# New lower bounds and constructions for binary codes correcting asymmetric errors

Fu, Fang-Wei; Ling, San; Xing, Chaoping

2003

Fu, F.-W., Ling, S., & Xing, C. (2003). New lower bounds and constructions for binary codes correcting asymmetric errors. IEEE Transactions on Information Theory, 49(12), 3294-3299.

https://hdl.handle.net/10356/79953

https://doi.org/10.1109/TIT.2003.820028

# New Lower Bounds and Constructions for Binary Codes Correcting Asymmetric Errors

Fang-Wei Fu, San Ling, and Chaoping Xing

***Abstract*—In this correspondence, we study binary asymmetric error-correcting codes. A general construction for binary asymmetric error-correcting codes is presented. We show that some previously known lower bounds for binary asymmetric error-correcting codes can be obtained from this general construction. Furthermore, some new lower bounds for binary asymmetric error-correcting codes are obtained from this general construction. These new lower bounds improve the existing ones.**

***Index Terms*—Asymmetric error-correcting codes, code construction, lower bounds, polynomials.**

## I. 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 a number of papers dedicated to the construction of good codes and the derivation of lower and upper bounds for the asymmetric error-correcting codes, see [1]–[33], [35], and references therein. Kløve [19] gave a unified account of error-correcting codes for the binary asymmetric channel.

For two binary $n$-tuples

$$\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \quad \text{and} \quad \boldsymbol{y} = (y_1, y_2, \ldots, y_n)$$

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

$$d_a(\boldsymbol{x}, \boldsymbol{y}) = \max\{N(\boldsymbol{x}, \boldsymbol{y}), N(\boldsymbol{y}, \boldsymbol{x})\}$$

where

$$N(\boldsymbol{x}, \boldsymbol{y}) = |\{i : \ x_i = 0 \text{ and } y_i = 1\}| .$$

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

$$\Delta(C) = \min\{d_a(\boldsymbol{x}, \boldsymbol{y}) : \ \boldsymbol{x}, \boldsymbol{y} \in C \text{ and } \boldsymbol{x} \neq \boldsymbol{y}\}.$$

F.-W. Fu is with the Temasek Laboratories, National University of Singapore, Singapore 119260, Republic of Singapore, on leave from the Department of Mathematics, Nankai University, Tianjin 300071, China (e-mail: tslfufw@nus.edu.sg).

S. Ling is with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore (e-mail: matlings@nus.edu.sg).

C. Xing is with the Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore, and the Department of Mathematics, University of Science and Technology of China, Hefei, Anhui 230026, China (e-mail: matxcp@nus.edu.sg).

Communicated by S. Litsyn, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2003.820028

It was shown in [24] that a binary code $C$ can correct $t$ or fewer asymmetric errors (1-errors) if and only if $\Delta(C) \geq t+1$. A binary code of length $n$ and minimum asymmetric distance $\Delta$ is called a binary $(n, \Delta)$ asymmetric code. Let $\Gamma(n, \Delta)$ denote the maximum number of codewords in a binary code of length $n$ and minimum asymmetric distance $\Delta$. 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.

In this correspondence, we give a general construction and some new lower bounds for binary asymmetric error-correcting codes. This correspondence is organized as follows. In Section II, we present a general construction for binary asymmetric error-correcting codes by modifying Xing's construction of binary constant-weight codes (see [34]). In Section III, we first give a general lower bound on the sizes of the binary asymmetric error-correcting codes constructed in Section II. Then, we show that some previously known lower bounds for binary asymmetric error-correcting codes can be obtained from this general construction. Furthermore, some new lower bounds for binary asymmetric error-correcting codes are obtained from this general construction. These new lower bounds improve the existing ones.

## II. A General Construction

Xing [34] gave a construction of binary constant-weight codes. By modifying his method, we present a general construction for binary asymmetric error-correcting codes.

Let $\boldsymbol{F}_q$ be a finite field of $q$ elements, where $q$ is a prime power. For a monic polynomial $f(x) \in \boldsymbol{F}_q[x]$, consider the residue class ring

$$R = \boldsymbol{F}_q[x]/(f(x)).$$

Actually, in the isomorphic meaning, here we can consider the residue class ring $R$ as

$$R = \{g(x) \in \boldsymbol{F}_q[x] : \ \deg(g(x)) < \deg(f(x))\}.$$

The addition and multiplication operations over $R$ are the polynomial addition and multiplication modulo $f(x)$.

