Primjene projektivne geometrije u teoriji kodiranja i kriptografiji

Marina Šimac

Odjel za matematiku

04.04.2011.

Literatura

- **A. Klein, L. Storme**: Applications of finite geometry in coding theory and cryptography

Projektivna geometrija

Aksiomi projektivne ravnine:

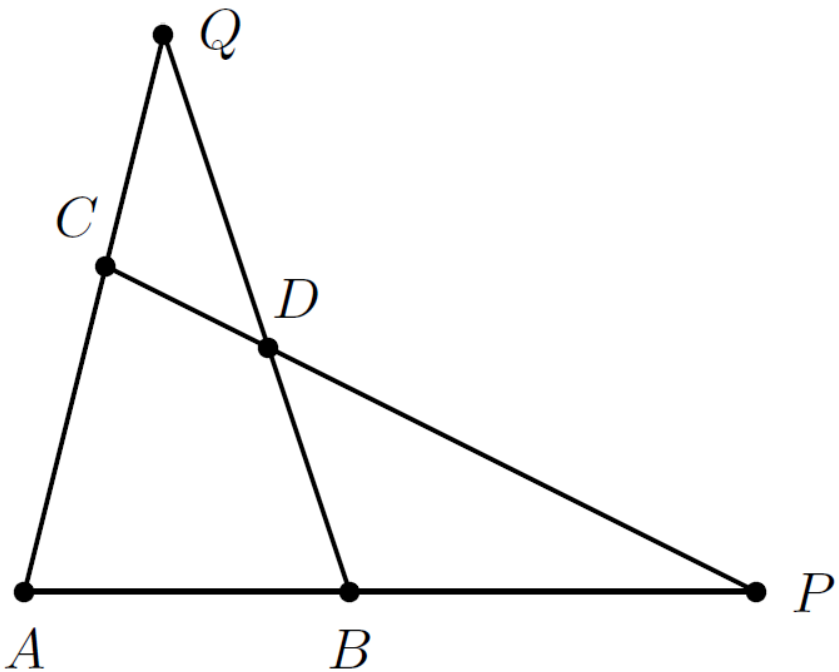
(P1) Svake dvije točke određuju točno jedan pravac.

(P2) Svaka dva pravca se sijeku u točno jednoj točki.

(P3) Postoje najmanje dva pravca i svaki pravac sadrži barem tri točke.

Veblen-Young aksiom

(P2') Neka su A, B, C i D četiri točke tako da se pravci AB i CD sijeku. Tada AC i BD imaju zajedničku točku.



Teorem

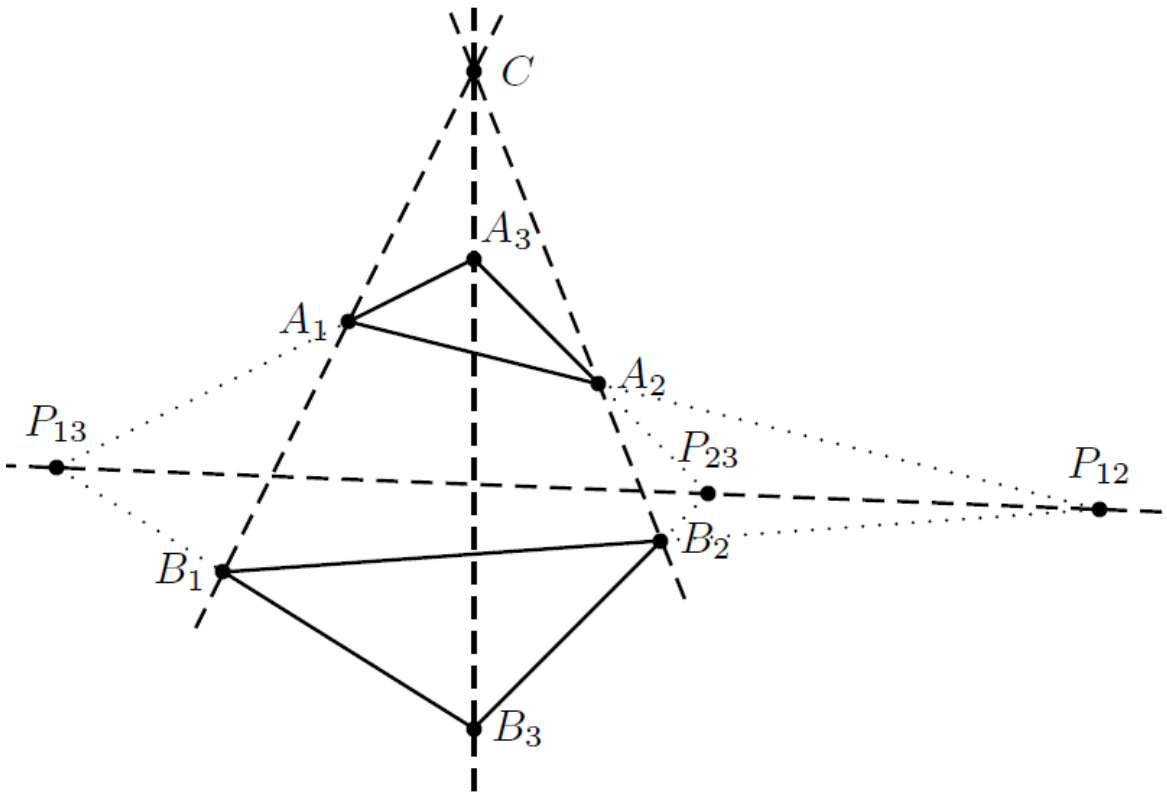
Neka je V vektorski prostor dimenzije $d+1 \geq 3$ nad poljem $\mathbb{F}_q$. Geometrija $PG(V)$ je definirana na sljedeći način:

- Točke u $PG(V)$ su 1-dimenzionalni potprostori od V.
- Pravci u $PG(V)$ su 2-dimenzionalni potprostori od V.
- Točka u $PG(V)$ je incidentna s pravcem iz $PG(V)$ ako je pripadni 1-dimenzionalni potprostor sadržan u odgovarajućem 2-dimenzionalnom potprostoru.

