On the generalized Hamming weights of Castle codes

Wilson Olaya León

Universidad Industrial de Santander - Grupo de investigación ALCOM

XXI Coloquio Latinoamericano de Álgebra
Buenos Aires - Argentina
Julio 28 de 2016

The generalized Hamming weights

Let $\mathbb{F}_q$ be a finite with q elements.

A $[n, k, d]_q$ code is a k-dimensional subspace of $\mathbb{F}_q^n$, with d the minimum distance between the elements C.

Definition

For $1 \leq r \leq k$, the r-th generalized Hamming weight of C is

$$d_r(C) = \min\{\#supp(C') : C' \leq C \text{ and } \dim(C') = r\}.$$

Proposition

1. *For $1 \leq r < k$, $d_r(C) < d_{r+1}(C)$.*
2. *For $1 \leq r \leq k$, $d_r(C) \leq n - k + r$.*
3. *If $d_{r'}(C) = n - k + r'$ for some r', then $d_r(C) = n - k + r$ for all r with $r' \leq r \leq k$.*

The generalized Hamming weights

Let $\mathbb{F}_q$ be a finite with q elements.

A $[n, k, d]_q$ code is a k-dimensional subspace of $\mathbb{F}_q^n$, with d the minimum distance between the elements C.

Definition

For $1 \leq r \leq k$, the r-th generalized Hamming weight of C is

$$d_r(C) = \min\{\#supp(C') : C' \leq C \text{ and } \dim(C') = r\}.$$

Proposition

1. *For $1 \leq r < k$, $d_r(C) < d_{r+1}(C)$.*
2. *For $1 \leq r \leq k$, $d_r(C) \leq n - k + r$.*
3. *If $d_{r'}(C) = n - k + r'$ for some r', then $d_r(C) = n - k + r$ for all r with $r' \leq r \leq k$.*

The generalized Hamming weights

Let $\mathbb{F}_q$ be a finite with q elements.

A $[n, k, d]_q$ code is a k-dimensional subspace of $\mathbb{F}_q^n$, with d the minimum distance between the elements C.

Definition

For $1 \leq r \leq k$, *the* r*-th generalized Hamming weight of* C *is*

$$d_r(C) = \min\{\#supp(C') : C' \leq C \text{ and } \dim(C') = r\}.$$

Proposition

1. *For* $1 \leq r < k$, $d_r(C) < d_{r+1}(C)$.
2. *For* $1 \leq r \leq k$, $d_r(C) \leq n - k + r$.
3. *If* $d_{r'}(C) = n - k + r'$ *for some* r', *then* $d_r(C) = n - k + r$ *for all* r *with* $r' \leq r \leq k$.

The generalized Hamming weights

Let $\mathbb{F}_q$ be a finite with q elements.

A $[n, k, d]_q$ code is a k-dimensional subspace of $\mathbb{F}_q^n$, with d the minimum distance between the elements C.

Definition

For $1 \leq r \leq k$, *the* r*-th generalized Hamming weight of* C *is*

$$d_r(C) = \min\{\#supp(C') : C' \leq C \text{ and } \dim(C') = r\}.$$

Proposition

1. *For* $1 \leq r < k$, $d_r(C) < d_{r+1}(C)$.
2. *For* $1 \leq r \leq k$, $d_r(C) \leq n - k + r$.
3. *If* $d_{r'}(C) = n - k + r'$ *for some* r', *then* $d_r(C) = n - k + r$ *for all* r *with* $r' \leq r \leq k$.

Algebraic Geometric (AG) codes

- Let $\mathcal{X}$ a curve of genus g over $\mathbb{F}_q$.
- Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be n rational distinct points of $\mathcal{X}$.
- Let G be a rational divisor with support disjoint from $D = P_1 + \cdots + P_n$. Let $\mathcal{L}(G) = \{f \in \mathbb{F}_q(\mathcal{X}) : \mathrm{div}(f) + G \geq 0\} \cup \{0\}$.

Definition

The algebraic geometric (AG) code is

$C(\mathcal{X}, D, G) = ev_{\mathcal{P}}(\mathcal{L}(G)) = \{ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}$

Theorem

The AG code $C(\mathcal{X}, D, G)$ satisfies

- *The dimension is $k = \ell(G) - \ell(G - D)$,*
- *the minimum distance satisfies $d \geq n - \deg(G)$,*

If $2g - 2 < \deg(G) < n$, then $k = \deg(G) + 1 - g$.

Algebraic Geometric (AG) codes

- Let $\mathcal{X}$ a curve of genus g over $\mathbb{F}_q$.
- Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be n rational distinct points of $\mathcal{X}$.
- Let G be a rational divisor with support disjoint from $D = P_1 + \cdots + P_n$. Let $\mathcal{L}(G) = \{f \in \mathbb{F}_q(\mathcal{X}) : \mathrm{div}(f) + G \geq 0\} \cup \{0\}$.

Definition

The algebraic geometric (AG) code is
$C(\mathcal{X}, D, G) = ev_{\mathcal{P}}(\mathcal{L}(G)) = \{ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}$

Theorem

The AG code $C(\mathcal{X}, D, G)$ satisfies

- *The dimension is $k = \ell(G) - \ell(G - D)$,*
- *the minimum distance satisfies $d \geq n - \deg(G)$,*

If $2g - 2 < \deg(G) < n$, then $k = \deg(G) + 1 - g$.

Algebraic Geometric (AG) codes

- Let $\mathcal{X}$ a curve of genus g over $\mathbb{F}_q$.
- Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be n rational distinct points of $\mathcal{X}$.
- Let G be a rational divisor with support disjoint from $D = P_1 + \cdots + P_n$. Let $\mathcal{L}(G) = \{f \in \mathbb{F}_q(\mathcal{X}) : \mathrm{div}(f) + G \geq 0\} \cup \{0\}$.

