Nonuniform Codes for Correcting Asymmetric Errors in Data Storage

Hongchao Zhou, Anxiao (Andrew) Jiang, *Member, IEEE,* Jehoshua Bruck, *Fellow, IEEE*

***Abstract*—Codes that correct asymmetric errors have important applications in storage systems, including flash memories and phase-change memories. The construction of asymmetric error correcting codes is a topic that was studied extensively, however, the existing approach for code construction is similar to the approach taken in the construction of symmetric error correcting codes, namely, it assumes that every codeword could sustain t asymmetric errors. Our main observation is that in contrast to symmetric errors, where the error probability of a codeword is context independent (since the error probability for 1s and 0s is identical), asymmetric errors are context dependent. For example, the all-1 codeword has a higher error probability than the all-0 codeword (since the only errors are $1 \to 0$). We call the existing codes uniform codes while we focus on the notion of nonuniform codes, namely, codes whose codewords can tolerate different numbers of asymmetric errors depending on their Hamming weights. We prove an almost explicit upper bound on the size of nonuniform asymmetric error correcting codes and present two general constructions. We also study the rate of nonuniform codes compared to uniform codes and show that there is a potential performance gain.**

***Index Terms*—Nonuniform codes, Asymmetric errors, Data storage, Bounds and constructions, Asymptotic efficiency.**

I. Introduction

ASYMMETRIC error-correcting codes have important applications in storage and communication systems, such as flash memories [1], phase-change memories, and optical communications. In such systems, the error probability from 1 to 0 is significantly higher than the error probability from 0 to 1, which is modeled by binary asymmetric channel (the $Z-$channel) where the transmitted sequences only suffer one type of errors, say $1 \to 0$. Asymmetric error-correcting codes have been widely studied: In [2], Kløve summarized and presented several such codes. In addition, a large amount of effort is contributed to the design of systematic codes [3], [4], constructing single or multiple error-correcting codes [5], [6], increasing the lower bounds [7]–[10] and applying LDPC codes in the context of asymmetric channels [11].

However, the existing approach for code construction is similar to the approach taken in the construction of symmetric error correcting codes, namely, it assumes that every codeword could sustain t asymmetric errors. As a result, different codewords might have different reliability. To see this, let's consider errors to be i.i.d., where every bit that is a 1 can change to a 0 by an asymmetric error with crossover probability $p > 0$. For a codeword $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \{0,1\}^n$, let $w(\mathbf{x}) = |\{i : 1 \leq i \leq n, x_i = 1\}|$ denote the Hamming weight of $\mathbf{x}$. Then the probability for $\mathbf{x}$ to have at most t asymmetric errors is $P_t(x) = P(t, w(\mathbf{x}), p)$, where

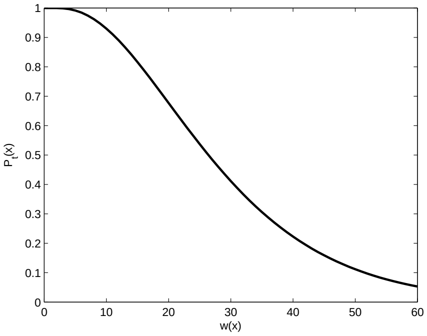


Fig. 1. The relation between $P_t(x)$ and $w(x)$ when $p = 0.1$ and $t = 2$.

$$P(t, m, p) \triangleq \sum_{i=0}^{t} \binom{m}{i} p^i (1-p)^{m-i}.$$

Since $\mathbf{x}$ can correct t errors, $P_t(x)$ is the probability of correctly decoding $\mathbf{x}$ (assuming codewords with more than t errors are uncorrectable). It can be readily observed that the reliability of codewords decreases when their Hamming weights increase, see Fig. 1 as an instance.

In some applications, like telecommunications, whose goal is to minimize the expected error probability of transmissions, it is fine to let codewords have different reliability. But when we are considering some other applications, like data storage, we need to consider the worst-case performance, namely, we need guarantee that every codeword can be correctly decoded with very high probability. In this case, it is not desired to let all the codewords tolerate the same number of asymmetric errors, since the codeword with the highest Hamming weight will become a 'bottleneck' and limit the code rate.

This motivated us to propose the concept of *nonuniform* codes, whose codewords can tolerate different numbers of asymmetric errors based on their Hamming weights. The objective is to guarantee the reliability of every codeword. That is, we consider the worst-case instead of the average-case reliability of the codewords. Given this constraint, we would like to maximize the size of the code. Specifically, let $q_e < 1$ to be maximal tolerated error probability for each codeword and let $t(x)$ denote the number of asymmetric errors that x can correct. Then given a code C, for every codeword $x \in C$,

H. Zhou and J. Bruck are with the Department of Electrical Engineering, California Institute of Technology, Pasadena, CA, 91125. *Email: hzhou@caltech.edu, bruck@caltech.edu*

A. Jiang is with the Computer Science and Engineering Department, Texas A&M University, College Station, TX 77843. *Email: ajiang@cse.tamu.edu*

Manuscript received April 19, 2005; revised January 11, 2007.

we have $P(t(x), w(x), p) \geq 1 - q_e$, so that every erroneous codeword can be corrected with probability at least $1 - q_e$. For such a code that satisfies the above constraint, we call it a nonuniform (n, p, q_e) code.

As comparison, most existing error-correcting codes are *uniform* codes, where every codeword has to sustain t asymmetric errors. For a code C of codeword length n, the Hamming weight of its codewords is at most n. (And in many existing asymmetric error-correcting codes, the maximum codeword weight indeed equals n [2].) Given the worst-case constraint and the maximal tolerated error probability q_e, we need to set t large enough that $P(t, n, p) \geq 1 - q_e$. In this case, we call the code as an uniform (n, p, q_e) code.

In this paper, we demonstrate that given the same parameters (n, p, q_e), nonuniform codes are much more efficient than uniform codes. The rest of the paper is organized as follows. In Section II, we provide some definitions and properties related to nonuniform codes. In Section III, we give an almost explicit upper bound for the size of nonuniform codes. Two general constructions, based on multiple layers or bit flips, are proposed in Section IV and Section V. Finally, Section VI studies the asymptotic rates of nonuniform codes and uniform codes (both upper bounds and lower bounds), followed by the concluding remarks in Section VII.

II. Basic Properties

According to our definitions, for a nonuniform (n, p, q_e) code C, each codeword x in it has to correct at least $t(w(x))$ asymmetric errors , where

$$t(w) = \min\{s \in N | P(s, w, p) \geq 1 - q_e\}.$$

The maximum size of a nonuniform (n, p, q_e) code is denoted by $B_\beta(n, p, q_e)$.

If C is an uniform (n, p, q_e) code, then each codeword in C can correct t asymmetric errors, where

$$t = t(n) = \min\{s \in N | P(s, n, p) \geq 1 - q_e\}.$$

The maximum size of an uniform (n, p, q_e) code is denoted by $B_\alpha(n, p, q_e)$.

Lemma 1. *For any* $0 < p, q_e < 1$ *and* $0 \leq w \leq n$, $0 \leq t(w+1) - t(w) \leq 1$.

