On the Feng-Rao Bound for Generalized Hamming Weights

O. Geil   C. Thommesen

Department of Mathematical Sciences
Aalborg University

AAECC-16, 2006

Outline

A First Description of the Area

Motivating Example - the Reed-Solomon Code

The General Theory in Headlines

Linear Codes:

$B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ a basis for $\mathbb{F}_q^n$. Choose any $G \subseteq B$.

$C^\perp(B,G) = (C(B,G))^\perp$ (parity check matrix)

$C(B,G) = \text{span}\{\mathbf{b}_i \mid \mathbf{b}_i \in G\}$ (generator matrix)

Linear Codes:

$B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ a basis for $\mathbb{F}_q^n$. Choose any $G \subseteq B$.

$C^\perp(B,G) = (C(B,G))^\perp$ (parity check matrix)

$C(B,G) = \mathrm{span}\{\mathbf{b}_i \mid \mathbf{b}_i \in G\}$ (generator matrix)

Linear Codes:

$B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ a basis for $\mathbb{F}_q^n$. Choose any $G \subseteq B$.

$C^\perp(B, G) = (C(B, G))^\perp$ (parity check matrix)

$C(B, G) = \text{span}\{\mathbf{b}_i \mid \mathbf{b}_i \in G\}$ (generator matrix)

Example:

$$\mathbb{F}_q = \{P_1, \ldots, P_n\}$$

$$\text{ev}: \begin{cases} \mathbb{F}_q[X] & \rightarrow & \mathbb{F}_q^n \\ F(X) & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

$$\begin{aligned} B &= \{\mathbf{b}_1 = \text{ev}(1), \mathbf{b}_2 = \text{ev}(X), \ldots, \mathbf{b}_n = \text{ev}(X^{n-1})\} \\ G &= \{\mathbf{b}_1, \ldots, \mathbf{b}_s\} \end{aligned}$$

$C^{\perp}(B, G)$ is (the dual of) a Reed-Solomon code

$C(B, G)$ is a Reed-Solomon code

Example:

$$\mathbb{F}_q = \{P_1, \ldots, P_n\}$$

$$\text{ev}: \begin{cases} \mathbb{F}_q[X] & \rightarrow & \mathbb{F}_q^n \\ F(X) & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

$$\begin{aligned} B &= \{\mathbf{b}_1 = \text{ev}(1), \mathbf{b}_2 = \text{ev}(X), \ldots, \mathbf{b}_n = \text{ev}(X^{n-1})\} \\ G &= \{\mathbf{b}_1, \ldots, \mathbf{b}_s\} \end{aligned}$$

$C^\perp(B, G)$ is (the dual of) a Reed-Solomon code

$C(B, G)$ is a Reed-Solomon code

Example:

$$\mathbb{F}_q = \{P_1, \ldots, P_n\}$$

$$\text{ev}: \begin{cases} \mathbb{F}_q[X] & \rightarrow & \mathbb{F}_q^n \\ F(X) & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

$$\begin{aligned} B &= \{\mathbf{b}_1 = \text{ev}(1), \mathbf{b}_2 = \text{ev}(X), \ldots, \mathbf{b}_n = \text{ev}(X^{n-1})\} \\ G &= \{\mathbf{b}_1, \ldots, \mathbf{b}_s\} \end{aligned}$$

$C^{\perp}(B, G)$ is (the dual of) a Reed-Solomon code

$C(B, G)$ is a Reed-Solomon code

Example:

$$\mathbb{F}_q = \{P_1, \ldots, P_n\}$$

$$\mathrm{ev} : \begin{cases} \mathbb{F}_q[X] & \rightarrow & \mathbb{F}_q^n \\ F(X) & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

$$\begin{aligned} B &= \{\mathbf{b}_1 = \mathrm{ev}(1), \mathbf{b}_2 = \mathrm{ev}(X), \ldots, \mathbf{b}_n = \mathrm{ev}(X^{n-1})\} \\ G &= \{\mathbf{b}_1, \ldots, \mathbf{b}_s\} \end{aligned}$$

$C^{\perp}(B, G)$ is (the dual of) a Reed-Solomon code

$C(B, G)$ is a Reed-Solomon code

Generalized Hamming Weights

$$D = \{(1,1,0,0,1,0)\ (1,0,1,0,0,0)\ (0,0,1,0,1,0)\}$$

$$\mathrm{Supp}(D) = \{1,2,3,5\}$$

$$d_t(C) := \min\{\#\mathrm{Supp}(D) \mid D \text{ is a subcode of } C \text{ of dimension } t\}$$

$$d_1(C) = d(C)$$

Generalized Hamming Weights

$$D = \{(1,1,0,0,1,0)\\ (1,0,1,0,0,0)\\ (0,0,1,0,1,0)\}$$

$$\mathrm{Supp}(D) = \{1,2,3,5\}$$

$$d_t(C) := \min\{\#\mathrm{Supp}(D) \mid D \text{ is a subcode of } C \text{ of dimension } t\}$$

$$d_1(C) = d(C)$$

Generalized Hamming Weights

$$D = \{(1,1,0,0,1,0)\\ (1,0,1,0,0,0)\\ (0,0,1,0,1,0)\}$$

$$\text{Supp}(D) = \{1,2,3,5\}$$

$$d_t(C) := \min\{\#\text{Supp}(D) \mid D \text{ is a subcode of } C \text{ of dimension } t\}$$

