Feng-Rao decoding of primary codes

Olav Geil, Diego Ruano
Aalborg University

Ryutaroh Matsumoto
Tokyo Institute of Technology

DTU, August 2012
Decoding of primary order domain codes up to half the designed distance given by Andersen-Geil’s bound.

Procedure: Given basis \( \{ \vec{g}_1, \ldots, \vec{g}_n \} \) for \( \mathbb{F}_q^n \). Write \( G = [\vec{g}_1, \ldots, \vec{g}_n]^T \) and let \( \vec{h}_n, \ldots, \vec{h}_1 \) be the columns of \( H = G^{-1} \). For any linear span of \( \vec{g}_i \)'s apply Feng-Rao decoding to the couple \((G, H)\).

The description and analysis of primary code may be given in any (abstract) language, but decoding involves translation to linear algebra.

The Feng-Rao bound and the bound by Andersen-Geil are consequences of each other (requires TWO bases).

Bases $\mathbf{B} = \{ \vec{b}_1, \ldots, \vec{b}_n \}$ and $\mathcal{U} = \{ \vec{u}_1, \ldots, \vec{u}_n \}$.

$C(\mathbf{B}, I) = \text{span}_{\mathbb{F}_q}\{ \vec{b}_i \mid i \in I \}$.

$L_{-1} = \emptyset$, $L_0 = \{ \vec{0} \}$, $L_s = \text{span}_{\mathbb{F}_q}\{ \vec{b}_1, \ldots, \vec{b}_s \}$.

$\bar{\rho}_\mathbf{B}(\vec{v}) = s$ if $\vec{v} \in L_s \setminus L_{s-1}$.

$(i, j)$ is WB with respect to $(\mathbf{B}, \mathcal{U})$ if

$$\bar{\rho}_\mathbf{B}(\vec{b}_u \ast \vec{u}_v) < \bar{\rho}_\mathbf{B}(\vec{b}_i \ast \vec{u}_j)$$

holds for all $u$ and $v$ with $1 \leq u \leq i$, $1 \leq v \leq j$ and $(u, v) \neq (i, j)$.

$(i, j)$ is OWB with respect to $(\mathbf{B}, \mathcal{U})$ if

$$\bar{\rho}_\mathbf{B}(\vec{b}_u \ast \vec{u}_j) < \bar{\rho}_\mathbf{B}(\vec{b}_i \ast \vec{u}_j)$$

holds for $u < i$. 
Bases $\mathcal{B} = \{\vec{b}_1, \ldots, \vec{b}_n\}$ and $\mathcal{U} = \{\vec{u}_1, \ldots, \vec{u}_n\}$.

\[\bar{\mu}_{\mathcal{B}}^\text{WB}(s) = \#\{i \in \{1, 2, \ldots, n\} \mid \tilde{\rho}(\vec{b}_i \ast \vec{u}_{\bar{j}}) = s \text{ for some } \vec{u}_j \in \mathcal{U} \text{ with } (i, j) \text{ WB}\}\]

\[\bar{\sigma}_{\mathcal{B}}^\text{WB}(i) = \#\{s \in \{1, 2, \ldots, n\} \mid \tilde{\rho}(\vec{b}_i \ast \vec{u}_{\bar{j}}) = s \text{ for some } \vec{u}_j \in \mathcal{U} \text{ with } (i, j) \text{ WB}\}\]

**Feng-Rao:**
\[d(C(\mathcal{B}, I)^\perp) \geq \min\{\bar{\mu}_{\mathcal{B}}^\text{WB}(s) \mid s \in \{1, 2, \ldots, n\} \setminus I\}.\]

**Andersen-Geil:**
\[d(C(\mathcal{B}, I)) \geq \min\{\bar{\sigma}_{\mathcal{B}}^\text{WB}(s) \mid s \in I\}.\]
Two choices of $\mathcal{B}$

- $\mathcal{G} = \{\vec{g}_1, \ldots, \vec{g}_n\}$ and $\mathcal{H} = \{\vec{h}_1, \ldots, \vec{h}_n\}$.
- Assume $\vec{g}_i \cdot \vec{h}_j = \delta_{i,n-j+1}$.
- $\bar{I} = \{1, \ldots, n\} \backslash \{n - i + 1 \mid i \in I\}$.

Keep $\mathcal{U}$ fixed.
Replace $\mathcal{B}$ with $\mathcal{G}$ and consider $C(\mathcal{G}, I)$.
Replace $\mathcal{B}$ with $\mathcal{H}$ and consider $C^\perp(\mathcal{H}, \bar{I})$.

We get,

$$C(\mathcal{G}, I) = C^\perp(\mathcal{H}, \bar{I}).$$
The bonds are consequences of each other

Lemma: The following statements are equivalent

1. \( \bar{\rho}_G(\tilde{g}_i \ast \tilde{u}_j) = k \)
   and \((i, j)\) is WB with respect to \((G, U)\).

