Distance bounds for AG codes

Iwan Duursma

September 28, 2009
Workshop on Sequences, Codes and Curves
Antalya, Turkey

Joint work with
Radoslav Kirov
Seungkook Park (KIAS)

Selection of references

van Lint and Wilson (1986)
Yang and Kumar (1992)
Garcia, Kim and Lax (1993)
Feng and Rao (1993), D (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)
Homma and Kim (2006)
Beelen (2007)
Andersen and Geil (2008)
D and Pellikaan (2008)
Guneri, Stichtenoth and Taskin (2009)

1 – The role of the minimum distance in coding theory, secret sharing, and secure computation

2 – Some geometry

Delta sets

3 – Basic methods to obtain bounds

AB method / ABZ Theorem

Shifting method / Main Theorem

4 – Comparison and numerical results

Coding theory

Let $C \subseteq \mathbb{F}^n$ be a linear code. The minimum distance d of the code is the minimum of $d(x, y) = \#\{i : x_i \neq y_i\}$ for any two distinct vectors $x, y \in C$.

Given a vector $c \in C$ and a subset $A \subset \{1, 2, \ldots, n\}$, the values of c on A give the following information about values of c outside A (as a function of $|A|$):

$$\underbrace{0 \ \cdots\cdots \ d^{\perp} - 2}_{\text{No information}} \ \underbrace{\cdots\cdots}_{?} \ \underbrace{n - d + 1 \ \cdots\cdots \ n}_{\text{Full information}}$$

Secret sharing (Quotient code version [D-Park'08])

Let $C_0 \subseteq C$ be a subcode with $\dim C/C_0 = 1$ and let $x \in C \backslash C_0$. For given $c \in C$, we seek to determine $s \in \mathbb{F}$ such that $c - s \cdot x \in C_0$.

Given a vector $c \in C$, the values of c on A give the following information about s (as a function of $|A|$):

$$\underbrace{0 \ \cdots\cdots \ d_0^{\perp} - 1}_{\text{No information about } s} \qquad \underbrace{\cdots\cdots}_{?} \qquad \underbrace{n - d_0 + 1 \ \cdots\cdots \ n}_{\text{Full information about } s}$$

Here $d_0 = d(C/C_0)$ and $d_0^{\perp} = d(C_0^{\perp}/C^{\perp})$.

Relation between $d = d(C)$ and $d_0 = d(C/C_0)$.

$$\begin{aligned} d(C/C_0) &= \min\{\, d(x + C_0, y + C_0) \;\; : \\ &\qquad\qquad \text{distinct } x + C_0, y + C_0 \in C/C_0 \,\}. \\ &= \min\{\, \mathrm{wt}(c) : c \in C \backslash C_0 \,\}. \end{aligned}$$

So that

$$d(C) = \min\{\, d(C/C_0), d(C_0) \,\}$$

Let the code C be defined by evaluation of $1, x, x^3, x^4, x^7$ in the ninth roots of unity.

$$C = \begin{pmatrix} 1 & 1 & \cdots & \cdots & 1 & 1 \\ 1 & \alpha & \cdots & \cdots & \alpha^7 & \alpha^8 \\ 1 & \alpha^3 & \cdots & \cdots & \alpha^3 & \alpha^6 \\ 1 & \alpha^4 & \cdots & \cdots & \alpha & \alpha^5 \\ 1 & \alpha^7 & \cdots & \cdots & \alpha^4 & \alpha^2 \end{pmatrix}$$

And let

$$C_0 = \mathsf{Ev}(x, x^3, x^4, x^7) \subset C = \mathsf{Ev}(1, x, x^3, x^4, x^7).$$

Then

$$d(C) = 3, \quad d(C/C_0) = 4, \quad d(C_0) = 3.$$

For codes A and B of same length n, let

$$A * B = \langle (a_i b_i) : (a_i) \in A, (b_i) \in B \rangle.$$

A quotient C/C_0 of dimension one is said to be multiplicative if $C*C/C_0*C$ is of dimension one. This is the case if and only if $x * x \in C * C \backslash C_0 * C$, for $x \in C \backslash C_0$.

