1 Testing Gabidulin Gao-like Decoder

Purpose of the Test Given the Gabidulin code $\mathrm{Gab}[n,k]$ over $\mathbb{F}_{q^m}$ of length $n \leq m$, dimension $k \leq n$ and minimum rank distance $d = n - k + 1$. The purpose is to check the correctness of the encoding and the decoding using the Gao-like decoder for different scenarios specified in the following sections.

1.1 Decoding with Number of Errors below the Decoding Radius

1.1.1 Using a Polynomial Basis and $n = m$

Test Parameters:

- $\mathrm{Gab}[5,2]$ over $\mathbb{F}_{4^5}$ with $n = m = 5$, dimension $k = 2$ and polynomial basis $1, \alpha, \alpha^2, \cdots, \alpha^4$.
- $\mathrm{Gab}[60,20]$ over $\mathbb{F}_{9^{60}}$ with $n = m = 60$, dimension $k = 20$ and polynomial basis $1, \alpha, \alpha^2, \cdots, \alpha^{59}$.
- Number of errors $t \leq \lfloor (n-k)/2 \rfloor$.
- Message polynomial $f(x) \in \mathcal{L}_{q^m}[x]$ where $\deg_q(f(x)) < k$.

Expected Results:

- Successful decoding for any $t \leq \lfloor (n-k)/2 \rfloor$.

Remarks:

- Successful decoding as expected.

1.1.2 Using a Polynomial Basis and $n < m$

Test Parameters:

- Gab[4, 2] over $\mathbb{F}_{4^5}$ with $n = 4$, $m = 5$, dimension $k = 2$ and polynomial basis $1, \alpha, \alpha^2, \cdots, \alpha^3$.
- Gab[30, 20] over $\mathbb{F}_{9^{60}}$ with $n = 30$, $m = 60$, $k = 20$ and polynomial basis $1, \alpha, \alpha^2, \cdots, \alpha^{29}$.
- Number of errors $t \leq \lfloor (n-k)/2 \rfloor$.
- Message polynomial $f(x) \in \mathcal{L}_{q^m}[x]$ where $\deg_q(f(x)) < k$.

Expected Results:

- Successful decoding for any $t \leq \lfloor (n-k)/2 \rfloor$.

Remarks:

- Successful decoding as expected.

1.1.3 Using a Normal Basis and $n = m$

Test Parameters:

- Gab[5, 2] over $\mathbb{F}_{4^5}$ with $n = m = 5$, dimension $k = 2$ and a normal basis $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^4}$.
- Gab[20, 10] over $\mathbb{F}_{9^{20}}$ with $n = m = 20$, dimension $k = 10$ and a normal basis $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{19}}$.
- Number of errors $t \leq \lfloor (n-k)/2 \rfloor$.
- Message polynomial $f(x) \in \mathcal{L}_{q^m}[x]$ where $\deg_q(f(x)) < k$.

Expected Results:

- Successful decoding for any $t \leq \lfloor (n-k)/2 \rfloor$.

Remarks:

- Successful decoding as expected.

1.1.4 Using a Normal Basis and $n < m$

Test Parameters:

- Gab[4, 2] over $\mathbb{F}_{4^8}$ with $n = 4$, $m = 8$, dimension $k = 2$ and a normal basis $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^3}$.
- Gab[10, 5] over $\mathbb{F}_{9^{20}}$ with $n = 10$, $m = 20$, $k = 5$ and a normal basis $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^9}$.
- Number of errors $t \leq \lfloor (n-k)/2 \rfloor$.
- Message polynomial $f(x) \in \mathcal{L}_{q^m}[x]$ where $\deg_q(f(x)) < k$.

Expected Results:

- Successful decoding for any $t \leq \lfloor (n-k)/2 \rfloor$.

Remarks:

- The code is not implemented for a normal basis when $n < m$.

1.2 Decoding with Number of Errors above the Decoding Radius

1.2.1 Using a Polynomial Basis and $n = m$

Test Parameters:

- Gab[5, 2] over $\mathbb{F}_{4^5}$ with $n = m = 5$, dimension $k = 2$ and polynomial basis $1, \alpha, \alpha^2, \cdots, \alpha^4$.
- Gab[60, 20] over $\mathbb{F}_{9^{60}}$ with $n = m = 60$, dimension $k = 20$ and polynomial basis $1, \alpha, \alpha^2, \cdots, \alpha^{59}$.
- Number of errors $t = \lfloor (n-k)/2 \rfloor + 1$.
- Message polynomial $f(x) \in \mathcal{L}_{q^m}[x]$ where $\deg_q(f(x)) < k$.

Expected Results:

- Decoding failure for any $t > \lfloor (n-k)/2 \rfloor$.

Remarks:

- Decoding failure as expected.

1.2.2 Using a Polynomial Basis and $n < m$

Test Parameters:

- Gab[4, 2] over $\mathbb{F}_{4^5}$ with $n = 4$, $m = 5$, dimension $k = 2$ and polynomial basis $1, \alpha, \alpha^2, \cdots, \alpha^3$.
- Gab[30, 20] over $\mathbb{F}_{9^{60}}$ with $n = 30$, $m = 60$, $k = 20$ and polynomial basis $1, \alpha, \alpha^2, \cdots, \alpha^{29}$.
- Number of errors $t = \lfloor (n-k)/2 \rfloor + 1$.
- Message polynomial $f(x) \in \mathcal{L}_{q^m}[x]$ where $\deg_q(f(x)) < k$.

Expected Results:

- Decoding failure for any $t > \lfloor (n-k)/2 \rfloor$.

Remarks:

- Decoding failure as expected.

1.2.3 Using a Normal Basis and $n = m$

Test Parameters:

- Gab[5, 2] over $\mathbb{F}_{4^5}$ with $n = m = 5$, dimension $k = 2$ and a normal basis $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^4}$.
- Gab[20, 10] over $\mathbb{F}_{9^{20}}$ with $n = m = 20$, dimension $k = 10$ and a normal basis $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{19}}$.
- Number of errors $t = \lfloor (n-k)/2 \rfloor + 1$.
- Message polynomial $f(x) \in \mathcal{L}_{q^m}[x]$ where $\deg_q(f(x)) < k$.

Expected Results:

- Decoding failure for any $t > \lfloor (n-k)/2 \rfloor$.

Remarks:

- Decoding failure as expected.

1.2.4 Using a Normal Basis and $n < m$

Test Parameters:

- Gab[4, 2] over $\mathbb{F}_{4^{12}}$ with $n = 4$, $m = 12$, dimension $k = 2$ and a normal basis $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^3}$.
- Gab[10, 5] over $\mathbb{F}_{9^{20}}$ with $n = 10$, $m = 20$, $k = 5$ and a normal basis $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^9}$.

- Number of errors $t = \lfloor (n-k)/2 \rfloor + 1$.
- Message polynomial $f(x) \in \mathcal{L}_{q^m}[x]$ where $\deg_q(f(x)) < k$.

Expected Results:

- Decoding failure for any $t > \lfloor (n-k)/2 \rfloor$.

Remarks:

- Decoding failure as expected.
- The code is not implemented for a normal basis when $n < m$.

1.3 Summary

In summary, these results show that the Gao-like decoder is always guaranteed to decode successfully up to $\lfloor (n-k)/2 \rfloor$ errors. However, when the number of errors exceeds $\lfloor (n-k)/2 \rfloor$, the Gao-like decoder results always in decoding failure.