Tada je $PG(V)$ projektivni prostor.

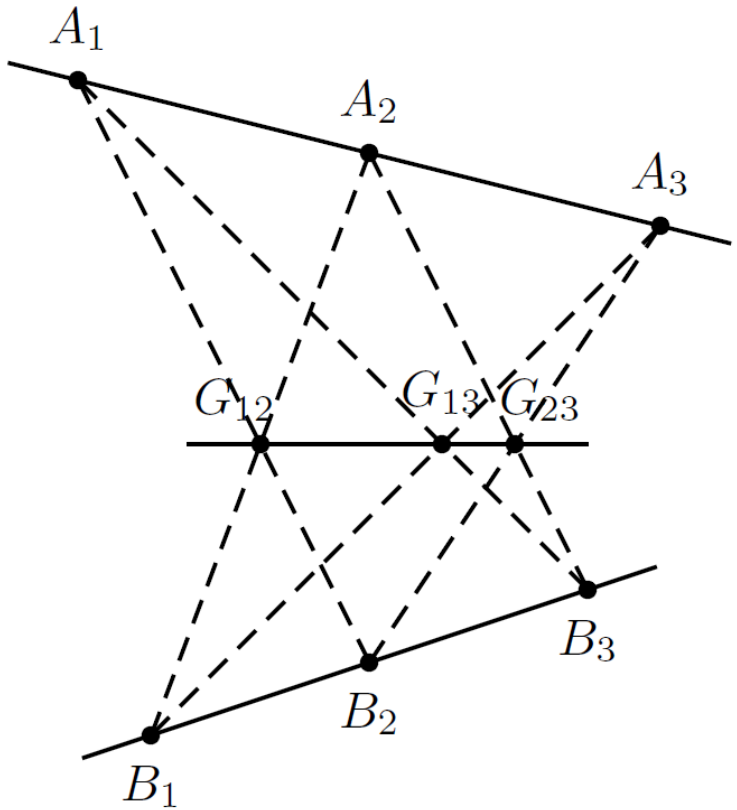
Desarguesov teorem

Neka su $A_1A_2A_3$ i $B_1B_2B_3$ dvije trojke nekolinearnih točaka takve da su pravci A_1B_1, A_2B_2 i A_3B_3 konkurentni i neka se sijeku u točki C.
Tada su točke $P_{12} = A_1A_2 \cap B_1B_2$, $P_{13} = A_1A_3 \cap B_1B_3$, i $P_{23} = A_2A_3 \cap B_2B_3$ kolinearne.



Pappusov teorem

Neka su l i h dva pravca koji se sijeku u točki S. Neka su A_1, A_2, A_3 različite točke pravca l različite od S, te B_1, B_2, B_3 različite točke pravca h različite od S.
Tada su točke $G_{12} = A_1B_2 \cap A_2B_1$, $G_{13} = A_1B_3 \cap A_3B_1$, i $G_{23} = A_2B_3 \cap A_3B_2$ kolinearne.



Teorem

- Projektivni prostor zadovoljava Desarguesov teorem akko je formiran kao $PG(V)$ za neki vektorski prostor V.
- Projektivni prostor zadovoljava Pappusov teorem akko je formiran kao $PG(V)$ za neki vektorski prostor V nad komutativnim poljem $\mathbb{F}_q$.

Teorem

- Projektivni prostor zadovoljava Desarguesov teorem akko je formiran kao $PG(V)$ za neki vektorski prostor V.
- Projektivni prostor zadovoljava Pappusov teorem akko je formiran kao $PG(V)$ za neki vektorski prostor V nad komutativnim poljem $\mathbb{F}_q$.

- V vektorski prostor dimenzije $d+1$ nad $\mathbb{F}_q \Rightarrow PG(d,q)$

Teorem

- Projektivni prostor zadovoljava Desarguesov teorem akko je formiran kao $PG(V)$ za neki vektorski prostor V.
- Projektivni prostor zadovoljava Pappusov teorem akko je formiran kao $PG(V)$ za neki vektorski prostor V nad komutativnim poljem $\mathbb{F}_q$.

- V vektorski prostor dimenzije $d+1$ nad $\mathbb{F}_q \Rightarrow PG(d,q)$
- homogene koordinate točke $\langle v \rangle$: $(a_0, \ldots, a_d)$

Točke u $PG(d, q)$

- Točke su klase uređenih $(d+1)$-torki, pri čemu je isključena $(0, 0, \ldots, 0)$.
- Dvije $(d+1)$-torke: $(a_0, \ldots, a_d)$, $(b_0, \ldots, b_d)$ predstavljaju istu točku ako pripadaju istoj klasi, tj. ako

$$(\exists \lambda \in \mathbb{F}_q, \lambda \neq 0)\ a_i = \lambda b_i,\ \ i = 0, \ldots, d$$

Točke u $PG(d, q)$

- Točke su klase uređenih $(d+1)$-torki, pri čemu je isključena $(0, 0, \ldots, 0)$.
- Dvije $(d+1)$-torke: $(a_0, \ldots, a_d)$, $(b_0, \ldots, b_d)$ predstavljaju istu točku ako pripadaju istoj klasi, tj. ako

$$(\exists \lambda \in \mathbb{F}_q, \lambda \neq 0)\ a_i = \lambda b_i,\ \ i = 0, \ldots, d$$

Primjer

- U $PG(2, 3) : (2, 0, 2) \equiv (1, 0, 1)$

Teorem

Projektivni prostor $PG(d, q)$ ima

$$\frac{q^{d+1}-1}{q-1} = q^d + q^{d-1} + \cdots + q + 1 \text{ točaka},$$

$$\frac{(q^d + q^{d-1} + \cdots + q + 1)(q^{d-1} + q^{d-2} + \cdots + q + 1)}{q+1} \text{ pravaca}.$$

Svaki pravac sadrži točno $q + 1$ točaka.

