Lower Bounds and Constructions for q-ary Codes Correcting Asymmetric Errors *

Qunying Liao** Liangjie Ye

Abstract: In this paper, we generalize some lower bounds, constructions and corresponding decoding algorithm from binary codes to the case q-ary codes. We show that some previously known bounds for binary asymmetric error-correcting codes can also be obtained for the generalization.
Keywords: Asymmetric error-correcting codes, code constructions, lower bounds, polynomials, decoding algorithm

1 Introduction

Binary error-correcting codes are usually designed for communication systems modeled by the binary-symmetric channel. However, in certain communication systems, such as optical communications and some computer memory systems, the error probability from 1 to 0 is significantly higher than the error probability from 0 to 1. These communication systems are modeled by the binary asymmetric channel(the Z-channel). Error correcting codes for the binary asymmetric channel have been studied since the 1950s. There are many papers dedicated to the construction of good codes and the derivation of lower and upper bounds for the symmetric error-correcting codes, see [1-17], and references therein. Klove[9] gave a unified account of error-correcting codes for the binary asymmetric channel.

For two binary n-tuples

$$\mathbf{x} = (x_1, \ldots, x_n) \text{ and } \mathbf{y} = (y_1, \ldots, y_n)$$

the asymmetric distance between $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$d_\alpha(\mathbf{x}, \mathbf{y}) = \max\{N(\mathbf{x}, \mathbf{y}), N(\mathbf{y}, \mathbf{x})\}$$

where

$$N(\mathbf{x}, \mathbf{y}) = \sharp\{i \,|\, x_i = 0 \text{ and } y_i = 1\}$$

For a binary code $\mathcal{C} \subseteq \{0,1\}^n$, the minimal asymmetric distance of $\mathcal{C}$ is defined as

$$\Delta(\mathcal{C}) = \min\{d_\alpha(\mathbf{x}, \mathbf{y}) \,|\, \mathbf{x}, \mathbf{y} \in \mathcal{C} \quad \text{and} \quad \mathbf{x} \neq \mathbf{y}\}$$

It was shown in [5] that a binary code $\mathcal{C} \in \{0,1\}^n$ can correct t or fewer asymmetric errors(1-errors) if and only if $\Delta(\mathcal{C}) \geq t+1$. A binary code of length n and minimum distance Δ is called a binary (n, Δ) asymmetric code. Let $\Gamma(n, \Delta)$ denote the maximum number of codewords in a binary code of length n and minimum distance Δ. One of the fundamental research problems in the theory of asymmetric error-correcting codes is to determine $\Gamma(n, \Delta)$ or give good lower and upper bounds.

* This research is supported by the National Science Foundation of China(No.A10990011), the Ph.D. Programs Foundation of Ministry of Education of China(No.20095134120001) and Scientific Research Fundation of the Education Department of Sichuan Province of China(No.09ZA087), Sichuan Provincial Advance Research Program for Excellent Youth Leaders of Disciplines in Science of China(No.2011JQ0037).

** Institute of Mathematics and Software Science, Sichuan Normal University, Chengdu, 610066, China. Email: liao_qunying@yahoo.com.cn

In 2002, Xing[17] gave a construction of binary constant-weight codes. The next year, by modifying the construction, Fu,*et al.*[8] presented a general construction for binary asymmetric error-correcting codes and first obtained a general lower bound on the sizes of these binary asymmetric error-correcting codes. They also proved that some new lower bounds for these asymmetric error-correcting codes improves the existing ones.

In the present paper, we generalize the construction for binary codes in [8] to the case q-ary codes and obtain the corresponding decoding algorithm some bounds for these q-ary asymmetric error-correcting codes.

2 The Generalized Construction and Decoding Algorithm

We first generalize the definition of the asymmetric distance from the binary asymmetric error-correcting code to the q-ary case,where q is a prime number.