Definition

The algebraic geometric (AG) code is

$C(\mathcal{X}, D, G) = ev_{\mathcal{P}}(\mathcal{L}(G)) = \{ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}$

Theorem

The AG code $C(\mathcal{X}, D, G)$ satisfies

- *The dimension is $k = \ell(G) - \ell(G - D)$,*
- *the minimum distance satisfies $d \geq n - \deg(G)$,*

If $2g - 2 < \deg(G) < n$, then $k = \deg(G) + 1 - g$.

One-point codes and dimension set

If $Q \in \mathcal{X}(\mathbb{F}_q)$, $C(m) = C(\mathcal{X}, D, mQ)$ is called *one-point*.

Let $H = H(Q) = \{-v_Q(f) : f \in \bigcup_{m=0}^{\infty} \mathcal{L}(mQ) \setminus \{0\}\}$ the Weierstrass semigroup of Q.
If $H = \{0 = h_1 < h_2 < \dots\}$, then

$$(0) = C(h_1) \subset C(h_2) \subset \cdots \subset C(n + 2g - 1) = \mathbb{F}_q^n.$$

Definition

We define the dimension set *of this chain as*

$$M = \{h_i \in H : C(h_{i-1}) \neq C(h_i)\}.$$

Let $M = \{m_1, \dots, m_n\}$. As a consequence we have the following chain

$$(\mathbf{0}) \subset C(m_1) \subset \cdots \subset C(m_n) = \mathbb{F}_q^n.$$

If $m \in \mathbb{N}_0$ then $\dim(C(m)) = \max\{i : m_i \leq m\}$.

One-point codes and dimension set

If $Q \in \mathcal{X}(\mathbb{F}_q)$, $C(m) = C(\mathcal{X}, D, mQ)$ is called *one-point*.

Let $H = H(Q) = \{-v_Q(f) : f \in \bigcup_{m=0}^{\infty} \mathcal{L}(mQ) \setminus \{0\}\}$ the Weierstrass semigroup of Q.

If $H = \{0 = h_1 < h_2 < \dots\}$, then

$$(0) = C(h_1) \subset C(h_2) \subset \cdots \subset C(n + 2g - 1) = \mathbb{F}_q^n.$$

Definition

We define the dimension set *of this chain as*

$$M = \{h_i \in H : C(h_{i-1}) \neq C(h_i)\}.$$

Let $M = \{m_1, \dots, m_n\}$. As a consequence we have the following chain

$$(\mathbf{0}) \subset C(m_1) \subset \cdots \subset C(m_n) = \mathbb{F}_q^n.$$

If $m \in \mathbb{N}_0$ then $\dim(C(m)) = \text{máx}\{i : m_i \leq m\}$.

One-point codes and dimension set

If $Q \in \mathcal{X}(\mathbb{F}_q)$, $C(m) = C(\mathcal{X}, D, mQ)$ is called *one-point*.

Let $H = H(Q) = \{-v_Q(f) : f \in \bigcup_{m=0}^{\infty} \mathcal{L}(mQ) \setminus \{0\}\}$ the Weierstrass semigroup of Q.
If $H = \{0 = h_1 < h_2 < \dots\}$, then

$$(0) = C(h_1) \subset C(h_2) \subset \cdots \subset C(n + 2g - 1) = \mathbb{F}_q^n.$$

Definition

We define the dimension set *of this chain as*

$$M = \{h_i \in H : C(h_{i-1}) \neq C(h_i)\}.$$

Let $M = \{m_1, \dots, m_n\}$. As a consequence we have the following chain

$$(\mathbf{0}) \subset C(m_1) \subset \cdots \subset C(m_n) = \mathbb{F}_q^n.$$

If $m \in \mathbb{N}_0$ then $\dim(C(m)) = \text{máx}\{i : m_i \leq m\}$.

One-point codes and dimension set

If $Q \in \mathcal{X}(\mathbb{F}_q)$, $C(m) = C(\mathcal{X}, D, mQ)$ is called *one-point*.

Let $H = H(Q) = \{-v_Q(f) : f \in \bigcup_{m=0}^{\infty} \mathcal{L}(mQ) \setminus \{0\}\}$ the Weierstrass semigroup of Q.
If $H = \{0 = h_1 < h_2 < \dots\}$, then

$$(0) = C(h_1) \subset C(h_2) \subset \cdots \subset C(n + 2g - 1) = \mathbb{F}_q^n.$$

Definition

We define the dimension set *of this chain as*

$$M = \{h_i \in H : C(h_{i-1}) \neq C(h_i)\}.$$

Let $M = \{m_1, \dots, m_n\}$. As a consequence we have the following chain

$$(\mathbf{0}) \subset C(m_1) \subset \cdots \subset C(m_n) = \mathbb{F}_q^n.$$

If $m \in \mathbb{N}_0$ then $\dim(C(m)) = \text{máx}\{i : m_i \leq m\}$.

One-point codes and dimension set

If $Q \in \mathcal{X}(\mathbb{F}_q)$, $C(m) = C(\mathcal{X}, D, mQ)$ is called *one-point*.

