PD-skupovi i antibloking sustavi

Loredana Simčić
(loredana.simcic@riteh.hr)

- **H.-J. Kroll, R. Vincenti**: Antiblocking systems and PD-sets, Discrete Math. 308 (2008) 408-414.
- **H.-J. Kroll, R. Vincenti**: Antiblocking decoding, Discrete Appl. Math. (2010)

Linearni kodovi

Definicija

Neka je q prim broj i neka je F konačno polje reda q, te neka je $n \in \mathbb{N}$. Linearan kod duljine n je linearni podprostor vektorskog prostora F^n.

Kod je binaran za $q = 2$.
Elementi koda zovu se riječi koda.

Primjer

$$C = \begin{Bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{Bmatrix}$$

Hammingova udaljenost

Neka je $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in F^n$.
Broj

$$d(x, y) = |\{i \,|\, 1 \leq i \leq n, x_i \neq y_i\}|$$

se naziva Hammingova udaljenost.

Težina riječi koda

Za $x \in F^n$, težina $w(x)$ od x je definirana sa

$$w(x) = d(x, 0) = |\{i \in \mathbb{N} |\, i \leq n,\ x_i \neq 0\}|$$

Linearni kod C duljine n se naziva $[n, k, d]$ kod ako je k dimenzija od C i $d = \min\{w(c) |\, c \in C,\ c \neq 0\}$ je minimalna težina od C.

Generirajuća matrica linearnog koda

Matrica dimenzije $k \times n$ čiji se retci sastoje od vektora baze koda $[n, k, d]$ zove se generirajuća matrica.

Primjer

$$C = \begin{Bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{Bmatrix}$$

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

Dualni kod

Skalarni produkt

Skalarni produkt vektora $x = (x_1 \dots x_n)$ i $y = (y_1 \dots y_n)$, $x, y \in F^n$ je skalar $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i \in F$.
Ako je $\langle x, y \rangle = 0$, kažemo da su x i y ortogonalni.

Dualni kod

Za linearni kod $C \subset F^n$ definiramo dualni kod $C^\perp \subset F^n$ sa

$$C^\perp = \{x \in F^n \mid (\forall y \in C)\, \langle x, y \rangle = 0\}$$

Ako je C $[n, k]$ kod, tada je $C^\perp$ $[n, n-k]$ kod.

Paritetna matrica

Neka je $C \subset F^n$ kod. Paritetna matrica za kod C je generirajuća matrica za dualni kod $C^\perp$.

Izomorfni kodovi

Ekvivalentni kodovi

Dva koda iste duljine i nad istim poljem su ekvivalentna ako se jedan može dobiti iz drugoga permutacijom koordinata u svim riječima koda i množenjem koordinatne pozicije sa ne-nul elementom polja.

Izomorfni kodovi

Dva koda iste duljine i nad istim poljem su izomorfna ako se jedan može dobiti iz drugoga permutacijom koordinata u svim riječima koda.

Automorfizam koda C je bilo koja permutacija koordinatnih pozicija koja preslikava riječi koda u riječi koda.

Standardni oblik generirajuće matrice

Svaki je linearni $[n, k, d]$ kod izomorfan kodu sa generirajućom matricom u tzv. standardnom obliku, tj. obliku $G = [I_k|A]$, gdje je I_k jedinična matrica reda k i A neka $k \times (n-k)$ matrica.

Paritetna matrica je tada oblika $H = [-A^T|I_{n-k}]$.

Primjer

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

Kodiranje linearnim kodom

Neka je $C \subset F^n$ linearni $[n, k, d]$ kod.

Svaka linearna bijekcija $\gamma : F^k \longrightarrow C$, $\mathbf{x} \mapsto \gamma(\mathbf{x})$ se zove *koder*, i svako linearno preslikavanje $\kappa : F^n \longrightarrow F^{n-k}$ za koje je $\mathrm{Ker}\kappa = C$ se zove *preslikavanje provjere pariteta*.

Linearni $[n, k, d]$ kod može otkriti najviše $d - 1$ pogrešaka u jednoj riječi i ispraviti najviše $t = \lfloor \frac{d-1}{2} \rfloor$ grešaka.

Dekodiranje linearnog koda

Za $I \subset \{1, \ldots, n\}$ neka je

$$p_I : F^n \to F^{|I|}, \quad \mathbf{x} \mapsto \mathbf{x}|_I$$

I-projekcija od F^n.