Let $\mathbb{F}_q$ be the q elements finite field. For two q-ary n-tuples

$$\mathbf{x} = (x_1, \ldots, x_n) \quad \text{and} \quad \mathbf{y} = (y_1, \ldots, y_n)$$

the asymmetric distance between $\mathbf{x}$ and $\mathbf{y}$ is defined as

$$d_\alpha(\mathbf{x}, \mathbf{y}) = \max\{N(\mathbf{x}, \mathbf{y}), N(\mathbf{y}, \mathbf{x})\}$$

where

$$N(\mathbf{x}, \mathbf{y}) = \sum_{i=1, y_i > x_i}^{n} (y_i - x_i)$$

For a q-ary code $\mathcal{C} \subseteq \mathbb{F}_q^n$, the minimal asymmetric distance of $\mathcal{C}$ is defined as

$$\Delta(\mathcal{C}) = \min\{d_\alpha(\mathbf{x}, \mathbf{y}) \,|\, \mathbf{x}, \mathbf{y} \in \mathcal{C} \quad \text{and} \quad \mathbf{x} \neq \mathbf{y}\}$$

Remark 1 For the case $q = 2$, the above definition just is the asymmetric distance between two binary n-tuples $\mathbf{x}, \mathbf{y} \in \{0, 1\}^n$ defined in [8].

Now let $\mathbb{F}_t$ be the t elements finite field, where t is a prime power. For a monic polynomial $f(x) \in \mathbb{F}_t[x]$, it is well-known that in the isomorphic meaning, the residue class ring $R = \mathbb{F}_t[x]/(f(x))$ and its unite group $R^* = (\mathbb{F}_t[x]/(f(x)))^*$ can be viewed as

$$R = \{g(x) \in \mathbb{F}_t[x] \,|\, \deg g(x) < \deg f(x)\}$$

and

$$R^* = \{g(x) \in \mathbb{F}_t[x] \,|\, \deg g(x) < \deg f(x) \quad \text{and} \quad gcd(g(x), f(x)) = 1\}$$

The addition and multiplication operations over R are polynomial addition and multiplication modulo $f(x)$. It is obvious that $\mathbb{F}_t^*$ is a subgroup of R^*. This means that in the isomorphic meaning we can consider the quotient group $G = R^*/\mathbb{F}_t^*$ as the set of all monic polynomials of R^*, that is,

$$G = \{g(x) \in \mathbb{F}_t[x] \,|\, \deg g(x) < \deg f(x), \quad g(x) \text{ is monic and } \quad gcd(g(x), f(x)) = 1\}$$

In the following, we use the quotient group G to construct q-ary asymmetric error-correcting codes.

Construction Let n and d be positive integers satisfying $n \leq t$ and $2 \leq d < n$, where t is a prime power. Let $f(x) \in \mathbb{F}_t[x]$ be a monic polynomial with degree d such that there exist n distinct elements

$\alpha_1, \ldots, \alpha_n \in \mathbb{F}_t$ with $f(\alpha_i) \neq 0$. Then $(x - \alpha_i)$ is coprime to $f(x)$ for $i = 1, \ldots, n$. Hence $(x - \alpha_i) \in G$ for any $i = 1, \ldots, n$. Consider the map

$$\Omega : \ \mathbb{F}_q^n \longrightarrow \ G$$

$$(c_1, \ldots, c_n) \longmapsto \ \prod_{i=1}^{n} (x - \alpha_i)^{c_i} \in G$$

For every $g(x) \in G$, denote $\mathcal{C}_g = \Omega^{-1}(g(x))$. Then $\mathcal{C}_g$ is a q-ary $(n, \Delta \geq d)$ asymmetric error-correcting code for every $g(x) \in G$ such that $\mathcal{C}_g \neq \emptyset$. Since $|G| = \phi^*(f(x))$, there exists $g \in G$ such that $|\mathcal{C}_g| \geq \frac{q^n}{\phi^*(f(x))}$, where $\phi^*(f(x))$ is the Euler function for the polynomial $f(x) \in \mathbb{F}_t[x]$.