Proof: We know

$$\begin{aligned} P(k, w, p) &= \sum_{i=0}^{k} \binom{w}{i} p^i (1-p)^{w-i} \\ &= (w-k)\binom{w}{k} \int_0^{1-p} t^{w-k-1}(1-t)^k dt \end{aligned}$$

which leads us to

$$\begin{aligned} & P(k, w, p) - P(k, w+1, p) \\ = \; & \frac{k+1}{w+1}[P(k+1, w+1, p) - P(k, w+1, p)] \end{aligned} \quad (1)$$

(1) First, let's prove that $t(w+1) \geq t(w)$. Since

$$P(k+1, w+1, p) - P(k, w+1, p) > 0$$

we have $P(k, w, p) > P(k, w+1, p)$.

We know that $P(t(w+1), w+1, p) \geq 1 - q_e$, so

$$P(t(w+1), w, p) > 1 - q_e$$

According to definition of $t(w)$, we can conclude that $t(w+1) \geq t(w)$.

(2) Let's prove that $t(w+1) - t(w) \leq 1$. Based on Equ. (1), we have

$$\begin{aligned} & P(k, w, p) - P(k+1, w+1, p) \\ = \; & \frac{w-k}{w+1}[P(k, w+1, p) - P(k+1, w+1, p)] \end{aligned}$$

So $P(k, w, p) < P(k+1, w+1, p)$.

We know that $P(t(w), w, p) \geq 1 - q_e$, therefore

$$P(t(w) + 1, w+1, p) > 1 - q_e$$

According to the definition of $t(w+1)$, we have $t(w+1) \leq t(w) + 1$. ∎

Given two binary vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$, we say $\mathbf{x} \leq \mathbf{y}$ if and only if $x_i \leq y_i$ for all $1 \leq i \leq n$. Let $S_s(\mathbf{x})$ be the set of vectors obtained by changing at most s 1's in $\mathbf{x}$ into 0's, i.e.,

$$S_s(\mathbf{x}) = \{\mathbf{v} \in \{0,1\}^n | \mathbf{v} \leq \mathbf{x} \text{ and } N(\mathbf{x}, \mathbf{v}) \leq s\}.$$

where

$$N(\mathbf{x}, \mathbf{y}) \triangleq |\{i : x_i = 1, y_i = 0\}|$$

Let $S_{s',s}(\mathbf{x})$ be the set of vectors obtained by changing at most s' 0's in $\mathbf{x}$ into 1's *or* at most s 1's in $\mathbf{x}$ into 0's, i.e.,

$$\begin{aligned} S_{s',s}(x) &= \{v \in \{0,1\}^n | v \leq x \text{ and } N(x, v) \leq s\} \\ & \bigcup \{v \in \{0,1\}^n | x \leq v \text{ and } N(v, x) \leq s'\} \end{aligned}$$

Note that $S_s(\mathbf{x}) = S_{0,s}(\mathbf{x})$.

The following properties of nonuniform codes can be easily proved, as the generalizations of those for uniform codes, including Lemmas 2.2, 2.3, 3.2, 3.3 in [2].

Lemma 2. *Code C is a nonuniform (n, p, q_e) code if and only if $S_{t(\mathbf{x})}(\mathbf{x}) \bigcap S_{t(\mathbf{y})}(\mathbf{y}) = \emptyset$ for all $\mathbf{x}, \mathbf{y} \in C$ with $\mathbf{x} \neq \mathbf{y}$.*

Proof: According to the definition of nonuniform codes, all the vectors in $S_{t(\mathbf{x})}(\mathbf{x})$ can be decoded as $\mathbf{x}$, and all the vectors in $S_{t(\mathbf{y})}(\mathbf{y})$ can be decoded as $\mathbf{y}$. Hence, $S_{t(\mathbf{x})}(\mathbf{x}) \bigcap S_{t(\mathbf{y})}(\mathbf{y}) = \emptyset$ for all $\mathbf{x}, \mathbf{y} \in C$. ∎

Lemma 3. *Let C be a nonuniform (n, p, q_e) code. If $\mathbf{x}, \mathbf{y} \in C$ with $\mathbf{x} \neq \mathbf{y}$, then $S_{s, t(\mathbf{x})-s}(\mathbf{x}) \bigcap S_{s, t(\mathbf{y})-s}(\mathbf{y}) = \emptyset$ for all $0 \leq s \leq \min(t(\mathbf{x}), t(\mathbf{y}))$.*

Proof: Let us prove this by contradiction. Assume that there exists $\mathbf{v} \in S_{s, t(\mathbf{x})-s}(\mathbf{x}) \bigcap S_{s, t(\mathbf{y})-s}(\mathbf{y})$.

If $\mathbf{v} \in S_{s,0}(\mathbf{x}) \bigcap S_{s,0}(\mathbf{y})$, then we let $\mathbf{u} = u_1 u_2 \ldots u_n \in \{0,1\}^n$ such that $u_i = \min\{x_i, y_i\}$ for $1 \leq i \leq n$. It is not hard to prove that $N(\mathbf{x}, \mathbf{u}) \leq N(\mathbf{v}, \mathbf{y}) \leq s$, and $N(\mathbf{y}, \mathbf{u}) \leq N(\mathbf{v}, \mathbf{x}) \leq s$. As a result, we have $\mathbf{u} \in S_s(\mathbf{x}) \bigcap S_s(\mathbf{y}) \subseteq S_{t(\mathbf{x})}(\mathbf{x}) \bigcap S_{t(\mathbf{y})}(\mathbf{y})$. According to the lemma above, C is not a nonuniform (n, p, q_e) code, which is a contradiction.

If $\mathbf{v} \in S_{0, t(\mathbf{x})-s} \bigcap S_{0, t(\mathbf{y})-s}(\mathbf{y})$, then we have that $\mathbf{v} \in S_{t(\mathbf{x})}(\mathbf{x}) \bigcap S_{t(\mathbf{y})}(\mathbf{y})$. So C is not a nonuniform (n, p, q_e) code, which is a contradiction.

If $\mathbf{v} \in S_{s,0}(\mathbf{x}) \bigcap S_{0,t(\mathbf{y})-s}(\mathbf{y})$, then $N(\mathbf{y},\mathbf{x}) \leq N(\mathbf{v},\mathbf{x}) + N(\mathbf{y},\mathbf{v}) \leq s + (t(\mathbf{y}) - s) = t(\mathbf{y})$ and $\mathbf{x} \leq \mathbf{v} \leq \mathbf{y}$, so $\mathbf{x} \in S_{t(\mathbf{x})}(\mathbf{x}) \bigcap S_{t(\mathbf{y})}(\mathbf{y})$ and C is not a nonuniform (n, p, q_e) code. Similarly, when $\mathbf{v} \in S_{0,t(\mathbf{x})-s}(\mathbf{x}) \bigcap S_{s,0}(\mathbf{y})$, we have the same result.

