An extension of the order bound for AG codes

Iwan Duursma and Radoslav Kirov

June 9, 2009

AAECC-18, Tarragona

Related work, jointly with Seungkook Park (KIAS)

- Minimum distance for Hermitian two-point codes (P'07)
- Algebraic geometry codes: general theory (D'08)
- Coset bounds for algebraic geometric codes (DP'08a)
- Delta sets for divisors supported in two points (DP'08b)
- An extension of the order bound for AG codes (DK'09)
- The AB method for algebraic geometric codes (DKP'09)

- `http://www.math.uiuc.edu/{~duursma,~rkirov2}`
- `http://arxiv.org`
- `http://agtables.appspot.com`

Hamming distance

The Hamming distance between two vectors $x, y \in \mathbb{F}^n$ is

$$d(x, y) = |\{i : x_i \neq y_i, i = 1, 2, \ldots, n\}|.$$

A nontrivial code $\mathcal{C} \subseteq \mathbb{F}^n$ has minimum distance

$$d(\mathcal{C}) = \min\{d(x, y) : x, y \in \mathcal{C}, x \neq y\}.$$

Geometric Goppa codes

(Goppa 1981)

For n distinct rational points $P_1, \ldots, P_n$ on a curve X, and for disjoint divisors $D = P_1 + \cdots + P_n$ and G, the geometric Goppa codes $C_L(D, G)$ and $C_\Omega(D, G)$ are defined as the images of the maps

$$\begin{array}{rcl} \alpha_L : L(G) & \longrightarrow & \mathbb{F}^n \\ f & \mapsto & (\, f(P_1), \ldots, f(P_n)\,) \end{array}$$

$$\begin{array}{rcl} \alpha_\Omega : \Omega(G-D) & \longrightarrow & \mathbb{F}^n \\ \omega & \mapsto & (\,\mathrm{Res}_{P_1}(\omega), \ldots, \mathrm{Res}_{P_n}(\omega)\,). \end{array}$$

Goppa bound

$$d(C_L(D,G)) \;=\; \text{min}\{\text{deg}\, A : \; 0 \le A \le D \;\wedge\; L(G-D+A) \ne L(G-D)\}.$$

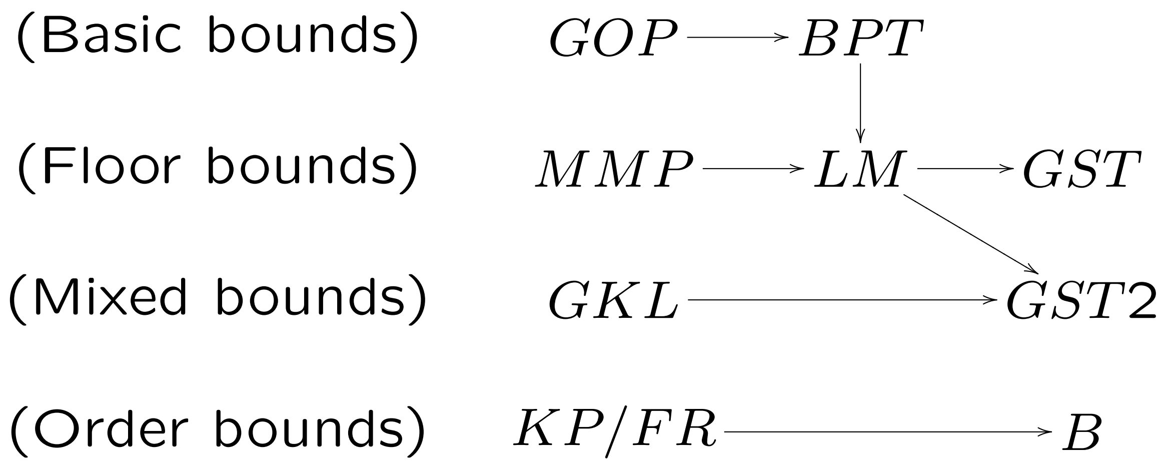
$$d(C_\Omega(D,G)) \;=\; \text{min}\{\text{deg}\, A : \; 0 \le A \le D \;\wedge\; L(K-G+A) \ne L(K-G)\}.$$

$$d(C_L(D,G)) \;\ge\; \text{min}\{0, \text{deg}(D-G)\}$$

$$d(C_\Omega(D,G)) \;\ge\; \text{min}\{0, \text{deg}(G-K)\}$$

Incomplete list of improvements

Garcia, Kim and Lax (1993)
Kirfel and Pellikaan (1995)
Hoeholdt, van Lint and Pellikaan (1998)
Maharaj, Matthews and Pirsic (2005)
Carvalho and Torres (2005)
Lundell and McCullough (2006)
Carvalho, Munuera, da Silva and Torres (2005)
Beelen (2007)
Guneri, Stichtenoth and Taskin (2009)



In general, the bounds d_{GST}, d_{GST2} and d_B are not comparable, as shown by the following codes constructed with the Suzuki curve over $\mathbb{F}_8$.

