View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by NASA Technical Reports Server

NASA-CR-201851

New Double-Byte Error-Correcting Codes for Memory Systems

Gui-Liang Feng, Xinwen Wu, T. R. N. Rao*

July 16, 1996

Abstract

Error-correcting or error-detecting codes have been used in the computer industry to increase reliability, reduce service costs, and maintain data integrity. The single-byte error-correcting and double-byte error-detecting (SbEC-DbED) codes have been successfully used in computer memory subsystems. There are many methods to construct double-byte error-correcting (DbEC) codes. In the present paper we construct a class of double-byte error-correcting codes, which are more efficient than those known to be optimum, and a decoding procedure for our codes is also considered.

Index Terms: Double-byte error-correcting codes, minimum distance, generalized Bezout's theorem, Decoding.

1 Introduction

Error-correcting or error-detecting codes are useful in computer semiconductor memory subsystems, which can be used to increase reliability, reduce service costs, and maintain data integrity. It is well known that the single-byte error-correcting and double-byte error-detecting (SbEC-DbED) codes have been successfully used in computer memory subsystems [1-4]. For a linear block code over the finite field $GF(q)$ of q elements, where q is a prime power, if its minimum distance is equal to or greater than d, then the code is capable of correcting $\lfloor \frac{d-1}{2} \rfloor$ byte errors and detecting $\lfloor \frac{d}{2} \rfloor$ byte errors. Thus the minimum distances of linear codes which are capable of correcting single byte errors and detecting double byte errors are equal to or greater than four, and the minimum distances of the codes which can correct double byte errors are equal to or greater than five. There are many methods to construct double-byte error- correcting (DbEC) codes. A class of codes with minimum distance ≥ 5 was constructed by adding appropriate parity checks to some cyclic codes [5].

Let C be a linear code over $GF(q)$, denote by n, r, and d the code length, number of parity checks, and minimum distance respectively. A code over $GF(q)$, where $q = 2^i$,

*Gui-Liang Feng, Xinwen Wu, T. R. N. Rao are with the Center for Advanced Computer Studies, University of Southwestern Louisiana, Lafayette, LA. 70504, USA. email: glf@cacs.usl.edu, xw@cacs.usl.edu and rao@cacs.usl.edu. This work was supported in part by the National Science Foundation under Grant NCR-9505619, Louisiana Education Quality Support Fund under Grant LEQSF-(1994-96)-RD-A-36, and NASA Project NAG-W-4013.

with minimum distance ≥ 5 was constructed with parameters $n = q^2$, and $r = 7$ [6]. Let $U_q^m(I)$ be a cyclic code over $F = GF(q)$, where $q = 2^i$, with a string $I = \{1, \frac{(q^m+q)}{2}\}$, and $U = U_q^m(I, F^{m-1})$ be the corresponding punctured code with length $n = q^{m-1}$ defined on a $(m-1)$-dimensional subspace F^{m-1} of F^m. A class of codes over $GF(2^i)$ with minimum distance ≥ 5 was constructed by adding some parity checks to U, these codes have the parameters $n = q^{m-1}$, $r \leq 2m + \lceil \frac{m-1}{3} \rceil$, $m = 2, 3, \cdots$. And when q is odd, a class of codes with minimum distance ≥ 5 was also constructed by a similar method. The above codes were constructed by Dumer in the Theorems 6 and 7 [5] respectively. According to Dumer, if q is even, when $n = q^2$, $r \leq 7$, when $n = q^3$, then $r \leq 9$; and if q is odd, when $n = q^2$, $r \leq 7$, when $n = q^3$, then $r \leq 8 \cdots$. Dumer's codes are known to be optimal in the sense that no other double-byte error-correcting codes with the same code lengths have fewer number of parity checks. But unfortunately, the codes in Theorem 7 were defined only over $GF(q)$, when q is odd. Dumer's method is very ingenious but is hard to read.

It is known that in the computer systems the codes over $GF(q)$ with $q = 2^i$ are useful. In the present paper, we will construct a class of double-byte error- correcting codes over $GF(2^i)$, which have the same parameters of Dumer's codes over $GF(q)$ with q is odd. And we also study the decoding procedure of our codes.

The organization of this paper is as follows. In section II, we review the generalized Bezout's theorem, which will be used to estimate the parameters of our codes. In section III, we construct our new double error correcting codes. In section IV, a decoding procedure is given. In section V, we give another construction of codes with minimum distances $d \geq 5$. Finally, we make some concluding remarks in section VI.

2 Generalized Bezout's Theorem

Let $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_p$, and $\mathbf{u}$ be n-tuple vectors. If there are p coefficients c_i such that $\mathbf{u} + \sum_{i=1}^{p} c_i \mathbf{v}_i = \mathbf{0}$, where $\mathbf{0}$ is the zero vector, then we say that $\mathbf{u}$ is totally linearly dependent on vectors $\mathbf{v}_1$, $\mathbf{v}_2$, ..., $\mathbf{v}_p$. Sometimes, $\mathbf{u}$ may be linearly dependent on the vectors for only some of the components (i.e., locations). Then $\mathbf{u}$ is said to be partially linearly dependent on the vectors $\mathbf{v}_i$ for $1 \leq i \leq p$. The maximal possible number of those components (i.e., locations) can be used to measure the linear dependence of the vector $\mathbf{u}$ on the vectors $\mathbf{v}_i$, for $1 \leq i \leq p$. The number of components, for which $\mathbf{u}$ is partially linearly dependent on the vectors, is called the *dependent-degree* of $\mathbf{u}$ on $\mathbf{v}_i$, for $1 \leq i \leq p$. Apparently, if the dependent-degree is equal to n, then $\mathbf{u}$ is totally linearly dependent on $\mathbf{v}_i$ for $1 \leq i \leq p$.

We generalize this concept to the case of a sequence of vectors $\mathbf{u}_i$. Let us consider two sequences of vectors $\mathbf{u}_i$ for $1 \leq i \leq p$, and vectors $\mathbf{v}_j$ for $1 \leq j \leq q$. Let there be some components, on which $\mathbf{u}_\mu$ $(1 \leq \mu \leq p)$ are partially linearly dependent on $\mathbf{v}_j$ for $1 \leq j \leq q$ and $\mathbf{u}_i$ for $1 \leq i < \mu$. The number of such components can be used to measure the consistent linear dependence of the vector $\mathbf{u}_1, ..., \mathbf{u}_p$ on vectors $\mathbf{v}_j$ for $1 \leq j \leq q$. The maximal possible number of such components is called the *consistent dependent-degree* of $\mathbf{u}_1$, ..., $\mathbf{u}_p$ on the vectors $\mathbf{v}_j$ for $1 \leq j \leq q$.

For a sequence of linearly independent vectors $\{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_r, ...\}$, let $\mathbf{v}_i^*$ express a linear combination $\mathbf{v}_i + \sum_{\mu=1}^{i-1} c_\mu \mathbf{v}_\mu$.

Definition 2.1 *$D_{\{\mathbf{v}^*_{i_1},\cdots,\mathbf{v}^*_{i_p}\}}$ denotes the maximal consistent dependent-degree of a set of $\{\mathbf{v}_{i_1},\cdots,\mathbf{v}_{i_p}\}$ on their previous vectors, respectively, i.e., $D_{\{\mathbf{v}^*_{i_1},\cdots,\mathbf{v}^*_{i_p}\}}$ denotes the maximal number of components (i.e., locations), on which $\mathbf{v}^*_{i_\mu}$ for $1 \le \mu \le p$ are all zero simultaneously.*

Definition 2.2 $D_p^{(r)} = \max\{D_{\{\mathbf{v}^*_{i_1},\cdots,\mathbf{v}^*_{i_p}\}} | i_1 < \cdots < i_p \le r\}$.

Let C_r be an $[n, n-r]$ linear code defined by a parity check matrix $\mathbf{H}_r = [\mathbf{h}_1, ..., \mathbf{h}_r]^T$, i.e. the parity check matrix has r rows. We have the following theorem:

Theorem 2.1 *([6]): Consider a linear code C_r defined by $\mathbf{H}_r$, i.e., the parity check matrix has r rows. If the consistent dependent-degree of any $(r - d^* + 2)$ rows of $\mathbf{H}_r$ is always less than $(d^* - 1)$, i.e., $D^{(r)}_{r-d^*+2} < d^* - 1$, then the minimum distance d of C_r is at least d^*, i.e., $d \ge d^*$.*

Let LS be a set of distinct points in a plane or a set of distinct roots of a plane curve (i.e. a polynomial). Let $LS = \{(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)\}$ and let $h(x, y)$ be a polynomial (or monomial), then a vector $(h(x_1, y_1), h(x_2, y_2), ..., h(x_n, y_n))$ is called an evaluated vector of polynomial $h(x, y)$ on the set LS. Hereinafter, sometimes $\mathbf{v}_i$ expresses an evaluated vector and sometimes it expresses a polynomial or a curve if no confusion arises. Thus, from Definition 1.1, $D_{\{\mathbf{v}^*_{i_1},\cdots,\mathbf{v}^*_{i_p}\}}$ denotes the number of distinct points of the intersection of curves $\mathbf{v}^*_{i_1} = 0$, ..., $\mathbf{v}^*_{i_p} = 0$ for the case of LS being the set of all points in a whole plane, or denotes the number of distinct points of the intersection of curves $\mathbf{v}^*_{i_1} = 0$, ..., $\mathbf{v}^*_{i_p} = 0$, and $f(x, y) = 0$ for the case of LS being the set of all points on the curve $f(x, y) = 0$. Similarly, $D_p^{(r)}$ for a given sequence of evaluated vectors expresses the maximal possible number of distinct points of the intersection of p curves among the first r curves of the given sequence of curves. Therefore, the calculation of $D_p^{(r)}$ reduces to the calculation of the number of distinct points of intersection of several curves.

Definition 2.3 *The x-resultant matrix, denoted by $RM(f, g)$ (or RM) of two polynomials*

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

$$g(x) = b_0 x^m + b_1 x^{m-1} + \cdots + b_m$$

is given by the following $(m + n) \times (m + n)$ matrix:

$$\begin{pmatrix}
a_0 & a_1 & \dots & \dots & \dots & a_n & & & & \\
 & a_0 & a_1 & \dots & \dots & \dots & a_n & & & \\
 & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \\
 & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\
 & & & & a_0 & a_1 & \dots & \dots & \dots & a_n \\
b_0 & b_1 & \dots & \dots & b_m & & & & & \\
 & b_0 & b_1 & \dots & \dots & b_m & & & & \\
 & & \cdot & \cdot & \cdot & \cdot & \cdot & & & \\
 & & & \cdot & \cdot & \cdot & \cdot & \cdot & & \\
 & & & & \cdot & \cdot & \cdot & \cdot & \cdot & \\
 & & & & & b_0 & b_1 & \dots & \dots & b_m
\end{pmatrix},$$

and its determinant is called the x-resultant of the two polynomials and denoted by $Res_x(f,g)$ (or R).

For convenience in the following discussion, we define

$$\vec{f}^{(0)} \equiv \vec{f} \equiv (a_0, a_1, ..., a_n, 0, ..., 0),$$

where on the rightmost side there are $(m-1)$ 0's, and

$$\vec{f}^{(i)} \equiv (0, ..., 0, a_0, a_1, ..., a_n, 0, ..., 0),$$

where on the leftmost side there are i 0's $(0 \leq i \leq m-1)$ and on the rightmost side there are $(m-i-1)$ 0's. Thus, the above matrix consists of the vectors $\vec{f}^{(\mu)}$ and $\vec{g}^{(\lambda)}$, for $0 \leq \mu \leq m-1$ and $0 \leq \lambda \leq n-1$.

The coefficients of f and g could be polynomials in y. We could have:

$$f(x,y) = a_0(y)x^m + a_1(y)x^{m-1} + \cdots + a_m(y),$$
$$g(x,y) = b_0(y)x^n + b_1(y)x^{n-1} + \cdots + b_n(y).$$

Theorem 2.2 *([6]): The number of distinct points of intersection of two polynomials $f(x,y)$ and $g(x,y)$ without common components is at most equal to the degree of their resultant $R(y)$.*

Let us consider p curves in affine plane curves without common components, i.e., $f_\mu(x,y) = 0$ for $\mu = 1, 2, ..., p$. Without loss of generality, $deg_x f_1 \geq deg_x f_2 \geq \cdots \geq deg_x f_p$, and let $deg_x f_1 = m$ and $deg_x f_2 = n$, where $deg_x f_\mu$ indicates the maximal i such that the monomial $x^i y^j$ is a term in f_μ. We define the x-resultant matrix of these p curves or polynomials as the following $\Sigma \times (m+n)$ matrix, where $\Sigma = \sum_{\mu=1}^{p} (m + n - deg_x f_\mu)$ and $s = deg_x f_p$:

$$\begin{pmatrix}
a_0^{(1)} & a_1^{(1)} & . & . & . & a_m^{(1)} & 0 & . & . & 0 \\
0 & a_0^{(1)} & a_1^{(1)} & . & . & . & a_m^{(1)} & 0 & . & 0 \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
0 & 0 & . & 0 & a_0^{(1)} & a_1^{(1)} & . & . & . & a_m^{(1)} \\
a_0^{(2)} & a_1^{(2)} & . & . & a_n^{(2)} & 0 & 0 & . & . & 0 \\
0 & a_0^{(2)} & a_1^{(2)} & . & . & a_n^{(2)} & 0 & . & . & 0 \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
0 & 0 & . & . & . & 0 & a_0^{(2)} & a_1^{(2)} & . & a_n^{(2)} \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
a_0^{(p)} & a_1^{(p)} & . & . & a_s^{(p)} & 0 & 0 & . & . & 0 \\
0 & a_0^{(p)} & a_1^{(p)} & . & . & a_s^{(p)} & 0 & . & . & 0 \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
0 & 0 & . & . & . & 0 & a_0^{(p)} & a_1^{(p)} & . & a_s^{(p)}
\end{pmatrix}.$$

Let $R(y) = Res_x(f_1, f_2, \cdots, f_p)$ be the non-zero determinant of the nonsingular submatrix with the smallest degree of y of the x-resultant matrix.