Let $H = H(Q) = \{-v_Q(f) : f \in \bigcup_{m=0}^{\infty} \mathcal{L}(mQ) \setminus \{0\}\}$ the Weierstrass semigroup of Q.
If $H = \{0 = h_1 < h_2 < \dots\}$, then

$$(0) = C(h_1) \subset C(h_2) \subset \cdots \subset C(n + 2g - 1) = \mathbb{F}_q^n.$$

Definition

We define the dimension set *of this chain as*

$$M = \{h_i \in H : C(h_{i-1}) \neq C(h_i)\}.$$

Let $M = \{m_1, \dots, m_n\}$. As a consequence we have the following chain

$$(\mathbf{0}) \subset C(m_1) \subset \cdots \subset C(m_n) = \mathbb{F}_q^n.$$

If $m \in \mathbb{N}_0$ then $\dim(C(m)) = \text{máx}\{i : m_i \leq m\}$.

One-point codes and dimension set

If $Q \in \mathcal{X}(\mathbb{F}_q)$, $C(m) = C(\mathcal{X}, D, mQ)$ is called *one-point*.

Let $H = H(Q) = \{-v_Q(f) : f \in \bigcup_{m=0}^{\infty} \mathcal{L}(mQ) \setminus \{0\}\}$ the Weierstrass semigroup of Q.
If $H = \{0 = h_1 < h_2 < \dots\}$, then

$$(0) = C(h_1) \subset C(h_2) \subset \cdots \subset C(n + 2g - 1) = \mathbb{F}_q^n.$$

Definition

We define the dimension set *of this chain as*

$$M = \{h_i \in H : C(h_{i-1}) \neq C(h_i)\}.$$

Let $M = \{m_1, \dots, m_n\}$. As a consequence we have the following chain

$$(\mathbf{0}) \subset C(m_1) \subset \cdots \subset C(m_n) = \mathbb{F}_q^n.$$

If $m \in \mathbb{N}_0$ then $\dim(C(m)) = \text{máx}\{i : m_i \leq m\}$.

Castle curves

Definition

A curve $\mathcal{X}$ over $\mathbb{F}_q$ is called Castle curve *if there is a rational point $Q \in \mathcal{X}(\mathbb{F}_q)$ with Weierstrass semigroups $H(Q)$ such that:*

(i) *$H(Q)$ is symmetric and*

(ii) *$\#\mathcal{X}(\mathbb{F}_q) = qh_2 + 1$, where h_2 is the multiplicity of $H(Q)$.*

Example

- *The* Hermitian curve *over* $\mathbb{F}_{q^2}$. $y^q + y = x^{q+1}$.
- *The* Norm-Trace *over* $\mathbb{F}_{q^r}$. $x^{(q^r-1)/(q-1)} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y$.
- *The* generalized Hermitian curve *over* $\mathbb{F}_{q^r}$.
  $y^{q^{r-1}} + \cdots + y^q + y = x^{1+q} + \cdots + x^{q^{r-2}+q^{r-1}}$.
- *The* Suzuki curve *over* $\mathbb{F}_q$, *with* $q = 2q_0^2$, *and* $q_0 = 2^r \geq 2$.
  $y^q - y = x^{q_0}(x^q - x)$.

Castle curves

Definition

A curve $\mathcal{X}$ over $\mathbb{F}_q$ is called Castle curve *if there is a rational point $Q \in \mathcal{X}(\mathbb{F}_q)$ with Weierstrass semigroups $H(Q)$ such that:*

(i) *$H(Q)$ is symmetric and*

(ii) *$\#\mathcal{X}(\mathbb{F}_q) = qh_2 + 1$, where h_2 is the multiplicity of $H(Q)$.*

Example

- *The* Hermitian curve *over* $\mathbb{F}_{q^2}$. $y^q + y = x^{q+1}$.
- *The* Norm-Trace *over* $\mathbb{F}_{q^r}$. $x^{(q^r-1)/(q-1)} = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y$.
- *The* generalized Hermitian curve *over* $\mathbb{F}_{q^r}$.
  $y^{q^{r-1}} + \cdots + y^q + y = x^{1+q} + \cdots + x^{q^{r-2}+q^{r-1}}$.
- *The* Suzuki curve *over* $\mathbb{F}_q$, *with* $q = 2q_0^2$, *and* $q_0 = 2^r \geq 2$.
  $y^q - y = x^{q_0}(x^q - x)$.

Castle codes

Definition

Let $\mathcal{X}$ a Castle curve with respect to Q, $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1 \ldots, P_n\}$ and $D = P_1 + \cdots + P_n$. The one-point code $C(m) = C(\mathcal{X}, D, mQ)$ is called Castle code*.*

Let $\mathrm{Gaps}(H) = \{l_1, \ldots, l_g\}$ the set of gaps of H.
For Castle codes, the dimension set is

$$M = \{m \in H : m < n\} \cup \{n + l_1, \ldots, n + l_g\} = H \setminus (n + H).$$

Lemma (Symmetry)

For Castle codes, $M = \{m \in H : n + 2g - 1 - m \in H\}$.
As a consequence $m_{n-i+1} = m_n - m_i$.

Proposition (Dual isometric)

For all $k = 1, \ldots, n$ there is $\mathbf{x} \in (\mathbb{F}_q^*)^n$ such that $C(m_k)^\perp = \mathbf{x} * C(m_{n-k})$.

Castle codes

Definition

Let $\mathcal{X}$ a Castle curve with respect to Q, $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1 \ldots, P_n\}$ and $D = P_1 + \cdots + P_n$. The one-point code $C(m) = C(\mathcal{X}, D, mQ)$ is called Castle code.

Let $\mathrm{Gaps}(H) = \{l_1, \ldots, l_g\}$ the set of gaps of H.
For Castle codes, the dimension set is

$$M = \{m \in H : m < n\} \cup \{n + l_1, \ldots, n + l_g\} = H \setminus (n + H).$$

Lemma (Symmetry)

For Castle codes, $M = \{m \in H : n + 2g - 1 - m \in H\}$.
As a consequence $m_{n-i+1} = m_n - m_i$.

