Multi-Dimensional Nonsystematic Reed-Solomon Codes

Akira Shiozaki *

May 2, 2014

Abstract

This paper proposes a new class of multi-dimensional nonsystematic Reed-Solomon codes that are constructed based on the multi-dimensional Fourier transform over a finite field. The proposed codes are the extension of the nonsystematic Reed-Solomon codes to multi-dimension. This paper also discusses the performance of the multi-dimensional nonsystematic Reed-Solomon codes.

Index terms: Reed-Solomon codes, multi-dimensional, Fourier transform, error correction, error-correcting-codes

1 Introduction

Many error-correcting-codes [1],[2] have been developed to enhance the reliability of data transmission systems and memory systems. One class of superior error-correcting-codes is the Reed-Solomon codes that are maximum-distance codes. The nonsystematic Reed-Solomon codes [3] are constructed based on the one-dimensional Fourier transforms over a finite field. The code length of the nonsystematic Reed-Solomon codes over a finite field \( GF(q) \) is \( q \), while the code length of the systematic and cyclic Reed-Solomon codes is \( q - 1 \).

The author presented the two-dimensional nonsystematic Reed-Solomon codes based on two-dimensional Fourier transform [4] and showed the extension of the codes to multi-dimensional codes [5]. On the other hand, Shen, et al. [6] presented the multidimensional extension of the Reed-Solomon codes using a location set contained in a multidimensional affine or projective space over a finite field. But they described only the two-dimensional extension concretely.

This paper proposes a new class of multi-dimensional nonsystematic Reed-Solomon codes that are constructed based on the multi-dimensional Fourier transform over a finite field. The proposed codes are the extension of the nonsystematic Reed-Solomon codes to multi-dimension, and are the developments of the codes in [5]. The code length of the \( n \)-dimensional nonsystematic Reed-Solomon codes over a finite field \( GF(q) \) is \( q^n \). This paper also discusses the performance of the multi-dimensional nonsystematic Reed-Solomon codes.

2 2-dimensional Reed-Solomon codes

Firstly, we consider the following codes based on 2-dimensional Fourier transform.

Let \( a_{ij} \) (\( 0 \leq i \leq K_j; 0 \leq j \leq L \)) be any elements of a finite field \( GF(q) \) and let \( f(x_1, x_2) \) be a polynomial of two variables whose coefficients are \( a_{ij} \):

\[
f(x_1, x_2) = \sum_{j=0}^{L} \left( \sum_{i=0}^{K_j} a_{ij} x_1^i \right) x_2^j
\]

\[
= \sum_{j=0}^{L} f_j(x_1) x_2^j \quad (L \leq q - 1)
\]

\[
f_j(x_1) = \sum_{i=0}^{K_j} a_{ij} x_1^i \quad (K_j \leq q - 1)
\]

We consider the code whose codeword consists of \( q^2 \) elements \( \{ f(\beta_k, \beta_l) \} \) (\( k = 0, 1, \cdots, q - 1; l = 0, 1, \cdots, q - 1 \)), where \( \beta_k \) and \( \beta_l \) are any elements of \( GF(q) \). The transformation of the information symbols \( \{ a_{ij} \} \) to a codeword

*Emeritus professor, Osaka Prefecture University, Japan. E-mail: shiozaki.akira@gmail.com
is at most $q - m$ because the number of the roots of $f_j(x_1)$ is at most $K_j$.

A nonzero codeword has at least one $f_j(x_1)$ ($0 \leq j \leq L$) such that $f_j(x_1) \neq 0$. Now let $m$ be the maximum $j$ of the nonzero $f_j(x_1)$, that is, $f_m(x_1) \neq 0$, $f_{m+1}(x_1) = f_{m+2}(x_1) = \cdots = f_L(x_1) = 0$. The number of $\beta_k$ such that $f_m(\beta_k) \neq 0$ is at least $q - K_m$. For an element $\beta_k$ such that $f_j(\beta_k) \neq 0$ ($0 \leq j \leq m$), the number of $\beta_i$ such that $f(\beta_i, \beta_i) \neq 0$ is at least $q - m$ because the number of the roots of