2. \( \bar{\rho}_H(\tilde{h}_{n-k+1} \ast \tilde{u}_j) = n - i + 1 \)
   and \((n - k + 1, j)\) is WB with respect to \((H, U)\).

Proposition:

1. \( \bar{\mu}_{WB}^H(n - i + 1) = \bar{\sigma}_{WB}^B(i) \)

2. \( \bar{\mu}_{OWB}^H(n - i + 1) = \bar{\sigma}_{OWB}^B(i) \)

Above holds also for OWB, but not for WWB.

We do need \( U \).
Decoding of primary code

- A primary code is often described as $C(\mathcal{B}, I)$ where $\mathcal{B} = \mathcal{U} = \mathcal{G}$.
- If algebraically defined then we often have information on $\bar{\sigma}^{WB}$.
- Determine $H = G^{-1}$.
- Apply Matsumoto-Miura’s generalization of the majority voting algorithm from Høholdt, van Lint, and Pellikaan’s chapter in the handbook.
- The generalization is needed because WB-properties of $C^\perp(\mathcal{H}, \bar{I})$ use two bases.
Previous work on Algebraic geometric codes

- **One-point codes**: Matsumoto-Miura (2000)
- **More-point codes**: Beelen-Høholdt (2008)

In their work:
- Use $\left( C_\Omega(D, G) \right)^\perp = C_\mathcal{L}(D, G)$.
- $GH$ is triangular (rather than equal to $I$).
- Connection to Andersen-Geil’s bound not easy to see.
- Not obvious how to generalize to higher transcendence degree or general linear code.
- Improved codes might be different from Andersen-Geil’s, but parameters the same.
Example: Higher transcendence degree

Point-ensemble \( \{1, 2, 3\} \times \{1, 2, 3\} \subseteq \mathbb{F}_5^2 \).

\( \vec{g}_1 = \text{ev}(1), \vec{g}_2 = \text{ev}(X), \vec{g}_3 = \text{ev}(Y), \vec{g}_4 = \text{ev}(X^2), \vec{g}_5 = \text{ev}(XY), \vec{g}_6 = \text{ev}(Y^2), \vec{g}_7 = \text{ev}(X^2Y), \vec{g}_8 = \text{ev}(XY^2), \vec{g}_9 = \text{ev}(X^2Y^2) \)

\( \vec{h}_1 = \text{ev}(X^2Y^2 + XY^2 + X^2Y + XY) \)
\( \vec{h}_2 = \text{ev}(X^2Y^2 + 3XY^2 + X^2Y + Y^2 + 3XY + Y) \)
\( \vec{h}_3 = \text{ev}(X^2Y^2 + XY^2 + 3X^2Y + 3XY + X^2 + X) \)
\( \vec{h}_4 = \text{ev}(XY^2 + Y^2 + XY + Y) \)
\( \vec{h}_5 = \text{ev}(X^2Y^2 + 3XY^2 + 3X^2Y + Y^2 + 4XY + X^2 + 3Y + 3X + 1) \)
\( \vec{h}_6 = \text{ev}(X^2Y + XY + X^2 + X) \)
\( \vec{h}_7 = \text{ev}(XY^2 + Y^2 + 3XY + 3Y + X + 1) \)
\( \vec{h}_8 = \text{ev}(X^2Y + 3XY + X^2 + Y + 3X + 1) \)
\( \vec{h}_9 = \text{ev}(XY + Y + X + 1) \).
A more predictable example

Point-ensemble $\mathbb{F}_3^2$.

$$
\mathcal{G} = \{ \vec{g}_1 = \text{ev}(1), \vec{g}_2 = \text{ev}(X), \vec{g}_3 = \text{ev}(Y), \vec{g}_4 = \text{ev}(X^2), \vec{g}_5 = \text{ev}(XY), \\
\vec{g}_6 = \text{ev}(Y^2), \vec{g}_7 = \text{ev}(X^2Y), \vec{g}_8 = \text{ev}(XY^2), \vec{g}_9 = \text{ev}(X^2Y^2) \}
$$

$$
\mathcal{H} = \{ \vec{h}_1 = \text{ev}(1), \vec{h}_2 = \text{ev}(X), \vec{h}_3 = \text{ev}(Y), \vec{h}_4 = \text{ev}(X^2 + 2), \\
\vec{h}_5 = \text{ev}(XY), \vec{h}_6 = \text{ev}(Y^2 + 2), \vec{h}_7 = \text{ev}(X^2Y + 2Y), \\
\vec{h}_8 = \text{ev}(XY^2 + 2X), \vec{h}_9 = \text{ev}(X^2Y^2 + 2X^2 + 2Y^2 + 1) \}.
$$
We propose the following names:

- The Feng-Rao bound for dual codes.
- The Feng-Rao bound for primary codes.
- The order bound for dual codes.
- The order bound for primary codes.