Proposition (Dual isometric)

For all $k = 1, \ldots, n$ there is $\mathbf{x} \in (\mathbb{F}_q^*)^n$ such that $C(m_k)^\perp = \mathbf{x} * C(m_{n-k})$.

Castle codes

Definition

Let $\mathcal{X}$ a Castle curve with respect to Q, $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1 \ldots, P_n\}$ and $D = P_1 + \cdots + P_n$. The one-point code $C(m) = C(\mathcal{X}, D, mQ)$ is called Castle code*.*

Let $\mathrm{Gaps}(H) = \{l_1, \ldots, l_g\}$ the set of gaps of H.
For Castle codes, the dimension set is

$$M = \{m \in H : m < n\} \cup \{n + l_1, \ldots, n + l_g\} = H \setminus (n + H).$$

Lemma (Symmetry)

For Castle codes, $M = \{m \in H : n + 2g - 1 - m \in H\}$.
As a consequence $m_{n-i+1} = m_n - m_i$.

Proposition (Dual isometric)

For all $k = 1, \ldots, n$ there is $\mathbf{x} \in (\mathbb{F}_q^*)^n$ such that $C(m_k)^\perp = \mathbf{x} * C(m_{n-k})$.

Castle codes

Definition

Let $\mathcal{X}$ a Castle curve with respect to Q, $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1 \ldots, P_n\}$ and $D = P_1 + \cdots + P_n$. The one-point code $C(m) = C(\mathcal{X}, D, mQ)$ is called Castle code.

Let $\mathrm{Gaps}(H) = \{l_1, \ldots, l_g\}$ the set of gaps of H.
For Castle codes, the dimension set is

$$M = \{m \in H : m < n\} \cup \{n + l_1, \ldots, n + l_g\} = H \setminus (n + H).$$

Lemma (Symmetry)

For Castle codes, $M = \{m \in H : n + 2g - 1 - m \in H\}$.
As a consequence $m_{n-i+1} = m_n - m_i$.

Proposition (Dual isometric)

For all $k = 1, \ldots, n$ there is $\mathbf{x} \in (\mathbb{F}_q^*)^n$ such that $C(m_k)^\perp = \mathbf{x} * C(m_{n-k})$.

The order bound

Let $I_n = \{1, \ldots, n\}$. For $i \in I_n$, let us consider the sets

$$\Lambda_i^* = \{j \in I_n : m_i + m_j \in M\}.$$

Theorem

For all $r = 1, \ldots, k$, the r-th generalized Hamming weight of C_k satisfies

$$d_r(C_k) \geq d_{ORD}(k)_r = \min_{1 \leq j_1 < \cdots < j_r \leq k} \#\left(\Lambda_{j_1} \cup \cdots \cup \Lambda_{j_r}\right).$$

In particular, $d(C_k) \geq d_{ORD}(k) = \min\{\#\Lambda_i : i = 1, \ldots, k\}$.

The order bound

Let $I_n = \{1, \ldots, n\}$. For $i \in I_n$, let us consider the sets

$$\Lambda_i^* = \{j \in I_n : m_i + m_j \in M\}.$$

Theorem

For all $r = 1, \ldots, k$, the r-th generalized Hamming weight of C_k satisfies

$$d_r(C_k) \geq d_{ORD}(k)_r = \min_{1 \leq j_1 < \cdots < j_r \leq k} \#\left(\Lambda_{j_1} \cup \cdots \cup \Lambda_{j_r}\right).$$

In particular, $d(C_k) \geq d_{ORD}(k) = \min\{\#\Lambda_i : i = 1, \ldots, k\}$.

The order bound

Let $I_n = \{1, \ldots, n\}$. For $i \in I_n$, let us consider the sets

$$\Lambda_i^* = \{j \in I_n : m_i + m_j \in M\}.$$

Theorem

For all $r = 1, \ldots, k$, the r-th generalized Hamming weight of C_k satisfies

$$d_r(C_k) \geq d_{ORD}(k)_r = \min_{1 \leq j_1 < \cdots < j_r \leq k} \#\left(\Lambda_{j_1} \cup \cdots \cup \Lambda_{j_r}\right).$$

In particular, $d(C_k) \geq d_{ORD}(k) = \min\{\#\Lambda_i : i = 1, \ldots, k\}$.

Minimum distance of Hermitian codes

Example

- *The Hermitian curve* $\mathcal{H} : y^q + y = x^{q+1}$ *of genus* $g = \frac{q(q-1)}{2}$ *over* $\mathbb{F}_{q^2}$.
- *It has* q^3 *rational affine points plus one point* Q *at infinity.*
- *The Weierstrass semigroup of* Q *is* $H = H(Q) = \langle q, q+1 \rangle$.
- *The Hermitian codes* $C_i = C(\mathcal{H}, D, m_i Q)$ *with* $m_i \in M$ *and* D *be the sum of all* q^3 *affine points on* $\mathcal{H}$.

k	$d(C_k)$	condition
$k \leq n - g$	$n - m_k$	if $n - m_k \in H$
	qt	if $n - m_k \in L_t$
$n - g < k \leq n$	$q - t$	$m_k - n \in L_t$

where L_t *is a desert of* H.