$$f(\beta_k, x_2) = \sum_{j=0}^{m} f_j(\beta_k)x_2^j$$

is at most $m$. Therefore the number of the pairs $(\beta_k, \beta_i)$ such that $f(\beta_k, \beta_i) \neq 0$ is at least

$$\min_{0 \leq m \leq L} [(q - K_m)(q - m)]$$

and it is equal to the minimum distance $d_{\text{min}}$ of the code. From Eq. (4), $K_m = q - \lceil \frac{d_{\text{min}}}{q - m} \rceil$ because $q - K_m$ ($m = 0, 1, \cdots, L$) must be $\lceil \frac{d_{\text{min}}}{q - m} \rceil$. $L$ should be determined as the maximum integer such that $K_L = q - \lceil \frac{d_{\text{min}}}{q - L} \rceil \geq 0$. Then the number of the information symbols $K$ is

$$K = \sum_{m=0}^{L} (K_m + 1) = \sum_{m=0}^{L} \left( q + 1 - \lceil \frac{d_{\text{min}}}{q - m} \rceil \right)$$

and the number of the check symbols $N - K = q^2 - K$ is

$$N - K = \sum_{m=0}^{L} \left( \lfloor \frac{d_{\text{min}}}{q - m} \rfloor - 1 \right) + q(q - L - 1).$$

The above statement is summarized in the following theorem:

[Theorem 1] Let $a_{ij}$ ($0 \leq i \leq K_j; 0 \leq j \leq L$) be any elements of a finite field $GF(q)$, where $K_j$ is $K_j = q - \lceil \frac{d_{\text{min}}}{q - j} \rceil$ and $L$ is the maximum integer such that $K_L = q - \lceil \frac{d_{\text{min}}}{q - L} \rceil \geq 0$.

For a polynomial of two variables such that

$$f(x_1, x_2) = \sum_{j=0}^{L} \sum_{i=0}^{K_j} a_{ij}x_1^ix_2^j,$$

the code whose codeword consists of $q^2$ elements $f(\beta_k, \beta_i)$ ($k = 0, 1, \cdots, q - 1; l = 0, 1, \cdots, q - 1$) is a linear code with minimum distance $d_{\text{min}}$, where $\beta_k$ and $\beta_i$ are the elements of $GF(q)$.

Figure 1 shows the example of a 2-dimensional Reed-Solomon code. Table 1 shows the distribution of $K_m$ in case of $q = 5$.

![Figure 1: 2-dimensional Reed-Solomon codes](image)

\[\text{[x]}\] denotes the minimum integer not less than $x$
Table 1: Number of information symbols of 2-dimensional Reed-Solomon code \((q = 5)\)

| \(d_{\text{min}}\) | \(m\) | \(K_m\) | \(d_{\text{min}}\) | \(m\) | \(K_m\) | \(d_{\text{min}}\) | \(m\) | \(K_m\) | \(d_{\text{min}}\) | \(m\) | \(K_m\) |
|-----------------|------|-------|-----------------|------|-------|-----------------|------|-------|-----------------|------|-------|
| 3               | 0    | 4     | 1               | 4    | 1     | 2               | 4    | 2     | 3               | 4    | 2     |
| 1               | 1    | 4     | 1               | 1    | 3     | 2               | 3    | 2     | 3               | 2    | 3     |
| 2               | 4    | 4     | 1               | 1    | 4     | 4               | 2    | 4     | 4               | 0    | 4     |
| 3               | 3    | 3     | 3               | 3    | 3     | 3               | 2    | 3     | 3               | 0    | 0     |
| 4               | 2    | 2     | 4               | 1    | 4     | 4               | 0    | 0     | 4               | 0    | 3     |
| \(K = 22\)     | \(K = 20\) | \(K = 17\) | \(K = 15\)     |

\[
K = L \sum_{m=0}^{L} \left( q + 1 - \left\lceil \frac{d_{\text{min}}}{q - m} \right\rceil \right)
\geq L \sum_{m=0}^{L} \left( q - \frac{d_{\text{min}}}{q - m} \right) \quad \text{(because} \left\lceil \frac{d_{\text{min}}}{q - m} \right\rceil \leq \frac{d_{\text{min}}}{q - m} + 1) \]

\[
K = L - L \sum_{m=0}^{L} \frac{d_{\text{min}}}{q - m} > L \left( q - \frac{d_{\text{min}}}{q - m} \right) - d_{\text{min}} L \sum_{m=0}^{L} \frac{1}{q - m} \quad \left( L > q - \frac{d_{\text{min}}}{q - m} \because q \geq \left\lceil \frac{d_{\text{min}}}{q - L} \right\rceil \right)
\]

\[
K > q^2 - d_{\text{min}} - \frac{d_{\text{min}}}{q - m} \sum_{m=0}^{L} \frac{1}{q - m} \quad \left( L \leq q - \frac{d_{\text{min}}}{q} \right). \quad (8)
\]

