Minimális kódok
Egyéni kutatómunka beszámoló

Szerző: Pituk Sára
Témavezető: Kiss György

2021. május 13.

1. Bevezetés

A minimális lineáris kódok napjainkban aktív kutatás tárgyát képezik. Különböző kriptográfiai alkalmazásaik miatt gyakorlati szempontból is fontosak. Ezen kívül érdekes a véges geometriához fűződő kapcsolatuk is, mert olyan véges projektív térbeli ponthalmazoknak feleltethetők meg, amiket előtte már ettől függetlenül is vizsgáltak.
A félév során ehhez a témához kapcsolódó szakirodalmat dolgoztuk fel, valamint kapcsolódó kérdéseken gondolkoztunk. Ezek közül néhányra negatív választ találtunk (vagyis nem lehetséges az általunk elképzelt konstrukciót megvalósítani), másokat pedig a kutatómunka folytatásaként szeretnénk tovább vizsgálni.

2. Minimális kódok

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. A d paramétert a $\mathcal{C}$ *minimális távolságának* nevezzük. Ez a kód hibajavító képességével van összefüggésben: minél több koordinátában térnek el egymástól a kódszavak, annál több bitnek kell megsérülnie a küldés során ahhoz, hogy a fogadó ne tudja egyértelműen kitalálni az eredeti kódszót.
Egy $[n,k,d]_q$-kódot többféleképpen meg tudunk adni. Az egyik lehetőség a *generátormátrixszal* történő megadás. Ez egy $k \times n$-es mátrix, melynek sorait az altér egy bázisának az elemei alkotják. A másik lehetőség, hogy megadunk egy olyan $(n-k) \times n$-es A mátrixot, amire teljesül, hogy $c \in \mathcal{C} \Leftrightarrow c \cdot A^T = 0$. Ez az A mátrix tulajdonképpen $\mathcal{C}$ *duális kódjának* a generátormátrixa, vagyis annak a $\mathcal{C}^\perp$ $[n, n-k, d']_q$-kódnak, ami $\mathcal{C}$ ortogonális kiegészítő altere $GF(q)^n$-ben. Ebben az esetben A-t a $\mathcal{C}$ kód *paritásellenőrző mátrixának* hívjuk.

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

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

A $|Supp(c)|$ értéket a c kódszó *súlyának* is szokás nevezni. Ismert, hogy egy lineáris kódban a legkisebb súlyú nemnulla kódszó súlya megegyezik a kód minimális távolságával.

2.2. 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.*

2.3. Definíció. *A $\mathcal{C}$ kód* nemdegenerált*, ha nincs olyan i koordinátapozíció, hogy minden $c \in \mathcal{C}$-re $c_i = 0$.*

2.4. Definíció. *Két lineáris kód* ekvivalens*, ha az egyikből a másik megkapható a következő két lépés véges sok alkalmazásával:*

- *Két koordinátát megcserélünk az összes kódszóban.*
- *Valamelyik koordinátát megszorozzuk ugyanazzal a $GF(q)$-beli nemnulla elemmel az összes kódszóban.*