Minimum distance of Hermitian codes

Example

- *The Hermitian curve* $\mathcal{H} : y^q + y = x^{q+1}$ *of genus* $g = \frac{q(q-1)}{2}$ *over* $\mathbb{F}_{q^2}$.
- *It has* q^3 *rational affine points plus one point* Q *at infinity.*
- *The Weierstrass semigroup of* Q *is* $H = H(Q) = \langle q, q+1 \rangle$.
- *The Hermitian codes* $C_i = C(\mathcal{H}, D, m_i Q)$ *with* $m_i \in M$ *and* D *be the sum of all* q^3 *affine points on* $\mathcal{H}$.

k	$d(C_k)$	*condition*
$k \leq n - g$	$n - m_k$	*if* $n - m_k \in H$
	qt	*if* $n - m_k \in L_t$
$n - g < k \leq n$	$q - t$	$m_k - n \in L_t$

where L_t *is a desert of* H.

Another interpretation

For $i \in I_n$, let us consider the sets

$$R_i^* = \{j \in I_{n-i} : m_i + m_j \notin M\}.$$

For Castle codes we have

$$\#\Lambda_i = n + 1 - i - \#R_i^*.$$

As a consequence,

$$d_{ORD}(k) = n + 1 - \max_{1 \leq i \leq k} \{i + \#R_i^*\}.$$

Another interpretation

For $i \in I_n$, let us consider the sets

$$R_i^* = \{j \in I_{n-i} : m_i + m_j \notin M\}.$$

For Castle codes we have

$$\#\Lambda_i = n + 1 - i - \#R_i^*.$$

As a consequence,

$$d_{ORD}(k) = n + 1 - \max_{1 \leq i \leq k} \{i + \#R_i^*\}.$$

Another interpretation

For $i \in I_n$, let us consider the sets

$$R_i^* = \{j \in I_{n-i} : m_i + m_j \notin M\}.$$

For Castle codes we have

$$\#\Lambda_i = n + 1 - i - \#R_i^*.$$

As a consequence,

$$d_{ORD}(k) = n + 1 - \max_{1 \leq i \leq k} \{i + \#R_i^*\}.$$

Generalized Hamming weights of Castle codes

For $i \in I_n$. Let $m_i \in M$, $C_i = C(m_i) = \langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle$ and us consider the chain of Castle codes

$$(0) \subset C_1 \subset \cdots \subset C_n = \mathbb{F}_q^n.$$

For each subset $I \subset I_n$ we define

$$C_i^I = \{\mathbf{c}^I \in \mathbb{F}_q^n : \mathbf{c} \in C_i\} \text{ where } c_i^I = \begin{cases} c_i & \text{if } i \in I \\ 0 & \text{if } i \notin I \end{cases}.$$

As $C_i^I = \langle \mathbf{b}_1^I, \ldots, \mathbf{b}_i^I \rangle$, we obtain the chain of codes

$$(0) \subset C_1^I \subset \cdots \subset C_n^I = \mathbb{F}_q^{nI}.$$

As consequence, $\#I = \dim \mathbb{F}_q^{nI} = \#\{k \in I_n : \mathbf{b}_k^I \notin C_{k-1}^I\}$.

Generalized Hamming weights of Castle codes

For $i \in I_n$. Let $m_i \in M$, $C_i = C(m_i) = \langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle$ and us consider the chain of Castle codes

$$(0) \subset C_1 \subset \cdots \subset C_n = \mathbb{F}_q^n.$$

For each subset $I \subset I_n$ we define

$$C_i^I = \{\mathbf{c}^I \in \mathbb{F}_q^n : \mathbf{c} \in C_i\} \text{ where } c_i^I = \begin{cases} c_i & \text{if } i \in I \\ 0 & \text{if } i \notin I \end{cases}.$$

As $C_i^I = \langle \mathbf{b}_1^I, \ldots, \mathbf{b}_i^I \rangle$, we obtain the chain of codes

$$(0) \subset C_1^I \subset \cdots \subset C_n^I = \mathbb{F}_q^{nI}.$$

As consequence, $\#I = \dim \mathbb{F}_q^{nI} = \#\{k \in I_n : \mathbf{b}_k^I \notin C_{k-1}^I\}$.

Generalized Hamming weights of Castle codes

For $i \in I_n$. Let $m_i \in M$, $C_i = C(m_i) = \langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle$ and us consider the chain of Castle codes

$$(0) \subset C_1 \subset \cdots \subset C_n = \mathbb{F}_q^n.$$

For each subset $I \subset I_n$ we define

$$C_i^I = \{\mathbf{c}^I \in \mathbb{F}_q^n : \mathbf{c} \in C_i\} \text{ where } c_i^I = \begin{cases} c_i & \text{if } i \in I \\ 0 & \text{if } i \notin I \end{cases}.$$

As $C_i^I = \langle \mathbf{b}_1^I, \ldots, \mathbf{b}_i^I \rangle$, we obtain the chain of codes

$$(0) \subset C_1^I \subset \cdots \subset C_n^I = \mathbb{F}_q^{nI}.$$

As consequence, $\#I = \dim \mathbb{F}_q^{nI} = \#\{k \in I_n : \mathbf{b}_k^I \notin C_{k-1}^I\}$.

Generalized Hamming weights of Castle codes

For $i \in I_n$. Let $m_i \in M$, $C_i = C(m_i) = \langle \mathbf{b}_1, \ldots, \mathbf{b}_i \rangle$ and us consider the chain of Castle codes

$$(0) \subset C_1 \subset \cdots \subset C_n = \mathbb{F}_q^n.$$

For each subset $I \subset I_n$ we define

$$C_i^I = \{\mathbf{c}^I \in \mathbb{F}_q^n : \mathbf{c} \in C_i\} \text{ where } c_i^I = \begin{cases} c_i & \text{if } i \in I \\ 0 & \text{if } i \notin I \end{cases}.$$

As $C_i^I = \langle \mathbf{b}_1^I, \ldots, \mathbf{b}_i^I \rangle$, we obtain the chain of codes

$$(0) \subset C_1^I \subset \cdots \subset C_n^I = \mathbb{F}_q^{nI}.$$

As consequence, $\#I = \dim \mathbb{F}_q^{nI} = \#\{k \in I_n : \mathbf{b}_k^I \notin C_{k-1}^I\}$.

