Minimum Weight Codewords of Schubert Codes

Prasant Singh
Indian Institute of Technology Bombay

AGC^{2}T-2017
CIRM, Luminy, France
June 20, 2017

Notations

- $\ell \leq m$ positive integers, V a vector space over $\mathbb{F}_q$ with $\dim V = m$
- Grassmannian: $G_{\ell,m} = \{L : \ L \text{ subspace of } V, \ \dim L = \ell\}$
- $\mathbb{I}(\ell, m) = \{(\beta_1, \ldots, \beta_\ell) \in \mathbb{Z}^\ell : 1 \leq \beta_1 < \cdots < \beta_\ell \leq m\}$
- Fix $\alpha = (\alpha_1, \ldots, \alpha_\ell) \in \mathbb{I}(\ell, m)$ and $A_1 \subset \cdots \subset A_\ell$ a flag of vector subspaces of V satisfying $\dim A_i = \alpha_i$, $1 \leq i \leq \ell$
- The Schubert Variety corresponding to α is:

$$\Omega_\alpha(\ell, m) = \{L \in G_{\ell,m} : \dim(L \cap A_i) \geq i \ \forall \ i = 1, \ldots, \ell\}$$

- $\delta = \ell(m - \ell)$ and $\delta(\alpha) = \sum_{i=1}^{\ell} (\alpha_i - i)$

Grassmann Code

- Let
$$n = |G_{\ell,m}(\mathbb{F}_q)| = \begin{bmatrix} m \\ \ell \end{bmatrix}_q \quad \text{and} \quad k = \binom{m}{\ell}.$$
- We have the Plücker embedding $G_{\ell,m} \hookrightarrow \mathbb{P}^{k-1} = \mathbb{P}(\bigwedge^{\ell} V)$. Fix representatives $\omega_1, \ldots, \omega_n$ in $\bigwedge^{\ell} V$ of distinct points of $G_{\ell,m}$.
- The image of the evaluation map
$$Ev : \bigwedge^{m-\ell} V \longrightarrow \mathbb{F}_q^n \quad \text{defined by} \quad \omega' \longmapsto (\omega' \wedge \omega_1, \ldots, \omega' \wedge \omega_n)$$
is a $[n,k]_q$-code, called the Grassmann code, denoted by $C(\ell, m)$.

Grassmann Code

- Let
$$n = |G_{\ell,m}(\mathbb{F}_q)| = \begin{bmatrix} m \\ \ell \end{bmatrix}_q \quad \text{and} \quad k = \binom{m}{\ell}.$$
- We have the Plücker embedding $G_{\ell,m} \hookrightarrow \mathbb{P}^{k-1} = \mathbb{P}(\bigwedge^{\ell} V)$. Fix representatives $\omega_1, \ldots, \omega_n$ in $\bigwedge^{\ell} V$ of distinct points of $G_{\ell,m}$.
- The image of the evaluation map
$$Ev : \bigwedge^{m-\ell} V \longrightarrow \mathbb{F}_q^n \quad \text{defined by} \quad \omega' \longmapsto (\omega' \wedge \omega_1, \ldots, \omega' \wedge \omega_n)$$
is a $[n,k]_q$-code, called the Grassmann code, denoted by $C(\ell, m)$.

Theorem (Nogin, 96)

The minimum distance of $C(\ell, m)$ is q^{δ}. Furthermore, $f \in \bigwedge^{m-\ell} V$ corresponds to a minimum weight codeword iff f is decomposable.