Code	d_{GST}	d_{GST2}	d_B
$C_\Omega(D, G = K + 2P + 2Q)$	8	8	7
$C_\Omega(D, G = K + 4P)$	7	6	8
$C_\Omega(D, G = K + 4P + Q)$	7	8	8

Definition

For a divisor C and for subsets S and S' of rational points, define

$$\begin{aligned}\gamma(C; S, S') \;=\; & \min\{\, \deg D : \\ & (\forall P \in S)\ L(D) \neq L(D-P) \\ & (\forall P \in S')\ L(D-C) \neq L(D-C-P)\,\}.\end{aligned}$$

Theorem 1 (DKP'09)

Let S, S' be finite sets of points and let Λ be the semi-group of effective divisors with support in S'. For $D \cap S = \emptyset$,

$d(C_L(D, G)) \geq$

$$\min\{\gamma(D - G + \lambda; S, S') : \lambda \in \Lambda\} \backslash \{0\}.$$

$d(C_\Omega(D, G)) \geq$

$$\min\{\gamma(G - K + \lambda; S, S') : \lambda \in \Lambda\} \backslash \{0\}.$$

Theorem 2 (DKP'09)

For a given divisor $C \sim D-E$, and for divisors $A_0, \ldots, A_n$, such that $A_i = A_{i-1} + P_i$, define the subsets

$$\Delta = \{i : L(A_i) \neq L(A_i - P) \wedge L(A_i - C) = L(A_i - C - P)\}$$

$$S = \{i : L(D) \neq L(D - P_i)\}$$

$$\Delta' = \{i : L(A_i) = L(A_i - P) \wedge L(A_i - C) \neq L(A_i - C - P)\}$$

$$S' = \{i : L(E) \neq L(E - P_i)\}.$$

Then $\deg D \geq |\Delta \cap S'| + |\Delta' \cap S| - |\Delta'|$.

In particular, $\gamma(C; S, S') \geq |\Delta|$ for

$\Delta \subseteq S'$ and $\Delta' \subseteq S$.

