



**FRI, Univerza v Ljubljani**

## **Verjetnostni račun in statistika**

**Aleksandar Jurišić**



Ljubljana, 6. oktober 2008

# Kazalo

|     |  |     |
|-----|--|-----|
| 5   | <b>Predstavitev</b> . . . . .                        | 5   |
| 6   | <b>Verjetnost in statistika [20116]</b> . . . . .    | 6   |
| 7   | <b>Obveznosti študenta</b> . . . . .                 | 7   |
| 8   | <b>Viri</b> . . . . .                                | 8   |
| 1   | <b>UVOD</b> . . . . .                                | 1   |
| 2   | <b>1. Igre na srečo</b> . . . . .                    | 2   |
| 6   | <b>2. Kaj je statistika?</b> . . . . .               | 6   |
| 63  | <b>3. Zamenjalna šifra</b> . . . . .                 | 63  |
| 74  | <b>KOMBINATORIKA (ponovitev)</b> . . . . .           | 74  |
| 89  | <b>I. VERJETNOST</b> . . . . .                       | 89  |
| 90  | <b>I.1. Poskusi, dogodki in verjetnost</b> . . . . . | 90  |
| 101 | <b>I.2. Definicija verjetnosti</b> . . . . .         | 101 |

|     |   |     |
|-----|---|-----|
| 114 | <b>I.3. Pogojna verjetnost</b> . . . . .  | 114 |
| 143 | <b>I.4. Bernoullijevo zaporedje neodvisnih poskusov</b> . . . . .                                 | 143 |
| 152 | <b>I.5. Slučajne spremenljivke in porazdelitve</b> . . . . .                                      | 152 |
| 184 | <b>I.6. Slučajni vektorji in neodvisnost slučajnih spremenljivk</b> . . .                         | 184 |
| 207 | <b>I.7. Funkcije slučajnih spremenljivk/vektorjev</b><br><b>in pogojne porazdelitve</b> . . . . . | 207 |
| 224 | <b>I.8. Momenti in kovarianca</b> . . . . .   | 224 |
| 247 | <b>I.9. Karakteristične funkcije in limitni izreki</b> . . . . .                                  | 247 |
| 264 | <b>I.10. Uporaba</b> . . . . .  | 264 |
| 272 | <b>II. STATISTIKA</b> . . . . .   | 272 |
| 273 | <b>II.1. Osnovni pojmi</b> . . . . .  | 273 |
| 291 | <b>II.2. Vzorčenje</b> . . . . .  | 291 |
| 313 | <b>II.3. Cenilke</b> . . . . .  | 313 |

|     |   |     |
|-----|---|-----|
| 372 | <b>II.4. Intervali zaupanja</b>                 | 372 |
| 421 | <b>II.5. Preizkušanje statističnih domnev</b>   | 421 |
| 574 | <b>II.6. Bivariantna analiza in regresija</b>   | 574 |
| 645 | <b>II.7 Časovne vrste</b>                       | 645 |
| 673 | <b>II.8. Načrtovanje eksperimentov</b>          | 673 |
| 685 | <b>III. ZAKLJUČKI</b>                           | 685 |
| 698 | <b>III.2. Ramseyjeva teorija</b>                | 698 |
| 714 | <b>III.3. Teorija informacij</b>                | 714 |
| 715 | <b>III.4. Teorije kodiranja, glavni mejniki</b> | 715 |

# Predstavitev

**Aleksandar Jurišić**

FRI, Jadranska 21, soba 5

e-pošta: [ajurisic@valjhun.fmf.uni-lj.si](mailto:ajurisic@valjhun.fmf.uni-lj.si)

WWW: <http://lkrv.fri.uni-lj.si/~ajurisic>

asistenta:

**mag. Gregor Šega** ([gregor.sega@fmf.uni-lj.si](mailto:gregor.sega@fmf.uni-lj.si)) in

**univ. dip. ing. Peter Nose** ([peter.nose@gmail.com](mailto:peter.nose@gmail.com))

## Verjetnost in statistika [20116]

**Cilj predmeta:** predstaviti osnove teorije verjetnosti in njeno uporabo v statistiki, predstaviti osnove statistike.

**Kratka vsebina:** definicija verjetnosti, slučajne spremenljivke in vektorji, diskretne in zvezne porazdelitve, matematično upanje, disperzija in višji momenti, karakteristične funkcije, zaporedja slučajnih spremenljivk in slučajni procesi, osnovna naloga statistike, ocenjevanje parametrov, testiranje statističnih hipotez, analiza variance, kovariance in linearne regresije.

## Obveznosti študenta

Uspešno opravljena *kolokvija*.  
Če ni šlo, je potrebno opraviti  
*pisni izpit* iz reševanja nalog.

Ko ima enkrat pozitivno oceno iz  
reševanja nalog, mora v tekočem letu  
opraviti še *izpit iz teorije*  
(lahko je pisni ali ustni -  
odvisno od števila prijavljenih).



## Viri

Pri predavanjih se bomo pretežno opirali na naslednje knjige/skripte:

W. Mendenhall in T. Sincich, *Statistics for engineering and the sciences*, 4th edition, Prentice Hall, 1995.

D. S. Moore (Purdue University), *Statistika: znanost o podatkih* (5. izdaja prevedena v slovenščino leta 2007).

M. Hladnik: *Verjetnost in statistika*. Založba FE in FRI, Ljubljana 2002.

A. Ferligoj: *Osnove statistike na prosojnicah*. Samozaložba, Ljubljana 1995.

L. Gonick in W. Smith, *The Cartoon guide to Statistics*, 1993.

Obstaja obilna literatura na spletu in v knjižnicah.



Gradiva bodo dosegljiva preko internetne učilnice (moodle).



Pri delu z dejanskimi podatki se bomo v glavnem naslonili na prosti statistični program **R**.

Program je prosto dostopen na:

<http://www.r-project.org/>

proti koncu semestra pa morda tudi Minitab.



## UVOD



# 1. Igre na srečo

Ste se kdaj vprašali, zakaj so igre na srečo, ki so za nekatere rekreacija ali pa droga, tako dober posel za igralnice?



Vsak uspešen posel mora iz uslug, ki jih ponuja, kovati napovedljive dobičke. To velja tudi v primeru, ko so te usluge igre na srečo.

Posamezni hazarderji lahko zmagajo ali pa izgubijo. Nikoli ne morejo vedeti, če se bo njihov obisk igralnice končal z dobičkom ali z izgubo.



Igralnica pa ne kocka, pač pa dosledno dobiva in država lepo služi na račun loterij ter drugih oblik iger na srečo.



Presenetljivo je, da lahko skupni rezultat več 1000 naključnih izidov poznamo s skoraj popolno gotovostjo. Igralnici ni potrebno obtežiti kock, označiti kart ali spremeniti kolesa rulete. Ve, da ji bo na dolgi rok vsak stavljeni euro prinesel približno 5 centov dobička.



Splača se ji torej osredotočiti na brezplačne predstave ali poceni avtobusne vozovnice, da bi privabili več gostov in tako povečali število stavljenega denarja. Posledica bo večji dobiček.

Igralnice niso edine, ki se okoriščajo z dejstvom,  
da so velikokratne ponovitve slučajnih izidov napovedljive.



Na primer, čeprav zavarovalnica ne ve, kateri  
od njenih zavarovancev bodo umrli v prihodnjem letu,  
lahko precej natančno napove, koliko jih bo umrlo.  
Premije življenjskih zavarovanj postavi v skladu  
s tem znanjem, ravno tako kot igralnica določi glavne dobitke.

## 2. Kaj je statistika?



Skozi življenje se prebijamo z odločitvami,  
ki jih naredimo na osnovi nepopolnih informacij ...

## Pogled od zunaj

*Števila so me pogosto begala,  
še posebej, če sem imel pred seboj  
neko njihovo razvrstitev,  
tako da je tem primeru obveljala misel,  
ki so jo pripisali Diaraeliju,  
z vso pravico in močjo:*

*“Obstajajo tri vrste laži:*

*laži,*

*preklete laži in*

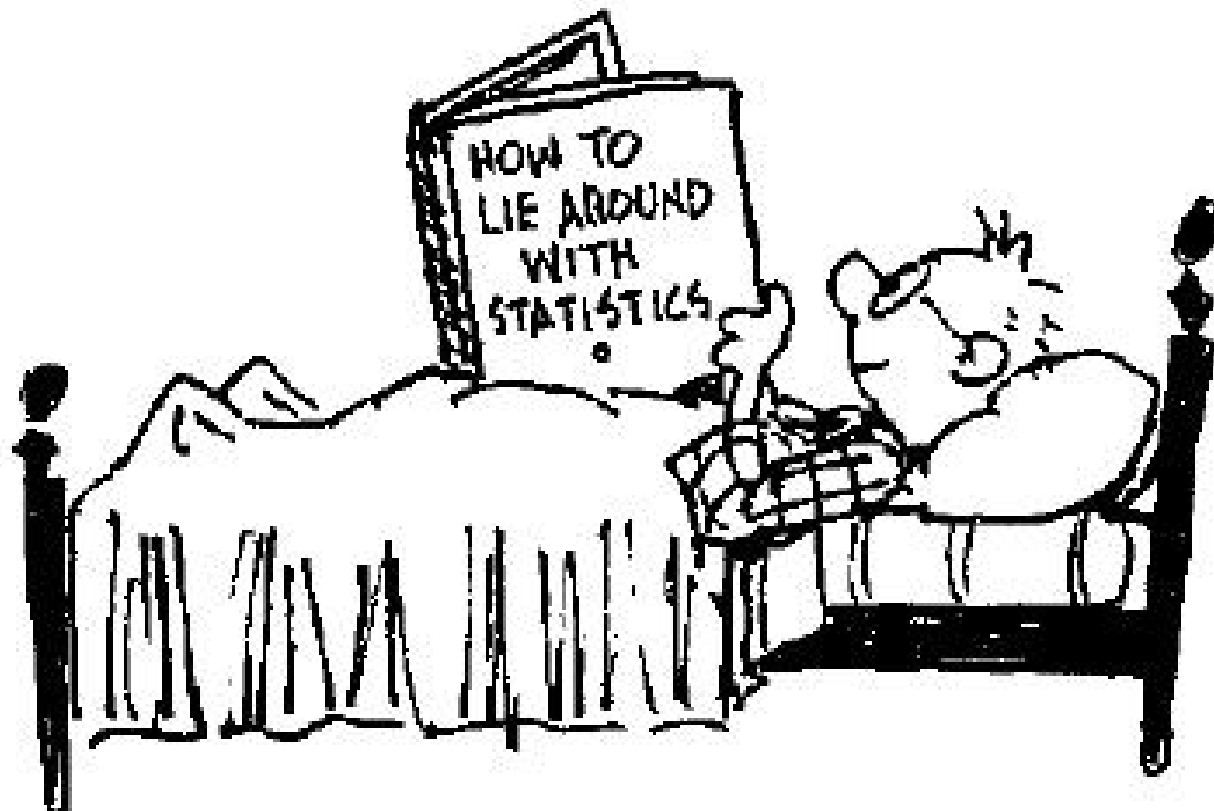
*statistika.”*

iz Autobiografije Marka Twaina



*Be good + you will be lonesome.  
Mark Twain*





## Okvirni načrt za statistiko

### Opisna statistika

#### ena spremenljivka

- mere centralne tendence
- mere razpršenosti
- mere oblike

#### dve spremenljivki

- mere asociacije

### Inferenčna (analitična) statistika

- točkovno in intervalno ocenjevanje
- 1- in 2- vzorčno testiranje hipotez
- kontingenčne tabele
- regresija

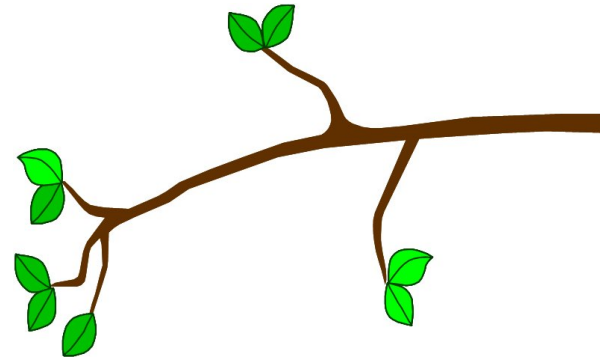
## Statistika

preučuje podatke, jih

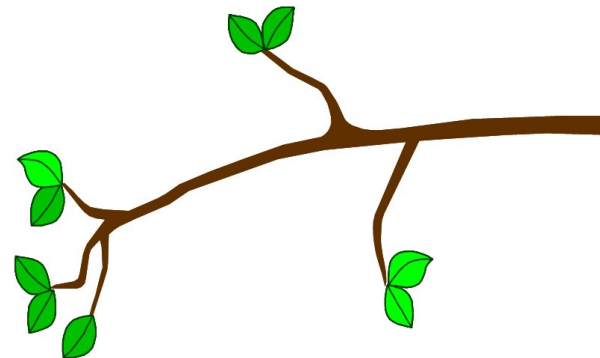
- zbira,
- klasificira,
- povzema,
- organizira,
- analizira in
- interpretira.



## Glavni veji statistike



**Opisna statistika** se ukvarja z organiziranjem, povzemanjem in opisovanjem zbirk podatkov (reduciranje podatkov na povzetke)

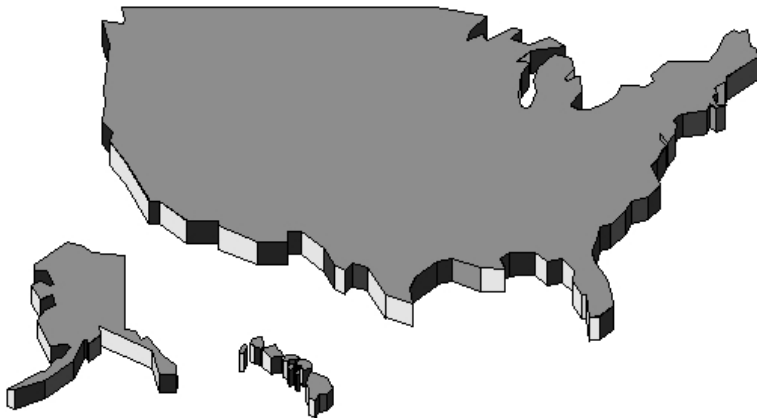


**Analitična statistika** jemlje vzorce podatkov in na osnovi njih naredi zaključke (inferenčnost) o populaciji (ekstrapolacija).