Informacijski skup

I se zove *informacijski skup* za C ako je $|I| = k$ i $p_I(C) = F^{|I|}$.

Za bilo koji informacijski skup I restrikcija $p_I|_C$ je bijekcija.

Za $I \subset \{1, \ldots, n\}$, neka je $I' = \{1, \ldots, n\} \setminus I$.

Za $\mathbf{x} \in F^{|I|}$, definiramo ${}^n\mathbf{x} \in F^n$ sa ${}^n\mathbf{x}(i) = \begin{cases} x_i, & i \in I \\ 0, & i \in I' \end{cases}$.

Tada je $F^n =^n p_I(F^n) \oplus^n p_{I'}(F^n)$.

Za $\mathbf{w} \in F^n$ imamo

$$\mathbf{w} =^n p_I(\mathbf{w}) +^n p_{I'}(\mathbf{w})$$

.

Neka je I informacijski skup za C, i neka je

$$\lambda := (p_I|_C)^{-1} : F^{|I|} \to C \quad \text{i} \quad \gamma_I := \lambda p_I : F^n \to C.$$

Lema 1.

Za $\mathbf{w} \in F^n$ vrijedi: $\mathbf{w} \in C$ ako i samo ako $p_{I'}\gamma_I(\mathbf{w}) = p_{I'}(\mathbf{w})$.

Dokaz. Za $\mathbf{w} \in F^n$ je $\lambda p_I(\mathbf{w}) = \mathbf{c} \in C$. Zato je

$$\mathbf{c} =^n p_I\lambda p_I(\mathbf{w}) +^n p_{I'}\lambda p_I(\mathbf{w}) =^n p_I(\mathbf{w}) +^n p_{I'}\lambda p_I(\mathbf{w}) = \mathbf{w}$$

ako i samo ako je $p_{I'}(\mathbf{w}) = p_{I'}\gamma_I(\mathbf{w})$. □

Za informacijski skup I definiramo preslikavanje

$$syn_I : F^n \longrightarrow F^{|I'|}, \quad \mathbf{w} \mapsto p_{I'}(\mathbf{w}) - p_{I'}\gamma_I(\mathbf{w})$$

Ono je prema Lemi 1. preslikavanje provjere pariteta.

Za $\mathbf{w} \in F^n$ slika $syn_I(\mathbf{w})$ se zove *sindrom* od $\mathbf{w}$ (s obzirom na I).

Teorem 1.

Neka je $C \subset F^n$ linearni $[n, k, d]$ kod koji može ispraviti t grešaka i neka je I informacijski skup za C. Za $\mathbf{w} \in F^n$, $\mathbf{c} \in C$ i $\mathbf{e} := \mathbf{w} - \mathbf{c}$ vrijedi:

(1) $p_I(\mathbf{e}) = \mathbf{0} \iff \mathbf{c} = \gamma_I(\mathbf{w})$

(2) $p_I(\mathbf{e}) = \mathbf{0} \implies w(syn_I(\mathbf{w})) = w(\mathbf{e})$

(3) $p_I(\mathbf{e}) \neq \mathbf{0}$, $w(\mathbf{e}) \leq t \implies w(syn_I(\mathbf{w})) > t$

(4) Ako je $w(\mathbf{e}) \leq t$, tada $p_I(\mathbf{e}) = \mathbf{0} \iff w(syn_I(\mathbf{w})) \leq t$

Dokaz. (1) $\gamma_I(\mathbf{w}) = \gamma_I(\mathbf{c}) + \gamma_I(\mathbf{e}) = \mathbf{c} + \lambda p_I(\mathbf{e}) = \mathbf{c} \iff p_I(\mathbf{e}) = \mathbf{0}$.
(2) $syn_I(\mathbf{w}) = syn_I(\mathbf{e}) = p_{I'}(\mathbf{e}) - p_{I'}(\lambda p_I(\mathbf{e})) = p_{I'}(\mathbf{e})$ i $w(\mathbf{e}) = w(p_{I'}(\mathbf{e}))$, pa je $w(syn_I(\mathbf{w})) = w(p_{I'}(\mathbf{e})) = w(\mathbf{e})$.
(3) Za $\mathbf{x} := \gamma_I(\mathbf{e}) \in C \backslash \{\mathbf{0}\}$ po Lemi 1. imamo $\mathbf{x} =^n p_I(\mathbf{e}) +^n p_{I'}\lambda p_I(\mathbf{e})$. Stoga je