Schubert Code

Let $\alpha \in \mathbb{I}(\ell, m)$ be as earlier and $\Omega_\alpha(\ell, m)$ be the corresponding Schubert variety. We have $\Omega_\alpha(\ell, m) \hookrightarrow \mathbb{P}^{k_\alpha - 1}$ and this corresponds to the $[n_\alpha, k_\alpha]$-linear code, called Schubert code, denoted by $C_\alpha(\ell, m)$, where

$$n_\alpha = |\Omega_\alpha(\ell, m)| \quad \text{and} \quad k_\alpha = |\{\beta \in \mathbb{I}(\ell, m) : \beta \leq \alpha\}|$$

with $\leq$ being the componentwise partial order (Bruhat order):

$$\beta = (\beta_1, \ldots, \beta_\ell) \leq \alpha = (\alpha_1, \ldots, \beta_\ell) \iff \beta_i \leq \alpha_i \ \forall \ i$$

Minimum Distance of Schubert Code

Proposition (Ghorpade-Lachaud, 2000)

For any $\alpha \in \mathbb{I}(\ell, m)$*,*

$$d(C_\alpha(\ell, m)) \leq q^{\delta(\alpha)}$$

It may be noted that when α is the “maximal element” $(m - \ell + 1, \ldots, m)$ of $\mathbb{I}(\ell, m)$ in Bruhat order, then $\Omega_\alpha(\ell, m) = G_{\ell,m}$ while $\delta(\alpha) = \ell(m - \ell)$ and so the above inequality is an equality. In fact, the following conjecture was made

Conjecture (Minimum Distance Conjecture (MDC))

For any $\alpha \in \mathbb{I}(\ell, m)$

$$d(C_\alpha(\ell, m)) = q^{\delta(\alpha)}$$

Length of Schubert Codes

- [H. Chen, (2000)] If $\ell = 2$ and $\alpha = (m-h-1, m)$, then the length

$$n_\alpha = \frac{(q^m - 1)(q^{m-1} - 1)}{(q^2 - 1)(q - 1)} - \sum_{j=1}^{h} \sum_{i=1}^{j} q^{2m-j-2-i}$$

- [Vincenti, (2001)] In general,

$$n_\alpha = \sum \prod_{i=0}^{\ell-1} \begin{bmatrix} \alpha_{i+1} - \alpha_i \\ k_{i+1} - k_i \end{bmatrix}_q q^{(\alpha_i - k_i)(k_{i+1} - k_i)}$$

where the sum is over $(k_1, \ldots, k_{\ell-1}) \in \mathbb{Z}^{\ell-1}$ satisfying $i \le k_i \le \alpha_i$ and $k_i \le k_{i+1}$ for $1 \le i \le \ell - 1$; by convention, $\alpha_0 = 0 = k_0$ and $k_\ell = \ell$.

Length of Schubert Codes (Contd.)

- [Ehresmann (1934); Ghorpade-Tsfasman (2005)]

$$n_\alpha = \sum_{\beta \le \alpha} q^{\delta(\beta)}$$

- Ghorpade-Tsfasman (2005) Suppose α has $u+1$ consecutive blocks: $\alpha = (\alpha_1, \ldots, \alpha_{p_1}, \ldots, \alpha_{p_u+1}, \ldots, \alpha_{p_{u+1}})$. Then

$$n_\alpha = \sum_{s_1=p_1}^{\alpha_{p_1}} \cdots \sum_{s_u=p_u}^{\alpha_{p_u}} \prod_{i=0}^{u} \lambda(\alpha_{p_i}, \alpha_{p_{i+1}}; s_i, s_{i+1})$$

where $s_0 = p_0 = 0$; $s_{u+1} = p_{u+1} = \ell$ and
$\lambda(a, b; s, t) = \sum_{r=s}^{t} (-1)^{r-s} q^{\binom{r-s}{2}} {\begin{bmatrix} a-s \\ r-s \end{bmatrix}}_q {\begin{bmatrix} b-r \\ t-r \end{bmatrix}}_q$.