This completes the proof. ■

Lemma 4. *There always exists a nonuniform (n, p, q_e) code of the maximum size that contains the all-zero codeword.*

Proof: Let C be a nonuniform (n, p, q_e) code, and assume that $00...00 \notin C$. If there exists a codeword $\mathbf{x} \in C$ such that $00...00 \in S_{t(\mathbf{x})}(\mathbf{x})$, then we can get a new nonuniform (n, p, q_e) code C' of the same size by replacing $\mathbf{x}$ with $00...00$ in C. If there does not exist a codeword $\mathbf{x} \in C$ such that $00...00 \in S_{t(\mathbf{x})}(\mathbf{x})$, then we can get a larger nonuniform (n, p, q_e) code C' by adding $00...00$ to C. ■

Given a nonuniform code C, let C_r denote the number of codewords with Hamming weight r in C, i.e.

$$C_r = |\{\mathbf{x} \in C | w(\mathbf{x}) = r\}|.$$

Lemma 5. *Let C be a nonuniform (n, p, q_e) code. For $0 \leq r \leq n$, let s be an integer such that $0 \leq s \leq t(r-s)$ and let $k = \max\{z | 0 \leq z \leq n, z - (t(z) - s) \leq r\}$, then we have*

$$\sum_{j=1}^{s} \binom{n-r+j}{j} C_{r-j} + \sum_{j=0}^{t(k)-s} \binom{r+j}{j} C_{r+j} \leq \binom{n}{r}.$$

Proof: If $\mathbf{x} \in C$ and $w(\mathbf{x}) = r - j$ with $1 \leq j \leq s$, then $S_{s,t(\mathbf{x})-s}(\mathbf{x})$ contains $\binom{n-r+j}{j}$ vectors of weight r. If $\mathbf{x} \in C$ with $w(\mathbf{x}) = r + j$ and $0 \leq j \leq t(k) - s$, then $S_{s,t(\mathbf{x})-s}(\mathbf{x})$ contains $\binom{r+j}{j}$ vectors of weight r. According to Lemma 3, we know that $\bigcup_{\mathbf{x} \in C, w(\mathbf{x}) = r} S_{s,t(\mathbf{x})-s}(\mathbf{x})$ is a disjoint union, so the number of vectors in $\bigcup_{\mathbf{x} \in C, w(\mathbf{x}) = r} S_{s,t(\mathbf{x})-s}(\mathbf{x})$ is

$$\sum_{j=1}^{s} \binom{n-r+j}{j} C_{r-j} + \sum_{j=0}^{t(k)-s} \binom{r+j}{j} C_{r+j}$$

which is at most $\binom{n}{r}$. The lemma follows. ■

Note that in Lemma 5, if we let $s = 0$, then we can get

$$\sum_{j=0}^{t(k)} \binom{r+j}{j} C_{r+j} \leq \binom{n}{r} \tag{2}$$

where $k = \max\{z | 0 \leq z \leq n, z - t(z) \leq r\}$. This inequality will be used to get an almost explicit upper bound for the size of nonuniform codes.

III. Upper Bounds

In this section, we first present some existing results on the upper bounds of $B_\alpha(n, p, q_e)$ for uniform codes. Then we derive an almost explicit upper bound of $B_\beta(n, p, q_e)$ for nonuniform codes, and compare it with the almost explicit upper bound of uniform codes given by Kløve.

A. Upper Bounds for Uniform Codes

For uniform codes of the maximum size, the value of t is uniquely determined by n, p and q_e, such that t is the minimum integer satisfying the condition $P(t, n, p) \geq 1 - q_e$. Hence we can also express $B_\alpha(n, p, q_e)$ as $B_\alpha(n, t)$ such that

$$t = \min\{s \in N | P(s, n, p) \geq 1 - q_e\}.$$

An explicit upper bound to $B_\alpha(n, t)$ was given by Varshamov [12]. Borden showed that $B_\alpha(n, t)$ is upper bounded by $\min\{A(n+t, 2t+1), (t+1)A(n, 2t+1)\}$ [2], where $A(n, d)$ is the maximal number of vectors in $\{0, 1\}^n$ with Hamming distance at least d. Goldbaum pointed out that the upper bounds can be obtained using integer programming. By adding more constrains to the integer programming, the upper bounds were later improved by Delsarte and Piret [19] and Weber *et al.* [14] [20]. Kløve generalized the bounds of Delsarte and Piret, and gave an almost explicit upper bound which is very easy to compute by relaxing some of the constrains [16], in the following way.

Theorem 6. *[16] For $n > 2t \geq 2$, let $y_0, y_1, ..., y_n$ be defined by*

1) $y_0 = 1$
2) $y_r = 0, \quad \forall 1 \leq r \leq t$
3) $y_{t+r} = \frac{1}{\binom{t+r}{t}}[\binom{n}{r} - \sum_{j=0}^{t-1} y_{r+j} \binom{r+j}{j}], \forall 1 \leq r \leq \frac{n}{2} - t$
4) $y_{n-r} = y_r, \quad \forall 0 \leq r < \frac{n}{2}$

Then $B_\alpha(n, t) \leq M_\alpha(n, t) \triangleq \sum_{r=0}^{n} y_r$.

This method obtains a good upper bound to $B_\alpha(n, t)$ (although it is not the best known one). Since it is very easy to compute, when n and t are large, it is every useful for analyzing the sizes of uniform codes. In the rest of this section, we will derive a similar almost explicit upper bound for nonuniform codes and compare them with each other.

B. Upper Bounds for Non-uniform Codes

We now derive an almost explicit upper bound for the size of nonuniform codes, followed the idea of Kløve [16] for uniform codes. First, we define

$$\overline{h}(r) = \max\{w | 0 \leq w \leq n, w - t(w) = r\},$$

$$\underline{h}(r) = \min\{w | 0 \leq w \leq n, w - t(w) = r\}.$$

And let $M_\beta(n, p, q_e) = \max \sum_{r=0}^{n} z_r$, where the maximum is taken over the following constraints:

1) z_r are non-negative real numbers;
2) $z_0 = 1$;
3) $\sum_{j=0}^{t(\overline{h}(r))} \binom{r+j}{j} z_{r+j} \leq \binom{n}{r}$ for $r \geq 0$.

Then $M_\beta(n, p, q_e)$ is an upper bound for $B_\beta(n, p, q_e)$. Here, condition 2) is given by Lemma 4, and condition 3) is given by Equ. (2) from Lemma 5. Our goal in this section is to find an almost explicit way to express $M_\beta(n, p, q_e)$.

Lemma 7. *Assume $\sum_{r=0}^{n} z_r$ is maximized over $z_0, z_1, ..., z_n$ in the problem above. Let*

$$Z_r = \sum_{j=0}^{min\{n-r, t(\overline{h}(r))\}} z_{r+j} \binom{r+j}{j}.$$

Then $Z_r = \binom{n}{r}$ for $r \leq n - t(n)$.

Proof: Suppose that $Z_r < \binom{n}{r}$ for some $r \leq n - t(n)$. Let $g = \overline{h}(r)$ and $k = \min\{w | z_w > 0, w > g\}$.

