Relative generalized Hamming weights of one-point algebraic geometric codes: an application to secret sharing

INdAM meeting: International meeting on numerical semigroups
Cortona 2014, September 10th.

Diego Ruano
http://people.math.aau.dk/~diego/
(Joint work with Olav Geil, Stefano Martin, Ryutaroh Matsumoto, Yuan Luo)

AALBORG UNIVERSITY
DENMARK

Reference

O. Geil, S. Martin, R. Matsumoto, D. Ruano, Y. Luo: “Relative generalized Hamming weights of one-point algebraic geometric codes”. To appear in *IEEE Transactions on Information Theory.* (available at arXiv:1403.7985)

- O. Geil, S. Martin: Aalborg University, Denmark.
- R. Matsumoto: Tokyo Institute of Technology, Japan.
- Y. Luo: Shanghai Jiao Tong University, China.

Ramp secret sharing schemes

A ramp secret sharing scheme

with t-privacy and r-reconstruction is an algorithm that,

1. given an input $\vec{s} \in \mathbb{F}_q^\ell$
2. outputs a vector $\vec{x} \in \mathbb{F}_q^n$, the vector of shares that we want to share among n players

such that, given a collection of shares $\{x_i \mid i \in \mathcal{I}\}, \mathcal{I} \subseteq \{1, \ldots, n\}$,

1. one has no information about $\vec{s}$ if $\#\mathcal{I} \leq t$
2. one can recover $\vec{s}$ if $\#\mathcal{I} \geq r$

Ramp secret sharing schemes

A ramp secret sharing scheme

with t-privacy and r-reconstruction is an algorithm that,

1. given an input $\vec{s} \in \mathbb{F}_q^\ell$
2. outputs a vector $\vec{x} \in \mathbb{F}_q^n$, the vector of shares that we want to share among n players

such that, given a collection of shares $\{x_i \mid i \in \mathcal{I}\}, \mathcal{I} \subseteq \{1, \ldots, n\}$,

1. one has no information about $\vec{s}$ if $\#\mathcal{I} \leq t$
2. one can recover $\vec{s}$ if $\#\mathcal{I} \geq r$

We shall always assume that t is largest possible and that r is smallest possible such that the above hold.

Example: Ramp Shamir's scheme

- $\vec{s} = (s_0, \ldots, s_{\ell-1}) \in \mathbb{F}_q^{\ell}$ a secret
- n participants
- Reconstruction $r = k$, privacy $t = k - \ell$.

Example: Ramp Shamir's scheme

- $\vec{s} = (s_0, \ldots, s_{\ell-1}) \in \mathbb{F}_q^\ell$ a secret
- n participants
- Reconstruction $r = k$, privacy $t = k - \ell$.

$f_\ell, f_{\ell+1}, \ldots, f_{k-1} \in \mathbb{F}_q$ random

$$f = s_0 + s_1 X + \cdots + s_{\ell-1} X^{\ell-1} + f_\ell X^\ell + \cdots + f_{k-1} X^{k-1} \in \mathbb{F}_q[x]$$

- Shares: $f(x_1), \ldots, f(x_n)$, with $x_i \in \mathbb{F}_q$ and $x_i \neq x_j$.

Example: Ramp Shamir's scheme

- $\vec{s} = (s_0, \ldots, s_{\ell-1}) \in \mathbb{F}_q^\ell$ a secret
- n participants
- Reconstruction $r = k$, privacy $t = k - \ell$.

$f_\ell, f_{\ell+1}, \ldots, f_{k-1} \in \mathbb{F}_q$ random

$$f = s_0 + s_1 X + \cdots + s_{\ell-1} X^{\ell-1} + f_\ell X^\ell + \cdots + f_{k-1} X^{k-1} \in \mathbb{F}_q[x]$$

- Shares: $f(x_1), \ldots, f(x_n)$, with $x_i \in \mathbb{F}_q$ and $x_i \neq x_j$.
- Privacy and reconstruction follows from Lagrange interpolation.

Example: Ramp Shamir's scheme

- $\vec{s} = (s_0, \ldots, s_{\ell-1}) \in \mathbb{F}_q^\ell$ a secret
- n participants
- Reconstruction $r = k$, privacy $t = k - \ell$.

$f_\ell, f_{\ell+1}, \ldots, f_{k-1} \in \mathbb{F}_q$ random

$$f = s_0 + s_1 X + \cdots + s_{\ell-1} X^{\ell-1} + f_\ell X^\ell + \cdots + f_{k-1} X^{k-1} \in \mathbb{F}_q[x]$$

- Shares: $f(x_1), \ldots, f(x_n)$, with $x_i \in \mathbb{F}_q$ and $x_i \neq x_j$.
- Privacy and reconstruction follows from Lagrange interpolation.

Disadvantage: note that $q \geq n$.

