AG codes defined by divisors with base points

Iwan Duursma

April 1, 2009
AGCT-12, Luminy

Joint work with
Seungkook Park
Radoslav Kirov

Goal

Understand (and along the way improve) all known bounds for the minimum distance of AG codes and for thresholds of AG linear secret sharing schemes (= quotients of AG codes) in the language of divisors

Motivated by work of Homma and Kim (2006) on the minimum distance of Hermitian codes and by work of Chen and Cramer (2006) on secure computation using AG codes

Hamming distance

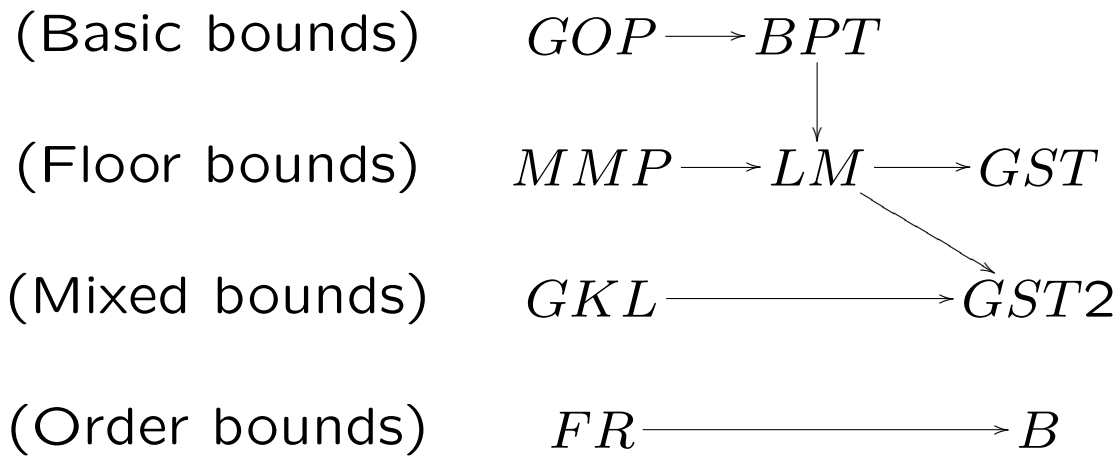
The Hamming distance of two vectors $x, y \in \mathbb{F}^n$ is $d(x, y) = |\{i : x_i \neq y_i, i = 1, 2, \ldots, n\}|$.

(Coding theory)

The minimum distance of a nontrivial code $\mathcal{C} \subseteq \mathbb{F}^n$ is $d(\mathcal{C}) = \min\{d(x, y) : x, y \in \mathcal{C}, x \neq y\}$.

(Secret sharing)

For a proper extension $\mathcal{C}' \subset \mathcal{C}$ of linear codes, the minimum distance of the quotient $\mathcal{C}/\mathcal{C}'$ is $d(\mathcal{C}/\mathcal{C}') = \min\{d(x + \mathcal{C}', y + \mathcal{C}') : x, y \in \mathcal{C}, x - y \notin \mathcal{C}'\}$.



The following codes, constructed with the Suzuki curve over $\mathbb{F}_8$, illustrate that the bounds d_{GST}, d_{GST2} and d_B, are in general not comparable.

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

Base points

$X/\mathbb{F}$ an algebraic curve

C a divisor on X

A point P is a base point of C

if $L(C) = L(C - P)$

Main problem

$X/\mathbb{F}$ an algebraic curve

C a divisor on X

S, S' finite sets of points on X

Give lower bounds for the degree
of divisors D and E such that

$C \sim D - E$

D has no base point in S

E has no base point in S'

Special cases

$C \sim D - E$

D has no base point in S

E has no base point in S'

(Coding theory)

S finite, S' empty

(Secret sharing)

$S = S' = \{P\}$

Remark

If

$$C \sim D - E$$

$$D \geq 0,\ D \cap S = \emptyset$$

$$E \geq 0,\ E \cap S' = \emptyset$$

then

$$C \sim D - E$$

D has no base point in S

E has no base point in S'

Example

Hermitian curve of degree m has lines

$H \sim mP$

$H \sim mQ$

$H \sim P + Q + R_1 + \cdots + R_{m-2}$

Let $C = H - 2P,\ S = S' = \{P\}$.