$$d_1(C) = d(C)$$

- $C^{\perp}(B, G)$
  - minimum distance
    - The Feng-Rao bound 1995
  - $d_2, \ldots, d_k$
    - P. Heijnen and R. Pellikaan 1998
    - T. Shibuya, K. Sakaniwa et al. 1997-2001
    - O. G. and C. Thommesen 2006
- $C(B, G)$
  - minimum distance
    - T. Shibuya and K. Sakaniwa 2001
    - H. E. Andersen and O. G. 2004
  - $d_2, \ldots, d_k$
    - H. E. Andersen and O. G. 2004

- $C^{\perp}(B,G)$
  - minimum distance
    - The Feng-Rao bound 1995
  - $d_2, \ldots, d_k$
    - P. Heijnen and R. Pellikaan 1998
    - T. Shibuya, K. Sakaniwa et al. 1997-2001
    - O. G. and C. Thommesen 2006
- $C(B,G)$
  - minimum distance
    - T. Shibuya and K. Sakaniwa 2001
    - H. E. Andersen and O. G. 2004
  - $d_2, \ldots, d_k$
    - H. E. Andersen and O. G. 2004

- $C^{\perp}(B, G)$
  - minimum distance
    - The Feng-Rao bound 1995
  - $d_2, \ldots, d_k$
    - P. Heijnen and R. Pellikaan 1998
    - T. Shibuya, K. Sakaniwa et al. 1997-2001
    - O. G. and C. Thommesen 2006
- $C(B, G)$
  - minimum distance
    - T. Shibuya and K. Sakaniwa 2001
    - H. E. Andersen and O. G. 2004
  - $d_2, \ldots, d_k$
    - H. E. Andersen and O. G. 2004

- $C^{\perp}(B,G)$
  - minimum distance
    - The Feng-Rao bound 1995
  - $d_2, \ldots, d_k$
    - P. Heijnen and R. Pellikaan 1998
    - T. Shibuya, K. Sakaniwa et al. 1997-2001
    - O. G. and C. Thommesen 2006
- $C(B,G)$
  - minimum distance
    - T. Shibuya and K. Sakaniwa 2001
    - H. E. Andersen and O. G. 2004
  - $d_2, \ldots, d_k$
    - H. E. Andersen and O. G. 2004

- $C^{\perp}(B, G)$
  - minimum distance
    - The Feng-Rao bound 1995
  - $d_2, \ldots, d_k$
    - P. Heijnen and R. Pellikaan 1998
    - T. Shibuya, K. Sakaniwa et al. 1997-2001
    - O. G. and C. Thommesen 2006
- $C(B, G)$
  - minimum distance
    - T. Shibuya and K. Sakaniwa 2001
    - H. E. Andersen and O. G. 2004
  - $d_2, \ldots, d_k$
    - H. E. Andersen and O. G. 2004

- $C^{\perp}(B, G)$
  - minimum distance
    - The Feng-Rao bound 1995
  - $d_2, \ldots, d_k$
    - P. Heijnen and R. Pellikaan 1998
    - T. Shibuya, K. Sakaniwa et al. 1997-2001
    - O. G. and C. Thommesen 2006
- $C(B, G)$
  - minimum distance
    - T. Shibuya and K. Sakaniwa 2001
    - H. E. Andersen and O. G. 2004
  - $d_2, \ldots, d_k$
    - H. E. Andersen and O. G. 2004

$$\mathbf{u} = (u_1, u_2, \ldots, u_n) \quad \mathbf{v} = (v_1, v_2, \ldots, v_n)$$
$$\mathbf{u} * \mathbf{v} = (u_1 v_1, u_2 v_2, \ldots, u_n v_n)$$

Consider word $\mathbf{c} = (c_1, 0, c_3, c_4)$, $c_1, c_3, c_4 \neq 0$

$$\mathbf{e}_1 = (1, 0, 0, 0) \quad \mathbf{e}_2 = (0, 1, 0, 0)$$
$$\mathbf{e}_3 = (0, 0, 1, 0) \quad \mathbf{e}_4 = (0, 0, 0, 1)$$

$$\mathbf{c} * \mathbf{e}_1 = c_1 \mathbf{e}_1, \quad \mathbf{c} * \mathbf{e}_2 = \mathbf{0}, \quad \mathbf{c} * \mathbf{e}_3 = c_3 \mathbf{e}_3, \quad \mathbf{c} * \mathbf{e}_4 = c_4 \mathbf{e}_4.$$

$$\dim\{\mathbf{c} * \mathbf{d} \mid \mathbf{d} \in \mathbb{F}_q^4\} = w_H(\mathbf{c}) = 3.$$

$$\mathbf{u} = (u_1, u_2, \ldots, u_n) \quad \mathbf{v} = (v_1, v_2, \ldots, v_n)$$
$$\mathbf{u} * \mathbf{v} = (u_1 v_1, u_2 v_2, \ldots, u_n v_n)$$