If $\mathcal{D}_r = \{C : C \subset C_i \text{ and } \dim C = r\}$, then

$$d_r(C_i) = \min\{\#I : I = \mathrm{sop}(C) \quad \text{and} \quad C \in \mathcal{D}_r\}.$$

Lemma

If $C \in \mathcal{D}_r$ and $I = sop(C)$, then $C \subset (C^I_{n-i})^{\perp}$.

Accordingly,

$$\begin{aligned} r = \dim(C) \leq \dim((C^I_{n-i})^{\perp}) &= \dim(\mathbb{F}_q^{nI}) - \dim {C_{n-i}}^I \\ &= \#\{k \in \bar{I}_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\}. \end{aligned}$$

Therefore,

$$\begin{aligned} \#I &= \#\{k \in I_n : \mathbf{b}^I_k \notin C^I_{k-1}\} \\ &= \#\{k \in I_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\} + \#\{k \in \bar{I}_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\}. \end{aligned}$$

If $\mathcal{D}_r = \{C : C \subset C_i \text{ and } \dim C = r\}$, then

$$d_r(C_i) = \min\{\#I : I = \mathrm{sop}(C) \quad \text{and} \quad C \in \mathcal{D}_r\}.$$

Lemma

If $C \in \mathcal{D}_r$ and $I = sop(C)$, then $C \subset (C^I_{n-i})^{\perp}$.

Accordingly,

$$\begin{aligned} r = \dim(C) \leq \dim((C^I_{n-i})^{\perp}) &= \dim(\mathbb{F}_q^{n^I}) - \dim {C_{n-i}}^I \\ &= \#\{k \in \bar{I}_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\}. \end{aligned}$$

Therefore,

$$\begin{aligned} \#I &= \#\{k \in I_n : \mathbf{b}^I_k \notin C^I_{k-1}\} \\ &= \#\{k \in I_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\} + \#\{k \in \bar{I}_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\}. \end{aligned}$$

If $\mathcal{D}_r = \{C : C \subset C_i \text{ and } \dim C = r\}$, then

$$d_r(C_i) = \min\{\#I : I = \mathrm{sop}(C) \quad \text{and} \quad C \in \mathcal{D}_r\}.$$

Lemma

If $C \in \mathcal{D}_r$ and $I = sop(C)$, then $C \subset (C^I_{n-i})^{\perp}$.

Accordingly,

$$\begin{aligned} r = \dim(C) \leq \dim((C^I_{n-i})^{\perp}) &= \dim(\mathbb{F}_q^{nI}) - \dim {C_{n-i}}^I \\ &= \#\{k \in \bar{I}_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\}. \end{aligned}$$

Therefore,

$$\begin{aligned} \#I &= \#\{k \in I_n : \mathbf{b}^I_k \notin C^I_{k-1}\} \\ &= \#\{k \in I_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\} + \#\{k \in \bar{I}_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\}. \end{aligned}$$

If $\mathcal{D}_r = \{C : C \subset C_i \text{ and } \dim C = r\}$, then

$$d_r(C_i) = \min\{\#I : I = \mathrm{sop}(C) \quad \text{and} \quad C \in \mathcal{D}_r\}.$$

Lemma

If $C \in \mathcal{D}_r$ and $I = sop(C)$, then $C \subset (C^I_{n-i})^{\perp}$.

Accordingly,

$$\begin{aligned} r = \dim(C) \leq \dim((C^I_{n-i})^{\perp}) &= \dim(\mathbb{F}_q^{nI}) - \dim {C_{n-i}}^I \\ &= \#\{k \in \bar{I}_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\}. \end{aligned}$$

Therefore,

$$\begin{aligned} \#I &= \#\{k \in I_n : \mathbf{b}^I_k \notin C^I_{k-1}\} \\ &= \#\{k \in I_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\} + \#\{k \in \bar{I}_{n-i} : \mathbf{b}^I_k \notin C^I_{k-1}\}. \end{aligned}$$

Lemma

Let $m_i + m_j = m_k$. If $\mathbf{b}_i^l \in C_{i-1}^l$ or $\mathbf{b}_j^l \in C_{j-1}^l$, then $\mathbf{b}_k^l \in C_{k-1}^l$.

For $C \in \mathcal{D}_r$, let us consider the sets

$$T_C = \{k \in I_{n-i} : \mathbf{b}_k^l \in C_{k-1}^l\} \text{ and } R_{T_C}^* = \bigcap_{t \in T_C} R_t^*.$$

Lemma

If $k \in \bar{I}_{n-i}$ and $\mathbf{b}_k^l \notin C_{k-1}^l$, then $n + 1 - k \in R_{T_C}^*$

For each $T \subset I_{n-i}$ us consider the sets

$$W_T = \{k \in \bar{I}_{n-i} : n + 1 - k \in R_T^*\}.$$

Therefore, If $\xi_r = \max\{\#T : T \subset I_{n-i} \text{ and } \#W_T \geq r\}$, then

$$\#\{k \in I_{n-i} : \mathbf{b}_k^l \notin C_{k-1}(l)\} \geq n - i - \xi_r.$$

Lemma

Let $m_i + m_j = m_k$. If $\mathbf{b}_i^l \in C_{i-1}^l$ or $\mathbf{b}_j^l \in C_{j-1}^l$, then $\mathbf{b}_k^l \in C_{k-1}^l$.