$C = (H - 2P) - 0$ (not valid)

$C = (2H - 2P) - H$ (valid)

$C = (2H - 2P - 2Q) - (H - 2Q)$ (optimal)

Secret sharing

(Chen and Cramer 2006)

For $f \in L(G)$, and for distinct points $\mathcal{P} = \{P_1, \ldots, P_n\}$ and P, what is the minimal size of a set $A \subset \mathcal{P}$ such that the values of f in A uniquely determine $f(P)$?

$f(P)$ is uniquely determined by $\{f(P_i) : P_i \in A\}$ if and only if

$$L(G - A) = L(G - A - P).$$

Riemann(-Roch):

$$\deg G = 2g + t \;\Rightarrow\; |A| > t.$$

Delta argument

(D'08)

For G of degree $2g + t$, 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

$$L(G - A) = L(G - A - P)$$

$$\Rightarrow |A| \geq |\Delta| > t.$$

Proof of Delta 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 $L(G-A) \neq L(G-A-P)$.

Example

Hermitian curve of degree $m = 5$ and genus $g = 6$

For $G = 14P$ $(t = 2)$,

$\Delta = \{0, 4, 5, 9, 10, 14\} \subseteq \{0, 1, 2, 4, 5, 6, 9, 10, 14\}$

and $|A| \geq 6$.

For $G = 15P$ $(t = 3)$,

$\Delta = \{0, 5, 10, 15\} \subseteq \{0, 1, 2, 3, 5, 6, 7, 10, 11, 15\}$

and $|A| \geq 4$.

Connecting lower bounds for $|A|$ with the problem $C \sim D - E$

We replace the assumption $A \subseteq \mathcal{P}$, $P \notin \mathcal{P}$, with $L(A) \neq L(A - P)$.

For $G = K + P + C$, $L(G - A) = L(G - A - P)$ becomes $L(A - C) \neq L(A - C - P)$.

Thus, $f(P)$ is uniquely determined by $\{f(P_i) : P_i \in A\}$ only if

$C \sim (A) - (A - C)$, such that

A has no base point at P ("A does not know $f(P)$")

$A - C$ has no base point at P ("A can determine $f(P)$")

Semigroups of divisor classes

Define

$\Gamma_P(C) = \{A \in \Gamma_P : A - C \in \Gamma_P\}$

"A does not know $f(P)$ but can determine $f(P)$"

$\Delta_P(C) = \{A \in \Gamma_P : A - C \notin \Gamma_P\}$

"A does not know $f(P)$ and can not determine $f(P)$"

where $\Gamma_P = \{A : L(A) \neq L(A - P)\}$

Restatement of Delta argument

Let

$$\gamma_P(C) = \min\{\deg A : A \in \Gamma_P(C)\}$$

and let

$$\Delta = \{\alpha P : \alpha \in \mathbb{Z}\} \cap \Delta_P(C).$$

Then

$$\gamma_P(C) \geq |\Delta|.$$

Properties of $\Delta_P(C)$

For a curve X of genus g with canonical divisor K,

$$A \in \Delta_P(C) \;\Leftrightarrow\; K + P + C - A \in \Delta_P(C).$$

For $A \in \Delta_P(C)$,

$$\min\{0, \deg C\} \;\leq\; \deg A \;\leq\; \max\{2g-1, \deg C + 2g - 1\}.$$

Geometric Goppa codes

(Goppa 1981)

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

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

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

Goppa bound

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

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

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

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

Grid argument

For $0 \leq A \leq D$ such that $L(G - D + A) \neq L(G - D)$, and for a point P, there exists $i \geq 0$ such that

$$L(G - D + A - iP) \neq L(G - D + A - iP - P)$$
$$L(G - D - iP) = L(G - D - iP - P)$$

If moreover $P \notin D$ then, for $C = D - G + iP$,

$$L(A) \neq L(A - P)$$
$$L(A - C) \neq L(A - C - P)$$

And $|A| \geq \gamma_P(D - G + iP)$.