3. Kriptográfiai alkalmazások

A minimális kódszavakat először Massey definiálta [Mas93] cikkében egy titokmegosztási séma kapcsán. Ez pedig a következő: Tegyük fel, hogy a titok egy $s \in GF(q)$ elem, amit n játékos között szeretnénk valahogy szétosztani. Ez azt jelenti, hogy minden játékosnak adunk egy kis darab információt, úgy, hogy a játékosok bizonyos részhalmazai az információikat összerakva meg tudják határozni s-et (ekkor ők *kvalifikált részhalmazt* alkotnak), más részhalmazok viszont ne. Világos, hogy a kvalifikált részhalmazok felszálló halmazrendszert alkotnak, ezért egy sémában az az érdekes, hogy mik a minimális kvalifikált részhalmazok.
Legyen $\mathcal{C}$ egy lineáris $[n+1, k, d]_q$-kód, és legyen G a generátormátrixa. Legyenek G oszlopai $G_0, G_1, \ldots, G_n$. Tegyük fel, hogy nincs köztük csupa nullából álló oszlop, vagyis $\mathcal{C}$ nemdegenerált. Válasszunk egy véletlen u vektort $GF(q)^k$-ból, amelyre $u \cdot G_0 = s$, majd számoljuk ki az $uG = (s, v_1, v_2, \ldots v_n)$ vektort. Ezután adjuk az i-edik játékosnak a $v_i \in GF(q)$ elemet. Belátható, hogy a játékosok egy $\{i_1, i_2, \ldots, i_m\}$ részhalmaza pontosan akkor tudja megfejteni s-et, ha G_1 előáll a $G_{i_1}, G_{i_2}, \ldots, G_{i_m}$ oszlopok lineáris kombinációjaként. Ebből következik, hogy a játékosok minimális kvalifikált részhalmazai megfeleltethetők a $\mathcal{C}^\perp$ duális kód azon minimális kódszavainak, amelyekben az első koordináta helyén 1 áll.
Általában nehéz meghatározni egy lineáris kód minimális kódszavait. Ezért megkönnyíti a helyzetet, ha olyan kódot használunk, amiben minden kódszó eleve minimális.
[CCP14]-ben találunk egy másik alkalmazást: Ebben a szerzők minimális kódokat felhasználva adtak egy olyan protokollt, aminek a segítségével egy kétszemélyes kommunikációs játékban a játékosok úgy tudják kiszámolni a célfüggvényt, hogy közben semmit nem tudnak meg a másik inputjáról. (A kétszemélyes kommunikációs játékban adott egy f függvény, és két játékos. Aliznál az x, Bobnál az y input van, és a céljuk közösen kiszámolni $f(x, y)$-t. Előfordulhat, hogy szeretnék titokban tartani a saját inputjukat. Erre egy példa, amikor Aliz és Bob két milliárdos, akik azt akarják eldönteni, melyikük gazdagabb, de nem akarják elárulni, mennyi pénzük van.)

4. Minimális kódok tulajdonságai

Vegyük észre, hogy ha $\mathcal{C}$ minimális, akkor a $\{Supp(c) \colon 0 \neq c \in \mathcal{C}\} \subset 2^{[n]}$ halmazrendszer tartalmazásmentes, vagyis Sperner tétele szerint legfeljebb $\binom{n}{\lfloor n/2 \rfloor}$ halmazból állhat. Így rögtön kapunk is egy felső becslést a kód méretére:

$$|C| = q^k \leq 1 + (q-1)\binom{n}{\lfloor n/2 \rfloor},$$

amiből n-re kapunk egy $(k-1)\log_2(q)$ nagyságrendű alsó korlátot. Ennél erősebb eredmény is ismert az irodalomban:

4.1. Tétel ([Alf+20]). *Legyen $\mathcal{C}$ egy minimális $[n,k,d]_q$-kód. Ekkor $n \geq (k-1)(q+1)$.*

Arra a kérdésre, hogy ez a korlát mennyire éles, még visszatérünk.
A minimális kódok minimális távolságáról pedig az alábbi mondható:

4.2. Tétel ([Alf+20]). *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 következő tételre Ashikhmin-Barg feltételként szoktak hivatkozni.

4.3. Tétel ([AB98]). *Legyen $\mathcal{C}$ egy lineáris $[n,k,d]_q$-kód. Jelölje w_{max} és w_{min} a maximális, illetve a minimális súlyú nemnulla kódszavak súlyát $\mathcal{C}$-ben. Ha*

$$\frac{w_{max}}{w_{min}} < \frac{q}{q-1},$$

akkor $\mathcal{C}$ minimális.

Több konstrukció mutatja, hogy ez a feltétel csupán elégséges, de nem szükséges.
Egy egyszerű szükséges feltételt a következőképpen kaphatunk. Mivel $\mathcal{C}$ egy lineáris altér, bármely két kódszó összege is kódszó. Ezért a két kódszó tartója nem lehet diszjunkt, különben az összeg tartója tartalmazná mindkettőét.