$$\begin{aligned} w(syn_I(\mathbf{w})) &= w(syn_I(\mathbf{e})) = w(p_{I'}(\mathbf{e}) - p_{I'}(\mathbf{x})) \geq w(-p_{I'}(\mathbf{x})) - w(p_{I'}(\mathbf{e})) \\ &= w(p_{I'}\lambda p_I(\mathbf{e})) + w(p_I(\mathbf{e})) - w(p_I(\mathbf{e})) - w(p_{I'}(\mathbf{e})) \\ &= w(\mathbf{x}) - w(\mathbf{e}) \geq d - t \geq 2t + 1 - t \geq t + 1. \end{aligned}$$

(4) slijedi iz (2) i (3). □

Dekodiranje linearnog koda korištenjem informacijskog skupa

E. Prange (1962.)

Za linearni $[n, k, d]$ kod koji može ispraviti t grešaka za svaku riječ r postoji informacijski skup I takav da je za riječ koda b za koju je $r_i = b_i$ za $i \in I$ Hammingova udaljenost $d(r, b)$ manja od d.

PD-skupovi

Neka je $C \subset F^n$ linearni $[n, k, d]$ kod koji može ispraviti t grešaka i neka je I informacijski skup za C. Podskup $\Sigma \subset \mathrm{Aut}C$ se zove *PD-skup* za C ako za svaki podskup $B \subset \{1, \ldots, n\}$ za koji je $|B| \leq t$ postoji automorfizam $\sigma \in \Sigma$ takav da je $\sigma(B) \cap I = \emptyset$.

Gordonova granica

Ako je Σ PD-skup za $[n, k, d]$ kod C koji može ispraviti t grešaka, i $r = n - k$, tada je

$$|\Sigma| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil.$$

Primjer.

Za binarni prošireni Golayev kod s parametrima $[24, 12, 8]$ je

$$|\Sigma| \geq \left\lceil \frac{24}{12} \left\lceil \frac{23}{11} \left\lceil \frac{22}{10} \right\rceil \right\rceil \right\rceil = 14$$

i nađen je PD-skup veličine 14 (Gordon, Wolfmann).

Primjer.

$$C = \begin{cases} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{cases}$$

je linearni $[5, 2, 3]$ kod, $t = 1$.

$$\begin{aligned} \mathrm{Aut}(C) = &\{id, (1,2)(4,5), (1,5)(2,4), (1,4)(2,5), (4,5), (1,2), \\ &(1,5,2,4), (1,4,2,5)\} \end{aligned}$$

Gordonova granica: $|\Sigma| \geq \left\lceil \frac{5}{3} \right\rceil = 2$

Za $I = \{2, 5\}$, $\Sigma = \{(1,2)(4,5), (1,4)(2,5)\}$

Permutacijsko dekodiranje

Neka je $\Sigma = \{\sigma_1, \ldots, \sigma_s\}$ PD-skup za linearni kod C koji može ispraviti t grešaka. Algoritam permutacijskog dekodiranja je sljedeći:

1. Za primljenu riječ $\mathbf{w} \in F^n$ izračunati $\sigma_i(\mathbf{w})$, $\gamma_I(\sigma_i(\mathbf{w}))$ i $w(syn_I(\sigma_i(\mathbf{w})))$ za $i = 1, 2, \ldots$ dok se ne nađe j takav da je $w(syn_I(\sigma_j(\mathbf{w}))) \leq t$.
2. Izračunati $\sigma_j^{-1}(\gamma_I(\sigma_j(\mathbf{w})))$
3. $\mathbf{w}$ se dekodira kao $\mathbf{c} := \sigma_j^{-1}(\gamma_I(\sigma_j(\mathbf{w}))) \in C$.
4. Ako $w(syn_I(\sigma_1(\mathbf{w}))), \ldots, w(syn_I(\sigma_s(\mathbf{w}))) > t$, tada ne postoji $\mathbf{c} \in C$ takva da je $d(\mathbf{w}, \mathbf{c}) \leq t$.