Moreover, $L(G - D - iP) = L(G - D - iP - P)$ implies that $\gamma_P(D - G + iP) > 0$

(by considering $D - G + iP \sim 0 - (G - D - iP)$).

Feng-Rao type bounds

(D-Park '08)

For a point $P \notin D$,

$d(C_L(D,G)) \geq \min\{\gamma_P(D-G+iP) : i \geq 0\}\backslash\{0\}.$

$d(C_\Omega(D,G)) \geq \min\{\gamma_P(G-K+iP) : i \geq 0\}\backslash\{0\}.$

Improvements

The Delta and Grid arguments use special choices

(Secret sharing)

$$\Delta = \{\underline{\alpha P} : \underline{\alpha \in \mathbb{Z}}\} \cap \Delta_P(C).$$

(Coding theory)

$$d(C_L(D,G)) \geq \underline{\min}\{\gamma_P(D - G + \underline{iP}) : \underline{i \geq 0}\}.$$

In each case the arguments remain valid for more general choices

Generalized order bound (Beelen'07)

Replace $\{\alpha P, \alpha \in \mathbb{Z}\}$ with $\{B + \alpha P, \alpha \in \mathbb{Z}\}$,
for an arbitrary divisor B.

Replace $\{iP, i \geq 0\}$ with an arbitrary increasing sequence.

(D-Park'08), (D-Kirov'09)

Other formats for $\{\alpha P, \alpha \in \mathbb{Z}\}$.

Theorem (D-Kirov-Park'09)

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

$$\Delta = \{i \mid A_i \in \Gamma_{P_i} \wedge A_i - C \notin \Gamma_{P_i}\}$$

$$S = \{i : D \in \Gamma_{P_i}\}$$

$$\Delta' = \{i \mid A_i \notin \Gamma_{P_i} \wedge A_i - C \in \Gamma_{P_i}\}$$

$$S' = \{i : E \in \Gamma_{P_i}\}.$$

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

In particular, $\deg D \geq |\Delta|$ for

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

Lemma

For divisors C, D, and $A_0, \ldots, A_n$, such that $A_i = A_{i-1} + P_i$, consider the statements, for $i = 1, \ldots, n$,

$$\begin{array}{lll} (0) & A_i - D \in \Gamma_{P_i} & \\ (1) & A_i \in \Gamma_{P_i} & (1') \quad A_i - C \in \Gamma_{P_i} \\ (2) & D \in \Gamma_{P_i} & (2') \quad D - C \in \Gamma_{P_i} \end{array}$$

and define subsets

$$\begin{aligned} S_0 &= \{i \mid (0)\}, \\ S_1 &= \{i \mid (1)\}, \\ T_0 &= \{i \mid ((1) \vee \neg(2)) \wedge ((1') \vee \neg(2'))\} \end{aligned}$$

Then $\deg D \geq |S_1| - |S_0| \geq |S_1| - |T_0|$.