## Tipi podatkovnih množic

- *Populacija*

- vsi objekti,  
ki jih opazujemo



**Primer:**

vsi registrirani glasovalci

- *Vzorec*

- podmnožica populacije



**Primer:**

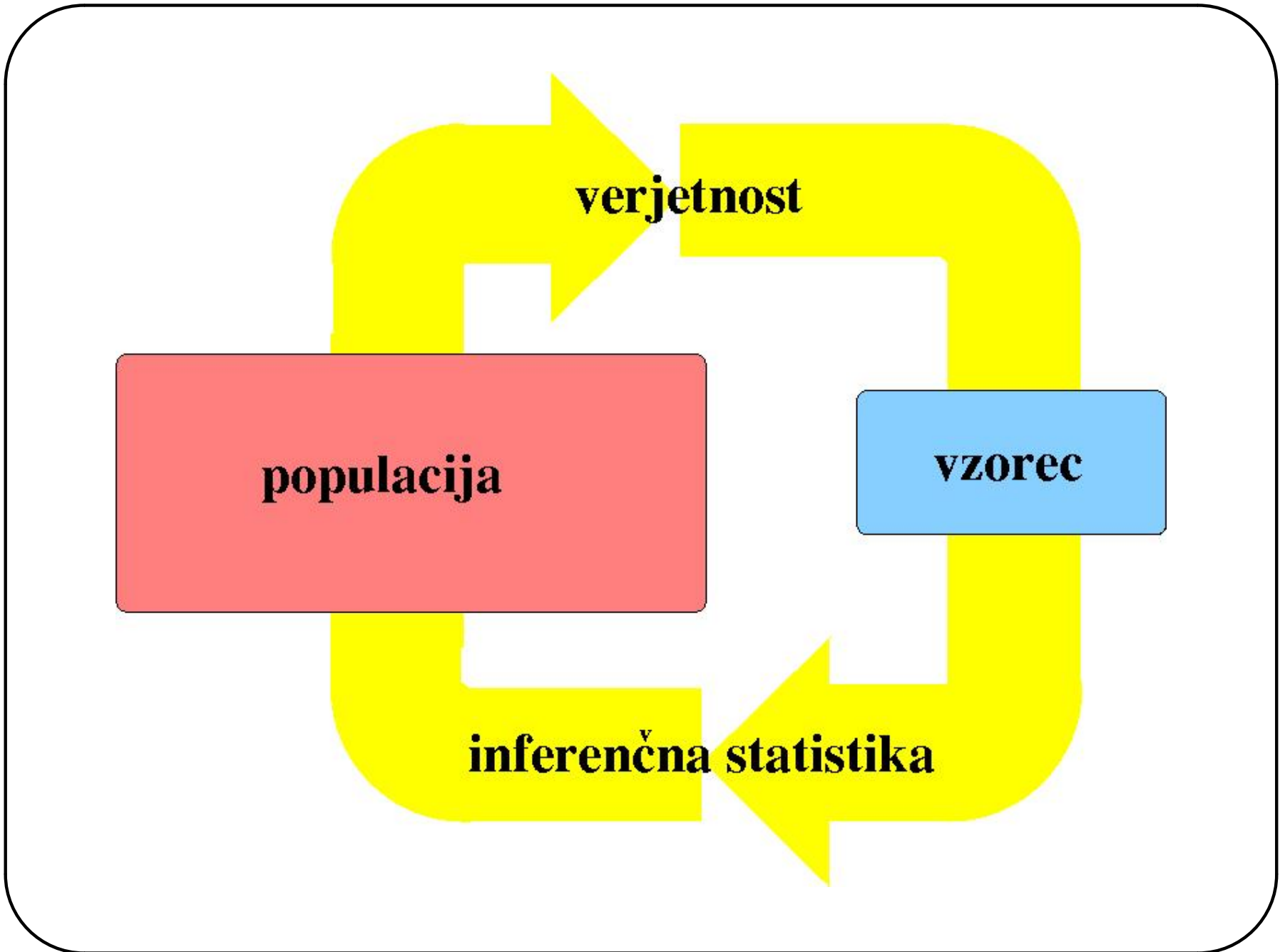
100 registriranih glasovalcev

**Populacija** je podatkovna množica, ki ji je namenjena naša pozornost.

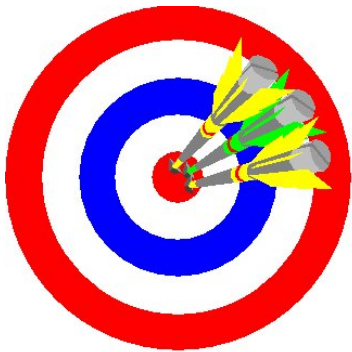


**Vzorec** je podmnožica podatkov, ki so izbrani iz populacije (po velikosti bistveno manjši od populacije).





## Tipi podatkov

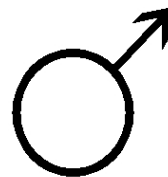


– *kvantitativni*  
(numerični)

predstavljajo kvantiteto  
ali količino nečesa.



– *kvalitativni* (kategorije) ni kvantitativnih interpretacij.





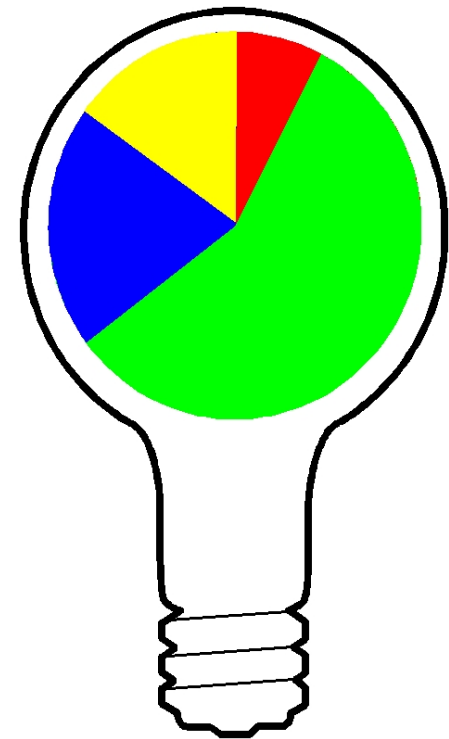
## Kvantitativni (numerični)

- **interval**

- poljubna ničla
- Enaki intervali predstavljajo enake količine.

- **razmerje**

- smiselna točka nič
- Operacije seštevanje, odštevanje, množenje in deljenje so smiselne.



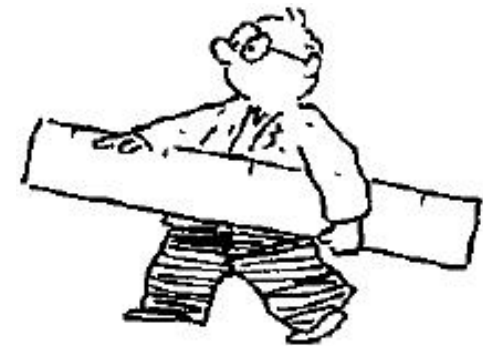
## Kvalitativni (kategorični)

- **nominalni**

- kategorije brez odgovarjajočega vrstnega reda / urejenosti

- **ordinalni/številski**

- kategorije z urejenostjo

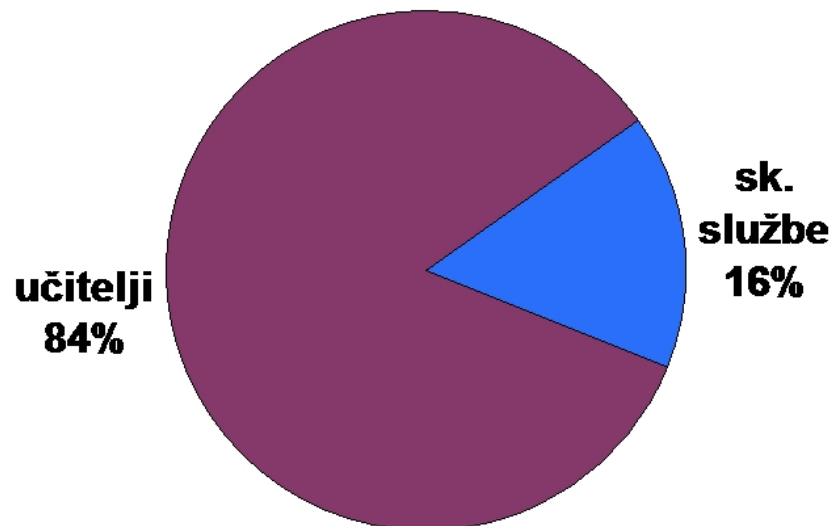
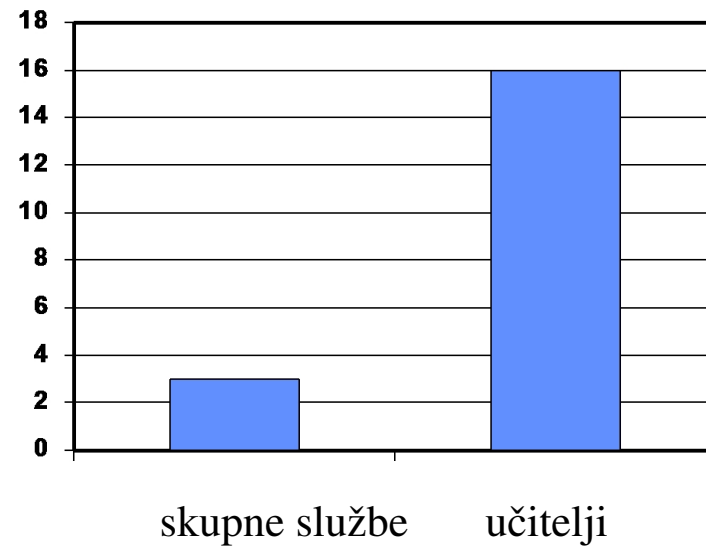


## Oddelek sistemskih inženirjev

| <b>kategorija</b> | <b>frekvenca</b> | <b>relativna<br/>frekvenca</b> |
|-------------------|------------------|--------------------------------|
| vrsta             | število          |                                |
| zaposlenih        | zaposlenih       | delež                          |
| učitelji          | 16               | 0,8421                         |
| skupne službe     | 3                | 0,1579                         |
| skupaj            | 19               | 1,0000                         |

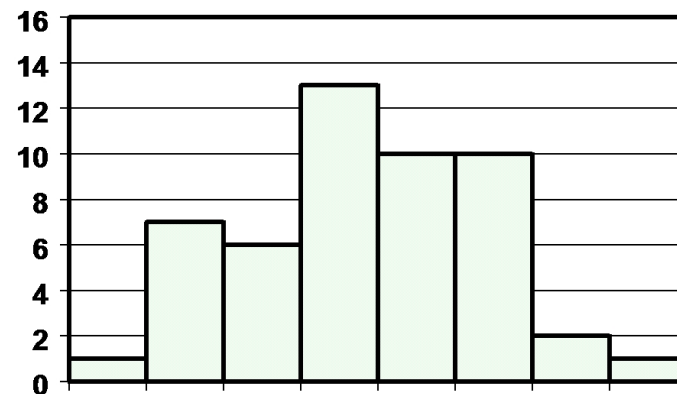
## Grafična predstavitev kvalitativnih podatkov

- **stolpčni graf**
  - poligonski diagram
- **strukturni krog**
  - pogača, kolač

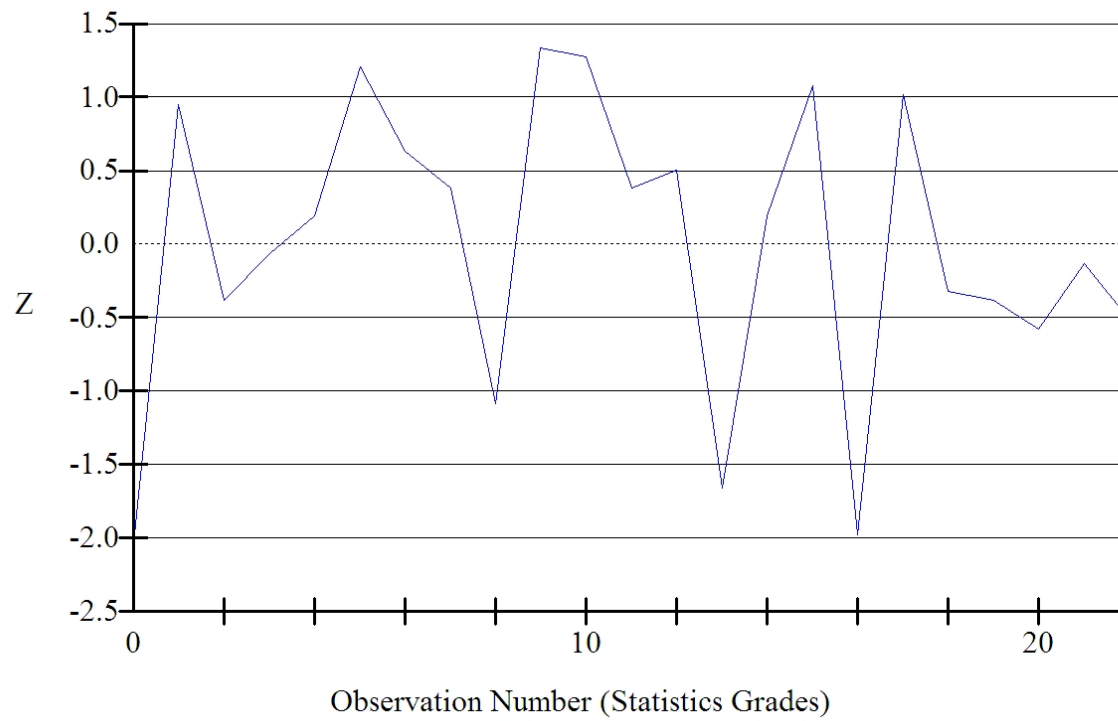


## Grafična predstavitev kvalitativnih podatkov

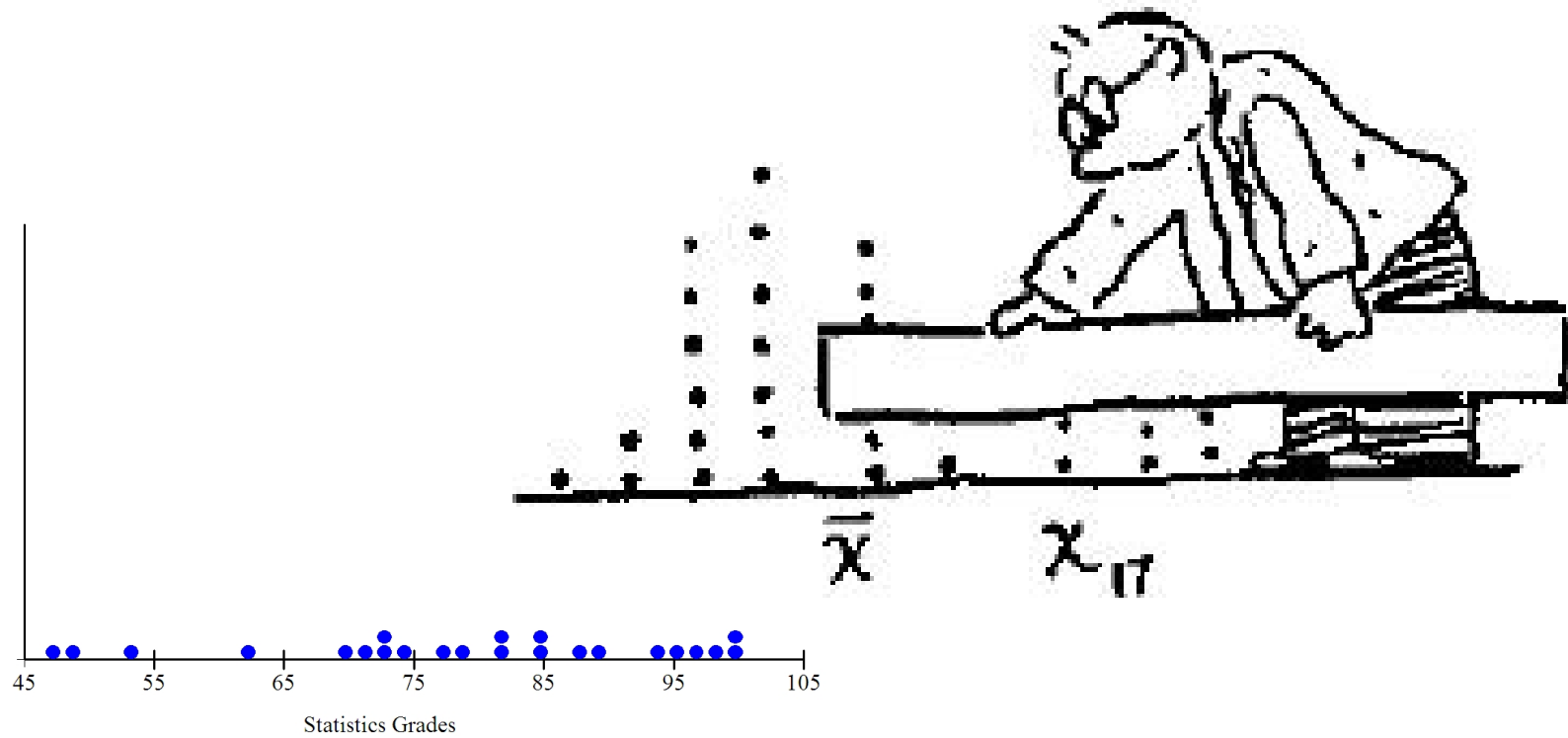
- runs plot ( $X, Y$  plot)
- zaporedje (dot plot)
- steblo-list predstavitev (angl. stem-and-leaf)
- histogrami
- škatla z brki (box plot)



