Minimális kódok

Egyéni kutatómunka beszámoló

Pituk Sára

Eötvös Loránd Tudományegyetem
Természettudományi Kar

Témavezető: Kiss György

2021. május 21.

Lineáris kódok

Definíció

Egy $\mathcal{C} \subseteq GF(q)^n$ halmazt lineáris $[n, k, d]_q$-kódnak nevezünk, ha $\mathcal{C}$ a $GF(q)^n$ vektortér egy k-dimenziós lineáris altere, és bármely két $\mathcal{C}$-beli vektor (kódszó) legalább d koordinátában különbözik egymástól.

- d: minimális távolság $\rightarrow$ hibajavítás
- Generátormátrix: $k \times n$-es mátrix, melynek sorai az altér egy bázisának az elemei
- Paritásellenőrző mátrix: $\mathcal{C}$ *duális kódjának* a generátormátrixa

$$c \in \mathcal{C} \Leftrightarrow c \cdot A^T = 0.$$

Lineáris kódok

Definíció

Egy $\mathcal{C} \subseteq GF(q)^n$ halmazt lineáris $[n, k, d]_q$-kódnak nevezünk, ha $\mathcal{C}$ a $GF(q)^n$ vektortér egy k-dimenziós lineáris altere, és bármely két $\mathcal{C}$-beli vektor (kódszó) legalább d koordinátában különbözik egymástól.

- d: minimális távolság $\rightarrow$ hibajavítás
- Generátormátrix: $k \times n$-es mátrix, melynek sorai az altér egy bázisának az elemei
- Paritásellenőrző mátrix: $\mathcal{C}$ *duális kódjának* a generátormátrixa

$$c \in \mathcal{C} \Leftrightarrow c \cdot A^T = 0.$$

Lineáris kódok

Definíció

Egy $\mathcal{C} \subseteq GF(q)^n$ halmazt lineáris $[n, k, d]_q$-kódnak nevezünk, ha $\mathcal{C}$ a $GF(q)^n$ vektortér egy k-dimenziós lineáris altere, és bármely két $\mathcal{C}$-beli vektor (kódszó) legalább d koordinátában különbözik egymástól.

- d: minimális távolság $\rightarrow$ hibajavítás
- Generátormátrix: $k \times n$-es mátrix, melynek sorai az altér egy bázisának az elemei
- Paritásellenőrző mátrix: $\mathcal{C}$ *duális kódjának* a generátormátrixa

$$c \in \mathcal{C} \Leftrightarrow c \cdot A^T = 0.$$

Lineáris kódok

Definíció

Egy $\mathcal{C} \subseteq GF(q)^n$ halmazt lineáris $[n, k, d]_q$-kódnak nevezünk, ha $\mathcal{C}$ a $GF(q)^n$ vektortér egy k-dimenziós lineáris altere, és bármely két $\mathcal{C}$-beli vektor (kódszó) legalább d koordinátában különbözik egymástól.

- d: minimális távolság $\rightarrow$ hibajavítás
- Generátormátrix: $k \times n$-es mátrix, melynek sorai az altér egy bázisának az elemei
- Paritásellenőrző mátrix: $\mathcal{C}$ *duális kódjának* a generátormátrixa

$$c \in \mathcal{C} \Leftrightarrow c \cdot A^T = 0.$$

Minimális lineáris kódok

Definíció

A $c \in \mathcal{C}$ kódszó tartója a nem nulla koordinátapozícióinak halmaza:

$$Supp(c) = \{i \in [n] \colon c_i \neq 0\}.$$

Definíció

A $c \in \mathcal{C}$ kódszó minimális, ha minden $d \in \mathcal{C}$ kódszóra teljesül, hogy

$$Supp(c) \subseteq Supp(d) \Rightarrow \exists \lambda \in GF(q) \colon d = \lambda c.$$

A $\mathcal{C}$ kód minimális, ha minden nemnulla kódszó minimális benne.