Let $f(x)$ have the factorization

$$f(x) = \prod_{i=1}^{k} p_i^{e_i}(x)$$

where $p_1(x), \ldots, p_k(x)$ are distinct monic irreducible polynomials in $\boldsymbol{F}_q[x]$ and $e_1, \ldots, e_k$ are positive integers. It is known that all invertible polynomials of the ring $R$ form a multiplicative group, denoted by

$$R^* = (\boldsymbol{F}_q[x]/(f(x)))^*.$$

It is a finite Abelian group and consists of all polynomials in $R$ which are co-prime to $f(x)$, that is,

$$R^* = \{g(x) \in \boldsymbol{F}_q[x] : \quad \deg(g(x)) < \deg(f(x)) \text{ and } (g(x), f(x)) = 1\}. \quad (1)$$

The multiplication operation $\bigodot$ over $R^*$ is the polynomial multiplication modulo $f(x)$. Hence, this group contains exactly

$$\Phi(f(x)) \triangleq \prod_{i=1}^{k} (q^{d_i} - 1) q^{d_i(e_i - 1)}$$

elements, where $d_i$ is the degree of $p_i(x)$. It is obvious that the set $\boldsymbol{F}_q^*$ of all nonzero elements of $\boldsymbol{F}_q$ is a subgroup of $R^*$. The quotient group

$$G = R^*/\boldsymbol{F}_q^*$$

is a finite Abelian group with

$$\Phi^*(f(x)) \triangleq \frac{1}{(q-1)}\Phi(f(x)) = \frac{1}{(q-1)}\prod_{i=1}^{k}(q^{d_i}-1)q^{d_i(e_i-1)}$$

elements. Actually, in the isomorphic meaning, here we can consider $G$ as the set of all monic polynomials of $R^*$, that is,

$$G = \{g(x) \in \boldsymbol{F}_q[x] : \quad \deg(g(x)) < \deg(f(x)),\ g(x) \text{ is monic, and } (g(x), f(x)) = 1\}. \quad (2)$$

The multiplication operation $\bigotimes$ over $G$ is given by

$$a(x) \bigotimes b(x) = M\left(a(x) \bigodot b(x)\right)$$

where

$$M(h(x)) = h_m^{-1}h(x)$$

for

$$h(x) = h_m x^m + h_{m-1}x^{m-1} + \cdots + h_1 x + h_0 \in \boldsymbol{F}_q[x].$$

Here $h_m \neq 0$ is the leading coefficient of $h(x)$.

In the following, we use the quotient group $G$ to construct binary asymmetric error-correcting codes. For simplicity, we assume that the finite Abelian groups $(R^*, \bigodot)$ and $(G, \bigotimes)$ are given by (1) and (2), respectively.

*Construction:* Let $n$ and $d$ be two positive integers satisfying $n \leq q$ and $2 \leq d < n$. Let $f(x) \in \boldsymbol{F}_q[x]$ be a monic polynomial of degree $d$ such that there exist $n$ distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in \boldsymbol{F}_q$ with $f(\alpha_i) \neq 0$ for all $i = 1, 2, \ldots, n$. Then $(x - \alpha_i)$ is co-prime to $f(x)$ for $i = 1, 2, \ldots, n$. Hence,

$$(x - \alpha_i) \in G, \qquad i = 1, 2, \ldots, n.$$

Consider the map

$$\Omega : \{0,1\}^n \to G$$
$$(c_1, c_2, \ldots, c_n) \mapsto \prod_{i=1}^{n} \bigotimes (x - \alpha_i)^{c_i} \in G.$$

For every $g(x) \in G$, denote

$$C_g = \Omega^{-1}(g(x)).$$

For every $g \in G$, if $C_g \neq \emptyset$, then $C_g$ is a binary $(n, \Delta \geq d)$ asymmetric code.

