuration $(\mathscr{X}, \overline{\mathscr{B}})$.

We may summarize the results of the foregoing observations:

Proposition 7. *In view of Proposition 1 we can prolongate a cyclic (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$ neither by $\alpha(B_0)$ nor by any one of $\alpha(B_p)$ $(p = 1, 2, \ldots, v-1)$.*

Proposition 8. *Given a cyclic (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$ and its isomorphism*

$$\alpha : x \mapsto v - x \quad \textit{for each} \quad x \in \mathscr{X},$$

then α is never an automorphism of $(\mathscr{X}, \mathscr{B})$.

Theorem 2. *If there exists a cyclic (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$, then if we define an isomorphism of $(\mathscr{X}, \mathscr{B})$ by $\alpha : x \mapsto v - x$ for each $x \in \mathscr{X}$, we get a cyclic (v, k, λ)-configuration $(\mathscr{X}, \overline{\mathscr{B}})$, where $\alpha(\mathscr{B}) = \overline{\mathscr{B}}$ and both the configurations $(\mathscr{X}, \mathscr{B})$, $(\mathscr{X}, \overline{\mathscr{B}})$ are distinct.*

Corollary. *Let v, k, λ be positive integers. If there exists a cyclic (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$ then the number of distinct cyclic (v, k, λ)-configurations is even.*

Consider now a cyclic (v, k, λ)-configuration $(\mathscr{X}, \mathscr{B})$. Since $v - (v - x) = x$, there exists an automorphism of $(\mathscr{X}, \mathscr{B})$

$$\alpha^2 : x \mapsto v - x \mapsto v - (v - x) \quad \text{for each} \quad x \in \mathscr{X} .$$

All this entitles us to express the results of this paper in the following way:

Two cyclic (v, k, λ)-configurations $(\mathscr{X}, \mathscr{B})$ and $(\mathscr{X}, \overline{\mathscr{B}})$ may be called conjugate.

References

[1] *Herbert John Ryser:* Combinatorial Mathematics. The Mathematical Association of America, 1963.

[2] *Marshall Hall,* Jr.: Combinatorial Theory. Blaisdell, Waltham (Massachusetts), 1967.

Author's address: 290 35 Poděbrady - Zámek (Katedra matematiky FEL ČVUT).