10. poglavje

Kode za overjanje

(angl. **Authentication Codes**)

- Uvod
- Računanje verjetnosti prevare
- Kombinatorične ocene
  - pravokotne škatje (ang. orthogonal arrays, OA)
  - konstrukcije in ocene za OA
- Karakterizaciji kod za overjanje
- Ocene entropije
- Incidenčne strukture

Kode za overjanje nam nudijo metode za zagotavljanje *integritete* sporočil,
tj. da kljub aktivnemu napadalcu

- sporočilo pošilja pričakovana oseba in da
- sporočilo ni spremenjeno.

Shema za overjanje mora biti *brezpogojno varna*, medtem ko smo preučevali sheme za digitalne podpise in MAC-e glede na *računsko varnost*.

Uporaba

Veliki datoteki priredimo potrdilo (hranjeno poleg te datoteke), ki omogoči Bojanu, da preveri, ali je vsebina še vedno nespremenjena (s ključem, ki je hranjen na varnem).

Avtentičnost lahko preveri le tisti, ki mu je sporočilo namenjeno (digitalni podpis pa lahko preveri vsak).

Koda za overjanje *je četverka* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$, *za katero velja:*

1. $\mathcal{S}$ *je končna množica vseh začetnih stanj.*
2. $\mathcal{A}$ *je končna množica vseh potrdil.*
3. $\mathcal{K}$ *je končna množica vseh ključev.*
4. *Za vsak* $K \in \mathcal{K}$ *je dano pravilo za overjanje* $e_K : \mathcal{S} \longrightarrow \mathcal{A}$.

Množica sporočil pa je $\mathcal{M} = \mathcal{S} \times \mathcal{A}$.

Za pošiljanje podpisanega sporočila preko nezavarovanega kanala opravita Anita in Bojan naslednji protokol:

1. *Anita in Bojan skupaj izbereta naključni ključ* $K \in \mathcal{K}$ *(to storita tajno, tako kot v primeru simetrične kriptografije).*
2. *Anita za sporočilo* $s \in \mathcal{S}$ *izračuna* $a = e_K(s)$ *in pošlje Bojanu par* (s, a).
3. *Bojan dobi* (s, a), *izračuna* $a' = e_K(s)$ *in preveri, če je* $a = a'$.

Lažna prestavitev (ang. impersonation)

Napadalec vstavi v kanal sporočilo (s, a) v upanju, da ga bo Bojan sprejel za overjenega.

$$\text{napadalec} \xrightarrow{(s,a)} \text{Bojan}$$

Zamenjava

Napadalec opazi na kanalu sporočilo (s, a) in ga zamenja s sporočilom (s', a') v upanju, da ga bo Bojan sprejel za overjenega.

$$\text{Anita} \xrightarrow{(s,a)} \text{napadalec} \xrightarrow{(s',a')} \text{Bojan}$$

Vsakemu od zgornjih napadov priredimo ustrezno **verjetnost prevare** in ju označimo s Pd_0 in Pd_1.

Računanje verjetnosti prevare

Primer: $\mathcal{S} = \mathcal{A} = \mathbb{Z}_3$, $\mathcal{K} = \mathbb{Z}_3 \times \mathbb{Z}_3$ in

$e_{ij}(s) = is + j \bmod 3 \quad$ za vsak $(i, j) \in \mathcal{K}$ in $s \in \mathcal{S}$.

Sestavimo $(|\mathcal{K}| \times |\mathcal{S}|)$-dim. matriko M za overjanje, tako da v K-ti vrstici na s-to mesto postavimo element $e_K(s) \in \mathcal{A}$.

