Good Stabilizer Codes from Quasi-Cyclic Codes over $\mathbb{F}_4$ and $\mathbb{F}_9$

Buket Özkaya

Joint work with Martianus Frederic Ezerman, San Ling and Patrick Solé

ISIT 2019
July 7 - 12, Paris
Quantum stabilizers and self-orthogonal linear codes

- $Q \subseteq \mathbb{C}^q \otimes n$ of dimension $K \geq 1 \quad \rightarrow \quad Q = [n, k, d]_q$ where $k = \log_q K$
Quantum stabilizers and self-orthogonal linear codes

- $Q \subseteq (\mathbb{C}^q)^\otimes n$ of dimension $K \geq 1 \rightarrow Q = [n, k, d]_q$ where $k = \log_q K$

- Let $\vec{v}, \vec{u} \in \mathbb{F}_q^n$ such that $\vec{v} := (v_1, \ldots, v_n)$ and $\vec{u} := (u_1, \ldots, u_n)$. Their Hermitian inner product is $\langle \vec{v}, \vec{u} \rangle_H = \sum_{i=1}^n v_i u_i^q$. 

Proposition (Calderbank, Rains, Shor, Sloane, 1998)
- Let $Q$ be a $[n, k, d]_q$ code. Then the following quantum codes exist.
  - i) $[n, k - 1, \geq d]_q$ (by subcode construction).
  - ii) $[n + 1, k, \geq d]_q$ (by lengthening).
  - iii) $[n - 1, k, \geq d - 1]_q$ (by puncturing).
Quantum stabilizers and self-orthogonal linear codes

- $Q \subseteq (\mathbb{C}^q)^\otimes n$ of dimension $K \geq 1$ $\rightarrow Q = [[n, k, d]]_q$ where $k = \log_q K$

- Let $\vec{v}, \vec{u} \in \mathbb{F}_{q^2}^n$ such that $\vec{v} := (v_1, \ldots, v_n)$ and $\vec{u} := (u_1, \ldots, u_n)$. Their Hermitian inner product is $\langle \vec{v}, \vec{u} \rangle_H = \sum_{i=1}^{n} v_i u_i^q$.

- A linear code $C$ over $\mathbb{F}_{q^2}$ is called Hermitian self-orthogonal if $C \subseteq C^\perp_H$. 

Proposition (Calderbank, Rains, Shor, Sloane, 1998)

Let $Q$ be a $[[n, k, d]]_q$ code. Then the following quantum codes exist.

i) $[[n, k - 1, \geq d]]_q$ (by subcode construction).

ii) $[[n + 1, k, \geq d]]_q$ (by lengthening).

iii) $[[n - 1, k, \geq d - 1]]_q$ (by puncturing).
Quantum stabilizers and self-orthogonal linear codes

- $Q \subseteq (\mathbb{C}^q)^\otimes n$ of dimension $K \geq 1 \rightarrow Q = [n, k, d]_q$ where $k = \log_q K$

- Let $\vec{v}, \vec{u} \in \mathbb{F}^n_{q^2}$ such that $\vec{v} := (v_1, \ldots, v_n)$ and $\vec{u} := (u_1, \ldots, u_n)$. Their Hermitian inner product is $\langle \vec{v}, \vec{u} \rangle_H = \sum_{i=1}^n v_i u_i^q$.

- A linear code $C$ over $\mathbb{F}_{q^2}$ is called Hermitian self-orthogonal if $C \subseteq C^\perp_H$.

- Hermitian self-orthogonal $[n, k]_{q^2}$ linear code $C \rightarrow Q = [n, n - 2k, d(Q)]_q$ where $d(Q) \geq d(C^\perp_H)$
Quantum stabilizers and self-orthogonal linear codes

- $Q \subseteq (\mathbb{C}^q)^\otimes n$ of dimension $K \geq 1 \rightarrow Q = \mathbb{F}^{[n, k, d]}_q$ where $k = \log_q K$

- Let $\vec{v}, \vec{u} \in \mathbb{F}^n_{q^2}$ such that $\vec{v} := (v_1, \ldots, v_n)$ and $\vec{u} := (u_1, \ldots, u_n)$. Their Hermitian inner product is $\langle \vec{v}, \vec{u} \rangle_H = \sum_{i=1}^{n} v_i u_i^q$.

- A linear code $C$ over $\mathbb{F}_{q^2}$ is called Hermitian self-orthogonal if $C \subseteq C_{\perp H}$.