Chen *et al.* Ramp secret sharing schemes

- Consider a secret $\vec{s} \in \mathbb{F}_q^\ell$
- $C_2 = \langle \vec{v}_1, \ldots, \vec{v}_{k_2} \rangle \subsetneq C_1 = \langle \vec{v}_1, \ldots, \vec{v}_{k_2}, \vec{v}_{k_2+1}, \ldots, \vec{v}_{k_1} \rangle \subseteq \mathbb{F}_q^n$

Chen *et al.* Ramp secret sharing schemes

- Consider a secret $\vec{s} \in \mathbb{F}_q^\ell$
- $C_2 = \langle \vec{v}_1, \ldots, \vec{v}_{k_2} \rangle \subsetneq C_1 = \langle \vec{v}_1, \ldots, \vec{v}_{k_2}, \vec{v}_{k_2+1}, \ldots, \vec{v}_{k_1} \rangle \subseteq \mathbb{F}_q^n$
- Set $L = \langle v_{K_2+1}, \ldots, v_{k_1} \rangle$, $C_1 = C_2 \oplus L$ (direct sum)
- $\ell = \dim(L) = \dim(C_1/C_2) = k_1 - k_2$

Chen *et al.* Ramp secret sharing schemes

- Consider a secret $\vec{s} \in \mathbb{F}_q^{\ell}$
- $C_2 = \langle \vec{v}_1, \ldots, \vec{v}_{k_2} \rangle \subsetneq C_1 = \langle \vec{v}_1, \ldots, \vec{v}_{k_2}, \vec{v}_{k_2+1}, \ldots, \vec{v}_{k_1} \rangle \subseteq \mathbb{F}_q^n$
- Set $L = \langle v_{K_2+1}, \ldots, v_{k_1} \rangle$, $C_1 = C_2 \oplus L$ (direct sum)
- $\ell = \dim(L) = \dim(C_1/C_2) = k_1 - k_2$

The *n* shares are the *n* coordinates of $\vec{x}$

$$\vec{x} = \vec{c}_2 + \psi(\vec{s}) = a_1\vec{v}_1 + \cdots + a_{k_2}\vec{v}_{k_2} + s_1\vec{v}_{k_2+1} + \cdots + s_\ell\vec{v}_{k_1} \in C_1$$

$a_1, \ldots, a_{k_2} \in \mathbb{F}_q$ random.

Chen *et al.* Ramp secret sharing schemes

- Consider a secret $\vec{s} \in \mathbb{F}_q^\ell$
- $C_2 = \langle \vec{v}_1, \ldots, \vec{v}_{k_2} \rangle \subsetneq C_1 = \langle \vec{v}_1, \ldots, \vec{v}_{k_2}, \vec{v}_{k_2+1}, \ldots, \vec{v}_{k_1} \rangle \subseteq \mathbb{F}_q^n$
- Set $L = \langle v_{K_2+1}, \ldots, v_{k_1} \rangle$, $C_1 = C_2 \oplus L$ (direct sum)
- $\ell = \dim(L) = \dim(C_1/C_2) = k_1 - k_2$

The *n* shares are the *n* coordinates of $\vec{x}$

$$\vec{x} = \vec{c}_2 + \psi(\vec{s}) = a_1\vec{v}_1 + \cdots + a_{k_2}\vec{v}_{k_2} + s_1\vec{v}_{k_2+1} + \cdots + s_\ell\vec{v}_{k_1} \in C_1$$

$a_1, \ldots, a_{k_2} \in \mathbb{F}_q$ random.

Algebraically:

1. $\vec{s}$ is represented by the coset $\psi(\vec{s}) + C_2$ in C_1/C_2
2. q^ℓ different cosets in C_1/C_2 and there are q^{k_2} representatives

How much information is leaked?

Bounds for privacy and reconstruction (Chen *et al.*)

1. $r < n - d(C_1)$
2. $t > d(C_2^{\perp})$

How much information is leaked?

Bounds for privacy and reconstruction (Chen *et al.*)

1. $r < n - d(C_1)$
2. $t > d(C_2^{\perp})$

One can be more precise with the first relative generalized Hamming weight (RGHW)

$$M_1(C_1, C_2) = \min\{wt(c) \mid c \in C_1 \setminus C_2\} \geq d(C_1)$$

How much information is leaked?

Bounds for privacy and reconstruction (Chen *et al.*)

1. $r < n - d(C_1)$
2. $t > d(C_2^\perp)$

One can be more precise with the first relative generalized Hamming weight (RGHW)

$$M_1(C_1, C_2) = \min\{wt(c) \mid c \in C_1 \setminus C_2\} \geq d(C_1)$$

Privacy and reconstruction (Kurihara, Matsumoto *et al.*)

1. $r = n - M_1(C_1, C_2) + 1$
2. $t = M_1(C_2^\perp, C_1^\perp) - 1$

A more precise definition
of the information leaked

Privacy and reconstruction

A ramp secret sharing scheme has $(t_1, \ldots, t_\ell)$-privacy and $(r_1, \ldots, r_\ell)$-reconstruction if $t_1, \ldots, t_\ell$ are chosen largest possible and $r_1, \ldots, r_\ell$ are chosen smallest possible such that:

1. an adversary cannot obtain m q-bits of information about $\vec{s}$ with any t_m shares,
2. it is possible to recover m q-bits of information about $\vec{s}$ with any collection of r_m shares.

In particular, one has $t = t_1$ and $r = r_\ell$.

A more precise definition
of the information leaked

Privacy and reconstruction

A ramp secret sharing scheme has $(t_1, \dots, t_\ell)$-privacy and $(r_1, \dots, r_\ell)$-reconstruction if $t_1, \dots, t_\ell$ are chosen largest possible and $r_1, \dots, r_\ell$ are chosen smallest possible such that:

1. an adversary cannot obtain m q-bits of information about $\vec{s}$ with any t_m shares,
2. it is possible to recover m q-bits of information about $\vec{s}$ with any collection of r_m shares.

In particular, one has $t = t_1$ and $r = r_\ell$.