Minimális lineáris kódok

Definíció

A $c \in \mathcal{C}$ kódszó tartója a nem nulla koordinátapozícióinak halmaza:

$$Supp(c) = \{i \in [n] \colon c_i \neq 0\}.$$

Definíció

A $c \in \mathcal{C}$ kódszó minimális, ha minden $d \in \mathcal{C}$ kódszóra teljesül, hogy

$$Supp(c) \subseteq Supp(d) \Rightarrow \exists \lambda \in GF(q) \colon d = \lambda c.$$

A $\mathcal{C}$ kód minimális, ha minden nemnulla kódszó minimális benne.

Massey titokmegosztási sémája

- J. L. Massey. “Minimal codewords and secret sharing.” *Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory* (1993), 33–47. old.

Minimális kódok tulajdonságai

Tétel (Alfarano, Borello, Neri, Ravagnani, 2021+)

Legyen $\mathcal{C}$ egy minimális $[n, k, d]_q$-kód. Ekkor $n \geq (k-1)(q+1)$.

Tétel (Alfarano, Borello, Neri, Ravagnani, 2021+)

Egy $\mathcal{C}$ lineáris $[n, k, d]_q$-kódban minden minimális kódszó súlya legalább $(k-1)(q-1)+1$. Speciálisan ha $\mathcal{C}$ minimális, akkor $d \geq (k-1)(q-1)+1$.

Minimális kódok tulajdonságai

Tétel (Alfarano, Borello, Neri, Ravagnani, 2021+)

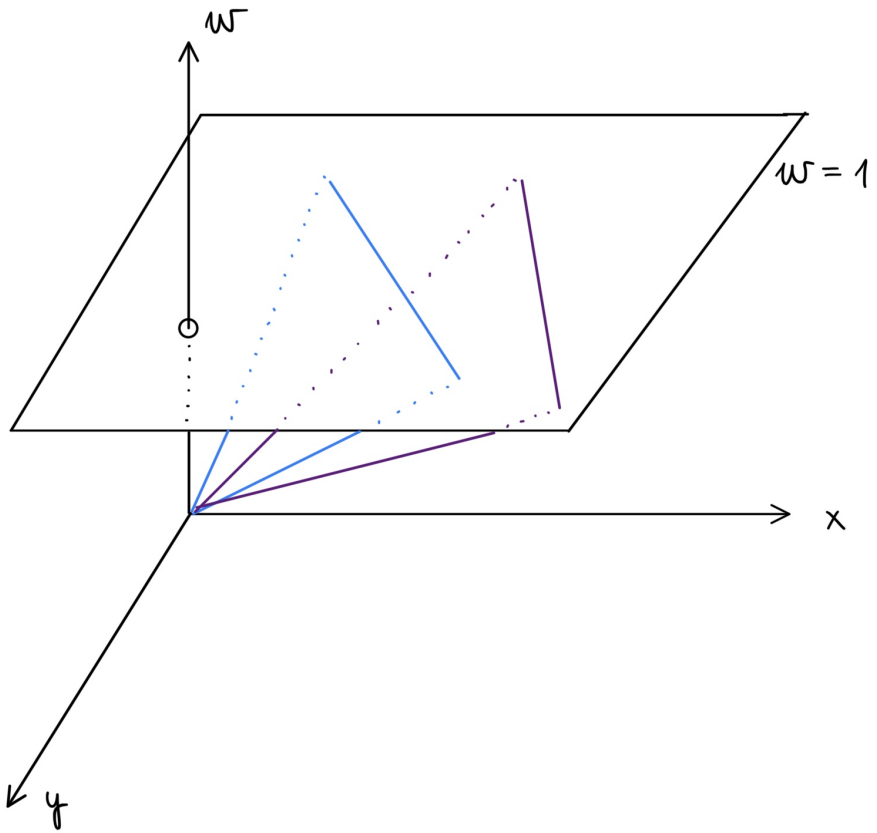
Legyen $\mathcal{C}$ egy minimális $[n, k, d]_q$-kód. Ekkor $n \geq (k-1)(q+1)$.