Če je v zgornjem primeru $p_{\mathcal{K}}(K)$=1/9 za vsak $K \in \mathcal{K}$, se ni težko prepričati, da je $Pd_0 = Pd_1 = 1/3$.

$$
\begin{array}{cc}
 & \begin{array}{ccc} 0 & 1 & 2 \end{array} \\
\begin{array}{c} (0,0) \\ (0,1) \\ (0,2) \\ (1,0) \\ (1,1) \\ (1,2) \\ (2,0) \\ (2,1) \\ (2,2) \end{array} &
\begin{pmatrix}
0 & 0 & 0 \\
1 & 1 & 1 \\
2 & 2 & 2 \\
0 & 1 & 2 \\
1 & 2 & 0 \\
2 & 0 & 1 \\
0 & 2 & 1 \\
1 & 0 & 2 \\
2 & 1 & 0
\end{pmatrix}
\end{array}
$$

Sedaj pa izračunajmo verjetnosti prevare v splošnem.

Označimo z $I(s,a)$, $s \in \mathcal{S}$, $a \in \mathcal{A}$ verjetnost, da bo Bojan sprejel sporočilo (s,a) za avtentično. Potem je

$$I(s,a) = P(a = e_K(s)) = \sum_{\{H \in \mathcal{K} \,|\, e_H(s)=a\}} p_{\mathcal{K}}(H).$$

Torej izračunamo $I(s,a)$ tako, da v matriki za overjanje izberemo vrstice, ki imajo v stolpcu s vrednost a in nato seštejemo verjetnosti ustreznih ključev.

Napadalec bo izbral tak (s,a), da bo $I(s,a)$ največji:

$$Pd_0 = \max\{I(s,a) \,|\, s \in \mathcal{S},\ a \in \mathcal{A}\}.$$

Medtem ko Pd_0 ni odvisna od porazdelitve $p_{\mathcal{S}}$, pa je Pd_1 lahko. Predpostavimo, da je napadalka na kanalu dobila (s, a) in ga hoče zamenjati s (s', a'), $s' \neq s$.

Za $s, s' \in \mathcal{S}$ in $a, a' \in \mathcal{A}$ je verjetnost, da Bojan ne bo opazil zamenjave, enaka

$$
\begin{aligned}
I(s', a'; s, a) &= P(a' = e_K(s')/a = e_K(s)) \\
&= \frac{P\big((a' = e_K(s')) \cap (a = e_K(s))\big)}{P\big(a = e_K(s)\big)} \\
&= \frac{\displaystyle\sum_{\{H \in \mathcal{K} \,|\, e_H(s) = a,\ e_H(s') = a'\}} p_{\mathcal{K}}(H)}{I(s, a)}.
\end{aligned}
$$

Napadalec maksimizira svoje možnosti, zato izračuna

$$p_{s,a} = \max\{I(s',a';s,a) \,|\, s' \in \mathcal{S},\ s \neq s' \text{ in } a' \in \mathcal{A}\}.$$

Torej je Pd_1 matematično upanje izrazov $p_{s,a}$ glede na porazdelitev $p_{\mathcal{M}}(s,a)$ in je enako

$$Pd_1 = \sum_{(s,a)\in\mathcal{M}} p_{\mathcal{M}}(s,a)\, p_{s,a}.$$

Verjetnostno porazdelitev za $p_{\mathcal{M}}$ preoblikujemo

$$\begin{aligned} p_{\mathcal{M}}(s,a) &= p_{\mathcal{S}}(s)\, p_{\mathcal{K}}(a/s) \\ &= p_{\mathcal{S}}(s) \sum_{\{K\in\mathcal{K},|\, e_K(s)=a\}} p_{\mathcal{K}}(K) \\ &= p_{\mathcal{S}}(s)\, I(s,a). \end{aligned}$$

Za vse $s \in \mathcal{S}$ in $a \in \mathcal{A}$ označimo s $q_{s,a}$ maksimalno vrednost vsote

$$\sum_{\{H \in \mathcal{K} \,|\, e_H(s)=a, e_H(s')=a'\}} p_{\mathcal{K}}(H)$$

glede na vse pare (s', a'), kjer je $s' \in \mathcal{S} \backslash \{s\}$ ter $a' \in \mathcal{A}$.