Let $m = \max\{w | k - t(k) > w\}$. Then we first prove that for all $r < w \leq m$, $Z_w < \binom{n}{w}$. In order to prove this, we let $s = w - r$, and get

$$\begin{aligned}
Z_w &= \sum_{j=0}^{t(\overline{h}(w))} z_{w+j} \binom{w+j}{w} \\
&= \sum_{j=0}^{g-r-s} z_{r+s+j} \binom{r+s+j}{r+s} \\
&= \sum_{j=s}^{t(g)} z_{r+j} \binom{r+j}{r+s} \\
&= \sum_{j=s}^{t(g)} z_{r+j} \binom{r+j}{r} \frac{\binom{j}{s}}{\binom{r+s}{s}} \\
&\leq \frac{\binom{t(g)}{s}}{\binom{r+s}{s}} \sum_{j=s}^{t(g)} z_{r+j} \binom{r+j}{r} \\
&< \frac{\binom{t(g)}{s}}{\binom{r+s}{s}} \binom{n}{r} \\
&= \frac{t(g) * ... * (t(g) - s + 1)}{(n-r) * ... * (n-r-s+1)} \binom{n}{r+s} \\
&\leq \binom{n}{w}.
\end{aligned}$$

Now, we construct a new group of real numbers $z_0^*, z_1^*, ..., z_n^*$ such that

1) $z_g^* = z_g + \Delta$
2) $z_k^* = z_k - \delta$
3) $z_r^* = z_r$ for $r \neq h, r \neq k$

with

$$\Delta = \min(\{\frac{\binom{n}{w} - Z_w}{\binom{g}{w}} | r \leq w \leq m\} \bigcup \{\frac{\binom{k}{w}}{\binom{g}{w}} z_k | m < w \leq g\}),$$

$$\delta = \frac{1}{\min\{\frac{\binom{k}{w}}{\binom{g}{w}} | m < w \leq g\}} \Delta.$$

For such Δ, δ, it is not hard to prove that $Z_r^* = \binom{n}{r}$ for $0 \leq r \leq n$. On the other hand,

$$\sum_{r=0}^{n} z_r^* = \sum_{r=0}^{n} z_r + \Delta - \delta > \sum_{r=0}^{n} z_r,$$

which contradicts our assumption that $\sum_{r=0}^n z_r$ is maximized over the constrains. So the lemma is true. ■

Lemma 8. *Assume $\sum_{r=0}^n z_r$ is maximized over $z_0, z_1, ..., z_n$ in the problem above. Let*

$$Y_r = \sum_{j=0}^{min\{n-r, t(\underline{h}(r))\}} z_{r+j} \binom{r+j}{j}.$$

Then $Y_r = \binom{n}{r}$ for $r \leq n - t(n)$.

Sketch of Proof: If $\overline{h}(r) = \underline{h}(r)$, then the lemma is true. So we only need to prove it for the case that $\overline{h}(r) > \underline{h}(r)$. Similar to Lemma 7, to get the contradiction, we can construct a new group of real numbers $z_0^*, z_1^*, ..., z_n^*$ such that

1) $z_{\underline{h}(r)}^* = z_{\underline{h}(r)}^* + \Delta$
2) $z_w^* = 0$ for $\underline{h}(r) < w \underline{\leq} \overline{h}(r)$
3) $z_r^* = z_r$ if $w \notin [\underline{h}(r), \overline{h}(r)]$

with

$$\Delta = \min\{\frac{\sum_{j=\underline{h}(r)+1}^{\overline{h}(r)} \binom{j}{w} z_j}{\binom{\underline{h}(r)}{w}} | r \leq w \leq \underline{h}(r)\}.$$

For this $z_0^*, z_1^*, ..., z_n^*$, they satisfy all the constrains and $Y_r^* = \binom{n}{r}$ for $r \leq n - t(n)$. At the same time, it can be proved that

$$\sum_{r=0}^{n} z_r^* > \sum_{r=0}^{n} z_r$$

which contradicts with our assumption that $\sum_{r=0}^n z_r$ is maximized over the constrains. This completes the proof. ■

Now let $y_0, y_1, ..., y_n$ be a group of optimal solutions to $z_0, z_1, ..., z_n$ that maximize $\sum_{r=0}^n z_r$. Then $y_0, y_1, ..., y_n$ satisfy the condition in Lemma 8. We see that $y_0 = 1$. Then based on Lemma 8, we can get $y_1, ..., y_n$ uniquely by iteration. Hence, we have the following theorem for the upper bound $M_\beta(n, p, q_e)$.

Theorem 9. *Let $y_0, y_1, ..., y_n$ be defined by*

1) $y_0 = 1$;
2) $y_r = 0, \quad \forall 1 \leq r \leq \max\{s | 1 \leq s \leq n, s \leq t(s)\}$;
3) $y_r = \frac{1}{\binom{r}{t(r)}} [\binom{n}{r-t(r)} - \sum_{j=1}^{t(r)} y_{r-j} \binom{r-j}{t(r)-j}]$,
$\forall \max\{s | 1 \leq s \leq n, s \leq t(s)\} < r \leq n$.

Then $B_\beta(n, p, q_e) \leq M_\beta(n, p, q_e) = \sum_{r=0}^n y_r$.

This theorem provides an almost explicit expression for the upper bound $M_\beta(n, p, q_e)$, which is much easier to calculate than the equivalent expression defined at the beginning of this subsection. Note that in the theorem, we do not have a constraint like the one (constraint 4) in Theorem 6. That is because that the optimal non-unform codes usually do not have symmetric weight distributions due to the fact that $t(w)$ monotonically increases with w.

C. Upper Bound Comparison

Given (n, p, q_e), we can define the efficiency of uniform codes as

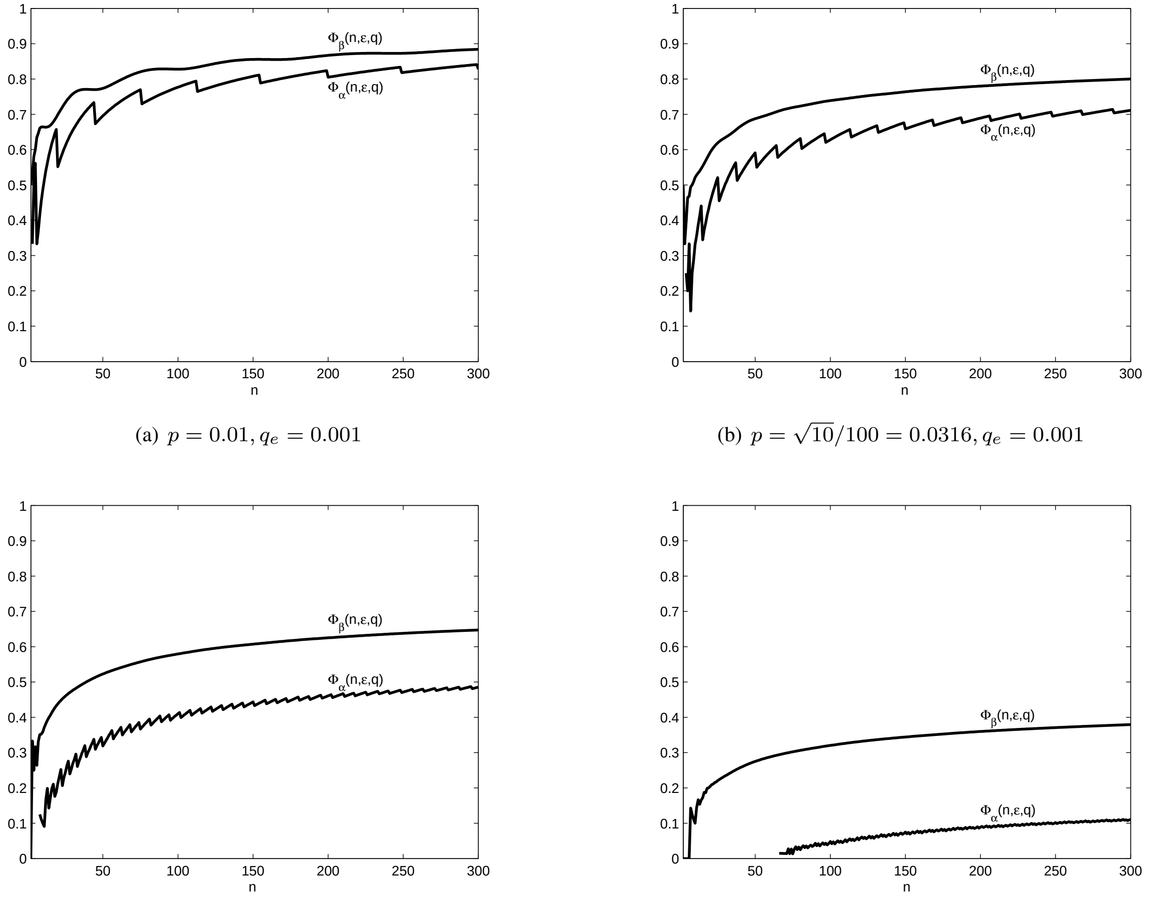
$$\eta_\alpha(n, p, q_e) \triangleq \frac{\log_2 B_\alpha(n, p, q_e)}{n}$$