- Hermitian self-orthogonal $[n, k]_{q^2}$ linear code $C \rightarrow Q = \mathbb{F}^{[n, n−2k, d(Q)]}_q$ where $d(Q) \geq d(C_{\perp H})$

Proposition (Calderbank, Rains, Shor, Sloane, 1998)

Let $Q$ be an $[n, k, d]_q$ code. Then the following quantum codes exist.

i) $[n, k − 1, \geq d]_q$ (by subcode construction).

ii) $[n + 1, k, \geq d]_q$ (by lengthening).

iii) $[n − 1, k, \geq d − 1]_q$ (by puncturing).
Theorem

For an $[n, k]_q^2$-linear code $C$, let $e := k - \dim(C \cap C^\perp_H)$. Then there exists an $[n + e, n - 2k + e, d(Q)]_q$ quantum stabilizer code $Q$ with $d(Q) \geq \min\{d(C^\perp_H), d(C + C^\perp_H) + 1\}$. 

Lisonek and Singh proved this result for $q = 2$ in 2014. Their method is to use Construction X to create an $[n + e, k + e]_2^2$-linear code $C'$ that is Hermitian self-orthogonal. The result is extended to arbitrary $p$ by Degwekar, Guenda and Gulliver in 2015 and it can be generalized to any prime power easily. Both papers study cyclic codes and their Hermitian duals based on their defining set.
Quantum Construction X

Theorem

For an $[n, k]_q^2$-linear code $C$, let $e := k - \dim(C \cap C^\perp_H)$. Then there exists an $[n + e, n - 2k + e, d(Q)]_q$ quantum stabilizer code $Q$ with $d(Q) \geq \min\{d(C^\perp_H), d(C + C^\perp_H) + 1\}$.

- Lisoněk and Singh proved this result for $q = 2$ in 2014.
Theorem

For an $[n, k]_{q^2}$-linear code $C$, let $e := k - \dim(C \cap C^\perp_H)$. Then there exists an $[[n + e, n - 2k + e, d(Q)]_q$ quantum stabilizer code $Q$ with $d(Q) \geq \min\{d(C^\perp_H), d(C + C^\perp_H) + 1\}$.

- Lisoněk and Singh proved this result for $q = 2$ in 2014.
- Their method is to use Construction X to create an $[n + e, k + e]_{q^2}$-linear code $C'$ that is Hermitian self-orthogonal.
Quantum Construction X

Theorem

For an \([n, k]_{q^2}\)-linear code \(C\), let \(e := k - \dim(C \cap C^\perp_H)\). Then there exists an \([n + e, n - 2k + e, d(Q)]_q\) quantum stabilizer code \(Q\) with \(d(Q) \geq \min\{d(C^\perp_H), d(C + C^\perp_H) + 1\}\).

- Lisoněk and Singh proved this result for \(q = 2\) in 2014.
- Their method is to use Construction X to create an \([n + e, k + e]_{q^2}\)-linear code \(C'\) that is Hermitian self-orthogonal.
- The result is extended to arbitrary \(p\) by Degwekar, Guenda and Gulliver in 2015 and it can be generalized to any prime power easily.
Theorem

For an $[n, k]_{q^2}$-linear code $C$, let $e := k - \dim(C \cap C^\perp_H)$. Then there exists an $[n + e, n - 2k + e, d(Q)]_q$ quantum stabilizer code $Q$ with $d(Q) \geq \min\{d(C^\perp_H), d(C + C^\perp_H) + 1\}$.

- Lisoněk and Singh proved this result for $q = 2$ in 2014.
- Their method is to use Construction X to create an $[n + e, k + e]_{q^2}$-linear code $C'$ that is Hermitian self-orthogonal.
- The result is extended to arbitrary $p$ by Degwekar, Guenda and Gulliver in 2015 and it can be generalized to any prime power easily.
- Both papers study cyclic codes and their Hermitian duals based on their defining set.
For \( m, \ell \) integers with \( \gcd(m, q) = 1 \), a QC code of length \( m\ell \) and index \( \ell \) over \( \mathbb{F}_q \) is a linear code \( C \subseteq \mathbb{F}_q^{m\ell} \) that is invariant under shift of codewords by \( \ell \) positions.
Quasi-cyclic codes

For $m, \ell$ integers with $\gcd(m, q) = 1$, a QC code of length $m\ell$ and index $\ell$ over $\mathbb{F}_q$ is a linear code $C \subseteq \mathbb{F}_q^{m\ell}$ that is invariant under shift of codewords by $\ell$ positions.