Consider word $\mathbf{c} = (c_1, 0, c_3, c_4),\ c_1, c_3, c_4 \neq 0$

$$\mathbf{e}_1 = (1, 0, 0, 0) \quad \mathbf{e}_2 = (0, 1, 0, 0)$$
$$\mathbf{e}_3 = (0, 0, 1, 0) \quad \mathbf{e}_4 = (0, 0, 0, 1)$$

$$\mathbf{c} * \mathbf{e}_1 = c_1 \mathbf{e}_1, \quad \mathbf{c} * \mathbf{e}_2 = \mathbf{0}, \quad \mathbf{c} * \mathbf{e}_3 = c_3 \mathbf{e}_3, \quad \mathbf{c} * \mathbf{e}_4 = c_4 \mathbf{e}_4.$$

$$\dim\{\mathbf{c} * \mathbf{d} \mid \mathbf{d} \in \mathbb{F}_q^4\} = w_H(\mathbf{c}) = 3.$$

$$\mathbf{u} = (u_1, u_2, \ldots, u_n) \quad \mathbf{v} = (v_1, v_2, \ldots, v_n)$$
$$\mathbf{u} * \mathbf{v} = (u_1 v_1, u_2 v_2, \ldots, u_n v_n)$$

Consider word $\mathbf{c} = (c_1, 0, c_3, c_4),\ c_1, c_3, c_4 \neq 0$

$$\mathbf{e}_1 = (1, 0, 0, 0) \quad \mathbf{e}_2 = (0, 1, 0, 0)$$
$$\mathbf{e}_3 = (0, 0, 1, 0) \quad \mathbf{e}_4 = (0, 0, 0, 1)$$

$$\mathbf{c} * \mathbf{e}_1 = c_1 \mathbf{e}_1, \quad \mathbf{c} * \mathbf{e}_2 = \mathbf{0}, \quad \mathbf{c} * \mathbf{e}_3 = c_3 \mathbf{e}_3, \quad \mathbf{c} * \mathbf{e}_4 = c_4 \mathbf{e}_4.$$

$$\dim\{\mathbf{c} * \mathbf{d} \mid \mathbf{d} \in \mathbb{F}_q^4\} = w_H(\mathbf{c}) = 3.$$

$$\mathbf{u} = (u_1, u_2, \ldots, u_n) \quad \mathbf{v} = (v_1, v_2, \ldots, v_n)$$
$$\mathbf{u} * \mathbf{v} = (u_1 v_1, u_2 v_2, \ldots, u_n v_n)$$

Consider word $\mathbf{c} = (c_1, 0, c_3, c_4),\ c_1, c_3, c_4 \neq 0$

$$\mathbf{e}_1 = (1,0,0,0) \quad \mathbf{e}_2 = (0,1,0,0)$$
$$\mathbf{e}_3 = (0,0,1,0) \quad \mathbf{e}_4 = (0,0,0,1)$$

$$\mathbf{c} * \mathbf{e}_1 = c_1\mathbf{e}_1, \quad \mathbf{c} * \mathbf{e}_2 = \mathbf{0}, \quad \mathbf{c} * \mathbf{e}_3 = c_3\mathbf{e}_3, \quad \mathbf{c} * \mathbf{e}_4 = c_4\mathbf{e}_4.$$

$$\dim\{\mathbf{c} * \mathbf{d} \mid \mathbf{d} \in \mathbb{F}_q^4\} = w_H(\mathbf{c}) = 3.$$

$$\mathbf{u} = (u_1, u_2, \ldots, u_n) \quad \mathbf{v} = (v_1, v_2, \ldots, v_n)$$
$$\mathbf{u} * \mathbf{v} = (u_1 v_1, u_2 v_2, \ldots, u_n v_n)$$

Consider word $\mathbf{c} = (c_1, 0, c_3, c_4),\ c_1, c_3, c_4 \neq 0$

$$\mathbf{e}_1 = (1,0,0,0) \quad \mathbf{e}_2 = (0,1,0,0)$$
$$\mathbf{e}_3 = (0,0,1,0) \quad \mathbf{e}_4 = (0,0,0,1)$$

$$\mathbf{c} * \mathbf{e}_1 = c_1 \mathbf{e}_1, \quad \mathbf{c} * \mathbf{e}_2 = \mathbf{0}, \quad \mathbf{c} * \mathbf{e}_3 = c_3 \mathbf{e}_3, \quad \mathbf{c} * \mathbf{e}_4 = c_4 \mathbf{e}_4.$$

$$\dim\{\mathbf{c} * \mathbf{d} \mid \mathbf{d} \in \mathbb{F}_q^4\} = w_H(\mathbf{c}) = 3.$$

Reed-Solomon codes - $C(B,G)$ description

$$\mathbb{F}_q = \{P_1, \ldots, P_n\}$$

$$\text{ev} : \begin{cases} \mathbb{F}_q[X] & \rightarrow & \mathbb{F}_q^n \\ F(X) & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

$$\begin{aligned} B &= \{\mathbf{b}_1 = \text{ev}(1), \mathbf{b}_2 = \text{ev}(X), \ldots, \mathbf{b}_n = \text{ev}(X^{n-1})\} \\ G_s &= \{\mathbf{b}_1, \ldots, \mathbf{b}_s\}, \quad s = 1, \ldots, n \end{aligned}$$