Od tod dobimo nekoliko bolj priročno formulo za verjetnost prevare

$$Pd_1 = \sum_{(s,a) \in \mathcal{M}} p_{\mathcal{S}}(s)\, q_{s,a}.$$

Kombinatorične ocene

Pri kodah za overjanje si želimo naslednje lastnosti:

- verjetnosti prevare Pd_0 in Pd_1 morata biti dovolj majhni,
- množica začetnih stanj $\mathcal{S}$ mora biti dovolj velika (saj želimo imeti dovolj veliko množico sporočil),
- množica ključev $\mathcal{K}$ naj bo kar se da majhna (saj pošiljamo ključe po varnem kanalu).

Izrek 1. *Za kodo za overjanje* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ *velja* $Pd_0 \geq 1/|\mathcal{A}|$. *Enakost velja, če in samo, če je*

$$\sum_{\{K \in \mathcal{K} \,|\, e_K(s)=a\}} p_{\mathcal{K}}(K) = \frac{1}{|\mathcal{A}|} \quad \text{za vsak } s \in \mathcal{S},\ a \in \mathcal{A}.$$

Dokaz: Za fiksen $s \in \mathcal{S}$ velja:

$$\begin{aligned} \sum_{a \in \mathcal{A}} I(s,a) &= \sum_{a \in \mathcal{A}} \sum_{\{H \in \mathcal{K} \,|\, e_H(s)=a\}} p_{\mathcal{K}}(H) \\ &= \sum_{H \in \mathcal{K}} p_{\mathcal{K}}(H) = 1. \qquad \blacksquare \end{aligned}$$

Izrek 2. *Za kodo za overjanje* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ *velja* $Pd_1 \geq 1/|\mathcal{A}|$. *Enakost velja, če in samo, če je*

$$\frac{\displaystyle\sum_{\{H \in \mathcal{K} \,|\, e_H(s)=a,\ e_H(s')=a'\}} p_{\mathcal{K}}(H)}{\displaystyle\sum_{\{H \in \mathcal{K} \,|\, e_H(s)=a\}} p_{\mathcal{K}}(H)} = \frac{1}{|\mathcal{A}|}$$

za vse $s, s' \in \mathcal{S}$, $s' \neq s$ *in* $a \in \mathcal{A}$.

Dokaz: Za fiksne $s, s' \in \mathcal{S}$, $s' \neq s$ in $a \in \mathcal{A}$, podobno kot v dokazu Izreka 1, izračunamo

$$\sum_{a' \in \mathcal{A}} I(s, a; s', a') = \sum_{a' \in \mathcal{A}} \frac{\displaystyle\sum_{\{H \in \mathcal{K} | e_H(s)=a,\, e_H(s')=a'\}} p_{\mathcal{K}}(H)}{\displaystyle\sum_{\{H \in \mathcal{K} \,|\, e_H(s)=a\}} p_{\mathcal{K}}(H)} = 1.$$

Od tod pa sledi

$$p_{s,a} = \max_{s \neq s'} I(s', a'; s, a) \geq 1/|\mathcal{A}|.$$

Verjetnost $\quad Pd_1 = \sum_{(s,a) \in \mathcal{M}} p_{\mathcal{M}}(s,a)\, p_{s,a}$

je torej navzdol omejena z

$$\sum_{(s,a) \in \mathcal{M}} \frac{p_{\mathcal{M}}(s,a)}{|\mathcal{A}|} = \frac{1}{|\mathcal{A}|}. \quad \blacksquare$$

Omenimo še dve očitni posledici izrekov 1 in 2.

