Sveučilište u Zagrebu

Prirodoslovno-matematički fakultet

Matematički odjel

Marko Špoljarec

Stinsonov algoritam za konstrukciju Steinerovih sustava trojki

Diplomski rad

Voditelj: doc. dr. sc. Vedran Krčadinac

Zagreb, studeni 2007.

Posvećeno obitelji,

teti Grozdani i tati Damiru.

Sadržaj

Sadržaj i

Sažetak ii

Zahvala iii

1. **Teorija dizajna** 1

1.1. *Dizajni* 2

1.2. *Uravnoteženi nepotpuni blokovni dizajni* 3

1.3. *Matrice incidencije* 11

1.4. *Fisherova nejednakost* 15

1.5. *Simetrični blokovni dizajni* 20

1.6. *Novi blokovni dizajni iz starih* 25

2. **Steinerovi sustavi trojki** 31

2.1. *Latinski kvadrati i kvazigrupe* 33

2.2. *Boseova konstrukcija* 41

2.3. *Skolemova konstrukcija* 45

2.4. *Izomorfizmi* 50

2.5. *Automorfizmi* 56

3. **Stinsonov algoritam** 61

3.1. *Opis algoritma* 62

3.2. *Implementacija algoritma* 70

3.3. *Rezultati izvršavanja algoritma* 79

Indeks A

Literatura B

Sažetak

Cilj diplomskog rada je proučavanje Stinsonovog algoritma za konstrukciju Steinerovih sustava trojki, najjednostavnije vrste uravnoteženih nepotpunih blokovnih dizajna.

U prvom poglavlju obrađene su osnove teorije dizajna. Na početku, definirani su dizajni. Dokazani su teoremi vezani uz uravnotežene nepotpune blokovne dizajne, te su navedeni primjeri blokovnih dizajna. Zatim je na dva načina dokazana Fisherova nejednakost korištenjem matrica incidencije. Na kraju, definirani su simetrični blokovni dizajni, te su iskazani teoremi koji predstavljaju jednostavne načine konstruiranja novih blokovnih dizajna iz starih.

U drugom poglavlju obrađeni su Steinerovi sustavi trojki. Dokazani su nužni i dovoljni uvjeti za egzistenciju sustava. Dovoljni uvjeti dobivaju se Boseovom i Skolemovom konstrukcijom korištenjem latinskih kvadrata i kvazigrupa. Definirani su izomorfizmi i automorfizmi koji se koriste za prebrojavanje sustava. Iskazan je teorem o približnom broju Steinerovih sustava trojki proizvoljnog reda, do na izomorfizam, te su navedeni primjeri automorfizama sustava dobivenih Boseovom i Skolemovom konstrukcijom.

U trećem poglavlju obrađen je Stinsonov algoritam, dani su njegov opis, implementacija i nekoliko rezultata izvršavanja, te je promatrana složenost algoritma.

Zahvala

Ovom prilikom zahvaljujem se mojoj obitelji

teti Grozdani i tati Damiru,

na pruženoj potpori tijekom cijelog svog školovanja, te mojoj djevojci

Ivani Urban,

na podršci i strpljenju tijekom studija.

Također, zahvaljujem se svim profesoricama i profesorima osnovne škole Silvije Strahimir Kranjčević, srednje škole III. gimnazija, te Matematičkog odjela Prirodoslovno-matematičkog fakulteta, koji su mi pružili potrebna znanja.

Posebne zahvale upućujem mojem voditelju

doc. dr. sc. Vedranu Krčadincu,

na uloženom trudu prilikom stvaranja diplomskog rada, te svima koji su na bilo koji način doprinijeli nastanku istog.

1. Teorija dizajna

Teorija dizajna je grana kombinatorne matematike koja nastoji pružiti odgovore na pitanja vezana uz mogućnost slaganja elemenata konačnog skupa u podskupove na način da su zadovoljena neka svojstva. Većina pitanja odnose se na samu egzistenciju, tj. za dano svojstvo pokušava se odrediti postoje li podskupovi koji ga zadovoljavaju. Druga pitanja odnose se na to koliko ima takvih familija podskupova, koja su njihova obilježja, itd. Postoji mnogo vrsta dizajna, primjerice, uravnoteženi nepotpuni blokovski dizajni, spareni uravnoteženi dizajni, grupno djeljivi dizajni, poprečni (transverzalni) dizajni, ortogonalna polja i mnogi drugi. Premda je poznato puno rezultata vezanih za pojedinu vrstu dizajna, još je uvijek dosta problema ostalo neriješeno.

Teorija dizajna vuče svoje korijene još iz 17.-og i 18.-og stoljeća kada su veliki matematički umovi tog vremena pokušavali riješiti matematičke slagalice i mozgalice. Pravi zamah teorija dizajna doživjela je početkom 20.-og stoljeća kada se javila potreba za oblikovanjem i analizom statističkih eksperimenata. Postoje i druge primjene kao, naprimjer, planiranje turnira, lutrija, matematička biologija, oblikovanje i analiza algoritama, rad s mrežom računala, te kriptografija.

1.1. *Dizajni*

Dizajni se sastoje od osnovnog skupa elemenata i multiskupa nepraznih podskupova sastavljenih od tih elemenata. Ono po čemu se dizajni razlikuju od proizvoljne kolekcije podskupova jest uvjet uravnoteženosti ili pravilnosti u nekom smislu. Naprimjer, jednakost veličina podskupova, ili broja podskupova u kojima je sadržan svaki t-podskup, ili veličina presjeka parova podskupova.

Definicija 1.1. Dizajn *je par* $(\mathcal{X}, \mathcal{A})$*, gdje su*

- $\mathcal{X}$ *skup elemenata koji se nazivaju* **točkama**,
- $\mathcal{A}$ *multiskup nepraznih podskupova od* $\mathcal{X}$ *koji se nazivaju* **blokovima** *ili* **pravcima**.

Definicija 1.2. *Dva identična bloka nazivaju se* **ponavljanim blokovima**.

Napomena 1.1. *Budući da mogu postojati ponavljani blokovi,* $\mathcal{A}$ *je definiran kao multiskup blokova, a ne kao skup.*

Definicija 1.3. *Dizajn se naziva* **jednostavanim dizajnom** *ukoliko ne sadrži ponavljane blokove.*

1.2. *Uravnoteženi nepotpuni blokovni dizajni*

Uravnoteženi nepotpuni blokovni dizajni su vrsta dizajna koja se vjerojatno najviše istražuje. Sustavno proučavanje uravnoteženih nepotpunih blokovnih dizajna započeli su Fisher i Yates 1930. godine.

Definicija 1.4. *Neka su v, k, λ pozitivni cijeli brojevi takvi da je $v > k \geq 2$. Tada je* (v, k, λ)**-uravnoteženi nepotpuni blokovni dizajn** *(eng.* **balanced incomplete block design***), ili ukratko* (v, k, λ)**-BIBD**, *odnosno* (v, k, λ)**-blokovni dizajn**, *dizajn $(\mathcal{X}, \mathcal{A})$ takav da vrijedi*

- *postoji točno v točaka,*
- *svaki blok sadrži točno k točaka,*
- *svake dvije točke sadržane su u točno λ blokova.*

Riječ „uravnoteženi“ proizlazi iz trećeg svojsta prethodne definicije koje se naziva ***svojstvom ravnoteže***.

Riječ „nepotpuni“ proizlazi iz uvjeta $v > k$ prethodne definicije pa se svi blokovi dizajna nazivaju ***nepotpunim blokovima***. Dakle, ni jedan blok ne sadrži sve točke. Ako bi vrijedilo $v = k$, onda bi svi uvjeti bili trivijalno zadovoljeni pa takav dizajn ne bi bio od posebnog interesa.

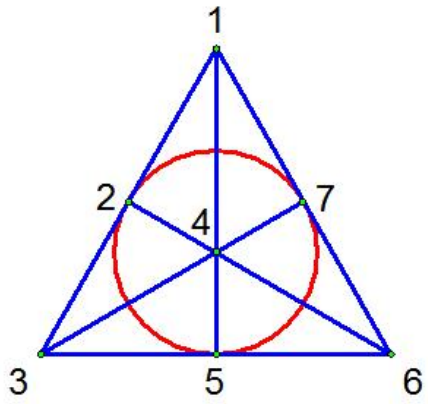
Napomena 1.2. *U daljnjem tekstu, umjesto „uravnoteženi nepotpuni blokovni dizajn“, kao kraći zapis, koristiti će se „blokovni dizajn“.*

Slijedi nekoliko primjera blokovnih dizajna.

Primjer 1.1. $(7,3,1)$*-BIBD je dizajn* $(\mathcal{X},\mathcal{A})$*, gdje su*

- $\mathcal{X} = \{1,2,3,4,5,6,7\}$,
- $\mathcal{A} = \{123, 145, 167, 246, 257, 347, 356\}$.

Navedeni blokovni dizajn može se prikazati dijagramom. Blokovi su šest linija i kružnica unutar trokuta.

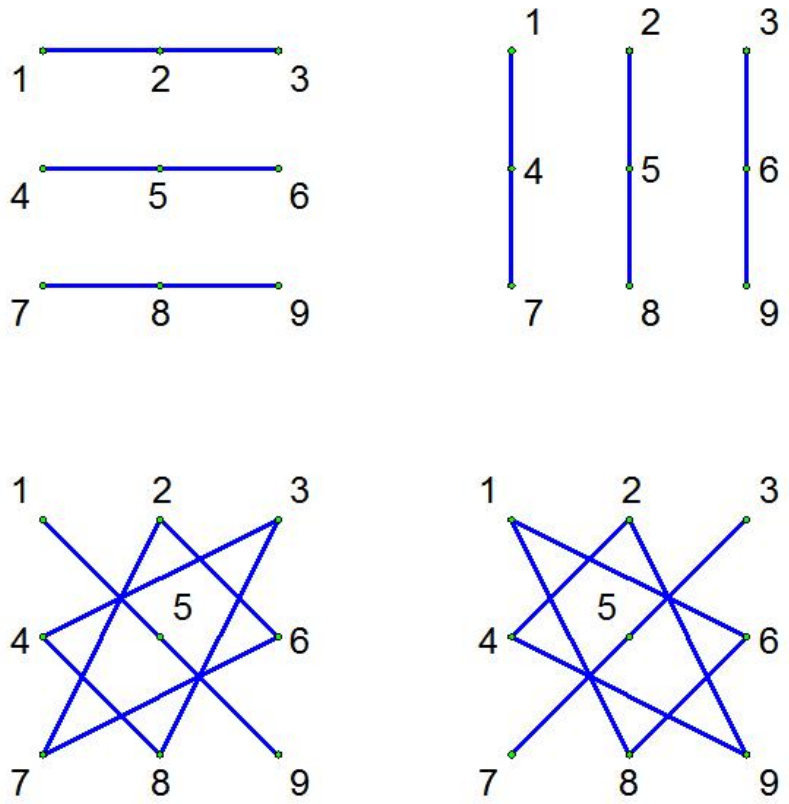


Slika 1. $(7,3,1)$-BIBD dijagram.

Primjer 1.2. $(9, 3, 1)$-*BIBD je dizajn* $(\mathcal{X}, \mathcal{A})$*, gdje su*

- $\mathcal{X} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$,
- $\mathcal{A} = \{123, 456, 789, 147, 258, 369, 159, 267, 348, 168, 249, 357\}$.

Navedeni blokovni dizajn može se, također, prikazati dijagramom. Blokovi su osam linija i četiri trokuta. Dijagram je podijeljen na četiri dijela od kojih svaki sadrži tri bloka.



Slika 2. $(9, 3, 1)$-BIBD dijagram.

Primjer 1.3. $(10, 4, 2)$-*BIBD je dizajn* $(\mathcal{X}, \mathcal{A})$*, gdje su*

- $\mathcal{X} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$,
- $\mathcal{A} = \{0123, 0145, 0246, 0378, 0579, 0689, 1278, 1369, 1479, 1568,$
  $2359, 2489, 2567, 3458, 3467\}$.

Ako vrijedi $\lambda = 1$, onda blokovni dizajn ne sadrži ponavljane blokove.

Primjer 1.4. $(7, 3, 2)$*-BIBD je dizajn* $(\mathcal{X}, \mathcal{A})$ *koji sadrži ponavljane blokove, gdje su*

- $\mathcal{X} = \{1, 2, 3, 4, 5, 6, 7\}$,
- $\mathcal{A} = \{\underline{123}, 145, 167, 246, 257, 347, 356, \underline{123}, 147, 156, 245, 267, 346, 357\}$.

Primjer 1.5. $(v, k, \binom{v-2}{k-2})$*-blokovni dizajn je dizajn* $(\mathcal{X}, \mathcal{A})$ *u kojem se* $\mathcal{A}$ *sastoji od svih* k*-podskupova od* $\mathcal{X}$*.*

Teorem 1.1. *U (v, k, λ)-blokovnom dizajnu svaka točka sadržana je u točno*

$$r = \frac{(v-1)\lambda}{k-1}$$

blokova.

Dokaz. Neka je $(\mathcal{X}, \mathcal{A})$ (v, k, λ)-blokovni dizajn, $x \in \mathcal{X}$ čvrsta točka, te r_x broj blokova koji sadrže x. Definira se skup

$$K := \{(y, A) | y \in \mathcal{X}, y \neq x, A \in \mathcal{A}, \{x, y\} \subseteq A\}.$$

Tada se računa $|K|$ na dva različita načina.

Prvo, postoji $v - 1$ načina za izbor $y \in \mathcal{X}$ takvih da je $y \neq x$, a za svaki takav y postoji λ blokova A takvih da je $\{x, y\} \subseteq A$. Stoga vrijedi

$$|K| = (v-1)\lambda.$$

Drugo, postoji r_x načina za izbor bloka $A \in \mathcal{A}$ takvih da je $x \in A$, a za svaki takav A postoji $k - 1$ načina za izbor $y \in A$, $y \neq x$. Stoga vrijedi

$$|K| = r_x(k-1).$$

Uvrštavanjem, iz navedenih jednadžbi dobiva se

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

te je rezultat nezavisan od izbora točke x, odakle slijedi tvrdnja.

□

Broj r naziva se ***replikacijskim brojem*** blokovnog dizajna.

Teorem 1.2. *(v, k, λ)-blokovni dizajn sadrži točno*

$$b = \frac{vr}{k} = \frac{v(v-1)\lambda}{k(k-1)}$$

blokova.

Dokaz. Neka je $(\mathcal{X}, \mathcal{A})$ (v, k, λ)-blokovni dizajn, te $b = |\mathcal{A}|$. Definira se skup

$$L := \{(x, A) | x \in \mathcal{X}, A \in \mathcal{A}, x \in A\}.$$

Tada se računa $|L|$ na dva različita načina.

Prvo, postoji v načina za izbor $x \in \mathcal{X}$, a za svaki takav x postoji r blokova A takvih da je $x \in A$. Stoga vrijedi

$$|L| = vr.$$

Drugo, postoji b načina za izbor bloka $A \in \mathcal{A}$, a za svaki takav A postoji k načina za izbor $x \in A$. Stoga vrijedi

$$|L| = bk.$$

Uvrštavanjem, iz navedenih jednadžbi dobiva se

$$vr = bk,$$

odakle slijedi tvrdnja.

□

Blokovni dizajni su obično određeni s pet parametara. To su broj točaka (v, od eng. variety), broj blokova (b), replikacijski broj (r), veličina blokova (k) i indeks (λ). Stoga se blokovni dizajn često naziva (v, b, r, k, λ)-***blokovnim dizajnom***. Međutim, tih pet parametara nisu međusobno nezavisni, jer se b i r mogu izračunati iz v, k i λ. Zato se umjesto „(v, b, r, k, λ)-blokovni dizajn“ može koristiti zapis „(v, k, λ)-blokovni dizajn“.

Budući da b i r moraju biti cijeli brojevi, prethodna dva teorema dovode do zaključka da ne postoje blokovni dizajni s određenim parametrima.

Korolar 1.1. *Ako postoji* (v, k, λ)*-blokovni dizajn, onda vrijedi*

$$(v-1)\lambda \equiv 0 (mod\ k-1)$$

i

$$v(v-1)\lambda \equiv 0 (mod\ k(k-1)).$$

Primjer 1.6. *Ne postoji* $(8, 3, 1)$*-BIBD jer vrijedi*

$$(v-1)\lambda = 7 \not\equiv 0 (mod\ k-1) = 0 (mod\ 2).$$

Također, ne postoji $(19, 4, 1)$*-BIBD jer vrijedi*

$$v(v-1)\lambda = 342 \not\equiv 0 (mod\ k(k-1)) = 0 (mod\ 12).$$

Jedan od glavnih ciljeva teorije dizajna je utvrđivanje nužnih i dovoljnih uvjeta za postojanje (v, k, λ)-blokovnih dizajna. To je općenito težak problem jer za mnoge skupove parametara nije poznato rješenje. Primjerice, nije poznato postoji li $(51, 6, 1)$-BIBD. Takav blokovni dizajn imao bi vrijednosti $b = 102$ i $r = 10$.