## Runs Chart

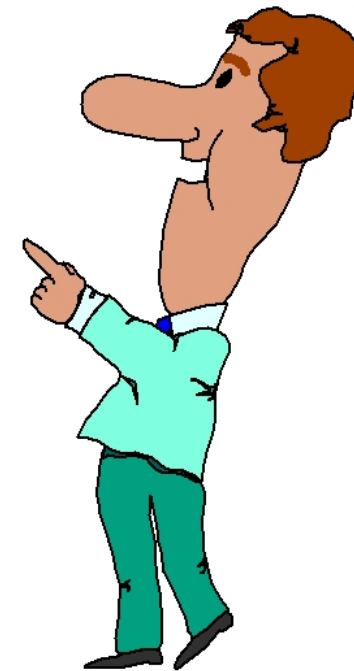


## Dot Plot



## Urejeno zaporedje/ranžirana vrsta

**Urejeno zaporedje** je zapis podatkov v vrsto po njihovi numerični velikosti (ustreznemu mestu pravimo *rang*).





## Primer zaporedja podatkov (nal. 2.48, str.64)

|  |     |     |     |     |     |
|--|-----|-----|-----|-----|-----|
| (a) Konstruiraj<br>urejeno<br>zaporedje. | 88  | 103 | 113 | 122 | 132 |
|  | 92  | 108 | 114 | 124 | 133 |
|  | 95  | 109 | 116 | 124 | 133 |
|  | 97  | 109 | 116 | 124 | 135 |
| (b) Nariši<br>steblo-list<br>diagram.    | 97  | 111 | 117 | 128 | 136 |
|  | 97  | 111 | 118 | 128 | 138 |
|  | 98  | 112 | 119 | 128 | 138 |
|  | 98  | 112 | 120 | 131 | 142 |
| (c) Naredi<br>histogram.                 | 100 | 112 | 120 | 131 | 146 |
|  | 100 | 113 | 122 | 131 | 150 |

## Koraki za konstrukcijo steblo-list predstavitev

- |  | stebila/listi                |
|--|------------------------------|
| 1. Razdeli vsako opazovanje-podatke na dva dela: <b>stebila</b> (angl. stem) in <b>listi</b> (angl. leaf). | 08 8                         |
|  | 09 2 5 7 7 7 8 8             |
| 2. Naštej stebila po vrsti v stolpec, tako da začneš pri najmanjšem in končaš pri največjem.               | 10 0 0 3 8 9 9               |
|  | 11 1 1 2 2 2 3 3 4 6 6 7 8 9 |
|  | 12 0 0 2 2 4 4 4 8 8 8       |
| 3. Upoštevaj vse podatke in postavi liste za vsak dogodek/meritev v ustrezno vrstico/steblo.               | 13 1 1 1 2 3 3 5 6 8 8       |
|  | 14 2 6                       |
|  | 15 0                         |
| 4. Preštej frekvence za vsako steblo.  |                              |

## Steblo-list diagram

| stebila | listi                     | rel. $\nu$ | $\nu$ |
|---------|---------------------------|------------|-------|
| 08      | 8                         | 1          | 2%    |
| 09      | 2 5 7 7 7 8 8             | 7          | 14%   |
| 10      | 0 0 3 8 9 9               | 6          | 12%   |
| 11      | 1 1 2 2 2 3 3 4 6 6 7 8 9 | 13         | 26%   |
| 12      | 0 0 2 2 4 4 4 8 8 8       | 10         | 20%   |
| 13      | 1 1 1 2 3 3 5 6 8 8       | 10         | 20%   |
| 14      | 2 6                       | 2          | 4%    |
| 15      | 0                         | 1          | 2%    |
|         |                           | 50         | 100%  |

## Histogrami

- (1) kako zgradimo histogram
- (2) število razredov
- (3) frekvenca
- (4) procenti



## (a) Kako zgradimo histogram

- (a) Izračunaj **razpon** podatkov.
- (b) Razdeli razpon na *5 do 20 razredov* enake širine.
- (c) Za vsak razred preštej število vzorcev, ki spadajo v ta razred.  
To število imenujemo **frekvenca razreda**.
- (d) Izračunaj vse **relativne frekvence razredov**.

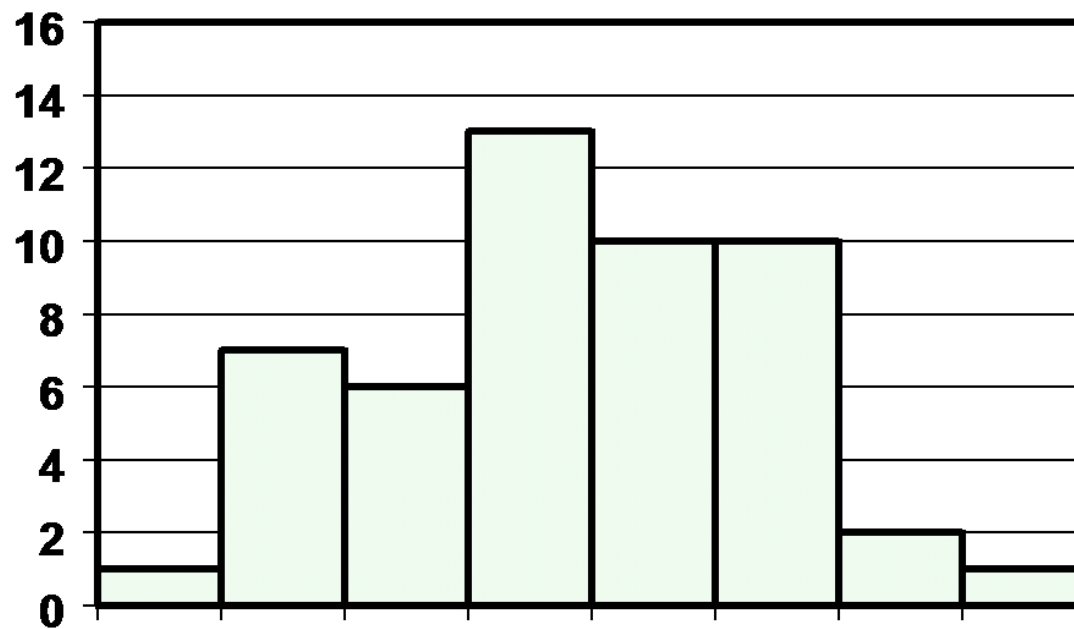
## (b) Pravilo za določanje števila razredov v histogramu

| število vzorcev v množici podatkov | število razredov |
|------------------------------------|------------------|
| manj kot 25                        | 5 ali 6          |
| 25 – 50                            | 7 – 14           |
| več kot 50                         | 15 – 20          |

### (c,d) Frekvenčna porazdelitev

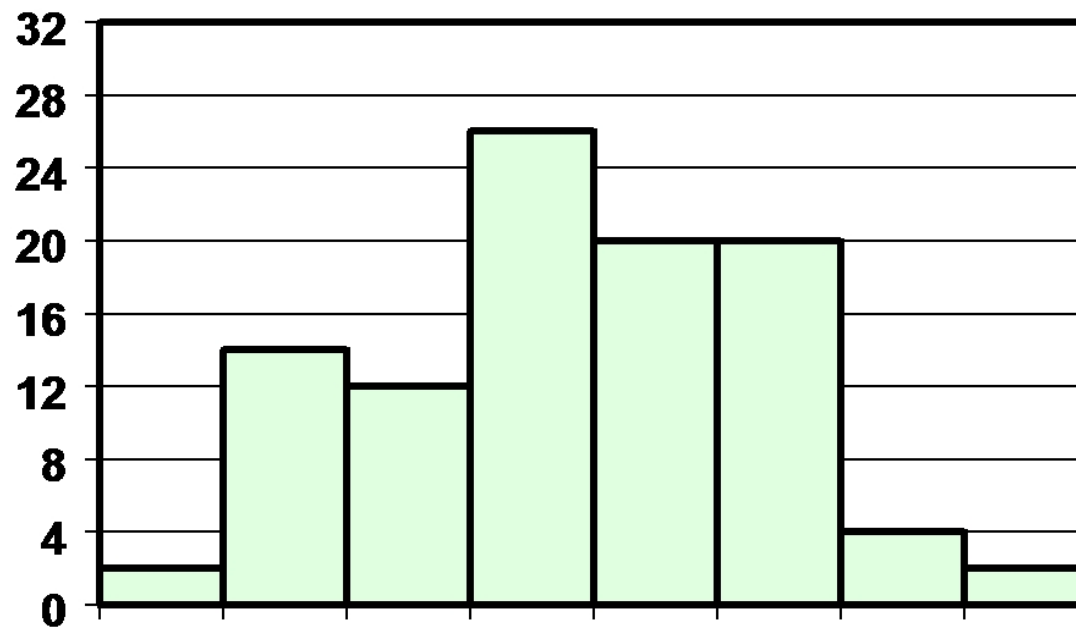
| razred | interval razreda | frekvenca | relativna frekvenca |
|--------|------------------|-----------|---------------------|
| 1      | 80 – 90          | 1         | 2%                  |
| 2      | 90 – 100         | 7         | 14%                 |
| 3      | 100 – 110        | 6         | 12%                 |
| 4      | 110 – 120        | 13        | 26%                 |
| 5      | 120 – 130        | 10        | 20%                 |
| 6      | 130 – 140        | 10        | 20%                 |
| 7      | 140 – 150        | 2         | 4%                  |
| 8      | 150 – 160        | 1         | 2%                  |

## Frekvenčni histogram



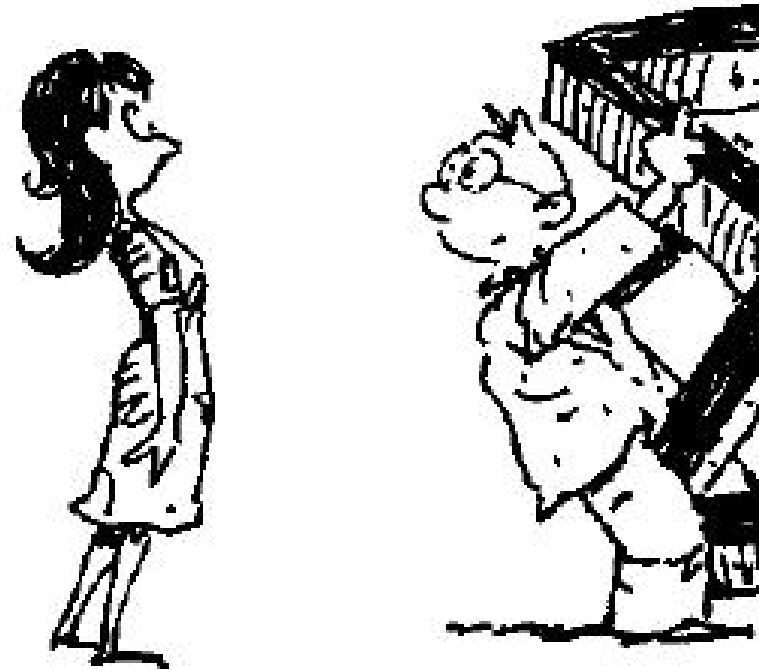


## Procentni histogram



## Mere za lokacijo in razpršenost

- srednje vrednosti
- razpon (min/max)
- centili, kvartili
- varianca
- standardni odklon
- $Z$ -vrednosti



## Modus

*Modus* (oznaka  $M_0$ ) množice podatkov je tista vrednost, ki se pojavi z največjo frekvenco.



## Mediana ( $M_e$ )

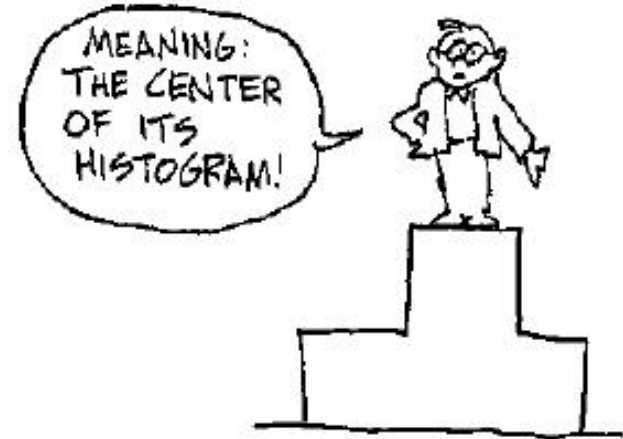
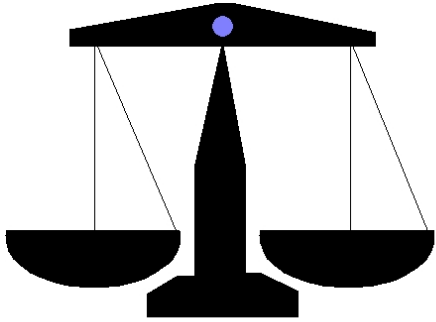
Da bi prišli do *mediane* (oznaka  $M_e$ ) za neko množico podatkov, naredimo naslednje:



1. Podatke uredimo po velikosti v naraščujočem vrstnem redu,
2. Če je število podatkov liho, potem je mediana podatek na sredini,
3. Če je število podatkov sodo, je mediana enaka povprečju dveh podatkov na sredini.