Exact values (Kurihara, Matsumoto *et al.*) and (Geil *et al.*)

1. $r_m = n - M_{\ell-m+1}(C_1, C_2) + 1$
2. $t_m = M_m(C_2^\perp, C_1^\perp) - 1$

RGHW

$\text{Supp}(D) = \{i \in \{1, \ldots, n\} : \exists \vec{c} \in D, c_i \neq 0\}$
Ex: $\text{Supp} = \{(0,0,1,1,0),(0,1,0,1,1)\} = 4$

Minimum Hamming weight

$$d(C) = \min\{wt(\vec{c}) = \text{Supp}(\vec{c}) \mid \vec{c} \in C\}$$

The *m*th generalized Hamming weight

$$d_m(C) = \min\{|\text{Supp}(D)| : D \subseteq C, \dim(D) = m\}$$

RGHW

$\text{Supp}(D) = \{i \in \{1, \ldots, n\} : \exists \vec{c} \in D, c_i \neq 0\}$
Ex: $\text{Supp} = \{(0,0,1,1,0),(0,1,0,1,1)\} = 4$

Minimum Hamming weight

$$d(C) = \min\{wt(\vec{c}) = \text{Supp}(\vec{c}) \mid \vec{c} \in C\}$$

The *m*th generalized Hamming weight

$$d_m(C) = \min\{|\text{Supp}(D)| : D \subseteq C, \dim(D) = m\}$$

The *m*th relative generalized Hamming weight (RGHW)

$$M_m(C_1, C_2) = \min\{|\text{Supp}(D)| : D \subseteq C, \dim(D) = m, D \cap C_2 = \{\vec{0}\}\}$$

Schemes based on MDS codes

Let C_1, C_2 MDS codes (Reed-Solomon): $C_1^\perp, C_2^\perp$ are also MDS and

- $M_m(C_1, C_2) = d_m(C_1) = n - k_1 + m$
- $M_m(C_2^\perp, C_1^\perp) = d_m(C_2^\perp) = k_2 + m$

Schemes based on MDS codes

Let C_1, C_2 MDS codes (Reed-Solomon): $C_1^{\perp}, C_2^{\perp}$ are also MDS and

- $M_m(C_1, C_2) = d_m(C_1) = n - k_1 + m$
- $M_m(C_2^{\perp}, C_1^{\perp}) = d_m(C_2^{\perp}) = k_2 + m$

Privacy and reconstruction:

$$M_m(C_2^{\perp}, C_1^{\perp}) = n - M_{\ell-m+1}(C_1, C_2) + 1,$$

$$t = t_1 = k_2, \;\; r = r_\ell = k_1.$$

Schemes based on MDS codes

Let C_1, C_2 MDS codes (Reed-Solomon): $C_1^\perp, C_2^\perp$ are also MDS and

- $M_m(C_1, C_2) = d_m(C_1) = n - k_1 + m$
- $M_m(C_2^\perp, C_1^\perp) = d_m(C_2^\perp) = k_2 + m$

Privacy and reconstruction:

$$M_m(C_2^\perp, C_1^\perp) = n - M_{\ell-m+1}(C_1, C_2) + 1,$$

$$t = t_1 = k_2, \; r = r_\ell = k_1.$$

$$t_m = r_m - 1, \; t_{m+1} = t_m + 1.$$

Schemes based on MDS codes

Let C_1, C_2 MDS codes (Reed-Solomon): $C_1^\perp, C_2^\perp$ are also MDS and

- $M_m(C_1, C_2) = d_m(C_1) = n - k_1 + m$
- $M_m(C_2^\perp, C_1^\perp) = d_m(C_2^\perp) = k_2 + m$

Privacy and reconstruction:

$$M_m(C_2^\perp, C_1^\perp) = n - M_{\ell-m+1}(C_1, C_2) + 1,$$

$$t = t_1 = k_2, \;\; r = r_\ell = k_1.$$

$$t_m = r_m - 1, \;\; t_{m+1} = t_m + 1.$$

Since $r - t = k_1 - k_2 = \ell$, it is optimal. However, when the number of participants is large compared to the field size we cannot assume C_1 and C_2 to be MDS.

One-point algebraic geometric codes

- F algebraic function field of transcendence degree one
- $P_1, \ldots, P_n$, Q be distinct rational places in F
- $\mathcal{L}(\mu Q) \subset \mathbb{F}_q(X)$ are rational functions that only have a pole at Q and of order at most μ.

One-point algebraic geometric codes

- F algebraic function field of transcendence degree one
- $P_1, \ldots, P_n$, Q be distinct rational places in F
- $\mathcal{L}(\mu Q) \subset \mathbb{F}_q(X)$ are rational functions that only have a pole at Q and of order at most μ.

- $H(Q) = -\nu_Q\big(\cup_{\mu=0}^{\infty} \mathcal{L}(\mu Q)\big)$ the Weierstrass semigroup of Q.

One-point algebraic geometric codes

- F algebraic function field of transcendence degree one
- $P_1, \ldots, P_n$, Q be distinct rational places in F
- $\mathcal{L}(\mu Q) \subset \mathbb{F}_q(X)$ are rational functions that only have a pole at Q and of order at most μ.

- $H(Q) = -\nu_Q\big(\cup_{\mu=0}^{\infty} \mathcal{L}(\mu Q)\big)$ the Weierstrass semigroup of Q.