1.3. *Matrice incidencije*

Za prikazivanje blokovnog dizajna često se koristi matrica incidencije.

Definicija 1.5. *Neka je* $(\mathcal{X}, \mathcal{A})$ (v, b, r, k, λ)*-blokovni dizajn, gdje su* $\mathcal{X} = \{x_1, ..., x_v\}$ *i* $\mathcal{A} = \{A_1, ..., A_b\}$*. Tada je* **matrica incidencije** *od* $(\mathcal{X}, \mathcal{A})$ *matrica* $M = (m_{i,j})$*,* $m_{i,j} \in \{0, 1\}$*, reda* $v \times b$*, definirana sa*

$$m_{i,j} := \begin{cases} 1, & za\ x_i \in A_j \\ 0, & za\ x_i \notin A_j \end{cases}.$$

Primjer 1.7. $(9, 3, 1)$*-BIBD iz primjera 1.2 ima matricu incidencije reda* 9×12*.*

$$M = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Slika 3. Matrica incidencije $(9, 3, 1)$-BIBD-a.

Matrica incidencije M (v, b, r, k, λ)-blokovnog dizajna zadovoljava sljedeća svojstva:

- svaki redak od M sadrži točno r jedinica;
- svaki stupac od M sadrži točno k jedinica;
- svaka dva retka od M sadrže jedinice u točno λ stupaca.

Teorem 1.3. *Neka je E_n jedinična matrica reda $n \times n$ (matrica koja na dijagonali ima znamenku 1, dok na ostalim mjestima ima znamenku 0), F_n matrica reda $n \times n$ i u_n vektor reda n koji na svim mjestima imaju znamenku 1, te M^τ transponirana matrica reda $v \times b$ matrice $M = (m_{i,j})$, $m_{i,j} \in \{0, 1\}$. Tada je M incidentna matrica (v, b, r, k, λ)-blokovnog dizajna, $2 \leq k < v$, ako i samo ako vrijedi*

$$MM^\tau = (r - \lambda)E_v + \lambda F_v$$

i

$$u_v M = k u_b.$$

Dokaz. ($\Rightarrow$) Neka je $(\mathcal{X}, \mathcal{A})$ (v, k, λ)-blokovni dizajn, gdje su $\mathcal{X} = \{x_1, ..., x_v\}$ i $\mathcal{A} = \{A_1, ..., A_b\}$, te M matrica incidencije od $(\mathcal{X}, \mathcal{A})$.

Matrica MM^τ na poziciji (i, j) ima vrijednost

$$\sum_{l=1}^{b} m_{i,l} m_{j,l} = \begin{cases} r, & \text{za } i = j \\ \lambda, & \text{za } i \neq j \end{cases}.$$

Tada, zbog drugog i trećeg svojstva matrice incidencije, MM^τ na dijagonali ima vrijednost r, dok na ostalim mjestima ima vrijednost λ. Stoga vrijedi

$$MM^\tau = (r - \lambda)E_v + \lambda F_v.$$

Nadalje, vektor $u_v M$ na poziciji (i) ima vrijednost jednaku broju jedinica i-tog stupca od M. Tada, zbog prvog svojstva matrice incidencije, navedena vrijednost iznosi k. Stoga vrijedi

$$u_v M = k u_b.$$

($\Leftarrow$) Neka je matrica $M = (m_{i,j})$, $m_{i,j} \in \{0, 1\}$, reda $v \times b$ takva da su $MM^\tau = (r - \lambda)E_v + \lambda F_v$ i $u_v M = k u_b$, te $(\mathcal{X}, \mathcal{A})$ blokovni dizajn čija je pripadna matrica incidencije M. Očito je $|\mathcal{X}| = v$ i $|\mathcal{A}| = b$. Tada iz jednadžbe $u_v M = k u_b$ slijedi da svaki blok u $\mathcal{A}$ sadrži točno k točaka, te iz jednadžbe $MM^\tau = (r - \lambda)E_v + \lambda F_v$ slijedi da su svake dvije točke sadržane u točno λ blokova, a svaka točka sadržana je u točno r blokova. Stoga je $(\mathcal{X}, \mathcal{A})$ (v, b, r, k, λ)-blokovni dizajn.

□

Napomena 1.3. *Obrat prethodnog teorema ne vrijedi ukoliko se izostavi drugo svojstvo matrice incidencije.*

Definicija 1.6. *Neka je* $(\mathcal{X}, \mathcal{A})$ *dizajn takav da su* $|\mathcal{X}| = v$ *i* $|\mathcal{A}| = b$*, te* M *matrica incidencije od* $(\mathcal{X}, \mathcal{A})$*. Tada se dizajn čija je matrica incidencije* M^τ *naziva* **dualnim dizajnom** *od* $(\mathcal{X}, \mathcal{A})$*.*

Ako je $(\mathcal{Y}, \mathcal{B})$ dualni dizajn od $(\mathcal{X}, \mathcal{A})$, onda vrijedi $|\mathcal{Y}| = |\mathcal{A}| = b$ i $|\mathcal{B}| = |\mathcal{X}| = v$.

Teorem 1.4. *Neka je* $(\mathcal{X}, \mathcal{A})$ (v, b, r, k, λ)*-blokovni dizajn, te* $(\mathcal{Y}, \mathcal{B})$ *dualni dizajn od* $(\mathcal{X}, \mathcal{A})$*. Tada su zadovoljena sljedeća svojstva:*

- *svaki blok u* $\mathcal{B}$ *ima veličinu* r*;*
- *svaka točka u* $\mathcal{Y}$ *sadržana je u točno* k *blokova u* $\mathcal{B}$*;*
- *svaka dva bloka* $B_i, B_j \in \mathcal{B}$*,* $i \neq j$*, sjeku se u točno* λ *točaka.*

Primjer 1.8. *Neka je* $(\mathcal{X}, \mathcal{A})$ $(9, 3, 1)$*-BIBD iz primjera 1.2. Tada je* $(\mathcal{Y}, \mathcal{B})$ *dualni dizajn od* $(\mathcal{X}, \mathcal{A})$*, gdje su*

- $\mathcal{Y} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, T, U, V\}$,
- $\mathcal{B} = \{147T, 158U, 169V, 248U, 257V, 268T, 348V, 359T, 367U\}$.

Svaki blok u $\mathcal{B}$ *ima veličinu* $r = 4$*, svaka točka u* $\mathcal{Y}$ *sadržana je u točno* $k = 3$ *blokova u* $\mathcal{B}$ *i svaka dva bloka* $B_i, B_j \in \mathcal{B}$*,* $i \neq j$*, sjeku se u točno* $\lambda = 1$ *točki.*

1.4. *Fisherova nejednakost*

Teorem 1.5 (Fisher)**.** *Za svaki* (v, b, r, k, λ)*-blokovni dizajn vrijedi*

$$b \geq v.$$

Navedena nejednakost naziva se ***Fisherovom nejednakošću***.

Prvi dokaz je linearno-algebarski.

Dokaz. Neka je $(\mathcal{X}, \mathcal{A})$ (v, b, r, k, λ)-blokovni dizajn, gdje su $\mathcal{X} = \{x_1, ..., x_v\}$ i $\mathcal{A} = \{A_1, ..., A_b\}$, M matrica incidencije od $(\mathcal{X}, \mathcal{A})$, te r_i i-ti redak i s_j j-ti stupac od M. $r_1, ..., r_b$ su v-dimenzionalni vektori realnog vektorskog prostora $\mathbb{R}^v$. Očito je $s_j = r_j^\tau$. Definiraju se skupovi

$$R := \{r_i | 1 \leq i \leq b\}$$

i

$$\mathcal{R} := \{\sum_{i=1}^{b} \alpha_i r_i | \alpha_1, ..., \alpha_b \in \mathbb{R}\}.$$

Također, definira se jedinični vektor $e_j \in \mathbb{R}^v$, $1 \leq j \leq v$ (vektor koji na j-tom mjestu ima znamenku 1, dok na ostalim mjestima ima znamenku 0). $\mathcal{R}$ sadrži sve linearne kombinacije vektora $r_1, ..., r_b$. Preciznije, $\mathcal{R}$ razapinju vektori $r_1, ..., r_b$, tj. svaki vektor iz $\mathcal{R}$ može se prikazati kao linearna kombinacija vektora iz R. Vektori $e_1, ..., e_v$ tvore kanonsku bazu u $\mathbb{R}^v$.

Tada je potrebno pokazati da vrijedi $\mathcal{R} = \mathbb{R}^v$. Naime, ako b vektora iz R razapinje $\mathbb{R}^v$ dimenzije v, onda mora vrijediti $b \geq v$.

U protivnom, kako se svaki vektor iz $\mathbb{R}^v$ može prikazati kao linearna kombinacija vektora iz R, to se jedinični vektori kanonske baze u $\mathbb{R}^v$, također, mogu prikazati kao linearna kombinacija vektora iz R. Međutim, zbog $b < v$, barem jedan od vektora $e_1, ..., e_v$ je linearno zavisan s nekim drugim jediničnim vektorom, a to je u kontradikciji s činjenicom da su vektori kanonske baze međusobno linearno nezavisni.

Da bi se dokazala jednakost $\mathcal{R} = \mathbb{R}^v$, mora se dokazati $\mathcal{R} \subseteq \mathbb{R}^v$ i $\mathcal{R} \supseteq \mathbb{R}^v$.

($\mathcal{R} \subseteq \mathbb{R}^v$) Trivijalno, iz definicije skupa $\mathcal{R}$ slijedi da je $\mathcal{R}$ potprostor od $\mathbb{R}^v$.

($\mathcal{R} \supseteq \mathbb{R}^v$) Kako vektori $e_1, ..., e_v$ tvore kanonsku bazu u $\mathbb{R}^v$, to se svaki vektor iz $\mathbb{R}^v$ može prikazati kao linearna kombinacija navedenih jediničnih vektora. Stoga je dovoljno pokazati da se svaki vektor e_j može prikazati kao linearna kombinacija vektora iz R, tj. da vrijedi $e_j \in \mathcal{R}$, $1 \leq j \leq v$. Prvo, iz jednadžbe

$$\sum_{i=1}^{b} r_i = (r, ..., r)$$

slijedi

$$\sum_{i=1}^{b} \frac{1}{r} r_i = (1, ..., 1).$$

Drugo, za proizvoljan j, $1 \leq j \leq v$, vrijedi

$$\sum_{\{i | x_j \in A_i\}} r_i = (r - \lambda)e_j + (\lambda, ..., \lambda).$$

Budući da je $(v-1)\lambda = r(k-1)$ i $v > k$, slijedi da je $\lambda < r$, tj. $r - \lambda \neq 0$. Iz navedene dvije jednadžbe slijedi

$$e_j = \sum_{\{i|x_j \in A_i\}} \frac{1}{r-\lambda} r_i - \sum_{i=1}^{b} \frac{\lambda}{r(r-\lambda)} r_i.$$

Stoga se svaki vektor e_j može prikazati kao linearna kombinacija vektora iz R, odakle slijedi da je $\mathbb{R}^v$ potprostor od $\mathcal{R}$.

□

Drugi dokaz je linearno-algebarski korištenjem teorema 1.3.

Dokaz. Pretpostavi se suprotno, tj. da vrijedi $b < v$. Neka je M matrica incidencije blokovnog dizajna. Tada se dodavanjem $v - b$ stupaca koji se sastoje samo od znamenki 0 dobiva kvadratna matrica N reda $v \times v$. Kako nadodani stupci ne mijenjaju umnožak, to vrijedi

$$MM^\tau = NN^\tau.$$

Budući da je $\det(N) = 0$ zbog nadodanih stupaca, slijedi

$$\det(MM^\tau) = \det(NN^\tau) = 0.$$

Prema teoremu 1.3 vrijedi

$$MM^\tau = (r-\lambda)E_v + \lambda F_v = \begin{pmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{pmatrix}.$$

Nadalje, potrebno je izračunati determinantu od MM^τ. U tu svrhu, od ostalih stupaca oduzme se prvi stupac, a zatim se prvi redak zbroji s ostalim recima.

$$\det(MM^\tau) = \begin{pmatrix} r & \lambda - r & \lambda - r & \cdots & \lambda - r \\ \lambda & r - \lambda & 0 & \cdots & 0 \\ \lambda & 0 & r - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \cdots & r - \lambda \end{pmatrix}$$

$$\det(MM^\tau) = \begin{pmatrix} r + (v-1)\lambda & 0 & 0 & \cdots & 0 \\ \lambda & r - \lambda & 0 & \cdots & 0 \\ \lambda & 0 & r - \lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \cdots & r - \lambda \end{pmatrix}$$

Stoga vrijedi

$$\det(MM^\tau) = \underbrace{[r + (v-1)\lambda]}_{>0} \underbrace{(r - \lambda)^{v-1}}_{>0} > 0.$$

Kako su $v, r, \lambda > 0$, to vrijedi $r + (v-1)\lambda > 0$, a kako je $r > \lambda$ zbog uvjeta $v > k$ iz definicije 1.4 blokovnog dizajna, to vrijedi $(r - \lambda)^{v-1} > 0$. Dakle, slijedi $\det(MM^\tau) > 0$, a to je u kontradikciji s činjenicom $\det(MM^\tau) = 0$.

□

Prethodni teorem može se, također, iskazati na sljedeća dva ekvivalentna načina.

Korolar 1.2. *Za svaki* (v, b, r, k, λ)*-blokovni dizajn vrijedi*

$$r \geq k.$$

Korolar 1.3. *Za svaki* (v, b, r, k, λ)*-blokovni dizajn vrijedi*

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

Primjer 1.9. *Ne postoji* $(16, 6, 1)$*-BIBD. Naime, za navedeni blokovni dizajn vrijedi* $r = 3$ *i* $k = 6$*, tj.* $r < k$*. Međutim, to je u kontradikciji s činjenicom* $r \geq k$ *iz korolara 1.2.*

1.5. *Simetrični blokovni dizajni*

Definicija 1.7. *Blokovni dizajn u kojem je* $b = v$ *ili, ekvivalentno,* $r = k$*, odnosno* $(v-1)\lambda = k(k-1)$*, naziva se* **simetričnim blokovnim dizajnom**.

Napomena 1.4. *Svojstvo simetričnosti odnosi se na blokovni dizajn, ali ne i na njegovu matricu incidencije, tj. da je proizvoljni blokovni dizajn simetričan ne znači nužno da je i njegova matrica incidencije simetrična.*

Primjer 1.10. $(v, k, \binom{v-2}{k-2})$*-blokovni dizajn iz primjera 1.5 za* $k = v-1$ *je simetrični* $(v, v-1, v-2)$*-blokovni dizajn.*

Sljedeći teorem govori o presjeku blokova simetričnog blokovnog dizajna.

Teorem 1.6. $(\mathcal{X}, \mathcal{A} = \{A_1, ..., A_b\})$ *je simetrični* (v, k, λ)*-blokovni dizajn ako i samo ako vrijedi* $|A_i \cap A_j| = \lambda$*,* $1 \leq i, j \leq v$*,* $i \neq j$*.*

Dokaz. ($\Rightarrow$) Koristi se notacija iz prvog dokaza Fisherovog teorema 1.5.

Neka je l proizvoljan, $1 \leq l \leq b$.

Iz jednadžbi

$$\sum_{i=1}^{b} \frac{1}{r} r_i = (1, ..., 1)$$

i

$$\sum_{\{i|x_j \in A_i\}} r_i = (r - \lambda)e_j + (\lambda, ..., \lambda)$$

slijedi

$$\begin{aligned} \sum_{\{j|x_j \in A_l\}} \sum_{\{i|x_j \in A_i\}} r_i &= \sum_{\{j|x_j \in A_l\}} ((r - \lambda)e_j + (\lambda, ..., \lambda)) \\ &= (r - \lambda)r_l + k(\lambda, ..., \lambda) \\ &= (r - \lambda)r_l + \sum_{i=1}^{b} \frac{k\lambda}{r} r_i \end{aligned} .$$

Navedena dvostruka suma može se, također, izračunati na način da se zamijeni poredak sumiranja, tj.

$$\begin{aligned} \sum_{\{j|x_j \in A_l\}} \sum_{\{i|x_j \in A_i\}} r_i &= \sum_{i=1}^{b} \sum_{\{j|x_j \in A_l \cap A_i\}} r_i \\ &= \sum_{i=1}^{b} |A_l \cap A_i| r_i \end{aligned} .$$

Izjednačavanjem navedenih dviju jednadžbi dobiva se

$$(r - \lambda)r_l + \sum_{i=1}^{b} \frac{k\lambda}{r} r_i = \sum_{i=1}^{b} |A_l \cap A_i| r_i,$$

odakle, zbog $b = v$ i $r = k$, slijedi

$$(r - \lambda)r_l + \sum_{i=1}^{v} \lambda r_i = \sum_{i=1}^{v} |A_l \cap A_i| r_i.$$

U prvom dokazu Fisherovog teorema 1.5 pokazano je da vrijedi $\mathcal{R} = \mathbb{R}^v$, gdje je

$$\mathcal{R} := \{\sum_{i=1}^{b} \alpha_i r_i | \alpha_1, ..., \alpha_b \in \mathbb{R}\}.$$

Kako vrijedi $b = v$, to je $\mathcal{R}$ baza u $\mathbb{R}^v$. Budući da je $\mathcal{R}$ baza u $\mathbb{R}^v$, slijedi da koeficijenti bilo kojeg vektora r_i s lijeve i s desne strane jednadžbe moraju biti jednaki. Tada je $|A_l \cap A_i| = \lambda$, $i \neq l$. Međutim, l je proizvoljan pa slijedi $|A_i \cap A_j| = \lambda$, $1 \leq i, j \leq v$, $i \neq j$.