For $C \in \mathcal{D}_r$, let us consider the sets

$$T_C = \{k \in I_{n-i} : \mathbf{b}_k^l \in C_{k-1}^l\} \text{ and } R_{T_C}^* = \bigcap_{t \in T_C} R_t^*.$$

Lemma

If $k \in \bar{I}_{n-i}$ and $\mathbf{b}_k^l \notin C_{k-1}^l$, then $n+1-k \in R_{T_C}^*$

For each $T \subset I_{n-i}$ us consider the sets

$$W_T = \{k \in \bar{I}_{n-i} : n+1-k \in R_T^*\}.$$

Therefore, If $\xi_r = \max\{\#T : T \subset I_{n-i} \text{ and } \#W_T \geq r\}$, then

$$\#\{k \in I_{n-i} : \mathbf{b}_k^l \notin C_{k-1}(l)\} \geq n - i - \xi_r.$$

Lemma

Let $m_i + m_j = m_k$. If $\mathbf{b}_i^l \in C_{i-1}^l$ or $\mathbf{b}_j^l \in C_{j-1}^l$, then $\mathbf{b}_k^l \in C_{k-1}^l$.

For $C \in \mathcal{D}_r$, let us consider the sets

$$T_C = \{k \in I_{n-i} : \mathbf{b}_k^l \in C_{k-1}^l\} \text{ and } R_{T_C}^* = \bigcap_{t \in T_C} R_t^*.$$

Lemma

If $k \in \bar{I}_{n-i}$ and $\mathbf{b}_k^l \notin C_{k-1}^l$, then $n + 1 - k \in R_{T_C}^*$

For each $T \subset I_{n-i}$ us consider the sets

$$W_T = \{k \in \bar{I}_{n-i} : n + 1 - k \in R_T^*\}.$$

Therefore, If $\xi_r = \max\{\#T : T \subset I_{n-i} \text{ and } \#W_T \geq r\}$, then

$$\#\{k \in I_{n-i} : \mathbf{b}_k^l \notin C_{k-1}(l)\} \geq n - i - \xi_r.$$

Lemma

Let $m_i + m_j = m_k$. If $\mathbf{b}_i^l \in C_{i-1}^l$ or $\mathbf{b}_j^l \in C_{j-1}^l$, then $\mathbf{b}_k^l \in C_{k-1}^l$.

For $C \in \mathcal{D}_r$, let us consider the sets

$$T_C = \{k \in I_{n-i} : \mathbf{b}_k^l \in C_{k-1}^l\} \text{ and } R_{T_C}^* = \bigcap_{t \in T_C} R_t^*.$$

Lemma

If $k \in \bar{I}_{n-i}$ and $\mathbf{b}_k^l \notin C_{k-1}^l$, then $n+1-k \in R_{T_C}^*$

For each $T \subset I_{n-i}$ us consider the sets

$$W_T = \{k \in \bar{I}_{n-i} : n+1-k \in R_T^*\}.$$

Therefore, If $\xi_r = \max\{\#T : T \subset I_{n-i} \text{ and } \#W_T \geq r\}$, then

$$\#\{k \in I_{n-i} : \mathbf{b}_k^l \notin C_{k-1}(l)\} \geq n - i - \xi_r.$$

Lemma

Let $m_i + m_j = m_k$. If $\mathbf{b}_i^l \in C_{i-1}^l$ or $\mathbf{b}_j^l \in C_{j-1}^l$, then $\mathbf{b}_k^l \in C_{k-1}^l$.

For $C \in \mathcal{D}_r$, let us consider the sets

$$T_C = \{k \in I_{n-i} : \mathbf{b}_k^l \in C_{k-1}^l\} \text{ and } R_{T_C}^* = \bigcap_{t \in T_C} R_t^*.$$

Lemma

If $k \in \bar{I}_{n-i}$ and $\mathbf{b}_k^l \notin C_{k-1}^l$, then $n + 1 - k \in R_{T_C}^*$

For each $T \subset I_{n-i}$ us consider the sets

$$W_T = \{k \in \bar{I}_{n-i} : n + 1 - k \in R_T^*\}.$$

Therefore, If $\xi_r = \max\{\#T : T \subset I_{n-i} \text{ and } \#W_T \geq r\}$, then

$$\#\{k \in I_{n-i} : \mathbf{b}_k^l \notin C_{k-1}(l)\} \geq n - i - \xi_r.$$

The bound for hierarchy weight

Theorem

For $r = 1, \ldots, i$, the r-th generalized Hamming weight of C_i satisfies

$$d_r(C_i) \geq n - i + r - \xi_r.$$

For $i, j \in I_n$, we define

$$X_i(j) = R_j^* \cap I_i \quad \text{and} \quad w_i = \max\{\#X_i(j) : j \in I_{n-i}\}.$$

Theorem

For each $i \in I_n$. If $w_i + 1 \leq r \leq i$, then $d_r(C_i) = n - i + r$.

The bound for hierarchy weight

Theorem

For $r = 1, \ldots, i$, the r-th generalized Hamming weight of C_i satisfies

$$d_r(C_i) \geq n - i + r - \xi_r.$$

For $i, j \in I_n$, we define

$$X_i(j) = R_j^* \cap I_i \quad \text{and} \quad w_i = \max\{\#X_i(j) : j \in I_{n-i}\}.$$

Theorem

For each $i \in I_n$. If $w_i + 1 \leq r \leq i$, then $d_r(C_i) = n - i + r$.