$$\vec{c} = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & \ddots & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} \in \mathbb{F}_q^{m\times\ell} \cong \mathbb{F}_q^{m\ell}$$

Invariance under shift by $\ell$ units is equivalent to being closed under row shift. In particular, a QC code of index $\ell = 1$ is a cyclic code.
Define $R := \mathbb{F}_q[x]/\langle x^m - 1 \rangle$ and one can view a QC code in $R^\ell$ as follows:

$$\mathbb{F}_q^{m \times \ell} \rightarrow R^\ell$$

$$\begin{pmatrix}
  c_{00} & c_{01} & \cdots & c_{0,\ell-1} \\
  \vdots & \vdots & & \vdots \\
  c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,\ell-1}
\end{pmatrix} \downarrow \downarrow \downarrow \mapsto \vec{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x))$$

where $c_j(x) = \sum_{i=0}^{m-1} c_{ij}x^i$, $\forall$ $0 \leq j \leq \ell - 1$. 
Algebraic Structure

Define $R := \mathbb{F}_q[x]/\langle x^m - 1 \rangle$ and one can view a QC code in $R^\ell$ as follows:

$$\begin{pmatrix}
  c_{00} & c_{01} & \cdots & c_{0,\ell-1} \\
  \vdots & \vdots & & \vdots \\
  c_{m-1,0} & c_{m-1,1} & \cdots & c_{m-1,\ell-1}
\end{pmatrix}
\mapsto
\begin{pmatrix}
  c_0(x) \\
  c_1(x) \\
  \vdots \\
  c_{\ell-1}(x)
\end{pmatrix}
\mapsto
\vec{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x))$$

where $c_j(x) = \sum_{i=0}^{m-1} c_{ij} x^i$, $\forall \ 0 \leq j \leq \ell - 1$.

Row shift in $\mathbb{F}_q^{m \times \ell}$ corresponds to coordinatewise multiplication by $x$ in $R^\ell$
\Rightarrow $\mathcal{C} \subseteq R^\ell$ is an $R$-submodule.
Assume that $x^m - 1$ factorizes into irreducibles over $\mathbb{F}_q$ as

$$x^m - 1 = g_1(x) \cdots g_s(x) h_1(x) h_1^*(x) \cdots h_r(x) h_r^*(x),$$

where $g_i$’s are self-reciprocal and $h_j^*$ denotes the reciprocal of $h_j$. 
Assume that $x^m - 1$ factorizes into irreducibles over $\mathbb{F}_q$ as

$$x^m - 1 = g_1(x) \cdots g_s(x) h_1(x) h_1^*(x) \cdots h_r(x) h_r^*(x),$$

where $g_i$'s are self-reciprocal and $h_j^*$ denotes the reciprocal of $h_j$.

By the Chinese Remainder Theorem (CRT) we have

$$R \simeq \left( \bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle g_i \rangle \right) \oplus \left( \bigoplus_{j=1}^{r} (\mathbb{F}_q[x]/\langle h_j \rangle) \oplus (\mathbb{F}_q[x]/\langle h_j^* \rangle) \right).$$
CRT Decomposition

Assume that $x^m - 1$ factorizes into irreducibles over $\mathbb{F}_q$ as

$$x^m - 1 = g_1(x) \cdots g_s(x) \, h_1(x) \, h_1^*(x) \cdots h_r(x) \, h_r^*(x),$$

where $g_i$'s are self-reciprocal and $h_j^*$ denotes the reciprocal of $h_j$.

By the Chinese Remainder Theorem (CRT) we have

$$R \simeq \left( \bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle g_i \rangle \right) \oplus \left( \bigoplus_{j=1}^{r} (\mathbb{F}_q[x]/\langle h_j \rangle) \oplus (\mathbb{F}_q[x]/\langle h_j^* \rangle) \right).$$

Let $G_i := \mathbb{F}_q[x]/\langle g_i(x) \rangle$, $H'_j := \mathbb{F}_q[x]/\langle h_j(x) \rangle$ and $H''_j := \mathbb{F}_q[x]/\langle h_j^*(x) \rangle$ denote the respective field extensions, for each $i$ and $j$. 
CRT Decomposition

Assume that $x^m - 1$ factorizes into irreducibles over $\mathbb{F}_q$ as

$$x^m - 1 = g_1(x) \cdots g_s(x) h_1(x) h_1^*(x) \cdots h_r(x) h_r^*(x),$$

where $g_i$'s are self-reciprocal and $h_j^*$ denotes the reciprocal of $h_j$.