So

\[
\frac{K}{N} > 1 - \frac{d_{\text{min}}}{N} - \frac{d_{\text{min}}}{N} \sum_{m=0}^{L} \frac{1}{q - m} \quad (9)
\]

Figure 2 shows the relation between \(d_{\text{min}}/N\) and \(K/N\).

### 3 3-dimensional Reed-Solomon codes

We extend the discussion in the preceding chapter to 3-dimensional Fourier transform over a finite field.

Let \(a_{ij,k} \quad (0 \leq i_1 \leq K_{ij} ; \ 0 \leq i_2 \leq L_i ; \ 0 \leq i_3 \leq L)\) be any elements of a finite field \(GF(q)\), and let \(f(x_1, x_2, x_3)\) be a polynomial of three variables whose coefficients are \(a_{ij,k}\):

\[
f(x_1, x_2, x_3) = \sum_{i_1=0}^{L_{i_1}} \sum_{i_2=0}^{L_{i_2}} \left( \sum_{i_3=0}^{K_{ij,k}} a_{ij,k} x_1^{i_1} x_2^{i_2} x_3^{i_3} \right)
\]

\[
= \sum_{i_2=0}^{L_{i_2}} \sum_{i_3=0}^{L} \left( f_{ij} (x_2) \ x_2^{i_2} x_3^{i_3} \right) \quad (10)
\]
We consider the code whose codeword consists of \( q^3 \) elements \( \{ f(\beta_{k_1}, \beta_{k_2}, \beta_{k_3}) \} \) \((k_j = 0, 1, \ldots, q - 1)\), where \( \beta_{k_j} \) \((j = 1, 2, 3)\) are any elements of \( GF(q) \). The transformation of the information symbols \( \{ a_{i_1i_2i_3} \} \) to a codeword \( \{ f(\beta_{k_1}, \beta_{k_2}, \beta_{k_3}) \} \) is the three-dimensional Fourier transform over \( GF(q) \), and so the code is the three-dimensional extension of a non-systematic Reed-Solomon code. The code length \( N \) is \( N = q^3 \).

When \( f_{i_1i_2i_3}(x_1) \neq 0 \), the number of \( \beta_{k_1} \) \((0 \leq k_1 \leq q - 1)\) such that \( f_{i_1i_2i_3}(\beta_{k_1}) \neq 0 \) is at least \( q - K_{i_1i_2} \), because the number of the roots of \( f_{i_1i_2i_3}(x_1) \) is at most \( K_{i_1i_2} \).

Now let \( m_2 \) be the maximum \( i_2 \) of the nonzero \( f_{i_1i_2i_3}(x_1) \) and let \( m_3 \) be the maximum \( i_3 \) of the nonzero \( f_{i_1i_2i_3}(x_1) \). Then let \( K_{m_2,m_3} \) be the maximum \( i_1 \) in this case.

For the equations

\[
f(\beta_{k_1}, x_2, x_3) = \sum_{i_3=0}^{m_3} \left( \sum_{i_2=0}^{m_2} f_{i_1i_2i_3}(\beta_{k_1}) x_2^{i_2} \right) x_3^{i_3} = \sum_{i_3=0}^{m_3} f_{i_1i_3}(\beta_{k_1}, x_2) x_3^{i_3}
\]

and

\[
f_{i_1i_2i_3}(\beta_{k_1}, x_2) = \sum_{i_3=0}^{m_3} f_{i_1i_2i_3}(\beta_{k_1}) x_2^{i_2},
\]