Tétel (Alfarano, Borello, Neri, Ravagnani, 2021+)

Egy $\mathcal{C}$ lineáris $[n, k, d]_q$-kódban minden minimális kódszó súlya legalább $(k-1)(q-1)+1$. Speciálisan ha $\mathcal{C}$ minimális, akkor $d \geq (k-1)(q-1)+1$.

A $PG(N,q)$ tér

- $PG(N,q)$ pontjai $\leftrightarrow$ $GF(q)^{N+1}$ 1-dimenziós alterei
- $PG(N,q)$ k-dimenziós projektív alterei $\leftrightarrow$ $GF(q)^{N+1}$ $(k+1)$-dimenziós lineáris alterei



Minimális kódok geometriai jellemzése

- $\mathcal{C}$ lineáris $[n, k, d]_q$-kód generátormátrixának oszlopai: n darab k hosszú vektor
- tegyük fel, hogy nincs csupa 0 oszlop
- ha egy oszlopot skalárral szorzunk, az eredetivel ekvivalens kódot kapunk
- $\rightarrow n$ darab pont $PG(k-1, q)$-ban: $\mathcal{P} = \{P_1, \ldots, P_n\}$
- $c \neq 0$ kódszó: $c = uG, u \in GF(q)^k \rightarrow U$ hipersík koordinátavektora
- $P_i \in U \Leftrightarrow c_i = 0$
- C minimális $\Leftrightarrow \nexists U \neq V$ hipersík: $\mathcal{P} \cap U \subseteq \mathcal{P} \cap V \Leftrightarrow \forall U$ hipersíkra $\langle \mathcal{P} \cap U \rangle = U$

Minimális kódok geometriai jellemzése

- $\mathcal{C}$ lineáris $[n, k, d]_q$-kód generátormátrixának oszlopai: n darab k hosszú vektor
- tegyük fel, hogy nincs csupa 0 oszlop
- ha egy oszlopot skalárral szorzunk, az eredetivel ekvivalens kódot kapunk
- $\rightarrow n$ darab pont $PG(k-1, q)$-ban: $\mathcal{P} = \{P_1, \ldots, P_n\}$
- $c \neq 0$ kódszó: $c = uG, u \in GF(q)^k \rightarrow U$ hipersík koordinátavektora
- $P_i \in U \Leftrightarrow c_i = 0$
- C minimális $\Leftrightarrow \nexists U \neq V$ hipersík: $\mathcal{P} \cap U \subseteq \mathcal{P} \cap V \Leftrightarrow \forall U$ hipersíkra $\langle \mathcal{P} \cap U \rangle = U$

Minimális kódok geometriai jellemzése

- $\mathcal{C}$ lineáris $[n, k, d]_q$-kód generátormátrixának oszlopai: n darab k hosszú vektor
- tegyük fel, hogy nincs csupa 0 oszlop
- ha egy oszlopot skalárral szorzunk, az eredetivel ekvivalens kódot kapunk
- $\rightarrow n$ darab pont $PG(k-1, q)$-ban: $\mathcal{P} = \{P_1, \ldots, P_n\}$
- $c \neq 0$ kódszó: $c = uG, u \in GF(q)^k \rightarrow U$ hipersík koordinátavektora
- $P_i \in U \Leftrightarrow c_i = 0$
- C minimális $\Leftrightarrow \nexists U \neq V$ hipersík: $\mathcal{P} \cap U \subseteq \mathcal{P} \cap V \Leftrightarrow \forall U$ hipersíkra $\langle \mathcal{P} \cap U \rangle = U$

Minimális kódok geometriai jellemzése

- $\mathcal{C}$ lineáris $[n, k, d]_q$-kód generátormátrixának oszlopai: n darab k hosszú vektor
- tegyük fel, hogy nincs csupa 0 oszlop
- ha egy oszlopot skalárral szorzunk, az eredetivel ekvivalens kódot kapunk
- $\rightarrow n$ darab pont $PG(k-1, q)$-ban: $\mathcal{P} = \{P_1, \ldots, P_n\}$
- $c \neq 0$ kódszó: $c = uG, u \in GF(q)^k \rightarrow U$ hipersík koordinátavektora
- $P_i \in U \Leftrightarrow c_i = 0$
- C minimális $\Leftrightarrow \nexists U \neq V$ hipersík: $\mathcal{P} \cap U \subseteq \mathcal{P} \cap V \Leftrightarrow \forall U$ hipersíkra $\langle \mathcal{P} \cap U \rangle = U$

