Lower Bounds on Distances of Improved Two-Point Codes

Radoslav Kirov

University of Illinois, Urbana-Champaign

July 21, 2009

joint work with Iwan Duursma

Algebraic Geometric (Goppa) Codes

$\mathcal{X}/\mathbb{F}_q$ - an algebraic curve (absolutely irreducible, smooth, projective).
$P_1, P_2, \ldots, P_n$ distinct rational points on $\mathcal{X}$.
$D = P_1 + P_2 + \ldots + P_n$
G - divisor with disjoint support from D.

Definition

$$\alpha_{ev} : L(G) \longrightarrow \mathbb{F}_q^n \qquad f \mapsto (f(P_1), \ldots, f(P_n))$$
$$\alpha_{res} : \Omega(G - D) \longrightarrow \mathbb{F}_q^n \qquad \omega \mapsto (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega))$$

Definition (AG Codes)

$$\mathcal{C}_L(D, G) = \mathrm{im}(\alpha_{ev})$$
$$\mathcal{C}_\Omega(D, G) = \mathrm{im}(\alpha_{res})$$

Basic Properties of AG Codes

- $\mathcal{C}_L(D,G)$ and $\mathcal{C}_\Omega(D,G)$ are dual codes (residue theorem).
- Length: $\deg(D) = n$.
- Dimension of $\mathcal{C}_L(D,G)$:

$$k = \dim L(G) - \dim L(G-D).$$

- Dimension of $\mathcal{C}_\Omega(D,G)$:

$$\begin{aligned} k &= \dim \Omega(G-D) - \dim \Omega(G) \\ &= \dim L(K-G+D) - \dim L(K-G) \end{aligned}$$

where K is the canonical divisor.

Set divisor $C = D - G$ for $\mathcal{C}_L$ and $C = G - K$ for $\mathcal{C}_\Omega$. Now both $\mathcal{C}_L$ and $\mathcal{C}_\Omega$ can be viewed as the same construction.

Observation

$\alpha_* \; : \; L(D - C) \; \longrightarrow \; \mathbb{F}_q^n$ with $\ker(\alpha_*) = L(-C)$.

Notation: $\mathcal{C}(C, D)$ - both evaluation and residue codes with given C and D.

Observation

$$
\begin{aligned}
k(\mathcal{C}(C,D)) &= \dim L(D-C) - \dim L(-C) \\
d(\mathcal{C}(C,D)) &= \min\{\deg(A) : 0 \le A \le D,\ L(A-C) \ne L(-C)\} \\
\min \mathrm{wt}(\mathcal{C}(C,D) \backslash \mathcal{C}(C+P,D)) &= \\
&= \min\{\deg(A) : 0 \le A \le D,\ L(A-C) \ne L(A-C-P)\}
\end{aligned}
$$

Gaps and semi-groups

D-divisor
P-point

Definition

P is a basepoint for D if $L(D) = L(D - P)$.

Theorem

P is not a basepoint for A and B, then P not a basepoint for $A + B$. Denote the semigroup of all divisor that don't have P as basepoint - Γ_P.

Definition

If S is a set of points, we write $\Gamma_S = \bigcap_{P \in S} \Gamma_P$.

By convention $\Gamma_\emptyset = \Gamma = \{D : \dim L(D) > 0\}$ (i.e. all effective divisor classes).

Geometric Distances

$D = P_1 + \ldots + P_n$
Let S be a set of points s.t. $S \cap D = \emptyset$
$0 \leq A \leq D \implies L(A) \neq L(A - P)$ for all $P \notin S$.

Definition ("Geometric Distance")

$\gamma(C; S, S') = \min\{\deg(A) : A \in \Gamma_S \text{ and } A - C \in \Gamma_{S'}\}$

Lemma (Distance Bounds)

Given $S \cap D = \emptyset$

$$\gamma(C; S, \emptyset) \leq d(\mathcal{C}(C, D))$$

$$\gamma(C; S, \{P\}) \leq min\ wt(\mathcal{C}(C, D) \backslash \mathcal{C}(C + P, D)).$$

Questions

- How to use geometry to get a bound on $\gamma(C, S, S')$?
- What are the connections between $\gamma(C, S, S')$ with different S'.

Feng-Rao Method for One Point Codes: Statement

Fix a point P outside $D = P_1 + P_2 + \ldots + P_n$.
Λ-Weierstrass numerical semigroup at P
$i \in \Lambda$ if $L((i-1)P) \neq L(iP)$ (i.e. all one point non-gaps).