Theorem 2.3 *([6]): The number of distinct points of the intersection of $f_\mu(x, y)$ without common components, for $\mu = 1, 2, ..., p$, is at most equal to the degree of their resultant $R(y)$, i.e., $degR(y)$.*

In order to get an upper bound of $degR(y)$, we introduce a new concept. Among the f's with the same degree of x, we select one. Thus, we can select f_{λ_μ}, for $\mu = 1, 2, ..., q(\leq p)$, such that $deg_x f_{\lambda_\sigma} > deg_x f_{\lambda_{\sigma+1}}$, $\{ deg_x f_{\lambda_\sigma} | \sigma = 1, 2, ..., q\} = \{deg_x f_\mu | \mu = 1, 2, ..., p\}$, and f_{λ_σ} have no common components. We define the x-partial resultant matrix of these p curves or polynomials as the following $(m+n) \times (m+n)$ matrix:

$$[\bar{f}_{\lambda_1}^{(0)}, ..., \bar{f}_{\lambda_1}^{(d_1+d_2-d_1-1)}, \bar{f}_{\lambda_2}^{(d_1+d_2-d_1)}, ..., \bar{f}_{\lambda_2}^{(d_1+d_2-d_2-1)}, ..., \bar{f}_{\lambda_q}^{(d_1+d_2-d_{q-1})}, ..., \bar{f}_{\lambda_q}^{(d_1+d_2-d_q-1)}]^T,$$

namely, $[\bar{f}_{\lambda_1}^{(0)}, ..., \bar{f}_{\lambda_1}^{(d_2-1)}, \bar{f}_{\lambda_2}^{(d_2)}, ..., \bar{f}_{\lambda_2}^{(d_1-1)}, ..., \bar{f}_{\lambda_q}^{(d_1+d_2-d_{q-1})}, ..., \bar{f}_{\lambda_q}^{(d_1+d_2-d_q-1)}]^T$, where d_σ denotes $deg_x f_{\lambda_\sigma}$.

Obviously, this matrix is an upper triangle matrix when $d_q = 0$. The determinant of this matrix can be easily calculated for the special case, i.e., the determinant is equal to the product of all elements on main diagonal of this matrix. This determinant is called a partial resultant and denoted by $PR(y)$.

Corollary 2.1 *([6]): The number of distinct points of the intersection of $f_\mu(x, y)$, for $\mu = 1, 2, ..., p$, is at most equal to the degree of their partial resultant $PR(y)$.*

Example 2.1 *Let us consider the number of common points on the following four curves over $GF(2^4)$:*

$$\begin{cases} x^5 + y^4 + y = 0 \\ x^3 + a(y)x^2 + b(y)x + c(y) = 0 \\ xy + e(y) = 0 \\ y^2 + fy + g = 0 \end{cases},$$

We have the following matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & y^4+y & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & y^4+y & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & y^4+y \\ 0 & 0 & 0 & 1 & a(y) & b(y) & c(y) & 0 \\ 0 & 0 & 0 & 0 & 1 & a(y) & b(y) & c(y) \\ 0 & 0 & 0 & 0 & 0 & y & e(y) & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & y & e(y) \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & y^2+fy+g \end{pmatrix}.$$

Thus, $PR(y) = y^2(y^2 + fy + g)$. Obviously, $degPR(y) = 4$. Therefore, the number of distinct points of the intersection of the four curves is at most 4.

Remark 2.1: Here we regard $f_\mu(x, y)$ as a polynomial of x and the coefficients are polynomials in y. We also can regard $f_\mu(x, y)$ as a polynomial of y and the coefficients are

polynomials in x. The number of the distinct points of intersection of $f_\mu(x,y)$'s is the same. The distinct points of intersection of $f_\mu(x,y)$'s obtained by the two approaches are also the same.

Remark 2.2: It is sufficient and necessary that f_μ, for $\mu = 1, 2, ..., p$, have no common components.

Definition 2.4 *$D_{\{f_1,f_2,\cdots,f_p\}}$ denotes the number of distinct points of the intersection of curves $f_\mu(x,y) = 0$, for $\mu = 1, 2, ..., p$.*

Definition 2.5 *Given a sequence of polynomials $\{f_\mu(x,y) | \mu = 1, 2, ..., r\}$.*

$$D_p^{(r)} = \max\{D_{\{f^*_{\lambda_1}, f^*_{\lambda_2}, \cdots, f^*_{\lambda_p}\}} | \lambda_1, \cdots, \lambda_p \leq r\},$$

where $f^*_{\lambda_\mu}$ expresses a linear combination of f_i for i =1, 2, ..., λ_μ, and the coefficient of f_{λ_μ} is 1, i.e., $f^*_{\lambda_\mu} = f_{\lambda_\mu} + \sum_{i=1}^{\lambda_\mu - 1} c_i f_i$.

3 Constructions of Double-Byte Error-Correcting Codes

Let $A^m(F_q)$ be a m-dimensional affine space over $F_q = GF(q)$, and let LS be the set of all points in $A^m(F_q)$. obviously, the number of points in LS, $n = |LS| = q^m$. We call the set LS, *a location set*, the points in LS will be the locations in our construction. For a given location set $LS = \{P_1, P_2, \cdots, P_n\}$, each monomial or polynomial h with m variables and coefficients in $GF(q)$ is associated with an n-tuple vector $(h(P_1), h(P_2), \cdots, h(P_n))$, which is called an *evaluated vector of h* at LS. In the subsequent discussion, usage of the words monomial or polynomial refer to the corresponding evaluated vector. Let $\{h_1, h_2, \cdots, h_r\}$ be a set of r polynomials, we denote by H^T or $[h_1, h_2, \cdots, h_r]^T$ the evaluated matrix

$$\begin{pmatrix} h_1(P_1) & h_1(P_2) & \cdots & h_1(P_n) \\ h_2(P_1) & h_2(P_2) & \cdots & h_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ h_r(P_1) & h_r(P_2) & \cdots & h_r(P_n) \end{pmatrix}.$$

Construction 3.1: Let $n = q^2$, where q is a power of an odd prime. Consider $H = \{1, x + y\beta, (x + y\beta + 0\beta^2)^2, (x + y\beta + 0\beta^2)^{q^2+q+1}\}$ over $GF(q)$, where $\beta \in GF(q^3) - GF(q)$ and $1, \beta, \beta^2$ is a basis of the vector space of $GF(q^3)$ over $GF(q)$. Let $[1, x + y\beta, (x + y\beta + 0\beta^2)^2, (x + y\beta + 0\beta^2)^{q^2+q+1}]^T$ be a parity check matrix. Then we have a code over $GF(q)$.

Theorem 3.1 *The code in Construction 3.1 has the parameters*

$$n = q^2, \qquad r = 7, \qquad \text{and } d \geq 5.$$

Proof: $GF(q^3)$ is a 3-dimensional vector space over $GF(q)$, by the hypothesis, $1, \beta, \beta^2$ is a basis of $GF(q^3)$. $x + y\beta = x + y\beta + 0\beta^2 \in GF(q^3)$. $N_3(x) = x^{q^2+q+1}$ is the *norm* function, because $(x^{q^2+q+1})^q = x^{q^2+q+1}$, the norm function maps any nonzero $x \in GF(q^3)$ into nonzero $N_3(x) \in GF(q)$. Because $(x+y\beta)^2 = x^2 + 2xy\beta + y^2\beta^2$, we know that the code in the above construction has $r = 7$ parity checks: $1, x, y, x^2, 2xy, y^2, (x + y\beta)^{q^2+q+1}$. To

prove $d \geq 5$, by Theorem 2.1, we need only to prove that $D_4^{(7)} \leq 3$. Denote $D_{\{h_{\lambda_1}^*,h_{\lambda_2}^*,h_{\lambda_3}^*,h_{\lambda_4}^*\}}$ by $D_{\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}}$ or $D_{\{[h_{\lambda_1}],[h_{\lambda_2}],[h_{\lambda_3}],[h_{\lambda_4}]\}}$. Let $D_4^{(7)} = D_{\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}}$. Obviously, if $\lambda_1 = 1$, then $D_{\{1,\lambda_2,\lambda_3,\lambda_4\}} = 0$. If $\lambda_1 = 2$, it is easy to check that

$$\begin{aligned}
&D_{\{[x],[y],[*],[*]\}} \leq 1,\\
&D_{\{[x],[x^2],[2xy],[y^2]\}} \leq 2,\\
&D_{\{[x],[x^2],[2xy],[(x+y\beta)^{q^2+q+1}]\}} \leq 3,\\
&D_{\{[x],[x^2],[y^2],[(x+y\beta)^{q^2+q+1}]\}} \leq 2.
\end{aligned}$$

If $\lambda_1 = 3$, it can be easy to check that $D_{\{[y],[x^2],[*],[*]\}} \leq 2$. So we need only to prove that $D_{\{[y],[2xy],[y^2],[(x+y\beta)^{q^2+q+1}]\}} \leq 3$ and $D_{\{[x^2],[2xy],[y^2],[(x+y\beta)^{q^2+q+1}]\}} \leq 3$. Consider firstly the following system of equations

$$\begin{cases}
y + A_1x + b_1 = 0,\\
2xy + A_2x^2 + B_2x + C_2 = 0,\\
y^2 + A_3x^2 + B_3x + C_3 = 0,\\
(x + y\beta)^{q^2+q+1} + A_4x^2 + B_4x + C_4 = 0,
\end{cases}$$

where A_i, B_i, C_i are in $GF(q)$ (in the sequel, without special explanation, we denote elements in $GF(q)$ by A_i, B_i, C_i or A_i', B_i', C_i' in systems of equations). Substitution of the first equation into the last equation gives $((1 - A_1\beta)x - B_1\beta)^{q^2+q+1} + A_4x^2 + B_4x + C_4 = 0$. Because $\beta \in GF(q^3) - GF(q)$, $A_1 \in GF(q)$, we have $1 - A_1\beta \neq 0$. Thus this is a polynomial equation with coefficients in $GF(q)$ and degree 3, it has at most 3 distinct roots. Hence the number of distinct roots of the above system of equation is at most 3, i.e., $D_{\{[y],[2xy],[y^2],[(x+y\beta)^{q^2+q+1}]\}} \leq 3$. Now consider

$$\begin{cases}
x^2 + A_1x + B_1y + C_1 = 0,\\
2xy + A_2x + B_2y + C_2 = 0,\\
y^2 + A_3x + B_3y + C_3 = 0,\\
(x + y\beta)^{q^2+q+1} + A_4x + B_4y + C_4 = 0.
\end{cases}$$

To prove that this system of equations has at most 3 distinct roots. We need only to prove the following system of equations has at most 3 distinct roots,

$$\begin{cases}
x^2 + A_1x + B_1y + C_1 = 0,\\
2xy + A_2x + B_2y + C_2 = 0,\\
y^2 + A_3x + B_3y + C_3 = 0.
\end{cases} \tag{3.1}$$

Consider the x-resultant matrix of the above polynomial equations,

$$\begin{pmatrix}
1 & A_1 & B_1y + C_1\\
2y + A_2 & B_2y + C_2 & 0\\
0 & 2y + A_2 & B_2y + C_2\\
A_3 & y^2 + B_3y + C_3 & 0\\
0 & A_3 & y^2 + B_3y + C_3
\end{pmatrix}.$$

We have

$$R(y) = \begin{vmatrix} 1 & A_1 & B_1y + C_1 \\ 0 & 2y + A_2 & B_2y + C_2 \\ 0 & A_3 & y^2 + B_3y + C_3 \end{vmatrix},$$

so $R(y)$ is a polynomial of degree 3. So by the generalized Bezout's Theorem (Theorem 2.3), the system of equations (3.1) has at most 3 distinct roots. We have $D_{\{[x^2],[2xy],[y^2],[(x+y\beta)^{q^2+q+1}]\}} \leq 3$. Combining the above results, we complete the proof. □

Construction 3.2: Let $n = q^2$, where $q = 2^i$. Consider $H = \{1, x + y\beta, (x + y\beta + 0\beta^2)^{q+1}, (x + y\beta + 0\beta^2)^{q^2+q+1}\}$ over $GF(q)$, where $\beta \in GF(q^3) - GF(q)$ and $1, \beta, \beta^2$ is a basis of the vector space of $GF(q^3)$ over $GF(q)$. Let $[1, x + y\beta, (x + y\beta + 0\beta^2)^{q+1}, (x + y\beta + 0\beta^2)^{q^2+q+1}]^T$ be a parity check matrix. Then we have a code over $GF(q)$.

