An Asymmetric MacWilliams Identity for Quantum Stabilizer Codes

Tefjol Pllaha

School of Electrical Engineering
Aalto University

July 13, 2019
SIAM Conference on Algebraic Geometry
Bern, Switzerland

Quantum Codes

- An $((n, K))$ **quantum code** is a K dimensional subspace $\mathcal{Q}$ of $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$.

Quantum Codes

- An $((n, K))$ **quantum code** is a K dimensional subspace $\mathcal{Q}$ of $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$.
- Let P denote the orthogonal projection onto $\mathcal{Q}$.

Quantum Codes

- An $((n, K))$ **quantum code** is a K dimensional subspace $\mathcal{Q}$ of $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$.
- Let P denote the orthogonal projection onto $\mathcal{Q}$.
- **Pauli Matrices:**

$$I_2, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_y = i\sigma_x\sigma_z.$$

Quantum Codes

- An $((n, K))$ **quantum code** is a K dimensional subspace $\mathcal{Q}$ of $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$.
- Let P denote the orthogonal projection onto $\mathcal{Q}$.
- **Pauli Matrices:**

$$I_2, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_y = i\sigma_x\sigma_z.$$

- Put $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$. Then

$$\begin{aligned} \sigma_x|0\rangle &= |1\rangle, \quad \sigma_x|1\rangle = |0\rangle, \\ \sigma_z|0\rangle &= |0\rangle, \quad \sigma_z|1\rangle = -|1\rangle. \end{aligned}$$

Quantum Codes

- An $((n, K))$ **quantum code** is a K dimensional subspace $\mathcal{Q}$ of $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$.
- Let P denote the orthogonal projection onto $\mathcal{Q}$.
- **Pauli Matrices:**

$$I_2, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_y = i\sigma_x\sigma_z.$$

- Put $|0\rangle = (1,0)^\mathsf{T}$, $|1\rangle = (0,1)^\mathsf{T}$. Then

$$\begin{aligned} \sigma_x|0\rangle &= |1\rangle, \quad \sigma_x|1\rangle = |0\rangle, \\ \sigma_z|0\rangle &= |0\rangle, \quad \sigma_z|1\rangle = -|1\rangle. \end{aligned}$$

- **Error Group:**

$$\mathcal{P}_n = \langle e_1 \otimes \cdots \otimes e_n \mid e_i \in \{I_2, \sigma_x, \sigma_y, \sigma_z\} \rangle$$

Quantum Codes

- An $((n, K))$ **quantum code** is a K dimensional subspace $\mathcal{Q}$ of $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$.
- Let P denote the orthogonal projection onto $\mathcal{Q}$.
- **Pauli Matrices:**

$$I_2, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_y = i\sigma_x\sigma_z.$$

- Put $|0\rangle = (1,0)^\mathsf{T}$, $|1\rangle = (0,1)^\mathsf{T}$. Then

$$\begin{aligned} \sigma_x|0\rangle &= |1\rangle, \quad \sigma_x|1\rangle = |0\rangle, \\ \sigma_z|0\rangle &= |0\rangle, \quad \sigma_z|1\rangle = -|1\rangle. \end{aligned}$$

- **Error Group:**

$$\begin{aligned} \mathcal{P}_n &= \langle e_1 \otimes \cdots \otimes e_n \mid e_i \in \{I_2, \sigma_x, \sigma_y, \sigma_z\}\rangle \\ &= \{i^\lambda(\sigma_x^{a_1}\sigma_z^{b_1}) \otimes \cdots \otimes (\sigma_x^{a_n}\sigma_z^{b_n}) \mid \lambda = 0,1,2,3; a_i, b_i \in \mathbb{F}_2\} \end{aligned}$$

Quantum Codes

- An $((n, K))$ **quantum code** is a K dimensional subspace $\mathcal{Q}$ of $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$.
- Let P denote the orthogonal projection onto $\mathcal{Q}$.
- **Pauli Matrices:**

$$I_2, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_y = i\sigma_x\sigma_z.$$

- Put $|0\rangle = (1, 0)^{\mathsf{T}}$, $|1\rangle = (0, 1)^{\mathsf{T}}$. Then

$$\begin{aligned} \sigma_x|0\rangle &= |1\rangle, \quad \sigma_x|1\rangle = |0\rangle, \\ \sigma_z|0\rangle &= |0\rangle, \quad \sigma_z|1\rangle = -|1\rangle. \end{aligned}$$