Theorem (Feng-Rao'95)

$$d(\mathcal{C}_\Omega(iP, D)) \geq \min\{v_j : j > i\}$$

$$v_j = \{k \in \mathbb{N}_0 : k \in \Lambda \; and \; j - k \in \Lambda\}$$

Feng-Rao Method can be viewed as a Two Step Process:

- Find bounds for cosets (v_j are $\gamma((j-1)P; \{P\}, \{P\})$ in disguise).
- Combine coset bounds to get bound for the code.

Example: Hermitian Curve over $\mathbb{F}_{16}$

- P - any point.
- genus - 6
- Weierstrass semigroup generated by $4, 5$.
- blue gaps.
- green non-gaps.

$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$

min $\mathrm{wt}(\mathcal{C}(14P)\backslash\mathcal{C}(15P)) =?$

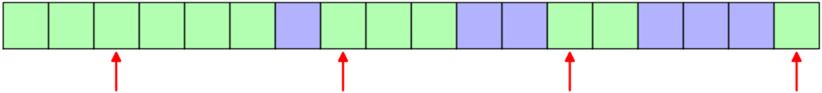
Example: Hermitian Curve over $\mathbb{F}_{16}$

- P - any point.
- genus - 6
- Weierstrass semigroup generated by $4, 5$.
- blue gaps.
- green non-gaps.

$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$

min wt$(\mathcal{C}(14P)\backslash\mathcal{C}(15P)) =?$

$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$



min wt$(\mathcal{C}(14P)\backslash\mathcal{C}(15P)) = 4$

Step II: Example

Using Step I, for all v_i we get:

D	$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$	$21P$	$22P$
$d(\mathcal{C}(D)\setminus\mathcal{C}(D+P))$	0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12

$d(\mathcal{C}(12P)) = ?$

Step II: Example

Using Step I, for all v_i we get:

D	$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$	$21P$	$22P$
$d(\mathcal{C}(D)\setminus\mathcal{C}(D+P))$	0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12

$d(\mathcal{C}(12P)) = ?$

D	$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$	$21P$	$22P$
$d(\mathcal{C}(D)\setminus\mathcal{C}(D+P))$	0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12

$d(\mathcal{C}(12P)) = \min\{6, 6, 4, 5, 8, 9, \ldots\} = 4$

Step II: Example

Using Step I, for all v_i we get:

D	$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$	$21P$	$22P$
$d(\mathcal{C}(D)\backslash\mathcal{C}(D+P))$	0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12

$d(\mathcal{C}(12P)) = ?$

D	$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$	$21P$	$22P$
$d(\mathcal{C}(D)\backslash\mathcal{C}(D+P))$	0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12

$d(\mathcal{C}(12P)) = \min\{6, 6, 4, 5, 8, 9, \ldots\} = 4$

Lemma

$$d(\mathcal{C}_\Omega(iP, D)) = \min_{j \geq i}\{min\ wt(\mathcal{C}_\Omega(jP)\backslash\mathcal{C}_\Omega((j+1)P))\}.$$

D	$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$	$21P$	$22P$
$d(\mathcal{C}(D)\backslash\mathcal{C}(D+P))$	0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12

Suppose we want biggest code with distance $d = 5$.

$d(\mathcal{C}(D)\backslash\mathcal{C}(D+P))$	0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12
D	$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$	$21P$	$22P$

Suppose we want biggest code with distance $d = 5$.

- blue empty cosets
- red cosets to remove (add checks)
- green good cosets

0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12

Best: $G = 15P$, $r = 9 + 1$ hidden(constants)

Definition

Redundancy of an AG code is the number of checks required to obtain the given code (i.e. dimension of the dual code).

D	$0P$	$1P$	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$11P$	$12P$	$13P$	$14P$	$15P$	$16P$	$17P$	$18P$	$19P$	$20P$	$21P$	$22P$
$d(\mathcal{C}(D)\backslash\mathcal{C}(D+P))$	0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12

Suppose we want biggest code with distance $d = 5$.

- blue empty cosets
- red cosets to remove (add checks)
- green good cosets

0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12

Best: $G = 15P$, $r = 9$ +1 hidden(constants)

Definition

Redundancy of an AG code is the number of checks required to obtain the given code (i.e. dimension of the dual code).

Q:Can we reduce the redundancy?
A:Yes, if we don't only take sequential checks. (Exploit the lack of monotonicity in the chain $\mathcal{C}_*(iP, D)$)

Improved One-Point Codes: Example and Definition

Definition

Improved one-point codes for a given distance d is the code obtained by removing only the cosets(adding checks) where $v_i < d$.