Non-zero codewords in $C(B, G_k)$ are of the form:

$$\mathbf{c} = \sum_{i=1}^{a} \alpha_i \mathbf{b}_i = \text{ev}\left(\sum_{i=1}^{a} \alpha_i X^{i-1}\right), \quad \alpha_a \neq 0 \text{ and } a \leq k.$$

Reed-Solomon codes - $C(B,G)$ description

$$\mathbb{F}_q = \{P_1, \ldots, P_n\}$$

$$\text{ev} : \begin{cases} \mathbb{F}_q[X] & \rightarrow & \mathbb{F}_q^n \\ F(X) & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

$$\begin{aligned} B &= \{\mathbf{b}_1 = \text{ev}(1), \mathbf{b}_2 = \text{ev}(X), \ldots, \mathbf{b}_n = \text{ev}(X^{n-1})\} \\ G_s &= \{\mathbf{b}_1, \ldots, \mathbf{b}_s\}, \quad s = 1, \ldots, n \end{aligned}$$

Non-zero codewords in $C(B, G_k)$ are of the form:

$$\mathbf{c} = \sum_{i=1}^{a} \alpha_i \mathbf{b}_i = \text{ev}\left(\sum_{i=1}^{a} \alpha_i X^{i-1}\right), \quad \alpha_a \neq 0 \text{ and } a \leq k.$$

Reed-Solomon codes - $C(B,G)$ description

$$\mathbb{F}_q = \{P_1, \ldots, P_n\}$$

$$\mathrm{ev}: \begin{cases} \mathbb{F}_q[X] & \rightarrow & \mathbb{F}_q^n \\ F(X) & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases}$$

$$\begin{aligned} B &= \{\mathbf{b}_1 = \mathrm{ev}(1), \mathbf{b}_2 = \mathrm{ev}(X), \ldots, \mathbf{b}_n = \mathrm{ev}(X^{n-1})\} \\ G_s &= \{\mathbf{b}_1, \ldots, \mathbf{b}_s\}, \quad s = 1, \ldots, n \end{aligned}$$

Non-zero codewords in $C(B, G_k)$ are of the form:

$$\mathbf{c} = \sum_{i=1}^{a} \alpha_i \mathbf{b}_i = \mathrm{ev}\left(\sum_{i=1}^{a} \alpha_i X^{i-1}\right), \quad \alpha_a \neq 0 \text{ and } a \leq k.$$

$\mathbf{e} * \mathbf{f} = (e_1 f_1, \ldots, e_n f_n)$ $\mathrm{ev}(F) * \mathrm{ev}(G) = \mathrm{ev}(FG)$

$$\begin{cases} \mathbf{c} * \mathbf{b}_1 & \in C(B, G_a) \backslash C(B, G_{a-1}) \\ \mathbf{c} * \mathbf{b}_2 & \in C(B, G_{a+1}) \backslash C(B, G_a) \\ & \vdots \\ \mathbf{c} * \mathbf{b}_{n-a+1} & \in C(B, G_n) \backslash C(B, G_{n-1}) \end{cases}$$

$\mathbf{c} * \mathbf{b}_1, \mathbf{c} * \mathbf{b}_2, \ldots, \mathbf{c} * \mathbf{b}_{n-a+1}$ are linearly independent.

From this one can deduce that $w_H(\mathbf{c}) \geq n - a + 1$.

$$d(C_k) \geq \min\{n - a + 1 \mid a = 1, \ldots, k\}\} = n - k + 1$$

AALBORG UNIVERSITY

$$\mathbf{e} * \mathbf{f} = (e_1 f_1, \ldots, e_n f_n) \qquad \mathrm{ev}(F) * \mathrm{ev}(G) = \mathrm{ev}(FG)$$

$$\begin{cases} \mathbf{c} * \mathbf{b}_1 & \in & C(B, G_a) \backslash C(B, G_{a-1}) \\ \mathbf{c} * \mathbf{b}_2 & \in & C(B, G_{a+1}) \backslash C(B, G_a) \\ & \vdots & \\ \mathbf{c} * \mathbf{b}_{n-a+1} & \in & C(B, G_n) \backslash C(B, G_{n-1}) \end{cases}$$

$\mathbf{c} * \mathbf{b}_1, \mathbf{c} * \mathbf{b}_2, \ldots, \mathbf{c} * \mathbf{b}_{n-a+1}$ are linearly independent.

From this one can deduce that $w_H(\mathbf{c}) \geq n - a + 1$.

$$d(C_k) \geq \min\{n - a + 1 \mid a = 1, \ldots, k\}\} = n - k + 1$$

$\mathbf{e} * \mathbf{f} = (e_1 f_1, \ldots, e_n f_n) \qquad \mathrm{ev}(F) * \mathrm{ev}(G) = \mathrm{ev}(FG)$

$$\begin{cases} \mathbf{c} * \mathbf{b}_1 & \in & C(B, G_a) \backslash C(B, G_{a-1}) \\ \mathbf{c} * \mathbf{b}_2 & \in & C(B, G_{a+1}) \backslash C(B, G_a) \\ & \vdots & \\ \mathbf{c} * \mathbf{b}_{n-a+1} & \in & C(B, G_n) \backslash C(B, G_{n-1}) \end{cases}$$

$\mathbf{c} * \mathbf{b}_1, \mathbf{c} * \mathbf{b}_2, \ldots, \mathbf{c} * \mathbf{b}_{n-a+1}$ are linearly independent.