- Let $D = P_1 + \cdots + P_n$
- $\mathrm{ev}(f) = (f(P_1), \ldots, f(P_n))$
- $\{f_\lambda \mid \lambda \in H(Q)\}$ with $\rho(f_\lambda) = \lambda$ for all $\lambda \in H(Q)$
- $C_{\mathcal{L}}(D, \mu Q) = \langle \mathrm{ev}(f_0), \ldots, \mathrm{ev}(f_\mu) \rangle$

One-point algebraic geometric codes

- F algebraic function field of transcendence degree one
- $P_1, \ldots, P_n$, Q be distinct rational places in F
- $\mathcal{L}(\mu Q) \subset \mathbb{F}_q(X)$ are rational functions that only have a pole at Q and of order at most μ.

- $H(Q) = -\nu_Q\big(\cup_{\mu=0}^{\infty} \mathcal{L}(\mu Q)\big)$ the Weierstrass semigroup of Q.

- Let $D = P_1 + \cdots + P_n$
- $\text{ev}(f) = (f(P_1), \ldots, f(P_n))$
- $\{f_\lambda \mid \lambda \in H(Q)\}$ with $\rho(f_\lambda) = \lambda$ for all $\lambda \in H(Q)$
- $C_{\mathcal{L}}(D, \mu Q) = \langle \text{ev}(f_0), \ldots, \text{ev}(f_\mu) \rangle$

$$\begin{aligned} H^*(Q) &= \{\mu \mid C_{\mathcal{L}}(D, \mu Q) \neq C_{\mathcal{L}}(D, (\mu - 1)Q)\} \\ &= \{\gamma_1, \ldots, \gamma_n\} \subsetneq H(Q). \end{aligned}$$

(note that $X^q \neq X \in \mathbb{F}_q(X)$ but $\text{ev}(X^q) = \text{ev}(X)$)

Feng-Rao bounds (or order bounds)

The Feng-Rao bound comes in two flavours:

1. The usual one bounds the (generalized) minimum distance of the dual code: $C_{\mathcal{L}}(D, \mu Q)^{\perp}$

   [T. Høholdt, J.H. van Lint, R. Pellikaan: Algebraic geometry of codes. Handbook of coding theory, Vol. I, II, 871-961, 1998.]

2. The Andersen-Geil bound, bounds the the (generalized) minimum distance of the primary code: $C_{\mathcal{L}}(D, \mu Q)$

   [H.E. Andersen, O. Geil: Evaluation Codes from Order Domain Theory. Finite Fields and Their Applications Vol. 14 (1), pp. 92-123 (2008)]

Feng-Rao bound

Proposition

Let $D \subseteq \mathbb{F}_q^n$ be a vector space of dimension m. There exist unique numbers $\gamma_{i_1} < \cdots < \gamma_{i_m}$ in $H^*(Q)$ such that

$$-\nu_Q(D \backslash \{\vec{0}\}) = \{i_1, \ldots, i_m\}$$

The support of D satisfies

$$\#\mathrm{Supp}(D) \quad \geq \quad \#\Big(H^*(Q) \cap \left(\cup_{s=1}^{m} \left(\gamma_{i_s} + H(Q)\right)\right)\Big)$$

Feng-Rao bound

Proposition

Let $D \subseteq \mathbb{F}_q^n$ be a vector space of dimension m. There exist unique numbers $\gamma_{i_1} < \cdots < \gamma_{i_m}$ in $H^*(Q)$ such that

$$-\nu_Q(D\backslash\{\vec{0}\}) = \{i_1, \ldots, i_m\}$$

The support of D satisfies

$$\begin{aligned}\#\mathrm{Supp}(D) &\geq \#\Big(H^*(Q) \cap \big(\cup_{s=1}^m (\gamma_{i_s} + H(Q))\big)\Big)\\ &\geq n - \gamma_{i_m} + \#\{\lambda \in \cup_{s=1}^{m-1}(\gamma_{i_s} + H(Q)) \mid \lambda \notin \gamma_{i_m} + H(Q)\}.\end{aligned}$$

$$\#(H^*(Q) \cap (\cup_{s=1}^m(\gamma_{i_s} + H(Q)))) = n - \#\big(H^*(Q)\backslash \cup_{s=1}^m (\gamma_{i_s} + H(Q))\big)$$

$$\text{and } \lambda = \#\big(\Gamma\backslash(\lambda + \Gamma)\big)$$

$H(Q) = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, \ldots\}$
$H^*(Q) = \{0, 3, 4, 6, 7, \ldots, 26, 28, 29, 32\}$

Let $D \subseteq C_{\mathcal{L}}(D, 20Q)$, $D \cap C_{\mathcal{L}}(D, 16Q) = \{0\}$ and $\dim D = 2$.

$H(Q) = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, \ldots\}$
$H^*(Q) = \{0, 3, 4, 6, 7, \ldots, 26, 28, 29, 32\}$

Let $D \subseteq C_{\mathcal{L}}(D, 20Q)$, $D \cap C_{\mathcal{L}}(D, 16Q) = \{0\}$ and $\dim D = 2$.

$D = \langle \{\mathrm{ev}(f_{i_1}), \mathrm{ev}(f_{i_2})\}$ such that

1. $-\nu_Q(f_{i_j}) \in \{17, 18, 19, 20\}$
2. $-\nu_q(f_{i_1}) \neq -\nu_q(f_{i_2})$

Feng-Rao bound

Example

$H(Q) = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, \ldots\}$
$H^*(Q) = \{0, 3, 4, 6, 7, \ldots, 26, 28, 29, 32\}$

Let $D \subseteq C_{\mathcal{L}}(D, 20Q)$, $D \cap C_{\mathcal{L}}(D, 16Q) = \{0\}$ and $\dim D = 2$.