4.4. Definíció. *Egy $\mathcal{C}$ lineáris kód* metsző*, ha bármely $c,d \in \mathcal{C}$ nemnulla kódszavak esetén $Supp(c) \cap Supp(d) \neq \emptyset$.*

Tehát a minimális kódok egyúttal metsző kódok is. Ha $q=2$, akkor ennek a megfordítása is igaz: Bináris esetben a kódszavak tartói meghatározzák a kódszavakat. Ha lenne $c \neq 0$ és $d \neq 0$, amire $Supp(c) \subset Supp(d)$, akkor $Supp(c+d) = Supp(d) \backslash Supp(c)$ nem metszené $Supp(c)$-t. Azonban ha $q > 2$, akkor általában nem igaz a megfordítás, ezt mutatja az alábbi állítás.

4.5. Állítás ([CMP13]). *Legyen $k \geq 2$. Egy $\mathcal{C}$ minimális $[n,k,d]_q$-kód bármely két c és d elemére $|Supp(c) \cap Supp(d)| \geq q-1$.*

Azonban még ez sem elég a minimalitáshoz, ahogy azt az 5.4. Példa fogja mutatni.

5. Geometriai jellemzés

Tegyük fel, hogy a $\mathcal{C}$ lineáris $[n,k,d]_q$-kód *nemdegenerált*, és tekintsük $\mathcal{C}$ generátormátrixát, ami egy $k \times n$-es mátrix. Ha egy oszlopot valamilyen $GF(q)$-beli skalárral szorzunk, akkor az eredetivel ekvivalens kódot határoz meg a mátrix, tehát az oszlopok csak skalárszoros erejéig számítanak. Ebből a megfigyelésből kiindulva tekinthetünk a mátrix oszlopaira úgy, mint n darab $PG(k-1,q)$-beli pont homogén koordinátavektorára. Ezek halmaza legyen $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$. (Mivel nincs csupa 0 oszlop, ezek a pontok valóban $PG(k-1,q)$-ban vannak.)
Minden nemnulla kódszó $c = uG$ alakban áll elő valamilyen $0 \neq u \in GF(q)^k$ vektor mellett. Ezekre az u vektorokra egy-egy hipersík koordinátavektoraként gondolhatunk. Az u-nak megfelelő hipersík pontosan akkor tartalmazza a G i-edik oszlopának megfelelő pontot, ha $c = uG$-ben az i-edik koordináta 0. Ezek szerint azt a feltételt, hogy nincs olyan c és d nemnulla kódszó, amelyek nem egymás skalárszorosai és $Supp(c) \subseteq Supp(d)$ (vagy ezzel ekvivalensen $\overline{Supp(d)} \subseteq \overline{Supp(c)}$), átfogalmazhatjuk úgy, hogy nincs két olyan U és V hipersík, hogy $\mathcal{P} \cap U \subseteq \mathcal{P} \cap V$. Ez pedig könnyen láthatóan pontosan akkor teljesül, ha minden U hipersíkra $\langle \mathcal{P} \cap U \rangle = U$. Ilyen tulajdonságú ponthalmazokat mint speciális többszörösen lefogó ponthalmazokat már a minimális kódokkal való kapcsolat felfedezése előtt többen is vizsgáltak.