By the Chinese Remainder Theorem (CRT) we have

$$R \cong \bigoplus_{i=1}^{s} \mathbb{G}_i \oplus \bigoplus_{j=1}^{r} \left( \mathbb{H}_j \oplus \mathbb{H}'_j \right).$$
CRT Decomposition

Assume that \( x^m - 1 \) factorizes into irreducibles over \( \mathbb{F}_q \) as

\[
x^m - 1 = g_1(x) \cdots g_s(x) h_1(x) h_1^*(x) \cdots h_r(x) h_r^*(x),
\]

where \( g_i \)'s are self-reciprocal and \( h_j^* \) denotes the reciprocal of \( h_j \).

By the Chinese Remainder Theorem (CRT) we have

\[
R^\ell \simeq \bigoplus_{i=1}^{s} \mathbb{G}^\ell_i \bigoplus \bigoplus_{j=1}^{r} \left( \mathbb{H}^\ell_j \bigoplus \mathbb{H}^{\ell'}_j \right)
\]
Constituents

Then a QC code $C \subseteq R^\ell$ decomposes as (Ling, Solé, 2001)

$$C \simeq \left( \bigoplus_{i=1}^{s} C_i \right) \oplus \left( \bigoplus_{j=1}^{r} (C'_j \oplus C''_j) \right),$$

where $C_i \subseteq \mathbb{G}_i^\ell$, $C'_j \subseteq (\mathbb{H}'_j)^\ell$ and $C''_j \subseteq (\mathbb{H}''_j)^\ell$. 
Constituents

Then a QC code $C \subseteq R^\ell$ decomposes as (Ling, Solé, 2001)

$$C \simeq \left( \bigoplus_{i=1}^{s} C_i \right) \oplus \left( \bigoplus_{j=1}^{r} (C'_j \oplus C''_j) \right),$$

where $C_i \subseteq \mathbb{G}_i^\ell$, $C'_j \subseteq (\mathbb{H}'_j)^\ell$ and $C''_j \subseteq (\mathbb{H}''_j)^\ell$.

$$C_{\perp H} = \left( \bigoplus_{i=1}^{s} C_{i \perp H} \right) \oplus \left( \bigoplus_{j=1}^{r} (C''_{j \perp E} \oplus C'_{j \perp E}) \right).$$
Constituents

Then a QC code $C \subseteq R^\ell$ decomposes as (Ling, Solé, 2001)

$$C \simeq \left( \bigoplus_{i=1}^{s} C_i \right) \oplus \left( \bigoplus_{j=1}^{r} (C'_j \oplus C''_j) \right),$$

where $C_i \subseteq G^\ell_i$, $C'_j \subseteq (H'_j)^\ell$ and $C''_j \subseteq (H''_j)^\ell$.

$$C_{\perp_H} = \left( \bigoplus_{i=1}^{s} C_i^{\perp_H} \right) \oplus \left( \bigoplus_{j=1}^{r} (C''_j^{\perp_E} \oplus C'_j^{\perp_E}) \right).$$

**Theorem**

$C$ is Hermitian self-orthogonal if and only if $C_i$ is Hermitian self-orthogonal over $G_i$, for all $1 \leq i \leq s$, and $C''_j \subseteq C'_j^{\perp_E}$ (or equivalently $C'_j \subseteq C''_j^{\perp_E}$) over $H'_j = H''_j$, for all $1 \leq j \leq r$. 
Designing the Hermitian hull

Let

\[ e_i := \left[ G_i : F_{q^2} \right] = \deg(g_i(x)), \]

\[ e_j := \left[ H'_j : F_{q^2} \right] = \left[ H''_j : F_{q^2} \right] = \deg(h'_j(x)) = \deg(h''_j(x)), \]

\[ k_i := \dim(G_i(C_i)), \text{ for all } 1 \leq i \leq s, \]

\[ k'_j := \dim(H'_j(C'_j)), \text{ and } k''_j := \dim(H''_j(C''_j)), \text{ for all } 1 \leq j \leq r. \]

Let \( g_1(x) := x \pm 1 \) so that \( G_1 = F_{q^2} \) and write

\[ k = \dim(C_1) + s \sum_{i=2}^e k_i + r \sum_{j=1} e_j (k'_j + k''_j). \]