Teorija kodiranja

Definicija

Kod C duljine n nad poljem $\mathbb{F}_q$ je podskup $C \subset \mathbb{F}_q^n$.
Elementi koda se zovu **riječi koda**.

Teorija kodiranja

Definicija

Kod C duljine n nad poljem $\mathbb{F}_q$ je podskup $C \subset \mathbb{F}_q^n$.
Elementi koda se zovu **riječi koda**.

Primjer

$\mathbb{F}_3 = \{0, 1, 2\}$
$C = \{0011, 0121, 1201, 2102\} \subset \mathbb{F}_3^4$

Definicija

Neka je $x = (x_1, \dots x_n), y = (y_1, \dots, y_n) \in \mathbb{F}_q^n$.
Broj

$$d(x, y) = |\{i | x_i \neq y_i\}|$$

se naziva **Hammingova udaljenost**.

Definicija

Neka je $x = (x_1, \dots x_n), y = (y_1, \dots, y_n) \in \mathbb{F}_q^n$.
Broj

$$d(x, y) = |\{i | x_i \neq y_i\}|$$

se naziva **Hammingova udaljenost**.

Definicija

Težina riječi $x \in C$:

$$w(x) = d(x, 0)$$

Definicija

Linearni $[n, k]_q$ **kod** C duljine n je k-dimenzionalni potprostor vektorskog prostora $\mathbb{F}_q^n$.

Definicija

Linearni $[n, k]_q$ **kod** C duljine n je k-dimenzionalni potprostor vektorskog prostora $\mathbb{F}_q^n$.
Minimalna udaljenost d linearnog koda C je definirana na sljedeći način:

$$d = \min_{x \neq y \in C} d(x, y) = \min_{0 \neq x \in C} w(x)$$

Definicija

Linearni $[n, k]_q$ **kod** C duljine n je k-dimenzionalni potprostor vektorskog prostora $\mathbb{F}_q^n$.
Minimalna udaljenost d linearnog koda C je definirana na sljedeći način:

$$d = \min_{x \neq y \in C} d(x, y) = \min_{0 \neq x \in C} w(x)$$

$[n, k, d]_q$ kod je $[n, k]_q$ kod s minimalnom udaljenosti d.

Definicija

Generirajuća matrica G $[n, k, d]_q$ koda C je $k \times n$ matrica čiji retci čine bazu koda C.

Definicija

Generirajuća matrica G $[n, k, d]_q$ koda C je $k \times n$ matrica čiji retci čine bazu koda C.

Primjer

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Matrica G generira $[7, 4, 3]$ kod nad $\mathbb{F}_2$.

Definicija

Generirajuća matrica G $[n, k, d]_q$ koda C je $k \times n$ matrica čiji retci čine bazu koda C.

Primjer

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Matrica G generira $[7, 4, 3]$ kod nad $\mathbb{F}_2$.

- Za $x \in C$ vrijedi:

$$x = m \cdot G,$$

pri čemu je $m = [m_1 m_2 \dots m_k]$

Definicija

Za matricu G $[n, k, d]_q$ koda se kaže da je u **standardnom obliku** ako je $G = [I_k|A]$, pri čemu je I_k jedinična matrica reda k, i A neka $k \times (n - k)$ matrica.

Definicija

Za matricu G $[n, k, d]_q$ koda se kaže da je u **standardnom obliku** ako je $G = [I_k|A]$, pri čemu je I_k jedinična matrica reda k, i A neka $k \times (n-k)$ matrica.

Primjer

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Matrica G generira $[7, 4, 3]$ kod nad $\mathbb{F}_2$.

Definicija

Neka su $x, y \in \mathbb{F}_q^n$, $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$. **Skalarni produkt** vektora x i y definiran je sa: $x \cdot y = \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_q$.

Vektori x i y su **ortogonalni** ako je $x \cdot y = 0$.

Definicija

Neka su $x, y \in \mathbb{F}_q^n$, $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$. **Skalarni produkt** vektora x i y definiran je sa: $x \cdot y = \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_q$.

Vektori x i y su **ortogonalni** ako je $x \cdot y = 0$.

Definicija

Za $[n, k, d]_q$ kod C definiramo **dualni kod** $C^\perp$:

$$C^\perp = \{y \in \mathbb{F}_q^n | x \cdot y = 0, \forall x \in C\}$$

Definicija

Paritetna matrica H $[n, k, d]_q$ koda C je $(n-k) \times n$ matrica čiji retci su ortogonalni riječima koda C, tj.

$$c \in C \Leftrightarrow c \cdot H^T = 0$$

H je generirajuća matrica dualnog koda $C^\perp$.

Definicija

Paritetna matrica H $[n, k, d]_q$ koda C je $(n-k) \times n$ matrica čiji retci su ortogonalni riječima koda C, tj.

$$c \in C \Leftrightarrow c \cdot H^T = 0$$

H je generirajuća matrica dualnog koda $C^\perp$.

Primjer

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

H je paritetna matrica $[7, 4, 3]_2$ koda.

Singletonova granica

Za $[n, k, d]_q$ kod vrijedi $n - k + 1 \geq d$.

Singletonova granica

Za $[n, k, d]_q$ kod vrijedi $n - k + 1 \geq d$.

Definicija

Kodovi za koje vrijedi jednakost $n - k + 1 = d$ se nazivaju **MDS (Maximum Distance Separable) kodovi**.

Singletonova granica

Za $[n, k, d]_q$ kod vrijedi $n - k + 1 \geq d$.

Definicija

Kodovi za koje vrijedi jednakost $n - k + 1 = d$ se nazivaju **MDS (Maximum Distance Separable) kodovi**.

- Neka je C $[n, k, d]_q$ MDS kod. Pripadna paritetna matrica H je $(n - k) \times n$ matrica sa svojstvom da su bilo koja $n - k$ stupca linearno nezavisna.

Definicija

C je **GRS (Generalized Reed-Solomon) kod** ako su elementi pripadne generirajuće matrice $G = [g_{ij}]$, $1 \leq i \leq k$, $1 \leq j \leq n$, $(n \leq q)$

$$g_{ij} = v_j \alpha_j^{i-1},$$

pri čemu su $\alpha_1, \ldots, \alpha_n$ različiti elementi polja $\mathbb{F}_q$ i $v_1, \ldots, v_n \in \mathbb{F}_q$ različiti od 0.