Note: such codes no longer have the form $\mathcal{C}_*(iP, D)$.
Example:

0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12

Improved one-point code with $d = 5$ here has $r = 7$ $+1$(constants).

Improved One-Point Codes on the Hermitian Curve

Weierstrass semi-group generated by $q, q+1$ over $\mathbb{F}_{q^2}$.
Redundancies for classical and improved one-point codes are known analytically for Hermitian curves.[Bras-Amorós - O'Sullivan]

$$r(t) = \begin{cases} t(2t+1), & \text{if } t \le a/2 \\ (a^2-a)/2 + (a+1)\lfloor \frac{2t}{a+1} \rfloor, & \text{if } a/2 < t < a(\lfloor \frac{2t}{a+1} \rfloor + 1)/2 \\ (a^2-a)/2 + 2t, & \text{if } t \ge a(\lfloor \frac{2t}{a+1} \rfloor + 1)/2. \end{cases}$$

$$\tilde{r}(t) = \begin{cases} t(2t+1) - \sum_{x'=\lceil 2\sqrt{2t+1}-2 \rceil}^{2t-1} (\lfloor \sqrt{x'^2+4x'-8t} \rfloor + \delta_{x't}), & \text{if } t \le a/2 \\ (a^2-a)/2 + (a+1)\lfloor \frac{2t}{a+1} \rfloor & \\ - \sum_{x'=\lceil 2\sqrt{2t+1}-2 \rceil}^{a-2+\lfloor \frac{2t}{a+1} \rfloor} (\lfloor \sqrt{x'^2+4x'-8t} \rfloor + \delta_{x't}), & \text{if } a/2 < t < a(\lfloor \frac{2t}{a+1} \rfloor + 1)/2 \\ (a^2-a)/2 + 2t - \sum_{x'=\lceil 2\sqrt{2t+1}-2 \rceil}^{a-1+\lfloor \frac{2t}{a+1} \rfloor} (\lfloor \sqrt{x'^2+4x'-8t} \rfloor + \delta_{x't}), & \text{if } a(\lfloor \frac{2t}{a+1} \rfloor + 1)/2 \le t \le \frac{a(a+1)}{2} \\ (a^2-a)/2 + 2t, & \text{if } t > \frac{a(a+1)}{2} \end{cases}$$

Not pretty!

Previous Generalizations of Feng-Rao

Definition

We call $\{A_i\}$ a sequence of divisors if $A_{i+1} = A_i + P_i$ for some point P_i.

Previous attempts to generalize Feng-Rao beyond one-point codes.

- Beelen'07
- Duursma-Park'08

bound	divisor	Step I sq	Step II sq
FR	kP	$\{iP\}$	$\{iP\}$
Beelen	any	$\{iP\}$	any
DP	any	any	any

Duursma - K. Method

Key Features:

- Step I: Instead of cosets uses finer subset.
- Step II: the same, combine subsets to get distance (or coset) bounds.
- Proof: One unifying theorem with all previous methods (Feng-Rao, Beelen, Duursma-Park, Duursma-K.) being consequences.

Statement Step I

$\gamma(C; S, S') = \min\{\deg(A) : A \in \Gamma_S \text{ and } A - C \in \Gamma_{S'}\}$

Theorem (Main Theorem (Technical))

(Roughly) Any sequence of divisors A_i gives a bound for $\gamma(C; S, S')$ by careful counting.

Lemma (Direct Consequence of Main Theorem)

Let A_i be a sequence with support in S. Then $\gamma(C; S, S) \geq |\{i : A_i \in \Gamma_{P_i} \text{ and } A_i - C \notin \Gamma_{P_i}\}|$

Observation

$$\gamma(C; S, S') \leq \min \operatorname{wt}(\mathcal{C}(C) \setminus \bigcup_{P \in S'} \mathcal{C}(C + P))$$

Statement Step II

Lemma

$$\gamma(C; S, S' \backslash P) = \min_{i \geq 0} \gamma(C + iP; S, S')$$

$$\gamma(C; S, \emptyset) = \min_{D \in \Lambda} \gamma(C + D; S, S')$$

where Λ is the semigroup of positive divisors generated by S'.

What were those γ's again?

- γ is a geometric lower bound for a subset of code.
- The subset is an intersections of certain cosets.
- To get the "right" generalization of Feng-Rao we need to go to finer sets than cosets.
- Codes and cosets can be reconstructed by taking unions of those subsets.