and define the efficiency of nonuniform codes as

$$\eta_\beta(n, p, q_e) \triangleq \frac{\log_2 B_\beta(n, p, q_e)}{n}$$

By the definition of uniform and nonuniform codes, it is simple to see that $\eta_\beta(n, p, q_e) \geq \eta_\alpha(n, p, q_e)$.

In this subsection, we compare the upper bounds of $\eta_\alpha(n, p, q_e)$ and $\eta_\beta(n, p, q_e)$, which are defined as $\Phi_\alpha(n, p, q_e)$ and $\Phi_\beta(n, p, q_e)$ separately. Here, assume $M_\alpha(n, p, q_e)$ is the almost explicit upper bound for uniform codes obtained from



(a) $p = 0.01, q_e = 0.001$

(b) $p = \sqrt{10}/100 = 0.0316, q_e = 0.001$

(c) $p = 0.1, q_e = 0.001$

(d) $p = \sqrt{10}/10 = 0.316, q_e = 0.001$

Fig. 2. Given p, q_e, the values of $\Phi_\alpha(n, p, q_e)$ and $\Phi_\beta(n, p, q_e)$ for different codeword length n. Here, $\Phi_\alpha(n, p, q_e)$ is the upper bound of the efficiency for uniform codes, and $\Phi_\beta(n, p, q_e)$ is the upper bound of the efficiency for nonuniform codes.

Theorem 6, and $M_\beta(n, p, q_e)$ is the almost explicit upper bound for nonuniform codes obtained from Theorem 9. Then we have

$$\Phi_\alpha(n, p, q_e) \triangleq \frac{\log M_\alpha(n, p, q_e)}{n},$$

$$\Phi_\beta(n, p, q_e) \triangleq \frac{\log M_\beta(n, p, q_e)}{n}.$$

The difference between $\Phi_\alpha(n, p, q_e)$ and $\Phi_\beta(n, p, q_e)$ implies the efficiency improvement of nonuniform codes compared to uniform codes.

Fig. 2 gives the values of $\Phi_\alpha(n, p, q_e)$ and $\Phi_\beta(n, p, q_e)$ for different n with fixed (p, q_e). Since the almost explicit upper bound of uniform codes given by Kløve only works for $n \geq 2 * t(n)$, only the available interval is plotted. It demonstrates that given the same parameters, the efficiency (upper bound) of nonuniform codes is substantially greater than that of uniform codes.

IV. Constructions Based on Multiple Layers

In [2], Kløve summarized some constructions of uniform codes for correcting asymmetric errors. The code of Kim and Freiman was the first code constructed for correcting multiple asymmetric errors. Varshamov [17] and Constrain and Rao [18] presented some constructions based group theory. Later, Delsarte and Piret [19] proposed a construction based on 'expurgating/puncturing' with some improvements given by Weber et. al. [20].

In this section, we propose a general construction of nonuniform codes based on multiple layers. Then we compare BCH codes with layered BCH codes under the same parameters. It shows that the sizes of the codes can be significantly increased by equalizing the reliability of all the codewords.

A. Layered Codes

From the definition of nonuniform codes, we know that $t(w)$ can be easily and uniquely determined by p, q_e. So a question arises: if $n, t(w)$ (for $0 \leq w \leq n$) are given, how to construct a nonuniform code efficiently? Intuitively, we can divide all the codewords of a nonuniform code into at most $t(n) + 1$ layers such that all the codewords in the i^{th} layer (with $0 \leq i \leq t(n)$) can tolerate at least i asymmetric errors. In other words, the code is the combination of up to $t(n) + 1$ uniform codes, each of which corrects a different number of asymmetric errors. However, we cannot design such a code by constructing codewords independently for different layers, because a simple combination of several independent codes may violate the error correction requirements of the nonuniform codes, due to the interference between two neighbor layers. Our idea is simple: let's first construct a code which can tolerate $t(n)$ asymmetric errors. Then we add some codewords to the lowest $t(n)$ layers such that the codewords in the top layer keep unchanged and they still can tolerate $t(n)$ asymmetric errors, and the codewords in the other layers can tolerate up to $t(n)-1$ asymmetric errors. Iteratively, we can continue to add many codeword into the lowest $t(n)-1$ layers ... Based on this idea, given $n, t(w)$, we construct layered codes as follows.

Theorem 10 (Layered Codes)**.** *Let $k = t(n)$ and let $C_0, C_1, ..., C_k$ be $k+1$ binary codes of codeword length n, where $C_0 \supset C_1 \supset ... \supset C_k$ and for $0 \leq t \leq k$, the code C_t can correct t asymmetric errors. Let*

$$C = \{\mathbf{x} \in \{0,1\}^n | \mathbf{x} \in C_{t'(w(\mathbf{x}))}\},$$

where

$$t'(w(\mathbf{x})) = t(\max\{w' | w' - t(w') \leq w(\mathbf{x})\}).$$

Then for all $\mathbf{x} \in C$, $\mathbf{x}$ can tolerate $t(w(\mathbf{x}))$ asymmetric errors.

Proof: We prove that for all $\mathbf{x}, \mathbf{y} \in C$ with $\mathbf{x} \neq \mathbf{y}$, $S_{t(w(\mathbf{x}))}(\mathbf{x}) \bigcap S_{t(w(\mathbf{y}))}(\mathbf{y}) = \emptyset$. W.l.o.g., we assume $w(\mathbf{x}) \geq w(\mathbf{y})$.

If $w(\mathbf{x}) - t(w(\mathbf{x})) > w(\mathbf{y})$, the conclusion is true.

If $w(\mathbf{x}) - t(w(\mathbf{x})) \leq w(\mathbf{y})$ and $w(\mathbf{x}) \geq w(\mathbf{y})$, we have $S_{t(w(\mathbf{x}))}(\mathbf{x}) \bigcap S_{t(w(\mathbf{y}))}(\mathbf{y}) \subseteq S_{t'(w(\mathbf{y}))}(\mathbf{x}) \bigcap S_{t'(w(\mathbf{y}))}(\mathbf{y})$. However, we know that $\mathbf{x} \in C_{t'(w(\mathbf{x}))} \subseteq C_{t'(w(\mathbf{y}))}$ and $\mathbf{y} \in C_{t'(w(\mathbf{y}))}$, therefore $S_{t'(w(\mathbf{y}))}(\mathbf{x}) \bigcap S_{t'(w(\mathbf{y}))}(\mathbf{y}) = \emptyset$. Furthermore, we have $S_{t(w(\mathbf{x}))}(\mathbf{x}) \bigcap S_{t(w(\mathbf{y}))}(\mathbf{y}) = \emptyset$. ■

We see that the constructions of layered codes are based on the provided group of codes $C_0, C_1, ..., C_k$ such that $C_0 \supset C_1 \supset ... \supset C_k$ and for $0 \leq t \leq k$, the code C_t can correct t asymmetric errors. Examples of such codes include Varshamov codes [17], BCH codes, etc.