Theorem 3.2 *The code in Construction 3.2 has the parameters*

$$n = q^2, \qquad r = 7, \qquad \text{and } d \geq 5.$$

Proof: $(x + y\beta)^{q+1} = (x + y\beta)^q(x + y\beta) = (x + y\beta^q)(x + y\beta) = x^2 + xy\beta + xy\beta^q + y^2\beta^{q+1}$. Suppose $\beta^q = a_0 + a_1\beta + a_2\beta^2$, $\beta^{q+1} = b_0 + b_1\beta + b_2\beta^2$, then $(x+y\beta)^{q+1} = x^2 + a_0xy + b_0y^2 + ((1+a_1)xy + b_1y^2)\beta + (a_2xy + b_2y^2)\beta^2$. So the code in the above construction has $r = 7$ parity checks: 1, $x, y, x^2 + a_0xy + b_0y^2, (1 + a_1)xy + b_1y^2, a_2xy + b_2y^2$, and $(x + y\beta + 0\beta^2)^{q^2+q+1}$. Now as in the proof of Theorem 3.1, we need to prove $D_4^{(7)} \leq 3$. Let $D_4^{(7)} = D_{\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}}$. Obviously, if $\lambda_1 = 1$, then $D_{\{1,\lambda_2,\lambda_3,\lambda_4\}} = 0$. If $\lambda_1 = 2$, it is easy to check that

$$\begin{aligned} &D_{\{[x],[y],[*],[*]\}} \leq 1, \\ &D_{\{[x],[x^2+a_0xy+b_0y^2],[*],[*]\}} \leq 2, \\ &D_{\{[x],[(1+a_1)xy+b_1y^2],[*],[*]\}} \leq 3. \end{aligned}$$

If $\lambda_1 = 3$, we have $D_{\{[y],[*],[*],[(x+y\beta)^{q^2+q+1}]\}} \leq 3$. So we need only to prove that

$$D_{\{[y],[x^2+a_0xy+b_0y^2],[(1+a_0)xy+b_1y^2],[a_2xy+b_2y^2]\}} \leq 3$$

and

$$D_{\{[x^2+a_0xy+b_0y^2],[(1+a_0)xy+b_1y^2],[a_2xy+b_2y^2],[(x+y\beta)^{q^2+q+1}]\}} \leq 3,$$

i.e., we need to prove the following two systems of equations have at most 3 distinct roots respectively,

$$\begin{cases} y + Ax + B = 0, \\ x^2 + a_0xy + b_0y^2 + A_1x + B_1 = 0, \\ (1 + a_1)xy + b_1y^2 + A_2x + B_2 = 0, \\ a_2xy + b_2y^2 + A_3x + B_3 = 0, \end{cases}$$

and

$$\begin{cases} x^2 + a_0xy + b_0y^2 + A_1x + B_1y + C_1 = 0, \\ (1 + a_1)xy + b_1y^2 + A_2x + B_2y + C_2 = 0, \\ a_2xy + b_2y^2 + A_3x + B_3y + C_3 = 0, \\ (x + y\beta)^{q^2+q+1} + A_4x + B_4y + C_4 = 0. \end{cases}$$

Now we prove that the system of the last three equations in the first system of equations and the system of the first three equations in the second system of equations are all equivalent to the following system of equations:

$$\begin{cases} x^2 + A_1'x + B_1'y + C_1' = 0, \\ xy + A_2'x + B_2'y + C_2' = 0, \\ y^2 + A_3'x + B_3'y + C_3' = 0. \end{cases} \tag{3.2}$$

We need only to prove the determinant of the matrix of the coefficients of x^2, xy, and y^2 is not zero, i.e.,

$$\begin{vmatrix} 1 & a_0 & b_0 \\ 0 & 1+a_1 & b_1 \\ 0 & a_2 & b_2 \end{vmatrix} = \begin{vmatrix} 1+a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \neq 0.$$

If it is not, we have a nonzero element $a \in GF(q)$, such that $(b_1, b_2) = a(1 + a_1, a_2)$. On the other hand, we have $\beta^q = a_0 + a_1\beta + a_2\beta^2$, $\beta^{q+1} = b_0 + b_1\beta + b_2\beta^2$. So, $\beta^{q+1} + a(\beta^q + \beta) = b_0 + aa_0 = b \in GF(q)$, from this equation, we have $(\beta^{q+1} + a(\beta^q + \beta))^q = b^q = b$, i.e., $\beta^{q^2+q} + a(\beta^{q^2} + \beta^q) = b$. Add this equation into the above equation, we obtain $\beta^{q^2+q} + \beta^{q+1} = a(\beta^{q^2} + \beta)$, it shows $\beta^q = a \in GF(q)$. So $\beta^{q^2} = (\beta^q)^q = \beta^q$, and $\beta^{q^3} = (\beta^{q^2})^q = (\beta^q)^q = \beta^q$. On the other hand $\beta \in GF(q^3)$, we have $\beta^{q^3} = \beta$, so we have $\beta^q = \beta$, and hence $\beta \in GF(q)$. It contradicts the hypothesis.

Now consider the system of equations (3.2), as (3.1) in the proof of Theorem 3.1, it has at most 3 distinct roots. Combining the above results, we complete the proof. □

Example 3.1: Let $q = 2^2 = 4$, and let β be a primitive element of $GF(q^3)$. Then $GF(q^3) = GF(2^6) = \{0, 1, \beta, \beta^2, \cdots, \beta^{61}, \beta^{62}\}$. Suppose $\alpha = \beta^{21}$, then $GF(q) = GF(4) = \{0, 1, \alpha, \alpha^2\}$. We know that $[GF(q^3) : GF(q)] = 3$, $GF(q^3)$ is a 3-dimensional vector space over $GF(q)$. We can prove that for any $a_0, a_1, a_2 \in GF(q) = \{0, 1, \alpha, \alpha^2\}$, $a_0 + a_1\beta + a_2\beta^2 = 0$ if and only if $a_0 = a_1 = a_2 = 0$, i.e., $1, \beta, \beta^2$ are linearly independent over $GF(q)$. So $1, \beta, \beta^2$ is a basis of $GF(q^3)$ over $GF(q)$. Now consider the code in Construction 3.2. $(x + y\beta)^{q+1} = x^2 + xy\beta + xy\beta^4 + y^2\beta^5$, but $\beta^4 = \alpha + \beta + \alpha\beta^2$, $\beta^5 = \alpha^2 + \alpha^2\beta + \alpha^2\beta^2$. So $(x + y\beta)^{q+1} = (x^2 + \alpha xy + \alpha^2y^2) + (\alpha^2y^2)\beta + (\alpha xy + \alpha^2y^2)\beta^2$. And $(x + y\beta)^{q^2+q+1} = x^3 + (\beta^{16} + \beta^4 + \beta)x^2y + (\beta^{20} + \beta^{17} + \beta^5)xy^2 + \beta^{21}y^3 = x^3 + x^2y + \alpha^2xy^2 + \alpha y^3$. Let $H^T = [1, x, y, x^2 + \alpha xy + \alpha^2y^2, \alpha^2y^2, \alpha xy + \alpha^2y^2, x^3 + x^2y + \alpha^2xy^2 + \alpha y^3]^T$ be a parity check matrix. Then we have a code over $GF(4)$ with $n = 16, r = 7$, and $d \geq 5$.

Let $f_1 = 1, f_2 = x, f_3 = y, f_4 = x^2 + \alpha xy + \alpha^2y^2, f_5 = \alpha^2y^2, f_6 = \alpha xy + \alpha^2y^2, f_7 = x^3 + x^2y + \alpha^2xy^2 + \alpha y^3$. And Let $P_1 = (0, 0)$, $P_2 = (0, 1)$, $P_3 = (0, \alpha)$, $P_4 = (0, \alpha^2)$, $P_5 = (1, 0)$, $P_6 = (1, 1)$, $P_7 = (1, \alpha)$, $P_8 = (1, \alpha^2)$, $P_9 = (\alpha, 0)$, $P_{10} = (\alpha, 1)$, $P_{11} = (\alpha, \alpha)$, $P_{12} = (\alpha, \alpha^2)$, $P_{13} = (\alpha^2, 0)$, $P_{14} = (\alpha^2, 1)$, $P_{15} = (\alpha^2, \alpha)$, $P_{16} = (\alpha^2, \alpha^2)$. Then we have the following evaluated table

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}
f_1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
f_2	0	0	0	0	1	1	1	1	α	α	α	α	α^2	α^2	α^2	α^2
f_3	0	1	α	α^2	0	1	α	α^2	0	1	α	α^2	0	1	α	α^2
f_4	0	α^2	1	α	1	0	0	1	α^2	α^2	0	0	α	0	α	0
f_5	0	α^2	1	α	0	α^2	α	1	0	α^2	α	1	0	α^2	α	1
f_6	0	α^2	1	α	0	1	1	0	0	0	α^2	α^2	0	α	0	α^2
f_7	0	α	α^2	1	1	1	α^2	1	1	1	1	α^2	1	α^2	1	1

So the parity check matrix is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha & \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha & \alpha^2 & 0 & 1 & \alpha & \alpha^2 & 0 & 1 & \alpha & \alpha^2 & 0 & 1 & \alpha & \alpha^2 \\ 0 & \alpha^2 & 1 & \alpha & 1 & 0 & 0 & 1 & \alpha^2 & \alpha^2 & 0 & 0 & \alpha & 0 & \alpha & 0 \\ 0 & \alpha^2 & 1 & \alpha & 0 & \alpha^2 & \alpha & 1 & 0 & \alpha^2 & \alpha & 1 & 0 & \alpha^2 & \alpha & 1 \\ 0 & \alpha^2 & 1 & \alpha & 0 & 1 & 1 & 0 & 0 & 0 & \alpha^2 & \alpha^2 & 0 & \alpha & 0 & \alpha^2 \\ 0 & \alpha & \alpha^2 & 1 & 1 & 1 & \alpha^2 & 1 & 1 & 1 & 1 & \alpha^2 & 1 & \alpha^2 & 1 & 1 \end{pmatrix}.$$

We can generalize Constructions 3.1 and 3.2 to higher dimensional cases as follows:

Construction 3.3: Let $n = q^{3k+2}$, $k = 1, 2, \cdots$, where q is a power of an odd prime. Let $[1, x_1+x_2\gamma+\cdots+x_{3k+2}\gamma^{3k+1}, (x_1+x_2\gamma+\cdots+x_{3k+2}\gamma^{3k+1})^2, (x_1+x_2\beta+x_3\beta^2)^{q^2+q+1}, \cdots, (x_{3k+1}+x_{3k+2}\beta+0\beta^2)^{q^2+q+1}]^T$ be a parity check matrix, where $\gamma \in GF(q^{3k+2}) - GF(q)$, $\beta \in GF(q^3) - GF(q)$, and $1, \gamma, \cdots, \gamma^{3k+1}$ is a basis of the vector space $GF(q^{3k+2})$ over $GF(q)$, $1, \beta, \beta^2$ is a basis of the vector space $GF(q^3)$ over $GF(q)$ respectively. Then we have a sequence of codes over $GF(q)$.

Theorem 3.3 *The codes in Construction 3.3 have the parameters*

$$n = q^{3k+2}, \qquad r = 7k + 6, \qquad \text{and } d \geq 5.$$

Construction 3.4: Let $n = q^{3k+2}$, $k = 1, 2, \cdots$, where $q = 2^i$. Let $[1, x_1 + x_2\gamma + \cdots + x_{3k+2}\gamma^{3k+1}, (x_1+x_2\gamma+\cdots+x_{3k+2}\gamma^{3k+1})^{q+1}, (x_1+x_2\beta+x_3\beta^2)^{q^2+q+1}, \cdots, (x_{3k+1}+x_{3k+2}\beta+0\beta^2)^{q^2+q+1}]^T$ be a parity check matrix, where γ and β are as in Construction 3.3. Then we have a sequence of codes over $GF(q)$.

Theorem 3.4 *The codes in Construction 3.4 have the parameters*

$$n = q^{3k+2}, \qquad r = 7k + 6, \qquad \text{and } d \geq 5.$$

At the end of this section, we will give a proof of Theorem 3.4. The proof of Theorem 3.3 is similar to the proof of Theorem 3.4, we omit the details.

Construction 3.5: Let $n = q^3$, where q is a power of an odd prime, and let $\beta \in GF(q^3) - GF(q)$, and 1, β, β^2 is a basis of the vector space $GF(q^3)$ over $GF(q)$. Let $[1, x + y\beta + z\beta^2, (x + y\beta + z\beta^2)^2, (x + y\beta + z\beta^2)^{q^2+q+1}]^T$ be a parity check matrix. Then we have a code over $GF(q)$.

Theorem 3.5 *The code in Construction 3.5 has the parameters*

$$n = q^3, \qquad r = 8, \qquad \text{and } d \geq 5.$$

Proof: We have $(x + y\beta + z\beta^2)^2 = x^2 + 2xy\beta + (y^2 + 2xz)\beta^2 + 2yz\beta^3 + z^2\beta^4$. Let $\beta^3 = a_0 + a_1\beta + a_2\beta^2$, $\beta^4 = b_0 + b_1\beta + b_2\beta^2$, and substitute them into the above equation, $(x + y\beta + z\beta^2)^2 = x^2 + 2a_0yz + b_0z^2 + (2xy + 2a_1yz + b_1z^2)\beta + (y^2 + 2xz + 2a_2yz + b_2z^2)\beta^2$. Hence the code has $r = 8$ parity checks: $1, x, y, z, x^2 + 2a_0yz + b_0z^2, 2xy + 2a_1yz + b_1z^2, y^2 + 2xz + 2a_2yz + b_2z^2$, and $(x + y\beta + z\beta^2)^{q^2+q+1}$. To prove that $d \geq 5$, we need to prove $D_5^{(8)} \leq 3$. Let $D_5^{(8)} = D_{\{\lambda_1,\lambda_2,\lambda_3,\lambda_4,\lambda_5\}}$. Obviously, if $\lambda_1 = 1$, $D_{\{1,*,*,*,*\}} = 0$. If $\lambda_1 = 2$, it is easy to check that

$$D_{\{[x],[y],[*],[*],[*]\}} \leq 3,$$
$$D_{\{[x],[z],[*],[*],[*]\}} \leq 3.$$

And if $\lambda_1 = 3$, we have $D_{\{[y],[z],[*],[*],[*]\}} \leq 3$. So we need only to prove that

$$D_{\{[z],[x^2+2a_0yz+b_0z^2],[2xy+2a_1yz+b_1z^2],[y^2+2xz+2a_0yz+b_2z^2],[(x+y\beta+z\beta^2)^{q^2+q+1}]\}} \leq 3,$$

i.e., we need to prove the following system of equations has at most 3 distinct roots:

$$\begin{cases} z + A_1x + B_1y + C_1 = 0, \\ x^2 + 2a_0yz + b_0z^2 + A_2x + B_2y + C_2 = 0, \\ 2xy + 2a_1yz + b_1z^2 + A_3x + B_3y + C_3 = 0, \\ y^2 + 2xz + 2a_0yz + b_2z^2 + A_4x + B_4y + C_4 = 0, \\ (x + y\beta + z\beta^2)^{q^2+q+1} + A_5x + B_5y + C_5 = 0. \end{cases}$$

When we substitute the first equations into the second, third and fourth equations, we obtain three equations on x and y of degree 2. If we can prove the system of these three equations is equivalent to the system of equations (3.2), then the proof is completed. Now we prove it as follows.