Posledica 3. *Za kodo za overjanje* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ *velja* $Pd_0 = Pd_1 = 1/|\mathcal{A}|$, *če in samo, če je*

$$\sum_{\{H \in \mathcal{K} \,|\, e_H(s)=a,\ e_H(s')=a'\}} p_{\mathcal{K}}(H) = \frac{1}{|\mathcal{A}|^2}$$

za vse $s, s' \in \mathcal{S}$, $s' \neq s$ *in* $a, a' \in \mathcal{A}$. ■

Posledica 4. *Za kodo za overjanje* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$, *v kateri so vsi ključi enako verjetni, velja* $Pd_0 = Pd_1 = 1/|\mathcal{A}|$, *če in samo, če je*

$$|\{H \in \mathcal{K} \,|\, e_H(s) = a,\ e_H(s') = a'\}| = \frac{|\mathcal{K}|}{|\mathcal{A}|^2}$$

za vse $s, s' \in \mathcal{S}$, $s' \neq s$ *in* $a, a' \in \mathcal{A}$. ■

Pravokotne škatle

Pravokotna škatla (angl. orthogonal array) $OA(v, s, \lambda)$ je taka $(\lambda v^2 \times s)$-dimenzionalna matrika z v simboli, da se v vsakih dveh stolpcih vsak izmed v^2 možnih parov simbolov pojavi v natanko λ vrsticah.

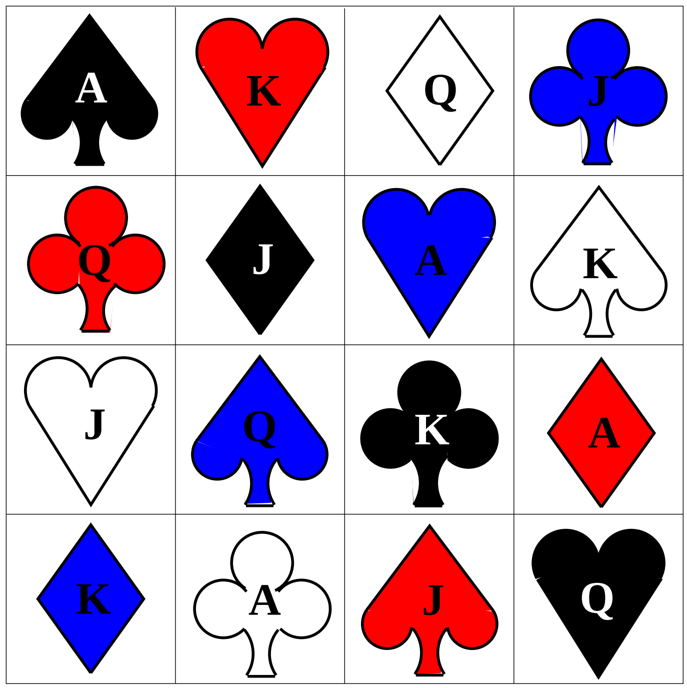
Te in njim ekvivalentne strukture (npr. transversalni designi, paroma pravokotni latinski kvadrati, mreže...) so del teorije designa.

Če dva stolpca $OA(v, s, 1)$ uporabimo za koordinate, lahko iz 3. stolpca sestavimo **latinski kvadrat**,

tj. $v \times v$-dimenzionalno matriko, v kateri vsi simboli iz $\{1, \ldots, v\}$ nastopajo v vsaki vrstici in vsakem stolpcu.

Primer : $OA(3, 3, 1)$

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 2 & 2 & 2 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}$$



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

Izrek 5. *Naj bo $OA(v, s, \lambda)$ pravokotna škatla. Potem obstaja koda za overjanje $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$, kjer je $|\mathcal{S}| = s$, $|\mathcal{A}| = v$, $|\mathcal{K}| = \lambda v^2$ in*

$$Pd_0 = Pd_1 = \frac{1}{v}.$$

Dokaz: Vsako vrstico $OA(v, s, \lambda)$ uporabimo kot pravilo za overjanje z verjetnostjo $1/(\lambda v^2)$:

pravokotna škatla	**koda za overjanje**
`vrstica`	`pravilo za overjanje`
`stolpec`	`začetno stanje`
`simbol`	`potrdilo`

■

Konstrukcije in ocene za OA

v je število potrdil, s določa število začetnih stanj, λ pa je povezan s številom ključev (λv^2).