Special cases of Theorem 2

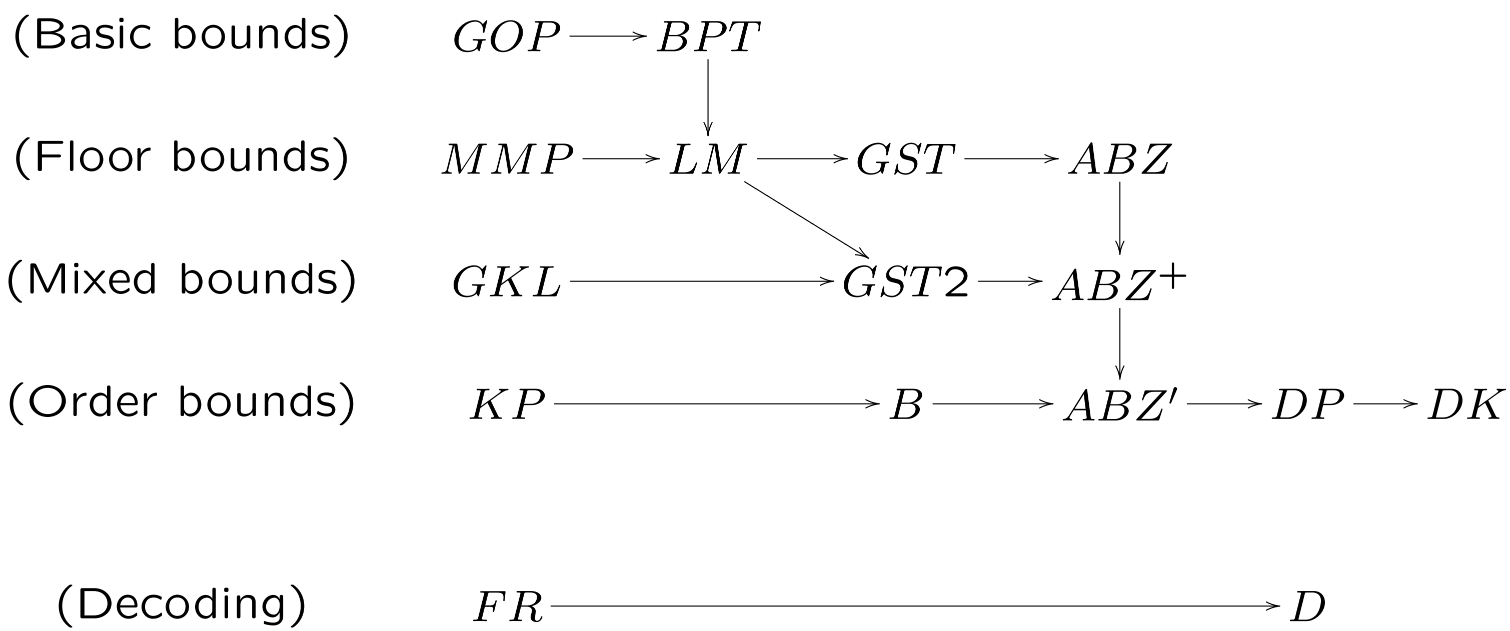
(1) Beelen'07

(2) DP'08a

(3) DK'09

Assumes	(1)	(2)	(3)
$S = \{1, 2, \ldots, n\}$	y	y	y
$\Delta \subseteq S'$	y	y	y
$P_i = P$, for $i \in \Delta$	y	y	
$P_i = P$, for $i = 1, 2, \ldots, n$	y		

Chart of known bounds



Comparison table

Code	d_{GST}	d_{GST2}	d_B	d_{ABZ}	d_{ABZ^+}	$d_{ABZ'}$
$C_\Omega(D, G = K + P + 2Q)$	8	8	7	8	8	8
$C_\Omega(D, G = K + 4P)$	7	6	8	7	7	8
$C_\Omega(D, G = K + 4P + Q)$	7	8	8	8	8	8
$C_\Omega(D, G = K + 4P + 2Q)$	9	9	9	10	10	10

Projective line over $\mathbb{F}_q$ (BCH bound)

For a cyclic code with zero set $I \supset \{1, \alpha, \ldots, \alpha^{m-2}\}$, $m \geq 2$, the minimum distance $d \geq m$.

	$C = mP$
Δ	0 P $\vdots$ $(m-1)P$
S'	$\{P\}$
Δ'	
S	$\emptyset$
$\gamma \geq$	m

$iP \in \Delta$
$\Leftrightarrow \; i \geq 0$ and $i - m < 0$

$iP \in \Delta'$
$\Leftrightarrow \; i < 0$ and $i - m \geq 0$

Hermitian curve over $\mathbb{F}_{16}$ (Feng-Rao bound)

	$C = 3P$	$C = 4P$
Δ	0 $4P$ $5P$ $9P$ $10P$ $14P$	0 $5P$ $10P$ $15P$
S'	$\{P\}$	$\{P\}$
Δ'	$3P$ $7P$ $11P$	
S	$\{P\}$	$\emptyset$
$\gamma \geq$	6	4

Grid for $C = 3P$

$C = mP$	3	4	5	6	7	8	9	10	11
$\gamma \geq$	6	4	5	8	9	8	9	10	12

$$d(C_\Omega(D, K + 3P) \geq 4$$

Suzuki curve over $\mathbb{F}_8$ ($C = 2P + 2Q$)

	(B)	(DP, DK)
Δ	0	0
	$8P$	$8P$
	$10P$	$10P$
	$13P$	$13P$
	$16P$	$16P + 2Q$
		$19P + 2Q$
	$21P$	$21P + 2Q$
	$29P$	$29P + 2Q$
S'	$\{P\}$	$\{P\}$
Δ'	$14P$	$14P$
	$15P$	$14P + Q^*$
	$27P$	$15P + Q$
		$15P + 2Q^*$
S	$\{P\}$	$\{P, Q\}$
$\gamma \geq$	7	8

Grid for $C = 2P + 2Q$

(B)

	2	3	4	5	6
2	7	8	9	10	10
3	8	8	10	11	
4	9	10	10		
5	10	11			
6	10				

(DP)

	2	3	4	5	6
2	8	9	10	11	10
3	9	8	10	11	
4	10	10	10		
5	11	11			
6	10				

$$d(C_\Omega(D, K + 2P + 2Q) \geq 8$$

Suzuki curve over $\mathbb{F}_8$ ($C = -5P + 8Q$)