*Proof of the Construction:* For every $g \in G$, if $C_g \neq \emptyset$, we want to show that

$$d_a(\boldsymbol{u}, \boldsymbol{v}) \geq d, \qquad \boldsymbol{u}, \boldsymbol{v} \in C_g \text{ and } \boldsymbol{u} \neq \boldsymbol{v}.$$

Let $\boldsymbol{u} = (u_1, u_2, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$. Then

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

Hence, the element $\Omega(\boldsymbol{u})/\Omega(\boldsymbol{v})$ is the identity in $G$. This implies that in the group $R^*$, the element

$$\frac{\Omega(\boldsymbol{u})}{\Omega(\boldsymbol{v})} = \frac{\prod_{i=1}^{n} \bigodot (x - \alpha_i)^{u_i}}{\prod_{i=1}^{n} \bigodot (x - \alpha_i)^{v_i}}$$

is equal to a nonzero element $\beta$ of $\boldsymbol{F}_q^*$. Denote

$$S = \{i : \ u_i = 0 \text{ and } v_i = 1\}$$

and

$$T = \{i : \ u_i = 1 \text{ and } v_i = 0\}.$$

Then $S \bigcap T = \emptyset$, and either $S \neq \emptyset$ or $T \neq \emptyset$ since $\boldsymbol{u} \neq \boldsymbol{v}$. Furthermore

$$|\ S\ | = N(\boldsymbol{u}, \boldsymbol{v}), \quad |\ T\ | = N(\boldsymbol{v}, \boldsymbol{u}).$$

It is easy to see that

$$\frac{\Omega(\boldsymbol{u})}{\Omega(\boldsymbol{v})} = \frac{\prod_{i \in T} \bigodot (x - \alpha_i)}{\prod_{j \in S} \bigodot (x - \alpha_j)} = \beta$$

in the group $R^*$. This is equivalent to the fact that $f(x)$ divides the polynomial

$$A(x) \triangleq \prod_{i \in T}(x - \alpha_i) - \beta \prod_{i \in S}(x - \alpha_i) \in \boldsymbol{F}_q[x].$$

The roots of the polynomial $\prod_{i \in T}(x - \alpha_i)$ are $\alpha_i, i \in T$, and the roots of the polynomial $\beta \prod_{i \in S}(x - \alpha_i)$ are $\alpha_i, i \in S$. Since

$$\{\alpha_i : i \in S\} \bigcap \{\alpha_i : i \in T\} = \emptyset$$

and either $S \neq \emptyset$ or $T \neq \emptyset$, we have

$$\prod_{i \in T}(x - \alpha_i) \neq \beta \prod_{i \in S}(x - \alpha_i).$$

Hence, $A(x) \neq 0$ and the degree of $A(x)$ is at most

$$\max\{|\ S\ |, |\ T\ |\} = d_a(\boldsymbol{u}, \boldsymbol{v}).$$

Therefore,

$$d_a(\boldsymbol{u}, \boldsymbol{v}) \geq \deg(f(x)) = d.$$

This completes the proof. □

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

*Decoding Algorithm:* Assume that the received vector is

$$\boldsymbol{y} = (y_1, y_2, \ldots, y_n) \in \{0,1\}^n.$$

Calculate

$$R_{\boldsymbol{y}}(x) = \prod_{i=1}^{n} \bigotimes (x - \alpha_i)^{y_i} \in G$$

and

$$E(x) = \frac{g(x)}{R_{\boldsymbol{y}}(x)} \in G \qquad (\text{since } g \in G).$$

To find the polynomial $E(x)$, we can use the Euclidean algorithm. Denote $l = \deg(E(x))$.

i) If $l = 0$, that is, $E(x) = 1$, then decode $\boldsymbol{y}$ into $\boldsymbol{y}$.

ii) If $0 < l \le d-1$ and $E(x)$ has $l$ distinct roots $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_l}$, then decode $\boldsymbol{y}$ into $\boldsymbol{c} = (c_1, c_2, \ldots, c_n)$ where

$$c_j = \begin{cases} y_j, & j \neq i_1, i_2, \ldots, i_l \\ y_j \oplus 1, & j = i_1, i_2, \ldots, i_l. \end{cases}$$

iii) Otherwise, we declare that the decoding has failed.