Oznake: mediana populacije:  $\mu$       mediana vzorca:  $m$

## Povprečja



**Povrečje populacije:**

$$\mu = \frac{1}{N}(y_1 + \cdots + y_N) = \frac{\sum_{i=1}^N y_i}{N}$$

**Povrečje vzorca:**

$$\bar{y} = \frac{1}{n}(y_1 + \cdots + y_n) = \frac{\sum_{i=1}^n y_i}{n}$$

## Razpon ali variacijski razmik

**Razpon** je razlika med največjo in najmanjšo meritvijo v množici podatkov.



## Centili

**100*p*-ti centil** ( $p \in [0, 1]$ )

je definiran kot število,  
od katerega ima 100*p* %  
meritev manjšo ali enako  
numerično vrednost.

Določanje 100*p*-tega centila:

Izračunaj vrednost  $p(n + 1)$

in jo zaokroži na najbližje celo število.

Naj bo to število enako  $i$ .

Izmerjena vrednost z  $i$ -tim rangom je 100*p*-ti centil.

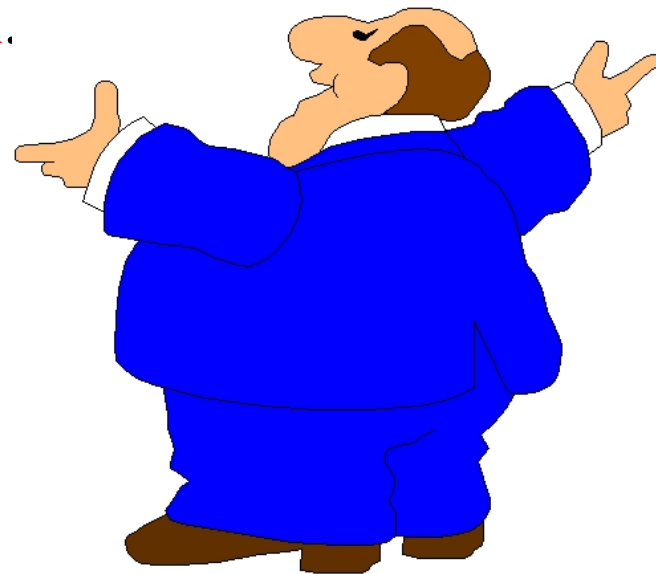


## ... Centili

25. centil se imenuje tudi **1. kvartil**.

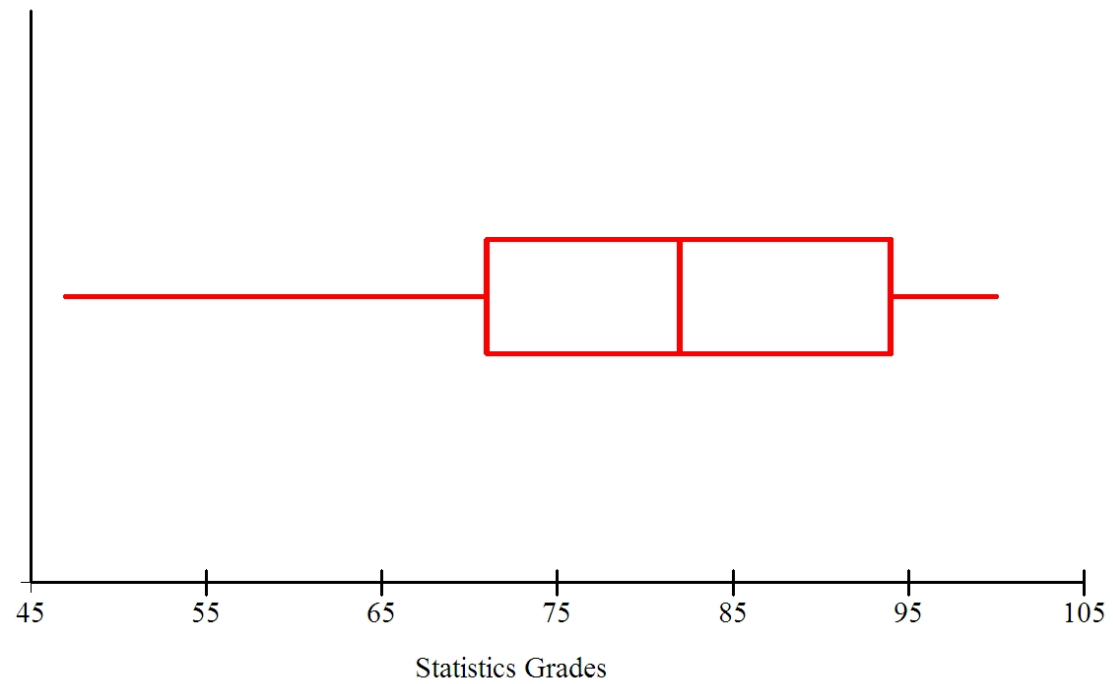
50. centil se imenuje **2. kvartil** ali **mediana**.

75. centil se imenuje tudi **3. kvartil**.





## Škatla z brki (angl. box plot)



## Mere razpršenosti

### varianca

- kvadrat pričakovanega odklona (populacije)
- vsota kvadratov odklonov deljena s stopnjo prostosti (vzorca)

### standardni odklon (deviacija)

- pozitivni kvadratni koren variance

### koeficient variacije

- standardni odklon deljen s povprečjem

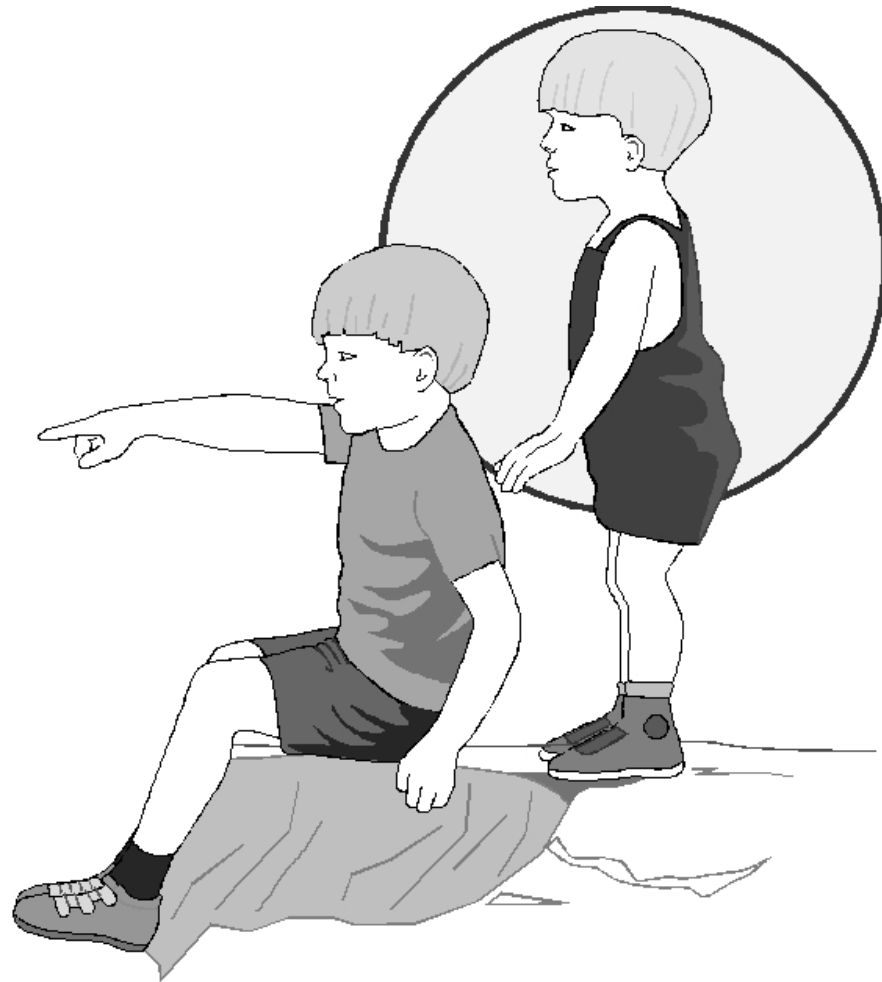
## ... Mere razpršenosti

|                   | populacija | vzorec     |
|-------------------|------------|------------|
| varianca          | $\sigma^2$ | $S^2, s^2$ |
|                   | $D, V$     |            |
| standardni odklon | $\sigma$   | $S, s$     |

Za vzorec smo vzeli osebe na FRI.

Zabeležili smo naslednje  
število otrok:

|   |   |   |
|---|---|---|
| 1 | 2 | 2 |
| 1 | 2 | 5 |
| 1 | 2 |   |



## Varianca in standardni odklon

**Varianca populacije** (končne populacije z  $N$  elementi):

$$\sigma^2 = \frac{\sum_{i=1}^N (y_i - \mu)^2}{N}.$$

**Varianca vzorca** ( $n$  meritvami):

$$s^2 = \frac{\sum_{i=1}^n (y_i - \mu)^2}{n - 1} = \frac{\sum_{i=1}^n y_i^2 - \frac{\left(\sum_{i=1}^n y_i\right)^2}{n}}{n - 1}$$

**Standardni odklon** je pozitivno predznačen kvadratni koren variance.

## Sredine

$$a_1, \dots, a_n \geq 0$$

**Aritmetična:**

$$A_n = \frac{a_1 + \dots + a_n}{n}$$

**Geometrična:**

$$G_n = \sqrt[n]{a_1 \cdot \dots \cdot a_n}$$

**Harmonična:**

$$H_n = \frac{1}{\frac{1}{a_1} + \dots + \frac{1}{a_n}}$$

**Kvadratna:**

$$K_n = \sqrt{\frac{a_1^2 + \dots + a_n^2}{n}}$$





## Sredine: $H_2 \leq G_2 \leq A_2 \leq K_2$

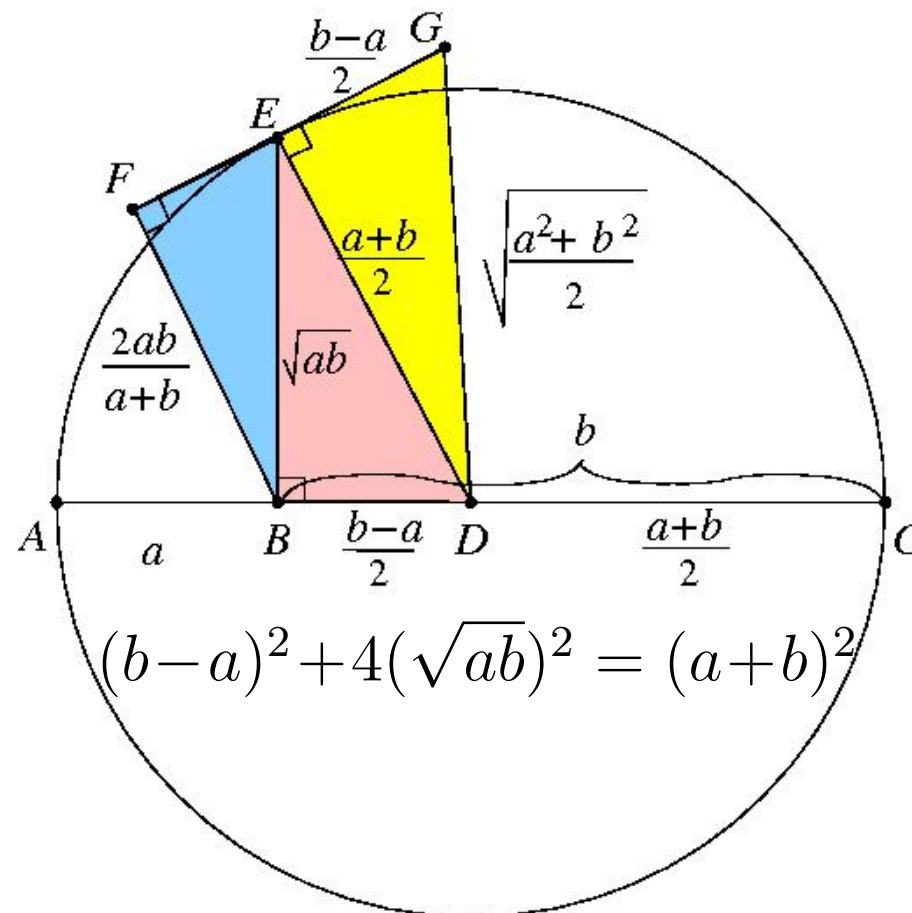
$$a, b \geq 0$$

$$H_2 = \frac{2}{\frac{1}{a} + \frac{1}{b}}$$

$$G_2 = \sqrt{ab}$$

$$A_2 = \frac{a+b}{2}$$

$$K_2 = \sqrt{\frac{a^2 + b^2}{2}}$$



Sidney H. Kung

(iz R.B. Nelsenove knjige "Dokazi brez besed")



## ... Sredine

**Potenčna (stopnje  $k$ ):**

$$P_{n,k} = \sqrt[k]{\frac{a_1^k + \dots + a_n^k}{n}}$$

Velja:

$$H_n = P_{n,-1}, \quad G_n = \lim_{k \rightarrow 0} P_{n,k} \quad A_n = P_{n,1} \quad \text{in} \quad K_n = P_{n,2}$$

ter

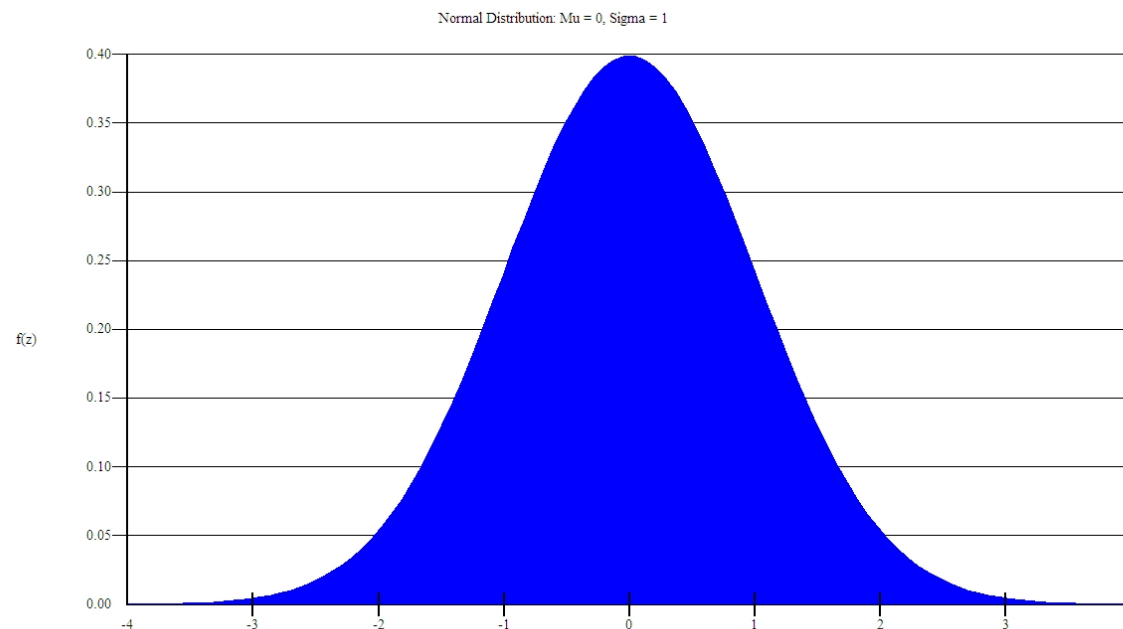
$$H_n \leq G_n \leq A_n \leq K_n$$

oziroma za  $k \leq m$ :

$$P_{n,k} \leq P_{n,m}$$

## Normalna porazdelitev

Veliko podatkovnih množic ima porazdelitev približno **zvonaste oblike** (unimodalna oblika - ima en sam vrh):



## Empirična pravila

Če ima podatkovna množica porazdelitev približno **zvonaste oblike**, potem veljajo naslednja pravila (angl. rule of thumb), ki jih lahko uporabimo za opis podatkovne množice:

1. Približno **68,3%** vseh meritev leži na razdalji  **$1 \times$  standardnega odklona** od njihovega povprečja.
2. Približno **95,4%** meritev leži na razdalji do  **$2 \times$  standardnega odklona** od njihovega povprečja.
3. Skoraj vse meritve (**99,7%**) ležijo na razdalji  **$3 \times$  standardnega odklona** od njihovega povprečja.