Secure multiplication of the product $s \cdot s'$ from the factors s and s' requires that

- $d_0^{\perp}(C) > t$ (privacy: no information about the factors s or s' when $|A| \leq t$))

- $d_0(C * C) > t$ (security: full information about the product $s \cdot s'$ when $|A| \geq n - t$)

Geometric Goppa codes

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 $C_L(G, D)$ and $C_\Omega(G, D)$ are defined as the images of the maps

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

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

Goppa bound

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

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

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

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

For a rational point P, for D the sum of the $N-1$ rational points outside P, and for G of degree $2g+t$,

$$d_0^{\perp}(C) \geq d^{\perp}(C_0) \geq t+1,$$
$$d_0(C*C) \geq d(C*C) \geq (N-1)-(4g+2t).$$

[Chen-Cramer'06] For a curve over $\mathbb{F}_q$ of genus g with N rational points, secure multiplication using codes of length $n = N-1$ is possible for

$$n > 3t+4g, \quad \text{or} \quad t/n < (1-4g/n)/3.$$

For a projective line, a Hermitian curve, or an optimal asymptotic tower over $\mathbb{F}_q$, $q = r^2$,

$t/n < 1/3$	$n = q$
$t/n < (1-2/(r+1))/3$	$n = r^3$
$t/n \lesssim (1-4/(r-1))/3$	$n \to \infty$.

2 – Some Geometry : Delta sets.

In the theory of linear secret sharing schemes, the subsets of $\{1, 2, \ldots, n\}$ are partitioned into qualified and unqualified subsets.

$$\Gamma_0(C) = \{A : A \text{ has acces to } s\}$$
$$\Delta_0(C) = \{A : A \text{ has no access to } s\}$$

In particular,

$$\{A : |A| \geq n - d_0 + 1\} \subseteq \Gamma_0(C)\}$$
$$\{A : |A| \leq d_0^{\perp} - 1\} \subseteq \Delta_0(C)\}$$

Delta sets in Gröbner basis theory.

Let $\mathbb{F}[x, y]$ be the coordinate ring of the affine plane, with ordered basis

$$1 < x < y < x^2 < xy < y^2 < x^3 < \cdots$$

For a set of points $\{P_1, P_2, \ldots, P_n\}$ with vanishing ideal

$$I = \{f : f(P_i) = 0, \text{ for } i = 1, 2, \ldots, n\},$$

the Delta set is a greedy basis for $\mathbb{F}[x, y]/I$ with respect to the given ordering. In general, $|\Delta| = n$.

Delta sets for divisors on curves.

Let $X : y^4 + y = x^5$ be the Hermitian curve of genus $g = 6$ over the field $\mathbb{F} = \mathbb{F}_{16}$. The functions x and y have poles only at P, of order 4 and 5, respectively. They generate the affine ring $\mathbb{F}[x, y] = \mathcal{O}$ of all functions with poles only at P. The ordered basis

$$1 < x < y < x^2 < xy < y^2 < x^3 < x^2y < \cdots$$

corresponds to an ordering

$$0 < 4P < 5P < 8P < 9P < 10P < 12P < 13P < \ldots$$

of the Weierstrass nongaps at P.

For divisors $0 \leq C \leq D$ such that C, D disjoint from P,

$$\Delta(D) \supseteq \Delta(C).$$

For the curve $X : y^4 + y = x^5$, let $Q = (0,0), R = (0,1)$.

$$\begin{array}{lll} \Delta(Q+R) & = \{1, y\}, & \text{or } \{0, 5\}. \\ \Delta(2Q+2R) & = \{1, x, y, xy\}, & \text{or } \{0, 4, 5, 9\}. \\ \Delta(3Q+3R) & = \{1, x, y, x^2, xy, x^2y\}, & \text{or } \{0, 4, 5, 8, 9, 13\}. \end{array}$$

Let $I(C) \subseteq \mathcal{O}$ be the vanishing ideal of C, for $C \geq 0$ disjoint from P. A basis for $\mathcal{O}/I(C)$ is given by $\{f_i : i \in \Delta(C)\}$, where

$$i \in \Delta(C) \;\Leftrightarrow\; \begin{cases} (1)\ L(iP) \neq L((i-1)P), \text{ and} \\ (2)\ L(iP - C) = L((i-1)P - C). \end{cases}$$

For $C \geq 0$ not disjoint from P, there are no functions in $\mathcal{O}$ vanishing on C. We can however compute $\Delta(C)$, as well as the set $\Delta'(C)$, where

$$i \in \Delta'(C) \;\Leftrightarrow\; \begin{cases} (1')\ L(iP) = L((i-1)P), \text{ and} \\ (2')\ L(iP - C) \neq L((i-1)P - C). \end{cases}$$

In general, $\deg C = |\Delta| - |\Delta'|$.