Definicija

C je **GRS (Generalized Reed-Solomon) kod** ako su elementi pripadne generirajuće matrice $G = [g_{ij}]$, $1 \leq i \leq k$, $1 \leq j \leq n$, $(n \leq q)$

$$g_{ij} = v_j \alpha_j^{i-1},$$

pri čemu su $\alpha_1, \ldots, \alpha_n$ različiti elementi polja $\mathbb{F}_q$ i $v_1, \ldots, v_n \in \mathbb{F}_q$ različiti od 0.

- **GDRS (Generalized Doubly Extended Reed-Solomon) kodovi**

Primjer

$\mathbb{F}_q = \{0, a_1, \ldots, a_{q-1}\}$, H generirajuća matrica GDRS koda:

$$H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 0 \\ 0 & a_1 & \ldots & a_{q-1} & 0 \\ 0 & a_1^2 & \ldots & a_{q-1}^2 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & a_1^{n-k-2} & \ldots & a_{q-1}^{n-k-2} & 0 \\ 0 & a_1^{n-k-1} & \ldots & a_{q-1}^{n-k-1} & 1 \end{bmatrix}$$

Primjer

$\mathbb{F}_q = \{0, a_1, \ldots, a_{q-1}\}$, H generirajuća matrica GDRS koda:

$$H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 0 \\ 0 & a_1 & \ldots & a_{q-1} & 0 \\ 0 & a_1^2 & \ldots & a_{q-1}^2 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & a_1^{n-k-2} & \ldots & a_{q-1}^{n-k-2} & 0 \\ 0 & a_1^{n-k-1} & \ldots & a_{q-1}^{n-k-1} & 1 \end{bmatrix}$$

- Svakih $n-k$ stupaca matrice H je linearno nezavisno $\Rightarrow$ H je paritetna matrica MDS koda.

Defincija

n-**luk** u $PG(k-1,q)$ je skup od n točaka od kojih je svakih k linearno nezavisno.

Defincija

n-**luk** u $PG(k-1,q)$ je skup od n točaka od kojih je svakih k linearno nezavisno.

Primjer

n-luk u $PG(2,q)$: n točaka od kojih niti jedna trojka točaka nije kolinearna.

Definicija

$(q+1)-luk$ u $PG(k-1,q)$ koji odgovara GDRS kodu se naziva **normalna racionalna krivulja**.

Definicija

$(q+1)-luk$ u $PG(k-1,q)$ koji odgovara GDRS kodu se naziva **normalna racionalna krivulja**.

Primjer

$\{(1,t,\ldots,t^{k-1}|t\in\mathbb{F}_q)\}\cup\{(0,\ldots,0,1)\}$ je definira $[q+1,k,d=q+2-k]$-GDRS sa generirajućom matricom:

$$G=\begin{bmatrix} 1 & \ldots & 1 & 0 \\ t_1 & \ldots & t_q & 0 \\ t_1^2 & \ldots & t_q^2 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ t_1^{k-1} & \ldots & t_q^{k-1} & 1 \end{bmatrix}$$

Teorem

Svaki $[q+1, k, q+2-k]$-MDS kod je GDRS kod za

- neparnu potenciju q prostog broja,
- $2 \leq k < \frac{\sqrt{q}}{4}$.

Teorem

Svaki $[q+1, k, q+2-k]$-MDS kod je GDRS kod za

- neparnu potenciju q prostog broja,
- $2 \leq k < \frac{\sqrt{q}}{4}$.

Teorem

Ako vrijedi:

- q neparan i $2 \leq k \leq q+3-6\sqrt{q \log q}$

  ili

- q paran i $4 \leq k \leq q+3-6\sqrt{q \log q}$,

Tada se $[q+1, k, q+2-k]_q$-GDRS kod ne može proširiti do $[q+2, k, q+3-k]_q$-MDS koda.

- $N_q(d, k)$ - najmanji n za koji postoji $[n, k, d]_q$ kod.

Griesmerova granica

Vrijedi:

1. $N_q(k, d) \geq d + N_q\left(k-1, \lceil \frac{d}{q} \rceil\right)$
2. $N_q(k, d) \geq G_q(k, d) = \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$

Geometrijska interpretacija

- Neka je C $[n,k]_q$ kod s generirajućom matricom G.
- Svaki stupac matrice G određuje točku u $PG(k-1,q)$.
- Kod C prikazujemo multiskupom M: i-**točka** je točka kratnosti i.
- Za svaki $S \subseteq PG(k-1,q)$ označimo s $c(S)$ broj točaka iz S koji se nalaze u M.
- $\gamma_i = \max\{c(S) | \dim(S) = i)\}$

Geometrijska interpretacija

- Neka je C $[n,k]_q$ kod s generirajućom matricom G.
- Svaki stupac matrice G određuje točku u $PG(k-1,q)$.
- Kod C prikazujemo multiskupom M: i-**točka** je točka kratnosti i.
- Za svaki $S \subseteq PG(k-1,q)$ označimo s $c(S)$ broj točaka iz S koji se nalaze u M.
- $\gamma_i = \max\{c(S) | \dim(S) = i)\}$

Lema

Neka je $(s-1)q^{k-1} < d \leq sq^{k-1}$ i neka je C $[n,k,d]_q$ kod koji postiže Griesmerovu granicu.
Tada $\gamma_0 = \max\{c(P) | P \in PG(k-1,q)\} = s$.

- Označimo sa $\theta_k = \frac{q^k-1}{q-1}$ broj točaka u $PG(k-1, q)$.

- Označimo sa $\theta_k = \frac{q^k-1}{q-1}$ broj točaka u $PG(k-1,q)$.