($\Leftarrow$) Neka je $(\mathcal{X}, \mathcal{A})$ (v, b, r, k, λ)-blokovni dizajn, te $|A_i \cap A_j| = \kappa$, $1 \leq i, j \leq v$, $i \neq j$. Prema teoremu 1.4 dualni dizajn od $(\mathcal{X}, \mathcal{A})$ je (b, v, k, r, κ)-blokovni dizajn. Iz Fisherove nejednakosti za $(\mathcal{X}, \mathcal{A})$ slijedi $b \geq v$, te za dualni dizajn od $(\mathcal{X}, \mathcal{A})$ slijedi $v \geq b$. Tada su $b = v$ i $\kappa = \lambda$.

□

Sljedeći korolar je direktna posljedica prethodnog teorema.

Korolar 1.4. *Dualni dizajn simetričnog blokovnog dizajna je ponovno simetrični blokovni dizajn.*

Napomena 1.5. *Navedena dva simetrična blokovna dizajna ne moraju biti ni identična ni izomorfna.*

Teorem 1.7 (Bruck-Ryser-Chowla/v paran)**.** *Neka postoji simetrični* (v, k, λ)*-blokovni dizajn, gdje je* v *paran. Tada je* $k - \lambda$ *potpun kvadrat.*

Primjer 1.11. *Ne postoji* $(22, 7, 2)$*-BIBD.*

Dokaz. Kada bi navedeni blokovni dizajn postojao, bio bi simetričan jer vrijedi $(22 - 1)2 = 7(7 - 1)$. Također, 22 je paran broj. Prema prethodnom teoremu, $7 - 2 = 5$ je potpun kvadrat. Međutim, 5 nije potpun kvadrat, a to je u kontradikciji s tvrdnjom prethodnog teorema. Stoga takav blokovni dizajn ne postoji.

□

Teorem 1.8 (Bruck-Ryser-Chowla/v neparan)**.** *Neka postoji simetrični* (v, k, λ)*-blokovni dizajn, gdje je* v *neparan. Tada postoje cijeli brojevi* x*,* y *i* z *koji nisu svi jednaki* 0 *takvi da je*

$$x^2 = (k - \lambda)y^2 + (-1)^{\frac{v-1}{2}}\lambda z^2.$$

Primjer 1.12. *Ne postoji* $(43, 7, 1)$*-BIBD.*

Dokaz. Kada bi navedeni blokovni dizajn postojao, bio bi simetričan jer vrijedi $(43 - 1)1 = 7(7 - 1)$. Također, 43 je neparan broj. Prema prethodnom teoremu, postoje cijeli brojevi x, y i z koji nisu svi jednaki 0 takvi da je

$$x^2 = 6y^2 - z^2.$$

Iz navedene jednadžbe slijedi

$$x^2 + z^2 \equiv 0(mod\ 3).$$

Kako je $x^2 \equiv 0, 1(mod\ 3)$, to je $x \equiv 0(mod\ 3)$ jedino moguće rješenje. Analogno, $z \equiv 0(mod\ 3)$ je jedino moguće rješenje. Neka su $x = 3x_1$ i $z = 3z_1$. Tada je

$$(3x_1)^2 + (3z_1)^2 = 6y^2,$$

odnosno

$$3x_1^2 + 3z_1^2 = 2y^2.$$

Kako je $3x_1^2 + 3z_1^2 \equiv 0(mod\ 3)$, to je $y \equiv 0(mod\ 3)$ jedino moguće rješenje. Neka je $y = 3y_1$. Tada je

$$3x_1^2 + 3z_1^2 = 2(3y_1)^2,$$

odnosno

$$x_1^2 + z_1^2 = 6y^2.$$

Dakle, ako je (x, y, z) cjelobrojno rješenje, onda je i $(\frac{x}{3}, \frac{y}{3}, \frac{z}{3})$ cjelobrojno rješenje. Navedeni postupak može se ponavljati u beskonačnost. Dakle, jedino cjelobrojno rješenje jednadžbe je $(x, y, z) = (0, 0, 0)$, a to je u kontradikciji s tvrdnjom prethodnog teorema. Stoga takav blokovni dizajn ne postoji.

□

1.6. *Novi blokovni dizajni iz starih*

Sljedeća tri teorema predstavljaju jednostavne načine konstruiranja novih blokovnih dizajna iz starih.

Prvi teorem predstavlja konstrukciju uzimanjem unije blokova.

Teorem 1.9. *Neka postoje* (v, k, λ_1)*-blokovni dizajn i* (v, k, λ_2)*-blokovni dizajn. Tada postoji* $(v, k, \lambda_1 + \lambda_2)$*-blokovni dizajn.*

Korolar 1.5. *Neka postoji* (v, k, λ)*-blokovni dizajn. Tada postoji* $(v, k, s\lambda)$*-blokovni dizajn za sve cijele brojeve* $s \geq 1$*.*

Primjer 1.13. *Kako postoje* $(16, 6, 2)$*-BIBD i i* $(16, 6, 3)$*-BIBD, to postoji i* $(16, 6, 5)$*-BIBD.*

Napomena 1.6. *Iz primjera 1.9 i prethodnog primjera slijedi da postoje* $(16, 6, \lambda)$*-blokovni dizajni ako i samo ako vrijedi* $\lambda > 1$*.*

Drugi teorem predstavlja konstrukciju uzimanjem komplementa blokova.

Teorem 1.10. *Neka postoji* (v, b, r, k, λ)*-blokovni dizajn,* $k \leq v - 2$*. Tada postoji* $(v, b, b - r, v - k, b - 2r + \lambda)$*-blokovni dizajn.*

Dokaz. Neka je $(\mathcal{X}, \mathcal{A})$ (v, b, r, k, λ)-blokovni dizajn. Tada je potrebno pokazati da se zamjenom svakog bloka $A \in \mathcal{A}$ sa $\mathcal{X} \setminus A$ ponovno dobiva blokovni dizajn, tj. da je

$$(\mathcal{X}, \{\mathcal{X} \setminus A | A \in \mathcal{A}\})$$

blokovni dizajn.

Očito, navedeni dizajn ima v točaka i b blokova, svaka točka sadržana je u točno $b - r$ blokova, te svaki blok sadrži točno $v - k \geq 2$ točaka. Stoga se još mora pokazati da su svake dvije točke sadržane u točno $b - 2r + \lambda$ blokova.

Neka su $x, y \in \mathcal{X}$, $x \neq y$. Definiraju se vrijednosti

$$w := |\{A \in \mathcal{A} | x, y \in A\}|,$$

$$x := |\{A \in \mathcal{A} | x \in A, y \notin A\}|,$$

$$y := |\{A \in \mathcal{A} | x \notin A, y \in A\}|,$$

$$z := |\{A \in \mathcal{A} | x, y \notin A\}|.$$

Tada vrijedi

$$w = \lambda,$$

$$w + x = r,$$

$$w + y = r,$$

$$w + x + y + z = b.$$

Rješavanjem navedenih četiriju jednadžbi dobiva se

$$z = b - 2r + \lambda.$$

□

Primjer 1.14. $(7, 3, 1)$*-BIBD iz primjera 1.1 ima za komplement blokovni dizajn s parametrima* $v = 7$*,* $k = 4$ *i* $\lambda = 2$*.*

Primjer 1.15. $(9, 3, 1)$*-BIBD iz primjera 1.2 ima za komplement blokovni dizajn s parametrima* $v = 9$*,* $k = 6$ *i* $\lambda = 5$*.*

Definicija 1.8. *Neka je* $(\mathcal{X}, \mathcal{A})$ *simetrični* (v, k, λ)*-blokovni dizajn, te* $A_0 \in \mathcal{A}$ *blok. Definiraju se skupovi*

$$Der(\mathcal{X}, \mathcal{A}, A_0) := (A_0, \{A \cap A_0 | A \in \mathcal{A}, A \neq A_0\}),$$

$$Res(\mathcal{X}, \mathcal{A}, A_0) := (\mathcal{X} \setminus A_0, \{A \setminus A_0 | A \in \mathcal{A}, A \neq A_0\}).$$

Tada se $Der(\mathcal{X}, \mathcal{A}, A_0)$ *i* $Res(\mathcal{X}, \mathcal{A}, A_0)$ *nazivaju* **derivirani blokovni dizajn**, *odnosno* **rezidualni blokovni dizajn**.

Derivirani blokovni dizajn konstruira se uklanjanjem svih točaka koje nisu dio bloka A_0, a zatim uklanjanjem i samog bloka A_0.

Rezidualni blokovni dizajn konstruira se uklanjanjem svih točaka bloka A_0.

Treći teorem predstavlja konstrukciju derivata i reziduala.

Teorem 1.11. *Neka je* $(\mathcal{X}, \mathcal{A})$ *simetrični* (v, k, λ)*-blokovni dizajn, te* $A_0 \in \mathcal{A}$ *blok. Tada su* $Der(\mathcal{X}, \mathcal{A}, A_0)$ *i* $Res(\mathcal{X}, \mathcal{A}, A_0)$ $(v-k, v-1, k, k-\lambda, \lambda)$*-blokovni dizajn, odnosno* $(k, v-1, k-1, \lambda, \lambda-1)$*-blokovni dizajn, uz uvjet* $\lambda \geq 2$*, odnosno* $\lambda \leq k-2$*.*

Dokaz. $Der(\mathcal{X}, \mathcal{A}, A_0)$ je blokovni dizajn koji ima k točaka, a blokovi imaju veličinu λ, uz uvjet $k > \lambda \geq 2$. Međutim, u simetričnom blokovnom dizajnu je uvijek $k > \lambda$, zbog $v > k$ i $(v-1)\lambda = k(k-1)$. Stoga je uvjet $k > \lambda$ nepotreban.

$Res(\mathcal{X}, \mathcal{A}, A_0)$ je blokovni dizajn koji ima $v-k$ točaka, a blokovi imaju veličinu $k-\lambda$, uz uvjet $v-k > k-\lambda \geq 2$. Potrebno je pokazati da u simetričnom blokovnom dizajnu vrijedi $v-k > k-\lambda$. Pretpostavi se suprotno. Neka je $v \leq 2k-\lambda$. Tada je

$$k(k-1) = (v-1)\lambda \leq (2k-\lambda-1),$$

tj.

$$(k-\lambda)(k-\lambda-1) \leq 0.$$

Međutim, k i λ su cijeli brojevi pa navedena nejednakost vrijedi ako i samo ako je $k = \lambda$ ili $k = \lambda + 1$, a to je u kontradikciji s činjenicom $k \geq \lambda + 2$. Stoga je uvjet $v - k > k - \lambda$ nepotreban.

□

Primjer 1.16. *Derivat simetričnog blokovnog dizajna s parametrima* $v = 11$, $k = 5$ *i* $\lambda = 2$ *je* $(5, 2, 1)$*-BIBD. Rezidual simetričnog blokovnog dizajna s parametrima* $v = 11$, $k = 5$ *i* $\lambda = 2$ *je* $(6, 3, 2)$*-BIBD.*

1	*3*	*4*	*5*	*9*
4	*5*	*2*	*6*	*10*
3	*5*	*6*	*7*	*0*
1	*4*	*6*	*7*	*8*
5	*9*	*2*	*7*	*8*
3	*9*	*6*	*8*	*10*
4	*9*	*0*	*7*	*10*
1	*5*	*0*	*8*	*10*
1	*9*	*2*	*6*	*0*
1	*3*	*2*	*7*	*10*
3	*4*	*0*	*2*	*8*

SLIKA 4. Derivat i rezidual simetričnog blokovnog dizajna s parametrima $v = 11$, $k = 5$ i $\lambda = 2$.

Simetrični $(11, 5, 2)$*-BIBD ima* 11 *blokova. Prvi blok je* $A_0 = \{1, 3, 4, 5, 9\}$. *Preostalih* 10 *blokova podijeljeno je na dva dijela koji tvore, redom,* $(5, 2, 1)$*-BIBD na skupu točaka* $\{1, 3, 4, 5, 9\}$ *i* $(6, 3, 2)$*-BIBD na skupu točaka* $\{0, 2, 6, 7, 8, 10\}$.

2. Steinerovi sustavi trojki

Definicija 2.1. Sustav trojki *(eng.* **triple system***), ili ukratko* **TS**(v, λ)*, je* (v, k, λ)*-blokovni dizajn s veličinom blokova* $k = 3$*.*

Definicija 2.2. Steinerov sustav trojki *(eng.* **Steiner triple system***), ili ukratko* **STS**(v)*, je TS*(v, λ) *s indeksom* $\lambda = 1$*.*

Budući da su za veličinu blokova $k = 2$ blokovni dizajni trivijalni, tj. sastoje se od svih dvočlanih podskupova v-članog skupa, Steinerovi sustavi trojki su najjednostavnija vrsta dizajna koja je zanimljiva za proučavanje. Primjeri 1.1 i 1.2 prikazuju STS(7), odnosno STS(9).

Sljedeći teorem govori o egzistenciji Steinerovih sustava trojki.

Teorem 2.1. *Postoji STS*(v) *ako i samo ako vrijedi* $v \equiv 1, 3 (mod\ 6)$*,* $v \geq 7$*.*

Dokaz. ($\Rightarrow$) Neka su $k = 3$ i $\lambda = 1$. Tada su, prema teoremu 1.1,

$$r = \frac{(v-1)\lambda}{k-1} = \frac{v-1}{2}$$

i, prema teoremu 1.2,

$$b = \frac{vr}{k} = \frac{v(v-1)}{6}.$$

Kako vrijedi

$$v = 2r + 1,$$

to je v neparan. Kako je b cijeli broj, to vrijedi

$$v(v-1) \equiv 0 (mod\ 6).$$

Navedena kongruencija vrijedi ako i samo ako je

$$v \equiv 0, 1, 3, 4 (mod\ 6).$$

No, budući da je v neparan, slijedi

$$v \equiv 1, 3 (mod\ 6).$$

Zbog uvjeta $v > k$ iz definicije 1.4 blokovnog dizajna, vrijedi $v \geq 7$.

($\Leftarrow$) Leme 2.5 i 2.6, tj. Boseova i Skolemova konstrukcija.

□

Napomena 2.1. *Tvrdnja teorema 2.1 o egzistenciji Steinerovih sustava trojki vrijedila bi i za svaki $v \geq 3$, $v \equiv 1, 3 (mod\ 6)$.*

Naime, STS(3) je dizajn $(\mathcal{X}, \mathcal{A})$, gdje su

- $\mathcal{X} = \{1, 2, 3\}$,
- $\mathcal{A} = \{123\}$.

Međutim, za $v = 3$, STS(v) je trivijalan pa nije od posebnog interesa.

2.1. *Latinski kvadrati i kvazigrupe*

Definicija 2.3. Latinski kvadrat *reda n čiji su članovi elementi n-članog skupa S je $n \times n$ matrica L_n u kojoj je svaki redak permutacija od S i svaki stupac permutacija od S.*

Konstrukcija latinskih kvadrata reda $n \geq 1$ je jednostavna. Primjerice, za prvi redak uzme se permutacija $(1, 2, ..., n)$, a zatim se navedeni redak ciklički pomiće udesno za $1, 2, ..., n-1$ da bi se dobilo preostalih $n-1$ redaka.

Primjer 2.1. *Latinski kvadrat reda* 4.

$$L_4 = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 4 & 1 & 2 & 3 \\ \hline 3 & 4 & 1 & 2 \\ \hline 2 & 3 & 4 & 1 \\ \hline \end{array}$$

Slika 5. Latinski kvadrat reda 4.