Furthermore, set $\Gamma(n, \Delta)$ to be the maximum number of codewords in a q-ary code of length n and minimum asymmetric distance Δ. Then $\Gamma(n, \Delta) \geq \max_{g \in G} |\mathcal{C}_g|$.

Proof of the Construction

For every $g(x) \in G$ such that $\mathcal{C}_g \neq \emptyset$, then it is sufficient to show that

$$d_\alpha(\mathbf{u}, \mathbf{v}) \geq d, \quad \mathbf{u}, \mathbf{v} \in \mathcal{C}_g \ \text{ and } \ \mathbf{u} \neq \mathbf{v}$$

Let $\mathbf{u} = (u_1, \ldots, u_n)$ and $\mathbf{v} = (v_1, \ldots, v_n)$, then

$$\Omega(\mathbf{u}) = \Omega(\mathbf{v}) = g(x) \in G$$

Thus the element $\Omega(\mathbf{u})/\Omega(\mathbf{v})$ is the identity in G. This means that

$$\frac{\Omega(\mathbf{u})}{\Omega(\mathbf{v})} = \frac{\prod_{i=1}^{n}(x - \alpha_i)^{u_i}}{\prod_{i=1}^{n}(x - \alpha_i)^{v_i}} = \beta \in R^*$$

Denote $S = \{i \,|\, u_i > v_i\}$, $T = \{i \,|\, v_i > u_i\}$, and $A(x) = \prod_{i \in S}(x - \alpha_i)^{(u_i - v_i)} - \beta \prod_{i \in T}(x - \alpha_i)^{(v_i - u_i)}$. Then $S \cap T = \emptyset$ and either $S \neq \emptyset$ or $T \neq \emptyset$ since $\mathbf{u} \neq \mathbf{v}$. Therefore

$$\{\alpha_i \,|\, i \in S\} \cap \{\alpha_i \,|\, i \in T\} = \emptyset$$

and either $S \neq \emptyset$ or $T \neq \emptyset$. Thus we have

$$f(x) | A(x) \in \mathbb{F}_t[x]$$

Which implies that

$$\deg f(x) \leq \deg A(x) \leq \max\{N(\mathbf{u}, \mathbf{v}), N(\mathbf{u}, \mathbf{v})\} = d_\alpha(\mathbf{u}, \mathbf{v})$$

This completes the proof. □

For every $g \in G$, if $C_g \neq \emptyset, C_g$ is a q-ary $(n, \Delta \geq d)$ asymmetric code. Hence, C_g can correct $d - 1$ or fewer asymmetric errors. Next we give a decoding algorithm for the q-ary asymmetric error-correcting code C_g.

Decoding Algorithm

For an arbitrary $g \in G$, suppose the codeword $c = (c_1, c_2, \cdots, c_n) \in C_g$ is transmitted and the vector $y = (y_1, y_2, \cdots, y_n) \in G$ is received. Calculate $R_y(x) = \prod_{i=0}^{n} (x - \alpha_i)^{y_i} \in G$.

(1) If $g(x) = R_y(x)$,thus y is the correct codeword.

(2) If $\frac{g(x)}{R_y(x)} \neq 1$, assume y has s errors, $i_1, i_2, \cdots, i_s$, respectively, and $1 \leq s \leq n$, $1 \leq i_1 < i_2 < \cdots < i_s \leq n$. Then by properties of the asymmetric code, we have

$$\frac{g(x)}{R_y(x)} = (x-\alpha_{i_1})^{b_{i_1}}(x-\alpha_{i_2})^{b_{i_2}}\cdots(x-\alpha_{i_s})^{b_{i_s}} \quad (1 \leq |b_j| \leq |q|, j = i_1, i_2, \cdots, i_s)$$

Hence the decoding is accomplished by $c_j = y_j + b_j, j = i_1, i_2, \cdots, i_s$.

(3) Otherwise, the decoding is considered to be failed.

Proof According to the above construction, we know that for each word $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$, there exists unique polynomial $\prod_{i=1}^n (x-\alpha_i)^{c_i} \in \mathbb{F}_t^*[x]$.