Neka je $[n,k,d]_q$ kod C koji postiže Griesmerovu granicu i neka je:

$$d = sq^{k-1} - \sum_{i=0}^{k-2} t_i q^i,\ 0 \leq t_i \leq q-1$$

- Označimo sa $\theta_k = \frac{q^k-1}{q-1}$ broj točaka u $PG(k-1, q)$.

Neka je $[n, k, d]_q$ kod C koji postiže Griesmerovu granicu i neka je:

$$d = sq^{k-1} - \sum_{i=0}^{k-2} t_i q^i, \ 0 \leq t_i \leq q-1$$

Vrijedi:

- $\gamma_0 = s$

- Označimo sa $\theta_k = \frac{q^k-1}{q-1}$ broj točaka u $PG(k-1, q)$.

Neka je $[n, k, d]_q$ kod C koji postiže Griesmerovu granicu i neka je:

$$d = sq^{k-1} - \sum_{i=0}^{k-2} t_i q^i, \ 0 \leq t_i \leq q-1$$

Vrijedi:

- $\gamma_0 = s$
- $n = s\theta_k - \sum_{i-0}^{k-2} t_i \theta_{i+1}$

Multiskup M':

Težina točke $P \in PG(k-1,q)$: $\omega(P) := \gamma_0 - c(P)$.

Težina potprostora $S \leq PG(k-1,q)$: $\omega(S) =: \sum_{P \in S} \omega(P)$.

Multiskup M':

Težina točke $P \in PG(k-1,q)$: $\omega(P) := \gamma_0 - c(P)$.

Težina potprostora $S \leq PG(k-1,q)$: $\omega(S) =: \sum_{P \in S} \omega(P)$.

Označimo sa ω_i minimalnu težinu i-dimenzionalnih potprostora.

Multiskup M':

Težina točke $P \in PG(k-1,q)$: $\omega(P) := \gamma_0 - c(P)$.

Težina potprostora $S \leq PG(k-1,q)$: $\omega(S) =: \sum_{P \in S} \omega(P)$.

Označimo sa ω_i minimalnu težinu i-dimenzionalnih potprostora.

Vrijedi:

- $\gamma_i + \omega_i = s \cdot \theta_{i+1}$

Multiskup M':

Težina točke $P \in PG(k-1,q)$: $\omega(P) := \gamma_0 - c(P)$.

Težina potprostora $S \leq PG(k-1,q)$: $\omega(S) =: \sum_{P \in S} \omega(P)$.

Označimo sa ω_i minimalnu težinu i-dimenzionalnih potprostora.

Vrijedi:

- $\gamma_i + \omega_i = s \cdot \theta_{i+1}$
- $\omega_{k-1} = \sum_{i=0}^{k-2} t_i \theta_{i+1}$

Multiskup M':

Težina točke $P \in PG(k-1,q)$: $\omega(P) := \gamma_0 - c(P)$.

Težina potprostora $S \leq PG(k-1,q)$: $\omega(S) =: \sum_{P \in S} \omega(P)$.

Označimo sa ω_i minimalnu težinu i-dimenzionalnih potprostora.

Vrijedi:

- $\gamma_i + \omega_i = s \cdot \theta_{i+1}$
- $\omega_{k-1} = \sum_{i=0}^{k-2} t_i \theta_{i+1}$
- $\omega_{k-2} = \sum_{i=0}^{k-2} t_i \theta_i$

Defincija

$(n, w; d, q)$-**minihyper** je multiskup od n točaka iz $PG(d, q)$ sa svojstvom da sa svakom hiperravninom ima najviše w zajedničkih točaka.

Defincija

$(n, w; d, q)$-**minihyper** je multiskup od n točaka iz $PG(d, q)$ sa svojstvom da sa svakom hiperravninom ima najviše w zajedničkih točaka.

Teorem

Neka je $k \leq d$. $(\theta_{k+1}, \theta_k; d, q)$ minihyper je k-dimenzionalni potprostor od $PG(d, q)$.

Defincija

$(n, w; d, q)$-**minihyper** je multiskup od n točaka iz $PG(d, q)$ sa svojstvom da sa svakom hiperravninom ima najviše w zajedničkih točaka.

Teorem

Neka je $k \leq d$. $(\theta_{k+1}, \theta_k; d, q)$ minihyper je k-dimenzionalni potprostor od $PG(d, q)$.

Teorem

Neka je F $\left(\sum_{i=0}^{k-2} \epsilon_i \theta_{i+1}, \sum_{i=0}^{k-2} \epsilon_i \theta_i; k-1, q\right)$ minihyper, pri čemu je $\sum_{i=0}^{k-2} \epsilon_i < \sqrt{q} + 1$. Tada je F unija od ϵ_0 točaka, ϵ_1 pravaca $\ldots$ ϵ_{k-2} $(k-2)$-dimenzionalnih potprostora koji su svi u parovima disjunktni.

Defincija

Neka je C $[n, k, d]_q$ kod. **Polumjer pokrivanja** koda C je najmanji cijeli broj R za koji vrijedi da je Hammingova udaljenost svake n-torke iz $\mathbb{F}_q^n$ i riječi koda C najviše R.

Defincija

Neka je C $[n, k, d]_q$ kod. **Polumjer pokrivanja** koda C je najmanji cijeli broj R za koji vrijedi da je Hammingova udaljenost svake n-torke iz $\mathbb{F}_q^n$ i riječi koda C najviše R.

Teorem

Neka je C $[n, k, d]_q$ kod s paritetnom matricom $H = (h_1, \ldots, h_n)$. Tada je polumjer pokrivanja koda C jednak R akko se svaka $(n-k)$-torka iz $\mathbb{F}_q^{n-k}$ može zapisati kao linearna kombinacija od najviše R stupaca matrice H.

Defincija

Neka je $S \subseteq PG(N, q)$. S se naziva ρ-**zasićeni skup** ako se svaka točka $P \in PG(N, q)$ može zapisati kao linearna kombinacija od najviše $\rho + 1$ točaka iz S.

Defincija

Neka je $S \subseteq PG(N, q)$. S se naziva ρ-**zasićeni skup** ako se svaka točka $P \in PG(N, q)$ može zapisati kao linearna kombinacija od najviše $\rho + 1$ točaka iz S.