Definicija 2.4. *Neka je S konačan skup od n elemenata, te $\circ : S \times S \to S$ binarna operacija. Tada je par $(S, \circ)$* **kvazigrupa** *reda n ukoliko vrijedi da za sve $x, y \in S$ jednadžbe $x \circ z = y$ i $z \circ x = y$ imaju jedinstveno rješenje $z \in S$.*

Definicija 2.5. Operacijska tablica *binarne operacije* $\circ$ *definirane na skupu* S *je* $|S| \times |S|$ *matrica* $A = (a_{x,y})$*, gdje je* $a_{x,y} = x \circ y$*.*

Latinski kvadrati i kvazigrupe su u bliskoj vezi. Oni prikazuju dva različita načina gledanja na istu stvar. Sljedeći teorem predstavlja tu vezu.

Teorem 2.2. *Neka je* $\circ$ *binarna operacija definirana na konačnom skupu* S *kardinaliteta* n*. Tada je* $(S, \circ)$ *kvazigrupa ako i samo ako je pripadna operacijska tablica latinski kvadrat reda* n*.*

Sljedeća definicija predstavlja dva posebna svojstva za kvazigrupe, odnosno latinske kvadrate.

Definicija 2.6. *Ako vrijedi* $x \circ x = x$ *za sve* $x \in S$*, onda se* $(S, \circ)$ *naziva* **idempotentnom kvazigrupom**. *Ako vrijedi* $x \circ y = y \circ x$ *za sve* $x, y \in S$*, onda se* $(S, \circ)$ *naziva* **simetričnom kvazigrupom**.

Analogna svojstva definiraju se i za latinske kvadrate. Ako vrijedi $l_{x,x} = x$ *za sve* x*, onda se* $L = (l_{x,y})$ *naziva* **idempotentnim latinskim kvadratom**. *Ako vrijedi* $l_{x,y} = l_{y,x}$ *za sve* x, y*, onda se* $L = (l_{x,y})$ *naziva* **simetričnim latinskim kvadratom**.

Primjer 2.2. *Za $S = \{1, 2\}$ postoje točno dva latinska kvadrata definirana na skupu S.*

$$L_2^{(1)} = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 & 1 \\ \hline \end{array}$$

$$L_2^{(2)} = \begin{array}{|c|c|}\hline 2 & 1 \\ \hline 1 & 2 \\ \hline \end{array}$$

SLIKA 6. Latinski kvadrati definirani na skupu $\{1, 2\}$.

Oba latinska kvadrata su simetrična, ali ni jedan od njih nije idempotentan.

Primjer 2.3. *Za $S = \{1, 2, 3\}$ postoji točno dvanaest latinskih kvadrata definiranih na skupu S.*

$$L_3^{(1)} = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array} \quad L_3^{(5)} = \begin{array}{|c|c|c|}\hline 2 & 1 & 3 \\ \hline 1 & 3 & 2 \\ \hline 3 & 2 & 1 \\ \hline \end{array} \quad L_3^{(9)} = \begin{array}{|c|c|c|}\hline 3 & 1 & 2 \\ \hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline \end{array}$$

$$L_3^{(2)} = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline \end{array} \quad L_3^{(6)} = \begin{array}{|c|c|c|}\hline 2 & 1 & 3 \\ \hline 3 & 2 & 1 \\ \hline 1 & 2 & 3 \\ \hline \end{array} \quad L_3^{(10)} = \begin{array}{|c|c|c|}\hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline 1 & 2 & 3 \\ \hline \end{array}$$

$$L_3^{(3)} = \begin{array}{|c|c|c|}\hline 1 & 3 & 2 \\ \hline 2 & 1 & 3 \\ \hline 3 & 2 & 1 \\ \hline \end{array} \quad L_3^{(7)} = \begin{array}{|c|c|c|}\hline 2 & 3 & 1 \\ \hline 1 & 2 & 3 \\ \hline 3 & 1 & 2 \\ \hline \end{array} \quad L_3^{(11)} = \begin{array}{|c|c|c|}\hline 3 & 2 & 1 \\ \hline 1 & 3 & 2 \\ \hline 2 & 1 & 3 \\ \hline \end{array}$$

$$L_3^{(4)} = \begin{array}{|c|c|c|}\hline 1 & 3 & 2 \\ \hline 3 & 2 & 1 \\ \hline 2 & 1 & 3 \\ \hline \end{array} \quad L_3^{(8)} = \begin{array}{|c|c|c|}\hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline 1 & 2 & 3 \\ \hline \end{array} \quad L_3^{(12)} = \begin{array}{|c|c|c|}\hline 3 & 2 & 1 \\ \hline 2 & 1 & 3 \\ \hline 1 & 3 & 2 \\ \hline \end{array}$$

SLIKA 7. Latinski kvadrati definirani na skupu $\{1, 2, 3\}$.

Jedini idempotentni latinski kvadrat je $L_3^{(4)}$, dok su latinski kvadrati $L_3^{(1)}$, $L_3^{(4)}$, $L_3^{(5)}$, $L_3^{(8)}$, $L_3^{(9)}$ i $L_3^{(12)}$ simetrični.

Sljedeće leme predstavljaju nužan i dovoljan uvjet za postojanje idempotentne simetrične kvazigrupe reda n.

Lema 2.1. *Ako postoji idempotentna simetrična kvazigrupa reda n, onda je n neparan.*

Dokaz. Neka je $(S, \circ)$ idempotentna simetrična kvazigrupa reda n. Za $z \in S$ definira se skup

$$T := \{(x, y) | x \circ y = z\}.$$

Budući da je $\circ$ idempotentna binarna operacija, slijedi $(x, x) \in T$ ako i samo ako vrijedi $x = z$. Budući da je $\circ$ simetrična binarna operacija, slijedi $(x, y) \in T$ ako i samo ako vrijedi $(y, x) \in T$. Tada je skup $\{\{x, y\} | x \neq y, x \circ y = z\}$ particija od $S \setminus \{z\}$ u skupove veličine dva kojih ima $\frac{n-1}{2}$. Zato je $|S| - 1$ paran pa je $|S|$ neparan.

□

Lema 2.2. *Ako je n neparan, onda postoji idempotentna simetrična kvazigrupa reda n.*

Dokaz. Potrebno je dati konstrukciju idempotentne simetrične kvazigrupe za sve neparne redove. Neka je n neparan i $(\mathbb{Z}_n, +)$ aditivna grupa modulo n. Budući da je $(\mathbb{Z}_n, +)$ grupa, slijedi da je također i kvazigrupa. Simetrična je, zbog toga što je zbrajanje modulo n komutativno. Međutim, nije idempotentna, pa ju je potrebno prilagoditi.

Kako je n neparan, to je lista vrijednosti na glavnoj dijagonali operacijske tablice od $(\mathbb{Z}_n, +)$ dana sa

$$((x+x)(mod\ n)|x \in \mathbb{Z}_n) = (0, 2, 4, ..., n-1, 1, 3, 5, ..., n-2),$$

a to je permutacija od $\mathbb{Z}_n$. Stoga operacijska tablica od $(\mathbb{Z}_n, +)$ ima sve elemente od $\mathbb{Z}_n$ na glavnoj dijagonali, ali u krivom poretku. Poredak se može ispraviti permutiranjem simbola na način da dijagonalni elementi budu, redom, $0, 1, ..., n-1$. U tu svrhu, definira se permutacija π sa

$$\pi := \begin{pmatrix} 0 & 2 & \cdots & n-1 & 1 & 3 & \cdots & n-2 \\ 0 & 1 & \cdots & \frac{n-1}{2} & \frac{n+1}{2} & \frac{n+3}{2} & \cdots & n-1 \end{pmatrix},$$

tj.

$$\pi(x) := \begin{cases} \frac{x}{2}(mod\ n), & \text{za } x \text{ paran} \\ \frac{n+x}{2}(mod\ n), & \text{za } x \text{ neparan} \end{cases}.$$

Tada je jedna binarna operacija $\circ$ na skupu $\{0, 1, ..., n-1\}$, koja daje idempotentnu simetričnu kvazigrupu, definirana sa

$$x \circ y := (\frac{n+1}{2})(x+y)(mod\ n). \qquad \square$$

Primjer 2.4. *Neka je $n = 5$. Tada je binarna operacija $\circ$ iz dokaza prethodne leme, koja daje idempotentnu simetričnu kvazigrupu, definirana sa*

$$x \circ y := 3(x+y)(mod\ 5).$$

Pripadni latinski kvadrat je

$$L_5 = \begin{array}{|c|c|c|c|c|} \hline 0 & 3 & 1 & 4 & 2 \\ \hline 3 & 1 & 4 & 2 & 0 \\ \hline 1 & 4 & 2 & 0 & 3 \\ \hline 4 & 2 & 0 & 3 & 1 \\ \hline 2 & 0 & 3 & 1 & 4 \\ \hline \end{array}$$

Slika 8. Latinski kvadrat reda 5.

Prethodne leme predstavljaju rješenje problema konstrukcije idempotentnih simetričnih kvazigrupa. Koristiti će se prilikom Boseove konstrukcije Steinerovih sustava trojki.

Definicija 2.7. *Neka je* $(S, \circ)$ *kvazigrupa, te* $S = \{0, 1, ..., n-1\}$*, gdje je* n *paran. Tada, ako vrijedi*

$$x \circ x = \begin{cases} x, & za\ 0 \leq x < \frac{n}{2} \\ x - \frac{n}{2}, & za\ \frac{n}{2} \leq x < n \end{cases},$$

onda se $(S, \circ)$ *naziva* **poluidempotentnom kvazigrupom**.

Sljedeće leme predstavljaju nužan i dovoljan uvjet za postojanje poluidempotentne simetrične kvazigrupe reda n.

Lema 2.3. *Ako postoji poluidempotentna simetrična kvazigrupa reda* n*, onda je* n *paran.*

Dokaz. Direktno iz prethodne definicije vrijedi da je n paran.

□

Lema 2.4. *Ako je* n *paran, onda postoji poluidempotentna simetrična kvazigrupa reda* n*.*

Dokaz. Potrebno je dati konstrukciju poluidempotentne simetrične kvazigrupe za sve parne redove. Neka je n paran i $(\mathbb{Z}_n, +)$ aditivna grupa modulo n, iz dokaza leme 2.2, koju je potrebno prilagoditi.

Kako je n paran, to je lista vrijednosti na glavnoj dijagonali operacijske tablice od $(\mathbb{Z}_n, +)$ dana sa

$$((x+x)(mod\ n)|x \in \mathbb{Z}_n) = (0, 2, 4, ..., n-2, 0, 2, 4, ..., n-2),$$

tj. sadrži svaki paran element od $\mathbb{Z}_n$ točno dvaput. Stoga je potrebno permutirati simbole na način da dijagonalni elementi budu, redom, $0, 1, ..., \frac{n}{2}-1, 0, 1, ..., \frac{n}{2}-1$. U tu svrhu, definira se permutacija π sa

$$\pi := \begin{pmatrix} 0 & 2 & 4 & \cdots & n-2 & 0 & 2 & 4 & \cdots & n-2 \\ 0 & 1 & 2 & \cdots & \frac{n}{2}-1 & 0 & 1 & 2 & \cdots & \frac{n}{2}-1 \end{pmatrix},$$

tj.

$$\pi(x) := \begin{cases} \frac{x}{2}(mod\ n), & \text{za } x \text{ paran} \\ \frac{n+x-1}{2}(mod\ n), & \text{za } x \text{ neparan} \end{cases}.$$

Tada je jedna binarna operacija $\circ$ na skupu $\{0, 1, ..., n-1\}$, koja daje poluidempotentnu simetričnu kvazigrupu, definirana sa

$$x \circ y := \pi((x+y)(mod\ n)).$$

□

Primjer 2.5. *Neka je $n = 6$. Tada je permutacija π iz dokaza prethodne leme, koja daje poluidempotentnu simetričnu kvazigrupu, definirana sa*

$$\pi := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 3 & 1 & 4 & 2 & 5 \end{pmatrix}.$$

Pripadna operacijska tablica je

0	*3*	*1*	*4*	*2*	*5*
3	*1*	*4*	*2*	*5*	*0*
1	*4*	*2*	*5*	*0*	*3*
4	*2*	*5*	*0*	*3*	*1*
2	*5*	*0*	*3*	*1*	*4*
5	*0*	*3*	*1*	*4*	*2*

Slika 9. Operacijska tablica reda 6.

Prethodne leme predstavljaju rješenje problema konstrukcije poluidempotentnih simetričnih kvazigrupa. Koristiti će se prilikom Skolemove konstrukcije Steinerovih sustava trojki.

2.2. *Boseova konstrukcija*

Boseova konstrukcija je vrsta konstrukcije STS(v)-a za sve vrijednosti v takve da je $v \equiv 3(mod\ 6)$.

Neka je $v = 6u + 3$, $u \geq 1$, $S := \{0, 1, ..., 2u\}$, $(S, \circ)$ idempotentna simetrična kvazigrupa (neparnog) reda $2u + 1$, te "$<$" totalni uređaj definiran na skupu S. Definira se skup

$$\mathcal{Y} := S \times \mathbb{Z}_3,$$

koji će predstavljati skup točaka STS(v)-a koji se konstruira.

Za svaki $x \in S$ definira se blok

$$A_x := \{(x, 0), (x, 1), (x, 2)\}.$$

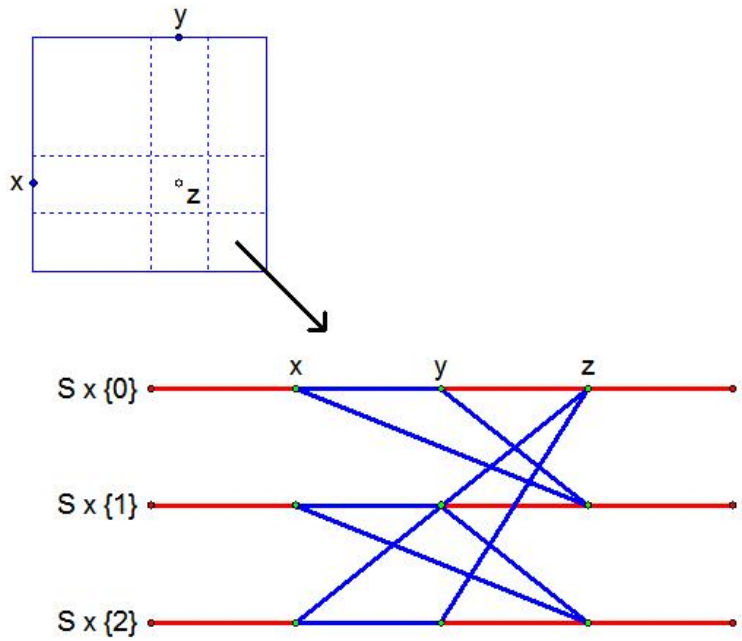
Za sve $x, y \in S$, $x < y$, i svaki $i \in \mathbb{Z}_3$ definira se blok

$$B_{x,y,i} := \{(x, i), (y, i), (x \circ y, i + 1(mod\ 3))\}.$$

Također, definira se skup blokova

$$\mathcal{B} := \{A_x | x \in S\} \cup \{B_{x,y,i} | x, y \in S, x < y, i \in \mathbb{Z}_3\}.$$

Sljedeća slika prikazuje kako se konstruiraju tri bloka koja odgovaraju jednom unosu operacijske tablice od $(S, \circ)$, primjerice $x \circ y = z$.



Slika 10. Boseova konstrukcija.

Tada je potrebno pokazati da je par $(\mathcal{Y}, \mathcal{B})$ Steinerov sustav trojki. Očito postoji v točaka u $\mathcal{Y}$ i svaki blok u $\mathcal{B}$ sadrži tri točke. Stoga je dovoljno pokazati da su svake dvije točke sadržane u točno jednom bloku.

Uzme se da su (α, k) i (β, l) dvije točke.

• Ako je $\alpha = \beta$, onda je $k \neq l$ i navedene dvije točke sadržane su samo u bloku A_α.

• Ako je $\alpha \neq \beta$, onda se bez smanjenja općenitosti može pretpostaviti da je $\alpha < \beta$ pa postoje tri slučaja:

1° $l = k$; Navedene dvije točke sadržane su samo u bloku $B_{\alpha,\beta,k}$.

2° $l = k + 1(mod\ 3)$; Jednadžba $x \circ \alpha = \beta$ ima jedinstveno rješenje $x = \gamma$. Budući da je $\alpha \neq \beta$ i $\circ$ idempotentna operacija, vrijedi $\gamma \neq \alpha$.

- Ako je $\gamma < \alpha$, onda su navedene dvije točke sadržane samo u bloku $B_{\gamma,\alpha,k}$.
- Ako je $\gamma > \alpha$, onda su, zbog toga što je $\circ$ simetrična operacija, navedene dvije točke sadržane samo u bloku $B_{\alpha,\gamma,k}$.

3° $k = l + 1(mod\ 3)$; Jednadžba $x \circ \beta = \alpha$ ima jedinstveno rješenje $x = \gamma$. Budući da je $\alpha \neq \beta$ i $\circ$ idempotentna operacija, vrijedi $\gamma \neq \beta$.