Minimális kódok geometriai jellemzése

- $\mathcal{C}$ lineáris $[n, k, d]_q$-kód generátormátrixának oszlopai: n darab k hosszú vektor
- tegyük fel, hogy nincs csupa 0 oszlop
- ha egy oszlopot skalárral szorzunk, az eredetivel ekvivalens kódot kapunk
- $\rightarrow n$ darab pont $PG(k-1, q)$-ban: $\mathcal{P} = \{P_1, \ldots, P_n\}$
- $c \neq 0$ kódszó: $c = uG, u \in GF(q)^k \rightarrow U$ hipersík koordinátavektora
- $P_i \in U \Leftrightarrow c_i = 0$
- C minimális $\Leftrightarrow \nexists U \neq V$ hipersík: $\mathcal{P} \cap U \subseteq \mathcal{P} \cap V \Leftrightarrow \forall U$ hipersíkra $\langle \mathcal{P} \cap U \rangle = U$

Minimális kódok geometriai jellemzése

- $\mathcal{C}$ lineáris $[n, k, d]_q$-kód generátormátrixának oszlopai: n darab k hosszú vektor
- tegyük fel, hogy nincs csupa 0 oszlop
- ha egy oszlopot skalárral szorzunk, az eredetivel ekvivalens kódot kapunk
- $\rightarrow n$ darab pont $PG(k-1, q)$-ban: $\mathcal{P} = \{P_1, \ldots, P_n\}$
- $c \neq 0$ kódszó: $c = uG, u \in GF(q)^k \rightarrow U$ hipersík koordinátavektora
- $P_i \in U \Leftrightarrow c_i = 0$
- C minimális $\Leftrightarrow \nexists U \neq V$ hipersík: $\mathcal{P} \cap U \subseteq \mathcal{P} \cap V \Leftrightarrow \forall U$ hipersíkra $\langle \mathcal{P} \cap U \rangle = U$

Erősen lefogó ponthalmazok

Definíció

Az $S \subseteq PG(k-1,q)$ ponthalmaz t-szeresen lefogó, ha minden hipersíkot legalább t pontban metsz.

Definíció

Egy $S \subseteq PG(k-1,q)$ ponthalmaz erősen lefogó, ha minden hipersíkot generátorrendszerben metsz.

$PG(k-1,q)$-ban egy erősen lefogó ponthalmaz mérete legalább $(k-1)(q+1)$.

Erősen lefogó ponthalmazok

Definíció

Az $S \subseteq PG(k-1,q)$ ponthalmaz t-szeresen lefogó, ha minden hipersíkot legalább t pontban metsz.

Definíció

Egy $S \subseteq PG(k-1,q)$ ponthalmaz erősen lefogó, ha minden hipersíkot generátorrendszerben metsz.

$PG(k-1,q)$-ban egy erősen lefogó ponthalmaz mérete legalább $(k-1)(q+1)$.

Erősen lefogó ponthalmazok

Definíció

Az $S \subseteq PG(k-1,q)$ ponthalmaz t-szeresen lefogó, ha minden hipersíkot legalább t pontban metsz.