The bound for hierarchy weight

Theorem

For $r = 1, \ldots, i$, the r-th generalized Hamming weight of C_i satisfies

$$d_r(C_i) \geq n - i + r - \xi_r.$$

For $i, j \in I_n$, we define

$$X_i(j) = R_j^* \cap I_i \quad \text{and} \quad w_i = \max\{\#X_i(j) : j \in I_{n-i}\}.$$

Theorem

For each $i \in I_n$. If $w_i + 1 \leq r \leq i$, then $d_r(C_i) = n - i + r$.

New bound for the minimum distance

Theorem

For each $i \in I_n$. The minimum distance of the Castle codes C_i satisfies

$$d(C_i) \geq d_w(i) = n + 1 - i - w_{n-i}.$$

Lemma

1. *If $n - m_i \in H$, then $d_w(i) = d_{ORD}(i) = d_G(C_i) = n - m_i$.*
2. *Let $n - m_i = l \in Gaps(H)$ and $m_{s-1} < l < m_s$. Then $d_w(i) = d_{ORD}(i) = min\{h \in H : h \geq n - m_i\}$.*

Theorem

For Hermitian codes. If $m_i = n + l$ with $l \in L_t$, then $d_w(i) = q - t$.

New bound for the minimum distance

Theorem

For each $i \in I_n$. The minimum distance of the Castle codes C_i satisfies

$$d(C_i) \geq d_w(i) = n + 1 - i - w_{n-i}.$$

Lemma

1. *If $n - m_i \in H$, then $d_w(i) = d_{ORD}(i) = d_G(C_i) = n - m_i$.*
2. *Let $n - m_i = l \in Gaps(H)$ and $m_{s-1} < l < m_s$. Then $d_w(i) = d_{ORD}(i) = min\{h \in H : h \geq n - m_i\}$.*

Theorem

For Hermitian codes. If $m_i = n + l$ with $l \in L_t$, then $d_w(i) = q - t$.

New bound for the minimum distance

Theorem

For each $i \in I_n$. The minimum distance of the Castle codes C_i satisfies

$$d(C_i) \geq d_w(i) = n + 1 - i - w_{n-i}.$$

Lemma

1. *If $n - m_i \in H$, then $d_w(i) = d_{ORD}(i) = d_G(C_i) = n - m_i$.*
2. *Let $n - m_i = l \in Gaps(H)$ and $m_{s-1} < l < m_s$. Then $d_w(i) = d_{ORD}(i) = min\{h \in H : h \geq n - m_i\}$.*

Theorem

For Hermitian codes. If $m_i = n + l$ with $l \in L_t$, then $d_w(i) = q - t$.

Theorem

For each $i \in I_n$, the integer $w_i + 1$ is the touch of the Hermitian code C_i.

Example (Hermitian codes over $\mathbb{F}_9$)

The sequence $(w_i : 1 \leq i \leq 27)$ is: (0, 1, 1, 2, 3, 3, 2, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 2, 2, 0, 0).

i	1	2	3	4	5	6	7	8	9	10	11	12	13
d_1	**27**	24	23	21	20	19	18	17	16	15	14	13	12
d_2		**27**	**26**	24	23	22	21	20	19	18	17	16	15
d_3				**26**	24	23	**23**	21	20	19	18	17	16
d_4					**26**	**25**		**23**	**22**	**21**	**20**	**19**	**18**

14	15	16	17	18	19	20	21	22	23	24	25	26	27
11	10	9	8	7	6	6	4	3	3	3	2	**2**	**1**
14	13	12	11	10	9	8	7	6	5	4	3		
15	14	13	12	11	10	9	8	7	6	**6**	**5**		
17	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**				

Theorem

For each $i \in I_n$, the integer $w_i + 1$ is the touch of the Hermitian code C_i.

Example (Hermitian codes over $\mathbb{F}_9$)

The sequence $(w_i : 1 \leq i \leq 27)$ is: (0, 1, 1, 2, 3, 3, 2, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 2, 2, 0, 0).

i	1	2	3	4	5	6	7	8	9	10	11	12	13
d_1	**27**	24	23	21	20	19	18	17	16	15	14	13	12
d_2		**27**	**26**	24	23	22	21	20	19	18	17	16	15
d_3				**26**	24	23	**23**	21	20	19	18	17	16
d_4					**26**	**25**		**23**	**22**	**21**	**20**	**19**	**18**

14	15	16	17	18	19	20	21	22	23	24	25	26	27
11	10	9	8	7	6	6	4	3	3	3	2	**2**	**1**
14	13	12	11	10	9	8	7	6	5	4	3		
15	14	13	12	11	10	9	8	7	6	**6**	**5**		
17	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**				

Theorem

For each $i \in I_n$, the integer $w_i + 1$ is the touch of the Hermitian code C_i.

Example (Hermitian codes over $\mathbb{F}_9$)

The sequence $(w_i : 1 \leq i \leq 27)$ is: (0, 1, 1, 2, 3, 3, 2, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 3, 2, 2, 0, 0).

i	1	2	3	4	5	6	7	8	9	10	11	12	13
d_1	**27**	24	23	21	20	19	18	17	16	15	14	13	12
d_2		**27**	**26**	24	23	22	21	20	19	18	17	16	15
d_3				**26**	24	23	**23**	21	20	19	18	17	16
d_4					**26**	**25**		**23**	**22**	**21**	**20**	**19**	**18**

14	15	16	17	18	19	20	21	22	23	24	25	26	27
11	10	9	8	7	6	6	4	3	3	3	2	**2**	**1**
14	13	12	11	10	9	8	7	6	5	4	3		
15	14	13	12	11	10	9	8	7	6	**6**	**5**		
17	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**				

¡Muchas Gracias!