Now suppose that we send a codeword $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$, and receive the word $\mathbf{y} = (y_1, \ldots, y_n)$. This means that we have a polynomial $\prod_{i=1}^n (x-\alpha_i)^{y_i} \in \mathbb{F}_t^*[x]$. Hence there is no errors if and only if $\mathbf{y} = c$, i.e., $c_i = y_i$ for any $i = 1, \ldots, n$. This is true if and only if $g(x) = R_y(x)$. Thus we complete the proof of the case (1).

Otherwise, there is errors and so $\frac{g(x)}{R_y(x)} \neq 1$. Namely we have

$$E(x) = \frac{g(x)}{R_y(x)} = \frac{\prod_{i=0}^n (x-\alpha_i)^{c_i}}{\prod_{i=0}^n (x-\alpha_i)^{y_i}} = \prod_{i=0}^n (x-\alpha_i)^{c_i - y_i}, \quad 0 \leq |c_i - y_i| \leq q, 1 \leq i \leq n$$

With $m_i = c_i - y_i \neq 0$ for some $i = i_1, \ldots, i_s (1 \leq s \leq n)$. Hence by decoding $c_i = y_i + m_i (0 \leq i \leq n)$ we can get the codeword $c = (c_1, \ldots, c_n)$.

Hence we complete the proof of the decoding algorithm. □

Remark 2 (i) By taking $q = 2$ in the above construction, one can get the construction for binary asymmetric error-correcting codes obtained in [8].

(ii) Since the error probability from 1 to 0 is significantly higher than the error probability from 0 to 1, so by taking $q = 2$ in the above decoding algorithm, one can show that $b_j = 1 (j = i_1, i_2, \cdots, i_s)$ and so obtain the corresponding algorithm in [8].

3 Lower Bounds

Several lower bounds for binary error-correcting codes were obtained by a discussion of Varshamov's constructions and their generalizations(see [6] and [8]). In this section, in the same proof as those for the corresponding results in [8], we show that these previously known lower bounds for binary asymmetric error-correcting codes can also be obtained for our general construction.

Theorem 1 (1) If n is a prime power, then for $d \geq 2$,

$$\Gamma(n,d) \geq \frac{q^n}{n^{d-1} + n^{d-2} + \ldots + d + 1}$$

(2) If $n+1$ is a prime power, then for $d \geq 3$,

$$\Gamma(n,d) \geq \frac{q^n}{(n+1)^{d-1} - 1}$$

(3) If t is the least prime power satisfying $t \geq n+2$, then for $d \geq 3$,

$$\Gamma(n,d) \geq \frac{q^n}{t^{d-1} - t^{d-2}}$$

Theorem 2 If n is a prime power and $2 \leq d \leq n$, then

$$\Gamma(n,d) \geq \frac{(n-1)q^n}{(n^2-1)^r (n^3-1)^s}$$

where r and s are the two unique nonnegative integers satisfying $d = 2r + 3s$ and $s \in \{0, 1\}$.

(2) If n is not a prime power, denote m as the least positive integer such that $t = n + m$ is a prime power. If $2 \leq d \leq m$, then

$$\Gamma(n, d) \geq \frac{q^n}{(t-1)^{d-1}}$$

If $d > m$, then

$$\Gamma(n, d) \geq \frac{q^n}{(t-1)^{m-1} t^{s'} (t^2-1)^{r'}}$$

where r' and s' are the two unique nonnegative integers satisfying $d - m = 2r' + s'$ and $s' \in \{0, 1\}$.

Corollary 1 If $n + 1$ is a prime power, then for $d \geq 2$,

$$\Gamma(n, d) \geq \frac{q^n}{((n+1)^s [(n+1)^2 - 1]^r}$$

where r and s are the two unique nonnegative integers satisfying $d - 1 = 2r + s$ and $s \in \{0, 1\}$.