- Ako je $\gamma < \beta$, onda su navedene dvije točke sadržane samo u bloku $B_{\gamma,\beta,l}$.
- Ako je $\gamma > \beta$, onda su, zbog toga što je $\circ$ simetrična operacija, navedene dvije točke sadržane samo u bloku $B_{\beta,\gamma,l}$.

Primjer 2.6. *Boseova konstrukcija STS*(15)*-a. Neka je dana idempotentna simetrična kvazigrupa iz primjera 2.4, reda* 5*, definirana na skupu* $\{0, 1, 2, 3, 4\}$*. Tada je skup točaka dizajna koji se konstruira*

$$\mathcal{Y} = \{0, 1, 2, 3, 4\} \times \{0, 1, 2\} = 00, 01, 02, 10, 11, 12, ..., 40, 41, 42.$$

Postoji 35 *blokova u STS*(15)*-u.*

Sljedeća slika prikazuje 5 *blokova* A_x, $0 \leq x \leq 4$, *i* 30 *blokova* $B_{x,y,i}$, $0 \leq x < y \leq 4$, $0 \leq i \leq 2$.

$\{00, 01, 02\}$	$\{10, 11, 12\}$	$\{20, 21, 22\}$
$\{30, 31, 32\}$	$\{40, 41, 42\}$	
$\{00, 10, 31\}$	$\{01, 11, 32\}$	$\{02, 12, 30\}$
$\{00, 20, 11\}$	$\{01, 21, 12\}$	$\{02, 22, 10\}$
$\{00, 30, 41\}$	$\{01, 31, 42\}$	$\{02, 32, 40\}$
$\{00, 40, 21\}$	$\{01, 41, 22\}$	$\{02, 42, 20\}$
$\{10, 20, 41\}$	$\{11, 21, 42\}$	$\{12, 22, 40\}$
$\{10, 30, 21\}$	$\{11, 31, 22\}$	$\{12, 32, 20\}$
$\{10, 40, 01\}$	$\{11, 41, 02\}$	$\{12, 42, 00\}$
$\{20, 30, 01\}$	$\{21, 31, 02\}$	$\{22, 32, 00\}$
$\{20, 40, 31\}$	$\{21, 41, 32\}$	$\{22, 42, 30\}$
$\{30, 40, 11\}$	$\{31, 41, 12\}$	$\{32, 42, 10\}$

Slika 11. 35 blokova STS(15)-a.

Boseova konstrukcija dokazuje sljedeću lemu, koja predstavlja dovoljan uvjet za postojanje STS(v)-a.

Lema 2.5. *Ako vrijedi* $v \equiv 3 (mod\ 6)$, $v \geq 9$, *onda postoji STS*(v).

2.3. *Skolemova konstrukcija*

Skolemova konstrukcija je vrsta konstrukcije STS(v)-a za sve vrijednosti v takve da je $v \equiv 1(mod\ 6)$.

Skolemova konstrukcija je modifikacija Boseove konstrukcije. Boseova konstrukcija koristi idempotentnu simetričnu kvazigrupu (neparnog reda). Budući da ne postoji takva kvazigrupa parnog reda, Skolemova konstrukcija koristi poluidempotentnu simetričnu kvazigrupu (parnog reda).

Neka je $v = 6u + 1$, $u \geq 1$, $S := \{0, 1, ..., 2u - 1\}$, $(S, \circ)$ poluidempotentna simetrična kvazigrupa (parnog) reda $2u$, te "$<$" totalni uređaj definiran na skupu S. Definira se skup

$$\mathcal{Y} := (S \times \mathbb{Z}_3) \cup \{\infty\},$$

koji će predstavljati skup točaka STS(v)-a koji se konstruira.

Za $0 \leq x \leq u - 1$ definira se blok

$$A_x := \{(x, 0), (x, 1), (x, 2)\}.$$

Za sve $x, y \in S$, $x < y$, i svaki $i \in \mathbb{Z}_3$ definira se blok

$$B_{x,y,i} := \{(x, i), (y, i), (x \circ y, i + 1(mod\ 3))\}.$$

Nadalje, za $0 \leq x \leq u - 1$ i svaki $i \in \mathbb{Z}_3$ definira se blok

$$C_{x,i} := \{\infty, (x + u, i), (x, i + 1(mod\ 3))\}.$$

Također, definira se skup blokova

$$\mathcal{B} := \{A_x | 0 \leq x \leq u-1\} \cup \{B_{x,y,i} | x, y \in \mathbb{Z}_{2u}, x < y, i \in \mathbb{Z}_3\} \cup$$

$$\cup \{C_{x,i} | 0 \leq x \leq u-1, i \in \mathbb{Z}_3\}.$$

Tada je potrebno pokazati da je par $(\mathcal{Y}, \mathcal{B})$ Steinerov sustav trojki. Očito postoji v točaka u $\mathcal{Y}$ i svaki blok u $\mathcal{B}$ sadrži tri točke. Stoga je dovoljno pokazati da su svake dvije točke sadržane u točno jednom bloku.

Prvo, uzme se da su (α, k) i ∞ dvije točke.

• Ako je $\alpha \leq u-1$, onda su navedene dvije točke sadržane samo u bloku $C_{\alpha,k-1(mod\ 3)}$.

• Ako je $\alpha \geq u$, onda su navedene dvije točke sadržane samo u bloku $C_{\alpha-u,k}$.

Drugo, uzme se da su (α, k) i (β, l) dvije točke.

• Ako je $\alpha = \beta \leq u-1$, onda su navedene dvije točke sadržane samo u bloku A_α.

• Ako je $\alpha = \beta \geq u$, onda je $k \neq l$ pa se bez smanjenja općenitosti može pretpostaviti da je $l = k + 1(mod\ 3)$. Jednadžba $\alpha \circ x = \alpha$ ima jedinstveno rješenje $x = \gamma$. Neka je $\gamma > \alpha$. Tada su navedene dvije točke sadržane samo u bloku $B_{\alpha,\gamma,k}$. Neka je $\gamma < \alpha$. Tada su, zbog toga što je $\circ$ simetrična operacija, navedene dvije točke sadržane samo u bloku $B_{\gamma,\alpha,k}$.

• Ako je $\alpha \neq \beta$, onda se bez smanjenja općenitosti može pretpostaviti da je $\alpha < \beta$ pa postoje tri slučaja:

1° $l = k$; Navedene dvije točke sadržane su samo u bloku $B_{\alpha,\beta,k}$.

2° $l = k + 1(mod\ 3)$; Jednadžba $x \circ \alpha = \beta$ ima jedinstveno rješenje $x = \gamma$. Budući da je $\alpha < \beta$ i $\alpha \circ \alpha \leq \alpha$, vrijedi $\gamma \neq \alpha$.

- Ako je $\gamma < \alpha$, onda su navedene dvije točke sadržane samo u bloku $B_{\gamma,\alpha,k}$.
- Ako je $\gamma > \alpha$, onda su, zbog toga što je $\circ$ simetrična operacija, navedene dvije točke sadržane samo u bloku $B_{\alpha,\gamma,k}$.

3° $k = l + 1(mod\ 3)$; Jednadžba $x \circ \beta = \alpha$ ima jedinstveno rješenje $x = \gamma$. Vrijedi da je $\gamma = \beta$ ako i samo ako je $\beta = \alpha + u$.

- Ako je $\gamma = \beta$, onda su navedene dvije točke sadržane samo u bloku $C_{\alpha,l}$.
- Ako je $\gamma < \beta$, onda su navedene dvije točke sadržane samo u bloku $B_{\gamma,\beta,l}$.
- Ako je $\gamma > \beta$, onda su, zbog toga što je $\circ$ simetrična operacija, navedene dvije točke sadržane samo u bloku $B_{\beta,\gamma,l}$.

Primjer 2.7. *Skolemova konstrukcija STS*(19)*-a. Neka je dana poluidempotentna simetrična kvazigrupa iz primjera 2.5, reda* 6*, definirana na skupu* $\{0, 1, 2, 3, 4, 5\}$*. Tada je skup točaka dizajna koji se konstruira*

$\mathcal{Y} = (\{0, 1, 2, 3, 4, 5\} \times \{0, 1, 2\}) \cup \{\infty\} = 00, 01, 02, 10, 11, 12, ..., 50, 51, 52, \infty.$

Postoji 57 *blokova u STS*(19)*-u.*

Sljedeća slika prikazuje 3 *bloka* A_x, $0 \leq x \leq 2$, 45 *blokova* $B_{x,y,i}$, $0 \leq x < y \leq 5$, $0 \leq i \leq 2$ *i* 9 *blokova* $C_{x,i}$, $0 \leq x \leq 2$, $0 \leq i \leq 2$.

$\{00, 01, 02\}$	$\{10, 11, 12\}$	$\{20, 21, 22\}$
$\{00, 10, 31\}$	$\{01, 11, 32\}$	$\{02, 12, 30\}$
$\{00, 20, 11\}$	$\{01, 21, 12\}$	$\{02, 22, 10\}$
$\{00, 30, 41\}$	$\{01, 31, 42\}$	$\{02, 32, 40\}$
$\{00, 40, 21\}$	$\{01, 41, 22\}$	$\{02, 42, 20\}$
$\{00, 50, 51\}$	$\{01, 51, 52\}$	$\{02, 52, 50\}$
$\{10, 20, 41\}$	$\{11, 21, 42\}$	$\{12, 22, 40\}$
$\{10, 30, 21\}$	$\{11, 31, 22\}$	$\{12, 32, 20\}$
$\{10, 40, 51\}$	$\{11, 41, 52\}$	$\{12, 42, 50\}$
$\{10, 50, 01\}$	$\{11, 51, 02\}$	$\{12, 52, 00\}$
$\{20, 30, 51\}$	$\{21, 31, 52\}$	$\{22, 32, 50\}$
$\{20, 40, 01\}$	$\{21, 41, 02\}$	$\{22, 42, 00\}$
$\{20, 50, 31\}$	$\{21, 51, 32\}$	$\{22, 52, 30\}$
$\{30, 40, 31\}$	$\{31, 41, 32\}$	$\{32, 42, 30\}$
$\{30, 50, 11\}$	$\{31, 51, 12\}$	$\{32, 52, 10\}$
$\{40, 50, 41\}$	$\{41, 51, 42\}$	$\{42, 52, 40\}$
$\{\infty, 30, 01\}$	$\{\infty, 31, 02\}$	$\{\infty, 32, 00\}$
$\{\infty, 40, 11\}$	$\{\infty, 41, 12\}$	$\{\infty, 42, 10\}$
$\{\infty, 50, 21\}$	$\{\infty, 51, 22\}$	$\{\infty, 52, 20\}$

Slika 12. 57 blokova STS(19)-a.

Skolemova konstrukcija dokazuje sljedeću lemu, koja predstavlja dovoljan uvjet za postojanje STS(v)-a.

Lema 2.6. *Ako vrijedi* $v \equiv 1 (mod\ 6)$, $v \geq 7$, *onda postoji STS*(v).

2.4. *Izomorfizmi*

Definicija 2.8. *Neka su* $(\mathcal{X}, \mathcal{A})$ *i* $(\mathcal{Y}, \mathcal{B})$ *dva blokovna dizajna takvi da je*

$$|\mathcal{X}| = |\mathcal{Y}|.$$

Tada, ako postoji bijekcija $\alpha : \mathcal{X} \to \mathcal{Y}$ *takva da je*

$$\{\{\alpha(x)|x \in A\}|A \in \mathcal{A}\} = \mathcal{B},$$

onda se $(\mathcal{X}, \mathcal{A})$ *i* $(\mathcal{Y}, \mathcal{B})$ *nazivaju* **izomorfnim blokovnim dizajnima**. *Preciznije, ako se svaka točka* $x \in \mathcal{X}$ *promijeni u* $\alpha(x)$*, onda se kolekcija blokova* $\mathcal{A}$ *promijeni u* $\mathcal{B}$*. Bijekcija* α *naziva se* **izomorfizmom**.

Primjer 2.8. *Neka su* $(\mathcal{X}, \mathcal{A})$ *i* $(\mathcal{Y}, \mathcal{B})$ *dva* $(7, 3, 1)$*-BIBD-a, odnosno STS*(7)*-a, gdje su*

- $\mathcal{X} = \{1, 2, 3, 4, 5, 6, 7\}$,
- $\mathcal{A} = \{123, 145, 167, 246, 257, 347, 356\}$,
- $\mathcal{Y} = \{a, b, c, d, e, f, g\}$,
- $\mathcal{B} = \{abd, bce, cdf, deg, aef, bfg, acg\}$.

Definira se bijekcija α *sa*

x	*1*	*2*	*3*	*4*	*5*	*6*	*7*
$\alpha(x)$	a	b	d	c	g	e	f

.

Tada se promjenom svake točke $x \in \mathcal{X}$ u $\alpha(x)$, blokovi od $\mathcal{A}$ preslikavaju u blokove od $\mathcal{B}$ na način

$$123 \mapsto abd, \quad 145 \mapsto acg, \quad 167 \mapsto aef,$$

$$246 \mapsto bce, \quad 257 \mapsto bfg, \quad 347 \mapsto cdf,$$

$$356 \mapsto deg.$$

Dakle, α je izomorfizam navedena dva blokovna dizajna.

Izomorfizmi blokovnih dizajna mogu se karakterizirati korištenjem matrica incidencije.

Teorem 2.3. *Neka su $M = (m_{i,j})$ i $N = (n_{i,j})$ matrice incidencije proizvoljna dva blokovna dizajna, reda $v \times b$. Tada su dva blokovna dizajna izomorfna ako i samo ako postoje permutacije γ od $\{1, ..., v\}$ i β od $\{1, ..., b\}$ takve da je*

$$m_{i,j} = n_{\gamma(i),\beta(j)},$$

za sve i, j, $1 \leq i \leq v$, $1 \leq j \leq b$.

Dokaz. Neka su $\mathcal{X} = \{x_1, ..., x_v\}$, $\mathcal{A} = \{A_1, ..., A_b\}$, $\mathcal{Y} = \{y_1, ..., y_v\}$, $\mathcal{B} = \{B_1, ..., B_b\}$, te $(\mathcal{X}, \mathcal{A})$ i $(\mathcal{Y}, \mathcal{B})$ dva blokovna dizajna čije su pripadne matrice incidencije, redom, M i N.

($\Rightarrow$) Pretpostavi se da su blokovni dizajni $(\mathcal{X}, \mathcal{A})$ i $(\mathcal{Y}, \mathcal{B})$ izomorfni. Slijedi da postoji bijekcija $\alpha : \mathcal{X} \to \mathcal{Y}$ takva da je

$$\{\{\alpha(x)|x \in A\}|A \in \mathcal{A}\} = \mathcal{B}.$$

Definira se permutacija γ sa

$$\gamma(i) := j \text{ ako i samo ako vrijedi } \alpha(x_i) = y_j, 1 \leq i \leq v.$$

Kako je α bijekcija sa X u Y, to je γ permutacija skupa $\{1, ..., v\}$. Kako je α izomorfizam od $(\mathcal{X}, \mathcal{A})$ i $(\mathcal{Y}, \mathcal{B})$, to postoji permutacija β skupa $\{1, ..., b\}$ sa svojstvom

$$\{\alpha(x)|x \in A_j\} = B_{\beta(j)}, 1 \leq j \leq b.$$

Tada je

$$m_{i,j} = 1 \Leftrightarrow x_i \in A_j \Leftrightarrow y_{\gamma(i)} \in B_{\beta(j)} \Leftrightarrow n_{\gamma(i),\beta(j)} = 1.$$

($\Leftarrow$) Pretpostavi se da su permutacije γ i β takve da je

$$m_{i,j} = n_{\gamma(i),\beta(j)},$$

za sve i, j, $1 \leq i \leq v$, $1 \leq j \leq b$. Definira se bijekcija $\alpha : \mathcal{X} \to \mathcal{Y}$ sa

$$\alpha(x_i) := y_j \text{ ako i samo ako vrijedi } \gamma(i) = j, 1 \leq i \leq v.$$

Očito je

$$\{\alpha(x)|x \in A_j\} = B_{\beta(j)}, 1 \leq j \leq b.$$

Tada α definira izomorfizam od $(\mathcal{X}, \mathcal{A})$ i $(\mathcal{Y}, \mathcal{B})$.

□

Definicija 2.9. Permutacijska matrica *je matrica* $P = (p_{i,j})$, $p_{i,j} \in \{0, 1\}$, *u kojoj svaki redak i svaki stupac sadrži točno jednu znamenku* 1.

Sljedeći korolar predstavlja alternativnu karakterizaciju izomorfnih blokovnih dizajna.

