

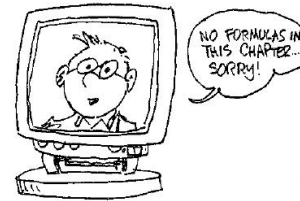
## II.8. Načrtovanje eksperimentov



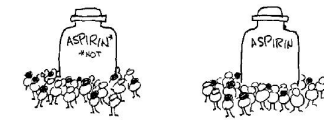
Načrtovanje eksperimentov se pogosto neposredno prevede v uspeh oziroma neuspeh.

V primeru parjenja lahko statistik spremeni svojo vlogo iz pasivne v aktivno.

Predstavimo samo osnovne ideje, podrobno numerično analizo pa prepustimo statistični programski opremi.



Elementi načrta so eksperimentalne enote ter terapije, ki jih želimo uporabiti na enotah.



- medicina: bolniki (enote) in zdravila (terapije),
- optimizacija porabe: taxi-ji (enote) in različne vrste goriva (terapije),
- agronomija: območja na polju in različne vrste kulture, gnojiva, špricanja,...

Danes uporabljamo ideje načrtovanja eksperimentov na številnih področjih:

- optimizacija industrijskih procesov,
- medicina,
- sociologija.



Na primeru bomo predstavili tri osnovne principe načrtovanja eksperimentov:

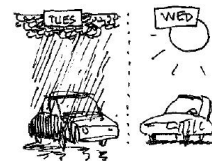
1. **Ponavljanje:** enake terapije pridružimo različnim enotam, saj ni mogoče oceniti naravno spremenljivost (ang. natural variability) in napake pri merjenju.

2. **Lokalna kontrola** pomeni vsako metodo, ki zmanjša naravno spremenljivost.

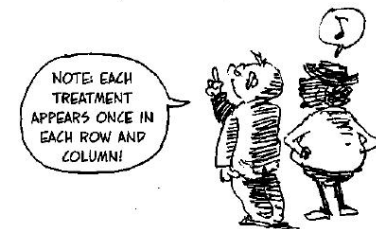
En od načinov grupira podobne enote eksperimentov v **bloke**. V primeru taxijev uporabimo obe vrsti goriva na vsakem avtomobilu in rečemo, da je avto blok.



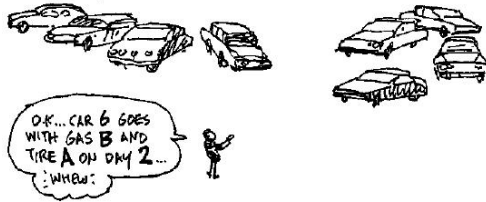
3. **Naključna izbira** je bistven korak povsod v statistiki! Terapije za enote izbiramo naključno. Za vsak taxi izberemo vrsto goriva za torek oziroma sredo z metom kovanca. Če tega ne bi storili, bi lahko razlika med torkom in sredo vplivala na rezultate.



		DAY			
		1	2	3	4
CAB	1	a	b	c	d
	2	b	c	d	a
	3	c	d	a	b
	4	d	a	b	c



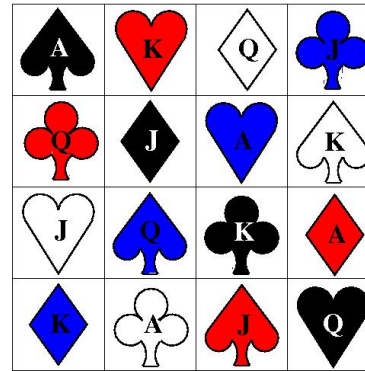
## Latinski kvadrati



**Latinski kvadrat** reda  $v$  je  $v \times v$ -razsežna matrika, v kateri vsi simboli iz množice

$$\{1, \dots, v\}$$

nastopajo v vsaki vrstici in vsakem stolpcu.



Trije paroma ortogonalni latinski kvadrati reda 4, tj. vsak par znak-črka ali črka-barva ali barva-znak se pojavi natanko enkrat.