Substituting $z = -A_1x - B_1y - C_1$ into $(x + y\beta + z\beta^2)^2$, $(x + y\beta - (A_1x + B_1y + C_1)\beta^2)^2$, the part of degree 2 of it is $((1 - A_1\beta^2)x + (1 - B_1\beta)\beta y)^2 = (1 - A_1\beta^2)^2(x + \frac{\beta - B_1\beta^2}{1 - A_1\beta^2}y)^2$, because $1 - A_1\beta^2 \neq 0$, we can divide it by $(1 - A_1\beta^2)^2$. Let $c = \frac{\beta - B_1\beta^2}{1 - A_1\beta^2} \in GF(q^3)$, then $(x + cy)^2 = x^2 + 2cxy + c^2y^2$. Suppose that $2c = c_0 + c_1\beta + c_2\beta^2$, and $c^2 = d_0 + d_1\beta + d_2\beta^2$, then $(x + cy)^2 = (x^2 + c_0xy + d_0y^2) + (c_1xy + d_1y^2)\beta + (c_2xy + d_2y^2)\beta^2$. So the system of the three equations we considered is equivalent to the following system of equations

$$\begin{cases} x^2 + c_0xy + d_0y^2 + A_1'x + B_1'y + C_1' = 0, \\ c_1xy + d_1y^2 + A_2'x + B_2'y + C_2' = 0, \\ c_2xy + d_2y^2 + A_3'x + B_3'y + C_3' = 0. \end{cases}$$

This system of equations is equivalent to (3.2) if and only if the determinant of the matrix of the coefficients of x^2, xy and y^2 is not equal to zero, i.e.,

$$\begin{vmatrix} 1 & c_0 & d_0 \\ 0 & c_1 & d_1 \\ 0 & c_2 & d_2 \end{vmatrix} = \begin{vmatrix} c_1 & d_1 \\ c_2 & d_2 \end{vmatrix} \neq 0.$$

In fact, if it is zero, then there exist a nonzero element $a \in GF(q)$, such that $(d_1, d_2) = a(c_1, c_2)$. On the other hand, $2c = c_0 + c_1\beta + c_2\beta^2$, $c^2 = d_0 + d_1\beta + d_2\beta^2$, so $c^2 - 2ac = d_0 - ac_0 = b \in GF(q)$, i.e., c is a root of the equation $x^2 - 2ax - b = 0$, whose coefficients are in $GF(q)$, so $c \in GF(q^2)$. But $c \in GF(q^3)$ and $GF(q^3) \cap GF(q^2) = GF(q)$, thus $c \in GF(q)$, so $(B_1 - A_1c)\beta^2 - \beta + c = 0$. But we know that $1, \beta, \beta^2$ are linearly independent over $GF(q)$. This is a contradiction. So the proof is completed. □

Construction 3.6: Let $n = q^3$, where $q = 2^i$. Let $[1, x + y\beta + z\beta^2, (x + y\beta + z\beta^2)^{q+1}, (x + y\beta + z\beta^2)^{q^2+q+1}]^T$ be a parity check matrix, where β is as in Construction 3.5. Then we have a code over $GF(q)$.

Theorem 3.6 *The code in Construction 3.6 has the parameters*

$$n = q^3, \qquad r = 8, \qquad \text{and } d \geq 5.$$

Proof: $(x + y\beta + z\beta^2)^{q+1} = x^2 + xy\beta + xz\beta^2 + xy\beta^q + y^2\beta^{q+1} + yz\beta^{q+2} + xz\beta^{2q} + yz\beta^{2q+1} + z^2\beta^{2q+2}$. Suppose that

$$\begin{aligned}
\beta^q &= a_0 + a_1\beta + a_2\beta^2, \\
\beta^{q+1} &= b_0 + b_1\beta + b_2\beta^2, \\
\beta^{q+2} &= c_0 + c_1\beta + c_2\beta^2, \\
\beta^{2q} &= d_0 + d_1\beta + d_2\beta^2, \\
\beta^{2q+1} &= e_0 + e_1\beta + e_2\beta^2, \\
\beta^{2q+2} &= f_0 + f_1\beta + f_2\beta^2.
\end{aligned}$$

Substitute these six equations into the above equation, we have $(x + y\beta + z\beta^2)^{q+1} = g_0(x, y, z) + g_1(x, y, z)\beta + g_2(x, y, z)\beta^2$, where

$$\begin{aligned}
g_0(x, y, z) &= x^2 + a_0xy + b_0y^2 + (c_0 + e_0)yz + d_0xz + f_0z^2, \\
g_1(x, y, z) &= (1 + a_1)xy + b_1y^2 + (c_1 + e_1)yz + d_1xz + f_1z^2, \\
g_2(x, y, z) &= a_2xy + b_2y^2 + (c_2 + e_2)yz + (1 + d_2)xz + f_2z^2.
\end{aligned}$$

Thus the code has $r = 8$ parity checks: $1, x, y, z, g_0(x, y, z), g_1(x, y, z), g_2(x, y, z), (x + y\beta + z\beta^2)^{q^2+q+1}$. As in the proof of Theorem 3.5, we need only to prove the following system of equations has at most 3 distinct roots.

$$\begin{cases}
z + A_1x + B_1y + C_1 = 0, \\
g_0(x, y, z) + A_2x + B_2y + C_2 = 0, \\
g_1(x, y, z) + A_3x + B_3y + C_3 = 0, \\
g_2(x, y, z) + A_4x + B_4y + C_4 = 0, \\
(x + y\beta + z\beta^2)^{q^2+q+1} + A_5x + B_5y + C_5 = 0.
\end{cases}$$

We employ the idea in the proof of Theorem 3.5. Substitute $z = A_1x + B_1y + C_1$ into $(x + y\beta + z\beta^2)^{q^2+q+1}$, and consider its part of degree 2, which is $((1 + A_1\beta^2)x + (\beta + B_1\beta^2)y)^{q+1} = (1 + A_1\beta^2)^{q+1}(x + y\frac{\beta + B_1\beta^2}{1 + A_1\beta^2})^{q+1}$, divide it by $(1 + A_1\beta^2)^{q+1}$ and let $c = \frac{\beta + B_1\beta^2}{1 + A_1\beta^2} \in GF(q^3)$. Then $(x + cy)^{q+1} = x^2 + (c^q + c)xy + c^{q+1}$. Suppose that $c^q + c = g_0 + g_1\beta + g_2\beta^2$, $c^{q+1} = h_0 + h_1\beta + h_2\beta^2$, then $(x + y\beta)^{q+1} = (x + g_0xy + h_0y^2) + (g_1xy + h_1y^2)\beta + (g_2xy + h_2y^2)\beta^2$.

Similar to the proof of Theorem 3.5, we have to prove the following determinant is not zero,

$$\begin{vmatrix} 1 & g_0 & h_0 \\ 0 & g_1 & h_1 \\ 0 & g_2 & h_2 \end{vmatrix} = \begin{vmatrix} g_1 & h_1 \\ g_2 & h_2 \end{vmatrix}.$$

If it is zero, then there exist a nonzero element $a \in GF(q)$ such that $(h_1, h_2) = a(g_1, g_2)$. So we have $c^{q+1} + ac^q + ac = h_0 + ag_0 = b \in GF(q)$, and $(c^{q+1} + ac^q + ac)^q = b^q = b$, i.e., $c^{q^2+q} + ac^{q^2} + ac^q = b$. Add the above two formulas, we obtain $c^{q^2+q} + c^{q+1} + ac^{q^2} = ac$, so

$$a = \frac{c^{q^2+q} + c^{q+1}}{c^{q^2} + c} = c^q.$$

As in the proof of Theorem 3.2. It shows $c \in GF(q)$, but $c = \frac{\beta + B_1\beta^2}{1 + A_1\beta^2}$. As in the proof of Theorem 3.5 it is a contradiction. So the proof is completed. □

Example 3.2: As in Example 3.1, let $q = 2^2 = 4$, and let β be a primitive element of $GF(q^3)$. Then $GF(q^3) = GF(2^6) = \{0, 1, \beta, \beta^2, \cdots, \beta^{61}, \beta^{62}\}$. Suppose $\alpha = \beta^{21}$, then $GF(q) = GF(4) = \{0, 1, \alpha, \alpha^2\}$. We know that $[GF(q^3) : GF(q)] = 3$, $GF(q^3)$ is a 3-dimensional vector space over $GF(q)$. We can prove that for any $a_0, a_1, a_2 \in GF(q) = \{0, 1, \alpha, \alpha^2\}$, $a_0 + a_1\beta + a_2\beta^2 = 0$ if and only if $a_0 = a_1 = a_2 = 0$, i.e., $1, \beta, \beta^2$ are linearly independent over $GF(q)$. So $1, \beta, \beta^2$ is a basis of $GF(q^3)$ over $GF(q)$. Now consider the code in Construction 3.6. $(x + y\beta + z\beta^2)^{q+1} = (x^2 + \alpha xy + \alpha^2 y^2 + yz + \alpha xz + z^2) + (\alpha^2 y^2 + yz + \alpha^2 xz + \alpha yz + \alpha z^2)\beta + (xz + \alpha xy + \alpha^2 y^2 + \alpha^2 yz + z^2)\beta^2$, $(x + y\beta + \beta^2)^{q^2+q+1} = x^3 + x^2y + x^2z + \alpha^2 xy^2 + xyz + \alpha xz^2 + \alpha y^3 + \alpha y^2 z + yz^2 + \alpha^2 z^3$. Let $H^T = [1, x, y, z, (x^2 + \alpha xy + \alpha^2 y^2 + yz + \alpha xz + z^2), (\alpha^2 y^2 + yz + \alpha^2 xz + \alpha yz + \alpha z^2), (xz + \alpha xy + \alpha^2 y^2 + \alpha^2 yz + z^2), x^3 + x^2y + x^2z + \alpha^2 xy^2 + xyz + \alpha xz^2 + \alpha y^3 + \alpha y^2 z + yz^2 + \alpha^2 z^3]^T$ be a parity check matrix. Then we have a code over $GF(4)$ with $n = 64, r = 8$, and $d \geq 5$.

Let $f_1 = 1, f_2 = x, f_3 = y, f_4 = z, f_5 = (x^2 + \alpha xy + \alpha^2 y^2 + yz + \alpha xz + z^2), f_6 = (\alpha^2 y^2 + yz + \alpha^2 xz + \alpha yz + \alpha z^2), f_7 = (xz + \alpha xy + \alpha^2 y^2 + \alpha^2 yz + z^2), f_8 = x^3 + x^2y + x^2z + \alpha^2 xy^2 + xyz + \alpha xz^2 + \alpha y^3 + \alpha y^2 z + yz^2 + \alpha^2 z^3$. And Let $P_1 = (0, 0, 0)$, $P_2 = (0, 0, 1)$, $P_3 = (0, 0, \alpha)$, $P_4 = (0, 0, \alpha^2)$, $P_5 = (1, 0, 0)$, $P_6 = (1, 0, 1)$, $P_7 = (1, 0, \alpha)$, $P_8 = (1, 0, \alpha^2)$, $\cdots$, $P_{59} = (\alpha^2, \alpha, \alpha)$, $P_{60} = (\alpha^2, \alpha, \alpha^2)$, $P_{61} = (\alpha^2, \alpha^2, 0)$, $P_{62} = (\alpha^2, \alpha^2, 1)$, $P_{63} = (\alpha^2, \alpha^2, \alpha)$, $P_{64} = (\alpha^2, \alpha^2, \alpha^2)$. Then we have the following evaluated table

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	$\cdots\cdots$	P_{59}	P_{60}	P_{61}	P_{62}	P_{63}	P_{64}
f_1	1	1	1	1	1	1	1	1	$\cdots\cdots$	1	1	1	1	1	1
f_2	0	0	0	0	1	1	1	1	$\cdots\cdots$	α^2	α^2	α^2	α^2	α^2	α^2
f_3	0	0	0	0	0	0	0	0	$\cdots\cdots$	α	α	α^2	α^2	α^2	α^2
f_4	0	1	α	α^2	0	1	α	α^2	$\cdots\cdots$	α	α^2	0	1	α	α^2
f_5	0	1	α^2	α	1	0	1	α	$\cdots\cdots$	0	α	0	α^2	0	α^2
f_6	0	α	1	α^2	0	α	0	1	$\cdots\cdots$	α	α^2	1	α^2	0	α
f_7	0	1	α^2	α	0	0	1	1	$\cdots\cdots$	0	α^2	α	α	α^2	α^2
f_8	0	α^2	α^2	α^2	1	1	1	α	$\cdots\cdots$	α^2	α	1	α^2	α	α^2

So the parity check matrix is

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha & \alpha & \cdots & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & \alpha & \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\
0 & 1 & \alpha & \alpha^2 & 0 & 1 & \alpha & \alpha^2 & 0 & 1 & \cdots & \alpha^2 & 0 & 1 & \alpha & \alpha^2 & 0 & 1 & \alpha & \alpha^2 \\
0 & 1 & \alpha^2 & \alpha & 1 & 0 & 1 & \alpha & \alpha^2 & 1 & \cdots & \alpha & \alpha & 0 & 0 & \alpha & 0 & \alpha^2 & 0 & \alpha^2 \\
0 & \alpha & 1 & \alpha^2 & 0 & \alpha & 0 & 1 & 0 & \alpha^2 & \cdots & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 & 1 & \alpha^2 & 0 & \alpha \\
0 & 1 & \alpha^2 & \alpha & 0 & 0 & 1 & 1 & 0 & \alpha^2 & \cdots & 0 & 0 & \alpha^2 & 0 & \alpha^2 & \alpha & \alpha & \alpha^2 & \alpha^2 \\
0 & \alpha^2 & \alpha^2 & \alpha^2 & 1 & 1 & 1 & \alpha & 1 & \alpha & \cdots & \alpha & 1 & \alpha^2 & \alpha^2 & \alpha & 1 & \alpha^2 & \alpha & \alpha^2
\end{pmatrix}.$$

We can generalize Constructions 3.5 and 3.6 to higher dimensional cases as follows:
Construction 3.7: Let $n = q^{3k}$, $k = 2, 3, \cdots$, where q is a power of an odd prime. Let $[1, x_1+x_2\gamma+\cdots+x_{3k}\gamma^{3k-1}, (x_1+x_2\gamma+\cdots+x_{3k}\gamma^{3k-1})^2, (x_1+x_2\beta+x_3\beta^2)^{q^2+q+1}, \cdots, (x_{3k-2}+x_{3k-1}\beta+x_{3k}\beta^2)^{q^2+q+1}]^T$ be a parity check matrix, where $\gamma \in GF(q^{3k}) - GF(q)$, $\beta \in GF(q^3) - GF(q)$ and $1, \gamma, \cdots, \gamma^{3k-1}$ is a basis of the vector space $GF(q^{3k})$ over $GF(q)$, $1, \beta, \beta^2$ is a basis of the vector space $GF(q^3)$ over $GF(q)$ respectively. Then we have a sequence of codes over $GF(q)$.