- ρ-zasićeni skupovi iz $PG(n - k - 1, q)$ određuju paritetnu matricu linearnog $[n, k, d]_q$ koda sa polumjerom pokrivanja $R = \rho + 1$.

Primjer: 1-zasićeni skup u $PG(3,q)$ kardinalnosti $2q+1$

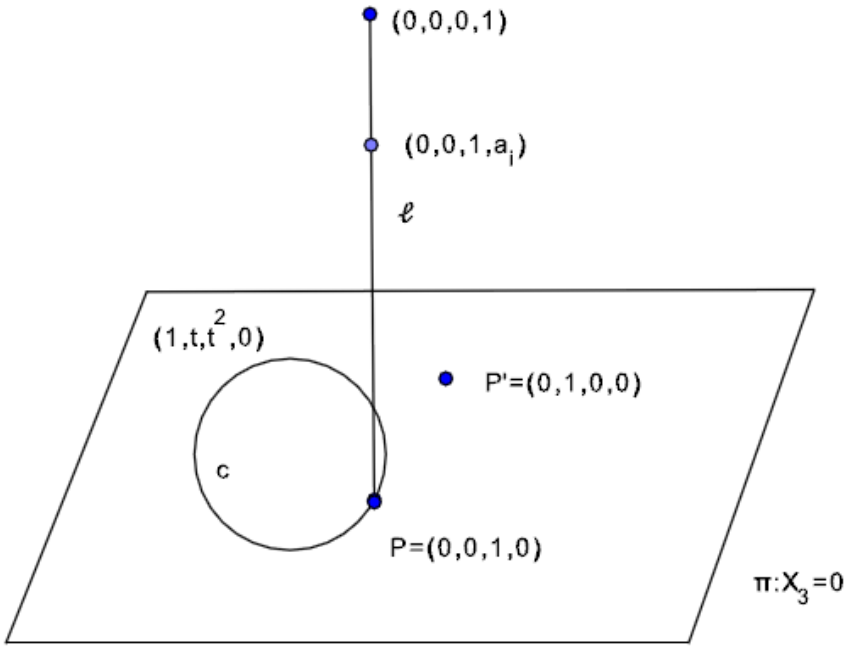
$$H = \begin{bmatrix} 1 & \dots & 1 & 0 & 0 & 0 & \dots & 0 \\ a_1 & \dots & a_q & 1 & 0 & 0 & \dots & 0 \\ a_1^2 & \dots & a_q^2 & 0 & 0 & 1 & \dots & 1 \\ 0 & \dots & 0 & 0 & 1 & a_2 & \dots & a_q \end{bmatrix}$$

Stupci matrice H definiraju 1-zasićeni skup kardinalnosti $2q+1$ u $PG(3,q)$

Primjer: 1-zasićeni skup u $PG(3,q)$ kardinalnosti $2q+1$

- Konika $c = \{(1,t,t^2,0) | t \in \mathbb{F}_q\} \cup \{P = (0,0,1,0)\}$ u ravnini $\pi : X_3 = 0$ u $PG(3,q)$
- Za paran q točka $P' = (0,1,0,0)$ je središte konike, dok za neparan q točka na tangenti postavljenoj u P
- l je pravac koji sadrži točku P i ne leži u ravnini π

$\Rightarrow S = (c \cup l \cup \{P'\}) \backslash \{P\}$ je 1-zasićeni skup u $PG(3,q)$



Kriptografija

Kriptografija

- djelitelj
- tajna
- sudionici

Kriptografija

- djelitelj
- tajna
- sudionici

Tajna D podijeljena na n dijelova: $D_1, \ldots D_n$ pri čemu vrijedi:

1. poznavanje k ili više dijelova D_i omogućava rekonstruiranje tajne D

Kriptografija

- djelitelj
- tajna
- sudionici

Tajna D podijeljena na n dijelova: $D_1, \ldots D_n$ pri čemu vrijedi:

1. poznavanje k ili više dijelova D_i omogućava rekonstruiranje tajne D
2. poznavanje $k-1$ ili manje dijelova D_i nije dovoljno za rekonstruiranje tajne D

Primjer: Shamirova shema

Djelitelj odabere polinom stupnja $k-1$:

$$f(x) = f_0 + f_1 x + \ldots + f_{k-1} x^{k-1} \in \mathbb{F}_q[x],$$

pri čemu je tajna $D = f(0) = f_0$.

i-ti sudionik: $(x_i, f(x_i))$ $(x_i \neq 0, 1 \leq 1 \leq n)$.

Primjer: Shamirova shema

Djelitelj odabere polinom stupnja $k-1$:

$$f(x) = f_0 + f_1 x + \ldots + f_{k-1} x^{k-1} \in \mathbb{F}_q[x],$$

pri čemu je tajna $D = f(0) = f_0$.

i-ti sudionik: $(x_i, f(x_i))$ $(x_i \neq 0, 1 \leq 1 \leq n)$.

- k sudionika može rekonstruirati tajnu

Primjer: Shamirova shema

Djelitelj odabere polinom stupnja $k-1$:

$$f(x) = f_0 + f_1 x + \ldots + f_{k-1} x^{k-1} \in \mathbb{F}_q[x],$$

pri čemu je tajna $D = f(0) = f_0$.

i-ti sudionik: $(x_i, f(x_i))$ $(x_i \neq 0, 1 \leq 1 \leq n)$.