From this one can deduce that $w_H(\mathbf{c}) \geq n - a + 1$.

$$d(C_k) \geq \min\{n - a + 1 \mid a = 1, \ldots, k\}\} = n - k + 1$$

$\mathbf{e} * \mathbf{f} = (e_1 f_1, \ldots, e_n f_n) \qquad \mathrm{ev}(F) * \mathrm{ev}(G) = \mathrm{ev}(FG)$

$$\begin{cases} \mathbf{c} * \mathbf{b}_1 & \in \; C(B, G_a) \backslash C(B, G_{a-1}) \\ \mathbf{c} * \mathbf{b}_2 & \in \; C(B, G_{a+1}) \backslash C(B, G_a) \\ & \vdots \\ \mathbf{c} * \mathbf{b}_{n-a+1} & \in \; C(B, G_n) \backslash C(B, G_{n-1}) \end{cases}$$

$\mathbf{c} * \mathbf{b}_1, \mathbf{c} * \mathbf{b}_2, \ldots, \mathbf{c} * \mathbf{b}_{n-a+1}$ are linearly independent.

From this one can deduce that $w_H(\mathbf{c}) \geq n - a + 1$.

$$d(C_k) \geq \min\{n - a + 1 \mid a = 1, \ldots, k\}\} = n - k + 1$$

AALBORG UNIVERSITY

$$\mathbf{e} * \mathbf{f} = (e_1 f_1, \ldots, e_n f_n) \qquad \mathrm{ev}(F) * \mathrm{ev}(G) = \mathrm{ev}(FG)$$

$$\begin{cases} \mathbf{c} * \mathbf{b}_1 & \in \quad C(B, G_a) \backslash C(B, G_{a-1}) \\ \mathbf{c} * \mathbf{b}_2 & \in \quad C(B, G_{a+1}) \backslash C(B, G_a) \\ & \vdots \\ \mathbf{c} * \mathbf{b}_{n-a+1} & \in \quad C(B, G_n) \backslash C(B, G_{n-1}) \end{cases}$$

$\mathbf{c} * \mathbf{b}_1, \mathbf{c} * \mathbf{b}_2, \ldots, \mathbf{c} * \mathbf{b}_{n-a+1}$ are linearly independent.

From this one can deduce that $w_H(\mathbf{c}) \geq n - a + 1$.

$$d(C_k) \geq \min\{n - a + 1 \mid a = 1, \ldots, k\} = n - k + 1$$

Reed-Solomon codes - $C^{\perp}(B,G)$ description

$$C^{\perp}(B,G_{n-k}) = \{\mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{c} \cdot \mathbf{b}_i = 0, i = 1,\ldots,n-k\}$$

If $\mathbf{c} \neq \mathbf{0}$ then let j be the smallest index in $\{n-k+1,\ldots,n\}$ such that $\mathbf{c} \cdot \mathbf{b}_j \neq 0$. We have

$$\mathbf{c} \cdot \mathbf{d} \neq 0, \ \forall \mathbf{d} \in C(B,G_j) \backslash C(B,G_{j-1})$$

$$\begin{cases} \mathbf{b}_1 * \mathbf{b}_j & \in \ C(B,G_j)\backslash C(B,G_{j-1}) \\ \mathbf{b}_2 * \mathbf{b}_{j-1} & \in \ C(B,G_j)\backslash C(B,G_{j-1}) \\ & \vdots \\ \mathbf{b}_j * \mathbf{b}_1 & \in \ C(B,G_j)\backslash C(B,G_{j-1}) \end{cases}$$

Reed-Solomon codes - $C^{\perp}(B,G)$ description

$$C^{\perp}(B,G_{n-k}) = \{\mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{c} \cdot \mathbf{b}_i = 0, i = 1, \ldots, n-k\}$$

If $\mathbf{c} \neq \mathbf{0}$ then let j be the smallest index in $\{n-k+1, \ldots, n\}$ such that $\mathbf{c} \cdot \mathbf{b}_j \neq 0$. We have

$$\mathbf{c} \cdot \mathbf{d} \neq 0, \ \forall \mathbf{d} \in C(B,G_j) \backslash C(B,G_{j-1})$$

$$\begin{cases} \mathbf{b}_1 * \mathbf{b}_j & \in \quad C(B,G_j) \backslash C(B,G_{j-1}) \\ \mathbf{b}_2 * \mathbf{b}_{j-1} & \in \quad C(B,G_j) \backslash C(B,G_{j-1}) \\ & \vdots \\ \mathbf{b}_j * \mathbf{b}_1 & \in \quad C(B,G_j) \backslash C(B,G_{j-1}) \end{cases}$$

Reed-Solomon codes - $C^{\perp}(B,G)$ description

$$C^{\perp}(B,G_{n-k}) = \{\mathbf{c}\in\mathbb{F}_q^n \mid \mathbf{c}\cdot\mathbf{b}_i = 0, i=1,\ldots,n-k\}$$