One construction of Varshamov codes can be described as follows: Let $\alpha_1, \alpha_2, ..., \alpha_n$ be distinct non-zero elements of F_q, and let $\alpha := (\alpha_1, \alpha_2, ..., \alpha_n)$. For $\mathbf{x} = (x_1, x_2, ..., x_n) \in \{0,1\}^n$, let $\mathbf{x}\alpha = (x_1\alpha_1, x_2\alpha_2, ..., x_n\alpha_n)$. For $g_1, g_2, ..., g_t \in F_q$ and $0 \leq t \leq k$, let

$$C_t := \{\mathbf{x} \in \{0,1\}^n | \sigma_l(\mathbf{x}\alpha) = g_l \text{ for } 1 \leq l \leq t\}$$

where the elementary symmetric function $\sigma_l(\mathbf{u})$ for $l \geq 0$ are defined by

$$\prod_{i=1}^{r}(z + u_i) = \sum_{l=0}^{\infty} \sigma_l(\mathbf{u}) z^{r-l}.$$

Then C_t can correct t asymmetric errors (for $0 \leq t \leq k$), and $C_0 \supset C_1 \supset ... \supset C_k$.

Such a group of codes can also be constructed by BCH codes: Let $(\alpha_0, \alpha_1, ..., \alpha_{n-1})$ be n distinct nonzero elements of G_{2^m} with $n = 2^m - 1$. For $0 \leq t \leq k$, let

$$C_t := \{\mathbf{x} \in \{0,1\}^n | \sum_{i=1}^{n} x_i \alpha_i^{(2l-1)} = 0 \text{ for } 1 \leq l \leq t\}.$$

In the above examples, assume $\mathbf{x}$ is a codeword in C_t and $\mathbf{y} = \mathbf{x} + \mathbf{e}$ is a received word with error e, then there is an efficient algorithm to decode $\mathbf{y}$ into a codeword, which is denoted by $D_t(\mathbf{y})$. If $\mathbf{y}$ has at most t asymmetric errors, then $D_t(\mathbf{y}) = \mathbf{x}$. In the following theorem, we show that the layered codes proposed above also have an efficient decoding algorithm if $D_t(\cdot)$ (for $0 \leq t \leq k$) are provided and efficient.

Theorem 11 (Decoding of Layered Codes)**.** *Let C be a layered code, let $\mathbf{x} \in C$ be a codeword, and let $\mathbf{y} = \mathbf{x} + \mathbf{e}$ be a received word such that $|e| = N(\mathbf{x}, \mathbf{y}) \leq t(w(\mathbf{x}))$. (Here $\mathbf{e}$ is the asymmetric-error vector.) Then there exists at least one integer t such that*

1) *$t'(w(\mathbf{y})) \leq t \leq t'(w(\mathbf{y}) + t'(w(\mathbf{y})))$;*
2) *$D_t(\mathbf{y}) \in C$;*
3) *$\mathbf{y} \leq D_t(\mathbf{y})$ and $N(D_t(\mathbf{y}), \mathbf{y}) \leq t(w(D_t(\mathbf{y})))$.*

For such t, we have $D_t(\mathbf{y}) = \mathbf{x}$.

Proof: If we let $t = t'(w(\mathbf{x}))$, then we can get that t satisfies the conditions and $D_\tau(\mathbf{y}) = \mathbf{x}$. So such t exists.

Now we only need to prove that once there exists t satisfying the conditions in the theorem, we have $D_t(\mathbf{y}) = \mathbf{x}$. We prove this by contradiction. Assume there exists t satisfying the conditions but $\mathbf{z} = D_t(\mathbf{y}) \neq \mathbf{x}$. Then $N(\mathbf{z}, \mathbf{y}) \leq t(w(\mathbf{z}))$ and $N(\mathbf{x}, \mathbf{y}) \leq t(w(\mathbf{x}))$, which contradicts the property of the layered codes. ■

According to the above theorem, to decode a noisy word $\mathbf{y}$, we can check all the integers between $t'(w(\mathbf{y}))$ and $t'(w(\mathbf{y}) + t'(w(\mathbf{y})))$ to find the value of t. Once we find the integer t satisfying the conditions in the theorem, we can decode $\mathbf{y}$ into $D_t(\mathbf{y})$ directly. (Note that $t'(w(\mathbf{y}) + t'(w(\mathbf{y}))) - t'(w(\mathbf{y}))$ is normally much smaller than $w(y)$. It is approximately $\frac{p^2}{(1-p)^2}w(y)$ when $w(y)$ is large.) We see that this decoding process is efficient if $D_t(.)$ is efficient for $0 \leq t \leq k$.

B. BCH codes vs. Layered BCH Codes

Typically, non-linear codes, like Varshamov codes are superior to BCH codes. But there are no evidences showing that the gap of efficiencies between them is very large [17]. On the other hand, it is not easy to study the properties of non-linear codes, such as their weight distributions. In this subsection, we compare BCH codes with layered BCH codes (layered codes based on BCH codes) under the same parameters (n, p, q_e).

First, for a BCH code of length $n = 2^m - 1$ over G_{2^m}, if it has to correct t errors such that

$$t = \min\{s \in N | P(s, n, p) \geq 1 - q_e\}$$

then it has about $\frac{2^n}{(n+1)^t}$ codewords.

Next, for a layered BCH code of length $n = 2^m - 1$ over G_{2^m}, the codewords with Hamming weight w have to correct $t(w)$ asymmetric errors such that

$$t(w) = \min\{s \in N | P(s, t(w), p) \geq 1 - q_e\}$$

If we can know the weight distribution for BCH codes, then the sizes of the layered BCH codes can be obtained by summing up the numbers of codewords with different weights. It is known that the weight distribution of binary primitive BCH codes can be approximated by the binomial distribution. Considering a BCH code with length $n = 2^m - 1$ and with

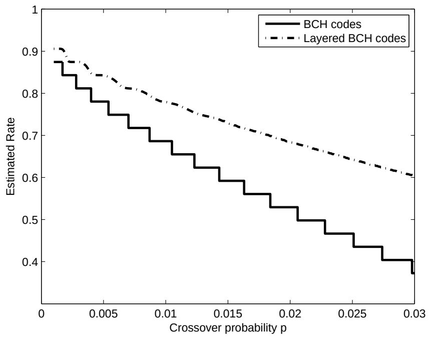


Fig. 3. The estimated rates of BCH codes and layered BCH codes with different p when $n = 255$ and $q_e = 10^{-4}$.

minimum distance $2t+1 \leq 2^{[(m+1)/2]}+1$, if b_i is the number of codewords with weight i in this code, then [22]

$$b_i = \frac{\binom{n}{i}}{(n+1)^t}(1+E_i)$$

with $|E_i|$ decreases with n. Here, for simplicity, given a BCH code, we use $\frac{\binom{n}{i}}{(n+1)^t}$ to approximate b_i for $0 \leq i \leq n$.