Corollary 2 If $n + 2$ is prime power, then for $d \geq 3$,

$$\Gamma(n, d) \geq \frac{q^n}{((n+1)(n+2)^s [(n+1)^2 - 1]^r}$$

where r and s are the two unique nonnegative integers satisfying $d - 2 = 2r + s$ and $s \in \{0, 1\}$.

Remark 3 (1) By taking $q = 2$ in Theorems 1-2 and corollaries 1-2, one can get the corresponding lower bounds given in [8].

(2) By the similar proof for the corresponding results as that in [8], the remained results for binary asymmetric codes in [8] can be generalized to the case q-ary just replacing 2^n to be q^n in all equations (12-20).

References

[1] K.A.S, Abdel-Ghaffar and H.C. Ferreira, Systematic encoding of the Varshamov-Tenengol'ts codes and the Constantin-Rao codes, IEEE.Trans.Inform.Theory, 1998, 44: 340-345.

[2] S.Al-Bassam and B. Bose, Asymmetric/unidirectional error correcting and detecting codes, IEEE. Trans.Comput., 1994, 43: 590-597.

[3] S.Al-Bassam, R.Venkatesan, and S.Al-Muhammadi, New single asymmetric error-correcting codes, IEEE.Trans.Inform.Theory, 1997, 43: 1619-1623.

[4] B.Bose and S.Al-Bassam, On systematic single asymmetric error-correcting codes, IEEE.Trans.Inform.Theory, 2000, 46: 669-672.

[5] T.R.N.Rao and A.S.Chawla, Asymmetric error codes for some lsisemi-conductor memories, in Proc. Annu.Southeastern Symp.Systems Theory, 1975: 170-171.

[6] S.D.Constantin and T.R.N.Rao, On the theroy of binary asymmetric error-correcting codes, Inform.Contr., 1979, 40: 20-36.

[7] G.Fang and H.C.A.van Tilborg, Bounds and constructions of asymmetric or unidirectional error-correcting codes, Appl.Algebra Engrg.Comm.Comput.,1992, 3(4):269-300.

[8] F.W.Fu, S.Ling, and C.P.Xing, New lower bounds and constructions for binary codes correcting asmmetric errors, IEEE.Trans.Inform.Theory, 2003, 49(12): 3294-3299.

[9] T.Klove, Error correcting codes fro the asymmetric channel, Dept.Mathematics, Univ. Bergen, Bergen, Norway, Tech.Rep.18-09-07-81,1995.

[10] R.J.McEliece and E.R.Rodemich, The Constantin-Rao construction for asymmetric error-correcting codes, Inform.Contr., 1980, 44:187-196.

[11] T.R.N.Rao and E.Fujiwara, Error-Control Coding for Computer Systems, Englewood Cliffs, NJ: Prentic-Hall, 1989.

[12] J.P.Robinson, An asymmetric error-coreccting tenary code, IEEE.Trans.Inform.Theory, 1978, IT-24: 258-261.

[13] Y.Saitoh, K.Yamaguchi, and H. imai, Some new binary codes correcting asymmetric /unidirectional errors, IEEE.Trans.Inform.Theory, 1990, 36: 645-647.

[14] A.Shiozaki,Construction for binary asymmetric error-correcting codes, IEEE.Trans. Inform.Theory, 1982, IT-28: 787-789.

[15] R.P.Stanley and M.F.Yoder, A study of Varshamove codes for asymmetric channels, Jet Propulsion Lab., Tech, Rep, 1973, 14: 32-1526.

[16] J.Weber, C.de Vroedt, and D.Boekee, New upper bounds on the size of codes correcting asymmetric errors, IEEE.Trans.Inform.Theory, 1987, IT-33: 434-437.

[17] C.P.Xing, Constrcution of codes from residue rings of polynomials, IEEE.Trans.Inform. Theory, 2002, 48: 2995-2997.

[18] Z.Zhang and X.Xia, New lower bounds for binary codes of asymmetric distance two, IEEE.Trans. Inform.Theory, 1992, 38: 1592-1597.