$D = \langle \{\mathrm{ev}(f_{i_1}), \mathrm{ev}(f_{i_2})\} \rangle$ such that

1. $-\nu_Q(f_{i_j}) \in \{17, 18, 19, 20\}$
2. $-\nu_q(f_{i_1}) \neq -\nu_q(f_{i_2})$

Let $-\nu_Q(f_{i_1}) = 19$, $-\nu_Q(f_{i_2}) = 20$

$$
\begin{aligned}
\#\mathrm{Supp}(D) &\geq \#\Big(H^*(Q) \cap \big(\cup_{s=1}^{m} (\gamma_{i_s} + H(Q))\big)\Big) \\
&= \#\Big(H^*(Q) \cap ((19 + H^*(Q)) \cup (20 + H^*(Q)))\Big)
\end{aligned}
$$

$19 + H^*(Q) = \{19, 22, 23, 25, \ldots, 45, 47, 48, 51\}$
$20 + H^*(Q) = \{20, 23, 24, 26, \ldots, 46, 48, 49, 52\}$

Feng-Rao bound

Example (cont).

$H(Q) = \langle 3,4 \rangle = \{0,3,4,6,7,\dots\}$
$H^*(Q) = \{0,3,4,6,7,\dots,26,28,29,32\}$

We count what 20 hits with a trick

$$|H^*(Q) \cap (20 + H^*(Q))| = n - 20 = 27 - 20 = 7$$

Feng-Rao bound
Example (cont).

$$H(Q) = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, \ldots\}$$
$$H^*(Q) = \{0, 3, 4, 6, 7, \ldots, 26, 28, 29, 32\}$$

We count what 20 hits with a trick

$$|H^*(Q) \cap (20 + H^*(Q))| = n - 20 = 27 - 20 = 7$$

We count now what 19 hits but 20 does not hit.

$$\begin{array}{lccccccccccc}
20 + H^*(Q) & & * & \cdot & \cdot & * & * & \cdot & * & * & * & \cdots \\
19 + H^*(Q) & * & \cdot & \cdot & * & * & \cdot & * & * & * & * & \cdots
\end{array}$$

Feng-Rao bound

Example (cont).

$H(Q) = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, \dots\}$
$H^*(Q) = \{0, 3, 4, 6, 7, \dots, 26, 28, 29, 32\}$

We count what 20 hits with a trick

$$|H^*(Q) \cap (20 + H^*(Q))| = n - 20 = 27 - 20 = 7$$

We count now what 19 hits but 20 does not hit.

$$\begin{array}{lcccccccccccc}
20 + H^*(Q) & & * & \cdot & \cdot & * & * & \cdot & * & * & * & \cdots \\
19 + H^*(Q) & * & \cdot & \cdot & * & * & \cdot & * & * & * & * & \cdots \\
& \uparrow & & & \uparrow & & & \uparrow & & & &
\end{array}$$

Feng-Rao bound
Example (cont).

$H(Q) = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, \ldots\}$
$H^*(Q) = \{0, 3, 4, 6, 7, \ldots, 26, 28, 29, 32\}$

We count what 20 hits with a trick

$$|H^*(Q) \cap (20 + H^*(Q))| = n - 20 = 27 - 20 = 7$$

We count now what 19 hits but 20 does not hit.

$$\begin{array}{lcccccccccccc} 20 + H^*(Q) & & * & \cdot & \cdot & * & * & \cdot & * & * & * & \cdots \\ 19 + H^*(Q) & * & \cdot & \cdot & * & * & \cdot & * & * & * & * & \cdots \\ & \uparrow & & & \uparrow & & & \uparrow & & & & \end{array}$$

For $-\nu_Q(f_{i_1}) = 19$, $-\nu_Q(f_{i_2}) = 20$

$$\begin{array}{rcl} \#\mathrm{Supp}(D) & \geq & n - \gamma_{i_m} + \#\{\lambda \in \cup_{s=1}^{m-1}(\gamma_{i_s} + H(Q)) \mid \lambda \notin \gamma_{i_m} + H(Q)\} \\ & = & (27 - 20) + 3 = 7 + 3 = 10 \end{array}$$

Let $-\nu_Q(f_{i_1}) = 18$, $-\nu_Q(f_{i_2}) = 20$.
We count now what 18 hits but 20 does not hit.

$$\begin{array}{lcccccccccccc}
20 + H^*(Q) & & & * & \cdot & \cdot & * & * & \cdot & * & * & * & \cdots \\
18 + H^*(Q) & * & \cdot & \cdot & * & * & \cdot & * & * & * & * & * & \cdots
\end{array}$$

Feng-Rao bound

Example (cont).

Let $-\nu_Q(f_{i_1}) = 18$, $-\nu_Q(f_{i_2}) = 20$.
We count now what 18 hits but 20 does not hit.

$$
\begin{array}{lcccccccccccc}
20 + H^*(Q) & & & * & \cdot & \cdot & * & * & \cdot & * & * & * & \cdots \\
18 + H^*(Q) & * & \cdot & \cdot & * & * & \cdot & * & * & * & * & * & \cdots \\
 & \uparrow & & & \uparrow & \uparrow & & & \uparrow & & & &
\end{array}
$$

Feng-Rao bound

Example (cont).