PD-skup cikličkog koda

$[n, k, d]$ kod C je ciklički ako je za $\mathbf{c} = c_1 c_2 \dots c_n \in C$ svaki ciklički pomak od $\mathbf{c}$ u C. Dakle, permutacija $\tau \in S_n$ definirana sa

$$\tau : i \mapsto i + 1$$

za $i \in \{1, \dots, n\}$ je u grupi automorfizama od C i vrijedi $\tau^n = 1$.

Ako je $k < \frac{n}{t}$, tada je ciklička grupa $< \tau >$ PD-skup za C.

Antibloking sustavi

Neka je P konačan skup, $t \in \mathbb{N}$ i neka je $\mathfrak{A}$ podskup partitivnog skupa skupa P. Elementi od P i $\mathfrak{A}$ se nazivaju *točke* i *blokovi*, respektivno.

$\mathfrak{A}$ se naziva t-antibloking sustav od P ako vrijedi

(AB) Za svaki $B \subset P$ takav da je $|B| = t$ postoji $A \in \mathfrak{A}$ takav da je $A \cap B = \emptyset$

i ako svaka dva bloka $A, A' \in \mathfrak{A}$ imaju istu kardinalnost $|A| = |A'| =: k$. k se naziva *red* t-antibloking sustava $\mathfrak{A}$.

Primjer.

Za svaki $t, k \in \mathbb{N}$ za koje je $t + k \leq |P|$ skup $\binom{P}{k}$ svih k-podskupova od P je t-antibloking sustav.

Neka je $C \subset F^n$ linearni $[n, k, d]$ kod koji može ispraviti t grešaka i neka je I informacijski skup za C.

Za svaki $\sigma \in \mathrm{Aut}(C)$ skup $\sigma^{-1}(I)$ je informacijski skup za C.

Neka je Σ PD-skup. Tada je $\mathfrak{A} = \{\sigma^{-1}(I) | \, \sigma \in \Sigma\}$ t-antibloking sustav od $P_n = \{1, \ldots, n\}$ sa svojstvom da je svaki blok $A \in \mathfrak{A}$ informacijski skup za C.

t-AI-sustav

Neka je $\mathfrak{A}$ t-antibloking sustav. $\mathfrak{A}$ se naziva *t-antibloking informacijski sustav za C*, skraćeno *t-AI-sustav za C*, ako je svaki blok $A \in \mathfrak{A}$ informacijski skup za C.

Skup svih informacijskih skupova za C je t-AI-sustav. Dakle, za svaki linearni kod koji može ispraviti t grešaka postoji t-AI-sustav.

Lema 2.

Neka je $\mathfrak{A}$ t-AI sustav za linearni kod C. Za $\mathbf{w} \in F^n$ i $\mathbf{c} \in C$, te $\mathbf{e} := \mathbf{w} - \mathbf{c}$ takav da je $w(\mathbf{e}) \leq t$, postoji $A \in \mathfrak{A}$ takav da je $w(syn_A(\mathbf{w})) \leq t$ i $\mathbf{c} = \gamma_A(\mathbf{w})$.

Dokaz. Neka je $B := \text{supp}(\mathbf{e}) = \{i \in \mathbb{N} | \, i \leq n, \, e_i \neq 0\}$. Po pretpostavci, $|B| \leq t$ pa postoji $A \in \mathfrak{A}$ takav da je $A \cap B = \emptyset$. Tada je $p_A(\mathbf{e}) = \mathbf{0}$, pa je po Teoremu 1. $w(syn_A(\mathbf{w})) \leq t$ i $\mathbf{c} = \gamma_A(\mathbf{w})$.

□

Antibloking dekodiranje

Neka je $\mathfrak{A}$ t-AI-sustav za linearni $[n, k, d]$ kod C. Algoritam antibloking dekodiranja je sljedeći:

1. Za primljenu riječ $\mathbf{w} \in F^n$ izračunati $\gamma_A(\mathbf{w})$ i $w(syn_A(\mathbf{w}))$ za $A \in \mathfrak{A}$ dok se ne nađe A' takav da je $w(syn_{A'}(\mathbf{w})) \leq t$.
2. $\mathbf{w}$ se dekodira kao $\mathbf{c} := \gamma_{A'}(\mathbf{w}) \in C$.
3. Ako je $w(syn_A(\mathbf{w})) > t$ za sve $A \in \mathfrak{A}$, tada ne postoji $\mathbf{c} \in C$ takva da je $d(\mathbf{w}, \mathbf{c}) \leq t$.