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

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

Eszerint az erősen lefogó ponthalmazok valóban speciális $(k-1)$-szeresen lefogó ponthalmazok. $PG(2,q)$-ban pedig éppen egybeesnek a 2-szeresen lefogó halmazokkal.
Most térjünk vissza arra a kérdésre, hogy mit mondhatunk a 4.1. Tételbeli korlát élességéről. A $(k-1)$-szeresen lefogó ponthalmazokra vonatkozó korábbi eredményeket felhasználva a [Alf+20] cikk szerzői megmutatták, hogy $4 \leq k \leq \sqrt{q}+2$ esetén sosem éles a korlát, és ha $k=3$, akkor pontosan $q=2$ mellett éles. (Ezekben az esetekben karakterizálva vannak a $(k-1)$-szeresen lefogó ponthalmazok.) Tudomásunk szerint jelenleg nem ismert olyan kódcsalád, ami minden k-ra és q-ra létezik, és a hossza mindkét paraméternek lineáris függvénye. Azonban nem konstruktív eszközökkel igazolható ilyeneknek a létezése, erről később még teszünk említést. A legáltalánosabb ismert ilyen konstrukció [FS14]-ben található, ami $q \geq 2k-3$ esetén minimális $[(2k-3)(q+1), k, d]_q$-kódokat ad meg. Ennek a hátránya, hogy a kódelméletben szokásos megközelítés szerint általában q (az ábécé elemszáma) kicsi, és rögzített q mellett szeretnénk tetszőleges dimenziójú kódokat konstruálni.
A minimalitási feltételhez hasonlóan azt is átfogalmazhatjuk a geometria nyelvére, hogy egy kód metsző. Ez pontosan akkor teljesül, ha a generátormátrix oszlopai által meghatározott $PG(k-1,q)$-beli pontok nem fedhetők le két hipersíkkal. Az a feltétel pedig, hogy bármely két nemnulla kódszó tartójának a metszete legalább $q-1$ elemű, annak felel meg, hogy bármely két hipersík unióján kívül esik legalább $q-1$ pont. Így adhatunk egy új, az eredetinél egyszerűbb bizonyítást a 4.5. Állításra:

5.3. Állítás. *Tegyük fel, hogy adott egy S erősen lefogó ponthalmaz $PG(k-1,q)$-ban. Ekkor bármely két hipersík unióján kívül esik legalább $q-1$ pontja S-nek.*

Bizonyítás. Vegyünk két tetszőleges hipersíkot, U-t és V-t, és tekintsük a metszetüket, ami egy 2-kodimenziós W altér. Ezen összesen $q+1$ hipersík megy keresztül, ami között ott van U és V. Mivel a maradék $q-1$ is generálva van, mindegyiken van W-n kívül még legalább egy pontja S-nek, és mivel csak W-ben metszi egymást ez a $q-1$ hipersík, ezek a pontok páronként különbözők. □

Az is könnyen látható így, hogy $q=2$-re a visszafele irány is igaz: Ha az S halmazt semelyik két hipersík nem fedi, és U tetszőleges hipersík, akkor nem eshet az $U \cap S$ minden pontja egy W 2-kodimenziós altérre. Ha ez lenne a helyzet, akkor ugyanis a W-n átmenő U-tól különböző két hipersíkon kívül nem lenne S-beli pont.

5.4. Példa. *Az 5.3. Állítás feltétele nem elég ahhoz, hogy S erősen lefogó legyen, ha $q>2$. Álljon ugyanis S három hipersíkból, amelyek egy W 2-kodimenziós altérben metszik egymást. Ekkor bármely két hipersík uniójából kimarad $(q-1)$-nél több S-beli pont. Viszont ha veszünk egy negyedik hipersíkot W-n át (ami létezik, ha $q>2$), azt S csak W-ben metszi, vagyis nem generálja.*

6. Kesze-kusza egyenesek

Most tehát átfogalmaztuk az eredeti problémát egy véges projektív térbeli kérdéssé: Mi az a minimális n szám, amire létezik $PG(k-1,q)$-ban n pontú erősen lefogó halmaz? Mivel az egyenesek rendelkeznek azzal a tulajdonsággal, hogy minden hipersíkot metszenek, jó ötletnek tűnhet egyenesek uniójaként keresni ilyen halmazokat. Ha néhány egyenes pontjainak uniója erősen lefogó halmazt alkot, akkor az egyenesek halmazát *kesze-kuszának* is szokás nevezni.
Kezdjük egy egyszerű konstrukcióval, ami minden q és k esetén működik: Vegyünk $PG(k-1,q)$-ban

k általános helyzetű pontot, és ezek páronkénti összekötő egyeneseit. Így egy $\binom{k}{2}(q-1)+k$ pontú erősen lefogó halmazt kapunk. Ennek az elnevezése az irodalomban *tetraéder*, bár a *szimplex* név találóbb lenne rá. [Alf+20]-ban található olyan konstrukció, ami szintén minden q és k esetén alkalmazható, és a tetraédernél konstans szorzóval kevesebb pontból áll. (A konstans $\frac{1}{2}$ vagy $\frac{4}{9}$, esettől függően.)