Based on the approximations above, Fig. 3 plots the estimated rates of BCH codes and layered BCH codes with variable p when $n = 255$ and $q_e = 10^{-4}$. Here, for a code C, let $\#C$ be the number of codewords, then the rate of C is defined as $\frac{\log_2(\#C)}{n}$. From this figure, we see that the rate of BCH codes is a step function of p, that is because t is a step function of p when n and q_e are fixed. It demonstrates that under the same parameters (n, p, q_e), the rate of layered BCH codes is much higher than that of BCH codes. It implies that by constructing nonuniform codes instead of uniform codes, we can significantly increase the code efficiency.

V. Constructions based on Flips

Many non-linear codes designed to correct asymmetric errors do not yet have efficient encoding algorithms. Namely, it is not easy to find an efficient encoding function $f : \{0,1\}^k \to C$ with $k \simeq \lfloor \log |C| \rfloor$. On the other hand, in [17], Varshamov showed that linear codes have nearly the same ability to correct asymmetric errors and symmetric errors (for the uniform code case). In this subsection, we focus on the approach of designing nonuniform codes for asymmetric errors with efficient encoding schemes, by utilizing the well studied linear codes for symmetric errors.

We can use a linear code to correct $t(n)$ asymmetric errors directly, but this method is inefficient not only because the decoding sphere for symmetric errors is greater than the sphere for asymmetric errors (and therefore an overkill), but also because for low-weight codewords, the number of asymmetric errors they need to correct can be much smaller than $t(n)$.

Our idea is to build a "flipping code" that uses only low-weight codewords (specifically, codewords of Hamming weight no more than $\sim \frac{n}{2}$), because they need to correct fewer asymmetric errors and therefore can increase the code's rate. In the rest of this section, we present two different constructions.

A. First Construction

First, construct a linear code C (like BCH codes) of length n with generator matrix G that corrects $t(\lfloor \frac{n}{2} \rfloor)$ symmetric errors. Assume the dimension of the code is k. For any binary message $\mathbf{u} \in \{0,1\}^k$, we can map it to a codeword $\mathbf{x}$ in C such that $\mathbf{x} = \mathbf{u}G$. Next, let $\overline{\mathbf{x}}$ denote a word obtained by flipping all the bits in $\mathbf{x}$ such that if $x_i = 0$ then $\overline{x}_i = 1$ and if $x_i = 1$ then $\overline{x}_i = 0$; and let y denote the final codeword corresponding to u. We check whether $w(\mathbf{x}) > \lfloor \frac{n}{2} \rfloor$ and construct y in the following way:

$$y = \begin{cases} x00...0 & \text{if } w(\mathbf{x}) > \lfloor \frac{n}{2} \rfloor \\ \overline{x}11...1 & \text{otherwise} \end{cases}$$

Here, the auxiliary bits (0's or 1's) are added to distinguish that whether x has been flipped or not, and they form a repetition code to tolerate errors.

The corresponding decoding process is straightforward: Assume we received a word y'. If there is at least one 1 in the auxiliary bits, then we "flip" the word by changing all 0's to 1's and all 1's to 0's; otherwise, we keep the word unchanged. Then we apply the decoding scheme of the code C to the first n bits of the word. Finally, the message u can be successfully decoded if y' has at most $t(\lfloor \frac{n}{2} \rfloor)$ errors in the first n bits.

B. Second Construction

In the previous construction, several auxiliary bits are needed to protect one bit of information, which is not very efficient. In this section, we try to move this bit into the message part of the codewords in C. This motivates us to give the following construction.

Let C be a linear code with length n that corrects t' symmetric errors (we will specify t' later). Assume the dimension of the code is k. Now, for any binary message $\mathbf{u} \in \{0,1\}^{k-1}$ of length $k-1$, we get $u' = 0u$ by adding one bit 0 in front of u. Then we can map u' to a codeword $\mathbf{x}$ in C such that

$$x = (0u)G = 0uv$$

where G is the generator matrix of C in systematic form and the length of v is $n-k$. Let α be a codeword in C such that the first bit $\alpha_1 = 1$ and its weight is the maximal one among all the codeword in C, i.e.,

$$\alpha = \arg \max_{x \in C, x_1 = 1} w(x)$$

Generally, $w(\alpha)$ is very close to n. In order to reduce the weights of the codewords, we use the following operations: Calculate the relative weight

$$w(x|\alpha) = |\{1 \leq i \leq n | x_i = 1, \alpha_i = 1\}|$$

Then we get the final codeword

$$y = \begin{cases} x + \alpha & \text{if } w(x|\alpha) > \frac{w(\alpha)}{2} \\ x & \text{otherwise} \end{cases}$$

where $+$ is the binary sum, so $x + \alpha$ is to flip the bits in x corresponding the ones in α. So far, we see that the maximal weight for y is $\lfloor n - \frac{w(\alpha)}{2} \rfloor$. That means we need to select t' such that

$$t' = t(\lfloor n - \frac{w(\alpha)}{2} \rfloor).$$

In the above encoding process, for different binary messages, they have different codewords. And for any codeword y, we have $y \in C$. That is because either $y = x$ or $y = x + \alpha$, where both x and α are codewords in C and C is a linear code. The decoding process is very simple: Given the received word $y' = y + e$, we can always get y by applying the decoding scheme if $|e| \leq t'$. If $y_1 = 1$, that means x has been flipped based on α, so we have $x = y + \alpha$; otherwise, $x = y$. Then the initial message $u = x_2 x_3 ... x_k$.

We see that the second construction is a little more efficient than the first one, by moving the 'flipping' bit from the outside of a codeword (of an error-correcting code) to the inside. Here is an example of the second construction: Let C be the $(7, 4)$ Hamming code, which is able to correct single-bit errors. The generating matrix of the $(7, 4)$ Hamming code is

$$G = \left(\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right)$$

Here we have $t' = 1$ and $k = 4$. Assume the binary message is $u = 011$, then we have $x = (0u)G = 0011100$. It is easy to see that α is the all-one codeword, i.e., $\alpha = 1111111$. In this case, $w(x|\alpha) <= \frac{w(\alpha)}{2}$, so the final codeword $y = 0011100$. Assume the binary message is $u = 110$, then we have $x = (0u)G = 0110110$. In this case, $w(x|\alpha) > \frac{w(\alpha)}{2}$, so the final codeword $y = x + \alpha = 1001001$.

Assume the received word is $y' = 0001001$. By applying the decoding algorithm of Hamming codes, we get $y = 1001001$. Since $y_1 = 1$, we have $x = y + \alpha$, and as a result, $x = 110$.

C. Comments

When n is sufficiently large, the codes based on flips above become nearly as efficient as a linear codes correcting $t(\lfloor \frac{n}{2} \rfloor)$ symmetric errors. (We define the codes' efficiency in Section VI.) It is much more efficient than designing a linear code correcting $t(n)$ symmetric errors. Note that when n is large and p is small, these codes can have very good performance on efficiency. That is because when n is sufficiently large, the efficiency of an optimal nonuniform code is dominated by the codewords with the same Hamming weight w_d $(\leq \frac{n}{2})$, and w_d approaches $\frac{n}{2}$ as p gets close to 0. We can intuitively understand it based on two facts when n is sufficiently large: (1) There are at most $n 2^{n(H(\frac{w_d}{n}) + \delta)}$ codewords in this optimal nonuniform code. (2) When p becomes small, we can get a nonuniform code with at least $2^{n(1-\delta)}$ codewords. So when n is sufficiently large and p is small, we have $w_d \rightarrow \frac{n}{2}$. Hence, the optimal nonuniform code has almost the same asymptotic efficiency with an optimal weight-bounded code (Hamming weight is at most n/2), which corrects $t(n/2)$ errors.