- k sudionika može rekonstruirati tajnu
- manje od k sudionika ne može rekonstruirati tajnu

Primjer

Neka je π hiperravnina u $PG(k, q)$ i $P_0, \ldots, P_n$ $(n+1)$-luk u π. Neka je l pravac u $PG(k, q)$ tako da $\pi \cap l = P_0$.

i-ti sudionik: P_i $(1 \leq 1 \leq n)$

Primjer

Neka je π hiperravnina u $PG(k,q)$ i $P_0,\ldots,P_n$ $(n+1)$-luk u π. Neka je l pravac u $PG(k,q)$ tako da $\pi \cap l = P_0$.

i-ti sudionik: P_i $(1 \leq 1 \leq n)$

- k sudionika mogu rekonstruirati tajnu:

$$\pi = \langle P_1,\ldots,P_k\rangle \Rightarrow P_0 = \pi \cap l$$

Primjer

Neka je π hiperravnina u $PG(k,q)$ i $P_0,\ldots,P_n$ $(n+1)$-luk u π. Neka je l pravac u $PG(k,q)$ tako da $\pi \cap l = P_0$.

i-ti sudionik: P_i $(1 \leq 1 \leq n)$

- k sudionika mogu rekonstruirati tajnu:

$$\pi = \langle P_1,\ldots,P_k\rangle \Rightarrow P_0 = \pi \cap l$$

- $i < k$ sudionika ne mogu rekonstruirati tajnu P_0

Defincija

Neka je P skup osoba. **Struktura pristupa** Γ je podskup od $\mathcal{P}(P)$ sa svojstvom:

$$A \in \Gamma \ \Rightarrow \ B \in \Gamma, \ \forall B \supset A$$

Defincija

Neka je P skup osoba. **Struktura pristupa** Γ je podskup od $\mathcal{P}(P)$ sa svojstvom:

$$A \in \Gamma \Rightarrow B \in \Gamma, \forall B \supset A$$

- **ovlašteni skupovi**
- **neovlašteni skupovi**

Defincija

Neka je Γ struktura pristupa za skup osoba P. **Konfiguracija potprostora** za Γ je skup potprostora $S_p, p \in P$, i S prostor tajne sa sljedećim svojstvima:

1. $S \cap \langle S_p | p \in A \rangle = \emptyset, \ \forall A \notin \Gamma$
2. $S \subseteq \langle S_p | p \in A \rangle \, , \ \forall A \in \Gamma$

Defincija

Neka je Γ struktura pristupa za skup osoba P. **Konfiguracija potprostora** za Γ je skup potprostora $S_p, p \in P$, i S prostor tajne sa sljedećim svojstvima:

1. $S \cap \langle S_p | p \in A \rangle = \emptyset, \ \forall A \notin \Gamma$
2. $S \subseteq \langle S_p | p \in A \rangle, \ \forall A \in \Gamma$

Teorem

Neka je Γ struktura pristupa.
Tada postoji konfiguracija potprostora za Γ u $PG(d, q)$ za dovoljno veliki d.

Defincija

Nosač riječi $c \in \mathbb{F}_q^n$ je definiran s:

$$\sup(c) = \{i | c_i \neq 0\}.$$

Defincija

Nosač riječi $c \in \mathbb{F}_q^n$ je definiran s:

$$\sup(c) = \{i | c_i \neq 0\}.$$

Neka je C linarni kod. Ne-nul riječ $c \in C$ se naziva **minimalna** ako vrijedi:

$$\forall c' \in C : \ \sup(c') \subseteq \sup(c) \ \Rightarrow \ c' \in \langle c \rangle$$

Defincija

Nosač riječi $c \in \mathbb{F}_q^n$ je definiran s:

$$\sup(c) = \{i | c_i \neq 0\}.$$

Neka je C linarni kod. Ne-nul riječ $c \in C$ se naziva **minimalna** ako vrijedi:

$$\forall c' \in C : \ \sup(c') \subseteq \sup(c) \ \Rightarrow \ c' \in \langle c \rangle$$

Lema

Neka je C $[n+1, k]_q$ kod. Shema dijeljenja tajne se konstruira iz C odabirom riječi $c = (c_0, \ldots, c_n)$. c_o je tajna, a informacije koji svaki sudionik dobiva su koordinate c_i $(1 \leq i \leq n)$.
Minimalni ovlašteni skup odgovara minimalnoj riječi u $C^\perp$ sa 0 u svom nosaču.

Defincija

MAC (Message Authentication Code) je četvorka $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$, pri čemu je:

1. $\mathcal{S}$ je konačan skup poruka
2. $\mathcal{A}$ je konačan skup autentifikacijskih oznaka
3. $\mathcal{K}$ je skup ključeva
4. Za svaki $K \in \mathcal{K}$ postoji autentifikacijsko pravilo $e_K \in \mathcal{E}$, $e_K : \mathcal{S} \to \mathcal{A}$

Definicija

MAC (Message Authentication Code) je četvorka $(\mathcal{S}, \mathcal{A}, \mathcal{K}, \mathcal{E})$, pri čemu je:

1. $\mathcal{S}$ je konačan skup poruka
2. $\mathcal{A}$ je konačan skup autentifikacijskih oznaka
3. $\mathcal{K}$ je skup ključeva
4. Za svaki $K \in \mathcal{K}$ postoji autentifikacijsko pravilo $e_K \in \mathcal{E}$, $e_K : \mathcal{S} \to \mathcal{A}$