$PG(2,q)$-ban két egyenes nem lehet elég, így akkor a tetraéder konstrukció optimális.

$PG(3,q)$-ban viszont hatnál kevesebb egyenest is meg tudunk adni, ahogy az például [FS14]-ben szerepel: Vegyünk először három kitérő egyenest. Ezek meghatároznak egy (egyértelmű) hiperbolikus kvádrikát. Tudjuk, hogy egy sík a kvádrikát vagy egy kúpszeletben, vagy egy metsző egyenespárban metszi. Az első esetben nincs baj, mert a kúpszeleten ott van a három egyenessel vett három metszéspont is, és egy kúpszelet semelyik három pontja nem eshet egy egyenesre. Az utóbbi fajta síkoknak viszont, amennyiben nem tartalmazzák a három egyenesből egyiket sem, egy egyenesre esik a három egyenessel vett metszetük; ezekkel kell már csak valamit kezdenünk. Ha veszünk egy negyedik egyenest, aminek nincs közös pontja a kvádrikával (tudjuk, hogy ilyen létezik), akkor annak az ilyen síkokkal vett metszete az első három egyenessel vett metszéspontok egyenesén kívül fog esni. Így ez a négy egyenes együtt már jó lesz.

A fenti érvelésből adódik az is, hogy három kitérő egyenes nem lehet elég, kivéve, ha $q=2$. Ebben az esetben ugyanis minden olyan sík, ami egyenespárban metszi a kvádrikát, tartalmazza valamelyik egyenest a megadott háromból. Így $PG(3,2)$-ben három kitérő egyenes mindig kesze-kusza. Ebből megállapíthatjuk, hogy $k=4, q=2$ esetén éles a 4.1. Tételbeli korlát. (Ez kívül esik a korábban említett $4 \le k \le \sqrt{q}+2$ tartományon.)

A következő eredményt már említettük korábban is:

6.1. Tétel ([FS14]). *Ha $q \ge 2k-3$, akkor $PG(k-1,q)$-ban megadható $2k-3$ páronként kitérő kesze-kusza egyenes, és így egy $(2k-3)(q+1)$ pontú erősen lefogó ponthalmaz.*

A konstrukció lényege, hogy a momentumgörbe $2k-3$ különböző érintőjét választjuk ki, és ezekről megmutatható, hogy nincs olyan 2-kodimenziós altér, ami mindegyiket metszi. Ez nyilvánvalóan egy szükséges feltétele annak, hogy az egyeneshalmaz kesze-kusza legyen, azonban ha q-nál kevesebb egyenesünk van, akkor kiderül, hogy ez elégséges is. Az érintőket akkor tudjuk így választani, ha az alaptest karakterisztikája legalább $k-1$. Viszont helyettük más, az érintőkhöz hasonló tulajdonságú egyeneseket véve kis karakterisztika esetén is működik hasonló konstrukció.

Ezek az egyenesek nem feltétlenül alkotnak minimális kesze-kusza egyeneshalmazt. Például $PG(4,11)$-ben az így kapott hét egyenesből egyet el tudunk hagyni úgy, hogy a maradék hat még mindig kesze-kusza [Bar+20a]. A következő két sporadikus példa mutatja, hogy máskor is elég lehet $(2k-3)$-nál kevesebb egyenes.

6.2. Tétel ([Bar+20b]). *$PG(4,q)$-ban megadható hat kesze-kusza egyenes, ha $q > 36086$.*

6.3. Tétel ([Bar+20a]). *$PG(5,q)$-ban megadható hét kesze-kusza egyenes.*

Ha nem is nagyon tudunk általános konstrukciókat lineáris méretű kesze-kusza egyeneshalmazokra, a létezésükre van bizonyítékunk az alábbi tételnek köszönhetően, amely véletlen módszerrel látható be.