Theorem 3.7 *The codes in Construction 3.7 have the parameters*

$$n = q^{3k}, \qquad r = 7k + 1, \qquad \text{and } d \geq 5.$$

Construction 3.8: Let $n = q^{3k}$, $k = 2, 3, \cdots$, where $q = 2^i$. Let $[1, x_1 + x_2\gamma + \cdots + x_{3k}\gamma^{3k-1}, (x_1 + x_2\gamma + \cdots + x_{3k}\gamma^{3k-1})^{q+1}, (x_1 + x_2\beta + x_3\beta^2)^{q^2+q+1}, \cdots, (x_{3k-2} + x_{3k-1}\beta + x_{3k}\beta^2)^{q^2+q+1}]^T$ be a parity check matrix, where γ, β are as in Construction 3.7. Then we have a sequence of codes over $GF(q)$.

Theorem 3.8 *The codes in Construction 3.8 have the parameters*

$$n = q^{3k}, \qquad r = 7k + 1, \qquad \text{and } d \geq 5.$$

The proofs of Theorems 3.7 and 3.8 are similar to the proofs of Theorems 3.3 and 3.4, we omit the details.

Construction 3.9 Let $n = q^4$, q is a power of an odd prime or 2, and Let $\gamma \in GF(q^4) - GF(q)$, $\beta \in GF(q^3) - GF(q)$, $1, \gamma, \gamma^2, \gamma^3$ is a basis of $GF(q^4)$ over $GF(q)$, $1, \beta, \beta^2$ is a basis of $GF(q^3)$ over $GF(q)$. When q is odd, we take $H = [1, x + y\gamma + z\gamma^2 + w\gamma^3, (x + y\gamma + z\gamma^2 + w\gamma^3)^2, (x + y\beta + z\beta^2)^{q^2+q+1}, (w + 0\beta + 0\beta^2)^{q^2+q+1}]$; when q is even, we take $H = [1, x+y\gamma+z\gamma^2+w\gamma^3, (x+y\gamma+z\gamma^2+w\gamma^3)^{q+1}, (x+y\beta+z\beta^2)^{q^2+q+1}, (w+0\beta+0\beta^2)^{q^2+q+1}]$; let H^T be a parity check matrix. Then we have a code over $GF(q)$.

Theorem 3.9 *The code in Construction 3.9 has the parameters*

$$n = q^4, \qquad r = 11, \qquad \text{and } d \geq 5.$$

Proof: We prove only the case of q is even, when q is odd, the proof is similar. $(x+y\gamma+z\gamma^2+w\gamma^3)^{q+1} = x^2+xy\gamma+xz\gamma^2+xw\gamma^3+xy\gamma^q+y^2\gamma^{q+1}+yz\gamma^{q+2}+yw\gamma^{q+3}+xz\gamma^{2q}+yz\gamma^{2q+1}+z^2\gamma^{2q+2}+zw\gamma^{2q+3}+xw\gamma^{3q}+yw\gamma^{3q+1}+zw\gamma^{3q+2}+w^2\gamma^{3q+3}$. Suppose that

$$\begin{aligned}
\gamma^q &= a_0+a_1\gamma+a_2\gamma^2+a_3\gamma^3,\\
\gamma^{q+1} &= b_0+b_1\gamma+b_2\gamma^2+b_3\gamma^3,\\
\gamma^{q+2} &= c_0+c_1\gamma+c_2\gamma^2+c_3\gamma^3,\\
\gamma^{q+3} &= d_0+d_1\gamma+d_2\gamma^2+d_3\gamma^3,\\
\gamma^{2q} &= e_0+e_1\gamma+e_2\gamma^2+e_3\gamma^3,\\
\gamma^{2q+1} &= f_0+f_1\gamma+f_2\gamma^2+f_3\gamma^3,\\
\gamma^{2q+2} &= g_0+g_1\gamma+g_2\gamma^2+g_3\gamma^3,\\
\gamma^{2q+3} &= h_0+h_1\gamma+h_2\gamma^2+h_3\gamma^3,\\
\gamma^{3q} &= i_0+i_1\gamma+i_2\gamma^2+i_3\gamma^3,\\
\gamma^{3q+1} &= j_0+j_1\gamma+j_2\gamma^2+j_3\gamma^3,\\
\gamma^{3q+2} &= k_0+k_1\gamma+k_2\gamma^2+k_3\gamma^3,\\
\gamma^{3q+3} &= l_0+l_1\gamma+l_2\gamma^2+l_3\gamma^3.
\end{aligned}$$

Substitute these 12 equations into the above equation, we have $(x+y\gamma+z\gamma^2+w\gamma^3)^{q+1} = g_0(x,y,z,w)+g_1(x,y,z,w)\gamma+g_2(x,y,z,w)\gamma^2+g_3(x,y,z,w)\gamma^3$, where $g_0(x,y,z,w) = x^2+b_0y^2+g_0z^2+l_0w^2+a_0xy+(c_0+f_0)yz+(d_0+j_0)yw+e_0xz+i_0xw+(h_0+k_0)zw$, $g_1(x,y,z,w) = b_1y^2+g_1z^2+l_1w^2+(1+a_1)xy+(c_1+f_1)yz+(d_1+j_1)yw+e_1xz+i_1xw+(h_1+k_1)zw$, $g_2(x,y,z,w) = b_2y^2+g_2z^2+l_2w^2+a_2xy+(c_2+f_2)yz+(d_2+j_2)yw+(1+e_2)xz+i_2xw+(h_2+k_2)zw$, and $g_3(x,y,z,w) = b_3y^2+g_3z^2+l_3w^2+a_3xy+(e_3+f_3)yz+(d_3+j_3)yw+e_3xz+(1+i_3)xw+(h_3+k_3)zw$.

So the code has $r = 11$ parity checks: $1, x, y, z, w, g_0(x,y,z,w), g_1(x,y,z,w), g_2(x,y,z,w), g_3(x,y,z,w), (x+y\beta+z\beta^2)^{q^2+q+1}, w^3$. To prove $d \geq 5$, we have to prove $D_8^{(11)} \leq 3$. As in the proofs of the above theorems, it is easy to check that when $\lambda_1 = 1,2,3$, $D_{\{\lambda_1,\lambda_2,\cdots,\lambda_8\}} \leq 3$. We need only to prove that

$$D_{\{[y],[w],[g_0(x,y,z,w)],[g_1(x,y,z,w)],[g_2(x,y,z,w)],[g_3(x,y,z,w)],[(x+y\beta+z\beta^2)^{q^2+q+1}],[w^3]\}} \leq 3,$$

i.e., we need to prove the following system of equations has at most 3 distinct roots.

$$\begin{cases}
z+A_1x+B_1y+C_1 = 0,\\
w+A_2x+B_2y+C_2 = 0,\\
g_0(x,y,z,w)+A_3x+B_3y+C_3 = 0,\\
g_1(x,y,z,w)+A_4x+B_4y+C_4 = 0,\\
g_2(x,y,z,w)+A_5x+B_5y+C_5 = 0,\\
g_3(x,y,z,w)+A_6x+B_6y+C_6 = 0,\\
(x+y\beta+z\beta^2)^{q^2+q+1}+A_7x+B_7y+C_7 = 0,\\
w^3+A_8x+B_8y+C_8 = 0.
\end{cases}$$

We employ the idea in the proof of Theorem 3.5. Substitute $z = A_1x+B_1y+c_1$ and $w = A_2x+B_2y+C_2$ into $(x+y\gamma+z\gamma^2+w\gamma^3)^{q+1}$ and consider its part of degree 2, which is $(x+y\gamma+(A_1x+B_1y)\gamma^2+(A_2x+B_2y)\gamma^3)^{q+1} = ((1+A_1\gamma^2+B_1\gamma^3)x+(r+B_1\gamma^2+B_2\gamma^3)y)^{q+1}$. Because $1,\gamma,\gamma^2,\gamma^3$ are linear independent over $GF(q)$, $1+A_1\gamma^2+B_1\gamma^3 \neq 0$. So we can

divide the above equation by $(1+A_1\gamma^2+B_1\gamma^3)^{q+1}$. And if we let $c=\frac{\gamma+B_1\gamma^2+B_1\gamma^3}{1+A_1\gamma^2+A_2\gamma^3}$, then we have $(x+cy)^{q+1}=x^2+(c^q+c)xy+c^{q+1}y^2$. Suppose that $c^q+c=m_0+m_1\gamma+m_2\gamma^2+m_3\gamma^3$, $c^{q+1}=n_0+n_1\gamma+n_2\gamma^2+n_3\gamma^3$, then $(x+yc)^{q+1}=x^2+m_0xy+n_0y^2+(m_1xy+n_1y^2)\gamma+(m_2xy+n_2y^2)\gamma^2+(m_3xy+n_3y^2)\gamma^3$. So the above system of equations is equivalent to

$$\begin{cases} z+A_1x+B_1y+C_1=0, \\ w+A_2x+B_2y+C_2=0, \\ x^2+m_0xy+n_0y^2+A_3'x+B_3'y+C_3'=0, \\ m_1xy+n_1y^2+A_4'x+B_4'y+C_4'=0, \\ m_2xy+n_2y^2+A_5'x+B_5'y+C_5'=0, \\ m_3xy+n_3y^2+A_6'x+B_6'y+C_6'=0, \\ (x+y\beta+z\beta^2)^{q^2+q+1}+A_7x+B_7y+C_7=0, \\ w^3+A_8x+B_8y+C_8=0. \end{cases}$$

If we can prove that in the following systems of equations, there exist at least one system of equations with the determinant of the matrix of the coefficients of x^2, xy and y^2 is not zero, then the proof is completed.

$$\begin{cases} x^2+m_0xy+n_0y^2+A_3'x+B_3'y+C_3'=0, \\ m_ixy+n_iy^2+A_{i+3}'x+B_{i+3}'y+C_{i+3}'=0, \\ m_jxy+n_jy^2+A_{j+3}'x+B_{j+3}'y+C_{j+3}'=0, \end{cases} \qquad \text{for } 1\le i<j\le 3.$$

Now we prove it as follows. If

$$\begin{vmatrix} 1 & m_0 & n_0 \\ 0 & m_i & n_i \\ 0 & m_j & n_j \end{vmatrix} = \begin{vmatrix} m_i & n_i \\ m_j & n_j \end{vmatrix} = 0,$$

for all i,j, $1\le i<j\le 3$. Then there is a nonzero element $a\in GF(q)$, such that $(n_1,n_2,n_3)=a(m_1,m_2,m_3)$. But $c^q+c=m_0+m_1\gamma+m_2\gamma^2+m_3\gamma^3$, $c^{q+1}=n_0+n_1\gamma+n_2\gamma^2+n_3\gamma^3$. Thus we have $c^{q+1}-n_0=a(c^q+c-m_0)$, it shows $c^{q+1}+a(c^q+c)=am_0+n_0=b\in GF(q)$. As in the proof of Theorem 3.6, we have

$$a=\frac{c^{q^2+q}+c^{q+1}}{c^{q^2}+c}=c^q.$$

So $c^q\in GF(q)$. Then $c^{q^2}=(c^q)^q=c^q$, $c^{q^3}=(c^{q^2})^q=(c^q)^q=c^q$, $\cdots$, $c^{q^4}=(c^{q^3})^q=(c^q)^q=c^q$. On the other hand, $c\in GF(q^4)$, $c^{q^4}=c$, so $c^q=c$, it shows $c\in GF(q)$. From $c=\frac{\gamma+B_1\gamma^2+B_1\gamma^3}{1+A_1\gamma^2+A_2\gamma^3}$, we have

$$(B_2-cA_2)\gamma^3+(B_1-cA_1)\gamma^2+\gamma+c=0,$$

But $1,\gamma,\gamma^2,\gamma^3$ are linearly independent over $GF(q)$. This is a contradiction. So the proof is completed. □

We can generalize Construction 3.9 to higher dimensional cases as follows:

Construction 3.10 Let $n=q^{3k+1}$, $k=2,3,\cdots$, where q is a power of an odd prime or 2, and let $\gamma\in GF(q^{3k+1})-GF(q)$, $1,\gamma,\cdots,\gamma^{3k}$ is a basis of $GF(q^{3k+1})$ over $GF(q)$, β is

as in Construction 3.9. When q is odd, we take $H = [1, x_1 + x_2\gamma + \cdots + x_{3k+1}\gamma^{3k}, (x_1 + x_2\gamma + \cdots + x_{3k+1}\gamma^{3k})^2, (x_1 + x_2\beta + x_3\beta^2)^{q^2+q+1}, \cdots, (x_{3k+1} + 0\beta + 0\beta^2)^{q^2+q+1}]$; when q is even, we take $H = [1, x_1 + x_2\gamma + \cdots + x_{3k+1}\gamma^{3k}, (x_1 + x_2\gamma + \cdots + x_{3k+1}\gamma^{3k})^{q+1}, (x_1 + x_2\beta + x_3\beta^2)^{q^2+q+1}, \cdots, (x_{3k+1} + 0\beta + 0\beta^2)^{q^2+q+1}]$. Let H^T be parity check matrices. Then we have a sequence of codes over $GF(q)$.