## Mere oblike

Če je spremenljivka približno normalno porazdeljena, potem jo statistični karakteristiki **povprečje** in **standardni odklon** zelo dobro opisujeta.

V primeru unimodalne porazdelitve spremenljivke, ki pa je bolj asimetrična in bolj ali manj sploščena (koničasta), pa je potrebno izračunati še stopnjo *asimetrije* in *sploščenosti* (*koničavosti*).

## Centralni momenti

**$\ell$ -ti centralni moment** je

$$m_\ell = \frac{(y_1 - \mu)^\ell + \dots + (y_n - \mu)^\ell}{n}.$$

$$m_1 = 0, m_2 = \sigma^2, \dots$$

**Koeficient asimetrije** (s centralnimi momenti):

$$g_1 = m_3 / m_2^{3/2}.$$

## Mere asimetrije

Razlike med srednjimi vrednostimi so tem večje,  
čim bolj je porazdelitev asimetrična:

$$KA_{M_0} = (\mu - M_0)/\sigma,$$

$$KA_{M_e} = 3(\mu - M_e)/\sigma.$$

## Mera sploščenosti (kurtosis)

**Koeficient sploščenosti** (s centralnimi momenti)

$$K = g_2 = m_4/m_2^2 - 3$$

–  $K = 3$  (ali 0)

normalna porazdelitev zvonaste-oblike (*mesokurtic*),

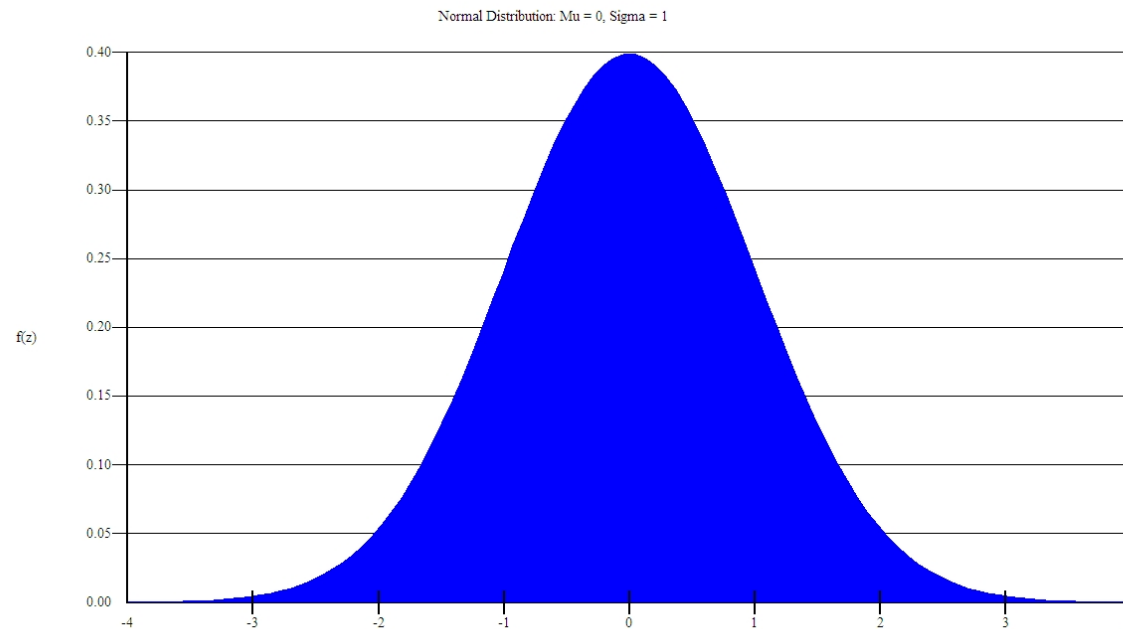
–  $K < 3$  (ali negativna)

bolj kopasta kot normalna porazdelitev, s krajšimi repi (*platykurtic*),

–  $K > 3$  (ali pozitivna)

bolj špičasta kot normalna porazdelitev, z daljšimi repi (*leptokurtic*).

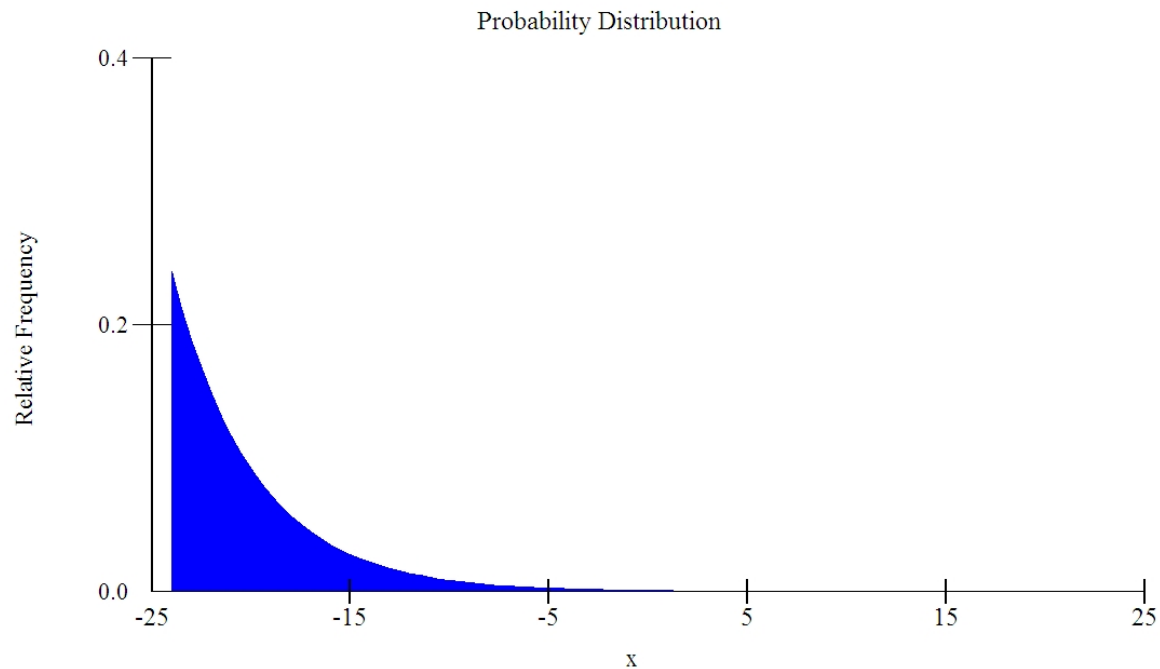
## Normalna porazdelitev



asimetričnost = 0, sploščenost = 3 (mesokurtic).

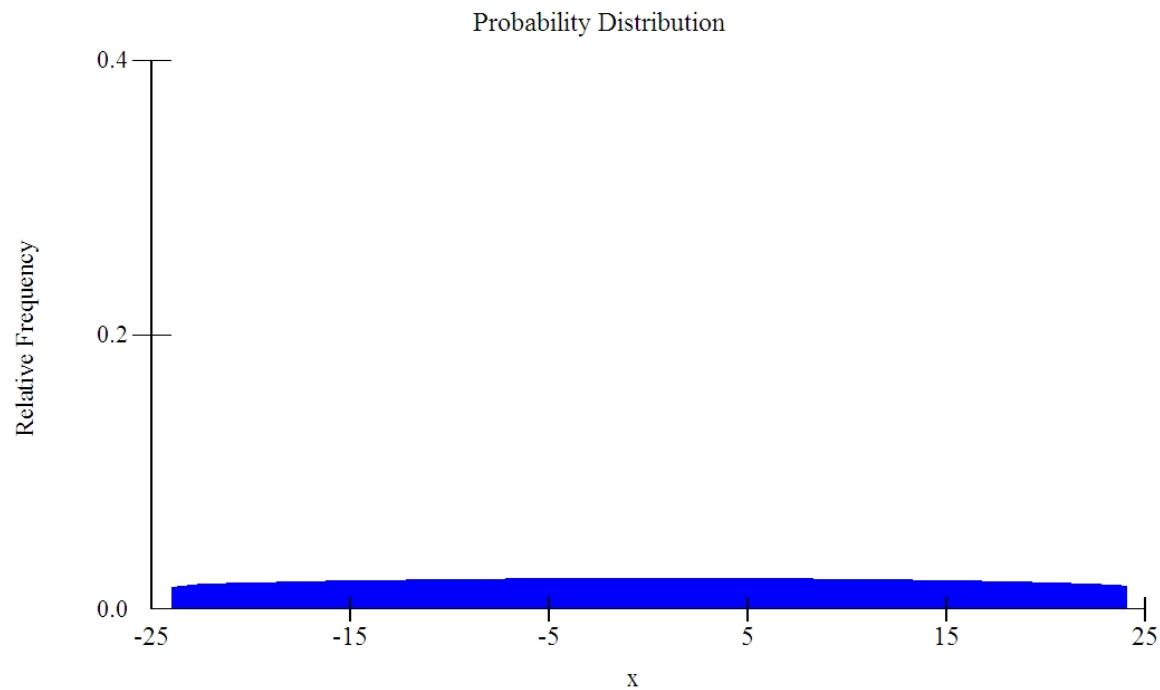


## Asimetrična v desno



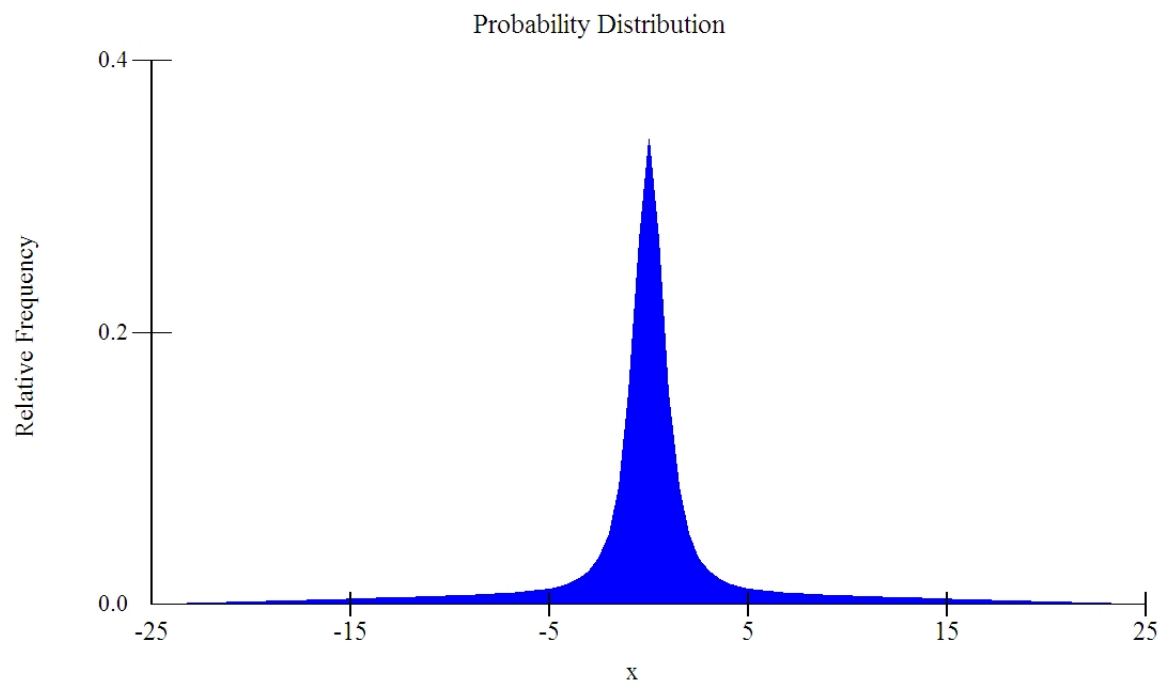
asimetričnost= 1,99, sploščenost= 8,85.

## Kopasta porazdelitev



asimetričnost = 0, sploščenost = 1,86 (platykurtic).

## Špičasta porazdelitev



asimetričnost =  $-1,99$ , sploščenost =  $8,85$  (leptokurtic).