- **Error Group:**

$$\begin{aligned} \mathcal{P}_n &= \langle e_1 \otimes \cdots \otimes e_n \mid e_i \in \{I_2, \sigma_x, \sigma_y, \sigma_z\}\rangle \\ &= \{i^\lambda(\sigma_x^{a_1}\sigma_z^{b_1}) \otimes \cdots \otimes (\sigma_x^{a_n}\sigma_z^{b_n}) \mid \lambda = 0, 1, 2, 3; a_i, b_i \in \mathbb{F}_2\} \\ &= \{i^\lambda X(a)Z(b) \mid \lambda = 0, 1, 2, 3; (a, b) \in \mathbb{F}_2^{2n}\}. \end{aligned}$$

Shor-Laflamme Weight Enumerators

- **Metric:** The weight of an error $e \in \mathcal{P}_n$ is

$$\mathrm{wt}(e) = \#\{i \mid e_i \neq I_2\}.$$

Shor-Laflamme Weight Enumerators

- **Metric:** The weight of an error $e \in \mathcal{P}_n$ is

$$\mathrm{wt}(e) = \#\{i \mid e_i \neq I_2\}.$$

- **Shor-Laflamme weight enumerators:**

$$A_i^{\mathsf{SL}} = \frac{1}{K^2} \sum_{\substack{e \in \mathcal{P}_n \\ \mathrm{wt}(e)=i}} \mathrm{Tr}(e^\dagger P)\mathrm{Tr}(eP), \qquad A(X,Y) = \sum_{i=1}^{n} A_i^{\mathsf{SL}} X^{n-i} Y^i.$$

$$B_i^{\mathsf{SL}} = \frac{1}{K} \sum_{\substack{e \in \mathcal{P}_n \\ \mathrm{wt}(e)=i}} \mathrm{Tr}(e^\dagger P e P), \qquad B(X,Y) = \sum_{i=1}^{n} B_i^{\mathsf{SL}} X^{n-i} Y^i.$$

Shor-Laflamme Weight Enumerators

- **Metric:** The weight of an error $e \in \mathcal{P}_n$ is

$$\mathrm{wt}(e) = \#\{i \mid e_i \neq I_2\}.$$

- **Shor-Laflamme weight enumerators:**

$$A_i^{\mathsf{SL}} = \frac{1}{K^2} \sum_{\substack{e \in \mathcal{P}_n \\ \mathrm{wt}(e)=i}} \mathrm{Tr}(e^\dagger P)\mathrm{Tr}(eP), \qquad A(X,Y) = \sum_{i=1}^{n} A_i^{\mathsf{SL}} X^{n-i} Y^i.$$

$$B_i^{\mathsf{SL}} = \frac{1}{K} \sum_{\substack{e \in \mathcal{P}_n \\ \mathrm{wt}(e)=i}} \mathrm{Tr}(e^\dagger P e P), \qquad B(X,Y) = \sum_{i=1}^{n} B_i^{\mathsf{SL}} X^{n-i} Y^i.$$

- **MacWilliams Identity:**

$$A(X,Y) = \frac{1}{K} B\left(\frac{X + (2^2-1)Y}{2}, \frac{X-Y}{2}\right).$$

Stabilizer Codes

- On $\mathbb{F}_2^{2n}$, consider the **symplectic** bilinear form

$$\langle\, (a, b) \,|\, (a', b') \,\rangle_{\mathrm{s}} := b \cdot a' + a \cdot b'.$$

Stabilizer Codes

- On $\mathbb{F}_2^{2n}$, consider the **symplectic** bilinear form
$$\langle\, (a, b) \,|\, (a', b') \,\rangle_{\mathrm{s}} := b \cdot a' + a \cdot b'.$$
- A self-orthogonal (with respect to $\langle\, \bullet \,|\, \bullet \,\rangle_{\mathrm{s}}$) subspace $C \leq \mathbb{F}_2^{2n}$ is called **stabilizer code**.