*Proof of the Decoding Algorithm:* Suppose the codeword $\boldsymbol{c} = (c_1, c_2, \ldots, c_n)$ is transmitted. Assume that errors occur in positions $i_1, i_2, \ldots, i_l$ where $0 \le l \le d-1$ and $1 \le i_1 < i_2 < \cdots < i_l \le n$. Then the received vector $\boldsymbol{y}$ is given by $\boldsymbol{y} = \boldsymbol{c}$ for $l = 0$ and $\boldsymbol{y} = (y_1, y_2, \ldots, y_n)$ for $1 \le l \le d-1$ where

$$\begin{aligned} y_j &= c_j, && \text{for } j \neq i_1, i_2, \ldots, i_l \\ y_j &= 0 \text{ and } c_j = 1, && \text{for } j = i_1, i_2, \ldots, i_l. \end{aligned}$$

Hence, if $l = 0$, then

$$R_{\boldsymbol{y}}(x) = R_{\boldsymbol{c}}(x) = \prod_{j=1}^{n} \bigotimes (x - \alpha_j)^{c_j} = g(x) \in G$$

and $E(x) = 1$.

If $1 \le l \le d-1$, by the fact that $c_j = 1$ for $j = i_1, i_2, \ldots, i_l$, we have

$$R_{\boldsymbol{y}}(x) = \prod_{j=1}^{n} \bigotimes (x - \alpha_j)^{y_j} = \prod_{j \neq i_1, i_2, \ldots, i_l} \bigotimes (x - \alpha_j)^{c_j}$$

and

$$E(x) = \frac{g(x)}{R_{\boldsymbol{y}}(x)} = (x - \alpha_{i_1})(x - \alpha_{i_2}) \cdots (x - \alpha_{i_l}).$$

Hence, $E(x)$ has $l$ distinct roots $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_l}$. Therefore, we decode $\boldsymbol{y}$ into $\boldsymbol{c}$. This completes the proof. □

## III. New Lower Bounds

From the general construction in Section II, we know that $C_g,\ g \in G$ form a partition of $\{0,1\}^n$. Since $|\ G\ | = \Phi^*(f(x))$, we can find one element $\pi(x) \in G$ such that

$$|\ C_\pi\ | \ge \frac{2^n}{\Phi^*(f(x))}.$$

Hence, we obtain the following result.

*Theorem 1:* Let $\boldsymbol{F}_q$ be a finite field of $q$ elements, where $q$ is a prime power. Let $n$ and $d$ be two positive integers satisfying $n \le q$ and $2 \le d < n$. Let $f(x) \in \boldsymbol{F}_q[x]$ be a monic polynomial of degree $d$ such that there exist $n$ distinct elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in \boldsymbol{F}_q$ with $f(\alpha_i) \neq 0$ for all $i = 1, 2, \ldots, n$. Then there exists a binary $(n, \Delta \ge d)$ asymmetric code $C$ with size

$$|\ C\ | \ge \frac{2^n}{\Phi^*(f(x))}. \quad (3)$$

From the general construction in Section II, it is easy to see the following.

*Corollary 1:* With notations as in Section II, we have

$$\Gamma(n, \Delta) \ge \max\nolimits_{g \in G} |\ C_g\ |. \quad (4)$$

Bound (4) is in general stronger than bound (3), but it is less explicit and requires more computation to determine.

Several lower bounds for binary asymmetric error-correcting codes were obtained by a discussion of Varshamov's constructions and their generalizations (see [17, Theorem 6.1] and [11], [12], [17], [29], and [31]). In this section, we first show that these previously known lower bounds for binary asymmetric error-correcting codes can also be obtained from our general construction and Theorem 1. Furthermore, some new lower bounds for binary asymmetric error-correcting codes are obtained from Theorem 1. These new lower bounds improve on the existing ones.

*Theorem 2:* (see [19, Theorem 6.1])

i) If $n$ is a prime power, then for $d \ge 2$

$$\Gamma(n, d) \ge \frac{2^n}{n^{d-1} + n^{d-2} + \cdots + n + 1}. \quad (5)$$

ii) If $n+1$ is a prime power, then for $d \ge 3$

$$\Gamma(n, d) \ge \frac{2^n}{(n+1)^{d-1} - 1}. \quad (6)$$

iii) If $q$ is the least prime power satisfying $q \ge n+2$, then for $d \ge 3$

$$\Gamma(n, d) \ge \frac{2^n}{q^{d-1} - q^{d-2}}. \quad (7)$$

*Proof:*

i) Let $q = n$ in Theorem 1 since $n$ is a prime power. Let

$$\boldsymbol{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}$$

and let $f(x) \in \boldsymbol{F}_q[x]$ be a monic irreducible polynomial of degree $d$ $(d \ge 2)$. Then

$$\Phi(f(x)) = q^d - 1$$

and

$$\Phi^*(f(x)) = \frac{q^d - 1}{q - 1} = n^{d-1} + n^{d-2} + \cdots + n + 1.$$

It is easy to see that $f(\alpha_i) \neq 0$ for all $i = 1, 2, \ldots, n$ since $f(x)$ is a monic irreducible polynomial of degree $d$ $(d \ge 2)$. Hence, (5) follows from Theorem 1.