Dimension of Schubert Codes [Ghorpade-Tsfasman, 2005]

- The dimension of the Schubert code $C_\alpha(\ell, m)$ is the determinant

$$k_\alpha = \det_{1 \le i,j \le \ell} \left(\binom{\alpha_j - j + 1}{i - j + 1} \right)$$

- If $\alpha_1, \ldots, \alpha_\ell$ are in arithmetic progression, i.e. $\alpha_i = c(i-1) + d \; \forall \; i$ for some $c, d \in \mathbb{Z}$, then

$$k_\alpha = \frac{\alpha_1}{\ell!} \prod_{i=1}^{\ell-1} (\alpha_{\ell+1-i}) = \frac{\alpha_1}{\alpha_{\ell+1}} \binom{\alpha_{\ell+1}}{\ell}$$

where $\alpha_{\ell+1} = c\ell + d$

What do we know about the MDC?

Recall that the MDC states that $d(C_\alpha(\ell, m)) = q^{\delta(\alpha)}$

- True if $\alpha = (m - \ell + 1, \ldots, m)$. [Nogin]
- True if $\ell = 2$. [H. Chen (2000); Guerra-Vincenti (2002)]
- Lower bound for $d(C_\alpha(\ell, m))$ [Guerra-Vincenti, 2002]

$$\frac{q^{\alpha_1}(q^{\alpha_2} - q^{\alpha_1}) \cdots (q^{\alpha_\ell} - q^{\alpha_{\ell-1}})}{q^{1+2+\cdots+\ell}} \geq q^{\delta(\alpha)-\ell}$$

- MDC is true for Schubert divisors in $G_{\ell,m}$[Ghorpade-Tsfasman, 2005]
- MDC is true, in general [X. Xiang (2008), Ghorpade- — (2016)]

Minimum Weight Codewords of Schubert Codes

Question: Do decomposable elements of $\bigwedge^{m-\ell} V$ correspond to minimum weight codewords of $C_\alpha(\ell, m)$?

Minimum Weight Codewords of Schubert Codes

Question: Do decomposable elements of $\bigwedge^{m-\ell} V$ correspond to minimum weight codewords of $C_\alpha(\ell, m)$?

Answer: No, in general! Let $\alpha = (\alpha_1, \alpha_2)$ satisfy $\alpha_1 \geq 2$. Fix a basis $\{e_1, \ldots, e_m\}$ of V. Take $A_1 = \langle e_1, \ldots, e_{\alpha_1} \rangle$ and $A_2 = \langle e_1, \ldots, e_{\alpha_2} \rangle$. Then $f = e_3 \wedge \cdots \wedge e_m$ is a decomposable element of $\bigwedge^{m-\ell} V$ and the codeword c_f of $C_\alpha(2, m)$ corresponding to f satisfies:

$$\mathrm{wt}(c_f) = q^{2\alpha_1 - 4} + (q+1) q^{\alpha_1 - 3}(q^{\alpha_2 - 1} - q^{\alpha_1 - 1}).$$

Therefore

$$\mathrm{wt}(c_f) = q^{\delta(\alpha)} \iff \alpha_2 = \alpha_1 + 1, \text{i.e., } C_\alpha(2, m) = C(2, \alpha_2).$$

On the other hand, $h = e_1 \wedge e_3 \wedge e_5 \wedge \cdots \wedge e_m$ is decomposable and

$$\mathrm{wt}(c_h) = q^{\delta(\alpha)} = q^{\alpha_1 + \alpha_2 - 3}$$

Schubert Decomposability

It turns out that we need a more subtle variant of decomposability in the context of Schubert codes.

- Write α uniquely as

  $$\alpha = (\alpha_1, \ldots, \alpha_{p_1},\ \alpha_{p_1+1}, \ldots, \alpha_{p_2},\ \ldots,\ \alpha_{p_{u-1}+1}, \ldots, \alpha_{p_u},\ \alpha_{p_u+1}, \ldots, \alpha_\ell)$$

  where $1 \leq p_1 < \cdots < p_u < \ell$ and $\alpha_{p_i+1}, \ldots, \alpha_{p_{i+1}}$ are consecutive for $0 \leq i \leq u$ and $\alpha_{p_i+1} - \alpha_{p_i} \geq 2$ for $i = 1, \ldots, u$. By convention, $p_0 = 0$ and $p_{u+1} = \ell$.
- α is called completely nonconsecutive if $u = \ell - 1$, i.e., $\alpha_i - \alpha_{i-1} \geq 2$ for all $2 \leq i \leq \ell$

Schubert Decomposability

It turns out that we need a more subtle variant of decomposability in the context of Schubert codes.