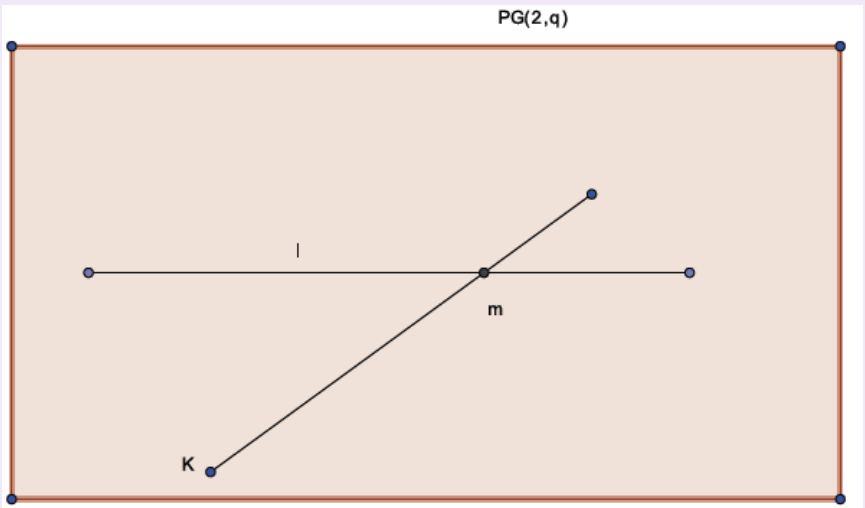
Definicija

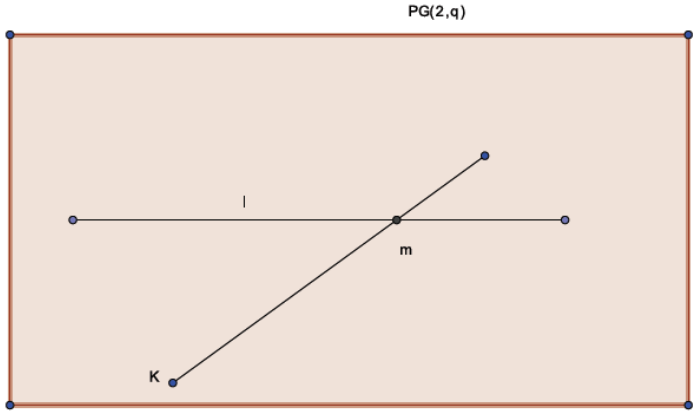
Označimo sa p_i vjerojatnost da napadač konstruira par $(s, e_K(s))$ bez poznavanja ključa K pomoću i različitih parova $(s_j, e_K(s_j))$. Najmanji broj r za koji vrijedi $p_{r+1} = 1$ se naziva **red sheme**. p_0 se naziva **vjerojatnost imitirajućeg napada**, a p_1 **vjerojatnost napada supstitucijom**.

Primjer

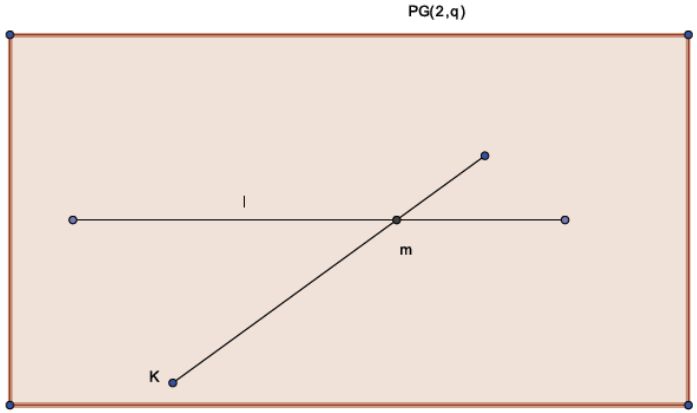
Neka je π projektivna ravnina reda q: $PG(2, q)$, i neka je l pravac u π.

- Poruka m = točka na pravcu l.
- Autentifikacijski ključ = točka u $PG(2, Q) \backslash l$.
- Autentifikacijska oznaka $e_K(s)$ = pravac koji sadrži m i K.





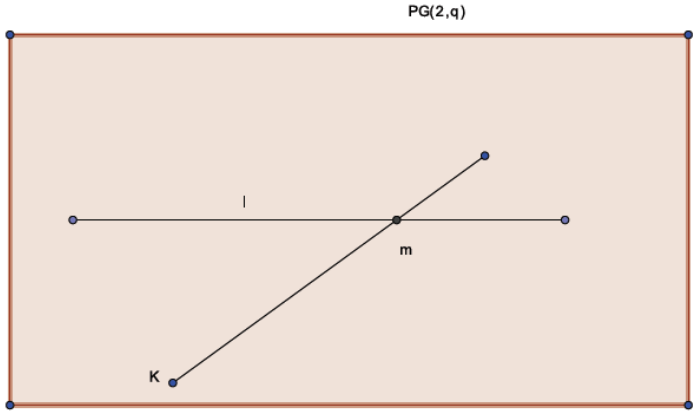
- vjerojatnost imitirajućeg napada: $\frac{1}{q}$
- vjerojatnost napada supstitucijom: $\frac{1}{q}$



- vjerojatnost imitirajućeg napada: $\frac{1}{q}$
- vjerojatnost napada supstitucijom: $\frac{1}{q}$

Teorem

Ukoliko MAC ima vjerojatnosti za napad $p_i = \frac{1}{n_i}$ $(0 \leq i \leq r)$, tada $|\mathcal{K}| \geq n_0 \cdots n_r$.



- vjerojatnost imitirajućeg napada: $\frac{1}{q}$
- vjerojatnost napada supstitucijom: $\frac{1}{q}$

Teorem

Ukoliko MAC ima vjerojatnosti za napad $p_i = \frac{1}{n_i}$ $(0 \leq i \leq r)$, tada $|\mathcal{K}| \geq n_0 \cdots n_r$.

Definicija

MAC za čije parametre se postiže jednakost $|\mathcal{K}| = n_0 \cdots n_r$ se naziva **savršeni MAC**.

Defincija

Generalizirani dualni luk $\mathcal{D}$ u $PG(n, q)$ reda l s dimenzijama $d_1 > d_2 > \ldots > d_{l+1}$ je skup potprostora dimenzije d_1 tako da vrijedi:

1. presjek j potprostora je potprostor dimenzije d_j, $1 \leq j \leq l+1$,
2. $l+2$ potprostora nemaju zajednički presjek.

$(n, d_1, \ldots, d_{l+1})$ nazivamo **parametrima** dualnog luka.

Teorem

Neka je π hiperravnina u $PG(n+1,q)$ i $\mathcal{D}$ generalizirani dualni luk reda l u π s parametrima $(n, d_1, \ldots, d_{l+1})$.
Neka su elementi od $\mathcal{D}$ poruke, a ključevi točke iz $PG(n+1,q)$ koje se ne nalaze u π. Autentifikacijska oznaka određena porukom i ključem je pripadni (d_1+1)-dimenzionalni potprostor.
Na navedeni način definiran je savršeni MAC pri čemu je:

$$p_i = q^{d_{i+1}-d_i}$$