Korolar 2.1. *Neka su* $M = (m_{i,j})$ *i* $N = (n_{i,j})$ *matrice incidencije proizvoljna dva blokovna dizajna, reda* $v \times b$. *Tada su dva blokovna dizajna izomorfna ako i samo ako postoje permutacijske matrice* P, *reda* $v \times v$, *i* Q, *reda* $b \times b$, *takve da je*

$$M = PNQ.$$

Općenito, utvrđivanje izomorfizma dva blokovna dizajna je teško izračunljiv problem. Naime, postoji $v!$ bijekcija za dva skupa kardinaliteta v. Stoga, da bi se provjerilo da dva blokovna dizajna nisu izomorfna, potrebno je pokazati da ni jedna od $v!$ bijekcija ne definira izomorfizam. Budući da $v!$ raste eksponencijalno brzo kao funkcija od v, slijedi da postaje nepraktično provjeravati svaku moguću bijekciju. Međutim, postoje napredniji algoritmi koji omogućavaju utvrđivanje izomorfizma velikih blokovnih dizajna.

Postavlja se pitanje koliko ima Steinerovih sustava trojki proizvoljnog reda, do na izomorfizam. Odgovor je za sada još uvijek nepoznat. Sljedeći teorem predstavlja približno rješenje navedenog problema.

Teorem 2.4 (Wilson)**.** *Broj STS*(v)*-a, do na izomorfizam, sadržan je u intervalu*

$$[(\frac{1}{e^5}v)^{\frac{v^2}{6}}, (\frac{1}{e^{\frac{1}{2}}}v)^{\frac{v^2}{6}}].$$

Propozicija 2.1. *Do na izomorfizam, postoji točno jedan STS*(3)*, STS*(7) *i STS*(9)*.*

Propozicija 2.2 (DePasquale-Brunel)**.** *Do na izomorfizam, postoje točno dva STS*(13)*-a.*

Primjer 2.9. *Neka su* $(\mathcal{X}, \mathcal{A}_1)$ *i* $(\mathcal{X}, \mathcal{A}_2)$ *dva* $(13, 3, 1)$*-BIBD-a, gdje su*

- $\mathcal{X} = \{a, b, c, d, e, f, g, h, i, j, k, l, m\}$,
- $\mathcal{A}_1 = \{abc, ade, afg, ahi, ajk, alm, bdf, beh, bgi, bjl, bkm, cdj, cef,$
  $cgk, chm, cil, dgl, dhk, dim, egm, eij, ekl, fhl, fik, fjm, ghj\}$,
- $\mathcal{A}_2 = \{abc, ade, afg, ahi, ajk, alm, bdf, beh, bgi, bjl, bkm, cdj, cef,$
  $cgk, chl, cim, dgl, dhm, dik, egm, eij, ekl, fhk, fil, fjm, ghj\}$.

Tada su $(\mathcal{X}, \mathcal{A}_1)$ *i* $(\mathcal{X}, \mathcal{A}_2)$ *dva STS*(13)*-a iz prethodne propozicije.*

Propozicija 2.3 (Cole-Cummings-White)**.** *Do na izomorfizam, postoji točno* 80 *STS*(15)*-a.*

Propozicija 2.4 (Kaski-Östergård)**.** *Do na izomorfizam, postoji točno* 11.084.874.829 *STS*(19)*-a.*

Sve navedene vrijednosti, osim za STS(19), dobivene su bez korištenja računala. Naime, propoziciju 2.2 dokazali su DePasquale 1899. godine i Brunel 1901. godine, a propoziciju 2.3 dokazali su Cole, Cummings i White 1917. godine. Točan izračun vrijednosti za STS(15) u to vrijeme je zadivljujuće postignuće. Trebalo je proći gotovo 40 godina da bi se rezultati provjerili korištenjem računala. Zanimljiva je i činjenica da je trebalo proći gotovo cijelo stoljeće da bi se riješio problem za STS(19). Naime, propoziciju 2.4 dokazali su Kaski i Östergård [KRJO04] 2004. godine. Međutim, za STS(21) izgledi nisu optimistični. Procijenjeno je da se upotrebom sadašnje tehnologije i znanja, računanje broja Steinerovih sustava trojki reda 21, do na izomorfizam, ne bi odvijalo u prihvatljivom vremenu.

2.5. *Automorfizmi*

Definicija 2.10. *Neka je* $(\mathcal{X}, \mathcal{A})$ *blokovni dizajn. Tada je* **automorfizam** *od* $(\mathcal{X}, \mathcal{A})$ *izomorfizam navedenog blokovnog dizajna u samog sebe. Bijekcija* α *je permutacija od* $\mathcal{X}$ *takva da je*

$$\{\{\alpha(x)|x \in A\}|A \in \mathcal{A}\} = \mathcal{A}.$$

Primjer 2.10. *Neka je* $(\mathcal{X}, \mathcal{A})$ $(7, 3, 1)$*-BIBD-a, odnosno STS*(7)*, gdje su*

- $\mathcal{X} = \{1, 2, 3, 4, 5, 6, 7\}$,
- $\mathcal{A} = \{123, 145, 167, 246, 257, 347, 356\}$.

Definira se bijekcija α *sa*

x	1	2	3	4	5	6	7
$\alpha(x)$	1	2	3	5	4	7	6

.

Tada se promjenom svake točke $x \in \mathcal{X}$ *u* $\alpha(x)$*, blokovi od* $\mathcal{A}$ *preslikavaju na način*

$$123 \mapsto 123, \quad 145 \mapsto 145, \quad 167 \mapsto 167,$$

$$246 \mapsto 257, \quad 257 \mapsto 246, \quad 347 \mapsto 356,$$

$$356 \mapsto 347.$$

Dakle, α *je automorfizam navedenog blokovnog dizajna.*

Definicija 2.11. Ciklus $(a_1 \ \dots \ a_k)$, $k \leq n$, *je permutacija* p_n *definirana sa*

$$p_n(a_i) := \begin{cases} a_{i+1}, & za\ i \neq k \\ a_1, & za\ i = k \end{cases}.$$

Broj k *naziva se* **duljinom ciklusa**.

Definicija 2.12. Red permutacije *je najmanji zajednički višekratnik duljina ciklusa u rastavu.* **Fiksna točka permutacije** *je točka koju permutacija preslikava u tu istu točku.*

Fiksne točke permutacije odgovaraju ciklusima duljine 1 u rastavu. Svaka permutacija može se prikazati kao produkt disjunktnih ciklusa. Disjunktni ciklusi međusobno komutiraju. Svaki ciklus može se prikazati kao produkt ciklusa duljine 2,

$$(a_1\ a_2)(a_1\ a_3)\cdots(a_1\ a_k).$$

Ponekad je korisno prikazati permutaciju α na skupu $\mathcal{X}$ kao produkt disjunktnih ciklusa. Svaki ciklus u produktu ima oblik

$$(x\ \alpha(x)\ \alpha(\alpha(x))\ \dots\ \alpha(\alpha(\dots\alpha(x)\dots))), x \in \mathcal{X}.$$

Zbroj duljina svih ciklusa u rastavu iznosi $|\mathcal{X}|$.

Primjer 2.11. *Permutacija* α *iz primjera 2.10 može se prikazati kao produkt disjunktnih ciklusa na način*

$$(1)(2)(3)(4\ 5)(6\ 7).$$

Riječ je o permutaciji reda 2 *koja ima tri fiksne točke,* 1, 2 *i* 3.

Lema 2.7. *Skup svih automorfizama blokovnog dizajna* $(\mathcal{X}, \mathcal{A})$ *je grupa s obzirom na operaciju kompozicije permutacija.*

Navedena grupa naziva se ***grupom automorfizama*** i označava s $Aut(\mathcal{X}, \mathcal{A})$. $Aut(\mathcal{X}, \mathcal{A})$ je podgrupa simetrične grupe $S_{|\mathcal{X}|}$ koja se sastoji od svih $v!$ permutacija na skupu od v točaka. Svaka podgrupa od $S_{|\mathcal{X}|}$ naziva se ***grupom permutacija***. Dakle, grupa automorfizama blokovnih dizajna je primjer grupe permutacija.

Primjer 2.12. *Neka je* $(\mathcal{X}, \mathcal{A})$ $(7, 3, 1)$*-BIBD, odnosno STS*(7)*, iz primjera 2.10. Tada je*

$$\beta = (1\ 2\ 4\ 3\ 6\ 7\ 5)$$

automorfizam od $(\mathcal{X}, \mathcal{A})$*. Ako je kompozicija* $\gamma = \alpha \circ \beta$ *definirana sa* $\gamma(x) := \beta(\alpha(x))$*, za sve* $x \in \mathcal{X}$*, onda je*

$$\gamma = (1\ 2\ 4)(3\ 6\ 5)(7)$$

automorfizam od $(\mathcal{X}, \mathcal{A})$*.*

Štoviše, blokovni dizajn $(\mathcal{X}, \mathcal{A})$ *ima mnogo automorfizama. Preciznije,* $Aut(\mathcal{X}, \mathcal{A})$ *je grupa reda* 168*.*

Sljedeći primjeri prikazuju automorfizme Steinerovih sustava trojki iz Boseove i Skolemove konstrukcije.

Primjer 2.13. *Neka je* $(\mathcal{Y}, \mathcal{B})$ *STS*(v), $v \equiv 3(mod\ 6)$, *dobiven Boseovom konstrukcijom od idempotentne simetrične kvazigrupe* $(S, \circ)$, *te* $\mathbb{Z}_3 = \{0, 1, 2\}$ *i* $\mathcal{Y} = S \times \mathbb{Z}_3$. *Tada je bijekcija* $\alpha : \mathcal{Y} \to \mathcal{Y}$, *definirana sa*

$$\alpha(s, z) := (s, z + n(mod\ 3)),$$

za $s \in S$, $z \in \mathbb{Z}_3$ *i* $n \in \mathbb{N}$, *automorfizam od* $(\mathcal{Y}, \mathcal{B})$. *Navedeni automorfizam preslikava blokove* A_x *i* $B_{x,y,i}$, $x, y \in S$, $0 \leq i \leq 2$, *u blokove istog tipa.*

Primjer 2.14. *Neka je* $(\mathcal{Y}, \mathcal{B})$ *STS*(v), $v \equiv 1(mod\ 6)$, *dobiven Skolemovom konstrukcijom od poluidempotentne simetrične kvazigrupe* $(S, \circ)$, *te* $\mathbb{Z}_3 = \{0, 1, 2\}$ *i* $\mathcal{Y} = (S \times \mathbb{Z}_3) \cup \{\infty\}$. *Tada je bijekcija* $\alpha : \mathcal{Y} \to \mathcal{Y}$, *definirana sa*

$$\alpha(s, z) := \begin{cases} (s, z + n(mod\ 3)), & za\ (s, z) \neq \infty \\ \infty, & za\ (s, z) = \infty \end{cases},$$

za $s \in S$, $z \in \mathbb{Z}_3$ *i* $n \in \mathbb{N}$, *automorfizam od* $(\mathcal{Y}, \mathcal{B})$. *Navedeni automorfizam preslikava blokove* A_x, $B_{x,y,i}$ *i* $C_{x,i}$, $x, y \in S$, $0 \leq i \leq 2$, *u blokove istog tipa.*

3. Stinsonov algoritam

Stinsonov algoritam služi za konstrukciju Steinerovih sustava trojki na brz i djelotvoran način. Algoritam pripada familiji ***algoritama „planinarenja“*** (eng. ***„hill-climbing“ algorithms***) koji koriste analogiju penjanja po planini. Naime, najbrži put do vrha planine je konstantnim penjanjem. Slično, strategija algoritama „planinarenja“ je da se svakim korakom izvršavanja dolazi sve bliže konačnom rješenju problema. Algoritam „planinarenja“ smatra se ***heurističkim algoritmom***. Pojam heurističkog algoritma koristi se za opisivanje algoritma koji nastoji pronaći određenu kombinatornu strukturu ili riješiti optimizacijski problem korištenjem ***heuristike*** (grč. ***heurisko***). U smislu heurističkih algoritama, heuristika označava metodu izvođenja niza promjena danog (parcijalnog) rješenja u svrhu dobivanja drugačijeg (parcijalnog) rješenja. Heuristički algoritam sastoji se od iterativnog primjenjivanja jedne ili više heuristika, u skladu sa određenom strategijom oblikovanja (parcijalnih) rješenja.

3.1. *Opis algoritma*

Stinsonov algoritam radi na način da slučajnim odabirom određenih točaka konstruira blokove koji čine Steinerov sustav trojki. Budući da algoritam koristi strategiju slučajnog traženja (eng. randomized search strategy), za oblikovanje (parcijalnih) rješenja, slijedi da nema garancije da će algoritam ikada stati, konstruirajući pritom Steinerov sustav trojki. Naime, može se dogoditi da u svakom koraku, na slučajan način, budu odabrane baš one točke koje nisu pogodne za oblikovanje (parcijalnog) rješenja. Međutim, u praksi je takav događaj malo vjerojatan pa će algoritam, nakon određenog broja iteracija, ipak konstruirati Steinerov sustav trojki.

Nadalje, potrebno je postaviti problem konstruiranja Steinerovih sustava trojki kao optimizacijski problem.

Definicija 3.1. Parcijalni Steinerov sustav trojki *(eng.* **partial Steiner triple system***), ili ukratko* **PSTS**(v)*, je dizajn* $(\mathcal{Y}, \mathcal{B})$ *takav da vrijedi*

- *postoji točno* v *točaka,*
- *svaki blok sadrži točno tri točke,*
- *svake dvije točke sadržane su u najviše jednom bloku.*

Primjer 3.1. *Dizajn* $(\mathcal{Y}, \mathcal{B})$*, gdje su*

- $\mathcal{Y} = \{1, 2, 3, 4, 5, 6, 7\}$,
- $\mathcal{B} = \{246, 257, 347, 356\}$,

je PSTS(7)*. Navedeni parcijalni Steinerov sustav trojki može se nadopuniti do STS*(7) *iz primjera 1.1 umetanjem prva tri bloka.*

Primjer 3.2. *Dizajn* $(\mathcal{Y}, \mathcal{B})$*, gdje su*

- $\mathcal{Y} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$,
- $\mathcal{B} = \{123, 456, 789, 147, 258\}$,

je PSTS(9)*. Navedeni parcijalni Steinerov sustav trojki može se nadopuniti do STS*(9) *iz primjera 1.2 umetanjem zadnjih sedam blokova.*

Napomena 3.1. *Parcijalni Steinerov sustav trojki ne može se uvijek nadopuniti do Steinerovog sustava trojki konstantnim umetanjem blokova.*

Primjer 3.3. *Dizajn* $(\mathcal{Y}, \mathcal{B})$*, gdje su*

- $\mathcal{Y} = \{1, 2, 3, 4, 5, 6, 7\}$,
- $\mathcal{B} = \{123, 145, 267, 347, 356\}$,

je PSTS(7)*. Navedeni parcijalni Steinerov sustav trojki ne može se nadopuniti do STS*(7) *umetanjem blokova jer ne postoje potrebna dva bloka.*

Teorem 3.1. *U PSTS(v)-u svaka točka sadržana je u najviše*

$$r \leq \frac{v-1}{2}$$

blokova.

Dokaz. Neka je $(\mathcal{Y}, \mathcal{B})$ PSTS(v), $y \in \mathcal{Y}$ čvrsta točka, te r_y broj blokova koji sadrže y. Definira se skup

$$K := \{(x, B) | x \in \mathcal{Y}, x \neq y, B \in \mathcal{B}, \{x, y\} \subseteq B\}.$$

Tada se računa $|K|$ na dva različita načina.

Prvo, postoji $v - 1$ načina za izbor $x \in \mathcal{Y}$ takvih da je $x \neq y$. Stoga vrijedi

$$|K| \leq v - 1.$$

Drugo, postoji r_y načina za izbor bloka $B \in \mathcal{B}$ takvih da je $y \in B$, a za svaki takav B postoje 2 načina za izbor $x \in B$, $x \neq y$. Stoga vrijedi

$$|K| = r_y \cdot 2.$$

Uvrštavanjem, iz navedene nejednadžbe i jednadžbe dobiva se

$$r_y \cdot 2 \leq v - 1,$$

te je rezultat nezavisan od izbora točke y, odakle slijedi tvrdnja.

□

Teorem 3.2. *PSTS(v) sadrži najviše*

$$b = \frac{vr}{3} \leq \frac{v(v-1)}{6}$$

blokova.

Dokaz. Neka je $(\mathcal{Y}, \mathcal{B})$ PSTS(v), te $b = |\mathcal{B}|$. Definira se skup

$$L := \{(y, B) | y \in \mathcal{Y}, B \in \mathcal{B}, y \in B\}.$$

Tada se računa $|L|$ na dva različita načina.