We will consider QC codes \( C \) with the Hermitian hull

\[ \dim(C \cap C^\perp_H) = \dim(C_1 \cap C_1^\perp_H) + s \sum_{i=2}^e k_i + r \sum_{j=1} e_j (k'_j + k''_j), \]

where \( e = k - \dim(C \cap C^\perp_H) = \dim(C_1) - \dim(C_1 \cap C_1^\perp_H) \).
Let

- $e_i := [G_i : \mathbb{F}_{q^2}] = \deg(g_i(x))$, 

where $e = \dim(C \cap C^\perp_H) - \dim(C_1 \cap C_1^\perp_H)$. 

Designing the Hermitian hull
Designing the Hermitian hull

Let

- $e_i := [G_i : \mathbb{F}_{q^2}] = \deg(g_i(x))$,
- $e_j := [H'_j : \mathbb{F}_{q^2}] = [H''_j : \mathbb{F}_{q^2}] = \deg(h'_j(x)) = \deg(h''_j(x))$, 

where $e = k - \dim(C \cap C^\perp_{\mathbb{H}}) = \dim(C_1) - \dim(C_1 \cap C^\perp_{\mathbb{H}_1})$. 
Designing the Hermitian hull

Let

- $e_i := [G_i : \mathbb{F}_{q^2}] = \deg(g_i(x))$,
- $e_j := [H'_j : \mathbb{F}_{q^2}] = [H''_j : \mathbb{F}_{q^2}] = \deg(h'_j(x)) = \deg(h''_j(x))$,
- $k_i := \dim_{G_i}(C_i)$, for all $1 \leq i \leq s$, 

We will consider QC codes $C$ with the Hermitian hull $\dim(C \cap C^\perp_H) = \dim(C_1 \cap C_1^\perp_H) + s \sum_{i=2} e_i k_i + r \sum_{j=1} e_j (k'_j + k''_j)$. 

Designing the Hermitian hull

Let

- \( e_i := [G_i : \mathbb{F}_{q^2}] = \deg(g_i(x)) \),
- \( e_j := [H'_j : \mathbb{F}_{q^2}] = [H''_j : \mathbb{F}_{q^2}] = \deg(h'_j(x)) = \deg(h''_j(x)) \),
- \( k_i := \dim_{G_i}(C_i) \), for all \( 1 \leq i \leq s \),
- \( k'_j := \dim_{H'_j}(C'_j) \) and \( k''_j := \dim_{H''_j}(C''_j) \), for all \( 1 \leq j \leq r \).
Designing the Hermitian hull

Let

- \( e_i := \deg(g_i(x)) \),
- \( e_j := \deg(h'_j(x)) = \deg(h''_j(x)) \),
- \( k_i := \dim_{G_i}(C_i) \), for all \( 1 \leq i \leq s \),
- \( k'_j := \dim_{H'_j}(C'_j) \) and \( k''_j := \dim_{H''_j}(C''_j) \), for all \( 1 \leq j \leq r \).

Then we have

\[
k = \sum_{i=1}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k'_j + k''_j).
\]
Designing the Hermitian hull

Let

- \( e_i := [G_i : \mathbb{F}_{q^2}] = \deg(g_i(x)) \),
- \( e_j := [H'_j : \mathbb{F}_{q^2}] = [H''_j : \mathbb{F}_{q^2}] = \deg(h'_j(x)) = \deg(h''_j(x)) \),
- \( k_i := \dim_{G_i}(C_i) \), for all \( 1 \leq i \leq s \),
- \( k'_j := \dim_{H'_j}(C'_j) \) and \( k''_j := \dim_{H''_j}(C''_j) \), for all \( 1 \leq j \leq r \).

Then we have

\[
k = \sum_{i=1}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k'_j + k''_j).
\]

Clearly, \( x - 1 \) is a self-reciprocal divisor of \( x^m - 1 \), for any \( m \), and \( x + 1 \) is another such divisor if \( m \) is even. Let \( g_1(x) := x \pm 1 \) so that \( G_1 = \mathbb{F}_{q^2} \) and
Designing the Hermitian hull

Let

- \( e_i := [G_i : \mathbb{F}_{q^2}] = \deg(g_i(x)) \),
- \( e_j := [H'_j : \mathbb{F}_{q^2}] = [H''_j : \mathbb{F}_{q^2}] = \deg(h'_j(x)) = \deg(h''_j(x)) \),
- \( k_i := \dim_{G_i}(C_i) \), for all \( 1 \leq i \leq s \),
- \( k'_j := \dim_{H'_j}(C'_j) \) and \( k''_j := \dim_{H''_j}(C''_j) \), for all \( 1 \leq j \leq r \).