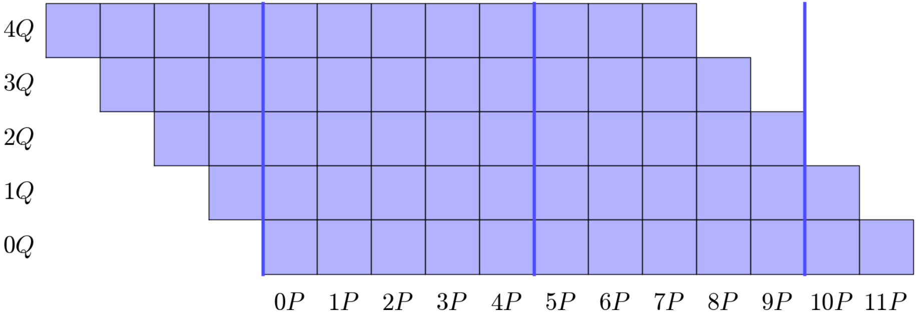
Connection with codes:

Observation

$$\gamma(C; S, S') \leq d(\mathcal{C}(C, D) \backslash \bigcap_{P \in S'} \mathcal{C}(C + P, D)) \text{ given } S \cap D = \emptyset$$

Example: two-point codes on Hermitian $\mathbb{F}_{16}$

curve - Hermitian over $\mathbb{F}_{16}$
P, Q - any two points
$D = P_1 + P_2 + \ldots + P_n$, where $P_i \notin P, Q$.
$C = aP + bQ$ Since $5P \sim 5Q$, $b < 5$.

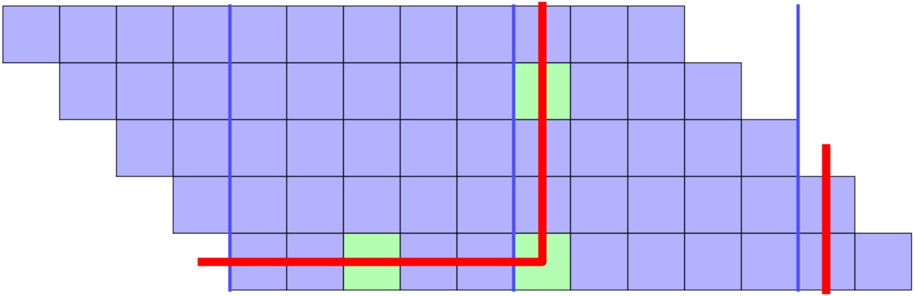


Step I: Example

$$\gamma(C; \{P, Q\}, \{P, Q\}) \leq \min \mathrm{wt}(\mathcal{C}(C) \setminus \mathcal{C}(C + P) \cup \mathcal{C}(C + Q))$$

Fixing C

1. Pick a divisor sequence A_i (ie. a path in the grid).
2. Count number of i where $A_i \in \Gamma_{P_i}$ and $A_i - C \notin \Gamma_{P_i}$ where $P_i = P$ or Q depending whether we took a vertical or horizontal step.
3. $\gamma(C; \{P, Q\}, \{P, Q\})$ is bounded below by that number



$\gamma(C; S, S')$'s with $S = S' = \{P, Q\}$ for Hermitian $\mathbb{F}_{16}$

1	1	1	1	2	2	2	3	2	3	3	5	5	3	4	7	8	7	8	9	11	11	12	13	14	15				
	0	0	1	2	2	2	2	3	4	4	4	4	5	6	6	7	6	7	8	10	10	11	12	13	14	15			
		0	1	0	0	0	2	2	3	3	3	4	5	6	6	6	7	8	9	9	9	10	11	12	13	14	15		
			1	0	0	0	2	2	0	0	3	4	3	4	4	6	6	7	8	8	9	10	11	12	12	13	14	15	
				0	0	0	2	2	0	0	3	4	3	0	4	6	6	4	5	8	9	8	9	10	12	12	13	14	15

- Analytic form available for all q.
- The bounds are sharp (by explicit construction of a divisor matching the bound).
- Best bound always achieved with a straight path.