the number of \( \beta_{k_1} \) such that \( f_{i_1}(\beta_{k_1}, \beta_{k_2}) \neq 0 \) is at least \( q - m_2 \) because the number of the roots of \( f_{i_1}(\beta_{k_1}, x_2) \) is at most \( m_2 \). For \( \beta_{k_2} \) such that \( f_{i_1}(\beta_{k_1}, \beta_{k_2}) \neq 0 \), the number of \( \beta_{k_3} \) such that \( f(\beta_{k_1}, \beta_{k_2}, \beta_{k_3}) \neq 0 \) is at least \( q - m_3 \) because the number of the roots of

\[
f(\beta_{k_1}, \beta_{k_2}, x_3) = \sum_{i_3=0}^{m_3} f_{i_1i_3}(\beta_{k_1}, \beta_{k_2}) x_3^{i_3}
\]

is at most \( m_3 \). Therefore the number of the three-tuples \( (\beta_{k_1}, \beta_{k_2}, \beta_{k_3}) \) such that \( f(\beta_{k_1}, \beta_{k_2}, \beta_{k_3}) \neq 0 \) is at least

\[
\min_{0 \leq m_2 \leq L, 0 \leq m_3 \leq L} \{ (q - K_{m_2,m_3})(q - m_2)(q - m_3) \},
\]

and it is equal to the minimum distance \( d_{\text{min}} \) of the code.

From Eq. (15), \( K_{m_2,m_3} = q - \lceil \frac{d_{\text{min}}}{(q-m_2)(q-m_3)} \rceil \) because \( q - K_{m_2,m_3} \) \((m_2 = 0, 1, \ldots, L; m_3 = 0, 1, \ldots, L)\) must be \( \lceil \frac{d_{\text{min}}}{(q-m_2)(q-m_3)} \rceil \). \( L_{m_2} \) and \( L \) should be respectively determined as the maximum \( m_2 \) and the maximum \( m_3 \) such that
\(K_{m_2m_1} = q - \left\lfloor \frac{d_{\text{min}}}{(q-m_2)(q-m_3)} \right\rfloor \geq 0\). Then the number of the information symbols \(K\) is

\[
K = \sum_{m_1=0}^{L} \sum_{m_2=0}^{L_{m_1}} (K_{m_2m_1} + 1) = \sum_{m_1=0}^{L} \sum_{m_2=0}^{L_{m_1}} \left( q + 1 - \left\lfloor \frac{d_{\text{min}}}{(q-m_2)(q-m_3)} \right\rfloor \right)
\]

(16)

and the number of the check symbols \(N-K = q^3-K\) is

\[
N-K = \sum_{m_1=0}^{L} \sum_{m_2=0}^{L_{m_1}} \left( \left\lfloor \frac{d_{\text{min}}}{(q-m_2)(q-m_3)} \right\rfloor - 1 \right) + q^3 - q(L+1)(L_{m_1} + 1).
\]

(17)

The above statement is summarized in the following theorem:

[Theorem 2] Let \(a_{i_1i_2i_3} (0 \leq i_1 \leq L_{i_1}; 0 \leq i_2 \leq L_{j}; 0 \leq i_3 \leq L)\) be any elements of a finite field \(GF(q)\), where \(K_{i_1j} = q - \left\lfloor \frac{d_{\text{min}}}{(q-i_1j)(q-i_3)} \right\rfloor\) and \(L_{i_3}\) and \(L\) are the maximum integers such that \(K_{L_{i_3}L} = q - \left\lfloor \frac{d_{\text{min}}}{(q-L_{i_3}L)} \right\rfloor \geq 0\). For a polynomial of three variables such that

\[
f(x_1, x_2, x_3) = \sum_{i_3=0}^{L} \sum_{i_2=0}^{L_{i_3}} \sum_{i_1=0}^{K_{i_1i_2i_3}} a_{i_1i_2i_3} x_1^{i_1} x_2^{i_2} x_3^{i_3},
\]

(18)

the code whose codeword consists of \(q^3\) elements \(\{f(\beta_{k_1}, \beta_{k_2}, \beta_{k_3})\} (k_l = 0, 1, \cdots, q-1; l = 1, 2, 3)\) is a linear code with minimum distance \(d_{\text{min}}\), where \(\beta_{k_1}, \beta_{k_2}, \beta_{k_3}\) are the elements of \(GF(q)\). \(\square\)

## 4 \(n\)-dimensional Reed-Solomon codes

We extend the discussion in the preceding chapter to \(n\)-dimensional Fourier transform over a finite field.