Theorem 3.10 *The codes in Construction 3.10 have the parameters*

$$n = q^{3k+1}, \qquad r = 7k + 4, \qquad \text{and } d \geq 5.$$

Now as a summary, we have the following theorem,

Theorem 3.11 *Over finite field $GF(q)$, q is odd or even, we have linear codes with the parameters:*

$$n = q^m, \qquad r = 2m + \lceil \frac{m}{3} \rceil + 1, \qquad \text{and } d \geq 5, \quad m = 3, 4, \cdots.$$

And when $m = 2$, we have q-ary codes with

$$n = q^2, \qquad r = 7, \qquad \text{and } d \geq 5.$$

Remark 3.1: In the Theorem 6[5], a class of codes over $GF(q)$,where $q = 2^i$, were constructed as follows. Let $U_q^m(I)$ be a cyclic code over $F = GF(2^i)$, with a string $I = \{1, \frac{(q^m+q)}{2}\}$, and $U = U_q^m(I, F^{m-1})$ be the corresponding punctured code with length $n = q^{m-1}$ defined on a $(m-1)$-dimensional subspace F^{m-1} of F^m. Then the code U' over $GF(2^i)$ with minimum distance ≥ 5 was constructed by adding some parity checks to U. U' has the parameters:

$$n = q^{m-1}, \quad r \leq 2m + \lceil \frac{m-1}{3} \rceil, \quad d \geq 5, \quad m = 2, 3, \cdots.$$

Let $N_m(*)$ be a norm function from $GF(q^m)$ to $GF(q)$ defined as

$$N_m(x) = x^{q^{m-1}+q^{m-2}+\cdots+1}.$$

Obviously, N_m maps any $x \neq 0$ into $GF(q) - 0$. Represent $GF(q^m)$ as F^m with a basis $g_1, \cdots, g_m$ over $F = GF(q)$. Then for any

$$x = \sum_{i=1}^{m} \tau_i g_i$$

its norm

$$N_m(x) = N_m(\sum_{i=1}^{m} \tau_i g_i) = N_m(\tau_1, \cdots, \tau_m)$$

is converted into a homogeneous form of variables $\tau, \cdots, \tau_m$ of degree m with nonzero values in F for any $(\tau_1, \cdots, \tau_m) \neq 0$.

Now for any $(\tau_1, \cdots, \tau_m)$ decompose the coordinates $\tau_1, \cdots, \tau_m$ into disjoint 3-tuples $((\tau_1, \tau_2, \tau_3), (\tau_4, \tau_5, \tau_6), \cdots)$, where for any $m < j \leq 3\lceil \frac{m}{3} \rceil$, define $\tau_j = 0$. For example, a vector $(\tau_1, \tau_2, \tau_3, \tau_4) \in GF(q^4)$ can be decomposed into $((\tau_1, \tau_2, \tau_3), (\tau_4, 0, 0))$.

Let q be an odd, and let $W = W_q^m(I, X = F^m)$ be an extended BCH codes with the string $I = \{0, 1, 2\}$ for any $m = 1, 2, \cdots$. Define for any locator $z = (\tau_1, \cdots, \tau_m) \in GF(q^m)$ the vector $p(z) = (p_1, \cdots, p_l)$ over $GF(q)$ of length $l = \lceil \frac{m}{3} \rceil$, where

$$p_{j+1} = p_{j+1}(z) = N_3(\tau_{3j+1}, \tau_{3j+2}, \tau_{3j+3}),$$

for all $j = 0, 1, \cdots, l-1$. Let p be the matrix of size $l \times n$ with columns $p^T(z_i)$, $i = 1, 2, \cdots, n$, and Let P be the code with the parity check matrix p. Finally, define $W' = W \cap P$.

Theorem 7 [5] showed that the code W' has the parameters:

$$n = q^m, \quad r \leq 2m + \lceil \frac{m}{3} \rceil + 1, \quad d \geq 5, \quad m = 2, 3, \cdots.$$

But there is an oversight in the Theorem 7 of [5]. When $m = 2$, in order to define code P, we have to consider an extened field $GF(q^{m'})$, where $m' = 3\lceil \frac{m}{3} \rceil = 3$. In the extended field, the string $I = \{0, 1, 2\}$ will raise $1 + m + 3\lceil \frac{m}{3} \rceil$ parity checks (not $2m + 1$). In fact, consider the q-ary code generated by a parity check matrix $[1, x + y\beta, (x + y\beta + 0\beta^2)^2]^T$, where $z = x + y\beta \in GF(q^{m'})$, because $(x + y\beta)^2 = x + 2xy\beta + y^2\beta^2$, so the code has parity checks: $1, x, y, x^2, 2xy, y^2$. $r = 1 + m + 3\lceil \frac{m}{3} \rceil = 1 + 2 + 3 = 6$. So when $n = q^2$, the number of parity checks of the codes in Theorem 7 should be 7.

Dumer's codes are known to be optimal in the sense that no other double-byte error-correcting codes with the same code lengths have fewer number of parity checks, but unfortunately, they are defined only on $GF(q)$, where q is odd. Our codes have the same parameters as Dumer's codes, but our codes are defined on $GF(2^i)$.

Now we give a proof of Theorem 3.4.

Proof of Theorem 3.4:

Let $(x_1 + x_2\gamma + \cdots + x_{3k+2}\gamma^{3k+1})^{q+1} = g_0(x_1, \cdots, x_{3k+2}) + \cdots + g_0(x_1, \cdots, x_{3k+2})\gamma^{3k+1}$. Then the code has $7k+6$ parity checks: $1, x_1, \cdots, x_{3k+2}, g_0(x_1, \cdots, x_{3k+2}), \cdots, g_{3k+1}(x_1, \cdots, x_{3k+2})$, $(x_1 + x_2\beta + x_3\beta^2)^{q^2+q+1}, \cdots, (x_{3k+1} + x_{3k+2}\beta + 0\beta^2)^{q^2+q+1}$. To prove $d \geq 5$, by Theorem 2.1, we need to prove $D_{7k+3}^{(7k+6)} \leq 3$. We need only to prove the following system of equations has at most 3 distinct roots:

$$\begin{cases} x_3 + A_1x_1 + B_1x_2 + C_1 = 0, \\ \quad \vdots \\ x_{3k+2} + A_{3k}x_1 + B_{3k}x_2 + C_{3k} = 0, \\ g_0(x_1, \cdots, x_{3k+2}) + A_{3k+1}x_1 + B_{3k+1}x_2 + C_{3k+1} = 0, \\ \quad \vdots \\ g_{3k+1}(x_1, \cdots, x_{3k+2}) + A_{6k+2}x_1 + B_{6k+2}x_2 + C_{6k+2} = 0, \\ (x_1 + x_2\beta + x_3\beta^2)^{q^2+q+1} + A_{6k+3}x_1 + B_{6k+3}x_2 + C_{6k+3} = 0, \\ \quad \vdots \\ (x_{3k+1} + x_{3k+2}\beta + 0\beta^2)^{q^2+q+1} + A_{7k+6}x_1 + B_{7k+6}x_2 + C_{7k+6} = 0. \end{cases} \tag{3.3}$$

Obviously, the number of distinct roots of (3.3) is not greater than the number of distinct roots of the following system of equations:

$$\begin{cases} x_3 + A_1x_1 + B_1x_2 + C_1 = 0, \\ \quad\vdots \\ x_{3k+2} + A_{3k}x_1 + B_{3k}x_2 + C_{3k} = 0, \\ g_0(x_1, \cdots, x_{3k+2}) + A_{3k+1}x_1 + B_{3k+1}x_2 + C_{3k+1} = 0, \\ \quad\vdots \\ g_{3k+1}(x_1, \cdots, x_{3k+2}) + A_{6k+2}x_1 + B_{6k+2}x_2 + C_{6k+2} = 0. \end{cases} \tag{3.4}$$

Substituting $x_3 = -A_1x_1 - B_1x_2 - C_1, \cdots, x_{3k+2} = -A_{3k}x_1 - B_{3k}x_2 - C_{3k}$ into $(x_1 + x_2\gamma + x_3\gamma^2 + \cdots + x_{3k+2}\gamma^{3k+1})^{q+1}$, we have $[(1 - A_1\gamma^2 - \cdots - A_{3k}\gamma^{3k+1})x_1 + (\gamma - B_1\gamma^2 - \cdots - B_{3k}\gamma^{3k+1})x_2 - (C_1\gamma^2 + \cdots + C_{3k}\gamma^{3k+1})]^{q+1}$. By the hypothesis, we have $1 - A_1\gamma^2 - \cdots - A_{3k}\gamma^{3k+1} \neq 0$. Dividing the formula by $(1 - A_1\gamma^2 - \cdots - A_{3k}\gamma^{3k+1})^{q+1}$, we obtain

$$\left(x_1 + \frac{\gamma - B_1\gamma^2 - \cdots - B_{3k}\gamma^{3k+1}}{1 - A_1\gamma^2 - \cdots - A_{3k}\gamma^{3k+1}}x_2 - \frac{C_1\gamma^2 + \cdots + C_{3k}\gamma^{3k+1}}{1 - A_1\gamma^2 - \cdots - A_{3k}\gamma^{3k+1}}\right)^{q+1},$$

whose part of degree 2 is

$$\left(x_1 + \frac{\gamma - B_1\gamma^2 - \cdots - B_{3k}\gamma^{3k+1}}{1 - A_1\gamma^2 - \cdots - A_{3k}\gamma^{3k+1}}x_2\right)^{q+1}. \tag{3.5}$$

Let $c = \frac{\gamma - B_1\gamma^2 - \cdots - B_{3k}\gamma^{3k+1}}{1 - A_1\gamma^2 - \cdots - A_{3k}\gamma^{3k+1}}$, and substitute it into (3.5), we have $(x_1 + cx_2)^{q+1} = x_1^2 + (c^q + c)x_1x_2 + c^{q+1}x_2^2$. Suppose

$$\begin{aligned} c^q + c &= a_0 + a_1\gamma + \cdots + a_{3k+1}\gamma^{3k+1}, \\ c^{q+1} &= b_0 + b_1\gamma + \cdots + b_{3k+1}\gamma^{3k+1}. \end{aligned}$$

Then $(x_1 + cx_2)^{q+1} = (x_1^2 + a_0x_1x_2 + b_0x_2^2) + (a_1x_1x_2 + b_1x_2^2)\gamma + \cdots + (a_{3k+1}x_1x_2 + b_{3k+1}x_2^2)\gamma^{3k+1}$. So (3.4) is equivalent to the following system of equations:

$$\begin{cases} x_3 + A_1x_1 + B_1x_2 + C_1 = 0, \\ \quad\vdots \\ x_{3k+2} + A_{3k}x_1 + B_{3k}x_2 + C_{3k} = 0, \\ x_1^2 + a_0x_1x_2 + b_0x_2^2 + A_1'x_1 + B_1'x_2 + C_1' = 0, \\ a_1x_1x_2 + b_1x_2^2 + A_2'x_1 + B_2'x_2 + C_2' = 0, \\ \quad\vdots \\ a_{3k+1}x_1x_2 + b_{3k+1}x_2^2 + A_{3k+2}'x_1 + B_{3k+2}'x_2 + C_{3k+2}' = 0. \end{cases} \tag{3.6}$$

As in the proof of Theorem 3.9, if we can prove there exists a determinant in the following determinants such that it is not equal to 0, then there are three equations of x_1 and x_2 in (3.6) are equivalent to (3.2), and the proof is completed:

$$\begin{vmatrix} 1 & a_0 & b_0 \\ 0 & a_i & b_i \\ 0 & a_j & b_j \end{vmatrix} = \begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix}, \quad 1 \leq i < j \leq 3k + 1.$$

If it is not, then we have

$$\begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix} = 0, \quad \text{for all } i, j, 1 \le i < j \le 3k+1.$$

Then there is a nonzero element $a \in GF(q)$ such that

$$(b_1, \cdots, b_{3k+1}) = a(a_1, \cdots, a_{3k+1}).$$

So we have $c^{q+1} - b_0 = a(c^q + c - a_0)$, where a_0, b_0 and a in $GF(q)$. As in the proof of Theorem 3.9, we can prove $c \in GF(q)$, but this is impossible, since

$$c = \frac{\gamma - B_1\gamma^2 - \cdots - B_{3k}\gamma^{3k+1}}{1 - A_1\gamma^2 - \cdots - A_{3k}\gamma^{3k+1}},$$

and $1, \gamma, \cdots, \gamma^{3k+1}$ is a basis of $GF(q^{3k+2})$. □

In the same way, we can prove Theorems 3.3, 3.7, 3.8 and 3.10.

4 Decoding

At first, we expound the decoding procedure of the codes in Construction 3.6.