For $C = 2P + Q$,

$$\Delta(2P+Q) = \{0,4,5,8,9,13\},$$
$$\Delta'(2P+Q) = \{6,7,11\}.$$

	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
(1)		$*$				$*$	$*$			$*$	$*$	$*$		$*$	$*$
(2)								$*$	$*$			$*$	$*$	$*$	
(3)	0	1	1	0	0	1	2	1	0	1	2	2	1	0	2

(1) $L(iP) \neq L((i-1)P)$,
(2) $L(iP - C) \neq L((i-1)P - C)$,
(3) $\dim L(iP)/L(iP - C)$.

Bounds for the representation of a fractional O-ideal as quotient of integral ideals.

For any divisor C, and for divisors $D, E \geq 0$ such that $C \sim D - E$, D, E disjoint from P,

$$\deg D \geq |\Delta(C)|, \quad \deg E \geq |\Delta'(C)|.$$

Moreover,

$$\Delta(D) \supseteq \Delta(C), \quad \Delta(E) \supseteq \Delta(-C).$$

For $K = (2g-2)P$,

$$\Delta(-C) = \{K + P - iP : iP \in \Delta'(C)\}.$$

For $D, E \geq 0$ disjoint from P, such that $2P + Q \sim D - E$,

$$\Delta(D) \supseteq \Delta(2P + Q) = \{0, 4, 5, 8, 9, 13\}.$$
$$\Delta(E) \supseteq \Delta(-2P - Q) = \{0, 4, 5\}.$$

The bounds are sharp.

$$2P + Q \sim (3S + 3T) - (Q + 2R).$$

Obtained from the relations

$$5S \sim 5T \sim P + Q + R + S + T.$$

3 – Basic methods to obtain bounds for the minimum distance

AB Method (gives bounds for $d(C)$)

For fiven code C, let A and B be codes of the same length such that

$$A * B \perp C$$

Then, for all nonzero $c \in C$,

$$\mathsf{wt}(c) \geq \mathsf{rank}(c * A) + \mathsf{rank}(c * B).$$

Applying the AB Method..

Let M be a MDS code of type $[n = 5, k = 2]$ with $M \perp M * M$, say

$$M = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3\alpha^4 \\ 1 & \alpha^4 & \alpha^3 & \alpha^2\alpha^1 \end{pmatrix}$$

Let

$$A = B = C = \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}$$

So that $C \perp A * B$. On any seven positions, A and B are of full rank 4. Thus C can not have a word of weight 7 (it is easy to see that the weights of C are $4, 5, 8, 9, 10$).

In general the AB method excludes weights that can occur in C depending on the weight hierarchies of the codes A and B.

The Hartmann-Tzeng and Roos bounds for cyclic codes appear as special cases and use only information about the minimum distances of A and B and their duals.

Let $d_i(A^\perp)$ be the $i-$th weight of $A^\perp$ and let $d_j(B^\perp)$ be the j-th weight of $B^\perp$. Then

$$\text{rank}(c * A) \geq \min\{\text{wt}(c) - (i-1), d_i(A^\perp) - i\}.$$
$$\text{rank}(c * B) \geq \min\{\text{wt}(c) - (j-1), d_j(B^\perp) - j\}.$$

If i and j are such that

$$(i-1) < d_j(B^\perp) - j \quad \text{and} \quad (j-1) < d_i(A^\perp) - i$$

then

$$\text{wt}(c) \leq (i-1)+(j-1) \text{ or } \text{wt}(c) \geq d_i(A^\perp)-i+d_j(B^\perp)-j.$$

ABZ Theorem (D-Park '08)

Let $K + C \sim A + B + Z$, for $Z \geq 0$.