ii) Let $q = n+1$ in Theorem 1 since $n+1$ is a prime power. Let

$$\boldsymbol{F}_q = \{0, \alpha_1, \alpha_2, \ldots, \alpha_n\}$$

and let $f(x) = x f_1(x)$ where $f_1(x) \in \boldsymbol{F}_q[x]$ is a monic irreducible polynomial of degree $d-1$. Then

$$\Phi(f(x)) = (q-1)(q^{d-1} - 1)$$

and

$$\Phi^*(f(x)) = q^{d-1} - 1 = (n+1)^{d-1} - 1.$$

It is easy to see that $f(\alpha_i) \neq 0$ for all $i = 1, 2, \ldots, n$ since $\alpha_i \in \boldsymbol{F}_q^*$ and $f_1(x)$ is a monic irreducible polynomial with degree $d - 1 \ge 2$. Hence, (6) follows from Theorem 1.

iii) Since $q$ is the least prime power satisfying $q \ge n+2$, we can assume in Theorem 1 that

$$\boldsymbol{F}_q = \{0, 1, \alpha_1, \alpha_2, \ldots, \alpha_n, \ldots\}.$$

Let $f(x) = x(x-1)^{d-1}$. Then

$$\Phi(f(x)) = (q-1)^2 q^{d-2}$$

and

$$\Phi^*(f(x)) = (q-1)q^{d-2} = q^{d-1} - q^{d-2}.$$

It is easy to see that $f(\alpha_i) \neq 0$ for all $i = 1, 2, \ldots, n$. Hence, (7) follows from Theorem 1. □

*Remark 1:* As pointed out by one referee, Bose and Cunningham [9] presented a construction of binary asymmetric error-correcting codes if $n+1$ is a prime power. This construction yields the following lower bound:

$$\Gamma(n,d) \geq \frac{2^n}{(n+1)^{d-1}}. \tag{8}$$

Note that bound (8) is slightly worse than bound (6). The referee observed that after redescribing the construction of Bose and Cunningham [9] in polynomial form it is somewhat similar to our construction here. We note that the construction of Bose and Cunningham is actually a special case of our general construction by taking $f(x) = x^d$ in the proof of Theorem 2 ii). Bound (8) follows from Theorem 1 by noting that $\Phi(x^d) = (q-1)q^{d-1}$ and $\Phi^*(x^d) = q^{d-1} = (n+1)^{d-1}$.

In the following theorem, we show that the lower bounds given by Theorem 2 can be generalized and improved by using Theorem 1. Note that the number of monic quadratic irreducible polynomials in $\boldsymbol{F}_q[x]$ is $q(q-1)/2$.

*Theorem 3:*

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

$$\Gamma(n,d) \geq \frac{(n-1)2^n}{(n^2-1)^r(n^3-1)^s} \tag{9}$$

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

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

$$\Gamma(n,d) \geq \frac{2^n}{(q-1)^{d-1}}. \tag{10}$$

If $d > m$, then

$$\Gamma(n,d) \geq \frac{2^n}{(q-1)^{m-1}q^{s'}(q^2-1)^{r'}} \tag{11}$$

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

*Proof:*

i) Let $q = n$ in Theorem 1 since $n$ is a prime power. Let

$$\boldsymbol{F}_q = \{\alpha_1, \alpha_2, \ldots, \alpha_q\}.$$

Since

$$r \leq \frac{d}{2} \leq \frac{n}{2} = \frac{q}{2} \leq \frac{q(q-1)}{2}$$

we can choose distinct monic quadratic irreducible polynomials

$$p_1(x), p_2(x), \ldots, p_r(x)$$

in $\boldsymbol{F}_q[x]$ and a monic cubic irreducible polynomials $p(x)$ in $\boldsymbol{F}_q[x]$. Let

$$f(x) = p^s(x)\prod_{i=1}^{r} p_i(x).$$

Then $\deg(f(x)) = d$ and

$$\Phi(f(x)) = (q^2-1)^r(q^3-1)^s$$

$$\Phi^*(f(x)) = \frac{(q^2-1)^r(q^3-1)^s}{q-1} = \frac{(n^2-1)^r(n^3-1)^s}{n-1}.$$