Naj bo $Pd_0 \leq \varepsilon$ in $Pd_1 \leq \varepsilon$.
Potem naj za $OA(v, s, \lambda)$ velja

– $v \geq 1/\varepsilon$,
– $s \geq |\mathcal{S}|$ (nekaj stolpcev OA lahko izpustimo),
– λ naj bo čim manjši.

Izrek 6. *Če obstaja* $OA(v, s, \lambda)$, *potem za* $\lambda = 1$ *velja* $s \leq v + 1$, *v splošnem pa*

$$\lambda \geq \frac{s(v-1)+1}{v^2}.$$

Transverzalni design $TD_\lambda(s, v)$ je incidenčna struktura z bloki velikosti s, v katerem so točke razdeljene v s skupin velikosti v tako, da sta poljubni točki v λ blokih, če sta v različnih skupinah, sicer pa ne obstaja noben blok, ki bi ju vseboval.

Dokaz Izreka 6: Število vseh premic, ki sekajo eno premico transverzalnega designa $TD_1(s, v)$ je enako $(v-1)s$ in je kvečjemu enako številu vseh premic brez začetne premice, tj. $v^2 - 1$.

V transverzalnem designu $TD_\lambda(s, v)$, $\lambda \neq 1$, pa štejemo na podoben način in nato uporabimo še neenakost med aritmetično in kvadratno sredino (ki jo lahko izpeljemo iz Jensenove neenakosti). ∎

Izrek 7. *Za praštevilo p obstaja $OA(p,p,1)$, za $d \in \mathbb{N}\backslash\{1\}$ pa tudi $OA(p,(p^d-1)/(p-1),p^{d-2})$.*

Dokaz: Naj bo $\lambda = 1$. Za $\mathcal{K} = \mathbb{Z}_p \times \mathbb{Z}_p$ in $\mathcal{S} = \mathcal{A} = \mathbb{Z}_p$ definiramo $e_{ij}(s) = is + j \bmod p$.

Za $\lambda \neq 1$ pa bomo ekzistenco izpeljali v zadnjem razdelku iz konstrukcije projektivnega prostora $PG(n,d)$. ■

Za DN se prepričaj, da se da vsak $OA(n,n,1)$ razširiti za en stolpec do $OA(n,n+1,1)$.

Karakterizaciji kod za overjanje

Kode za overjanje z najmanjšimi verjetnostmi prevare so prav tiste, ki jih dobimo iz ortogonalnih škatel.

Izrek 8. *Če je* $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ *taka koda za overjanje, da je* $|\mathcal{A}| = v$ *in* $Pd_0 = Pd_1 = 1/v$*, potem je*

$$|\mathcal{K}| \geq v^2.$$

Enačaj velja natanko tedaj, ko obstaja $OA(v, s, 1)$

$$\text{in je} \quad |\mathcal{S}| = s \qquad \text{ter} \qquad p_{\mathcal{P}}(K) = \frac{1}{v^2} \quad \forall\, K \in \mathcal{K}.$$

Dokaz: Naj bosta $s, s' \in \mathcal{S}$, $s \neq s'$.