If $C \sim D - E$, for $D, E \geq 0$

such that $D \cap Z = \emptyset$ then

$$\deg D \geq l(A) - l(A - C) + l(B) - l(B - C)$$

$$(= \deg C + \deg Z + l(A) - l(A + Z) + l(B) - l(B + Z))$$

Proof.

We may assume that $D \cap E = \emptyset$. With $E, Z \geq 0$ and $D \cap E = D \cap Z = \emptyset$, the natural maps

$$L(A)/L(A-D) \longrightarrow L(A+E)/L(A+E-D)$$
$$L(B)/L(B-D) \longrightarrow L(B+Z)/L(B+Z-D)$$

are well defined and injective. Therefore

$$\begin{aligned}
&\deg D \ = \\
&= \ l(A+E) - l(A+E-D) + i(A+E-D) - i(A+E) \\
&= \ l(A+E) - l(A+E-D) + l(B+Z) - l(B+Z-D) \\
&\geq \ l(A) - l(A-D) + l(B) - l(B-D) \\
&\geq \ l(A) - l(A-C) + l(B) - l(B-C).
\end{aligned}$$

For the Hermitian curve of degree 5, with $K = 10P$, let $C = 2P + Q$.

For $A = 5P, B = 5P, Z = 2P + Q$, $K + C = A + B + Z$.

Thus, if $C \sim D - E$ for divisors $D, E \geq 0$ with D disjoint from Z then D has degree at least

$$\begin{aligned}\deg D &\geq l(A) - l(A - C) + l(B) - l(B - C) \\ &= l(5P) - l(3P - Q) + l(5P) - l(3P - Q) \\ &= 3 - 0 + 3 - 0 = 6.\end{aligned}$$

The bound is sharp, $3S + 3T \sim (2P + Q) + (Q + 2R)$.

Shift bound (gives bounds for $d_0(C)$)

Let C/C_0 be an extension of $\mathbb{F}$-linear codes with corresponding extension of dual codes D/D_0 such that $\dim C/C_0 = \dim D/D_0 = 1$.

If there exist vectors $a_1, \ldots, a_w$ and $b_1, \ldots, b_w$ such that

$$\begin{cases} a_i * b_j \in D_0 & \text{for } i+j \leq w, \\ a_i * b_j \in D \backslash D_0 & \text{for } i+j = w+1, \end{cases}$$

then $d(C/C_0) \geq w$.

Proof: For a vector $c \in C \backslash C_0$, the vectors $a_1 * c, \ldots, a_w * c$ are linearly independent (with the functionals $b_1, \ldots, b_w$ as witnesses). But then c has weight $\geq w$.

For

$$C_0 = \mathsf{Ev}(x, x^3, x^4, x^7) \ \subset \ C = \mathsf{Ev}(1, x, x^3, x^4, x^7).$$

we can choose

$$\begin{aligned} a_1 = b_1 &= \mathsf{Ev}(x^5), \\ a_2 = b_2 &= \mathsf{Ev}(x^2), \\ a_3 = b_3 &= \mathsf{Ev}(x^7), \\ a_4 = b_4 &= \mathsf{Ev}(x^4). \end{aligned}$$

And $d_0(C) = d(C/C_0) \geq 4$.

Two-variable example

Who can recover $f(0,0)$?

- For $f(x,y) \in \langle 1, x, y, xy, x^2y, y^2, xy^2, x^2y^2 \rangle$.
- For $f(x,y) \in \langle 1, y, y^2, x, xy, xy^2, xy^3, xy^4 \rangle$.

$$f(x,y) \in \langle (1,x), \quad (1,x,x^2)y, \quad (1,x,x^2)y^2 \rangle$$

	b_1	b_2	b_3	b_4	b_5
a_1	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
a_2	$\cdot$	$*$	$*$	$*$	$\cdot$
a_3	$\cdot$	$\cdot$	$*$	$*$	$*$

$$f(x,y) \in \langle (1,y,y^2), \quad (1,y,y^2,y^3,y^4)x \rangle.$$

	b_1	b_2	b_3	b_4	b_5
a_1	$\cdot$	$\cdot$	$*$	$\cdot$	$*$
a_2	$\cdot$	$*$	$*$	$\cdot$	$*$
a_3	$\cdot$	$*$	$\cdot$	$\cdot$	$\cdot$