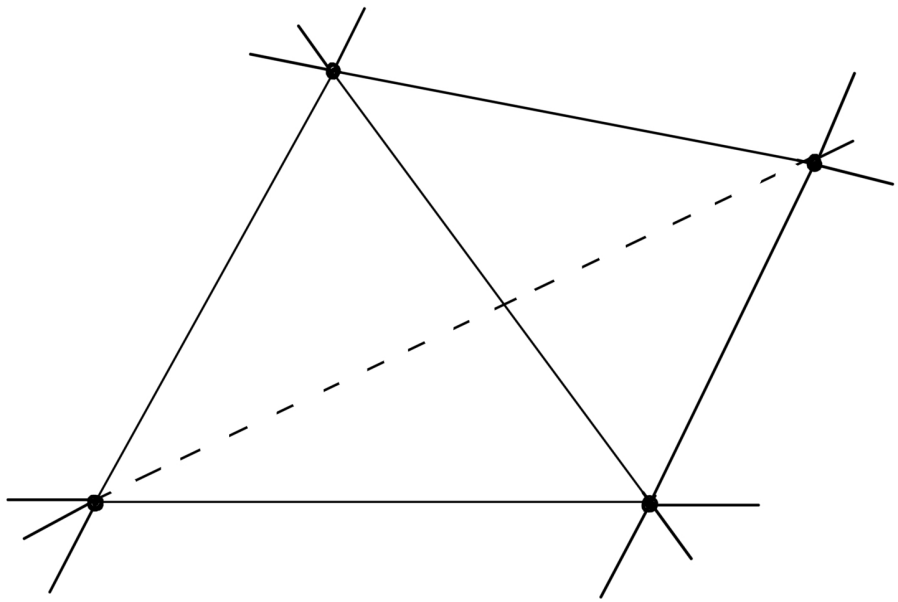
Definíció

Egy $S \subseteq PG(k-1,q)$ ponthalmaz erősen lefogó, ha minden hipersíkot generátorrendszerben metsz.

$PG(k-1,q)$-ban egy erősen lefogó ponthalmaz mérete legalább $(k-1)(q+1)$.

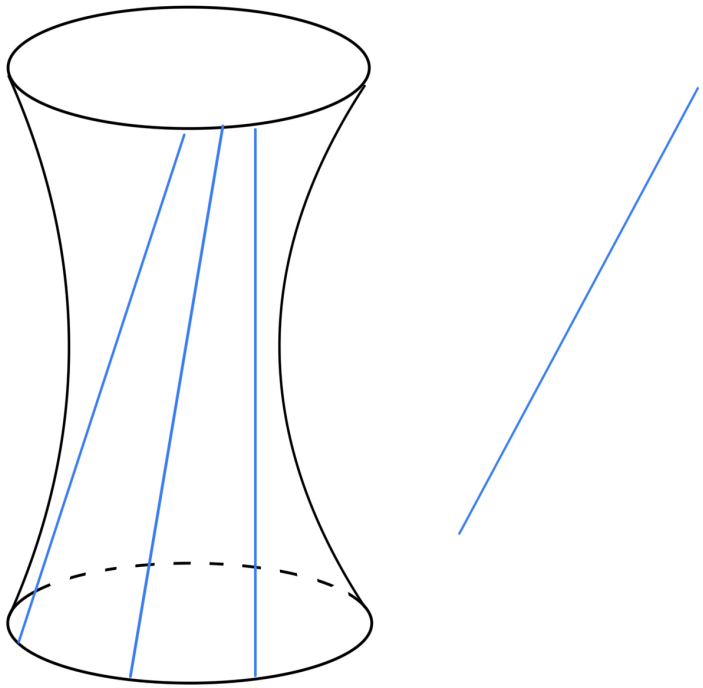
Példák erősen lefogó ponthalmazra I

- Szimplex: $PG(k-1)$-ben k általános helyzetű pont, ezek páronkénti összekötő egyenesei $\rightarrow \binom{k}{2}(q-1)+k$ pont



Példák erősen lefogó ponthalmazra I

- Szimplex: $PG(k-1)$-ben k általános helyzetű pont, ezek páronkénti összekötő egyenesei $\rightarrow \binom{k}{2}(q-1)+k$ pont
- $PG(3,q)$-ban három kitérő egyenes: ℓ_1, ℓ_2, ℓ_3, és egy negyedik, aminek nincs közös pontja az első három által generált hiperbolikus kvádrikával