If $\mathbf{c}\neq\mathbf{0}$ then let j be the smallest index in $\{n-k+1,\ldots,n\}$ such that $\mathbf{c}\cdot\mathbf{b}_j\neq 0$. We have

$$\mathbf{c}\cdot\mathbf{d}\neq 0,\ \forall\mathbf{d}\in C(B,G_j)\backslash C(B,G_{j-1})$$

$$\begin{cases} \mathbf{b}_1 * \mathbf{b}_j & \in & C(B,G_j)\backslash C(B,G_{j-1}) \\ \mathbf{b}_2 * \mathbf{b}_{j-1} & \in & C(B,G_j)\backslash C(B,G_{j-1}) \\ & \vdots & \\ \mathbf{b}_j * \mathbf{b}_1 & \in & C(B,G_j)\backslash C(B,G_{j-1}) \end{cases}$$

Consider $\mathbf{r}_h = \sum_{i=1}^{h} \alpha_i \mathbf{b}_i$, $h \in \{1, \ldots, j\}$, $\alpha_h \neq 0$.

$$\mathbf{r}_h * \mathbf{b}_{j-h} \in C(B, G_j) \setminus C(B, G_{j-1})$$

$$\mathbf{c} \cdot (\mathbf{r}_h * \mathbf{b}_{j-h}) \neq 0$$

$$\Downarrow$$

$$\mathbf{c} * \mathbf{r}_h \neq \mathbf{0}$$

But set of all possible $\mathbf{r}_h$'s, $h = 1, \ldots, j$ is a space of dimension j.
From this one can deduce that $w_H(\mathbf{c}) \geq j$.

$$d(C^{\perp}(B, G_{n-k})) \geq \min\{j \mid j \in \{n-k+1, \ldots, n\}\} = n-k+1$$

Consider $\mathbf{r}_h = \sum_{i=1}^{h} \alpha_i \mathbf{b}_i$, $h \in \{1, \ldots, j\}$, $\alpha_h \neq 0$.

$$\mathbf{r}_h * \mathbf{b}_{j-h} \in C(B, G_j) \setminus C(B, G_{j-1})$$

$$\mathbf{c} \cdot (\mathbf{r}_h * \mathbf{b}_{j-h}) \neq 0$$

$$\Downarrow$$

$$\mathbf{c} * \mathbf{r}_h \neq \mathbf{0}$$

But set of all possible $\mathbf{r}_h$'s, $h = 1, \ldots, j$ is a space of dimension j.
From this one can deduce that $w_H(\mathbf{c}) \geq j$.

$$d(C^{\perp}(B, G_{n-k})) \geq \min\{j \mid j \in \{n-k+1, \ldots, n\} = n-k+1$$

Consider $\mathbf{r}_h = \sum_{i=1}^{h} \alpha_i \mathbf{b}_i$, $h \in \{1, \ldots, j\}$, $\alpha_h \neq 0$.

$$\mathbf{r}_h * \mathbf{b}_{j-h} \in C(B, G_j) \backslash C(B, G_{j-1})$$

$$\mathbf{c} \cdot (\mathbf{r}_h * \mathbf{b}_{j-h}) \neq 0$$

$$\Downarrow$$

$$\mathbf{c} * \mathbf{r}_h \neq \mathbf{0}$$

But set of all possible $\mathbf{r}_h$'s, $h = 1, \ldots, j$ is a space of dimension j.
From this one can deduce that $w_H(\mathbf{c}) \geq j$.

$$d(C^{\perp}(B, G_{n-k})) \geq \min\{j \mid j \in \{n-k+1, \ldots, n\}\} = n-k+1$$

Consider $\mathbf{r}_h = \sum_{i=1}^{h} \alpha_i \mathbf{b}_i$, $h \in \{1, \ldots, j\}$, $\alpha_h \neq 0$.

$$\mathbf{r}_h * \mathbf{b}_{j-h} \in C(B, G_j) \backslash C(B, G_{j-1})$$

$$\mathbf{c} \cdot (\mathbf{r}_h * \mathbf{b}_{j-h}) \neq 0$$

$$\Downarrow$$

$$\mathbf{c} * \mathbf{r}_h \neq \mathbf{0}$$

But set of all possible $\mathbf{r}_h$'s, $h = 1, \ldots, j$ is a space of dimension j.
From this one can deduce that $w_H(\mathbf{c}) \geq j$.

$$d(C^{\perp}(B, G_{n-k})) \geq \min\{j \mid j \in \{n-k+1, \ldots, n\} = n-k+1$$

Consider $\mathbf{r}_h = \sum_{i=1}^{h} \alpha_i \mathbf{b}_i$, $h \in \{1, \dots, j\}$, $\alpha_h \neq 0$.

$$\mathbf{r}_h * \mathbf{b}_{j-h} \in C(B, G_j) \backslash C(B, G_{j-1})$$

$$\mathbf{c} \cdot (\mathbf{r}_h * \mathbf{b}_{j-h}) \neq 0$$

$$\Downarrow$$

$$\mathbf{c} * \mathbf{r}_h \neq \mathbf{0}$$

But set of all possible $\mathbf{r}_h$'s, $h = 1, \dots, j$ is a space of dimension j.
From this one can deduce that $w_H(\mathbf{c}) \geq j$.