$C_0 = \mathsf{Ev}(1, x, x^2, y, xy, x^2y, y^2) \ \subset \ C = \langle C_0, \mathsf{Ev}(xy^2) \rangle.$

1	x	y	xy	y^2	xy^2
x	x^2	xy	x^2y	xy^2	
y	xy	y^2	xy^2		
xy	x^2y	xy^2			
y^2	xy^2				
xy^2					

$C_0 = \mathsf{Ev}(1, x, x^2, x^3, x^4, y, xy) \ \subset \ C = \langle C_0, \mathsf{Ev}(x^2y) \rangle.$

1	x	x^2	y	xy	x^2y
x	x^2	1	xy	x^2y	
x^2	x^3	x^4	x^2y		
y	xy	x^2y			
xy	x^2y				
x^2y					

We use the shifting method to show that wt$(c) \geq 6$ for $c \in C_\Omega(K + 2P + Q, D) \backslash C_\Omega(K + 3P + Q, D)$.

We need functions $f_1, \ldots, f_6$ and $g_1, \ldots, g_6$ such that

$$f_i g_j \in L(12P + Q), \quad \text{for } i + j \leq 6.$$
$$f_i g_j \in L(13P + Q) \backslash L(12P + Q), \quad \text{for } i + j = 7.$$

Choose

$$\begin{aligned}
f_1 = g_1 &= 1 \\
f_2 = g_2 &\in L(4P) \backslash L(3P) \\
f_3 = g_3 &\in L(5P) \backslash L(4P) \\
f_4 = g_4 &\in L(8P) \backslash L(7P) \\
f_5 = g_5 &\in L(9P) \backslash L(8P) \\
f_6 = g_6 &\in L(13P) \backslash L(12P)
\end{aligned}$$

The functions $f_1, \ldots, f_6$ and their pole divisors correspond to the Delta set

$$\Delta(2P + Q) = \{0, 4, 5, 8, 9, 13\}$$

Indeed, for a pair f, g with $fg \in L(K+C+P)\backslash L(K+C)$, say

$$f \in L(A)\backslash L(A-P), g \in L(K+C+P-A) \neq L(K+C-A)$$

the divisor A meets the conditions

(1) $L(A) \neq L(A - P)$.
(2) $L(A - C) = L(A - C - P)$.

$$d(C_\Omega(D,G)) \;=$$

$$= \min\{\deg A : 0 \le A \le D \;\wedge\; \Omega(G-A) \neq \Omega(G)\}.$$

Let S and S' be finite sets of primes. For $D \cap S = \emptyset$,

$$0 \le A \le D \;\Rightarrow\; (\forall P \in S)\; L(A) \neq L(A-P).$$

For $c \in C_\Omega(D,G) \setminus \cup_{P \in S'} C_L(D, G+P')$, the support A of c satisfies

$$(\forall P \in S')\; \Omega(G-A) \neq \Omega(G+P'-A)$$

Or, for $G = K + C$,

$$(\forall P \in S')\; L(A-C) \neq L(A-C-P).$$

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

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

Theorem 1 (DKP'09)

Let S, S' be finite sets of points and let Λ be the semigroup 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