Proof of Theorem

Let

$$S_1 = \{i \mid A_i \in \Gamma_{P_i}\}$$
$$T_1 = \{i \mid A_i \in \Gamma_{P_i} \vee D \notin \Gamma_{P_i}\}$$

$$S_1' = \{i \mid A_i - C \in \Gamma_{P_i}\}$$
$$T_1' = \{i \mid A_i - C \in \Gamma_{P_i} \vee D - C \notin \Gamma_{P_i}\}.$$

In general, for $S_1 \subseteq T_1$ and $S_1' \subseteq T_1'$,

$$(S_1 \cup S_1')\backslash(T_1 \cap T_1') = S_1\backslash T_1' \cup S_1'\backslash T_1.$$

We may assume that $D \in \Gamma_{P_i}$ or $D - C \in \Gamma_{P_i}$, and $T_1 \cap T_1' \subseteq S_1 \cup S_1'$.

$$|S_1 \cup S_1'| - |T_1 \cup T_1'| = |S_1 \backslash T_1'| + |S_1' \backslash T_1|$$

$$\begin{aligned} \Leftrightarrow \quad & |S_1| + |S_1' \backslash S_1| - |T_1 \cup T_1'| \\ & = |S_1 \backslash S_1' \cap S'| + |S_1' \backslash S_1 \cap S|. \end{aligned}$$

Now use the lemma with $T_0 = T_1 \cup T_1'$.

Remark

The theorem contains as special cases

(1) Beelen'07
(2) D-Park'08
(3) D-Kirov'09

Assumption	(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		

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

	(1)	(2,3)
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	$\{P\}$	$\{P, Q\}$
	7	8

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

	$(1,2)$	(3)
Δ	$10P - 3Q$	$10P - 3Q$
	$12P - 3Q$	$22P - 3Q$
	$13P - 3Q$	$13P - 3Q$
		$16P - 2Q^*$
	$22P - 3Q$	$22P - 2Q$
	$23P - 3Q$	$23P - 2Q$
	$25P - 3Q$	$25P - 2Q$
S'	$\{P\}$	$\{P, Q\}$
Δ'	$8P - 3Q$	$8P - 3Q$
	$16P - 3Q$	$16P - 3Q$
	$27P - 3Q$	$19P - 2Q$
		$27P - 2Q$
S	$\{P\}$	$\{P\}$
	6	7

Grid vs sequences

Rather than replacing the sequence $\{iP, i \geq 0\}$ with a different sequence, fix the support S' of the sequence and minimize over the semigroup Λ of effective divisors with support in S' (different approach, same bounds).

$$\begin{aligned} & \{D \sim C + E : \\ & \quad D, E \geq 0, D \cap S = \emptyset\} \\ = \; & \cup_{\lambda \in \Lambda} \{D \sim C + \lambda + E : \\ & \quad D, E \geq 0, D \cap S = E \cap S' = \emptyset\} \end{aligned}$$

Improvements are obtained when the subsets in the partition have better lower bounds than the original set.

Generalized Feng-Rao type bounds

(D-Kirov-Park'09)

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

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

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

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

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

Grid for $C = 2P + 2Q$

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

(Beelen'07)

	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				

(D-Park'08)

	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				

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

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

(D-Park'08)

	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				

(D-Kirov'09)

	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				

Floor bounds

Floor bounds are bounds of a different type that use no grid and that are easy to obtain. In special cases floor bounds give better results than the generalized order bound in (Beelen'07).

We first prove the ABZ bound as a new best bound of floor type. We then formulate an order type bound ABZ' that includes both the ABZ bound and the Beelen order bound.

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

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

Remark

When applied to $C = D - G$ or $C = G - K$ the theorem includes as special cases minimum distance bounds for AG codes in

(1) Maharaj, Matthews and Pirsic (2005)
(2) Lundell and McCullough (2006)
(3) Guneri, Stichtenoth and Taskin (2009)

Assumption	(1)	(2)	(3)	(ABZ)
$L(B+Z) = L(B)$	Y	Y	Y	
$L(A+Z) = L(A)$	Y	Y		
$A = B$	Y			

For $Z = 0$, the theorem returns the trivial $\deg D \geq \deg C$.

Remark

The proof has two inequalities. The first is essentially a linear algebra argument (first) used by C. Roos (1983) and baptized AB method by vanLint and Wilson (1986).