Rezultati Jennifer D. Key:

Za kodove iz affinih ravnina redova $p = 5, 7$ i 11 pronašla je 2-AI-sustave i 2-PD-skupove sljedećih kardinalnosti:

p	5	7	11
Gordonova granica	8	7	4
kardinalnost 2-AI-sustava	15	19	24
kardinalnost 2-PD-skupa	18	23	26

Neka je P konačan skup, $I \subset P$ i $t \in \mathbb{N}$. Podskup Σ simetrične grupe S_P od P se naziva *t-PD-skup* za $I \subset P$ ako za svaki $B \subset P$ takav da je $|B| \leq t$ postoji $\sigma \in \Sigma$ takva da je $\sigma(B) \cap I = \emptyset$.

Lema

Neka je P konačan skup.

(1) Ako je $\mathfrak{A}$ t-antibloking sustav od P reda k i $I \subset P$ takav da je $|I| = k$, tada postoji t-PD-skup Σ za I takav da je $|\Sigma| = |\mathfrak{A}|$.

(2) Za svaki t-PD-skup Σ za $I \subset P$ sa svojstvom $\sigma^{-1}(I) \neq \tau^{-1}(I)$ za različite $\sigma, \tau \in \Sigma$, skup $\mathfrak{A} := \{\sigma^{-1}(I) | \, \sigma \in \Sigma\}$ je t-antibloking sustav takav da je $|\Sigma| = |\mathfrak{A}|$.

Gordonova granica

Neka je $\mathfrak{A}$ t-antibloking sustav reda k. Tada je

$$|\mathfrak{A}| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil.$$

Za $n, k, t \in \mathbb{N}$ takve da je $k + t \leq n$ broj

$$g(n,k,t) = \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil$$

se naziva *Gordonova granica od* (n,k,t).

Neka je P konačan skup. Za $k, t \in \mathbb{N}$ takve da je $k + t \leq n = |P|$ neka je

$$b(n,k,t) := \min\{|\mathfrak{A}| \,|\, \mathfrak{A} \subset 2^P \text{ je } t\text{-antibloking sustav reda } k\}.$$

t-antibloking sustav reda k se naziva *optimalan* ako je $|\mathfrak{A}| = b(n,k,t)$.

Očito,

$$b(n, k, t) \geq g(n, k, t).$$

Jednakost vrijedi za, na primjer, $n = 10, 12$, $k = 4$, $t = 2$ i za $n = 16$, $k = 5$, $t = 2$ jer u tom slučaju postoje odgovarajući PD-skupovi.

(H.-J. Kroll, R. Vincenti, PD-sets for the codes related to some classical varieties, Discrete Math. 301 (2005) 89-105.)

Neka svojstva antibloking sustava

Neka je $\mathfrak{A} \subset 2^P$ t-antibloking sustav reda k. Označimo $n := |P|$ i $r := n - k$.

Blokirajući skup

Podskup $B \subset P$ se naziva *blokirajući skup*, ako za svaki $A \in \mathfrak{A}$ vrijedi $A \cap B \neq \emptyset$.

Kako je $\mathfrak{A}$ t-antibloking sustav svaki blokirajući skup B je kardinalnosti barem $t + 1$.

Neka je $\mathfrak{A} \subset 2^P$ i $p \in P$. Tada se

$$\mathfrak{A}^p := \{A \in \mathfrak{A} | \, p \notin A\}$$

naziva (vanjska) derivacija od $\mathfrak{A}$ u točki p.

Lema 3.

Neka je $\mathfrak{A}$ t-antibloking sustav reda k. Za svaku točku $p \in P$ derivacija $\mathfrak{A}^p \subset 2^{P\setminus\{p\}}$ je $(t-1)$-antibloking sustav od $P\setminus\{p\}$ reda k.

Za $p \in P$ neka je $r_p := |\{A \in \mathfrak{A} | \, p \in A\}|$ broj blokova koji sadrže točku p, i za $i \in \mathbb{N}_0$ neka je $x_i := |\{p \in P | \, r_p = i\}|$ broj točaka incidentnih s točno i blokova.

Lema 4.