Let $-\nu_Q(f_{i_1}) = 18$, $-\nu_Q(f_{i_2}) = 20$.
We count now what 18 hits but 20 does not hit.

$$\begin{array}{lcccccccccccc}
20 + H^*(Q) & & & \ast & \cdot & \cdot & \ast & \ast & \cdot & \ast & \ast & \ast & \cdots \\
18 + H^*(Q) & \ast & \cdot & \cdot & \ast & \ast & \cdot & \ast & \ast & \ast & \ast & \ast & \cdots \\
 & \uparrow & & & \uparrow & \uparrow & & & \uparrow & & & &
\end{array}$$

For $-\nu_Q(f_{i_1}) = 18$, $-\nu_Q(f_{i_2}) = 20$

$$\begin{aligned}
\#\mathrm{Supp}(D) &\geq n - \gamma_{i_m} + \#\{\lambda \in \cup_{s=1}^{m-1}(\gamma_{i_s} + H(Q)) \mid \lambda \notin \gamma_{i_m} + H(Q)\} \\
&= (27 - 20) + 4 = 7 + 4 = 11
\end{aligned}$$

Feng-Rao bound

Example (cont).

Let $-\nu_Q(f_{i_1}) = 18$, $-\nu_Q(f_{i_2}) = 20$.
We count now what 18 hits but 20 does not hit.

$$\begin{array}{lccccccccccccc}
20 + H^*(Q) & & & * & \cdot & \cdot & * & * & \cdot & * & * & * & \cdots \\
18 + H^*(Q) & * & \cdot & \cdot & * & * & \cdot & * & * & * & * & * & \cdots \\
 & \uparrow & & & \uparrow & \uparrow & & & \uparrow & & & &
\end{array}$$

For $-\nu_Q(f_{i_1}) = 18$, $-\nu_Q(f_{i_2}) = 20$

$$\begin{aligned}
\#\mathrm{Supp}(D) &\geq n - \gamma_{i_m} + \#\{\lambda \in \cup_{s=1}^{m-1}(\gamma_{i_s} + H(Q)) \mid \lambda \notin \gamma_{i_m} + H(Q)\} \\
&= (27 - 20) + 4 = 7 + 4 = 11
\end{aligned}$$

We should consider $-\nu_Q(f_{i_1}) = 17$ and $-\nu_Q(f_{i_2}) = 20$ as well.

1. $-\nu_Q(f_{i_1}) \in \{17, 18, 19\}$
2. $-\nu_Q(f_{i_2}) = 20$

Bounding RGHWs

Theorem

Let μ_1, μ_2 be positive integers with $\mu_2 < \mu_1$, and $\mu = \mu_1 - \mu_2$.
For $m = 1, \ldots, \dim C_{\mathcal{L}}(D, \mu_1 Q) - \dim C_{\mathcal{L}}(D, \mu_2 Q)$ we have

$$
\begin{aligned}
& M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) \\
\geq \quad & \min\Big\{ \#\big(H^*(Q) \cap \big(\cup_{s=1}^{m} (\gamma_{i_s} + H(Q))\big)\big) \\
& \qquad \mid \gamma_{i_1}, \ldots, \gamma_{i_m} \in H^*(Q), \mu_2 < \gamma_{i_1} < \cdots < \gamma_{i_t} \leq \mu_1 \Big\} \qquad (1) \\
\geq \quad & \min\Big\{ n - \gamma_{i_m} + \#\{\lambda \in \cup_{s=1}^{m-1} (\gamma_{i_s} + H(Q)) \mid \lambda \notin \gamma_{i_m} + H(Q)\} \\
& \qquad \mid \gamma_{i_1}, \ldots, \gamma_{i_m} \in H^*(Q), \mu_2 < \gamma_{i_1} < \cdots < \gamma_{i_t} \leq \mu_1 \Big\} \qquad (2)
\end{aligned}
$$

Bounding RGHWs

One can even use the previous bound when one does not know $H^*(Q)$: $\lambda_1 < \cdots < \lambda_m$, let $i_j = \lambda_j - \lambda_m$, $j = 1, \ldots, m-1$ then

$$\begin{aligned}
&\#\{\lambda \in \cup_{s=1}^{m-1}(\lambda_i + H(Q) \mid \lambda \notin \lambda_m + H(Q)\} \\
&\qquad = \#\{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\}
\end{aligned}$$

Bounding RGHWs

One can even use the previous bound when one does not know $H^*(Q)$: $\lambda_1 < \cdots < \lambda_m$, let $i_j = \lambda_j - \lambda_m$, $j = 1, \ldots, m-1$ then

$$\begin{aligned}
&\#\{\lambda \in \cup_{s=1}^{m-1}(\lambda_i + H(Q) \mid \lambda \notin \lambda_m + H(Q)\} \\
&\quad = \#\{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\}
\end{aligned}$$

Then we define $Z(\Gamma, \mu, m) =$

$\min\big\{\#\{\alpha \in \cup_{s=1}^{m-1}(i_s + \Gamma) \mid \alpha \notin \Gamma\} \mid -\mu + 1 \leq i_1 < \cdots < i_{m-1} \leq -1\big\}$

Bounding RGHWs

One can even use the previous bound when one does not know $H^*(Q)$: $\lambda_1 < \cdots < \lambda_m$, let $i_j = \lambda_j - \lambda_m$, $j = 1, \ldots, m-1$ then

$$\#\{\lambda \in \cup_{s=1}^{m-1}(\lambda_i + H(Q) \mid \lambda \notin \lambda_m + H(Q)\}$$
$$= \#\{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\}$$