## Standardizacija

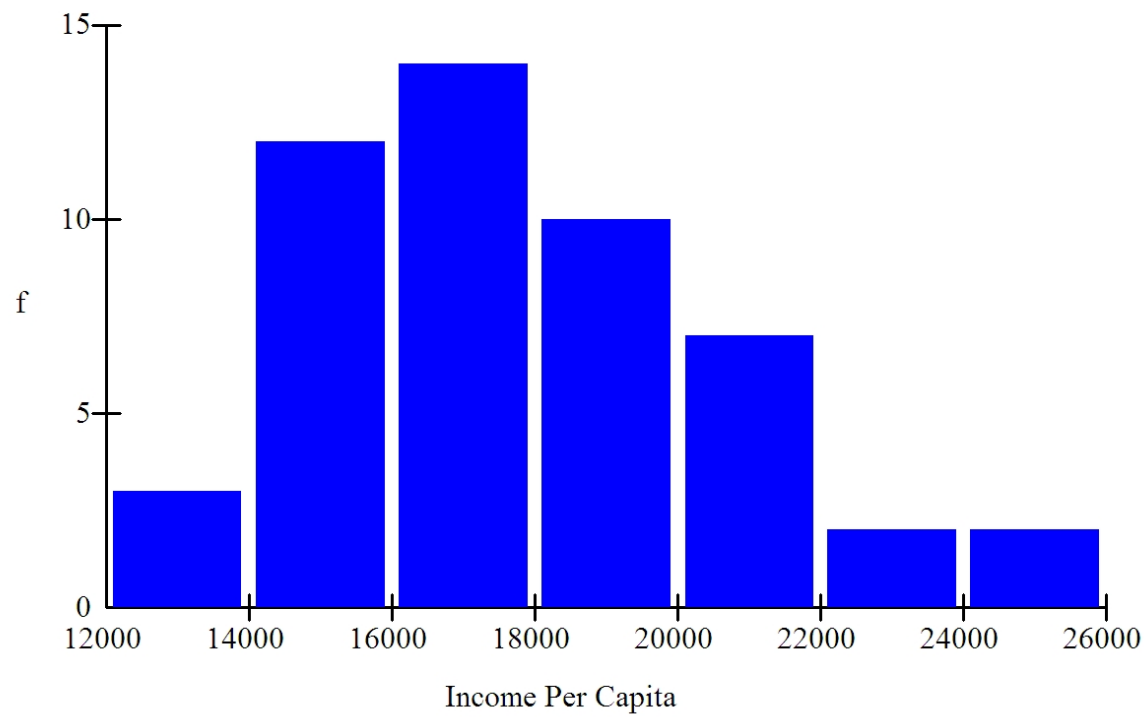
Vsaki vrednosti  $x_i$  spremenljivke  $X$  odštejemo njeno povprečje  $\mu$  in delimo z njenim standardnim odklonom  $\sigma$ :

$$z_i = \frac{x_i - \mu}{\sigma}.$$

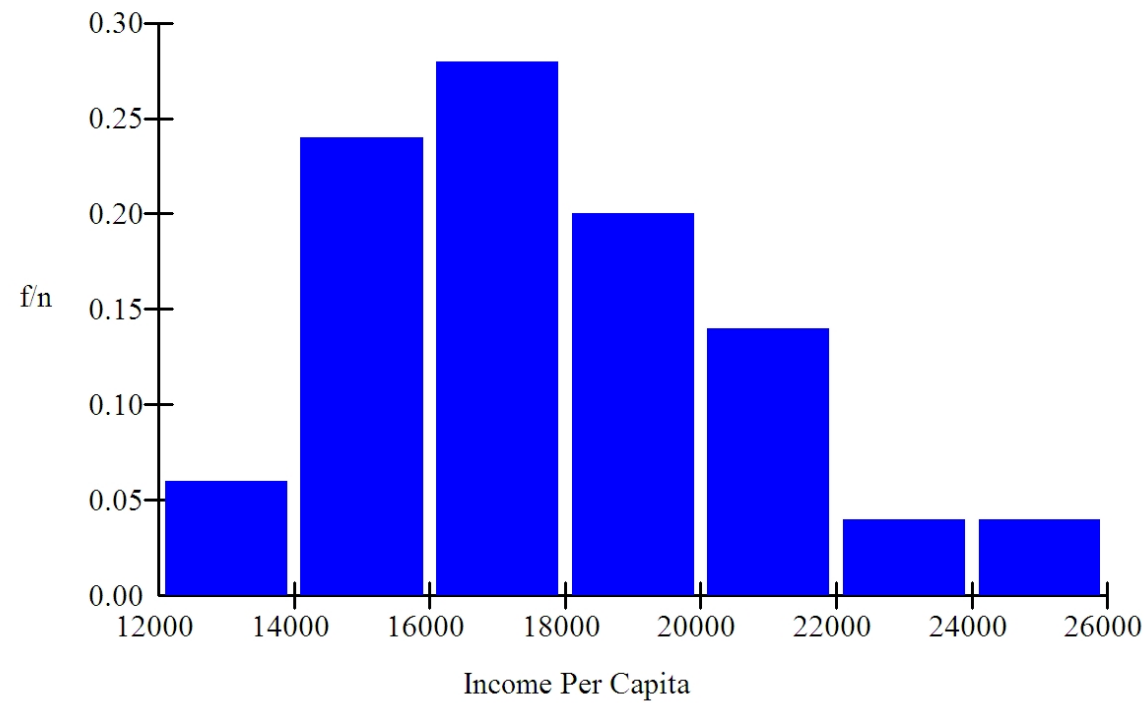
Za novo spremenljivko  $Z$  bomo rekli, da je **standardizirana**,  $z_i$  pa je **standardizirana vrednost**.

Potem je  $\mu(Z) = 0$  in  $\sigma(Z) = 1$ .

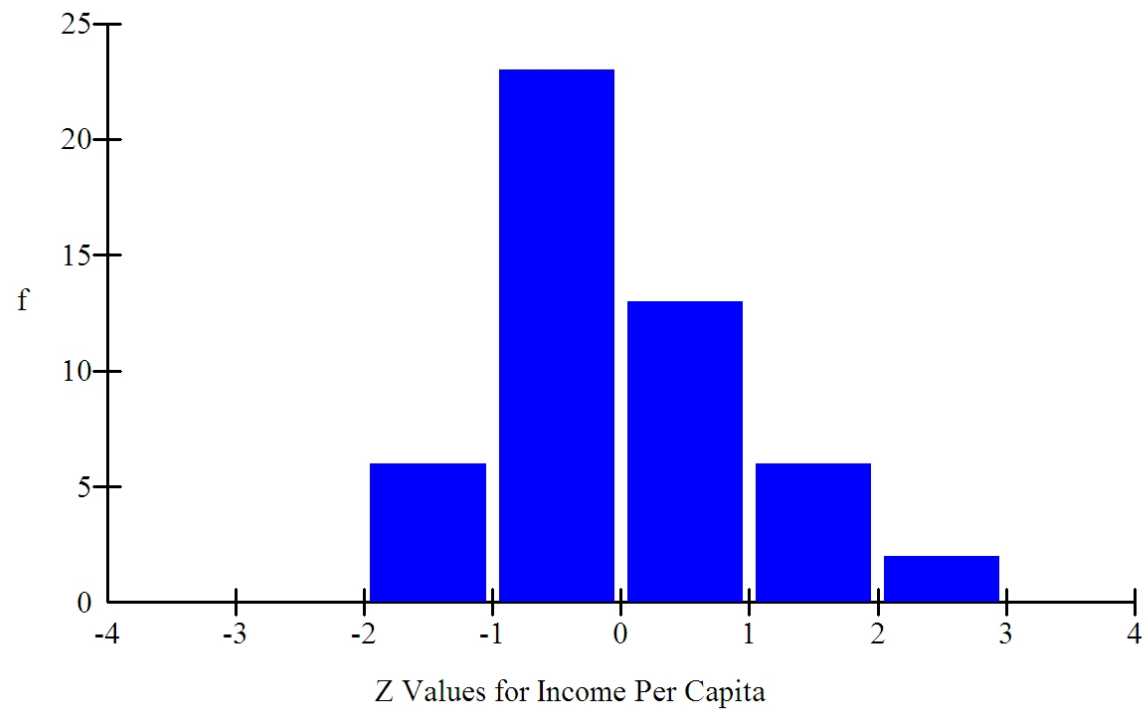
## Frekvenčni histogram



## Relativni frekvenčni histogram



## Histogram standardiziranih $Z$ -vrednosti



### 3. Zamenjalna šifra

Tomaž Pisanski, Skrivnostno sporočilo

Presek V/1, 1977/78, str. 40-42.

YHW?HD+CVODHVTHVO-!JVG: CDCYJ (JV/-V?HV (  
 -T?HVW-4YC4 (?-DJV/- (?S-VO3CWC%J (-V4-DC  
 V!CW-?CVNJDJVD-?+-VO3CWC%J (-VQW-DQ-VJ+  
 V?HVDWHN-V3C: CODCV!H+?-DJVD-?+CV3JO-YC

(črko Č smo zamenjali s C, črko Ć pa z D)



Imamo  $26! = 40329146112665635584000000$

možnosti z direktnim preizkušanjem,

zato v članku dobimo naslednje nasvete:

(0) Relativna frekvenca črk in presledkov v slovenščini: presledek 173,

|    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|
| E  | A  | I  | O  | N  | R  | S  | L  | J  | T  | V  | D  |
| 89 | 84 | 74 | 73 | 57 | 44 | 43 | 39 | 37 | 37 | 33 | 30 |

|    |    |    |    |    |    |    |    |   |    |   |    |   |
|----|----|----|----|----|----|----|----|---|----|---|----|---|
| K  | M  | P  | U  | Z  | B  | G  | "C | H | "S | C | "Z | F |
| 29 | 27 | 26 | 18 | 17 | 15 | 12 | 12 | 9 | 9  | 6 | 6  | 1 |

- (1) Na začetku besed so najpogostejše črke  
N, S, K, T, J, L.
- (2) Najpogostejše končnice pa so  
E, A, I, O, U, R, N.
- (3) Ugotovi, kateri znaki zagotovo predstavljajo samoglasnike in kateri  
soglasnike.
- (4) V vsaki besedi je vsaj en samoglasnik  
ali samoglasniški R.
- (5) V vsaki besedi z dvema črkama je ena  
črka samoglasnik, druga pa soglasnik.
- (6) detektivska sreča

|     |    |    |    |    |    |    |   |   |   |   |   |   |
|-----|----|----|----|----|----|----|---|---|---|---|---|---|
| (0) | V  | -  | C  | D  | J  | ?  | H | W | O | ( | + | 3 |
|     | 23 | 19 | 16 | 12 | 11 | 10 | 9 | 7 | 6 | 6 | 5 | 4 |
|     | Y  | 4  | !  | /  | Q  | :  | % | T | N | S | G |   |
|     | 4  | 3  | 3  | 2  | 2  | 2  | 2 | 2 | 2 | 1 | 1 |   |

Zaključek  $V \rightarrow ' '$  (drugi znaki z visoko frekvenco ne morejo biti).

Dve besedi se ponovita: 03CWC%J (-,  
opazimo pa tudi eno sklanjatev:  
D-?+- ter D-?+C.

Torej nadaljujemo z naslednjim tekstom:

YHW?HD+C ODH TH O-!J G:CDYJ(J /- ?H  
(-T?H W-4YD4 (?-DJ /-(?S- 03CWC%J(- 4-DC  
!CW-?C NJDJ D-?+- 03CWC%J(- QW-DQ- J+  
?H DWHN- 3C:C0DC !H+?-DJ D-?+C 3J0-YC

(3) Kandidati za samoglasnike e,a,i,o so znaki z visokimi frekvencami.

Vzamemo:

$$\{e,a,i,o\} = \{-,C,J,H\}$$

(saj D izključi -,H,J,C in ? izključi -,H,C,  
znaki -,C,J,H pa se ne izključujejo)

Razporeditev teh znakov kot samoglasnikov izgleda prav verjetna.  
To potrdi tudi gostota končnic, gostota parov je namreč:

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| AV | CV | HV | JV | VO | ?H | -D | DC | JM | W- | DJ | UC | CW | -? | VD |
| 7  | 5  | 5  | 5  | 4  | 4  | 4  | 3  | 3  | 3  | 3  | 3  | 3  | 3  | 3  |

(5) Preučimo besede z dvema črkama:

Samoglasnik na koncu

- 1) da ga na pa ta za (ha ja la)
- 2) "ce je le me ne se "se te ve "ze (he)
- 3) bi ji ki mi ni si ti vi
- 4) bo do (ho) jo ko no po so to
- 5) ju mu tu (bu)
- 6) r"z rt

Samoglasnik na začetku

- 1) ar as (ah aj au)
- 2) en ep (ej eh)
- 3) in iz ig
- 4) on ob od os on (oh oj)
- 5) uk up u's ud um ur (uh ut)

in opazujemo besedi: /- ?H

ter besedi: J+ ?H.

J+ ima najmanj možnosti, + pa verjetno ni črka n, zato nam ostane samo še:

|              |                        |
|--------------|------------------------|
| J+ ?H        | DWHN-                  |
| /- ?H        |                        |
| iz te        | (ne gre zaradi: D-?+C) |
| ob ta (e, o) | (ne gre zaradi: D-?+C) |
| od te        | (ne gre zaradi: D-?+C) |

tako da bo potrebno nekaj spremeniti in preizkusiti še naslednje:  
on bo; on jo; in so; in se; in je; in ta; en je; od tu ...



(6) Če nam po dolgem premisleku ne uspe najti rdeče niti, bo morda potrebno iskati napako s prijatelji (tudi računalniški program z metodo lokalne optimizacije ni zmožgel problema zaradi premajhne dolžine tajnopisa, vsekakor pa bi bilo problem mogoče rešiti s pomočjo elektronskega slovarja).

Tudi psihološki pristop pomaga, je svetoval Martin Juvan in naloga je bila rešena (poskusite sami!).

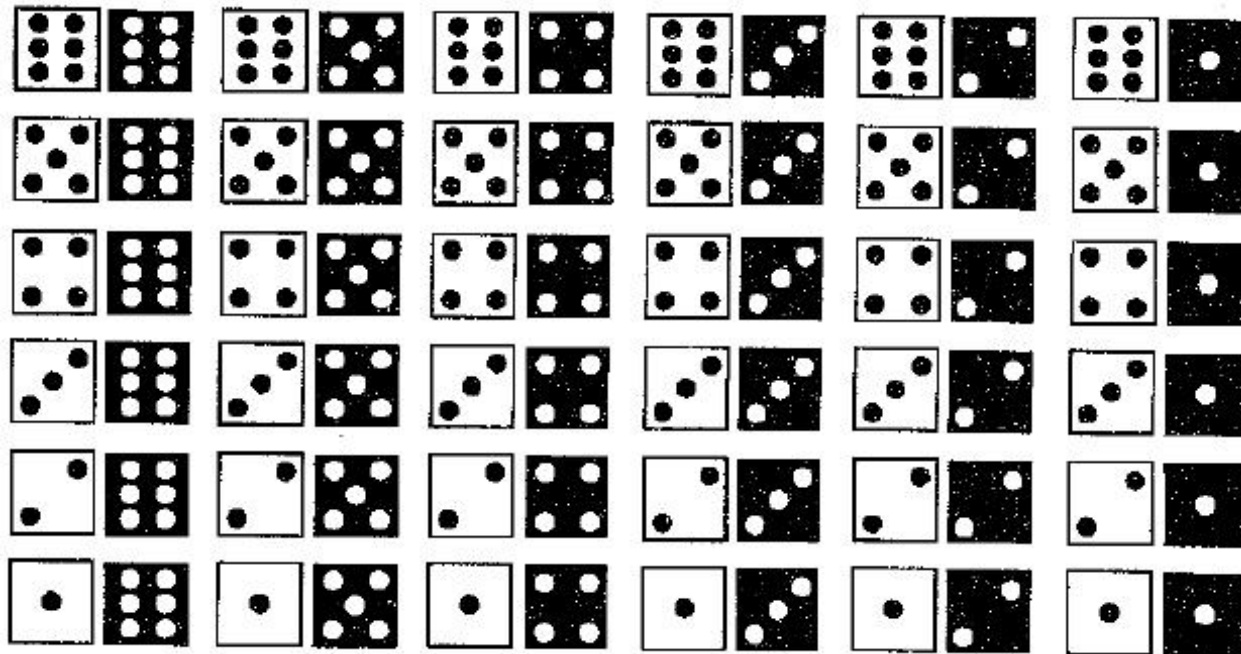
Podobna naloga je v angleščini dosti lažja, saj je v tem jeziku veliko členov THE, A in AN, vendar pa zato običajno najprej izpustimo presledke iz teksta, ki ga želimo spraviti v tajnopis. V angleščini imajo seveda črke drugačno gostoto kot v slovenščini. Razdelimo jih v naslednjih pet skupin:

1. E, z verjetnostjo okoli 0,120,
2. T, A, O, I, N, S, H, R, vse z verjetnostjo med 0,06 in 0,09,
3. D, L, obe z verjetnostjo okoli 0,04,
4. C, U, M, W, F, G, Y, P, B, vse z verjetnostjo med 0,015 in 0,028,
5. V, K, J, X, Q, Z, vse z verjetnostjo manjšo od 0,01.