Neka je $\mathfrak{A}$ t-antibloking sustav reda k. Tada

(1) Za svaku točku $p \in P$,
$r_p \leq |\mathfrak{A}| - b(n-1, k, t-1) \leq |\mathfrak{A}| - g(n-1, k, t-1)$.

(2) Ako je $x_0 \neq 0$, tada $|\mathfrak{A}| \geq b(n-1, k, t) \geq g(n-1, k, t)$.

Dokaz. (1) Po Lemi 3., $|\mathfrak{A}^p| \geq b(n-1, k, t-1) \geq g(n-1, k, t-1)$, pa je $r_p = |\mathfrak{A}| - |\mathfrak{A}^p| \leq |\mathfrak{A}| - b(n-1, k, t-1) \leq |\mathfrak{A}| - g(n-1, k, t-1)$.
(2) Postoji točka $p \in P$ za koju je $r_p = 0$, pa je $\mathfrak{A} \subset 2^{P \setminus \{p\}}$ t-antibloking sustav reda k i vrijedi $|\mathfrak{A}| \geq b(n-1, k, t)$.

□

Lema 5.

Za $n, k, t \in \mathbb{N}$ takve da je $k + t < n$ vrijedi $g(n, k, t) \leq g(n-1, k, t)$.

Za t-antibloking sustav $\mathfrak{A}$ reda k neka je $R(\mathfrak{A}) := |\mathfrak{A}| - g(n-1, k, t-1)$.

Lema 6.

Neka je $\mathfrak{A}$ t-antibloking sustav reda k. Tada je

$$\sum_{i=0}^{R(\mathfrak{A})} i \cdot x_i = |\mathfrak{A}| \cdot k \qquad \text{i} \qquad \sum_{i=0}^{R(\mathfrak{A})} x_i = n.$$

Primjeri optimalnih antibloking sustava

$n = 6,\ k = 3,\ t = 2$

Sustav $\mathfrak{A} = \{\{1,2,3\},\{3,4,5\},\{1,4,5\},\{6,2,4\},\{6,2,5\},\{6,1,3\}\}$ je 2-antibloking sustav reda 3 za $P = \{1,2,3,4,5,6\}$.

$n = 7,\ k = 3,\ t = 2$

Za skup P od 7 elemenata za $k = 3$ ne postoji 2-antibloking sustav kardinalnosti 4, a postoji 2-antibloking sustav kardinalnosti 5: $b(7,3,2) = 5 > 4 = g(7,3,2)$.

$n = 7,\ k = 3,\ t = 3$

Za skup P od 7 elemenata za $k = 3$ ne postoji 3-antibloking sustav kardinalnosti 11, a postoji optimalni 3-antibloking sustav kardinalnosti 12: $b(7,3,2) = 12 > 11 = g(7,3,2)$.

Pravci afine ravnine kao antibloking sustav

Propozicija 1.

Neka je $(P, \mathfrak{L})$ konačna afina ravnina reda $k > 2$ i neka je $t = k + \lceil \sqrt{k} \rceil - 1$. Tada je $\mathfrak{L}$ t-antibloking sustav.

Za $k = 3, 4, 5, 7, 8, 9$ u tablici su izlistani $t = k + \lceil \sqrt{k} \rceil - 1$, Gordonova granica $g = g(k^2, k, t)$ i $|\mathfrak{L}|$:

k	3	4	5	7	8	9
t	4	5	7	9	10	11
g	11	10	14	14	15	16
$\lvert\mathfrak{L}\rvert$	12	20	30	56	72	90

Propozicija 2.

Neka je $(P, \mathfrak{L})$ konačna afina ravnina reda $k > 3$ i neka je $w \in P$. Tada je $\mathfrak{A} = \mathfrak{L}^w$ $(k+1)$-antibloking sustav od $P \backslash \{w\}$.

$n = 9,\ k = 3,\ t = 4$

Za skup P od 9 elemenata za $k = 3$ ne postoji 4-antibloking sustav kardinalnosti 11, a postoji optimalan 4-antibloking sustav kardinalnosti 12: $b(9, 3, 4) = 12 > 11 = g(9, 3, 4)$.

$n = 15,\ k = 4,\ t = 5$

Za skup P od 15 elemenata za $k = 4$ ne postoji 5-antibloking sustav kardinalnosti 10, a postoji 5-antibloking sustav kardinalnosti 15: $15 \geq b(15, 4, 5) > g(15, 4, 5) = 10$.