6.4. Tétel ([HN21]). *$PG(k-1,q)$-ban létezik*

$$m = \begin{cases} \left\lceil \frac{2}{1+\frac{1}{\ln(q)(q+1)^2}}(k-1) \right\rceil, & \text{ha } q > 2, \\ \left\lceil \frac{\ln 8}{\ln 8/3}(k-1) \right\rceil, & \text{ha } q = 2 \end{cases}$$

méretű kesze-kusza egyeneshalmaz.

Itt az ötlet az, hogy véletlenül választunk legalább m egyenest, és felülről becsüljük annak a valószínűségét, hogy valamelyik hipersík nincs generálva. Belátható, hogy ez a valószínűség 1-nél kisebb, amiből következik, hogy van olyan választás, aminél mindegyik hipersík generálva van.
Az olyan erősen lefogó halmazok méretére, amelyek egyenesek uniójaként állnak elő, az alábbi alsó korlát érvényes:

6.5. Tétel ([HN21]). *$PG(k-1,q)$-ban egy kesze-kusza egyeneshalmaz legalább*

$$k-1+\left\lfloor\frac{k-1}{2}\right\rfloor-\left\lfloor\frac{k-2}{q}\right\rfloor$$

egyenest tartalmaz.

Lehet, hogy ha nem egyenesekkel próbálkozunk, akkor kisebb méretű halmazokat is meg tudunk adni. Egy másik standard konstrukció $(k-1)$-szeresen lefogó ponthalmazra $PG(k-1,q^{k-1})$-ben $k-1$ darab diszjunkt *q-rendű részgeometria* uniója. Ilyen részgeometriát kapunk akkor, ha valamilyen koordinátázás szerint pontosan a $GF(q)$-beli koordinátájú pontokat választjuk ki. Mivel ezeknek minden hipersíkon van pontja, ha ilyenből $k-1$ diszjunktat veszünk, akkor az $(k-1)$-szeresen lefogó lesz. Nyitott kérdés, hogy tudjuk-e ezeket úgy választani, hogy erősen lefogó is legyen. 3 dimenzióban erre nemrég pozitív válasz született:

6.6. Tétel ([Bar+20a]). *$PG(3,q^3)$-ben három alkalmasan választott diszjunkt q-adrendű részgeometria uniója egy $3(q+1)(q^2+1)$ pontú erősen lefogó halmazt alkot.*

Hivatkozások

[Mas93] J. L. Massey. "Minimal codewords and secret sharing." *Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory* (1993), 33–47. old.

[AB98] A. Ashikhmin és A. Barg. "Minimal vectors in linear codes". *IEEE Trans. Inf. Theory* 44.5 (1998).

[CMP13] G. D. Cohen, S. Mesnager és A. Patey. "On minimal and quasi-minimal linear codes". *IMACC 2013, LNCS* 8308 (2013). Szerk. M. Stam, 85–98. old.

[CCP14] H. Chabanne, G. D. Cohen és A. Patey. "Towards secure two-party computation from the wire-tap channel". *Information Security and Cryptology, LNCS* 8565 (2014). Szerk. H. S. Lee és D. G. Han, 34–46. old.

[FS14] Sz. L. Fancsali és P. Sziklai. "Lines in higgledy-piggledy arrangement." *Electon. J. Comb.* 21.2 (2014).

[Alf+20] G. N. Alfarano és tsai. "Three combinatorial perspectives on minimal codes." (2020). arXiv: 2010.16339.

[Bar+20a] D. Bartoli és tsai. "On cutting blocking sets and their codes". (2020). arXiv: 2011.11101.

[Bar+20b] D. Bartoli és tsai. "Resolving sets for higher dimensional projective spaces". *Finite Fields Appl.* 67.101723 (2020).

[HN21] T. Héger és Z. L. Nagy. *Short minimal codes and covering codes via strong blocking sets in projective spaces*. 2021. arXiv: 2103.07393.