	(B, DP)	(DK)
Δ	$10P - 3Q$	$10P - 3Q$
	$12P - 3Q$	$12P - 3Q$
	$13P - 3Q$	$13P - 3Q$
		$16P - 2Q^*$
		$16P - Q^*$
		$16P^*$
	$22P - 3Q$	$22P$
	$23P - 3Q$	$23P$
	$25P - 3Q$	
S'	$\{P\}$	$\{P, Q\}$
Δ'	$8P - 3Q$	$8P - 3Q$
	$16P - 3Q$	$16P - 3Q$
		$17P$
		$19P$
	$27P - 3Q$	$27P$
S	$\{P\}$	$\{P\}$
$\gamma \geq$	6	8

Grid for $C = -5P + 8Q$

(DP)

	8	9	10	11	12
-5	6	8	7	9	7
-4	8	9	10	11	
-3	7	10	7		
-2	9	11			
-1	7				

(DK)

	8	9	10	11	12
-5	8	8	9	9	7
-4	8	9	10	11	
-3	9	10	7		
-2	9	11			
-1	7				

$$d(C_\Omega(D, K - 5P + 8Q) \geq 7$$

Suzuki curve over $\mathbb{F}_8$

$X/\mathbb{F}_8 : y^8 + y = x^{10} + x^3$

has $g = 14, N = 65$, and $m = 13 = 3^2 + 2^2$.

The m inequivalent divisor classes in $D(P, Q)$ with support in P and Q are represented by the divisors

$(0, 0)$	$\cdot$	$(-5, 12)$	$\cdot$	$(-10, 24)$
$\cdot$	$(-3, 10)$	$\cdot$	$(-8, 22)$	$\cdot$
$(-1, 8)$	$\cdot$	$(-6, 20)$	$\cdot$	$(-11, 32)$
$\cdot$	$(-4, 18)$	$\cdot$	$(-9, 30)$	$\cdot$
$(-2, 16)$	$\cdot$	$(-7, 28)$	$\cdot$	$(-12, 40)$

	Floor bounds		
	d_{LM}	d_{GST}	d_{ABZ}
d_{GOP}	6352	6352	6352
d_{LM}	·	2245	2852
d_{GST}	·	·	2213
d_{ABZ}	·	·	·
d_{B}	1	1	1
$d_{ABZ'}$	·	·	·
d_{GOP}	8	13	21
d_{LM}	·	7	15
d_{GST}	·	·	8
d_{ABZ}	·	·	·
d_{B}	1	1	1
$d_{ABZ'}$	·	·	·

Number of improvements of one bound over another (top), and the maximum improvement (bottom), based on 10168 two-point codes for the Suzuki curve over $\mathbb{F}_{32}$.

	Order bounds		
	d_B	d_{DP}	d_{DK}
d_{GOP}	6352	6352	6352
d_{LM}	4729	4731	4757
d_{GST}	4729	4731	4757
d_{ABZ}	4683	4685	4711
d_B	·	236	1565
d_{DP}	·	·	1366
d_{GOP}	33	33	33
d_{LM}	28	28	28
d_{GST}	24	24	24
d_{ABZ}	24	24	24
d_B	·	5	6
d_{DP}	·	·	6

Number of improvements of one bound over another (top), and the maximum improvement (bottom), based on 10168 two-point codes for the Suzuki curve over $\mathbb{F}_{32}$.

Argument used in Theorem 2

For G of degree $2g+t$, and for A of degree at most t,

$$L(G-A) \neq L(G-A-P).$$

For an improvement, let

$$0 \leq \alpha_1 \leq \cdots \leq \alpha_{g+t+1} \leq 2g+t$$

be the vanishing orders at P, and let

$$\Delta = \{\alpha_i : \alpha_i \text{ is a nongap for } P\}.$$

Then $|\Delta| \geq t+1$ and $L(G-A) \neq L(G-A-P)$ for all A of degree less than $|\Delta|$.

Proof of the argument

For $\alpha_i \in \Delta$, choose

$$f_i \in L(G - \alpha_i P)\backslash L(G - \alpha_i - P)$$

$$g_i \in L(\alpha_i P)\backslash L(\alpha_i P - P)$$

Then $f_i g_i \in L(G)\backslash L(G - P)$.

Assume $|A| < |\Delta|$. There exists $g \in \langle g_i | \alpha_i \in \Delta \rangle$ such that g vanishes at A. If g has pole order α_i at P then $f_i g \in L(G-A)\backslash L(G-A-P)$ and $L(G-A) \neq L(G-A-P)$.