Let \(a_{i_1i_2i_3} (0 \leq i_1 \leq K_{i_1j}; 0 \leq i_2 \leq L_{i_1i_2}; 0 \leq i_3 \leq L)\) be any elements of a finite field \(GF(q)\), and let a polynomial of \(n\) variables whose coefficients are \(a_{i_1i_2i_3}\):

\[
f(x_1, x_2, \cdots, x_n) = \sum_{i_3=0}^{L} \sum_{i_2=0}^{L_{i_3}} \sum_{i_1=0}^{K_{i_1i_2i_3}} a_{i_1i_2i_3} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_3} = \sum_{i_3=0}^{L} \sum_{i_2=0}^{L_{i_3}} \sum_{i_1=0}^{K_{i_1i_2i_3}} a_{i_1i_2i_3} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_3} = \sum_{i_3=0}^{L} \sum_{i_2=0}^{L_{i_3}} \sum_{i_1=0}^{K_{i_1i_2i_3}} a_{i_1i_2i_3} x_1^{i_1}, \quad (K_{i_1i_2i_3} \leq q-1)\]

(19)

(20)

We consider the code whose codeword consists of \(q^n\) elements \(\{f(\beta_{k_1}, \beta_{k_2}, \cdots, \beta_{k_n})\} (k_l = 0, 1, \cdots, q-1)\), where \(\beta_{k_j} (j = 1, 2, \cdots, n)\) are any elements of \(GF(q)\). The transformation of the information symbols \(\{a_{i_1i_2i_3}\}\) to a codeword \(\{f(\beta_{k_1}, \beta_{k_2}, \cdots, \beta_{k_n})\}\) is the \(n\)-dimensional Fourier transform over \(GF(q)\), and so the code is the \(n\)-dimensional extension of a nonsystematic Reed-Solomon code. The code length \(N\) is \(N = q^n\).

From the discussion in the preceding chapter, the number of \(n\)-tuples \((\beta_{k_1}, \beta_{k_2}, \cdots, \beta_{k_n})\) such that \(f(\beta_{k_1}, \beta_{k_2}, \cdots, \beta_{k_n}) \neq 0\) is at least

\[
\min_{0 \geq m_j \leq L} \prod_{0 \leq m_j \leq L} \left( q - K_{m_2m_1} - m_j(q-m_3) \cdots (q-m_n) \right)
\]

(21)

ant it is equal to the minimum distance \(d_{\text{min}}\) of the code.

From Eq.(21), \(K_{m_2m_1} - m_j = q - \left\lfloor \frac{d_{\text{min}}}{(q-m_2)(q-m_3)} \right\rfloor\) because \(q - K_{m_2m_1} - m_j = 0, \cdots, L_{m_jm_2m_1} - m_j; j = 2, 3, \cdots, n-1; m_0 = 0, 1, \cdots, L\) must be \(\left\lfloor \frac{d_{\text{min}}}{(q-m_2)(q-m_3)} \right\rfloor\). \(L_{m_2m_1} = L_{m_3m_2} = \cdots = L_{m_n} = L\) should be respectively determined as the maximum \(m_2, m_3, \cdots, m_n\) such that \(K_{m_2m_1} = q - \left\lfloor \frac{d_{\text{min}}}{(q-m_2)(q-m_3)} \right\rfloor \geq 0\).

The above statement is summarized in the following theorem:

[Theorem 3] Let \(a_{i_1i_2i_3} (0 \leq i_1 \leq K_{i_1j}; 0 \leq i_2 \leq L_{i_1i_2}; 0 \leq i_3 \leq L)\) be any elements of a finite field \(GF(q)\), where \(K_{i_1j} = q - \left\lfloor \frac{d_{\text{min}}}{(q-i_1j)(q-i_3)} \right\rfloor\) and \(L_{i_1i_2} = L_{i_1j}, L_{i_2j}, \cdots, L_i, \cdots, L\) are the maximum integers such that \(K_{i_1i_2i_3} = q - \left\lfloor \frac{d_{\text{min}}}{(q-i_1j)(q-i_3)} \right\rfloor \geq 0\).
For a polynomial of \( n \) variables such that

\[
f(x_1, x_2, \cdots, x_n) = \sum_{i_1=0}^{L} \sum_{i_2=0}^{L} \cdots \sum_{i_n=0}^{L} a_{i_1i_2\cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}
\]  