- Write α uniquely as

  $$\alpha = (\alpha_1, \dots, \alpha_{p_1},\ \alpha_{p_1+1}, \dots, \alpha_{p_2},\ \dots,\ \alpha_{p_{u-1}+1}, \dots, \alpha_{p_u},\ \alpha_{p_u+1}, \dots, \alpha_\ell)$$

  where $1 \leq p_1 < \cdots < p_u < \ell$ and $\alpha_{p_i+1}, \dots, \alpha_{p_{i+1}}$ are consecutive for $0 \leq i \leq u$ and $\alpha_{p_i+1} - \alpha_{p_i} \geq 2$ for $i = 1, \dots, u$. By convention, $p_0 = 0$ and $p_{u+1} = \ell$.
- α is called completely nonconsecutive if $u = \ell - 1$, i.e., $\alpha_i - \alpha_{i-1} \geq 2$ for all $2 \leq i \leq \ell$

Definition

A decomposable element $f = f_1 \wedge \dots \wedge f_{m-\ell} \in \bigwedge^{m-\ell} V$ is said to be Schubert decomposable if $\dim\left(\mathrm{V_f} \cap \mathrm{A_{p_i}}\right) = \alpha_{\mathrm{p_i}} - \mathrm{p_i}$ for $i = 1, \dots, u$, where $V_f := \{v \in V : v \wedge f = 0\} = \langle f_1, \dots, f_{m-\ell}\rangle$.

Main Results

Theorem (Ghorpade,—)

If $f \in \bigwedge^{m-\ell} V$ is Schubert decomposable, then c_f is a minimum weight codeword of $C_\alpha(\ell, m)$.

Main Results

Theorem (Ghorpade,—)

If $f \in \bigwedge^{m-\ell} V$ is Schubert decomposable, then c_f is a minimum weight codeword of $C_\alpha(\ell, m)$.

Conjecture: Minimum weight codewords of the Schubert code $C_\alpha(\ell, m)$ are precisely the codewords corresponding to Schubert decomposable elements of $\bigwedge^{m-\ell} V$.

Main Results

Theorem (Ghorpade,—)

If $f \in \bigwedge^{m-\ell} V$ is Schubert decomposable, then c_f is a minimum weight codeword of $C_\alpha(\ell, m)$.

Conjecture: Minimum weight codewords of the Schubert code $C_\alpha(\ell, m)$ are precisely the codewords corresponding to Schubert decomposable elements of $\bigwedge^{m-\ell} V$.

Theorem (Ghorpade, —)

Assume that $f \in \bigwedge^{m-\ell} V$ is decomposable. If c_f is a minimum weight codeword of $C_\alpha(\ell, m)$, then f is Schubert decomposable.

Main Results (Contd.)

Theorem (Ghorpade, —)

Assume that α is completely non-consecutive. If c is a minimum weight codeword of $C_\alpha(\ell, m)$, then $c = c_h$ for some decomposable $h \in \bigwedge^{m-\ell} V$.

Main Results (Contd.)

Theorem (Ghorpade, —)

Assume that α is completely non-consecutive. If c is a minimum weight codeword of $C_\alpha(\ell, m)$, then $c = c_h$ for some decomposable $h \in \bigwedge^{m-\ell} V$.