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

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

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

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

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

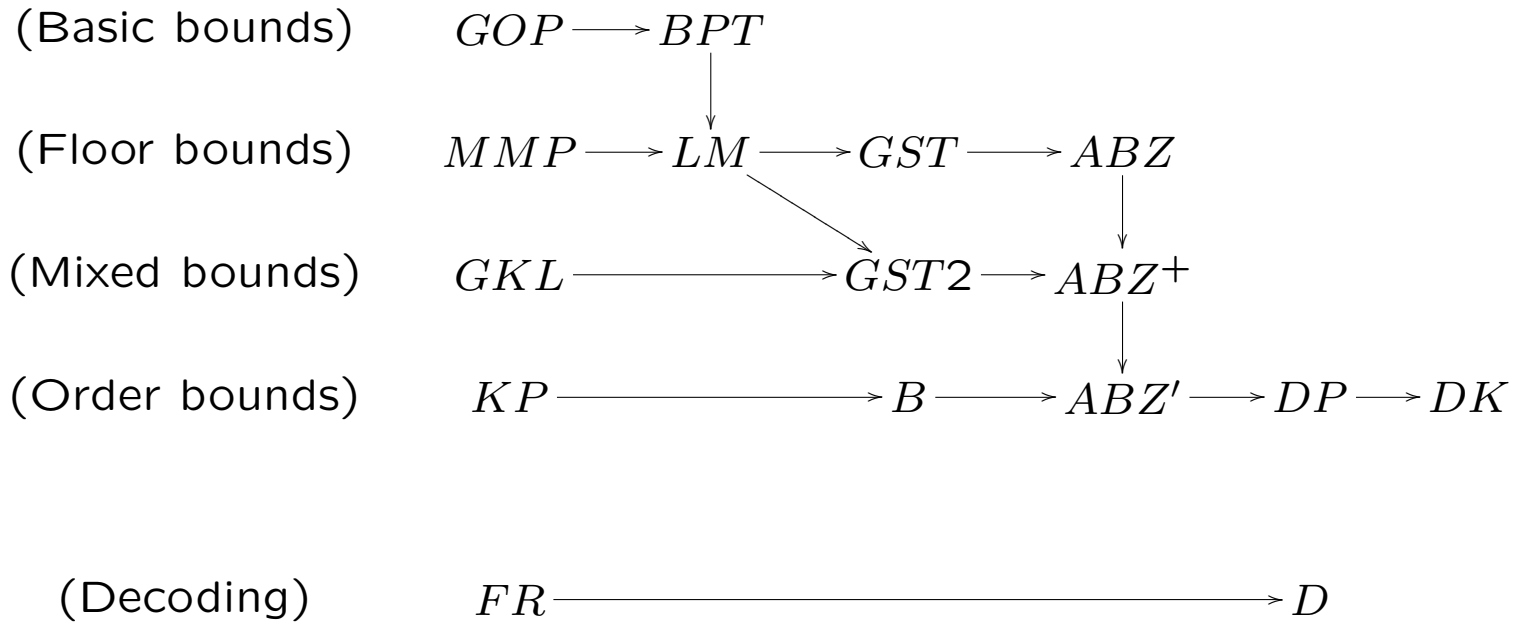
(2) D-Park'08a

(3) D-Kirov'09

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

4 - Comparison and Numerical results

Chart of known bounds



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 $\vdots$ $(m-1)P$	$iP \in \Delta$ $\Leftrightarrow$ $i \geq 0$ and $i - m < 0$
S'	$\{P\}$	
Δ'		$iP \in \Delta'$ $\Leftrightarrow$ $i < 0$ and $i - m \geq 0$
S	$\emptyset$	
$\gamma \geq$	m	

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

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

Suzuki curve over $\mathbb{F}_8$.

$$C = C_\Omega(K - 5P + 8Q, D) \supset C_0 = C_\Omega(K - 4P + 8Q, D).$$

The Beelen bound yields $d(C_0) \geq 7$ and $d(C/C_0) \geq 6$. So that

$$d(C) \geq \min\{d(C/C_0), d(C_0)\} = 6.$$

Using $C_0 = C_\Omega(K - 5P + 9Q, D)$ produces the same numbers (since $13P \sim 13Q$). To improve the distance we only need to analyse words in the subset

$$C_\Omega(K - 5P + 8Q, D) \setminus C_\Omega(K - 4P + 8Q, D) \cup C_\Omega(K - 5P + 9Q, D).$$

The D-Kirov bound yields $\mathrm{wt}(c) \geq 8$ for such words. Thus $d(C) \geq 7$. The bound is sharp and is attained for words with support $A \sim 8Q - P \geq 8Q - 5P$.

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

	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 $\mathbb{F}_{32}$.

Joint work with Radoslav Kirov and Seungkook Park (KIAS)

- 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)
- Distance bounds for algebraic geometric codes (DKP'09)

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

Conclusions / Open problems

General theorems that cover all known bounds.

One of the bounds contains all other known bounds.

Bounds depend heavily on knowledge of multipoint non-gap structure.

Efficient implementations of the bounds available in python, numerical results available online.

Possible extensions: Improved codes, Multipoint codes, Bounds for generic error correction.

Question: What is the maximum $\gamma_\infty(C)$ of $\{\gamma(C; S, S')\}$ taken over all finite sets S, S'.