Za vsak par (a, a') potrdil sledi iz Posledice 3

$$\sum_{\{H \in \mathcal{K} \,|\, e_H(s)=a,\ e_H(s')=a'\}} p_{\mathcal{K}}(H) = \frac{1}{|\mathcal{A}|^2}.$$

Zato je

$$\mathcal{K}_{a,a'} = \{K \in \mathcal{K} \,|\, e_K(s) = a,\, e_K(s') = a'\} \neq \emptyset.$$

Ker je vseh takih množic v^2 in so disjunktne, velja $|\mathcal{K}| \geq v^2$. V primeru enakosti velja $|\mathcal{K}_{a,a'}| = 1$ za vsak par potrdil (a, a'), kar pomeni, da v matriki za overjanje v stolpcih s in s' vsak par potrdil pojavi natanko enkrat in imamo $OA(v, s, 1)$ za $s = |\mathcal{S}|$.

V primeru enakosti dobimo iz zgornje enakosti tudi

$$p_{\mathcal{K}}(K) = 1/v^2 \quad \text{za vsak} \ \ K \in \mathcal{K}. \ \blacksquare$$

Naslednja karakterizacija je še močnejša in jo predstavljamo brez dokaza.

Izrek 9. *Če je $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ taka koda za overjanje, da je $|\mathcal{S}| = s$, $|\mathcal{A}| = v$ in $Pd_0 = Pd_1 = 1/v$, potem je*

$$|\mathcal{K}| \geq s(v-1) + 1.$$

Enačaj velja natanko tedaj, ko obstaja $OA(v, s, \lambda)$ z

$$\lambda = \frac{s(v-1)+1}{v^2} \quad \text{in} \quad p_{\mathcal{P}}(K) = \frac{1}{s(v-1)+1} \quad \forall K \in \mathcal{K}.$$

Ocene entropije

Z Jensenovo neenakostjo lahko izpeljete še naslednji spodnji meji in se prepričate, da ju druga konstrukcija iz Izreka 7 doseže.

Izrek 10. *Če je $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$ koda za overjanje, potem velja*

$$\log Pd_0 \geq H(K/M) - H(K)$$

in

$$\log Pd_1 \geq H(K/M^2) - H(K/M).$$

Incidenčne strukture

t-(v, s, λ_t) **design** je

- zbirka s-elementnih podmnožic (**blokov**)
- množice z v elementi (**točkami**),
- kjer je vsaka t-elementna podmnožica vsebovana v natanko λ_t blokih.

Če je $\lambda_t = 1$, imenujemo t-design **Steinerjev sistem** in ga označimo s $S(t, s, v)$.

Naj bo za $i \in \mathbb{N}$, $0 \leq i \leq t$, in λ_i število blokov, ki vsebujejo neko i-elementno podmnožico točk S. Potem velja

$$\lambda_i \binom{s-i}{t-i} = \lambda_t \binom{v-i}{t-i}$$

in je število λ_i neodvisno od izbire podmnožice S.

Za $\lambda_0 = b$ in $\lambda_1 = r$, kadar je $t \geq 2$, velja

$$bs = rv \qquad \text{in} \qquad r(s-1) = \lambda_2(v-1).$$

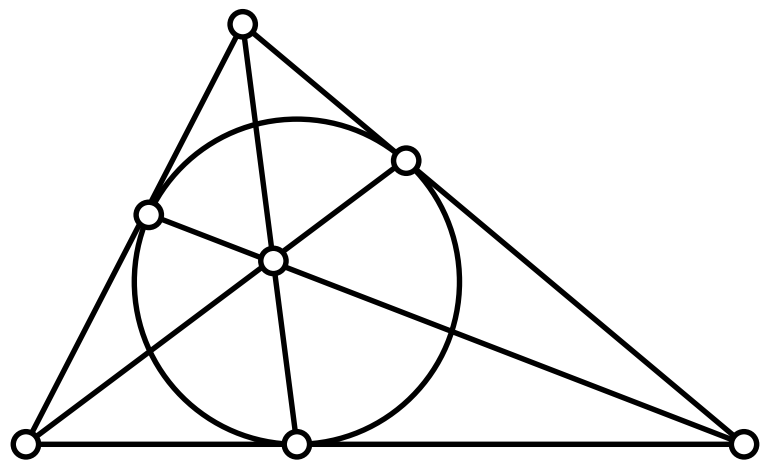
Projektivni prostor $PG(d, q)$ (dimenzije d nad q) dobimo iz vektorskega prostora $[GF(q)]^{d+1}$, tako da naredimo kvocient po 1-dimenzionalnih podprostorih.