Step II: Example

Q: What is the distance of the coset $\mathcal{C}(2Q-P)\backslash\mathcal{C}(3Q-P)$

3	5	5	3	4	7	8	7	8	9	11	11	12	13	14	15				
	4	4	5	6	6	7	6	7	8	10	10	11	12	13	14	15			
		4	5	6	6	6	7	8	9	9	9	10	11	12	13	14	15		
			3	4	4	6	6	7	8	8	9	10	11	12	12	13	14	15	
				0	4	6	6	4	5	8	9	8	9	10	12	12	13	14	15

A: 5

Step II: Example

Q: What is the distance of the coset $\mathcal{C}(2Q-P)\backslash\mathcal{C}(3Q-P)$

3	5	5	3	4	7	8	7	8	9	11	11	12	13	14	15				
	4	4	5	6	6	7	6	7	8	10	10	11	12	13	14	15			
		4	5	6	6	6	7	8	9	9	9	10	11	12	13	14	15		
			3	4	4	6	6	7	8	8	9	10	11	12	12	13	14	15	
				0	4	6	6	4	5	8	9	8	9	10	12	12	13	14	15

A: 5

Q: What is the distance for whole code $\mathcal{C}(2Q-P)$.

3	5	5	3	4	7	8	7	8	9	11	11	12	13	14	15				
	4	4	5	6	6	7	6	7	8	10	10	11	12	13	14	15			
		4	5	6	6	6	7	8	9	9	9	10	11	12	13	14	15		
			3	4	4	6	6	7	8	8	9	10	11	12	12	13	14	15	
				0	4	6	6	4	5	8	9	8	9	10	12	12	13	14	15

A: 3

Improved Two Point Codes

We need cosets to talk about redundancies, and consequently improved codes. Two choices:

- Obtain all coset bounds on the grid and then find best path.
  or
- Directly use $\gamma(C, \{P, Q\}, \{P, Q\})$ to choose an optimal path.

We will demonstrate the second option.

Improved Codes from $\gamma(C, \{P, Q\}, \{P, Q\})$ table

$$0 \rightarrow P \rightarrow P + Q \rightarrow P + 2Q$$

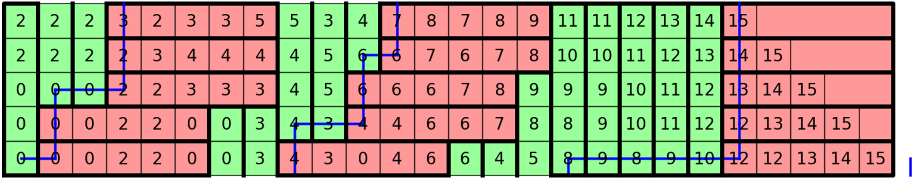
Lemma

If $mP \sim mQ$ then $\gamma(C, \{P, Q\}, \{P, Q\}) \leq \gamma(C + mP, \{P, Q\}, \{P, Q\})$

2	2	2	3	2	3	3	5	5	3				
2	2	2	2	3	4	4	4	4	5	6			
0	0	0	2	2	3	3	3	4	5	6	6		
0	0	0	2	2	0	0	3	4	3	4	4	6	
0	0	0	2	2	0	0	3	4	3	0	4	6	6

blue - path red - Q step (coset) green - P step (coset)

Full Path



Coset bounds along that path:

0	0	0	0	0	2	2	2	0	4	3	4	6	4	6	7	8	9	8	9	10	12	12	13	14	15

Ex: This gives improved code with $d = 5$ and $r = 7$ $(+1)$.
This happens to be maximal, but also achievable by one-point improved codes.

Results: Distances vs. redundancies

nCl - Classical n-point code nIm - Improved n-point code

$$1Cl \geq \{1Im, 2Cl\} \geq 2Im$$

Hermitian over $\mathbb{F}_{16}$

Low is better!

$d \backslash r$	$1Cl$	$1Im$	$2Cl$	$2Im$	$impr$
3	3	3	3	3	0
4	6	5	6	5	0
5	10	8	8	8	0
6	11	9	8	8	0
7	11	11	10	10	0
8	11	11	11	11	0
9	14	13	13	13	0
10	15	15	14	14	0
11	16	16	15	15	0

$$impr = \min\{2Cl, 1Im\} - 2Im$$

Hermitian over $\mathbb{F}_{64}$

$d \backslash r$	$1Cl$	$1Im$	$2Cl$	$2Im$	$impr$
5	10	8	10	8	0
7	21	14	21	14	0
9	36	20	30	20	0
11	37	24	30	23	1
13	37	28	30	27	1
15	37	30	36	29	1
17	44	35	39	35	0
19	46	39	39	37	2
21	46	41	39	39	0
23	46	43	45	42	1
25	52	47	48	47	0
27	54	50	48	48	0
29	55	53	52	50	2
31	55	55	54	54	0