(22)

the code whose codeword consists of \( q^n \) elements \((f(\beta_{k_1}, \beta_{k_2}, \cdots, \beta_{k_l})) \) \( (k_l = 0, 1, \cdots, q - 1; l = 1, 2, \cdots, n) \) is a linear code with minimum distance \( d_{\text{min}} \), where \( \beta_{k_1}, \beta_{k_2}, \cdots, \beta_{k_n} \) are the elements of \( GF(q) \). \( \square \)

The number of the information symbols \( K \) is

\[
K = \sum_{i_k=0}^{L} \sum_{i_{k+1}=0}^{L} \cdots \sum_{i_{n}=0}^{L} (K_{i_1i_2\cdots i_n} + 1) = \sum_{i_k=0}^{L} \sum_{i_{k+1}=0}^{L} \cdots \sum_{i_{n}=0}^{L} \left(q + 1 - \left\lceil \frac{d_{\text{min}}}{\prod_{j=2}^{n} (q - i_j)} \right\rceil \right)
\]  

(23)

and the number of the check symbols \( N - K = q^n - K \) is

\[
N - K = \sum_{i_k=0}^{L} \sum_{i_{k+1}=0}^{L} \cdots \sum_{i_{n}=0}^{L} \left( \left\lceil \frac{d_{\text{min}}}{\prod_{j=2}^{n} (q - i_j)} \right\rceil - 1 \right) + q^n - q(L + 1) \prod_{j=2}^{n} (L_{j,i+1,i+1} - i_n + 1).
\]  

(24)

When \( L = q - 1 \) and \( L_{j,i+1,i+1,i_n} = q - 1 \) \( (j = 2, 3, \cdots, n - 1) \), that is, \( d_{\text{min}} \leq q \), the number of the check symbols \( N - K \) is

\[
N - K = \sum_{i_k=0}^{q-1} \sum_{i_{k+1}=0}^{q-1} \cdots \sum_{i_{n}=0}^{q-1} \left( \left\lceil \frac{d_{\text{min}}}{\prod_{j=2}^{n} (q - i_j)} \right\rceil - 1 \right)
\]  

\[
= \sum_{i_k=q-d_{\text{min}}+1}^{q-1} \sum_{i_{k+1}=q-d_{\text{min}}+1}^{q-1} \cdots \sum_{i_{n}=q-d_{\text{min}}+1}^{q-1} \left( \left\lceil \frac{d_{\text{min}}}{\prod_{j=2}^{n} (q - i_j)} \right\rceil - 1 \right)
\]  

\[
= \sum_{i_k=1}^{d_{\text{min}}-1} \sum_{i_{k+1}=1}^{d_{\text{min}}-1} \cdots \sum_{i_{n}=1}^{d_{\text{min}}-1} \left( \left\lceil \frac{d_{\text{min}}}{\prod_{j=2}^{n} (i_j)} \right\rceil - 1 \right).
\]  

(25)

The number of the check symbols \( N - K \) has no relation to the number \( q \) of the elements of a finite field \( GF(q) \) and is determined by only the minimum distance \( d_{\text{min}} \). Table 2 shows the number of the check symbols when \( d_{\text{min}} \leq q \).

| \( d_{\text{min}} \) | \( n = 2 \) | \( n = 3 \) | \( n = 4 \) | \( n = 5 \) |
|---|---|---|---|---|
| 2 | 1 | 1 | 1 | 1 |
| 3 | 3 | 4 | 5 | 6 |
| 4 | 5 | 7 | 9 | 11 |
| 5 | 8 | 13 | 19 | 26 |
| 6 | 10 | 16 | 23 | 31 |
| 7 | 14 | 25 | 39 | 56 |
| 8 | 16 | 28 | 43 | 61 |
| 9 | 20 | 38 | 63 | 96 |
| 10 | 23 | 44 | 73 | 111 |
| 11 | 27 | 53 | 89 | 136 |
| 12 | 29 | 56 | 93 | 141 |
| 13 | 35 | 74 | 133 | 216 |
| 14 | 37 | 77 | 137 | 221 |
| 15 | 41 | 86 | 153 | 246 |
| 16 | 45 | 95 | 169 | 271 |
5 Performance