ABZ Theorem for cosets (D-Park'08)

The format

$$\Delta = (\{B+\alpha P : \alpha \leq 0\} \cup \{B + Z + \alpha P : \alpha > 0\}) \cap \Delta_P(C)$$

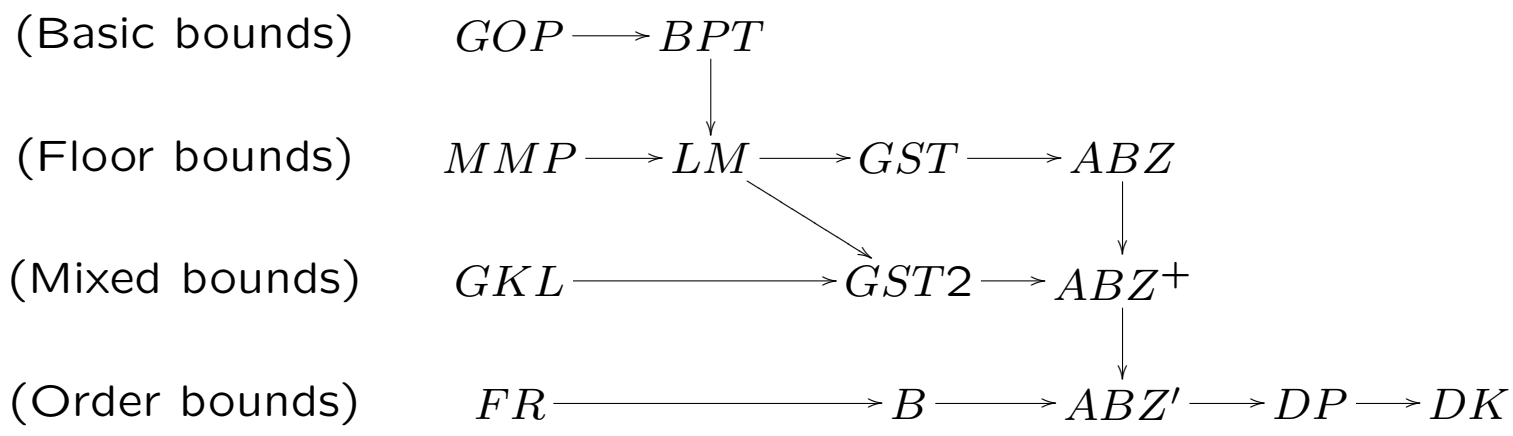
unifies the Beelen order bound (case $Z = 0$) and the ABZ theorem.

For $G = K + C = A + B + Z$, $Z \geq 0$,

$$|\Delta| = |(\{A+\alpha P : \alpha \leq 0\} \cap \Delta_P(C)| + |\{B + \alpha P : \alpha \leq 0\}) \cap \Delta_P(C)|$$

$$\geq l(A) - l(A - C) + l(B) - l(B - C).$$

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

Two-point nongaps

Let P, Q be distinct points on X.

(Joe Harris 1985)

The subsemigroup $H(P,Q) \subset \mathbb{N} \times \mathbb{N}$ consists of all ordered pairs (a,b) such that there exists a rational function with polar divisor $aP + bQ$.

(Seon Jeong Kim 1994)

$$\Gamma(P,Q) = \{(a,b) \in H(P,Q) : \text{for given } a,b \text{ is minimal with } (a,b) \in H(P,Q)\}.$$

d-function, definition

For distinct points P and Q, there is a well defined function $d : \mathbb{Z} \longrightarrow \mathbb{Z}$ such that

$$aP + bQ \in \Gamma_P \;\Leftrightarrow\; a + b \geq d(a).$$

Clearly, $0 \leq d(a) \leq 2g$. Also, for $mP \sim mQ$, $d(a)$ only depends on a modulo m, and d is well-defined as a function

$$d : \mathbb{Z}/m\mathbb{Z} \longrightarrow \{0, 1, \ldots, 2g\}.$$

d-function, properties

The following are equivalent

$a + b = d(a)$

$aP + bQ \in \Gamma_P$ and $aP + bQ - Q \notin \Gamma_P$,

$aP + bQ \in \Delta_P(Q)$

$aP + bQ \in \Delta_Q(P)$

$(a, b) \in \Gamma(P, Q)$ (for $a, b \geq 0$)