Let $Z = x + y\beta + z\beta^2$, and $Z_1 = Z(P_1), Z_2 = Z(P_2), \cdots, Z_n = Z(P_n)$, where $P_1, P_2, \cdots, P_n$ are all points of $GF(q^3)$, $n = q^3$. Suppose $y = (y_1, y_2, \cdots, y_n) \in GF(q)^n$ is a received vector. We define the the following syndromes of y:

$$S_1 = y_1 + y_2 + \cdots + y_n,$$

$$S_Z = Z_1y_1 + Z_2y_2 + \cdots + Z_ny_n,$$

$$S_{Z^{q+1}} = Z_1^{q+1}y_1 + Z_2^{q+1}y_2 + \cdots + Z_n^{q+1}y_n,$$

$$S_{Z^{q^2+q+1}} = Z_1^{q^2+q+1}y_1 + Z_2^{q^2+q+1}y_2 + \cdots + Z_n^{q^2+q+1}y_n.$$

Moreover, define

$$S_{Z^q} = (S_Z)^q = Z_1^q y_1 + Z_2^q y_2 + \cdots + Z_n^q y_n,$$

$$S_{Z^{q^2+q}} = (S_{Z^{q+1}})^q = Z_1^{q^2+q}y_1 + Z_2^{q^2+q}y_2 + \cdots + Z_n^{q^2+q}y_n,$$

$$S_{Z^{q^2}} = (S_Z)^{q^2} = Z_1^{q^2}y_1 + Z_2^{q^2}y_2 + \cdots + Z_n^{q^2}y_n,$$

$$S_{Z^{q^2+1}} = (S_{Z^{q+1}})^{q^2} = Z_1^{q^2+1}y_1 + Z_2^{q^2+1}y_2 + \cdots + Z_n^{q^2+1}y_n.$$

We have two *syndrome matrices* as follows

$$\begin{pmatrix} S_1 & S_{Z^q} & S_{Z^{q^2+q}} \\ S_Z & S_{Z^{q+1}} & S_{Z^{q^2+q+1}} \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} S_1 & S_{Z^q} & S_{Z^{q^2}} \\ S_Z & S_{Z^{q+1}} & S_{Z^{q^2+1}} \end{pmatrix}.$$

If y is corrupted by two errors (ξ_i, Z_i) and (ξ_j, Z_j), where ξ_i and ξ_j are error values, Z_i and Z_j are the corresponding locators. Then we have

$$\begin{aligned}
&S_1 = \xi_i + \xi_j,\\
&S_Z = Z_i\xi_i + Z_j\xi_j,\\
&S_{Z^{q+1}} = Z_i^{q+1}\xi_i + Z_j^{q+1}\xi_j,\\
&S_{Z^{q^2+q+1}} = Z_i^{q^2+q+1}\xi_j + Z_j^{q^2+q+1}\xi_j,\\
&S_{Z^q} = Z_i^q\xi_i + Z_j^q\xi_j,\\
&S_{Z^{q^2+q}} = Z_i^{q^2+q}\xi_i + Z_j^{q^2+q}\xi_j,\\
&S_{Z^{q^2}} = Z_i^{q^2}\xi_i + Z_j^{q^2}\xi_j,\\
&S_{Z^{q^2+1}} = Z_i^{q^2+1}\xi_i + Z_j^{q^2+1}\xi_j.
\end{aligned}$$

The syndrome matrices can be decomposed into

$$\begin{pmatrix} S_1 & S_{Z^q} & S_{Z^{q^2+q}} \\ S_Z & S_{Z^{q+1}} & S_{Z^{q^2+q+1}} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ Z_i & Z_j \end{pmatrix} \begin{pmatrix} \xi_i & 0 \\ 0 & \xi_j \end{pmatrix} \begin{pmatrix} 1 & Z_i^q & Z_i^{q^2+q} \\ 1 & Z_j^q & Z_j^{q^2+q} \end{pmatrix} \tag{4.1}$$

and

$$\begin{pmatrix} S_1 & S_{Z^q} & S_{Z^{q^2}} \\ S_Z & S_{Z^{q+1}} & S_{Z^{q^2+1}} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ Z_i & Z_j \end{pmatrix} \begin{pmatrix} \xi_i & 0 \\ 0 & \xi_j \end{pmatrix} \begin{pmatrix} 1 & Z_i^q & Z_i^{q^2} \\ 1 & Z_j^q & Z_j^{q^2} \end{pmatrix}. \tag{4.2}$$

The three column vectors in the syndrome matrices must be linearly dependent over $GF(q^3)$. In fact we can find A, B, C and D in $GF(q^3)$, such that

$$\begin{pmatrix} S_{Z^{q^2+q}} \\ S_{Z^{q^2+q+1}} \end{pmatrix} + A \begin{pmatrix} S_{Z^q} \\ S_{Z^{q+1}} \end{pmatrix} + B \begin{pmatrix} S_1 \\ S_Z \end{pmatrix} = 0, \tag{4.3}$$

and

$$\begin{pmatrix} S_{Z^{q^2}} \\ S_{Z^{q^2+1}} \end{pmatrix} + C \begin{pmatrix} S_{Z^q} \\ S_{Z^{q+1}} \end{pmatrix} + D \begin{pmatrix} S_1 \\ S_Z \end{pmatrix} = 0. \tag{4.4}$$

Because the matrices $\begin{pmatrix} 1 & 1 \\ z_i & z_j \end{pmatrix}$ and $\begin{pmatrix} \xi_i & 0 \\ 0 & \xi_j \end{pmatrix}$ are nondegenerate, so we have

$$\begin{pmatrix} Z_i^{q^2+q} \\ Z_j^{q^2+q} \end{pmatrix} + A \begin{pmatrix} Z_i^q \\ Z_j^q \end{pmatrix} + B \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 0, \tag{4.5}$$

and

$$\begin{pmatrix} Z_i^{q^2} \\ Z_j^{q^2} \end{pmatrix} + C \begin{pmatrix} Z_i^q \\ Z_j^q \end{pmatrix} + D \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 0. \tag{4.6}$$

It is well known that, in $GF(q^3)$, if $x_1^q = x_2^q$, then $x_1 = x_2$. In fact, by $x_1^q = x_2^q$, we have

$$x_1^{q^3} = x_2^{q^3},$$

but $x_1^{q^3} = x_1, x_2^{q^3} = x_2$, so

$$x_1 = x_2.$$

So we can take substitutions $Y_i = Z_i^q$ and $Y_j = Z_j^q$. Then by (4.5) and (4.6), Y_i, Y_j are the roots of the following equations

$$Y^{q+1} + AY + B = 0, \tag{4.7}$$

and

$$Y^q + CY + D = 0. \tag{4.8}$$

Multiply (4.8) by Y and then add it into (4.7), we have

$$CY^2 + (A + D)Y + B = 0. \tag{4.9}$$

If $C = 0$, then (4.8) has only one root, but $Y_i = Z_i^q \neq Y_j = Z_j^q$ are all its roots, so it is impossible. When $C \neq 0$, (4.9) is an equation of degree 2, it has two roots. Hence we can completely determine the error locators Z_i and Z_j. Then by (4.1) or (4.2), the error values are determined.

Example 4.1: Let C be the code in Example 3.2. The following matrix is a parity check matrix of C

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \alpha & \alpha & \cdots & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 1 & \alpha & \alpha & \alpha & \alpha & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\
0 & 1 & \alpha & \alpha^2 & 0 & 1 & \alpha & \alpha^2 & 0 & 1 & \cdots & \alpha^2 & 0 & 1 & \alpha & \alpha^2 & 0 & 1 & \alpha & \alpha^2 \\
0 & 1 & \alpha^2 & \alpha & 1 & 0 & 1 & \alpha & \alpha^2 & 1 & \cdots & \alpha & \alpha & 0 & 0 & \alpha & 0 & \alpha^2 & 0 & \alpha^2 \\
0 & \alpha & 1 & \alpha^2 & 0 & \alpha & 0 & 1 & 0 & \alpha^2 & \cdots & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 & 1 & \alpha^2 & 0 & \alpha \\
0 & 1 & \alpha^2 & \alpha & 0 & 0 & 1 & 1 & 0 & \alpha^2 & \cdots & 0 & 0 & \alpha^2 & 0 & \alpha^2 & \alpha & \alpha & \alpha^2 & \alpha^2 \\
0 & \alpha^2 & \alpha^2 & \alpha^2 & 1 & 1 & 1 & \alpha & 1 & \alpha & \cdots & \alpha & 1 & \alpha^2 & \alpha^2 & \alpha & 1 & \alpha^2 & \alpha & \alpha^2
\end{pmatrix}.$$

We have $Z_1 = 0$, $Z_2 = \beta^2$, $Z_3 = \beta^{23}$, $Z_4 = \beta^{44}$, $Z_5 = 1$, $Z_6 = \beta^{12}$, $Z_7 = \beta^{15}$, $Z_8 = \beta^{37}$, $\cdots$, $Z_{59} = \beta^{17}$, $Z_{60} = \beta^{25}$, $Z_{61} = \beta^{48}$, $Z_{62} = \beta^{32}$, $Z_{63} = \beta^{34}$, $Z_{64} = \beta^5$. Let $y = (0, \alpha, 0, \cdots, 0, \alpha^2)$ be a received vector. Then $S_1 = 1$, $S_Z = \beta^{27}$, $S_{Z^{q+1}} = \beta^{22}$, $S_{Z^{q^2+q+1}} = \beta^{42}$, $S_{Z^q} = \beta^{45}$, $S_{Z^{q^2+q}} = \beta^{25}$, $S_{Z^q} = \beta^{54}$, and $S_{Z^{q^2+1}} = \beta^{37}$. So the syndrome matrices are

$$\begin{pmatrix} 1 & \beta^{45} & \beta^{25} \\ \beta^{27} & \beta^{22} & \beta^{42} \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 & \beta^{45} & \beta^{54} \\ \beta^{27} & \beta^{22} & \beta^{37} \end{pmatrix}.$$

Then by

$$\begin{pmatrix} \beta^{25} \\ \beta^{42} \end{pmatrix} + A \begin{pmatrix} \beta^{45} \\ \beta^{22} \end{pmatrix} + B \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 0,$$

and

$$\begin{pmatrix} \beta^{54} \\ \beta^{37} \end{pmatrix} + C \begin{pmatrix} \beta^{45} \\ \beta^{22} \end{pmatrix} + D \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 0,$$

we have $A = \beta^{59}$, $B = \beta^{58}$, $C = \beta^{30}$, $D = \beta^{33}$. So by (4.9), we have

$$\beta^{30}Y^2 + (\beta^{59} + \beta^{33})Y + \beta^{58} = 0,$$

i.e.,

$$Y^2 + \beta^{30}Y + \beta^{33} = 0.$$

This equation has two roots in $GF(q^3)$:

$$Y_i = \beta^8, \qquad \text{and} \quad Y_j = \beta^{20}.$$

So we have

$$Z_i = \beta^2, \qquad \text{and} \quad Z_j = \beta^5.$$

Then we know $i = 2$, and $j = 64$, and by (4.1) or (4.2) the error values are $\xi_2 = \beta^{21} = \alpha$, $\xi_{64} = \beta^{42} = \alpha^2$.

Now we give a general decoding procedure for the codes in the last section.

Let $Z = x_1 + x_2\gamma + \cdots + x_m\gamma^{m-1}$, and $Z_1 = Z(P_1), Z_2 = Z(P_2), \cdots, Z_n = Z(P_n)$, where $P_1, P_2, \cdots, P_n$ are all points of $GF(q^m)$, $n = q^m$. Suppose $y = (y_1, y_2, \cdots, y_n) \in GF(q)^n$ is a received vector. We define the following syndromes of y:

$$S_1 = y_1 + y_2 + \cdots + y_n,$$

$$S_Z = Z_1y_1 + Z_2y_2 + \cdots + Z_ny_n,$$

$$S_{Z^{q+1}} = Z_1^{q+1}y_1 + Z_2^{q+1}y_2 + \cdots + Z_n^{q+1}y_n.$$

Moreover, define

$$S_{Z^q} = (S_Z)^q = Z_1^q y_1 + Z_2^q y_2 + \cdots + Z_n^q y_n,$$

$$S_{Z^{q^{m-1}}} = (S_Z)^{q^{m-1}} = Z_1^{q^{m-1}} y_1 + Z_2^{q^{m-1}} y_2 + \cdots + Z_n^{q^{m-1}} y_n,$$

$$S_{Z^{q^{m-1}+1}} = (S_{Z^{q+1}})^{q^{m-1}} = Z_1^{q^{m-1}+1}y_1 + Z_2^{q^{m-1}+1}y_2 + \cdots + Z_n^{q^{m-1}+1}y_n.$$

We have the *syndrome matrix*

$$\begin{pmatrix} S_1 & S_{Z^q} & S_{Z^{q^{m-1}}} \\ S_Z & S_{Z^{q+1}} & S_{Z^{q^{m-1}+1}} \end{pmatrix}.$$

If y is corrupted by two errors (ξ_i, Z_i) and (ξ_j, Z_j), where ξ_i and ξ_j are error values, Z_i and Z_j are the corresponding locators. Then we have

$$\begin{aligned}
&S_1 = \xi_1 + \xi_2, \\
&S_Z = Z_1\xi_1 + Z_2\xi_2, \\
&S_{Z^{q+1}} = Z_1^{q+1}\xi_1 + Z_2^{q+1}\xi_2, \\
&S_{Z^q} = Z_1^q\xi_1 + Z_2^q\xi_2, \\
&S_{Z^{q^{m-1}}} = Z_1^{q^{m-1}}\xi_1 + Z_2^{q^{m-1}}\xi_2, \\
&S_{Z^{q^{m-1}+1}} = Z_1^{q^{m-1}+1}\xi_1 + Z_2^{q^{m-1}+1}\xi_2.
\end{aligned}$$

The syndrome matrix can be decomposed into

$$\begin{pmatrix} S_1 & S_{Z^q} & S_{Z^{q^{m-1}}} \\ S_Z & S_{Z^{q+1}} & S_{Z^{q^{m-1}+1}} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ Z_i & Z_j \end{pmatrix} \begin{pmatrix} \xi_i & 0 \\ 0 & \xi_j \end{pmatrix} \begin{pmatrix} 1 & Z_i^q & Z_i^{q^{m-1}} \\ 1 & Z_j^q & Z_j^{q^{m-1}} \end{pmatrix} \tag{4.10}$$

The three column vectors in the syndrome matrix must be linearly dependent over $GF(q^m)$. We can find A, B in $GF(q^3)$, such that

$$\begin{pmatrix} S_{Z^{q^{m-1}}} \\ S_{Z^{q^{m-1}+1}} \end{pmatrix} + A \begin{pmatrix} S_{Z^q} \\ S_{Z^{q+1}} \end{pmatrix} + B \begin{pmatrix} S_1 \\ S_Z \end{pmatrix} = 0, \tag{4.11}$$

So by (4.10) we have

$$\begin{pmatrix} Z_i^{q^{m-1}} \\ Z_j^{q^{m-1}} \end{pmatrix} + A \begin{pmatrix} Z_i^q \\ Z_j^q \end{pmatrix} + B \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 0, \tag{4.12}$$

So Z_i and Z_j are the solutions of the following equation

$$Z^{q^{m-1}} + AZ^q + B = 0.$$

From the above equation, we obtain

$$A^q Z^{q^2} + Z + B^q = 0.$$

Let $A' = \frac{1}{A^q}$, $B' = \frac{B^q}{A^q}$, we have

$$Z^{q^2} + A'Z + B' = 0. \tag{4.13}$$

This equation has at most q^2 roots in $GF(q^m)$.