5.1 Comparison between 2-dimensional Reed-Solomon codes and product codes

The product code of a \((n_1, k_1, d_1)\) linear code and a \((n_2, k_2, d_2)\) linear code is a \((N, K, d_{\text{min}}) = (n_1 n_2, k_1 k_2, d_1 d_2)\) linear code. When two linear codes are the same \((n, k, d)\) Reed-Solomon codes over \(GF(q)\), the number of the check symbols of the product code is

\[ N - K = (d - 1)(2n - d + 1) \]  

(26)

Then the relation between \(\frac{d_{\text{min}}}{N}\) and \(\frac{K}{N}\) is

\[ 1 - \frac{K}{N} = \left( \sqrt{\frac{d_{\text{min}}}{N} - \frac{1}{q}} \right) \left( 1 - \sqrt{\frac{d_{\text{min}}}{N}} + \frac{1}{q} \right) \]  

(27)

when \(n = q\).

Figure 3 shows the relations between \(\frac{d_{\text{min}}}{N}\) and \(\frac{K}{N}\) of the 2-dimensional Reed-Solomon codes and the product codes when \(q = 8\) and \(q = 16\). As shown in Fig 3, the performance of the 2-dimensional codes is higher than that of the product codes.

![Figure 3: Performances of 2-dimensional codes and product codes](image)

5.2 Relation between dimension and performance

Figure 4 shows the relation between \(\frac{d_{\text{min}}}{N}\) and \(\frac{K}{N}\) when \(q = 4\). The code length increases exponentially when the dimension increases, but \(K/N\) much decreases.

5.3 Performance of shortened codes

Figure 5 shows the relation between \(\frac{d_{\text{min}}}{N}\) and \(\frac{K}{N}\) of the shortened 2-dimensional codes when \(q = 16\). Gilbert-Varshamov bounds are also shown in Fig 5. When \(\frac{d_{\text{min}}}{N}\) is small, the shortened codes have higher performance. Especially the shortened code of length \(N = 32\) is beyond the Gilbert-Varshamov bound when \(\frac{d_{\text{min}}}{N} \leq 0.15\).

6 Conclusion

This paper has proposed a new class of multi-dimensional nonsystematic Reed-Solomon codes that are constructed based on the multi-dimensional Fourier transform over a finite field. The proposed codes are the extension of the nonsystematic Reed-Solomon codes to multi-dimension. The code length of the Reed-Solomon codes can be lengthened by extending the dimension. Though the code length increases exponentially when the dimension increases, the code rate decreases. The nonsystematic Reed-Solomon codes are the maximum distance separable codes, but the proposed codes are not. However there exist some superior shortened 2-dimensional codes that are beyond the Gilbert-Varshamov bound when the minimum distance is small.
The codes presented by Shen, et al., which are constructed using a location set contained in a multidimensional affine or projective space over a finite field, seem to be equivalent to the proposed codes.

References

[1] F.J.MacWilliams and N.J.A.Sloane: "The theory of error-correcting codes," North Holland Publishing Company (1977).

[2] R.E.Blahut: "Theory and practice of error control codes," Addison-Wesley Publishing Company (1983).

[3] I.S.Reed and G.Solomon, "Polynomial codes over certain finite fields," J.SIAM, vol.8, pp.300-304 (1960).

[4] A.Shiozaki: "New class of codes based on two-dimensional Fourier transforms over finite fields," Electronics Letters, Vol.30, No.22, pp.1832-1833 (1994).

[5] A.Shiozaki: "A new class of error-correcting-codes based on multi-dimensional Fourier transform over finite field," Proc. of the 17th Symposium on Information Theory and Its Applications (SITA '94), pp.225-228 (Hi-roshima, Japan, Dec.6-9, 1994). (in Japanese)

[6] B.Z.Shen and K.K.Tzeng: "Multidimensional extension of Reed-Solomon codes," Proc. of 1998 IEEE International Symposium on Information Theory, p.54 (Cambridge, MA, USA, Aug.16-21, 1998).