**Projektivni prostor**  $PG(d, q)$  (razsežnosti  $d$  nad  $q$ ) dobimo iz vektorskega prostora  $[GF(q)]^{d+1}$ , tako da naredimo kvocient po 1-razsežnih podprostorih.

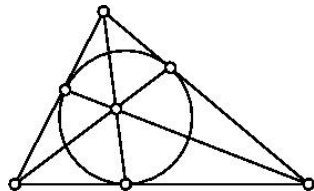
**Projektivna ravnina**  $PG(2, q)$  je incidenčna struktura z 1- in 2-dim. podprostori prostora  $[GF(q)]^3$  kot **točkami** in **premicami**, kjer je “ $\subset$ ” incidenčna relacija. To je  $2$ - $(q^2 + q + 1, q + 1, 1)$ -design, tj.,

- $v = q^2 + q + 1$  je število točk (in število premic  $b$ ),
- vsaka premica ima  $k = q + 1$  točk (in skozi vsako točko gre  $r = q + 1$  premic),
- vsak par točk leži na  $\lambda = 1$  premicah (in vsaki premici se sekata v natanko eno točki).

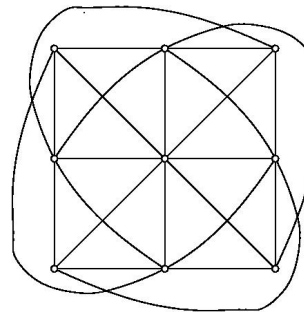
Primeri:

1. Projektivno ravnino  $PG(2, 2)$  imenujemo

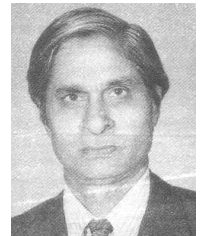
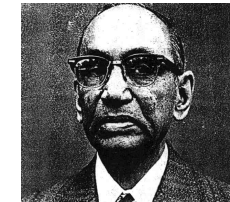
**Fano ravnina** (7 točk in 7 premic).



2.  $PG(2, 3)$  lahko skonstruiramo iz  $3 \times 3$  mreže oziroma afine ravnine  $AG(2, 3)$ .



Bose in Shrikhande

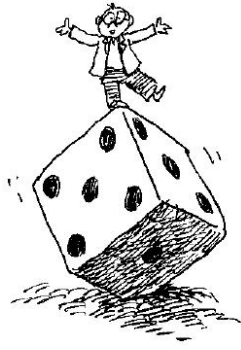


Prva sta konec tridesetih let prejšnjega stoletja vpeljala **asociativne sheme Bose in Nair** a potrebe statistike.

Toda **Delsarte** je pokazal, da nam lahko služijo kot povezava med številnimi področji matematike, naprimer teorijo kodiranja in teorijo načrtov.

### III. ZAKLJUČKI

Osnovni principi in orodja, ki smo jih spoznali pri VIS, lahko posplošimo in razširimo do te mere, da se dajo z njimi rešiti tudi bolj kompleksni problemi.



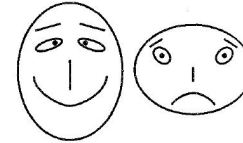
Spoznali smo kako predstaviti **eno** spremenljivko (dot-plot, histogrami,...) in **dve** spremenljivki (razsevni diagram).

#### Kako pa predstavimo več kot dve spremenljivki na ravnem listu papirja?

Med številnimi možnostmi moramo omeniti idejo **Hermana Chernoffa**, ki je uporabil človeški obraz, pri čemer je vsako lastnost povezal z eno spremenljivko.

Oglejmo si Chernoffov obraz:

$X$  = naklon obrvi,  
 $Y$  = velikost oči,  
 $Z$  = dolžina nosu,  
 $T$  = dolžina ust,  
 $U$  = višino obraza,  
 itd.