Példák erősen lefogó ponthalmazra I

- Szimplex: $PG(k-1)$-ben k általános helyzetű pont, ezek páronkénti összekötő egyenesei $\rightarrow \binom{k}{2}(q-1)+k$ pont
- $PG(3,q)$-ban három kitérő egyenes: ℓ_1, ℓ_2, ℓ_3, és egy negyedik, aminek nincs közös pontja az első három által generált hiperbolikus kvádrikával
- Fancsali, Sziklai, 2014: ha $q \geq 2k-3$ és char$(GF(q)) \geq k-1$, akkor a momentumgörbe $2k-3$ különböző érintője $\rightarrow (2k-3)(q+1)$ pont
- Bartoli, Kiss, Marcugini, Pambianco, 2020: $PG(4,q)$-ban hat egyenes, ha $q > 36086 \rightarrow 6(q+1)$ pont

Példák erősen lefogó ponthalmazra I

- Szimplex: $PG(k-1)$-ben k általános helyzetű pont, ezek páronkénti összekötő egyenesei $\to \binom{k}{2}(q-1)+k$ pont
- $PG(3,q)$-ban három kitérő egyenes: ℓ_1, ℓ_2, ℓ_3, és egy negyedik, aminek nincs közös pontja az első három által generált hiperbolikus kvádrikával
- Fancsali, Sziklai, 2014: ha $q \geq 2k-3$ és char$(GF(q)) \geq k-1$, akkor a momentumgörbe $2k-3$ különböző érintője $\to (2k-3)(q+1)$ pont
- Bartoli, Kiss, Marcugini, Pambianco, 2020: $PG(4,q)$-ban hat egyenes, ha $q > 36086 \to 6(q+1)$ pont

Példák erősen lefogó ponthalmazra II

- Bartoli, Cossidente, Marino, Pavese, 2021+: $PG(5,q)$-ban hét egyenes

  $PG(3,q^3)$-ban három diszjunkt q-adrendű résztér $\to 3(q+1)(q^2+1)$ pont

Tétel (Héger, Nagy, 2021+)

$PG(k-1,q)$-ban létezik

$$m = \begin{cases} \left\lceil \frac{2}{1+\frac{1}{\ln(q)(q+1)^2}}(k-1) \right\rceil, & \text{ha } q > 2, \\ \lceil 1.95(k-1) \rceil, & \text{ha } q = 2 \end{cases}$$

egyenes, amelyek uniója erősen lefogó ponthalmazt alkot.

Példák erősen lefogó ponthalmazra II

- Bartoli, Cossidente, Marino, Pavese, 2021+: $PG(5,q)$-ban hét egyenes
  $PG(3,q^3)$-ban három diszjunkt q-adrendű résztér
  $\to 3(q+1)(q^2+1)$ pont

Tétel (Héger, Nagy, 2021+)

$PG(k-1,q)$-ban létezik

$$m = \begin{cases} \left\lceil \frac{2}{1+\frac{1}{\ln(q)(q+1)^2}}(k-1) \right\rceil, & \text{ha } q > 2, \\ \lceil 1.95(k-1) \rceil, & \text{ha } q = 2 \end{cases}$$

egyenes, amelyek uniója erősen lefogó ponthalmazt alkot.

Példák erősen lefogó ponthalmazra II

- Bartoli, Cossidente, Marino, Pavese, 2021+: $PG(5,q)$-ban hét egyenes
  $PG(3,q^3)$-ban három diszjunkt q-adrendű résztér
  $\to 3(q+1)(q^2+1)$ pont

Tétel (Héger, Nagy, 2021+)

$PG(k-1,q)$-ban létezik

$$m = \begin{cases} \left\lceil \frac{2}{1+\frac{1}{\ln(q)(q+1)^2}}(k-1) \right\rceil, & \text{ha } q > 2, \\ \lceil 1.95(k-1) \rceil, & \text{ha } q = 2 \end{cases}$$

egyenes, amelyek uniója erősen lefogó ponthalmazt alkot.

Köszönöm a figyelmet!