$$d(C^{\perp}(B, G_{n-k})) \geq \min\{j \mid j \in \{n-k+1, \dots, n\} = n-k+1$$

General Theory

Define $G_0 := \{\mathbf{0}\}$ and $G_s := \{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$ for $s = 1, \ldots, n$.

$$C(B, G_0) \subsetneq C(B, G_1) \subsetneq C(B, G_2) \subsetneq \cdots \subsetneq C(B, G_n)$$

Let $\mathbf{b}_i * \mathbf{b}_j \in C(B, G_s) \backslash C(B, G_{s-1})$. Then (i, j) is said to be OWB if $\mathbf{b}_u * \mathbf{b}_j \in C(B, G_{s-1})$ for all $u < i$.

General Theory

Define $G_0 := \{\mathbf{0}\}$ and $G_s := \{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$ for $s = 1, \ldots, n$.

$$C(B, G_0) \subsetneq C(B, G_1) \subsetneq C(B, G_2) \subsetneq \cdots \subsetneq C(B, G_n)$$

Let $\mathbf{b}_i * \mathbf{b}_j \in C(B, G_s) \backslash C(B, G_{s-1})$. Then (i, j) is said to be OWB if $\mathbf{b}_u * \mathbf{b}_j \in C(B, G_{s-1})$ for all $u < i$.

General Theory

Define $G_0 := \{\mathbf{0}\}$ and $G_s := \{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$ for $s = 1, \ldots, n$.

$$C(B, G_0) \subsetneq C(B, G_1) \subsetneq C(B, G_2) \subsetneq \cdots \subsetneq C(B, G_n)$$

Let $\mathbf{b}_i * \mathbf{b}_j \in C(B, G_s) \backslash C(B, G_{s-1})$. Then (i, j) is said to be OWB if $\mathbf{b}_u * \mathbf{b}_j \in C(B, G_{s-1})$ for all $u < i$.

Minimum distance of $C^{\perp}(B, G)$:
For every $\mathbf{b}_l \notin G$ count number of $\mathbf{b}_i$'s such that a $\mathbf{b}_j$ exists with (i, j) OWB and $\mathbf{b}_i * \mathbf{b}_j \in C(B, G_l) \backslash C(B, G_{l-1})$. Minimum distance greater or equal to smallest found value.

tth generalized Hammingweight of $C^{\perp}(B, G)$:
Consider all possible combinations of t different $\mathbf{b}_l \notin G$.

Minimum distance of $C^{\perp}(B,G)$:
For every $\mathbf{b}_l \notin G$ count number of $\mathbf{b}_i$'s such that a $\mathbf{b}_j$ exists with (i,j) OWB and $\mathbf{b}_i * \mathbf{b}_j \in C(B,G_l)\backslash C(B,G_{l-1})$. Minimum distance greater or equal to smallest found value.

tth generalized Hammingweight of $C^{\perp}(B,G)$:
Consider all possible combinations of t different $\mathbf{b}_l \notin G$.

AALBORG UNIVERSITY

Minimum distance of $C(B,G)$:
For every $\mathbf{b}_i \in G$ *count number of* $\mathbf{b}_l$*'s such that a* $\mathbf{b}_j$ *exists with* (i,j) *OWB and* $\mathbf{b}_i * \mathbf{b}_j \in C(B,G_l) \backslash C(B,G_{l-1})$. *Minimum distance greater or equal to smallest found value.*

tth generalized Hammingweight of $C(B,G)$:
Consider all possible combinations of t *different* $\mathbf{b}_i \in G$.

Minimum distance of $C(B,G)$:
For every $\mathbf{b}_i \in G$ count number of $\mathbf{b}_l$'s such that a $\mathbf{b}_j$ exists with (i,j) OWB and $\mathbf{b}_i * \mathbf{b}_j \in C(B,G_l) \backslash C(B,G_{l-1})$. Minimum distance greater or equal to smallest found value.

tth generalized Hammingweight of $C(B,G)$:
Consider all possible combinations of t different $\mathbf{b}_i \in G$.

- improved bounds on one-point geometric Goppa codes
- improved bounds on duals of one-point geometric Goppa codes
- improved one-point geometric Goppa codes
- improved duals of one-point geometric Goppa codes
- generalizations of above codes to algebraic structures of higher transcendence degree
- BCH bound a special case of Feng-Rao bound
- Generalized Hamming weights for all the above and more codes.

- improved bounds on one-point geometric Goppa codes
- improved bounds on duals of one-point geometric Goppa codes
- improved one-point geometric Goppa codes
- improved duals of one-point geometric Goppa codes
- generalizations of above codes to algebraic structures of higher transcendence degree
- BCH bound a special case of Feng-Rao bound
- Generalized Hamming weights for all the above and more codes.

- improved bounds on one-point geometric Goppa codes
- improved bounds on duals of one-point geometric Goppa codes
- improved one-point geometric Goppa codes
- improved duals of one-point geometric Goppa codes
- generalizations of above codes to algebraic structures of higher transcendence degree
- BCH bound a special case of Feng-Rao bound
- Generalized Hamming weights for all the above and more codes.