Stabilizer Codes

- On $\mathbb{F}_2^{2n}$, consider the **symplectic** bilinear form

$$\langle\,(a,b)\,|\,(a',b')\,\rangle_{\mathrm{s}} := b\cdot a' + a\cdot b'.$$

- A self-orthogonal (with respect to $\langle\,\bullet\,|\,\bullet\,\rangle_{\mathrm{s}}$) subspace $C \leq \mathbb{F}_2^{2n}$ is called **stabilizer code**.
- **Metric:**

$$\mathrm{wt}(a,b) = \#\{i \mid a_i \neq 0 \textbf{ or } b_i \neq 0\}.$$

Stabilizer Codes

- On $\mathbb{F}_2^{2n}$, consider the **symplectic** bilinear form

$$\langle\, (a,b) \,|\, (a',b') \,\rangle_{\mathrm{s}} := b \cdot a' + a \cdot b'.$$

- A self-orthogonal (with respect to $\langle\, \bullet \,|\, \bullet \,\rangle_{\mathrm{s}}$) subspace $C \leq \mathbb{F}_2^{2n}$ is called **stabilizer code**.
- **Metric:**

$$\mathrm{wt}(a,b) = \#\{i \mid a_i \neq 0 \textbf{ or } b_i \neq 0\}.$$

- One-to-one correspondence between stabilizer codes and **quantum stabilizer codes**:

$[2n, k]$ stabilizer code $\iff$ $((n, 2^{n-k}))$ quantum stabilizer code

Stabilizer Codes

- On $\mathbb{F}_2^{2n}$, consider the **symplectic** bilinear form

$$\langle\, (a,b) \,|\, (a',b') \,\rangle_{\mathrm{s}} := b \cdot a' + a \cdot b'.$$

- A self-orthogonal (with respect to $\langle\, \bullet \,|\, \bullet \,\rangle_{\mathrm{s}}$) subspace $C \leq \mathbb{F}_2^{2n}$ is called **stabilizer code**.
- **Metric:**

$$\mathrm{wt}(a,b) = \#\{i \mid a_i \neq 0 \textbf{ or } b_i \neq 0\}.$$

- One-to-one correspondence between stabilizer codes and **quantum stabilizer codes**:

$[2n,k]$ stabilizer code $\iff$ $((n, 2^{n-k}))$ quantum stabilizer code

- **Weight enumerators:**

$$A_i = \#\{(a,b) \in C \mid \mathrm{wt}(a,b) = i\},$$
$$B_i = \#\{(a,b) \in C^{\perp} \mid \mathrm{wt}(a,b) = i\}.$$

Shor-Laflamme Weight Enumerators: Explained

$$\mathrm{Tr}(e^\dagger P)\mathrm{Tr}(eP) = \begin{cases} 2^{2(n-k)}, & \text{if } e \in C, \\ 0, & \text{if } e \notin C, \end{cases}$$

Shor-Laflamme Weight Enumerators: Explained

$$\mathrm{Tr}(e^\dagger P)\mathrm{Tr}(eP) = \begin{cases} 2^{2(n-k)}, & \text{if } e \in C, \\ 0, & \text{if } e \notin C, \end{cases}$$

implies $A_i = A_i^{\mathsf{SL}}$.

Shor-Laflamme Weight Enumerators: Explained

$$\mathrm{Tr}(e^\dagger P)\mathrm{Tr}(eP) = \begin{cases} 2^{2(n-k)}, & \text{if } e \in C, \\ 0, & \text{if } e \notin C, \end{cases}$$

implies $A_i = A_i^{\mathsf{SL}}$.

$$\mathrm{Tr}(e^\dagger PeP) = \begin{cases} 2^{n-k}, & \text{if } e \in C^\perp, \\ 0, & \text{if } e \notin C^\perp, \end{cases}$$

Shor-Laflamme Weight Enumerators: Explained

$$\mathrm{Tr}(e^\dagger P)\mathrm{Tr}(eP) = \begin{cases} 2^{2(n-k)}, & \text{if } e \in C, \\ 0, & \text{if } e \notin C, \end{cases}$$

implies $A_i = A_i^{\mathsf{SL}}$.

$$\mathrm{Tr}(e^\dagger P e P) = \begin{cases} 2^{n-k}, & \text{if } e \in C^\perp, \\ 0, & \text{if } e \notin C^\perp, \end{cases}$$

implies $B_i = B_i^{\mathsf{SL}}$.