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.,

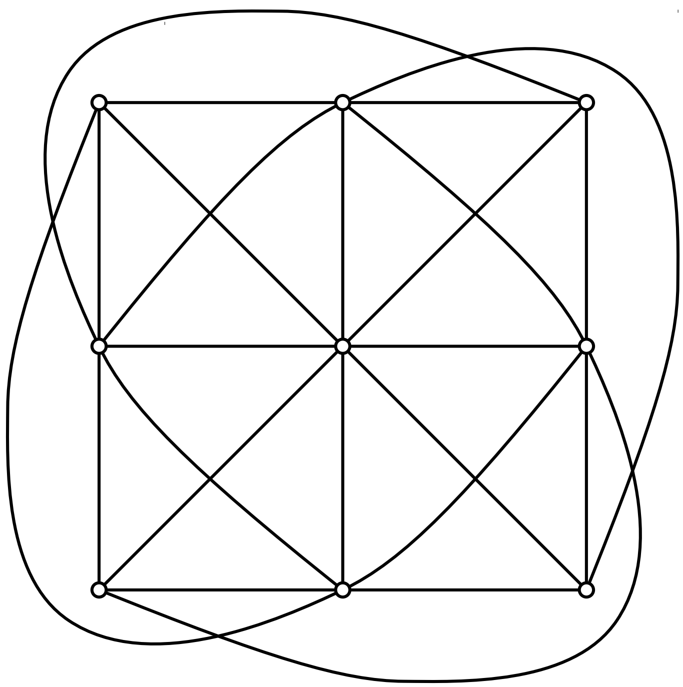
- $v = q^2 + q + 1$ je število točk (in število premic b),
- vsaka premica ima $k = q + 1$ točk
  (in skozi vsako točko gre $r = q + 1$ premic),
- vsak par točk leži na $\lambda = 1$ primicah
  (in vsaki premici se sekata v natanko eno točki).

Primeri:

1. Projektivno ravnino $PG(2,2)$ imenujemo **Fano ravnina** (7 točk in 7 premic).



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



3. $PG(2,4)$ lahko konstruiramo iz $\mathbb{Z}_{21}$:
točke $= \mathbb{Z}_{21}$ in premice $= \{S + x \mid x \in \mathbb{Z}_{21}\}$,
kjer je S 5-elementna podmnožica $\{3, 6, 7, 12, 14\}$.

$\{0, 3, 4, 9, 11\}$ $\{1, 4, 5, 10, 12\}$ $\{2, 5, 6, 11, 13\}$
$\{3, 6, 7, 12, 14\}$ $\{4, 7, 8, 13, 15\}$ $\{5, 8, 9, 14, 16\}$
$\{6, 9, 10, 15, 17\}$ $\{7, 10, 11, 16, 18\}$ $\{8, 11, 12, 17, 19\}$
$\{9, 12, 13, 18, 20\}$ $\{10, 13, 14, 19, 0\}$ $\{11, 14, 15, 20, 1\}$
$\{12, 15, 16, 0, 2\}$ $\{13, 16, 17, 1, 3\}$ $\{14, 17, 18, 2, 4\}$
$\{15, 18, 19, 3, 5\}$ $\{16, 19, 20, 4, 6\}$ $\{17, 20, 0, 5, 7\}$
$\{18, 0, 1, 6, 8\}$ $\{19, 1, 2, 7, 9\}$ $\{20, 2, 3, 8, 10\}$

Opozorilo: Podobno lahko Fano ravnino konstruiramo iz $\{0, 1, 3\}$ v $\mathbb{Z}_7$.