Prvo, postoji v načina za izbor $y \in \mathcal{Y}$, a za svaki takav y postoji r blokova B takvih da je $y \in B$. Stoga vrijedi

$$|L| = vr.$$

Drugo, postoji b načina za izbor bloka $B \in \mathcal{B}$, a za svaki takav B postoje 3 načina za izbor $y \in B$. Stoga vrijedi

$$|L| = b \cdot 3.$$

Uvrštavanjem, iz navedenih jednadžbi dobiva se

$$b \cdot 3 = vr,$$

odakle slijedi tvrdnja.

□

Napomena 3.2. *Jednakost u prethodnom teoremu dostiže se ukoliko su svake dvije točke sadržane u točno jednom bloku, tj. ukoliko je parcijalni Steinerov sustav trojki upravo Steinerov sustav trojki.*

Za $v \equiv 1, 3 (mod\ 6)$, potrebno je pronaći maksimalni kardinalitet skupa blokova PSTS(v)-a. Za dani v i $\mathcal{Y}$ definira se skup $\mathcal{T}$ svih skupova blokova $\mathcal{B}$ takvih da je $(\mathcal{Y}, \mathcal{B})$ PSTS(v), tj.

$$\mathcal{T} := \{\mathcal{B} | (\mathcal{Y}, \mathcal{B})\ je\ \text{PSTS}(v)\}.$$

Dopustivo rješenje je svaki $\mathcal{B} \in \mathcal{T}$, a optimalno rješenje je neki $\mathcal{B} \in \mathcal{T}$ kardinaliteta

$$|\mathcal{B}| = b = \frac{v(v-1)}{6}.$$

Definicija 3.2. *Neka je $(\mathcal{Y}, \mathcal{B})$ parcijalni Steinerov sustav trojki. Tada se točka $x \in \mathcal{Y}$ naziva* **nezasićenom točkom** *ukoliko vrijedi*

$$r_x < \frac{v-1}{2},$$

gdje je r_x broj blokova u $\mathcal{B}$ koji sadrže x. Navedena točka naziva se **zasićenom točkom** *ukoliko nije nezasićena.*

Definicija 3.3. *Neka je $(\mathcal{Y}, \mathcal{B})$ parcijalni Steinerov sustav trojki. Tada se par $\{y, z\}$ različitih točaka $y, z \in \mathcal{Y}$ naziva* **nezasićenim parom** *ukoliko ne postoji blok $B \in \mathcal{B}$ takav da je $\{y, z\} \subseteq B$. Navedeni par naziva se* **zasićenim parom** *ukoliko nije nezasićen.*

Primjer 3.4. *Točka 5 iz primjera 3.1 je nezasićena jer je sadržana u manje od $\frac{7-1}{2} = 3$ bloka. Par $\{3, 7\}$ iz primjera 3.2 je nezasićen jer nije sadržan ni u jednom bloku.*

Lema 3.1. *Ako u PSTS(v)-u vrijedi*

$$b < \frac{v(v-1)}{6},$$

onda postoji barem jedna nezasićena točka.

Dokaz. Pretpostavi se suprotno. Neka su sve točke zasićene. Tada je, prema teoremu 3.1 i definiciji 3.2 zasićene točke, svaka točka sadržana u točno $r = \frac{(v-1)}{2}$ blokova, a, prema teoremu 3.2, PSTS(v) sadrži točno $b = \frac{vr}{3} = \frac{v(v-1)}{6}$ blokova. Međutim, to je u kontradikciji s činjenicom da u PSTS(v)-u vrijedi

$$b < \frac{v(v-1)}{6}.$$

□

Lema 3.2. *Svaka nezasićena točka sadržana je u barem dva nezasićena para.*

Dokaz. Neka je $x \in \mathcal{Y}$ nezasićena točka, tj. vrijedi $r_x < \frac{v-1}{2}$. Budući da je $r_x \leq \frac{v-1}{2} - 1 = \frac{v-3}{2}$ i veličina blokova jednaka 3, slijedi da x sudjeluje u blokovima s najviše $v-3$ ostalih točaka. Stoga postoje barem dvije točke $y, z \in \mathcal{Y}$ takve da parovi $\{x, y\}$ i $\{x, z\}$ nisu sadržani ni u jednom bloku. Tada su, prema definiciji 3.3 nezasićenog para, parovi $\{x, y\}$ i $\{x, z\}$ nezasićeni.

□

Na početku izvođenja algoritma, korisnik zadaje red v Steinerovog sustava trojki kojeg želi konstruirati, a broj blokova u PSTS(v)-u iznosi 0. U svakom koraku moguća su dva slučaja. Ili se umeće novi blok u sustav i time se broj blokova u sustavu povećava za jedan, ili se određeni blok u sustavu zamijenjuje novim blokom i time se broj blokova u sustavu ne mijenja. Na kraju izvođenja algoritma, broj blokova u PSTS(v)-u iznosi $\frac{v(v-1)}{6}$, te korisnik dobiva željeni STS(v).

Algoritam poziva heuristiku $konstruirajBlok()$ sve dok je broj blokova u sustavu manji od $\frac{v(v-1)}{6}$, tj. sve dok se PSTS(v) ne nadopuni do STS(v)-a.

$konstruirajBlok()$

Na slučajan način odaberi, iz polja nezasićenih točaka, točku x
(takva točka postoji prema lemi 3.1).
Na slučajan način odaberi, iz polja nezasićenih parova, parove $\{x, y\}$ i $\{x, z\}$
(takvi parovi postoje prema lemi 3.2).
Ako je par $\{y, z\}$ nezasićen,
onda umetni blok $\{x, y, z\}$ u sustav i povećaj broj blokova,
inaće pronađi točku w takvu da je $\{w, y, z\}$ blok u sustavu i zamijeni w točkom x,
tj. zamijeni blok $\{w, y, z\}$ u sustavu blokom $\{x, y, z\}$.

Umetanje bloka $\{x, y, z\}$ u sustav odvija se pozivom

metode $umetniBlok(x, y, z)$.

$umetniBlok(x, y, z)$

Parovima $\{x, y\}$, $\{x, z\}$ i $\{y, z\}$ pridruži, redom, točke z, y i x.
Obriši parove $\{x, y\}$, $\{x, z\}$ i $\{y, z\}$ iz polja nezasićenih parova.

Zamjena bloka $\{w, y, z\}$ u sustavu blokom $\{x, y, z\}$ odvija se pozivom

metode $zamijeniBlok(x, y, z, w)$.

$zamijeniBlok(x, y, z, w)$

Parovima $\{x, y\}$, $\{x, z\}$ i $\{y, z\}$ pridruži, redom, točke z, y i x.
Parovima $\{w, y\}$ i $\{w, z\}$ pridruži vrijednost 0.
Zapiši parove $\{w, y\}$ i $\{w, z\}$ u polje nezasićenih parova.
Obriši parove $\{x, y\}$, $\{x, z\}$ i $\{y, z\}$ iz polja nezasićenih parova.

Brisanje para $\{x, y\}$ iz polja nezasićenih parova odvija se pozivom

metode $obrisiPar(x, y)$.

$obrisiPar(x, y)$

Par $\{x, y\}$ postaje zasićen, tj. zadnji nezasićen par u polju zauzima mjesto od $\{x, y\}$,
te se broj nezasićenih parova smanji za jedan.
Ako točka x postaje zasićena, onda zadnja nezasićena točka u polju zauzima mjesto od x,
te se broj nezasićenih točaka smanji za jedan.
Ako točka y postaje zasićena, onda zadnja nezasićena točka u polju zauzima mjesto od y,
te se broj nezasićenih točaka smanji za jedan.

Pisanje para $\{x, y\}$ u polje nezasićenih parova odvija se pozivom

metode $zapisiPar(x, y)$.

$zapisiPar(x, y)$

Ako točka x postaje nezasićena, onda se broj nezasićenih točaka poveća za jedan,
te x dolazi na kraj polja nezasićenih točaka.
Ako točka y postaje nezasićena, onda se broj nezasićenih točaka poveća za jedan,
te y dolazi na kraj polja nezasićenih točaka.
Par $\{x, y\}$ postaje nezasićen, tj. broj nezasićenih parova poveća se za jedan,
te $\{x, y\}$ dolazi na kraj polja nezasićenih parova.

3.2. *Implementacija algoritma*

Prvo, potrebno je zadati veličinu $v = |\mathcal{Y}|$. Potom se za zadani kardinalitet od $\mathcal{Y}$ provjerava da li zadovoljava uvjet $v \equiv 1, 3 (mod\ 6)$, $v \geq 7$.

STS.cpp

```
#include <ctime> #include <fstream> #include <iostream> #include <set>

#include "STS.h"

using namespace std;

int main() {
    cout << ">>> Stinsonov algoritam <<<" << endl << endl;
obradaGreske: obradaIznimke:
    try {
        while(true) {
            int v(0);
            cout << endl << endl << "- konstruiraj STS reda v = ";
            cout << "(0 je izlaz) ";
            cin >> v;
            if(v == 0)
                exit(0);
            int mod(v % 6);
            if(((mod == 1) || (mod == 3)) && (v >= 7)) {
                STS Sts(v);
                cout << endl;
            } else {
                cout << "Greska: v != 1,3(mod 6) i/ili v < 7;" << endl;
                cout << endl;
                clock_t spavanje(3210 + clock());
                while(spavanje > clock());
                goto obradaGreske;
            }
        }
    } catch(exception e) {
        cout << "Iznimka: " << e.what() << ";" << endl << endl;
        clock_t spavanje(3210 + clock());
        while(spavanje > clock());
        goto obradaIznimke;
    }
    return(0);
}
```

Drugo, potrebno je definirati varijable.

Varijabla *tocka* predstavlja jednodimenzionalno polje svih nezasićenih točaka. Nije potrebno da navedeno polje bude uređeno. Ako točka postane zasićena, onda zadnja nezasićena točka u polju zauzima njezino mjesto. Ako točka postane nezasićena, onda dolazi na kraj polja. Da bi se navedene operacije obavljale djelotvorno i izbjeglo pretraživanje polja, koristi se varijabla $indeksTocke$ koja prati poziciju točke u polju svih nezasićenih točaka.

Analogno, varijabla *par* predstavlja dvodimenzionalno polje svih nezasićenih parova, a varijabla $indeksPara$ prati poziciju para u polju svih nezasićenih parova.

Varijable $brojTocaka$, $brojParova$ i $brojBlokova$ čuvaju podatke o broju nezasićenih točaka, odnosno parova, te broju blokova.

Varijabla $trecaTockaBloka$ za svaki par različitih točaka čuva podatak o trećoj točki bloka koji sadrži navedeni par. Preciznije, za svaki PSTS(v) $(\mathcal{Y}, \mathcal{B})$ i sve točke $x, y \in \mathcal{Y}$ varijabla je definirana sa $trecaTockaBloka[x][y] = z$ ako i samo ako vrijedi $\{x, y, z\} \in \mathcal{B}$, a nije definirana ukoliko je $\{x, y\}$ nezasićeni par.

Konstruktor klase STS nakon inicijalizacije varijabli pozivom funkcije $inicijalizirajVarijable()$, pokušava u svakom koraku konstruirati novi blok kandidat pozivom funkcije $konstruirajBlok()$, sve dok je $brojBlokova < \frac{v(v-1)}{6}$. Zatim, konstruira i ispisuje $\mathcal{B}$ pozivom funkcija $konstruirajB()$, odnosno $ispisiB()$.

STS.h

```
#ifndef STEINEROV_SUSTAV_TROJKI

#define STEINEROV_SUSTAV_TROJKI

using namespace std;

class STS {
    int v, w, x, y, z;
    int brojTocaka, *indeksTocke, *tocka, **trecaTockaBloka;
    int *brojParova, **indeksPara, **par;
    int brojBlokova, brojIteracija;
    set<int> blok;
    set<set<int> > B;
    ofstream izlazniTokDatoteke;
    void inicijalizirajVarijable();
    void zapisiPar(const int, const int);
    void obrisiPar(const int, const int);
    void zamijeniBlok(const int, const int, const int, const int);
    void umetniBlok(const int, const int, const int);
    void konstruirajBlok();
    void ispisiBlok(const int);
    void konstruirajB();
    void ispisiB();
public:
    STS(int dimenzija):
      v(dimenzija ++), w(1), x(1), y(1), z(1),
          brojTocaka(0), brojBlokova(0), brojIteracija(0) {
        indeksTocke = new int[dimenzija]();
        tocka = new int[dimenzija]();
        trecaTockaBloka = new int*[dimenzija]();
        for(int brojac = 0; brojac != dimenzija; ++ brojac)
            trecaTockaBloka[brojac] = new int[dimenzija]();
        brojParova = new int[dimenzija]();
        indeksPara = new int*[dimenzija]();
        for(int brojac = 0; brojac != dimenzija; ++ brojac)
            indeksPara[brojac] = new int[dimenzija]();
        par = new int*[dimenzija]();
        for(int brojac = 0; brojac != dimenzija; ++ brojac)
            par[brojac] = new int[dimenzija]();
        izlazniTokDatoteke.open("STS.txt", ofstream::app);
        inicijalizirajVarijable();
        srand((unsigned)clock());
        int b(v * (v - 1) / 6);
        while(brojBlokova < b) {
            brojIteracija += 1;
            konstruirajBlok();
        }
        cout << endl;
        izlazniTokDatoteke << endl;
        konstruirajB();
        ispisiB();
        izlazniTokDatoteke.close();
    }
};
```

Inicijalizacija varijabli izvršava se na početku algoritma.

STS.h

```
void STS::inicijalizirajVarijable() {
    brojTocaka = v;
    for(x = 1; x <= v; ++ x) {
        indeksTocke[x] = x;
        tocka[x] = x;
        brojParova[x] = v - 1;
        for(y = 1; y <= v; ++ y) {
            if(y >= x)
                indeksPara[x][y] = (y - x) % v;
            else
                indeksPara[x][y] = v - ((x - y) % v);
            if(y < v)
                par[x][y] = ((x + y - 1) % v) + 1;
            trecaTockaBloka[x][y] = 0;
        }
    }
}
```

Za pisanje parova u polje nezasićenih parova i brisanje parova iz polja nezasićenih parova potrebne su funkcije $zapisiPar(x, y)$, odnosno $obrisiPar(x, y)$.

STS.h

```
void STS::zapisiPar(const int x, const int y) {
    if(brojParova[x] == 0) {
        brojTocaka += 1;
        indeksTocke[x] = brojTocaka;
        tocka[brojTocaka] = x;
    }
    brojParova[x] += 1;
    indeksPara[x][y] = brojParova[x];
    par[x][brojParova[x]] = y;
}
```

STS.h

```
void STS::obrisiPar(const int x, const int y) {
    z = par[x][brojParova[x]];
    indeksPara[x][z] = indeksPara[x][y];
    par[x][indeksPara[x][y]] = z;
    indeksPara[x][y] = 0;
    par[x][brojParova[x]] = 0;
    brojParova[x] -= 1;
    if(brojParova[x] == 0) {
        z = tocka[brojTocaka];
        indeksTocke[z] = indeksTocke[x];
        tocka[indeksTocke[x]] = z;
        indeksTocke[x] = 0;
        tocka[brojTocaka] = 0;
        brojTocaka -= 1;
    }
}
```

Za zamjenu i umetanje blokova potrebne su funkcije $zamijeniBlok(x, y, z, w)$, odnosno $umetniBlok(x, y, z)$.

STS.h

```
void STS::zamijeniBlok(const int x, const int y, const int z, const int w) {
    ispisiBlok(w);
    trecaTockaBloka[x][y] = z;
    trecaTockaBloka[y][x] = z;
    trecaTockaBloka[x][z] = y;
    trecaTockaBloka[z][x] = y;
    trecaTockaBloka[y][z] = x;
    trecaTockaBloka[z][y] = x;
    trecaTockaBloka[w][y] = 0;
    trecaTockaBloka[y][w] = 0;
    trecaTockaBloka[w][z] = 0;
    trecaTockaBloka[z][w] = 0;
    zapisiPar(w, y);
    zapisiPar(y, w);
    zapisiPar(w, z);
    zapisiPar(z, w);
    obrisiPar(x, y);
    obrisiPar(y, x);
    obrisiPar(x, z);
    obrisiPar(z, x);
}
```

STS.h

```
void STS::umetniBlok(const int x, const int y, const int z) {
    ispisiBlok(0);
    trecaTockaBloka[x][y] = z;
    trecaTockaBloka[y][x] = z;
    trecaTockaBloka[x][z] = y;
    trecaTockaBloka[z][x] = y;
    trecaTockaBloka[y][z] = x;
    trecaTockaBloka[z][y] = x;
    obrisiPar(x, y);
    obrisiPar(y, x);
    obrisiPar(x, z);
    obrisiPar(z, x);
    obrisiPar(y, z);
    obrisiPar(z, y);
}
```

U svakom koraku konstruira se novi blok kandidat $\{x, y, z\}$ takav da su bilo dva bilo tri para sadržana u njemu nezasićeni parovi. Ako su sva tri para nezasićena, onda se umeće novi blok $\{x, y, z\}$ u sustav. Pritom se veličina sustava povećava za jedan. Ako su samo dva para nezasićena, onda se umeće novi blok $\{x, y, z\}$ u sustav, a uklanja jedinstveni blok $\{w, y, z\}$ koji sadrži par $\{y, z\}$ iz sustava. Pritom se veličina sustava ne mijenja. Dakle, vrši se pretvorba starog parcijalnog Steinerovog sustava trojki u novi parcijalni Steinerov sustav trojki na način da se veličina sustava poveća za jedan ili se ne mijenja. U tu svrhu, koristi se strategija slučajnog traženja.