### Multivariantna analiza

Širok izbor multivariantnih modelov nam omogoča analizo in ponazoritev  $n$ -razsežnih podatkov.

Združevalna/grozdna tehnika (ang. cluster technique):

Iskanje delitve populacije na homogene podskupine, npr. z analizo vzorcev senatorskih glasovanj v ZDA zaključimo, da *jug* in *zahod* tvorita dva različna grozda.



### Diskriminacijska analiza

je obraten proces. Npr. odbor/komisija za sprejem novih študentov bi rad našel podatke, ki bi že vnaprej opozorili ali bodo prijavljeni kandidati nekega dne uspešno zaključili program (in finančno pomagali šoli - npr. z dobrodelnimi prispevki) ali pa ne bodo uspešni (gre delati dobro po svetu in šola nikoli več ne sliši zanj(o)).



### Analiza faktorjev

išče poenostavljeno razlago večrazsežnih podatkov z manjšo skupino spremenljivk.

Npr. Psihiater lahko postavi 100 vprašanj, skrivoma pa pričakuje, da so odgovori odvisni samo od nekaterih faktorjev:

ekstravertiranost,  
 avtoritativnost,  
 alutarizem, itd.



Rezultate testa lahko potem povzamemo le z nekaterimi sestavljenimi rezultati v ustreznih dimenzijah.

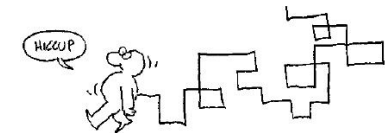
### Naključni sprehodi

pričnejo z metom kovanca, recimo, da se pomaknemo korak nazaj, če pade grb, in korak naprej, če pade cifra. (z dvema kovancema se lahko gibljemo v 2-razsežnem prostoru - tj. ravnini).

Če postopek ponavljamo, pridemo do

*stohastičnega procesa*,

ki ga imenujemo naključni sprehod (ang. random walk).

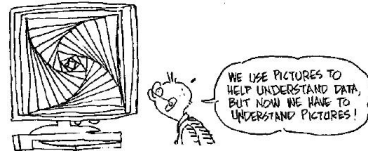


Modeli na osnovi naključnih sprehodov se uporabljajo za nakup/prodajo delnic in portfolio management.

## Vizualizacija in analiza slik

Sliko lahko sestavlja  $1000 \times 1000$  pikselov, ki so predstavljeni z eno izmed 16,7 milijonov barv.

Statistična analiza slik želi najti nek pomen iz "informacije" kot je ta.



## Ponovno vzorčenje

Pogosto ne moremo izračunati standardne napake in limite zaupanja.

Takrat uporabimo tehniko ponovnega vzorčenja, ki tretira vzorec, kot bi bila celotna populacija.

Za takšne tehnike uporabljamo pod imeni:

randomization  
Jackknife, in  
Bootstrapping.



## Kvaliteta podatkov

navidezno majhne napake pri vzorčenju, merjenju, zapisovanju podatkov, lahko povzročijo katastrofalne učinke na vsako analizo.

R. A. Fisher, genetik in ustanovitelj moderne statistike ni samo načrtoval in analiziral eksperimentalno rejo, pač pa je tudi čistil kletke in pazil na živali. Zavedal se je namreč, da bi izguba živali vplivala na rezultat.



Moderni statistiki, z njihovimi računalniki in podatkovnimi bazami ter vladnimi projekti (beri denarjem) si pogosto ne umažejo rok.

## Inovacija

Najboljše rešitve niso vedno v knjigah (no vsaj najti jih ni kar tako).

Npr. Mestni odpad je najel strokovnjake, da ocenijo kaj sestavljajo odpadki, le-ti pa so se znašli pred zanimivimi problemi, ki se jih ni dalo najti v standardnih učbenikih.



## Komunikacija

Še tako uspešna in bistroumna analiza je zelo malo vredna, če je ne znamo jasno predstaviti, vključujoč stopnjo statistične značilnosti? v zaključku.