- improved bounds on one-point geometric Goppa codes
- improved bounds on duals of one-point geometric Goppa codes
- improved one-point geometric Goppa codes
- improved duals of one-point geometric Goppa codes
- generalizations of above codes to algebraic structures of higher transcendence degree
- BCH bound a special case of Feng-Rao bound
- Generalized Hamming weights for all the above and more codes.

- improved bounds on one-point geometric Goppa codes
- improved bounds on duals of one-point geometric Goppa codes
- improved one-point geometric Goppa codes
- improved duals of one-point geometric Goppa codes
- generalizations of above codes to algebraic structures of higher transcendence degree
- BCH bound a special case of Feng-Rao bound
- Generalized Hamming weights for all the above and more codes.

$$\mathbb{F}_9[X,Y]/\langle X^4 - Y^3 - Y\rangle, \qquad w(X)=3, w(Y)=4$$

Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2	X^5Y^2	X^6Y^2	X^7Y^2	X^8Y^2
Y	XY	X^2Y	X^3Y	X^4Y	X^5Y	X^6Y	X^7Y	X^8Y
1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8

8	11	14	17	20	23	26	29	32
4	7	10	13	16	19	22	25	28
0	3	6	9	12	15	18	21	24

$$\mathbb{F}_9[X,Y]/\langle X^4 - Y^3 - Y\rangle, \quad w(X) = 3, w(Y) = 4$$

Y^2	XY^2	X^2Y^2	X^3Y^2	X^4Y^2	X^5Y^2	X^6Y^2	X^7Y^2	X^8Y^2
Y	XY	X^2Y	X^3Y	X^4Y	X^5Y	X^6Y	X^7Y	X^8Y
1	X	X^2	X^3	X^4	X^5	X^6	X^7	X^8

8	11	14	17	20	23	26	29	32
4	7	10	13	16	19	22	25	28
0	3	6	9	12	15	18	21	24

$$w: \quad \begin{array}{ccccccccc} 8 & 11 & 14 & 17 & 20 & 23 & 26 & 29 & 32 \\ 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \end{array}$$

$$\mu: \quad \begin{array}{ccccccccc} 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 & 27 \\ 2 & 4 & 6 & 8 & 11 & 14 & 17 & 20 & 23 \\ 1 & 2 & 3 & 4 & 7 & 10 & 13 & 16 & 19 \end{array}$$

$$\mu(6) = 3 \text{ as } 6 = 0 + 6 = 3 + 3 = 6 + 0$$

$C^{\perp}(B, G)$ codes: $C(8), k = 27 - 6 = 21, d = 4$

$\tilde{C}(4), k = 27 - 5 = 22, d = 4$

	8	11	14	17	20	23	26	29	32
w :	4	7	10	13	16	19	22	25	28
	0	3	6	9	12	15	18	21	24

	3	6	9	12	15	18	21	24	27
μ :	2	4	6	8	11	14	17	20	23
	1	2	3	4	7	10	13	16	19

$\mu(6) = 3$ as $6 = 0 + 6 = 3 + 3 = 6 + 0$

$C^{\perp}(B, G)$ codes: $C(8), k = 27 - 6 = 21, d = 4$
$\tilde{C}(4), k = 27 - 5 = 22, d = 4$

$$w: \quad \begin{array}{ccccccccc} 8 & 11 & 14 & 17 & 20 & 23 & 26 & 29 & 32 \\ 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \end{array}$$

$$\sigma: \quad \begin{array}{ccccccccc} 19 & 16 & 13 & 10 & 7 & 4 & 3 & 2 & 1 \\ 23 & 20 & 17 & 14 & 11 & 8 & 6 & 4 & 2 \\ 27 & 24 & 21 & 18 & 15 & 12 & 9 & 6 & 3 \end{array}$$

$\sigma(25) = 4$ as $25+0 = 25, 25+3 = 28, 25+4 = 29, 25+7 = 32$

$C(B,G)$ codes: $E(23), k = 21, d = 4$
$\tilde{E}(4), k = 22, d = 4$

$$w: \quad \begin{matrix} 8 & 11 & 14 & 17 & 20 & 23 & 26 & 29 & 32 \\ 4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & 28 \\ 0 & 3 & 6 & 9 & 12 & 15 & 18 & 21 & 24 \end{matrix}$$

$$\sigma: \quad \begin{matrix} 19 & 16 & 13 & 10 & 7 & 4 & 3 & 2 & 1 \\ 23 & 20 & 17 & 14 & 11 & 8 & 6 & 4 & 2 \\ 27 & 24 & 21 & 18 & 15 & 12 & 9 & 6 & 3 \end{matrix}$$

$\sigma(25) = 4$ as $25+0 = 25, 25+3 = 28, 25+4 = 29, 25+7 = 32$

$C(B, G)$ codes: $E(23), k = 21, d = 4$
$\tilde{E}(4), k = 22, d = 4$

$$\mathbb{F}_{16}[X,Y]/\langle X^5 - Y^4 - Y\rangle, \quad n = 64$$

	k	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9
$\tilde{C}(6)$	55	6	8	9	11	12	14	15	16	**18**
$C(14)$	55	4	8	9	12	13	14	**16**	**17**	**18**