Discrepancies

Denote by $D(P,Q)$ the set $\Delta_P(Q) = \Delta_Q(P)$, We call $A \in D(P,Q)$ a discrepancy.

To describe the $d-$function for points P and Q on a curve, we give the m inequivalent divisor classes in $D(P,Q)$ with support in P and Q.

Hermitian curve

$X/\mathbb{F}_{q^2} : y^q + y = x^{q+1}$

For $P, Q \in X(\mathbb{F}_{q^2})$, $mP \sim mQ$ for $m = q + 1$

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

$$dH - dP - dQ, \quad \text{for } d = 0, 1, \ldots, q.$$

Theorem (D-Park'08)

Let $C = dH - aP - bQ$, for $d \in \mathbb{Z}$, and for $0 \leq a, b \leq q$.

$(a, b \leq d)$	$\gamma_P(C) \;=\; \gamma_Q(C) \;=\; \deg C.$
$(b \leq d \leq a)$	$\gamma_P(C) \;\geq\; \deg C + a - d.$
$(a \leq d \leq b)$	$\gamma_Q(C) \;\geq\; \deg C + b - d.$
$(d \leq a \leq b, a < q)$	$\gamma_P(C) \;\geq\; \deg C + a - d + b - d.$
$(d \leq b \leq a, b < q)$	$\gamma_Q(C) \;\geq\; \deg C + a - d + b - d.$
$(d \leq a = b = q)$	$\gamma_P(C) \;=\; \gamma_Q(C) \;\geq\; \deg C + q - d.$

Suzuki curve

$X/\mathbb{F}_q : y^q + y = x^{q_0}(x^q + x)$, for $q = 2q_0^2$.

The curve has $q^2 + 1$ rational points and genus $g = q_0(q-1)$.

For any two rational points P and Q there exists a function with divisor $(q + 2q_0 + 1)(P - Q)$.

Let $m = q + 2q_0 + 1 = (q_0 + 1)^2 + {q_0}^2$, and let H be the divisor class containing $mP \sim mQ$.

The divisor H is very ample and gives an embedding of the Suzuki curve in P^4 as a smooth curve of degree m.

The canonical divisor $K \sim 2(q_0 - 1)H$.

Suzuki curve, discrepancies

Let

$$D_0 = H - (2q_0 + 1)P - Q,$$

$$D_1 = H - (q_0 + 1)(P + Q),$$

$$D_2 = H - P - (2q_0 + 1)Q.$$

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

$iD_0 + jD_2$, for $0 \leq i, j \leq q_0$, and

$D_1 + i'D_0 + j'D_2$, for $0 \leq i', j' \leq q_0 - 1$.

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

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

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

(Chen and Cramer 2006)

For a divisor G of degree $\deg G = 2g + t$, for a set of rational points $\mathcal{P} = \{P_1, \ldots, P_n\}$, and for a rational point $P_0 \notin \mathcal{P}$, such that $3t + 4g < n \leq N - 1$, the AG linear secret sharing scheme with functions $f \in L(G)$, secret $f(P_0)$, and shares $\{f(P_i) : P_i \in \mathcal{P}\}$ has the properties

(1) all subsets of size t or less are rejected, and
(2) products of secrets can be reconstructed from any $n - t$ products of shares.

In particular, secure multi-party computation for an increasing number of participants can be realizd over a small base field using asymptotically good families of curves.

Joint work with Seungkook Park and Radoslav Kirov

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`