Then we have

\[
k = \sum_{i=1}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k'_j + k''_j).\]

Clearly, \( x - 1 \) is a self-reciprocal divisor of \( x^m - 1 \), for any \( m \), and \( x + 1 \) is another such divisor if \( m \) is even. Let \( g_1(x) := x \pm 1 \) so that \( G_1 = \mathbb{F}_{q^2} \) and

\[
k = \dim(C_1) + \sum_{i=2}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k'_j + k''_j).\]
Let
\[ e_i := [G_i : \mathbb{F}_{q^2}] = \deg(g_i(x)), \]
\[ e_j := [H_j' : \mathbb{F}_{q^2}] = [H_j'' : \mathbb{F}_{q^2}] = \deg(h_j'(x)) = \deg(h_j''(x)), \]
\[ k_i := \dim_{G_i}(C_i), \text{ for all } 1 \leq i \leq s, \]
\[ k_j' := \dim_{H_j'}(C_j') \text{ and } k_j'' := \dim_{H_j''}(C_j''), \text{ for all } 1 \leq j \leq r. \]

Let \( g_1(x) := x \pm 1 \) so that \( G_1 = \mathbb{F}_{q^2} \) and write \( k \) as

\[ k = \dim(C_1) + \sum_{i=2}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k_j' + k_j''). \]
Designing the Hermitian hull

Let

- $e_i := [G_i : \mathbb{F}_{q^2}] = \deg(g_i(x))$,
- $e_j := [H'_j : \mathbb{F}_{q^2}] = [H''_j : \mathbb{F}_{q^2}] = \deg(h'_j(x)) = \deg(h''_j(x))$,
- $k_i := \dim G_i(C_i)$, for all $1 \leq i \leq s$,
- $k'_j := \dim H'_j(C'_j)$ and $k''_j := \dim H''_j(C''_j)$, for all $1 \leq j \leq r$.

Let $g_1(x) := x \pm 1$ so that $G_1 = \mathbb{F}_{q^2}$ and write $k$ as

$$k = \dim(C_1) + \sum_{i=2}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k'_j + k''_j).$$

We will consider QC codes $C$ with the Hermitian hull

$$\dim(C \cap C^\perp_H) = \dim(C_1 \cap C_1^\perp_H) + \sum_{i=2}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k'_j + k''_j),$$
Designing the Hermitian hull

Let

- \( e_i := [G_i : \mathbb{F}_{q^2}] = \deg(g_i(x)) \),
- \( e_j := [H'_j : \mathbb{F}_{q^2}] = [H''_j : \mathbb{F}_{q^2}] = \deg(h'_j(x)) = \deg(h''_j(x)) \),
- \( k_i := \dim_{G_i}(C_i) \), for all \( 1 \leq i \leq s \),
- \( k'_j := \dim_{H'_j}(C'_j) \) and \( k''_j := \dim_{H''_j}(C''_j) \), for all \( 1 \leq j \leq r \).

Let \( g_1(x) := x \pm 1 \) so that \( G_1 = \mathbb{F}_{q^2} \) and write \( k \) as

\[
k = \dim(C_1) + \sum_{i=2}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k'_j + k''_j).
\]

We will consider QC codes \( C \) with the Hermitian hull

\[
\dim(C \cap C^\perp_H) = \dim(C_1 \cap C^\perp_{1H}) + \sum_{i=2}^{s} e_i k_i + \sum_{j=1}^{r} e_j (k'_j + k''_j),
\]

where \( e = k - \dim(C \cap C^\perp_H) = \dim(C_1) - \dim(C_1 \cap C^\perp_{1H}) \).
Qubit example

Let $\zeta$ be a primitive element in $\mathbb{F}_4$, $m = 15$ and $\ell = 2$. 
Qubit example

Let \( \zeta \) be a primitive element in \( \mathbb{F}_4 \), \( m = 15 \) and \( \ell = 2 \).