STS.h

```
void STS::konstruirajBlok() {
    int p((rand() % brojTocaka) + 1);
    x = tocka[p];
    int q((rand() % (brojParova[x] - 1)) + 1);
    int r((rand() % (brojParova[x] - q)) + q + 1);
    y = par[x][q];
    z = par[x][r];
    if(trecaTockaBloka[y][z] == 0) {
        brojBlokova += 1;
        umetniBlok(x, y, z);
    } else {
        w = trecaTockaBloka[y][z];
        zamijeniBlok(x, y, z, w);
    }
}
```

Ispis bloka kandidata $\{x, y, z\}$ izvršava se prilikom zamjene i umetanja bloka.

STS.h

```
void STS::ispisiBlok(const int w) {
    cout << endl << "{x,y,z} = ";
    izlazniTokDatoteke << endl << "{x,y,z} = ";
    cout << "{" << x << "," << y << "," << z << "}";
    izlazniTokDatoteke << "{" << x << "," << y << "," << z << "}";
    cout << "   |B| = " << brojBlokova;
    izlazniTokDatoteke << "   |B| = " << brojBlokova;
    if(w != 0) {
        cout << "   w = " << w;
        izlazniTokDatoteke << "   w = " << w;
    }
}
```

Korištenjem polja *trecaTockBloka* nije potrebno eksplicitno pratiti skup blokova $\mathcal{B}$ tijekom izvršavanja algoritma. Dakle, $\mathcal{B}$ se može izravno konstruirati iz varijable *trecaTockaBloka*.

STS.h

```
void STS::konstruirajB() {
    B.clear();
    for(x = 1; x <= v; ++ x)
        for(y = x + 1; y <= v; ++ y) {
            z = trecaTockaBloka[x][y];
            if(z > y) {
                blok.clear();
                blok.insert(x);
                blok.insert(y);
                blok.insert(z);
                B.insert(blok);
            }
        };
}
```

Ispis skupa blokova $\mathcal{B}$ izvršava se na kraju algoritma.

STS.h

```
void STS::ispisiB() {
    int brojac(0);
    set<int>::iterator blokIter;
    set<set<int> >::iterator BIter;
    cout << endl << "Y = {1,...," << v << "}" << endl;
    izlazniTokDatoteke << endl << "Y = {1,...," << v << "}" << endl;
    cout << "B = {";
    izlazniTokDatoteke << "B = {";
    BIter = B.begin();
    while(BIter != B.end()) {
        blok = *BIter;
        cout << "{";
        izlazniTokDatoteke << "{";
        blokIter = blok.begin();
        while(blokIter != blok.end()) {
            cout << *blokIter;
            izlazniTokDatoteke << *blokIter;
            if(blokIter != (-- blok.end())) {
                cout << ",";
                izlazniTokDatoteke << ",";
            } else {
                cout << "}";
                izlazniTokDatoteke << "}";
            }
            ++ blokIter;
        }
        ++ brojac;
        if(BIter != (-- B.end())) {
            cout << ",";
            izlazniTokDatoteke << ",";
            if((brojac % 3) == 0) {
                cout << endl << "     ";
                izlazniTokDatoteke << endl << "     ";
            }
        } else {
            cout << "}";
            izlazniTokDatoteke << "}";
        }
        ++ BIter;
    }
    cout << endl << "b = " << brojBlokova << endl;
    izlazniTokDatoteke << endl << "b = " << brojBlokova << endl;
    cout << "broj iteracija = " << brojIteracija << endl;
    izlazniTokDatoteke << "broj iteracija = " << brojIteracija << endl;
}

#endif
```

3.3. *Rezultati izvršavanja algoritma*

Prvi rezultat konstruiranja STS(7)-a.

```
{x,y,z} = {5,7,3}   |B| = 1
{x,y,z} = {5,1,2}   |B| = 2
{x,y,z} = {5,6,4}   |B| = 3
{x,y,z} = {1,3,4}   |B| = 4
{x,y,z} = {1,6,7}   |B| = 5
{x,y,z} = {4,7,2}   |B| = 6
{x,y,z} = {6,2,3}   |B| = 7

Y = {1,...,7}
B = {{1,2,5},{1,3,4},{1,6,7},
     {2,3,6},{2,4,7},{3,5,7},
     {4,5,6}}
b = 7
broj iteracija = 7
```

Drugi rezultat konstruiranja STS(7)-a.

```
{x,y,z} = {3,7,1}   |B| = 1
{x,y,z} = {6,7,3}   |B| = 1   w = 1
{x,y,z} = {6,2,4}   |B| = 2
{x,y,z} = {6,5,1}   |B| = 3
{x,y,z} = {4,7,1}   |B| = 4
{x,y,z} = {4,5,3}   |B| = 5
{x,y,z} = {3,2,1}   |B| = 6
{x,y,z} = {2,5,7}   |B| = 7

Y = {1,...,7}
B = {{1,2,3},{1,4,7},{1,5,6},
     {2,4,6},{2,5,7},{3,4,5},
     {3,6,7}}
b = 7
broj iteracija = 8
```

Treći rezultat konstruiranja STS(7)-a.

```
{x,y,z} = {3,1,2}   |B| = 1
{x,y,z} = {3,5,6}   |B| = 2
{x,y,z} = {3,4,7}   |B| = 3
{x,y,z} = {6,1,2}   |B| = 3   w = 3
{x,y,z} = {7,2,6}   |B| = 3   w = 1
{x,y,z} = {7,1,5}   |B| = 4
{x,y,z} = {4,5,1}   |B| = 4   w = 7
{x,y,z} = {6,1,4}   |B| = 4   w = 5
{x,y,z} = {4,2,5}   |B| = 5
{x,y,z} = {2,1,3}   |B| = 6
{x,y,z} = {1,7,5}   |B| = 7

Y = {1,...,7}
B = {{1,2,3},{1,4,6},{1,5,7},
     {2,4,5},{2,6,7},{3,4,7},
     {3,5,6}}
b = 7
broj iteracija = 11
```

Prvi rezultat konstruiranja STS(9)-a.

```
{x,y,z} = {8,3,4}   |B| = 1
{x,y,z} = {8,2,5}   |B| = 2
{x,y,z} = {8,9,7}   |B| = 3
{x,y,z} = {8,6,1}   |B| = 4
{x,y,z} = {1,5,7}   |B| = 5
{x,y,z} = {1,4,9}   |B| = 6
{x,y,z} = {1,2,3}   |B| = 7
{x,y,z} = {4,7,2}   |B| = 8
{x,y,z} = {4,5,6}   |B| = 9
{x,y,z} = {3,6,7}   |B| = 10
{x,y,z} = {5,9,3}   |B| = 11
{x,y,z} = {9,6,2}   |B| = 12

Y = {1,...,9}
B = {{1,2,3},{1,4,9},{1,5,7},
     {1,6,8},{2,4,7},{2,5,8},
     {2,6,9},{3,4,8},{3,5,9},
     {3,6,7},{4,5,6},{7,8,9}}
b = 12
broj iteracija = 12
```

Drugi rezultat konstruiranja STS(9)-a.

```
{x,y,z} = {3,1,2}   |B| = 1
{x,y,z} = {3,6,8}   |B| = 2
{x,y,z} = {3,4,9}   |B| = 3
{x,y,z} = {1,6,7}   |B| = 4
{x,y,z} = {1,8,5}   |B| = 5
{x,y,z} = {1,4,9}   |B| = 5   w = 3
{x,y,z} = {3,7,9}   |B| = 6
{x,y,z} = {3,4,5}   |B| = 7
{x,y,z} = {5,7,9}   |B| = 7   w = 3
{x,y,z} = {4,6,8}   |B| = 7   w = 3
{x,y,z} = {4,2,7}   |B| = 8
{x,y,z} = {5,6,2}   |B| = 9
{x,y,z} = {2,9,8}   |B| = 10
{x,y,z} = {6,9,3}   |B| = 11
{x,y,z} = {8,7,3}   |B| = 12

Y = {1,...,9}
B = {{1,2,3},{1,4,9},{1,5,8},
     {1,6,7},{2,4,7},{2,5,6},
     {2,8,9},{3,4,5},{3,6,9},
     {3,7,8},{4,6,8},{5,7,9}}
b = 12
broj iteracija = 15
```

Treći rezultat konstruiranja STS(9)-a.

```
{x,y,z} = {1,6,9}   |B| = 1
{x,y,z} = {1,8,7}   |B| = 2
{x,y,z} = {5,7,9}   |B| = 3
{x,y,z} = {5,6,1}   |B| = 3   w = 9
{x,y,z} = {5,8,3}   |B| = 4
{x,y,z} = {5,2,4}   |B| = 5
{x,y,z} = {7,6,2}   |B| = 6
{x,y,z} = {7,4,3}   |B| = 7
{x,y,z} = {9,3,6}   |B| = 8
{x,y,z} = {9,1,4}   |B| = 9
{x,y,z} = {9,8,2}   |B| = 10
{x,y,z} = {1,2,3}   |B| = 11
{x,y,z} = {6,4,8}   |B| = 12

Y = {1,...,9}
B = {{1,2,3},{1,4,9},{1,5,6},
     {1,7,8},{2,4,5},{2,6,7},
     {2,8,9},{3,4,7},{3,5,8},
     {3,6,9},{4,6,8},{5,7,9}}
b = 12
broj iteracija = 13
```

Rezultat konstruiranja STS(13)-a.

```
{x,y,z} = {5,12,4}   |B| = 1
{x,y,z} = {5,10,2}   |B| = 2
{x,y,z} = {5,8,13}   |B| = 3
{x,y,z} = {5,6,11}   |B| = 4
{x,y,z} = {5,1,3}   |B| = 5
{x,y,z} = {5,9,7}   |B| = 6
{x,y,z} = {7,11,13}   |B| = 7
{x,y,z} = {11,2,10}   |B| = 7   w = 5
{x,y,z} = {13,4,10}   |B| = 8
{x,y,z} = {13,1,9}   |B| = 9
{x,y,z} = {2,13,5}   |B| = 9   w = 8
{x,y,z} = {2,3,12}   |B| = 10
{x,y,z} = {2,4,1}   |B| = 11
{x,y,z} = {2,8,7}   |B| = 12
{x,y,z} = {3,4,6}   |B| = 13
{x,y,z} = {3,11,13}   |B| = 13   w = 7
{x,y,z} = {3,10,7}   |B| = 14
{x,y,z} = {3,9,8}   |B| = 15
{x,y,z} = {9,10,11}   |B| = 15   w = 2
{x,y,z} = {9,4,12}   |B| = 15   w = 5
{x,y,z} = {9,2,6}   |B| = 16
{x,y,z} = {4,5,8}   |B| = 17
{x,y,z} = {4,11,7}   |B| = 18
{x,y,z} = {8,13,6}   |B| = 19
{x,y,z} = {7,6,12}   |B| = 20
{x,y,z} = {7,1,13}   |B| = 20   w = 9
{x,y,z} = {9,1,13}   |B| = 20   w = 7
{x,y,z} = {7,1,13}   |B| = 20   w = 9
{x,y,z} = {12,8,10}   |B| = 21
{x,y,z} = {12,13,5}   |B| = 21   w = 2
{x,y,z} = {12,11,1}   |B| = 22
{x,y,z} = {9,1,13}   |B| = 22   w = 7
{x,y,z} = {13,7,2}   |B| = 22   w = 8
{x,y,z} = {7,1,8}   |B| = 23
{x,y,z} = {11,2,8}   |B| = 24
{x,y,z} = {1,10,6}   |B| = 25
{x,y,z} = {2,5,10}   |B| = 26

Y = {1,...,13}
B = {{1,2,4},{1,3,5},{1,6,10},
     {1,7,8},{1,9,13},{1,11,12},
     {2,3,12},{2,5,10},{2,6,9},
     {2,7,13},{2,8,11},{3,4,6},
     {3,7,10},{3,8,9},{3,11,13},
     {4,5,8},{4,7,11},{4,9,12},
     {4,10,13},{5,6,11},{5,7,9},
     {5,12,13},{6,7,12},{6,8,13},
     {8,10,12},{9,10,11}}
b = 26
broj iteracija = 37
```

Naravno, ne postoji jamstvo da algoritam ikada staje. Međutim, budući da su izbori koje radi funkcija *konstruirajBlok*() slučajni, čini se da će u praksi algoritam uvijek stati konstruirajući pritom STS(v). Također, algoritam se u praksi često izvršava jako brzo.

Primjer 3.5. *Za svaki* $v \in \{31, 61, 91, ..., 301\}$ *izvedeno je deset izvršavanja algoritma, te je prilikom svakog zabilježen broj iteracija do dobivanja STS*(v)*-a.*

v	b	*prosječan broj iteracija*	$b \ln b$	$\frac{\text{prosječan broj iteracija}}{b \ln b}$
31	*155*	*563,6*	*781,731*	*0,721*
61	*610*	*2.410,3*	*3.912,210*	*0,616*
91	*1365*	*5.523,3*	*9.853,812*	*0,561*
121	*2420*	*10.125,2*	*18.855,485*	*0,537*
151	*3775*	*15.927,8*	*31.091,488*	*0,512*
181	*5430*	*23.727,9*	*46.696,341*	*0,508*
211	*7385*	*32.895,2*	*65.779,718*	*0,500*
241	*9640*	*43.289,6*	*88.434,240*	*0,490*
271	*12195*	*55.711,7*	*114.740,088*	*0,486*
301	*15050*	*69.288,3*	*144.767,956*	*0,479*

Slika 13. Prosječan broj iteracija.

Iz navedenih podataka vidljivo je da prosječan broj iteracija raste dosta sporo s porastom vrijednosti v*, odnosno* b*. Štoviše, hipoteza je da je prosječan broj iteracija asimptotski jednak broju* $b \ln b$*. Hipotezu potvrđuje tablica iz koje je vidljivo da vrijedi*

$$\textit{prosječan broj iteracija} = O(b \ln b).$$

Indeks

algoritam
  „planinarenja“, 61
  heuristički, 61
  Stinsonov, 61
automorfizam, 56

blokovi, 2
  nepotpuni, 3
  ponavljani, 2

ciklus, 57
  duljina, 57

dizajn, 2
  blokovni, 3
    derivirani, 27
    izomorfni, 50
    rezidualni, 27
    simetrični, 20
  dulani, 14
  jednostavni, 2

Fisherova nejednakost, 15

grupa
  automorfizama, 58
  permutacija, 58

heuristika, 61

izomorfizam, 50

konstrukcija
  Boseova, 41
  Skolemova, 45
kvazigrupa, 33
  idempotentna, 34
  poluidempotentna, 38
  simetrična, 34

latinski kvadrat, 33
  idempotentni, 34
  simetrični, 34

matrica incidencije, 11

operacijska tablica, 34

par
  nezasićeni, 66
  zasićeni, 66

permutacije
  fiksna točka, 57
  red, 57
permutacijska matrica, 53
pravci, 2

replikacijski broj, 7

sustav trojki, 31
  Steinerov, 31
    parcijalni, 62
svojstvo ravnoteže, 3

teorija dizajna, 1
točka, 2
  nezasićena, 66
  zasićena, 66

Literatura

[Che] **Bill Cherowitzo**,
Combinatorial designs: balanced incomplete block designs,
`http://www-math.cudenver.edu/~wcherowi/courses/m6409/Blockdesigns.pdf`.

[JC] **Peter J. Cameron**,
Encyclopaedia of design theory,
`http://designtheory.org/library/encyc`.

[JCR99] **Charles J. Colbourn**, **Alexander Rosa**,
Triple systems,
Oxford University Press, 1999.

[KRJO04] **Pettrei Kaski**, **Patric R. J. Östergård**,
The Steiner triple systems of order 19,
Mathematics of Computation, 2004, svezak 73, broj 248,
stranice 2075–2092.

[LKRS99] **Donald L. Kreher**, **Douglas R. Stinson**,
Combinatorial algorithms: generation, enumeration, and search,
CRC Press LLC, 1999.

[RS04] **Douglas R. Stinson**,
Combinatorial designs: constructions and analysis,
Springer-Verlag, 2004.

[WW] **Eric W. Weisstein**,
MathWorld,
`http://mathworld.wolfram.com`.