Asymmetric Version

- (Some) Physicists claim that phase errors are more likely than flip errors.

Asymmetric Version

- (Some) Physicists claim that phase errors are more likely than flip errors.
- For $x = (a, b) \in \mathbb{F}_2^{2n}$ denote

$$\mathrm{wt}_{\mathrm{X}}(x) := \mathrm{wt}_{\mathrm{H}}(a) \text{ and } \mathrm{wt}_{\mathrm{Z}}(x) := \mathrm{wt}_{\mathrm{H}}(b).$$

Asymmetric Version

- (Some) Physicists claim that phase errors are more likely than flip errors.
- For $x = (a, b) \in \mathbb{F}_2^{2n}$ denote

$$\mathrm{wt}_{\mathrm{X}}(x) := \mathrm{wt}_{\mathrm{H}}(a) \text{ and } \mathrm{wt}_{\mathrm{Z}}(x) := \mathrm{wt}_{\mathrm{H}}(b).$$

- The **asymmetric weight enumerator** of C is defined as

$$\mathrm{AWE}_C(U_1, V_1, U_2, V_2) := \sum_{i,j=1}^{n} A_{i,j} U_1^{n-i} V_1^{i} U_2^{n-j} V_2^{j},$$

where

$$A_{i,j} = \#\{x \in C \mid \mathrm{wt}_{\mathrm{X}}(x) = i \textbf{ and } \mathrm{wt}_{\mathrm{Z}}(x) = j\}.$$

Asymmetric Version

- (Some) Physicists claim that phase errors are more likely than flip errors.
- For $x = (a, b) \in \mathbb{F}_2^{2n}$ denote

$$\mathrm{wt_X}(x) := \mathrm{wt_H}(a) \text{ and } \mathrm{wt_Z}(x) := \mathrm{wt_H}(b).$$

- The **asymmetric weight enumerator** of C is defined as

$$\mathrm{AWE}_C(U_1, V_1, U_2, V_2) := \sum_{i,j=1}^{n} A_{i,j} U_1^{n-i} V_1^i U_2^{n-j} V_2^j,$$

where

$$A_{i,j} = \#\{x \in C \mid \mathrm{wt_X}(x) = i \textbf{ and } \mathrm{wt_Z}(x) = j\}.$$

- Similarly, one puts $\mathrm{AWE}_{C^\perp}$ with

$$B_{i,j} = \#\{x \in C^\perp \mid \mathrm{wt_X}(x) = i \textbf{ and } \mathrm{wt_Z}(x) = j\}.$$

Asymmetric Version

Theorem:

$$\mathrm{AWE}_C(U_1, V_1, U_2, V_2) = \frac{1}{|C^\perp|}\mathrm{AWE}_{C^\perp}(U_1{+}V_1, U_1{-}V_1, U_2{+}V_2, U_2{-}V_2).$$

Asymmetric Version

Theorem:

$$\mathrm{AWE}_C(U_1, V_1, U_2, V_2) = \frac{1}{|C^\perp|}\mathrm{AWE}_{C^\perp}(U_1{+}V_1, U_1{-}V_1, U_2{+}V_2, U_2{-}V_2).$$

- **Complete Weight Enumerator:** For $x = (a, b) \in \mathbb{F}_2^{2n}$ and for $c \in \mathbb{F}_2^2$ define

$$\mathrm{wt}_c(x) := \#\{i \mid (a_i, b_i) = c\}.$$

Asymmetric Version

Theorem:

$$\mathrm{AWE}_C(U_1, V_1, U_2, V_2) = \frac{1}{|C^\perp|}\mathrm{AWE}_{C^\perp}(U_1+V_1, U_1-V_1, U_2+V_2, U_2-V_2).$$

- **Complete Weight Enumerator:** For $x = (a, b) \in \mathbb{F}_2^{2n}$ and for $c \in \mathbb{F}_2^2$ define

$$\mathrm{wt}_c(x) := \#\{i \mid (a_i, b_i) = c\}.$$

- $$\mathrm{CWE}_{\mathcal{C}}(U_{(0,0)}, U_{(1,0)}, U_{(1,1)}, U_{(0,1)}) := \sum_{x\in C} \prod_{c\in\mathbb{F}_2^2} U_c^{\mathrm{wt}_c(x)}.$$

Thank You!