\[
x^{15} - 1 = (x + 1)(x^2 + \zeta x + 1)(x^2 + \zeta^2 x + 1)[(x + \zeta)(x + \zeta^2)]
\]
\[
[ (x^2 + x + \zeta)(x^2 + \zeta^2 x + \zeta^2) ][ (x^2 + x + \zeta^2)(x^2 + \zeta x + \zeta) ].
\]
Let $\zeta$ be a primitive element in $\mathbb{F}_4$, $m = 15$ and $\ell = 2$.

$$x^{15} - 1 = (x + 1)(x^2 + \zeta x + 1)(x^2 + \zeta^2 x + 1)[(x + \zeta)(x + \zeta^2)]$$

$$[(x^2 + x + \zeta)(x^2 + \zeta^2 x + \zeta^2)] [(x^2 + x + \zeta^2)(x^2 + \zeta x + \zeta)].$$

We have $s = r = 3$ such that $G_1 = \mathbb{F}_4$, $G_2 = G_3 = \mathbb{F}_{16}$, $H'_1 = H''_1 = \mathbb{F}_4$ and $H'_2 = H''_2 = \mathbb{F}_{16}$, for $j \in \{2, 3\}$. 
Let \( \zeta \) be a primitive element in \( \mathbb{F}_4 \), \( m = 15 \) and \( \ell = 2 \).

\[
x^{15} - 1 = (x + 1)(x^2 + \zeta x + 1)(x^2 + \zeta^2 x + 1)[(x + \zeta)(x + \zeta^2)]
\]
\[
\quad [(x^2 + x + \zeta)(x^2 + \zeta^2 x + \zeta^2)][(x^2 + x + \zeta^2)(x^2 + \zeta x + \zeta)].
\]

We have \( s = r = 3 \) such that \( G_1 = \mathbb{F}_4, G_2 = G_3 = \mathbb{F}_{16}, H'_1 = H''_1 = \mathbb{F}_4 \)
and \( H'_j = H''_j = \mathbb{F}_{16} \), for \( j \in \{2, 3\} \).

\[
C_1 : \begin{pmatrix} 0 & 1 \\ \end{pmatrix}, C_2 : 0_2, C_3 : \begin{pmatrix} 1 & \xi^{10} \end{pmatrix},
\]
\[
C'_1 = C''_1 : \begin{pmatrix} 1 & \zeta \end{pmatrix}, C'_2 : \begin{pmatrix} 1 & 1 \end{pmatrix}, C''_2 : l_2, C'_3 = C''_3 : 0_2,
\]
where \( \xi \) is a primitive element of \( \mathbb{F}_{16} \) satisfying \( \xi^2 + \xi + \zeta = 0 \),
\( 0_2 := \begin{pmatrix} 0 & 0 \end{pmatrix} \), and \( l_2 \) denotes the \( 2 \times 2 \) identity matrix.
The QC code $C \subseteq \mathbb{F}_4^{30}$ of index 2 with those constituents has dimension 11.
Qubit example

The QC code $C \subseteq \mathbb{F}_4^{30}$ of index 2 with those constituents has dimension 11.

$C_1 : \begin{pmatrix} 0 & 1 \end{pmatrix} \implies \dim(C_1 \cap C_1^\perp_{\text{H}}) = 0 \implies e = 1 \implies \dim(C \cap C_{\perp_{\text{H}}}) = 10.$
The QC code $C \subseteq \mathbb{F}_4^{30}$ of index 2 with those constituents has dimension 11.

$C_1 : \begin{pmatrix} 0 & 1 \end{pmatrix} \implies \dim(C_1 \cap C_1^\perp) = 0 \implies e = 1 \implies \dim(C \cap C^\perp) = 10.$

$C^\perp_H$ is $[30, 19, 7]_4$ and has the best-known distance for a quaternary code of this length and dimension, and $d(C + C^\perp_H) = 6$. Thus, we get a $[31, 9, 7]_2$ stabilizer, which is strictly better than the prior best-known $[31, 9, 6]_2$ code!
The QC code $C \subseteq \mathbb{F}_4^{30}$ of index 2 with those constituents has dimension 11.

$C_1 : \begin{pmatrix} 0 & 1 \end{pmatrix} \implies \dim(C_1 \cap C_1^\perp) = 0 \implies e = 1 \implies \dim(C \cap C_1^\perp) = 10$.

$C_1^\perp$ is $[30, 19, 7]_4$ and has the best-known distance for a quaternary code of this length and dimension, and $d(C + C_1^\perp) = 6$. Thus, we get a $[31, 9, 7]_2$ stabilizer, which is strictly better than the prior best-known $[31, 9, 6]_2$ code!