It is easy to see that $f(\alpha_i) \neq 0$ for all $i = 1, 2, \ldots, n$. Hence, by Theorem 1

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

ii) In Theorem 1, let

$$\boldsymbol{F}_q = \{\beta_1, \beta_2, \ldots, \beta_m, \alpha_1, \alpha_2, \ldots, \alpha_n\}.$$

If $2 \leq d \leq m$, let

$$f(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_d).$$

Then

$$\Phi(f(x)) = (q-1)^d, \qquad \Phi^*(f(x)) = (q-1)^{d-1}.$$

If $d > m$, by the fact that $d - m = 2r' + s'$, we have

$$r' \leq \frac{d}{2} \leq \frac{n}{2} \leq \frac{q}{2} \leq \frac{q(q-1)}{2}.$$

Hence, we can choose distinct monic quadratic irreducible polynomials

$$p_1(x), p_2(x), \ldots, p_{r'}(x)$$

in $\boldsymbol{F}_q[x]$. Let

$$f(x) = (x-\beta_1)^{1+s'}(x-\beta_2)\cdots(x-\beta_m)\prod_{i=1}^{r'} p_i(x).$$

Then $\deg(f(x)) = d$ and

$$\Phi(f(x)) = (q-1)^m q^{s'}(q^2-1)^{r'}$$

$$\Phi^*(f(x)) = (q-1)^{m-1} q^{s'}(q^2-1)^{r'}.$$

It is easy to see that $f(\alpha_i) \neq 0$ for all $i = 1, 2, \ldots, n$. Hence, by Theorem 1, we obtain (10) and (11). □

The lower bound (9) in Theorem 3 is better than the lower bound (5) in Theorem 2. Note that for $d \geq 2$

$$(n^2-1)^r(n^3-1)^s \leq n^{2r+3s} - 1 = n^d - 1$$

and the equality holds if and only if $d = 2$ or $3$. Hence, for $d \geq 2$

$$\frac{(n^2-1)^r(n^3-1)^s}{n-1} \leq n^{d-1} + n^{d-2} + \cdots + n + 1$$

and the equality holds if and only if $d = 2$ or $3$.

The lower bound (9) in Theorem 3 can be rewritten in the following form. If $n$ is a prime power, then

$$\Gamma(n,d) \geq \frac{(n-1)2^n}{(n^2-1)^{\frac{d}{2}}}, \qquad d \text{ even and } d \geq 2 \tag{12}$$

$$\Gamma(n,d) \geq \frac{(n-1)2^n}{(n^2-1)^{\frac{(d-3)}{2}}(n^3-1)}, \qquad d \text{ odd and } d \geq 3. \tag{13}$$

For two sequences $\{g(n)\}_{n=1}^{\infty}$ and $\{h(n)\}_{n=1}^{\infty}$, we say

$$g(n) = O(h(n)), \qquad \text{if } \lim_{n\to\infty}\frac{g(n)}{h(n)} = 1.$$

By direct computation, it is not hard to see that

$$\text{Bound (12)} - \text{Bound (5)} = O\left(\frac{d2^{n-1}}{n^{d+1}}\right), \qquad d \text{ even and } d \geq 4$$

$$\text{Bound (13)} - \text{Bound (5)} = O\left(\frac{(d-3)2^{n-1}}{n^{d+1}}\right), \qquad d \text{ odd and } d \geq 5.$$

Let $m = 1$ in Theorem 3 ii), then we obtain the following.

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

$$\Gamma(n,d) \geq \frac{2^n}{(n+1)^s[(n+1)^2-1]^r} \tag{14}$$

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

The lower bound (14) in Corollary 2 is better than the lower bound (6) in Theorem 2. Note that for $d \geq 3$

$$(n+1)^s[(n+1)^2 - 1]^r \leq (n+1)^{2r+s} - 1 = (n+1)^{d-1} - 1$$

and the equality holds if and only if $d = 3$.