Suzuki over $\mathbb{F}_{32}$

$d \backslash r$	$1Cl$	$1Im$	$2Cl$	$2Im$	$impr$
21	128	79	97	77	2
23	128	82	98	80	2
25	128	95	101	93	2
27	128	100	103	96	4
29	128	102	103	99	3
31	128	102	103	101	1
33	156	112	131	108	4
35	156	116	131	111	5
37	160	123	131	119	4
39	160	123	134	121	2
41	164	128	134	125	3
43	165	132	134	127	5
45	165	136	138	132	4
47	165	138	138	135	3
49	165	144	141	140	1

Giulietti-Kochmáros over $\mathbb{F}_{729}$

$d \backslash r$	$1Cl$	$1Im$	$2Cl$	$2Im$	im
29	127	88	114	84	4
31	127	92	114	90	2
33	127	94	114	92	2
35	127	96	114	94	2
37	127	102	121	101	1
39	127	105	121	104	1
41	127	109	121	108	1
43	141	114	135	112	2
45	141	115	135	114	1
47	141	119	135	118	1
49	147	124	135	122	2
51	148	127	142	124	3
53	148	129	142	128	1
55	153	133	142	131	2
57	155	137	149	134	3
59	155	138	149	135	3

$d \backslash r$	$1Cl$	$1Im$	$2Cl$	$2Im$	im
61	155	143	149	141	2
63	155	144	155	143	1
65	162	147	156	144	3
67	162	149	156	148	1
69	162	151	162	151	0
71	169	156	163	154	2
73	169	160	163	156	4
75	169	160	163	158	2
77	175	164	170	163	1
79	176	167	170	165	2
81	176	169	170	167	2
83	181	171	176	169	2
85	183	176	177	171	5
87	183	178	177	175	2
89	183	178	182	177	1
91	189	181	184	179	2

Open Problems / Future Work

- Is the path $iP + Q$ always optimal for improved two point codes on Hermitian curves? True for $\mathbb{F}_{16}$ and $\mathbb{F}_{64}$ for all d.
- How to find the best path in general.
- Decoding based on our generalization of Feng-Rao.
- Can we construct improved codes based directly on the subset bounds (maybe non-linear).

Online Resources

All data is availble at **http://agtables.appspot.com**

Parameters on Algebraic Geometric Codes

Curve
- Suzuki over F_8
- Suzuki over F_32
- Hermitian over F_16
- Hermitian over F_64 (selected)
- Klein over F_8
- GK over F_64
- GK over F_729

Bounds
- Threshold/Cosets
- Distances (selected)

Order Bound Methods
- Duursma-Kirov [ref] (checked)
- Duursma-Park [ref]
- Beelen [ref]

Floor Bound Methods
- ABZ [ref]
- Güneri-Stichtenoth-Taşkın [ref]
- Lundell-McCullough [ref]

Degree and Q support of C

0≤ 0 ≤deg≤ 10 ≤56

0≤ 0 ≤Cq≤ 8 ≤8

Canonical Divisor = 54P~54Q

Get Table!

degC\Cq	0	1	2	3	4	5	6	7	8
0 DK	0	7	7	7	7	7	7	7	7
1 DK	8	8	7	7	7	7	7	7	7
2 DK	8	8	8	7	7	7	7	7	7
3 DK	8	14	14	8	7	7	7	7	7
4 DK	8	14	14	14	8	7	7	7	7
5 DK	8	14	14	14	14	8	7	7	7
6 DK	8	14	14	14	14	14	8	7	7
7 DK	8	14	14	14	14	14	14	8	7
8 DK	8	14	14	14	14	14	14	14	8
9 DK	9	15	14	14	14	14	14	14	15
10 DK	16	16	15	14	14	14	14	14	15

Highest numbers is a row are marked in red.

M. Bras-Amorós, M. O'Sullivan, "On Semigroups Generated by Two Consecutive Integers and Improved Hermitian Codes", *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2560-2566, 2007.

G.-L. Feng and T. R. N. Rao, "Improved geometric Goppa codes. I. basic theory, Special issue on algebraic geometry codes," *IEEE Trans. Inf. Theory*, vol. 41, pt. 1, pp. 1678-1693, 1995.

M. Homma and S. J. Kim. "The complete determination of the minimum distance of two-point codes on a Hermitian curve." *Des. Codes Cryptogr.*, 40(1):524, 2006.