In order to determine Z_i and Z_j, we give other equations about them. Let $Z_k = (x_{1k}, x_{2k}, \cdots, x_{mk})$, $k = 1, 2, \cdots, n = q^m$. We define the following syndromes

$$\begin{aligned} &s_1 = y_1 + y_2 + \cdots + y_n, \\ &s_{x_1} = x_{11}y_1 + x_{12}y_2 + \cdots + x_{1n}y_n, \\ &s_{f(x_1,x_2,x_3)} = f(x_{11}, x_{21}, x_{31})y_1 + f(x_{12}, x_{22}, x_{32})y_2 + \cdots + f(x_{1n}, x_{2n}, x_{3n})y_n, \end{aligned}$$

where $f(x, y, z) = (x + y\beta + z\beta^2)^{q^2+q+1}$. We have

$$\begin{aligned} &s_1 = \xi_i + \xi_j, \\ &s_{x_1} = x_{1i}\xi_i + x_{1j}\xi_j, \\ &s_{f(x_1,x_2,x_3)} = f(x_{1i}, x_{2i}, x_{3i})\xi_i + f(x_{1j}, x_{2j}, x_{3j})\xi_j \end{aligned}$$

By the above three equations, we know the following matrix is degenerate

$$\begin{pmatrix} 1 & 1 & s_1 \\ x_{1i} & x_{1j} & s_{x_1} \\ f(x_{1i}, x_{2i}, x_{3i}) & f(x_{1j}, x_{2j}, x_{3j}) & s_{f(x_1,x_2,x_3)} \end{pmatrix}.$$

So we have

$$\begin{vmatrix} 1 & 1 & s_1 \\ x_{1i} & x_{1j} & s_{x_1} \\ f(x_{1i},x_{2i},x_{3i}) & f(x_{1j},x_{2j},x_{3j}) & s_{f(x_1,x_2,x_3)} \end{vmatrix} = 0. \tag{4.14}$$

This is an equation about $x_{1i}, x_{2i}, x_{3i}, x_{1j}, x_{2j}$, and x_{3j} of degree 4. By the same way, we can obtain a sequence of equations about $x_{l,i}, x_{l+1,i}, x_{l+2,i}, x_{l,j}, x_{l+1,j}$, and $x_{l+1,j}$, $l = 1, 4, \cdots, 3\lceil \frac{m}{3} \rceil - 2$. By these equations and (4.13), we can determine Z_i and Z_j. Then by (4.10), the error values ξ_i and ξ_j are determined.

5 Another Class of Double-Byte Error-Correcting Codes

Let $n = q^m$, when $3|m$, we have another construction of codes with minimum distance ≥ 5.

Construction 5.1 Let $n = q^m$, $m = 3, 6, \cdots$, where q is a power of 2 or an odd prime, and let $m = 3l$. Suppose that $\gamma \in GF(q^m) - GF(q)$, $1, \gamma, \cdots, \gamma^{m-1}$ is a basis of $GF(q^m)$ over $GF(q)$. Let $H = [1, (x_1 + x_2\gamma + \cdots + x_m\gamma^{m-1})^{q^l}, (x_1 + x_2\gamma + \cdots + x_m\gamma^{m-1})^{q^l+1}, (x_1 + x_2\gamma + \cdots + x_m\gamma^{m-1})^{q^{2l}+q^l+1}]$. Let H^T be a parity check matrix, we have a sequence of codes over $GF(q)$.

Theorem 5.1 *The codes in Construction 5.1 are double-byte error-correcting codes and have the parameters*

$$n = q^m, \qquad r = 7l + 1.$$

Proof: Obviously, $((x_1 + x_2\gamma + \cdots + x_m\gamma^{m-1})^{q^{2l}+q^l+1})^{q^l} = (x_1 + x_2\gamma + \cdots + x_m\gamma^{m-1})^{q^{2l}+q^l+1}$, it shows, $(x_1 + x_2\gamma + \cdots + x_m\gamma^{m-1})^{q^{2l}+q^l+1} \in GF(q^l)$. So the code has $r = 7l + 1$ parity checks.

Let $Z = x_1 + x_2\gamma + \cdots + x_m\gamma^{m-1}$, and $Z_1 = Z(P_1), Z_2 = Z(P_2), \cdots, Z_n = Z(P_n)$, where $P_1, P_2, \cdots, P_n$ are all points of $GF(q^m)$, $n = q^m$. Suppose $y = (y_1, y_2, \cdots, y_n) \in GF(q)^n$ is a received vector. We define the the following syndromes of y as follows.

$$S_1 = y_1 + y_2 + \cdots + y_n,$$

$$S_{Z^{q^l}} = Z_1^{q^l} y_1 + Z_2^{q^l} y_2 + \cdots + Z_n^{q^l} y_n,$$

$$S_{Z^{q^l+1}} = Z_1^{q^l+1} y_1 + Z_2^{q^l+1} y_2 + \cdots + Z_n^{q^l+1} y_n,$$

$$S_{Z^{q^{2l}+q^l+1}} = Z_1^{q^{2l}+q^l+1} y_1 + Z_2^{q^{2l}+q^l+1} y_2 + \cdots + Z_n^{q^{2l}+q^l+1} y_n.$$

Moreover, define

$$S_Z = (S_{Z^{q^l}})^{\frac{1}{q^l}} = Z_1 y_1 + Z_2 y_2 + \cdots + Z_n y_n,$$

$$S_{Z^{q^{2l}}} = (S_{Z^{q^l}})^{q^l} = Z_1^{q^{2l}} y_1 + Z_2^{q^{2l}} y_2 + \cdots + Z_n^{q^{2l}} y_n,$$

$$S_{Z^{q^{2l}+1}} = (S_Z)^{q^{2l}+1} = Z_1^{q^{2l}+1} y_1 + Z_2^{q^{2l}+1} y_2 + \cdots + Z_n^{q^{2l}+1} y_n,$$

$$S_{Z^{q^{2l}+q^l}} = (S_{Z^{q^l+1}})^{q^l} = Z_1^{q^{2l}+q^l} y_1 + Z_2^{q^{2l}+q^l} y_2 + \cdots + Z_n^{q^{2l}+q^l} y_n.$$

We have two *syndrome matrices* as follows

$$\begin{pmatrix} S_1 & S_{Z^{q^l}} & S_{Z^{q^{2l}+q^l}} \\ S_Z & S_{Z^{q^l+1}} & S_{Z^{q^{2l}+q^l+1}} \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} S_1 & S_{Z^{q^l}} & S_{Z^{q^{2l}}} \\ S_Z & S_{Z^{q^l+1}} & S_{Z^{q^{2l}+1}} \end{pmatrix}.$$

If y is corrupted by two errors (ξ_i, Z_i) and (ξ_j, Z_j), where ξ_i and ξ_j are error values, Z_i and Z_j are the corresponding locators. Then we have

$$\begin{aligned}
S_1 &= \xi_i + \xi_j, \\
S_{Z^{q^l}} &= Z_i^{q^l} \xi_i + Z_j^{q^l} \xi_j, \\
S_{Z^{q^l+1}} &= Z_i^{q^l+1} \xi_i + Z_j^{q^l+1} \xi_j, \\
S_{Z^{q^{2l}+q^l+1}} &= Z_i^{q^{2l}+q^l+1} \xi_i + Z_j^{q^{2l}+q^l+1} \xi_j, \\
S_Z &= Z_i \xi_i + Z_j \xi_j, \\
S_{Z^{q^{2l}}} &= Z_i^{q^{2l}} \xi_i + Z_j^{q^{2l}} \xi_j, \\
S_{Z^{q^{2l}+1}} &= Z_i^{q^{2l}+1} \xi_i + Z_j^{q^{2l}+1} \xi_j, \\
S_{Z^{q^{2l}+q^l}} &= Z_i^{q^{2l}+q^l} \xi_i + Z_j^{q^{2l}+q^l} \xi_j.
\end{aligned}$$

The syndrome matrices can be decomposed into

$$\begin{pmatrix} S_1 & S_{Z^{q^l}} & S_{Z^{q^{2l}+q^l}} \\ S_Z & S_{Z^{q^l+1}} & S_{Z^{q^{2l}+q^l+1}} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ Z_i & Z_j \end{pmatrix} \begin{pmatrix} \xi_i & 0 \\ 0 & \xi_j \end{pmatrix} \begin{pmatrix} 1 & Z_i^{q^l} & Z_i^{q^{2l}+q^l} \\ 1 & Z_j^{q^l} & Z_j^{q^{2l}+q^l} \end{pmatrix} \tag{5.1}$$

and

$$\begin{pmatrix} S_1 & S_{Z^q} & S_{Z^{q^{2l}}} \\ S_Z & S_{Z^{q+1}} & S_{Z^{q^{2l}+1}} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ Z_i & Z_j \end{pmatrix} \begin{pmatrix} \xi_i & 0 \\ 0 & \xi_j \end{pmatrix} \begin{pmatrix} 1 & Z_i^{q^l} & Z_i^{q^{2l}} \\ 1 & Z_j^{q^l} & Z_j^{q^{2l}} \end{pmatrix}. \tag{5.2}$$

The three column vectors in the syndrome matrices must be linearly dependent over $GF(q^3)$. In fact we can find A, B, C and D in $GF(q^3)$, such that

$$\begin{pmatrix} S_{Z^{q^{2l}+q^l}} \\ S_{Z^{q^{2l}+q^l+1}} \end{pmatrix} + A \begin{pmatrix} S_{Z^{q^l}} \\ S_{Z^{q^l+1}} \end{pmatrix} + B \begin{pmatrix} S_1 \\ S_Z \end{pmatrix} = 0, \tag{5.3}$$

and

$$\begin{pmatrix} S_{Z^{q^{2l}}} \\ S_{Z^{q^{2l}+1}} \end{pmatrix} + C \begin{pmatrix} S_{Z^{q^l}} \\ S_{Z^{q^l+1}} \end{pmatrix} + D \begin{pmatrix} S_1 \\ S_Z \end{pmatrix} = 0. \tag{5.4}$$

So we have

$$\begin{pmatrix} Z_i^{q^{2l}+q^l} \\ Z_j^{q^{2L}+q^l} \end{pmatrix} + A \begin{pmatrix} Z_i^{q^l} \\ Z_j^{q^l} \end{pmatrix} + B \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 0, \tag{5.5}$$

and

$$\begin{pmatrix} Z_i^{q^{2l}} \\ Z_j^{q^{2l}} \end{pmatrix} + C \begin{pmatrix} Z_i^{q^l} \\ Z_j^{q^l} \end{pmatrix} + D \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 0. \tag{5.6}$$

If $x_1^{q^l} = x_2^{q^l}$, then $(x_1^{q^l})^{q^{m-l}} = (x_2^{q^l})^{q^{m-l}}$, i.e., $x_1^{q^m} = x_2^{q^m}$, but $x_1^{q^m} = x_1, x_2^{q^m} = x_2$, so $x_1 = x_2$. So we can take substitutions $Y_i = Z_i^{q^l}$ and $Y_j = Z_j^{q^l}$. Then by (5.5) and (5.6), Y_i, Y_j are the roots of the following equations

$$Y^{q^l+1} + AY + B = 0, \tag{5.7}$$

and

$$Y^{q^l} + CY + D = 0. \tag{5.8}$$

Multiply (5.8) by Y and then add it into (5.7), we have

$$CY^2 + (A + D)Y + B = 0. \tag{5.9}$$

If $C = 0$, then (5.8) has only one root, but $Y_i = Z_i^{q^l} \neq Y_j = Z_j^{q^l}$ are all its roots, so it is impossible. When $C \neq 0$, (5.9) is an equation of degree 2, it has two roots. Hence we can completely determine the error locators Z_i and Z_j. Then by (5.1) or (5.2), the error values are determined. The proof is completed. □

6 Conclusions

In the present paper, we constructed a class of codes with the parameters: $n = q^m$, $r \leq 2m + \lceil \frac{m}{3} \rceil + 1$, and $d \geq 5$ over $GF(q)$, where $q = 2^i$ or a power of an odd prime. It is well known that the codes over $GF(2^i)$ are very useful in computer semiconductor memory subsystems. The single-byte error-correcting and double-byte error-detecting codes, i.e., the codes with minimum distance ≥ 4 are thoroughly studied. There are many methods to construct the double-byte error-correcting codes, i.e., the codes with minimum distance ≥ 5. Dumer's codes are known to be optimal in the sense that no other double-byte error-correcting codes with the same code lengths have fewer number of parity checks, but his codes were defined on $GF(q)$ when q is odd. Our codes have the same parameters with Dumer's codes, but our codes are defined on $GF(2^i)$.

References

[1] T. R. N. Rao, E. Fujiwara, *Error-Control Coding for Computer Systems*, Prentice Hall, Englewood Cliffs, New Jersey, 1989.

[2] C. L. Chen, "Error-correcting codes with byte error-detection capablity", IEEE Transactions on Computers, Vol. C-32, No. 7(1983), 615-621.

[3] C. L. Chen, "Byte-oriented-correcting codes for semiconductor memory systems", IEEE Transactions on Computers, Vol. C-35, No. 7(1986), 646-648.

[4] C. L. Chen, "Error-correcting codes for byte-organized memory systems", IEEE Transactions on Information Theory, Vol. IT-32, No. 2(1986), 181-185.

[5] I. Dumer, "Nonbinary double-error-correcting codes designed by means of algebraic varieties", IEEE Trans. on Infor. Theory, Vol. IT-41, No. 6(1995), 1657-1666.

[6] G. L. Feng, T. R. N. Rao, G. A. Berg, "Generalized Bezout's thoerem and its applications in coding theory", submitted to IEEE Trans. on Infor. Theory.