Theorem (Ghorpade, —)

The number of codewords of $C_\alpha(\ell, m)$ corresponding to Schubert decomposable elements of $\bigwedge^{m-\ell} V$ is equal to

$$N_\alpha := (q-1)q^{\mathsf{P}} \prod_{j=0}^{u} \begin{bmatrix} \alpha_{p_{j+1}} - \alpha_{p_j} \\ p_{j+1} - p_j \end{bmatrix}_q$$

where

$$\mathsf{P} = \sum_{j=1}^{u} p_j \left(\alpha_{p_{j+1}} - \alpha_{p_j} - p_{j+1} + p_j \right).$$

Idea of Proof

- Let $\alpha' = (\alpha_1, \dots, \alpha_{\ell-1})$ and $C_{\alpha'}(\ell-1, m)$ be the corresponding Schubert code
- $E = \{x \in A_\ell : c_{f\wedge x} \in C_{\alpha'}(\ell-1,m)$ is the zero codeword$\}$
- $F = A_\ell \setminus E$
- $Z(\alpha, f) = \{(L', x) \in \Omega_{\alpha'}(\ell-1, m) \times A_\ell : f \wedge x(L) \neq 0\}$
- $W(f) = \{L \in \Omega_\alpha(\ell, m) : f(L) \neq 0\}$
- $\phi : Z(\alpha, f) \longrightarrow W(f)$ defined by $(L', x) \mapsto L' + \langle x \rangle$

Idea of Proof

- Let $\alpha' = (\alpha_1, \ldots, \alpha_{\ell-1})$ and $C_{\alpha'}(\ell - 1, m)$ be the corresponding Schubert code
- $E = \{x \in A_\ell : c_{f \wedge x} \in C_{\alpha'}(\ell - 1, m)$ is the zero codeword$\}$
- $F = A_\ell \setminus E$
- $Z(\alpha, f) = \{(L', x) \in \Omega_{\alpha'}(\ell - 1, m) \times A_\ell : f \wedge x(L) \neq 0\}$
- $W(f) = \{L \in \Omega_\alpha(\ell, m) : f(L) \neq 0\}$
- $\phi : Z(\alpha, f) \longrightarrow W(f)$ defined by $(L', x) \mapsto L' + \langle x \rangle$

Lemma (X. Xiang (2008))

If $\mathrm{codim}_{A_\ell} E \leq t$, then $A_{\ell-t} \subseteq E$

Fiber Lemma

Lemma

For a given $L \in W(f)$ the following holds

1. If $L \nsubseteq A_{\ell-1}$, then $|\phi^{-1}(L)| = q^{\ell-1}(q-1)$
2. If $L \subseteq A_{\ell-1}$ and $t := \mathrm{codim}_{\mathrm{A}_\ell}\mathrm{E}$, then $|\phi^{-1}(L)| \leq q^{\ell-1}(q^t - 1)$
3. If f is Schubert decomposable, then $|\phi^{-1}(L)| = q^{\ell-1}(q^t - 1)$

Fiber Lemma

Lemma

For a given $L \in W(f)$ the following holds

1. If $L \nsubseteq A_{\ell-1}$, then $|\phi^{-1}(L)| = q^{\ell-1}(q-1)$
2. If $L \subseteq A_{\ell-1}$ and $t := \mathrm{codim}_{\mathrm{A}_\ell}\mathrm{E}$, then $|\phi^{-1}(L)| \leq q^{\ell-1}(q^t-1)$
3. If f is Schubert decomposable, then $|\phi^{-1}(L)| = q^{\ell-1}(q^t-1)$

Lemma

For any $f \in \bigwedge^{m-\ell} V$ the weight of the codeword c_f satisfies

$$\mathrm{wt}(c_f) \geq \frac{1}{q^{\ell-1}(q-1)} \sum_{x \in F \cap A_{\ell-1}} \mathrm{wt}(c_{f\wedge x}) + \frac{1}{q^{\ell-1}(q^t-1)} \sum_{x \in F \setminus A_{\ell-1}} \mathrm{wt}(c_{f\wedge x})$$

Thank You!