Then we define $Z(\Gamma, \mu, m) =$

$$\min\left\{\#\{\alpha \in \cup_{s=1}^{m-1}(i_s + \Gamma) \mid \alpha \notin \Gamma\} \mid -\mu + 1 \leq i_1 < \cdots < i_{m-1} \leq -1\right\}$$

Theorem (cont)

Let μ_1, μ_2 be positive integers with $\mu_2 < \mu_1$, and $\mu = \mu_1 - \mu_2$. For $m = 1, \ldots, \dim C_{\mathcal{L}}(D, \mu_1 Q) - \dim C_{\mathcal{L}}(D, \mu_2 Q)$ we have

$$M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) \geq n - \mu_1 + Z(H(Q), \mu, m) \qquad (3)$$

Bounding RGHWs

One can even use the previous bound when one does not know $H^*(Q)$: $\lambda_1 < \cdots < \lambda_m$, let $i_j = \lambda_j - \lambda_m$, $j = 1, \ldots, m-1$ then

$$\#\{\lambda \in \cup_{s=1}^{m-1}(\lambda_i + H(Q) \mid \lambda \notin \lambda_m + H(Q)\}$$
$$= \#\{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\}$$

Then we define $Z(\Gamma, \mu, m) =$

$$\min\big\{\#\{\alpha \in \cup_{s=1}^{m-1}(i_s + \Gamma) \mid \alpha \notin \Gamma\} \mid -\mu + 1 \leq i_1 < \cdots < i_{m-1} \leq -1\big\}$$

Theorem (cont)

Let μ_1, μ_2 be positive integers with $\mu_2 < \mu_1$, and $\mu = \mu_1 - \mu_2$. For $m = 1, \ldots, \dim C_{\mathcal{L}}(D, \mu_1 Q) - \dim C_{\mathcal{L}}(D, \mu_2 Q)$ we have

$$M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) \geq n - \mu_1 + Z(H(Q), \mu, m) \quad (3)$$

Note: (3) may be strictly smaller than (2).

Bounding RGHWs

One can even use the previous bound when one does not know $H^*(Q)$: $\lambda_1 < \cdots < \lambda_m$, let $i_j = \lambda_j - \lambda_m$, $j = 1, \ldots, m-1$ then

$$\#\{\lambda \in \cup_{s=1}^{m-1}(\lambda_i + H(Q) \mid \lambda \notin \lambda_m + H(Q)\}$$
$$= \#\{\alpha \in \cup_{s=1}^{m-1}(i_s + H(Q)) \mid \alpha \notin H(Q)\}$$

Then we define $Z(\Gamma, \mu, m) =$

$$\min\left\{\#\{\alpha \in \cup_{s=1}^{m-1}(i_s + \Gamma) \mid \alpha \notin \Gamma\} \mid -\mu + 1 \leq i_1 < \cdots < i_{m-1} \leq -1\right\}$$

Theorem (cont)

Let μ_1, μ_2 be positive integers with $\mu_2 < \mu_1$, and $\mu = \mu_1 - \mu_2$. For $m = 1, \ldots, \dim C_{\mathcal{L}}(D, \mu_1 Q) - \dim C_{\mathcal{L}}(D, \mu_2 Q)$ we have

$$M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) \geq n - \mu_1 + Z(H(Q), \mu, m) \qquad (3)$$

Note: (3) may be strictly smaller than (2).
Note: for $m = 1$, (3) is the Goppa bound.

Feng-Rao bound for dual codes

For duals of one-point algebraic geometric codes we have a bound similar to (1), but no bounds similar to (2) or (16).

Theorem

Let μ_1, μ_2 and m be as before. We have

$$\begin{aligned} & M_m(C_{\mathcal{L}}^{\perp}(D, \mu_2 Q), C_{\mathcal{L}}^{\perp}(D, \mu_1 Q)) \\ \geq \quad & \min \Big\{ \#\big(H(Q) \cap \big(\cup_{s=1}^{m} (\gamma_{i_s} - H(Q))\big)\big) \mid \\ & \gamma_{i_1}, \ldots, \gamma_{i_m} \in H^*(Q), \mu_2 < \gamma_{i_1} < \cdots < \gamma_{i_m} \leq \mu_1 \Big\}. \end{aligned} \tag{4}$$

RGHWs of Hermitian codes

- Hermitian curve $x^{q+1} - y^q - y$ over $\mathbb{F}_{q^2}$
- Let $P_1, \ldots, P_{n=q^3}$, and Q be the rational places
- The Wierstrass semigroup at Q: $H(Q) = \langle q, q+1 \rangle$, $c = q(q-1)$

RGHWs of Hermitian codes

- Hermitian curve $x^{q+1} - y^q - y$ over $\mathbb{F}_{q^2}$
- Let $P_1, \ldots, P_{n=q^3}$, and Q be the rational places
- The Wierstrass semigroup at Q: $H(Q) = \langle q, q+1 \rangle$, $c = q(q-1)$

Theorem: For Hermitian curve

Let μ_1, μ_2 be non-negative integers with $1 \leq \mu_1 - \mu_2 \leq q+1$.
For $1 \leq m \leq \dim(C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_{\mathcal{L}}(D, \mu_2 Q))$ we have

$$
\begin{aligned}
M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) &\geq n - \mu_1 + \sum_{s=0}^{m-2} (q - s) \qquad (5) \\
&= n - \mu_1 + (m-1)(q-(m-2))/2.
\end{aligned}
$$