Npr. V medijih danes veliko bolj natančno poročajo o velikosti napake pri svojih anketah.

## Timsko delo

V današnji kompleksni družbi.

Reševanje številnih problemov zahteva *timsko delo*.

Inženirji, statistiki in delavci sodelujejo, da bi izboljšali kvaliteto produktov.

Biostatistiki, zdravniki, in AIDS-aktivisti združeno sestavljajo klinične poiskuse, ki bolj učinkovito ocenijo terapije.



## III.2. Ramseyjeva teorija

- intuitivna ideja
- Ramseyjev izrek
- Erdősev izrek
- primeri uporabe



Po 3,500 let starem zapisu je antični sumerski učenjak pogledal v nebo in zagledal leva, bika in škorpijona.

### Ali gre za kozmične sile?

Astronom bi rekel: kolekcija zvezd, tj. začasna konfiguracija zvezd, ki jo gledamo z roba navadne galaksije.

### 1928 Frank Plumpton Ramsey

(26 let, angleški matematik, filozof in ekonomist)

**Popoln nered je nemogoč.**

**Ramseyjeva teorija:** Vsaka dovolj velika struktura vsebuje urejeno podstrukturo.

**Konkretna naloga:** Koliko objektov nam zagotavlja željeno podstrukturo?

### “Intuicija”

**Izrek (SIM).** V družbi šestih ljudi obstaja trojica v kateri se vsaka dva poznata ali pa vsaka dva ne poznata.

- naivni prestop: preverimo  $2^{15} = 32.768$  možnosti,
- barvanje povezav polnega grafa  $K_6$  in Dirichletov princip.

### Nekaj težja naloga

V družbi 17ih znanstvenikov se vsaka dva dopisujeta o eni izmed treh tem. Dokaži, da obstajajo trije, ki se dopisujejo o isti temi!

**Ramseyjevo število**  $r(k, \ell)$  je najmanjše število za katerega vsak graf na  $r(k, \ell)$  vozliščih vsebuje bodisi  $k$ -kliko bodisi  $\ell$ -antikliko.

Prepričaj se, da je  $r(k, \ell) = r(\ell, k)$ .

### Primeri:

$$r(k, 1) = 1 = r(1, \ell),$$

$$r(2, \ell) = \ell, \quad r(k, 2) = k,$$

$$\text{SIM: } r(3, 3) \leq 6.$$

### Ramseyjev izrek

**Izrek.**  $\forall k, \ell \in \mathbb{N}$

$$r(k, \ell) \leq r(k, \ell - 1) + r(k - 1, \ell).$$

Če sta obe števili na desni strani neenakosti sodi, potem velja stroga neenakost.

Zgled uporabe:

$$r(3, 3) \leq r(3, 2) + r(2, 3) = 3 + 3 = 6.$$

**Dokaz:** 1935 Erdős & Szekeres, 1955 Greenwood & Gleason

Naj bo  $G$  graf na  $r(k, \ell - 1) + r(k - 1, \ell)$  vozliščih.

Potem velja ena izmed naslednjih možnosti:

(a) Vozlišče  $v$  ni sosednje množici  $S$  z vsaj  $r(k, \ell - 1)$  vozlišči. kar pomeni, da  $G[S]$  vsebuje ali  $k$ -kliko ali  $(\ell - 1)$ -antikliko.

(b) Vozlišče  $v$  je sosednje množici  $T$  z vsaj  $r(k - 1, \ell)$  vozlišči. kar pomeni, da  $G[T]$  vsebuje ali  $(k - 1)$ -kliko ali  $\ell$ -antikliko.

Od tod sledi, da  $G$  vsebuje bodisi  $k$ -kliko bodisi  $\ell$ -antikliko.