The lower bound (14) in Corollary 2 can be rewritten in the following form. If $n + 1$ is a prime power, then

$$\Gamma(n,d) \geq \frac{2^n}{(n+1)[(n+1)^2-1]^{\frac{(d-2)}{2}}}, \quad d \text{ even and } d \geq 2 \quad (15)$$

$$\Gamma(n,d) \geq \frac{2^n}{[(n+1)^2-1]^{\frac{(d-1)}{2}}}, \quad d \text{ odd and } d \geq 3. \quad (16)$$

By direct computation, it is not hard to see that

$$\text{Bound (15)} - \text{Bound (6)} = O\left(\frac{(d-2)2^{n-1}}{n^{d+1}}\right), \quad d \text{ even and } d \geq 4$$

$$\text{Bound (16)} - \text{Bound (6)} = O\left(\frac{(d-1)2^{n-1}}{n^{d+1}}\right), \quad d \text{ odd and } d \geq 5.$$

Let $m = 2$ in Theorem 3 ii), then we obtain the following.

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

$$\Gamma(n,d) \geq \frac{2^n}{(n+1)(n+2)^s[(n+2)^2-1]^r} \quad (17)$$

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

The lower bound (17) in Corollary 3 is better than the lower bound (7) in Theorem 2. Note that for $d \geq 3$ and $q = n + 2$

$$q^s(q^2-1)^r \leq q^{2r+s} = q^{d-2}$$

and the equality holds if and only if $d = 3$. Hence, for $d \geq 3$

$$(q-1)q^s(q^2-1)^r \leq q^{d-1} - q^{d-2}$$

and the equality holds if and only if $d = 3$.

The lower bound (17) in Corollary 3 can be rewritten in the following form. If $n + 2$ is a prime power, then for even $d$ and $d \geq 4$

$$\Gamma(n,d) \geq \frac{2^n}{(n+1)[(n+2)^2-1]^{\frac{(d-2)}{2}}} \quad (18)$$

and for odd $d$ and $d \geq 3$,

$$\Gamma(n,d) \geq \frac{2^n}{(n+1)(n+2)[(n+2)^2-1]^{\frac{(d-3)}{2}}}. \quad (19)$$

Note that if $n + 2$ is a prime power, the lower bound (7) in Theorem 2 is given by

$$\Gamma(n,d) \geq \frac{2^n}{(n+1)(n+2)^{d-2}}, \quad d \geq 3. \quad (20)$$

By direct computation, it is not hard to see that for even $d$ and $d \geq 4$

$$\text{Bound (18)} - \text{Bound (20)} = O\left(\frac{(d-2)2^{n-1}}{n^{d+1}}\right)$$

and for odd $d$ and $d \geq 5$

$$\text{Bound (19)} - \text{Bound (20)} = O\left(\frac{(d-3)2^{n-1}}{n^{d+1}}\right).$$


## Acknowledgment

The authors would like to thank the anonymous reviewers and Associate Editor Simon Litsyn for their valuable suggestions and comments that helped to improve the correspondence.


## 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*, vol. 44, pp. 340–345, Jan. 1998.

[2] S. Al-Bassam and B. Bose, "Asymmetric/unidirectional error correcting and detecting codes," *IEEE Trans. Comput.*, vol. 43, pp. 590–597, May 1994.

[3] S. Al-Bassam, R. Venkatesan, and S. Al-Muhammadi, "New single asymmetric error-correcting codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1619–1623, Sept. 1997.

[4] S. Al-Bassam and S. Al-Muhammadi, "A single asymmetric error-correcting code with $2^{13}$ codewords of dimension 17," *IEEE Trans. Inform. Theory*, vol. 46, pp. 269–271, Jan. 2000.

[5] J. M. Berger, "A note on error detection codes for asymmetric channels," *Inform. Contr.*, vol. 4, pp. 68–73, 1961.

[6] M. Blaum, *Codes for Detecting and Correcting Unidirectional Errors*. Los Alamitos, CA: IEEE Computer Soc. Press, 1993.

[7] J. M. Borden, "Optimal asymmetric error detecting codes," *Inform. Contr.*, vol. 53, pp. 66–73, 1982.

[8] ——, "A low-rate bound for asymmetric error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 600–602, July 1983.

[9] B. Bose and S. Cunningham, "Asymmetric error correcting codes," in *Sequences II: Methods in Communication, Security, and Computer Science*, R. Capocelli, A. De Santis, and U. Vaccaro, Eds. Berlin, Germany: Springer-Verlag, 1993, pp. 24–35.