RGHWs of Hermitian codes

- Hermitian curve $x^{q+1} - y^q - y$ over $\mathbb{F}_{q^2}$
- Let $P_1, \ldots, P_{n=q^3}$, and Q be the rational places
- The Wierstrass semigroup at Q: $H(Q) = \langle q, q+1 \rangle$, $c = q(q-1)$

Theorem: For Hermitian curve

Let μ_1, μ_2 be non-negative integers with $1 \leq \mu_1 - \mu_2 \leq q + 1$.
For $1 \leq m \leq \dim(C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_{\mathcal{L}}(D, \mu_2 Q))$ we have

$$\begin{aligned} M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) &\geq n - \mu_1 + \sum_{s=0}^{m-2}(q - s) \qquad (5) \\ &= n - \mu_1 + (m-1)(q - (m-2))/2. \end{aligned}$$

If $c - 1 \leq \mu_2$ and $\mu_1 < n - c = q(q-1)$, then we have

$$\dim(C_{\mathcal{L}}(D, \mu_1 Q)) - \dim(C_{\mathcal{L}}(D, \mu_2 Q)) = \mu_1 - \mu_2$$

and equality in (5).

Ramp schemes based on Hermitian codes

For $\mu \in H^*(Q)$ we have $C_{\mathcal{L}}(D, \mu Q)^\perp = C_{\mathcal{L}}(D, (n + c - 2 - \mu)Q)$.

Theorem

Let $\mu, \tilde{\mu}$ be positive integers satisfying

$$\tilde{\mu} \leq q + 1, \ c - 1 + \tilde{\mu} \leq \mu \leq n - 1. \tag{6}$$

Consider the ramp secret sharing scheme $D_1/D_2 = C_2^\perp/C_1^\perp$ where $C_1 = C_{\mathcal{L}}(D, \mu Q)$ and $C_2 = C_{\mathcal{L}}(D, (\mu - \tilde{\mu})Q)$. Hence $\ell = \tilde{\mu}$.

For $m = 1, \ldots, \tilde{\mu}$ it holds that

1. $t_m = M_m(C_1, C_2) - 1 \geq n - \mu + \sum_{s=0}^{m-2}(q - s) - 1$
2. $r_m = n - M_{\ell-m+1}(D_1, D_2) + 1 \leq n - \mu + c + \tilde{\mu} - 1 - \sum_{s=0}^{\tilde{\mu}-m-1}(q - s)$

Equality holds when the second condition in (6) is replaced with

$$2c - 2 + \tilde{\mu} < \mu < n - c.$$

A comparison between RGHW and GHW

From Munuera *et al.* computations for GHW of Hermitian codes:

Proposition: For $m = 1, 2$

Let $m \leq \mu_1 - \mu_2 \leq q + 1$, $c - 1 \leq \mu_2$ and $\mu_1 < n - c$, then

$$M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) = d_m(C_{\mathcal{L}}(D, \mu_1 Q))$$

A comparison between RGHW and GHW

From Munuera *et al.* computations for GHW of Hermitian codes:

Proposition: For $m = 1, 2$

Let $m \leq \mu_1 - \mu_2 \leq q + 1$, $c - 1 \leq \mu_2$ and $\mu_1 < n - c$, then

$$M_m(C_{\mathcal{L}}(D, \mu_1 Q), C_{\mathcal{L}}(D, \mu_2 Q)) = d_m(C_{\mathcal{L}}(D, \mu_1 Q))$$

Theorem: For $m = 3, \ldots, \tilde{\mu}$ with $q > 2$

Let $3 \leq \tilde{\mu} \leq q + 1$ be fixed. There are at least $q^3 - 3q^2 + 1$ different codes $C_{\mathcal{L}}(D, \mu Q)$ for which

1. $d_m(C_{\mathcal{L}}(D, \mu Q)) = n - \mu + \rho_m$
2. $M_m(C_{\mathcal{L}}(D, \mu Q), C_{\mathcal{L}}(D, (\mu - \tilde{\mu})Q)) = n - \mu + \sum_{i=0}^{m-2}(q - i)$
3. The difference 2. $-$ 1. $= \left(\sum_{s=0}^{m-2}(q - s)\right) - \rho_m > 0$

A comparison between RGHW and GHW

The ratio of codes that verify the previous result
$R(q) \geq (q^3 - 3q^2 + 1)/q^3 \geq 1 - 3/q \xrightarrow[q\to\infty]{} 1.$

q	4	5	7	8	9	16
R(q)>	0.25	0.4	0.57	0.62	0.66	0.81

A comparison between RGHW and GHW

The ratio of codes that verify the previous result
$R(q) \geq (q^3 - 3q^2 + 1)/q^3 \geq 1 - 3/q \xrightarrow[q\to\infty]{} 1.$

q	4	5	7	8	9	16
R(q)>	0.25	0.4	0.57	0.62	0.66	0.81

Diff(m, q) is $M_m(\cdot,\cdot) - d_m(\cdot)$.

m	3	4	5	6	7	8	9	10
Diff(m,4)	2	1	1					
Diff(m,5)	3	2	3	3				
Diff(m,7)	5	4	7	9	6	6		
Diff(m,8)	6	5	9	12	9	10	10	
Diff(m,16)	14	13	25	36	33	42	50	57

m	11	12	13	14	15	16	17
Diff(m,16)	51	56	60	63	65	55	55

Thank you for your attention

AALBORG UNIVERSITY
DENMARK