Naj bosta  $r(k, \ell - 1)$  in  $r(k - 1, \ell)$  sodi števili in

$$|G| = r(k, \ell - 1) + r(k - 1, \ell) - 1.$$

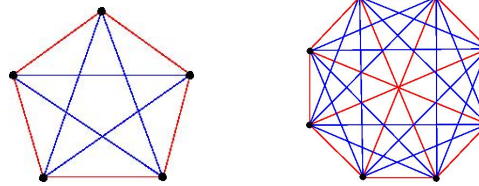
Potem obstaja vozlišče  $v \in V(G)$ , katerega stopnja je sodo število.

Torej  $v$  ni sosedeno točno  $r(k - 1, \ell) - 1$  vozliščem in velja bodisi (a) bodisi (b). ■

Pokaži:

$$r(3, 4) \leq 9, \quad r(3, 5) \leq 14, \quad r(4, 4) \leq 18, \quad r(k, \ell) \leq \binom{k + \ell - 2}{k - 1}.$$

To je bila zgornja meja. Kaj pa spodnja meja?



$$5 < r(3, 3) = 6$$

$$8 < r(3, 4) = 9$$

Podobno dobimo tudi  $13 < r(3, 5) = 14$ ,  $17 < r(3, 6) = 18$ ,  
 $22 < r(3, 7) = 23$ ,  $27 < r(3, 8) \leq 29$  in  $35 < r(3, 9) = 36$ .

## Erdős ev izrek

**Izrek.**  $\forall k \in \mathbb{N}$

$$r(k, k) \geq 2^{k/2}.$$

Zgled uporabe:

$$r(3, 3) \geq 3 \quad \text{and} \quad r(4, 4) \geq 4.$$

## Marsovci napadejo Zemljo

Morda nam uspe izračunati  $r(5, 5) \in [43, 49]$   
 (Exoo 1989, McKay and Radziszowski 1995),

nikakor pa ne moremo izračunati  $r(6, 6) \in [102, 165]$   
 (Kalbfleisch 1965, Mackey 1994).

Znana Ramseyeva števila:

$k \setminus \ell$	3	4	5	6	7	8	9	10
3	6	9	14	18	23	28	36	?
4	9	18	25	?	?	?	?	?
6	18	?	?	?	?	?	?	?

Ester Klein je leta 1933 predstavil naslednjo geometrijsko nalogo:

Med petimi točkami v ravnini, od katerih nobene tri niso kolinearne (ležijo na premici), lahko vedno izberemo štiri, ki določajo konveksen četverokotnik.

Rešitev: Vpeljemo pojem **konveksne ogrinjače** ...

Če je konveksna ogrinjača teh petih točk

- petkotnik, potem vsake 4 točke med njimi sestavljajo konveksen četverokotnik,
  - štirikotnik, potem so njegovi vrhovi tiste 4 točke, ki smo jih iskali,
  - trikotnik, potem ga lahko označimo z  $A$ ,  $B$  in  $C$ , preostali točki pa z  $D$  in  $E$ , tako da sta točki  $A$  in  $B$  na isti strani premice  $DE$ .
- V tem primeru je četverokotnik  $ABCD$  konveksen. ■

Nalogo lahko posplošimo na 9 točk in iskanje konveksnega petkotnika ter počasi pridemo do Erdős eve domneve, da za konveksen  $k$ -kotnik potrebujemo v ravnini vsaj

$$n = 1 + 2^{k-2}$$

točk od katerih nobene 3 niso kolinearne.

Pravzaprav se je najprej Szekeres prepričal, da za dovolj velik  $n$  vedno obstaja konveksen  $k$ -kotnik, potem pa je Erdős postavil svojo domnevo.

Erdőseva probabilistična metoda (1947)

34 točk določa 561 premic. Da se to zgodi v eni barvi, je verjetnost

$$2^{-561} \approx 2,6 \cdot 10^{-169}.$$

Velja tudi  $\binom{1.000.000}{34} = 3,4 \cdot 10^{165}$ . Torej lahko pričakujemo

$$\left(\frac{10^6}{34}\right) = 3,4 \cdot 10^{165} \approx 0,01$$

oziroma 0,01% enobarvnih.