[10] B. Bose and S. Al-Bassam, "On systematic single asymmetric error-correcting codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 669–672, Mar. 2000.

[11] S. D. Constantin and T. R. N. Rao, "On the theory of binary asymmetric error-correcting codes," *Inform. Contr.*, vol. 40, pp. 20–36, 1979.

[12] P. Delsarte and P. Piret, "Spectral enumerators for certain additive-error-correcting codes over integer alphabets," in *Inform. Contr.*, vol. 48, 1981, pp. 193–210.

[13] ——, "Bounds and constructions for binary asymmetric error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 125–128, Jan 1981.

[14] T. Etzion, "Lower bounds for asymmetric and unidirectional codes," *IEEE Trans. Inform. Theory*, vol. 37, pp. 1696–1704, Nov 1991.

[15] G. Fang and H. C. A. van Tilborg, "Bounds and constructions of asymmetric or unidirectional error-correcting codes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 3, no. 4, pp. 269–300, 1992.

[16] C. V. Freiman, "Optimal error detection codes for completely asymmetric binary channels," *Inform. Contr.*, vol. 5, pp. 64–71, 1962.

[17] T. Helleseth and T. Kløve, "On group-theoretic codes for asymmetric channels," *Inform. Contr.*, vol. 49, pp. 1–9, 1981.

[18] H. Kim and C. Freiman, "Single error-correcting codes for asymmetric binary channels," *IRE Trans. Inform. Theory*, vol. IT-5, pp. 62–66, Jun 1959.

[19] T. Kløve, "Error correcting codes for the asymmetric channel," Dept. Mathematics, Univ. Bergen, Bergen, Norway, Tech. Rep.18–09-07–81, 1995.

[20] ——, "Upper bounds on codes correcting asymmetric errors," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 128–131, Jan. 1981.

[21] ——, "On Robinson's coding problem," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 450–454, May 1983.

[22] R. J. McEliece, "Comment on 'A class of codes for asymmetric channels and a problem from the additive theory of numbers'," *IEEE Trans. Inform. Theory*, vol. IT-19, p. 137, Jan. 1973.

[23] R. J. McEliece and E. R. Rodemich, "The Constantin–Rao construction for asymmetric error-correcting-codes," *Inform. Contr.*, vol. 44, pp. 187–196, 1980.

[24] T. R. N. Rao and A. S. Chawla, "Asymmetric error codes for some lsi semi-conductor memories," in *Proc. Annu. Southeastern Symp. Systems Theory*, 1975, pp. 170–171.

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

[26] J. P. Robinson, "An asymmetric error-correcting ternary code," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 258–261, Mar. 1978.

[27] Y. Saitoh, K. Yamaguchi, and H. Imai, "Some new binary codes correcting asymmetric/unidirectional errors," *IEEE Trans. Inform. Theory*, vol. 36, pp. 645–647, May 1990.

[28] A. Shiozaki, “Construction for binary asymmetric error-correcting codes,” *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 787–789, Sept. 1982.

[29] R. P. Stanley and M. F. Yoder, “A study of Varshamov codes for asymmetric channels,” Jet Propulsion Lab., Tech. Rep. 32–1526, vol. 14, 1973.

[30] R. R. Varshamov, “A class of codes for asymmetric channels and a problem from the additive theory of numbers,” *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 92–95, Jan 1973.

[31] R. R. Varshamov and G. M. Tenenholtz, “Correction code for single asymmetric error,” *Automat. Remote Contr.*, vol. 26, pp. 286–290, 1965.

[32] J. Weber, C. De Vroedt, and D. Boekee, “New upper bounds on the size of codes correcting asymmetric errors,” *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 434–437, May 1987.

[33] ——, “Bounds and constructions for binary codes of length less than 24 and asymmetric distance less than 6,” *IEEE Trans. Inform. Theory*, vol. 34, pp. 1321–1331, Sept. 1988.

[34] C. P. Xing, “Constructions of codes from residue rings of polynomials,” *IEEE Trans. Inform. Theory*, vol. 48, pp. 2995–2997, Nov. 2002.

[35] Z. Zhang and X. Xia, “New lower bounds for binary codes of asymmetric distance two,” *IEEE Trans. Inform. Theory*, vol. 38, pp. 1592–1597, Sept 1992.