The propagation rules give codes with parameters $[31, 8, 7]_2$, $[32, 9, 7]_2$ and $[30, 9, 6]_2$. Their performance matches the current best.
Let $\omega$ be a primitive element in $\mathbb{F}_9$, $m = 8$ and $\ell = 2$. 
Let $\omega$ be a primitive element in $\mathbb{F}_9$, $m = 8$ and $\ell = 2$.

$$x^8 - 1 = \prod_{j=0}^{7} (x + \omega^j) = (x + 1)(x - 1) \prod_{j=1}^{3} [(x + \omega^j)(x + \omega^{-j})] ,$$
Let $\omega$ be a primitive element in $\mathbb{F}_9$, $m = 8$ and $\ell = 2$.

$$x^8 - 1 = \prod_{j=0}^{7}(x + \omega^j) = (x + 1)(x - 1) \prod_{j=1}^{3} [(x + \omega^j)(x + \omega^{-j})],$$

We have $s = 2$ and $r = 3$ such that $G_i = H_j' = H_j'' = \mathbb{F}_9$, for all $i \in \{1, 2\}$ and $j \in \{1, 2, 3\}$. 
Let $\omega$ be a primitive element in $\mathbb{F}_9$, $m = 8$ and $\ell = 2$.

$$x^8 - 1 = \prod_{j=0}^{7} (x + \omega^j) = (x + 1)(x - 1) \prod_{j=1}^{3} [(x + \omega^j)(x + \omega^{-j})],$$

We have $s = 2$ and $r = 3$ such that $G_i = H'_j = H''_j = \mathbb{F}_9$, for all $i \in \{1, 2\}$ and $j \in \{1, 2, 3\}$.

$$C_1 : \begin{pmatrix} 1 & \omega^2 \end{pmatrix}, C_2 : 0_2, C'_1 : l_2, C''_1 : 0_2,$$
$$C'_2 : 0_2, C''_2 : \begin{pmatrix} 1 & \omega^7 \end{pmatrix}, C'_3 : \begin{pmatrix} 1 & \omega^6 \end{pmatrix}, C''_3 : 0_2.$$
Qutrit example

The QC code $C$ of index 2 over $\mathbb{F}_9$ with those constituents has dimension 5.
Qutrit example

The QC code $C$ of index 2 over $\mathbb{F}_9$ with those constituents has dimension 5.

$C_1 : \begin{pmatrix} 1 & \omega^2 \end{pmatrix} \implies \dim(C_1 \cap C_1^{\perp_H}) = 0 \implies e = 1 \implies \dim(C \cap C^{\perp_H}) = 4.$
Qutrit example

The QC code $C$ of index 2 over $\mathbb{F}_9$ with those constituents has dimension 5.

$C_1 : \begin{pmatrix} 1 & \omega^2 \end{pmatrix} \implies \dim(C_1 \cap C_1^{\perp_H}) = 0 \implies e = 1 \implies \dim(C \cap C^{\perp_H}) = 4.$

$C^{\perp_H}$ is a $[16, 11, 5]_9$ code, which attains the best-known distance for a nonary code of this length and dimension. The minimum distance of $C + C^{\perp_H}$ is 4 and we obtain an optimal $[17, 7, 5]_3$ code whose distance reaches the upper bound. The previous best-known was a $[17, 7, 4]_3$ code.
Qutrit example

The QC code $C$ of index 2 over $\mathbb{F}_9$ with those constituents has dimension 5.

$$C_1 : \begin{pmatrix} 1 & \omega^2 \end{pmatrix} \implies \dim(C_1 \cap C_1^\perp_H) = 0 \implies e = 1 \implies \dim(C \cap C_1^\perp_H) = 4.$$ 

$C_1^\perp_H$ is a $[16, 11, 5]_9$ code, which attains the best-known distance for a nonary code of this length and dimension. The minimum distance of $C + C_1^\perp_H$ is 4 and we obtain an optimal $[17, 7, 5]_3$ code whose distance reaches the upper bound. The previous best-known was a $[17, 7, 4]_3$ code.

The propagation rules give us two codes, with respective parameters $[17, 6, 5]_3$ and $[18, 7, 5]_3$. They are strictly better than the $[17, 6, 4]_3$ and $[18, 7, 4]_3$ codes that held the previous record. The other derived code, with parameter $[16, 7, 4]_3$, merely matches that of the current record holder.