To pomeni, da v 99,9% ne dobimo enobarvnega  $K_{34}$ .

Slednjo idejo pretvorimo v Erdősev dokaz....

**Dokaz Erdősevega izreka:**

probabilistična metoda (ni konstruktivna) in štetje

Naj bo  $\mathcal{G}_n$  množica grafov z vozlišči  $v_1, v_2, \dots, v_n$ .

Naj bo  $\mathcal{G}_n^k$  množica grafov iz  $\mathcal{G}_n$ , ki vsebujejo  $k$ -klike.

Potem je  $|\mathcal{G}_n| = 2^{\binom{n}{2}}$ ,  $|\mathcal{G}_n^k| = 2^{\binom{n}{2} - \binom{k}{2}} \binom{n}{k}$  in

$$q = \frac{|\mathcal{G}_n^k|}{|\mathcal{G}_n|} \leq \frac{n^k 2^{-\binom{k}{2}}}{k!}.$$

Če je  $n < 2^{k/2}$ , velja  $q \leq \frac{2^{\frac{k^2}{2} - \binom{k}{2}}}{k!} < \frac{1}{2}$ .

Se pravi, da manj kot polovica grafov iz  $\mathcal{G}_n$  vsebuje  $k$ -klike.

Iz  $\mathcal{G}_n = \{G \mid \bar{G} \in \mathcal{G}_n\}$  pa sledi, da manj kot polovica grafov iz  $\mathcal{G}_n$  vsebuje  $k$ -antiklike. ■

**Posledica.** Za  $m := \min(k, \ell)$  velja

$$r(k, \ell) \geq 2^{m/2}.$$

### Uporaba

Pobarvaj z **modro** in **rdečo** števila

1 2 3 4 5 6 7 8 9.

**Posledica Ramseyjevega izreka (Waerden 1926):**

3 rdeča ali 3 modra števila tvorijo aritmetično zaporedje.

**Dodatno branje:**

R. L. Graham and J. H. Spencer, Ramsey Theory,

Scientific American July 1990, 112–117.

PODVOJ(x) = 2x

EKSPONENT(x) = 2<sup>x</sup>

STOLP(x) = 2<sup>2<sup>...<sup>2</sup></sup></sup> (x dvojk)

UAU(1) = STOLP(1)=2.

UAU(2) = STOLP(2)=4.

UAU(3) = STOLP(4)=65,536

UAU(4) = prevelik za vse knjige, za vse računalnike ...

UAU(x) = ...

Zaporedje 1, 2, ..., ACKERMANN(k) pobarvamo z dvema barvama. Potem obstaja monokromatično (enobarvno) aritmetično podzaporedje s k členi.

## III.3. Teorija informacij

**Claude Shannon** je postavil teoretične osnove **teorije informacij** in zanesljivega prenosa digitalnih podatkov kmalu po koncu druge svetovne vojne.



## III.4. Teorije kodiranja, glavni mejniki

**1947-48:** začetki teorije informacij: znamenita izreka o “**Source Coding**” in pa “**Channel Capacity**” (C. Shannon)

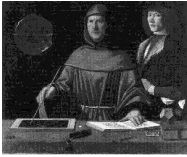
**1949-50:** odkritje **prvih kod** za odpravljanje napak (M. Golay, R. Hamming).

**1959-60:** odkritje **BCH-kod** (R. Bose, D. Ray-Chaudhuri, A. Hocquenghem).

**1967:** Viterby algoritma za odkodiranje **konvolucijskih kod**, (ki sta jih predlagala Elias 1955, Hagelbarger 1959).

**1993:** razvoj **turbo kod** (C. Berrou, A. Glavieux, P. Titimajshima).

Pacioli, Euler, Poincare,...



OUR HUMBLE OPINION IS THAT LEARNING A LITTLE MORE ABOUT THE SUBJECT MIGHT NOT BE SUCH A BAD IDEA... AND THAT'S WHY WE WROTE THIS BOOK!