Najbolj pogosti pari so (v padajočem zaporedju): TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI in OF,

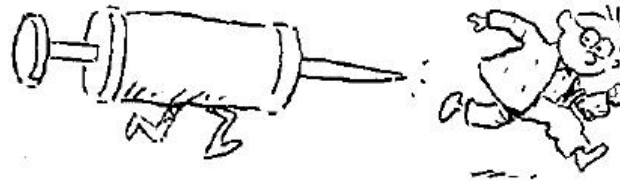
Najbolj pogoste trojice pa so (v padajočem zaporedju): THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR in DTH.

# KOMBINATORIKA (ponovitev)



## Funkcije/preslikave

**Funkcija**  $f$  iz množice  $A$  v množico  $B$  je predpis, ki vsakemu elementu iz množice  $A$  priredi natanko določen element iz množice  $B$ , oznaka  $f : A \longrightarrow B$ .



Funkcija  $f : A \longrightarrow B$  je:

- **injektivna** (angl. one to one) če za  $\forall x, y \in A$

$$x \neq y \Rightarrow f(x) \neq f(y),$$

- **surjektivna** (angl. on to), če za  $\forall b \in B$

$$\exists a \in A, \text{ tako da je } f(a) = b.$$

Injektivni in surjektivni funkciji pravimo **bijekcija**.

Množicama med katerima obstaja bijekcija pravimo **bijektivni** množici.

Bijektivni množici imata enako število elementov  
(npr. končno, števno neskončno, itd).

**Trditev:** *Če sta množici  $A$  in  $B$  končni ter je  $f : A \longrightarrow B$  funkcija iz injektivnosti funkcije  $f$  sledi surjektivnost, in obratno, iz surjektivnosti funkcije  $f$  sledi injektivnost.*

## Permutacije

**Permutacija** elementov  $1, \dots, n$  je bijekcija, ki slika iz množice  $\{1, \dots, n\}$  v množico  $\{1, \dots, n\}$ .

Npr. permutacija kart je običajno premešanje kart (spremeni se vrstni red, karte pa ostanejo iste).

**Število permutacij**  $n$  elementov, tj. razvrstitev  $n$ -tih različnih elementov, je enako  $n! := 1 \cdot 2 \cdot \dots \cdot n$  (oziroma definirano rekurzivno  $n! = (n-1)!n$  in  $0! = 1$ ).

Permutacijo lahko opišemo z zapisom:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

kjer je  $\{1, 2, \dots, n\} = \{a_1, a_2, \dots, a_n\}$ .

To pomeni  $\pi(1) = a_1, \pi(2) = a_2, \dots, \pi(n) = a_n$ .

**Primer:**  $n = 11$ ,

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 4 & 5 & 10 & 2 & 1 & 7 & 9 & 11 & 6 & 8 \end{pmatrix}$$

Naj bo  $A$  neka množica. Permutacije množice  $A$  med seboj množimo po naslednjem pravilu:  $\pi = \pi_1 \circ \pi_2$  je permutacija množice  $A$ , ki preslika  $a \in A$  v  $\pi_2(\pi_1(a))$ .

Primer:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 4 & 5 & 10 & 2 & 1 & 7 & 9 & 11 & 6 & 8 \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 8 & 2 & 1 & 3 & 10 & 9 & 4 & 5 & 7 & 6 & 11 \end{pmatrix}$$

Potem je

$$\pi = \pi_1 \circ \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 3 & 10 & 6 & 2 & 8 & 4 & 7 & 11 & 9 & 5 \end{pmatrix}$$



**Cikel** je permutacija, za katero je

$$\pi(a_1) = a_2, \pi(a_2) = a_3, \dots, \pi(a_r) = a_1,$$

ostale elementi pa so fiksni (tj.  $\pi(a) = a$ ).

Na kratko jo zapišemo z  $(a_1 a_2 \dots a_r)$ .

**Trditev:** *Vsako permutacijo lahko zapišemo kot produkt disjunktnih ciklov.*

Primer:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 4 & 5 & 10 & 2 & 1 & 7 & 9 & 11 & 6 & 8 \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 8 & 2 & 1 & 3 & 10 & 9 & 4 & 5 & 7 & 6 & 11 \end{pmatrix}$$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 3 & 10 & 6 & 2 & 8 & 4 & 7 & 11 & 9 & 5 \end{pmatrix}$$

Potem je

$$\pi_1 = (1\ 3\ 5\ 2\ 4\ 10\ 6)(8\ 9\ 11),$$

$$\pi_2 = (1\ 8\ 5\ 10\ 6\ 9\ 7\ 4\ 3),$$

$$\pi = (2\ 3\ 10\ 9\ 11\ 5\ 2)(4\ 6\ 8\ 7)$$

**Transpozicija** je cikel dolžine 2. Vsak cikel pa je produkt transpozicij:

$$(a_1 a_2 a_3 \dots a_r) = (a_2 a_3) \circ (a_2 a_3) \circ \dots \circ (a_{r-1} a_r),$$

torej je tudi vsaka permutacija produkt transpozicij.

Seveda ta produkt ni nujno enolično določen,  
vseeno pa velja:

**Trditev:** *Nobena permutacija se ne da zapisati kot produkt sodega števila in kot produkt lihega števila permutacij.*



**Dokaz:** Naj bodo  $x_1, x_2, \dots, x_n$  različna realna števila. Poglejmo si produkt:  $P = \prod_{i < j} (x_i - x_j)$ . Izberimo indeksa  $a$  in  $b$ ,  $a < b$ , in pogledimo v katerih razlikah se pojavita:

|                                    |              |  |              |                                    |
|------------------------------------|--------------|--|--------------|------------------------------------|
| $x_1 - x_a, \dots, x_{a-1} - x_a,$ |              | $x_a - x_{a+1}, \dots, x_a - x_{b-1},$ | $x_a - x_b,$ | $x_a - x_{b+1}, \dots, x_a - x_n,$ |
| $x_1 - x_b, \dots, x_{a-1} - x_b,$ | $x_a - x_b,$ | $x_{a+1} - x_b, \dots, x_{b-1} - x_b,$ |              | $x_b - x_{b+1}, \dots, x_b - x_n.$ |

Razliko  $x_a - x_b$  smo navedli dvakrat, a se v produktu  $P$  pojavi samo enkrat. Če na množici indeksov opravimo transpozicijo  $(a b)$ , razlika  $x_a - x_b$  preide v razliko  $x_b - x_a$ , torej zamenja predznak, razlike iz prvega in zadnjega stolpca se med seboj zamenjajo, razlike iz srednjega stolpca pa tudi zamenjajo predznake (vendar je le-teh sodo mnogo in zato ne vplivajo na produkt  $P$ ).

Sedaj pa napravimo na množici indeksov permutacijo  $\pi$ .

V tem primeru je produkt

$$P_\pi = \prod_{i < j} (x_{\pi(i)} - x_{\pi(j)}).$$

enak  $\pm P$ . Če uporabimo sodo število transpozicij, potem je  $P_\pi = P$ , sicer pa  $P_\pi = -P$ . ■

Glede na sodo oziroma liho število transpozicij imenujemo permutacijo **soda** oziroma **liha** permutacija.

## Permutacije s ponavljanjem

**Permutacije s ponavljanjem** so nekakšne permutacije, pri katerih pa ne ločimo elementov v skupinah s  $k_1, k_2, \dots, k_r$  elementi - zato delimo število vseh permutacij s številom njihovih vrstnih redov, tj. permutacij:

$$\frac{n!}{k_1!k_2!\cdots k_r!}$$

## Kombinacije

**Binomski koeficient** oz. število **kombinacij**, tj. število  $m$ -elementnih podmnožic množice moči  $n$ , je

$$\binom{n}{m} = \frac{n \cdot (n-1) \cdots (n-m+1)}{1 \cdot 2 \cdots m} = \frac{n!}{m!(n-m)!},$$

saj lahko prvi element izberemo na  $n$  načinov,  
drugi na  $n-1$  načinov, ...,  
zadnji na  $n-m+1$  načinov,  
ker pa vrstni red izbranih elementov ni pomemben,  
dobljeno število še delimo s številom permutacij).

## Binomski obrazec - ponovitev

**Trditev:** *Za binomske koeficiente velja*

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \quad \text{in} \quad \binom{n}{m} + \binom{n}{m+1} = \binom{n+1}{m+1}.$$

*Dokaz:* Po definiciji je desna enakost ekvivalentna z

$$\frac{n!}{m!(n-m)!} + \frac{n!}{(m+1)!(n-m-1)!} = \frac{(n+1)!}{(m+1)!(n-m)!},$$

oziroma po množenju z  $m!(n-m-1)!/n!$  z

$$\frac{1}{n-m} + \frac{1}{m+1} = \frac{n+1}{(m+1)(n-m)}.$$

Prvi del trditve dokažemo s kombinatoriko (štetje)  
ali matematično indukcijo. ■



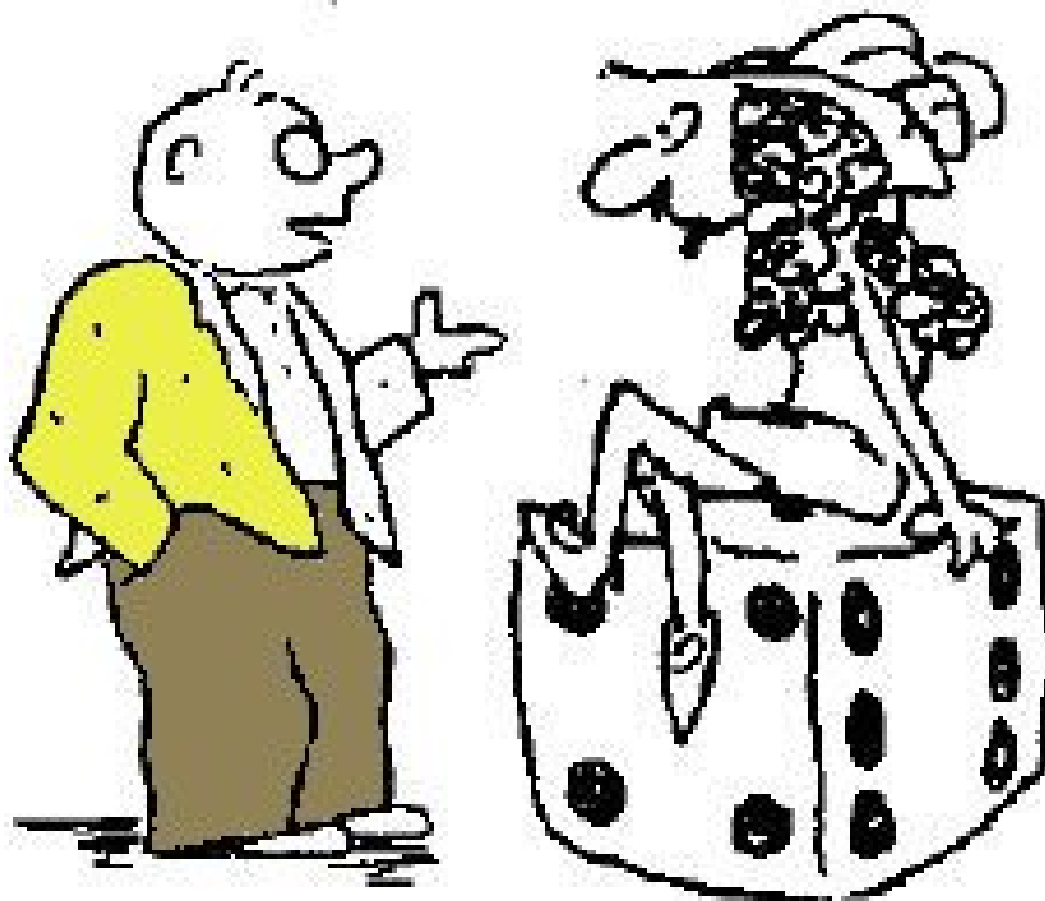
## Pascalov trikotnik - ponovitev

|  |  |  |  |  |  |  |  |  |   |  |   |  |    |  |    |  |     |  |     |  |    |  |    |  |   |  |   |
|--|--|--|--|--|--|--|--|--|---|--|---|--|----|--|----|--|-----|--|-----|--|----|--|----|--|---|--|---|
|  |  |  |  |  |  |  |  |  | 1 |  |   |  |    |  |    |  |     |  |     |  |    |  |    |  |   |  |   |
|  |  |  |  |  |  |  |  |  | 1 |  | 1 |  |    |  |    |  |     |  |     |  |    |  |    |  |   |  |   |
|  |  |  |  |  |  |  |  |  | 1 |  | 2 |  | 1  |  |    |  |     |  |     |  |    |  |    |  |   |  |   |
|  |  |  |  |  |  |  |  |  | 1 |  | 3 |  | 3  |  | 1  |  |     |  |     |  |    |  |    |  |   |  |   |
|  |  |  |  |  |  |  |  |  | 1 |  | 4 |  | 6  |  | 4  |  | 1   |  |     |  |    |  |    |  |   |  |   |
|  |  |  |  |  |  |  |  |  | 1 |  | 5 |  | 10 |  | 10 |  | 5   |  | 1   |  |    |  |    |  |   |  |   |
|  |  |  |  |  |  |  |  |  | 1 |  | 6 |  | 15 |  | 20 |  | 15  |  | 6   |  | 1  |  |    |  |   |  |   |
|  |  |  |  |  |  |  |  |  | 1 |  | 7 |  | 21 |  | 35 |  | 35  |  | 21  |  | 7  |  | 1  |  |   |  |   |
|  |  |  |  |  |  |  |  |  | 1 |  | 8 |  | 28 |  | 56 |  | 70  |  | 56  |  | 28 |  | 8  |  | 1 |  |   |
|  |  |  |  |  |  |  |  |  | 1 |  | 9 |  | 36 |  | 84 |  | 126 |  | 126 |  | 84 |  | 36 |  | 9 |  | 1 |



To so v obliki trikotnika zapisani binomski koeficienti, vsaka vrstica pa ustreza enemu binoskemu obrazcu.

# I. VERJETNOST



## I.1. Poskusi, dogodki in verjetnost



## Začetki verjetnosti



Ahil in Ajaks kockata, amfora, okrog 530 pr.n.š, Eksekias, Vatikan

Leta 1662 je plemič Chevalier de Mere zastavil matematiku Blaise Pascalu vprašanje:

**zakaj določene stave prinašajo dobiček druge pa ne.**

Le-ta si je o tem začel dopisovati s Fermatom in iz tega so nastali začetki verjetnostnega računa.

## ...začetki



Prvo tovrstno razpravo je napisal že leta 1545 italijanski kockar in matematik Cardano, a ni bila širše znana.

Tudi leta 1662 je anglež John Graunt sestavil na osnovi podatkov prve zavarovalniške tabele.

Leta 1713 je Jakob Bernoulli objavil svojo knjigo *Umetnost ugibanja* s katero je verjetnostni račun postal resna in splošno uporabna veda.

Njegov pomen je še utrdil Laplace, ko je pokazal njegov pomen pri analizi astronomskih podatkov (1812).



Leta 1865 je avstrijski menih Gregor Mendel uporabil verjetnostno analizo pri razlagi dednosti v genetiki.

V 20. stoletju se je uporaba verjetnostnih pristopov razširila skoraj na vsa področja.

## Poskus

Verjetnostni račun obravnava zakonitosti, ki se pokažejo v velikih množicah enakih ali vsaj zelo podobnih pojavov. Predmet verjetnostnega računa je torej empirične narave in njegovi osnovni pojmi so povzeti iz izkušnje. Osnovni pojmi v verjetnostnem računu so: poskus, dogodek in verjetnost dogodka.

**Poskus** je realizacija neke množice skupaj nastopajočih dejstev (kompleksa pogojev). Poskus je torej vsako dejanje, ki ga opravimo v natanko določenih pogojih.

### Primeri:

- met igralne kocke,
- iz kupa 20 igralnih kart izberemo eno karto.

## Dogodki

Pojav, ki v množico skupaj nastopajočih dejstev ne spada in se lahko v posameznem poskusu zgodi ali pa ne, imenujemo **dogodek**.

### Primeri:

- v poskusu meta igralne kocke je na primer dogodek, da vržemo 6 pik;
- v poskusu, da vlečemo igralno karto iz kupa 20 kart, je dogodek, da izvlečemo rdečo barvo.

Za poskuse bomo privzeli, da jih lahko neomejeno velikokrat ponovimo. Dogodki se bodo nanašali na isti poskus.

Poskuse označujemo z velikimi črkami iz konca abecede, npr.  $X$ ,  $Y$ ,  $X_1$ . Dogodke pa označujemo z velikimi črkami iz začetka abecede, npr.  $A$ ,  $C$ ,  $E_1$ .



## Vrste dogodkov

Dogodek je lahko:

- **gotov** dogodek –  $G$ : ob vsaki ponovitvi poskusa se zgodi.  
**Primer:** dogodek, da vržemo 1, 2, 3, 4, 5, ali 6 pik pri metu igralne kocke;
- **nemogoč** dogodek –  $N$ : nikoli se ne zgodi.  
**Primer:** dogodek, da vržemo 7 pik pri metu igralne kocke;
- **slučajen** dogodek: včasih se zgodi, včasih ne.  
**Primer:** dogodek, da vržemo 6 pik pri metu igralne kocke.

## Računanje z dogodki

Dogodek  $A$  je **poddogodek** ali **način** dogodka  $B$ , kar zapišemo  $A \subset B$ , če se vsakič, ko se zgodi dogodek  $A$ , zagotovo zgodi tudi dogodek  $B$ .

**Primer:** Pri metu kocke je dogodek  $A$ , da pade šest pik, način dogodka  $B$ , da pade sodo število pik.

Če je dogodek  $A$  način dogodka  $B$  in sočasno dogodek  $B$  način dogodka  $A$ , sta dogodka **enaka**:  $(A \subset B) \wedge (B \subset A) \iff A = B$ .

**Vsota** dogodkov  $A$  in  $B$ , označimo jo z  $A \cup B$  ali  $A + B$ , se zgodi, če se zgodi **vsaj** eden od dogodkov  $A$  in  $B$ .

**Primer:** Vsota dogodka  $A$ , da vržemo sodo število pik, in dogodka  $B$ , da vržemo liho število pik, je gotov dogodek.

*Velja:*  $A \cup B = B \cup A$ ;  $A \cup N = A$ ;  $A \cup G = G$ ;  $A \cup A = A$

$B \subset A \iff A \cup B = A$ ;  $A \cup (B \cup C) = (A \cup B) \cup C$

## ... Računanje z dogodki

**Produkt** dogodkov  $A$  in  $B$ , označimo ga z  $A \cap B$  ali  $AB$ , se zgodi, če se zgodita  $A$  in  $B$  **hkrati**.

**Primer:** Produkt dogodka  $A$ , da vržemo sodo število pik, in dogodka  $B$ , da vržemo liho število pik, je nemogoč dogodek.

*Velja:*  $A \cap B = B \cap A$ ;  $A \cap N = N$ ;  $A \cap G = A$ ;  $A \cap A = A$

$B \subset A \iff A \cap B = B$ ;  $A \cap (B \cap C) = (A \cap B) \cap C$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Dogodku  $A$  **nasproten** dogodek  $\bar{A}$  imenujemo negacijo dogodka  $A$ .

**Primer:** Nasproten dogodek dogodku, da vržemo sodo število pik, je dogodek, da vržemo liho število pik.

*Velja:*  $A \cap \bar{A} = N$ ;  $A \cup \bar{A} = G$ ;  $\bar{N} = G$ ;  $\bar{\bar{A}} = A$

$\overline{A \cup B} = \bar{A} \cap \bar{B}$ ;  $\overline{A \cap B} = \bar{A} \cup \bar{B}$

## ... Računanje z dogodki

Dogodka  $A$  in  $B$  sta **nezdružljiva**, če se ne moreta zgoditi hkrati, njun produkt je torej nemogoč dogodek,  $A \cap B = N$ .

**Primer:** Dogodka,  $A$  – da pri metu kocke pade sodo število pik in  $B$  – da pade liho število pik, sta nezdružljiva.

Poljuben dogodek in njegov nasprotni dogodek sta vedno nezdružljiva. Ob vsaki ponovitvi poskusa se zagotovo zgodi eden od njiju, zato je njuna vosta gotov dogodek:  $(A \cap \bar{A} = N) \wedge (A \cup \bar{A} = G)$ .

Če lahko dogodek  $A$  izrazimo kot vsoto nezdružljivih in mogočih dogodkov, rečemo, da je  $A$  **sestavljen** dogodek. Dogodek, ki ni sestavljen, imenujemo **osnoven** ali **elementaren** dogodek.

**Primer:** Pri metu kocke je šest osnovnih dogodkov:  $E_1$ , da pade 1 pika,  $E_2$ , da padeta 2 piki, ... ,  $E_6$ , da pade 6 pik. Dogodek, da pade sodo število pik je sestavljen dogodek iz treh osnovnih dogodkov ( $E_2$ ,  $E_4$  in  $E_6$ ).

## ... Računanje z dogodki

Množico dogodkov  $S = \{A_1, A_2, \dots, A_n\}$  imenujemo **popoln sistem dogodkov**, če se v vsaki ponovitvi poskusa zgodi natanko eden od dogodkov iz množice  $S$ .

To pomeni, da so vsi mogoči

$$A_i \neq N,$$

paroma nezdružljivi

$$A_i \cap A_j = N \quad i \neq j$$

in njihova vsota je gotov dogodek

$$A_1 \cup A_2 \cup \dots \cup A_n = G.$$

**Primer:** Popoln sistem dogodkov pri metu kocke sestavljajo na primer osnovni dogodki ali pa tudi dva dogodka: dogodek, da vržem sodo število pik, in dogodek, da vržem liho število pik.



Opišimo najpreprostejšo verjetnostno zakonitost. Denimo, da smo  $n$ -krat ponovili dan poskus in da se je  $k$ -krat zgodil dogodek  $A$ . Ponovitve poskusa, v katerih se  $A$  zgodi, imenujemo ugodne za dogodek  $A$ , število

$$f(A) = \frac{k}{n}$$

pa je **relativna frekvenca** (pogostost) dogodka  $A$  v opravljenih poskusih.

Statistični zakon, ki ga kaže izkušnja, je:

*Če poskus  $X$  dolgo ponavljamo, se relativna frekvenca slučajnega dogodka ustali in sicer skoraj zmeraj toliko bolj, kolikor več ponovitev poskusa napravimo.*

## Statistična definicija verjetnosti

To temeljno zakonitost so empirično preverjali na več načinov. Najbolj znan je poskus s kovanci, kjer so določali relativno frekvenco grba ( $f(A)$ ):

- Buffon je v 4040 metih dobil  $f(A) = 0,5069$ ,
- Pearson je v 12000 metih dobil  $f(A) = 0,5016$ ,
- Pearson je v 24000 metih dobil  $f(A) = 0,5005$ .

Ti poskusi kažejo, da se relativna frekvenca grba pri metih kovanca običajno ustali blizu 0,5. Ker tudi drugi poskusi kažejo, da je ustalitev relativne frekvence v dovolj velikem številu ponovitev poskusa splošna zakonitost, je smiselna naslednja *statistična definicija verjetnosti*:

*Verjetnost dogodka  $A$  v danem poskusu je število  $P(A)$ , pri katerem se navadno ustali relativna frekvenca dogodka  $A$  v velikem številu ponovitev tega poskusa.*



## Osnovne lastnosti verjetnosti

1. Ker je relativna frekvenca vedno nenegativna, je verjetnost  $P(A) \geq 0$ .

2.  $P(G) = 1$ ,  $P(N) = 0$  in  $A \subset B \Rightarrow P(A) \leq P(B)$ .

3. Naj bosta dogodka  $A$  in  $B$  nezdružljiva. Tedaj velja

$$P(A \cup B) = P(A) + P(B).$$

## Klasična definicija verjetnosti

Pri določitvi verjetnosti si pri nekaterih poskusih in dogodkih lahko pomagamo s *klasično definicijo verjetnosti*:

*Vzemimo, da so dogodki iz popolnega sistema dogodkov*

$\{E_1, E_2, \dots, E_s\}$  *enako verjetni:*

$$P(E_1) = P(E_2) = \dots = P(E_s) = p.$$

*Tedaj je*  $P(E_i) = 1/s$   $i = 1, \dots, s$ .

*Če je nek dogodek*  $A$  *sestavljen iz*  $r$  *dogodkov iz tega popolnega sistema dogodkov, potem je njegova verjetnost*  $P(A) = r/s$ .

**Primer:** Izračunajmo verjetnost dogodka  $A$ ,

da pri metu kocke padejo manj kot 3 pike.

Popolni sistem enako verjetnih dogodkov sestavlja 6 dogodkov.

Od teh sta le dva ugodna za dogodek  $A$  (1 in 2 piki).

Zato je verjetnost dogodka  $A$  enaka  $\frac{2}{6} = \frac{1}{3}$ .

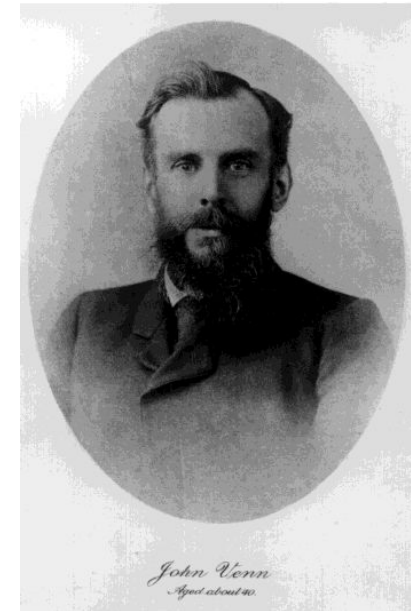
## Geometrijska verjetnost

V primerih, ko lahko osnovne dogodke predstavimo kot 'enakovredne' točke na delu premice (ravnine ali prostora), določimo verjetnost sestavljenega dogodka kot razmerje dolžin (ploščin, prostornin) dela, ki ustreza ugodnim izidom, in dela, ki ustreza vsem možnim izidom.

## Še dve lastnosti verjetnosti

4. Za dogodka  $A$  in  $B$  velja:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$



**Primer:** Denimo, da je verjetnost, da študent naredi izpit iz Sociologije  $P(S) = 2/3$ . Verjetnost, da naredi izpit iz Politologije je  $P(P) = 5/9$ . Če je verjetnost, da naredi vsaj enega od obeh izpitov  $P(S \cup P) = 4/5$ , kolikšna je verjetnost, da naredi oba izpita?

$$\begin{aligned} P(S \cap P) &= P(S) + P(P) - P(S \cup P) = \\ &= \frac{2}{3} + \frac{5}{9} - \frac{4}{5} = 0,42. \end{aligned}$$

*Za dogodke  $A$ ,  $B$  in  $C$  velja:*

$$\begin{aligned}
 P(A \cup B \cup C) &= P(A) + P(B) + P(C) \\
 &\quad - P(A \cap B) - P(A \cap C) - P(B \cap C) \\
 &\quad + P(A \cap B \cap C).
 \end{aligned}$$

**Kako lahko to pravilo posplošimo še na več dogodkov?**

Namig: Pravilo o vključitvi in izključitvi za množice  $A_1, A_2, \dots, A_n$ :

$$\begin{aligned}
 |A_1 \cup A_2 \cup \dots \cup A_n| &= \sum_{i=1}^n |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| \\
 &+ \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|.
 \end{aligned}$$

## ...Še dve lastnosti verjetnosti

$$5. P(\bar{A}) = 1 - P(A)$$

**Primer:** Iz kupa 32 kart slučajno povlečemo 3 karte. Kolikšna je verjetnost, da je med tremi kartami vsaj en as (dogodek  $A$ )?

Pomagamo si z nasprotnim dogodkom. Nasprotni dogodek  $\bar{A}$  dogodka  $A$  je, da med tremi kartami ni asa. Njegova verjetnost po klasični definiciji verjetnosti je določena s kvocientom števila vseh ugodnih dogodkov v popolnem sistemu dogodkov s številom vseh dogodkov v tem sistemu dogodkov. Vseh dogodkov v popolnem sistemu dogodkov je  $\binom{32}{3}$ , ugodni pa so tisti, kjer zbiramo med ne-asi, t.j.  $\binom{28}{3}$ . Torej je

$$P(\bar{A}) = \frac{\binom{28}{3}}{\binom{32}{3}} = 0,66 ; P(A) = 1 - P(\bar{A}) = 1 - 0,66 = 0,34.$$

## ...Še dve lastnosti verjetnosti

**Posledica.** Če so dogodki  $A_i$ ,  $i \in I$  paroma nezdružljivi, velja

$$P\left(\bigcup_{i \in I} A_i\right) = \sum_{i \in I} P(A_i).$$

Velja tudi za števno neskončne množice dogodkov.



## Aksiomi Kolmogorova

Dogodek predstavimo z množico zanj ugodnih izidov; gotov dogodek  $G$  ustreza univerzalni množici; nemogoč dogodek pa prazni množici.

Neprazna družina dogodkov  $\mathcal{D}$  je **algebra**, če velja:

- $A \in \mathcal{D} \Rightarrow \bar{A} \in \mathcal{D}$ ,
- $A, B \in \mathcal{D} \Rightarrow A \cup B \in \mathcal{D}$ .

Pri neskončnih množicah dogodkov moramo drugo zahtevo posplošiti

- $A_i \in \mathcal{D}, i \in I \Rightarrow \bigcup_{i \in I} A_i \in \mathcal{D}$ .

Dobljeni strukturi rečemo  **$\sigma$ -algebra**.



## ... Aksiomi Kolmogorova

Naj bo  $\mathcal{D}$   $\sigma$ -algebra v  $G$ . **Verjetnost na  $G$**  je preslikava  $P : \mathcal{D} \rightarrow \mathbb{R}$  z lastnostmi:

1.  $P(A) \geq 0$ ,
2.  $P(G) = 1$ ,
3. Če so dogodki  $A_i, i \in I$  paroma nezdružljivi, je

$$P\left(\bigcup_{i \in I} A_i\right) = \sum_{i \in I} P(A_i).$$

Trojica  $(G, \mathcal{D}, P)$  določa **verjetnostni prostor**.

Iz teh treh aksiomov lahko izpeljemo vse ostale lastnosti verjetnosti (Hladnik, str. 12).