Beside simplicity and efficiency, another advantage of these codes is that they do not require the Z-channel to be perfect, i.e., it is allowed to have $0 \rightarrow 1$ errors with very small probability (as long as this probability is smaller than the probability of $1 \rightarrow 0$ errors). All these properties make these codes very useful in practice.

VI. Asymptotic Efficiencies

In this section, given $0 < p, q_e < 1$, we study the asymptotic behavior of $\eta_\alpha(n, p, q_e)$ and $\eta_\beta(n, p, q_e)$ as $n \rightarrow \infty$, i.e., $\lim_{n\rightarrow\infty} \eta_\alpha(n, p, q_e)$ and $\lim_{n\rightarrow\infty} \eta_\beta(n, p, q_e)$. By the definition of nonuniform and uniform codes, the 'balls' containing up to $t(\mathbf{x})$ (or t) errors that are centered at codewords $\mathbf{x}$ need to be disjoint.

Before giving the asymptotic efficiencies, we first present the following known result: For any $\delta > 0$, when n is large enough, we have

$$2^{n(H(\frac{k}{n}) - \delta)} \leq \binom{n}{k} \leq 2^{n(H(\frac{k}{n}) + \delta)}$$

where $H(p)$ is the entropy function with

$$H(p) = p \log \frac{1}{p} + (1-p) \log \frac{1}{1-p} \text{ for } 0 \leq p \leq 1$$

and

$$H(p) = 0 \text{ for } p > 1 \text{ or } p < 0$$

Lemma 12. *Let $A(n, d, w)$ be the maximum size of a constant-weight binary code of codeword length n, whose Hamming weight is w and minimum distance is d. Let $R(n, t, w)$ be the maximum size of a binary code with Hamming weight w and codeword length n where every codeword can correct t asymmetric errors. Then*

$$R(n, t, w) = A(n, 2(t+1), w).$$

Proof: Let C be a code of length n, constant weight w and size $R(n, t, w)$ that corrects t asymmetric errors. $\forall \mathbf{x}, \mathbf{y} \in C$, by Lemma 2, we know that $S_t(\mathbf{x}) \bigcap S_t(\mathbf{y}) = \emptyset$.

Let $\mathbf{u} = (u_1, \ldots, u_n)$ be a vector such that $u_i = \min\{x_i, y_i\}$ for $1 \leq i \leq n$. Then $N(\mathbf{x}, \mathbf{u}) = N(\mathbf{y}, \mathbf{u})$ and $\mathbf{u} \notin S_t(\mathbf{x}) \bigcap S_t(\mathbf{y})$. W.l.o.g, suppose that $\mathbf{u} \notin S_t(\mathbf{x})$. Then $N(\mathbf{x}, \mathbf{u}) > t$, and the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$ is

$$d(\mathbf{x}, \mathbf{y}) = N(\mathbf{x}, \mathbf{u}) + N(\mathbf{y}, \mathbf{u}) \geq 2(t+1).$$

So the minimum distance of C is at least $2(t+1)$. As a result, $A(n, 2(t+1), w) \geq R(n, t, w)$.

On the other hand, if a constant-weight code has minimum distance at least $2(t+1)$, it can correct t asymmetric errors. As a result, $R(n, t, w) \geq A(n, 2(t+1), w)$. ■

A. Bounds of $\lim_{n\rightarrow\infty} \eta_\alpha(n, p, q_e)$

Let's first give the lower bound of $\lim_{n\rightarrow\infty} \eta_\alpha(n, p, q_e)$ and then provide the upper bound.

Theorem 13 (Lower bound)**.** *Given $0 < q_e < 1$, if $0 < p \leq \frac{1}{4}$, we have*

$$\eta_\alpha(n, p, q_e)_{n\rightarrow\infty} \geq 1 - H(2p).$$

Proof: Based on the definition of uniform codes, we have $t = \min\{s | B(s, n, p) \geq 1 - q_e\}$.

According to Hoeffding's inequality, for any $\delta > 0$, as n becomes large enough, we have $(p - \delta)n \leq t \leq (p + \delta)n$. Let $t = \gamma n$, when n is large enough, we have $p - \delta \leq \gamma \leq p + \delta$.

Now let each codeword tolerate t asymmetric errors. Then

$$B_\alpha(n, p, q_e) = B_\alpha(n, t) \geq R(n, t, w) = A(n, 2(t+1), w)$$

for every w with $0 \leq w \leq n$. The Gilbert Bound gives that (see Graham and Sloane [23])

$$A(n, 2(t+1), w) \geq \frac{\binom{n}{w}}{\sum_{i=0}^{t}\binom{w}{i}\binom{n-w}{i}}.$$

Hence

$$\begin{aligned} B_\alpha(n,p,q_e) &\geq \max_w \frac{\binom{n}{w}}{\sum_{i=0}^{t}\binom{w}{i}\binom{n-w}{i}} \\ &\geq \max_w \frac{\binom{n}{w}}{n \max_{i\in[0,t]}\binom{w}{i}\binom{n-w}{i}} \\ &\geq \max_{w:\frac{w(n-w)}{n}>t} \frac{\binom{n}{w}}{n \max_{i\in[0,t]}\binom{w}{i}\binom{n-w}{i}} \\ &\geq \max_{w:\frac{w(n-w)}{n}>t} \frac{\binom{n}{w}}{n\binom{w}{t}\binom{n-w}{t}} \end{aligned}$$

For a binomial term $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ and $\delta > 0$, when n is large enough,

$$2^{n(H(\frac{k}{n})-\delta)} \leq \binom{n}{k} \leq 2^{n(H(\frac{k}{n})+\delta)}$$

Let $w = \theta n$ and $t = \gamma n$ with $0 \leq \theta, \gamma \leq 1$, as n becomes large enough, we have

$$\begin{aligned} &\eta_\alpha(n,p,q_e) \\ \geq\ & \frac{1}{n}\log \max_{\theta:\theta(1-\theta)>\gamma} \frac{2^{(H(\theta)-\delta)n}}{n2^{(H(\frac{\gamma}{\theta})+\delta)\theta n}2^{(H(\frac{\gamma}{1-\theta})+\delta)(1-\theta)n}} \\ \geq\ & \max_{\theta:\theta(1-\theta)\geq\gamma} H(\theta) - \theta H(\frac{\gamma}{\theta}) - (1-\theta)H(\frac{\gamma}{1-\theta}) - 2\delta \\ & +\frac{1}{n}\log\frac{1}{n} \end{aligned}$$

Since $\theta(1-\theta) \geq \gamma$, we know that $\theta > \gamma > 0$; then $H(\frac{\gamma}{\theta})$ is a continuous function of γ. As n becomes large, we have $p - \delta \leq \gamma \leq p + \delta$, so we can approximate $H(\frac{\gamma}{\theta})$ with $H(\frac{p}{\theta})$. Similarly, we can approximate $H(\frac{\gamma}{1-\theta})$ with $H(\frac{p}{1-\theta})$. Then we can get

$$\eta_\alpha(n,p,q_e) \gtrsim \max_{\theta:\theta(1-\theta)>p} H(\theta) - \theta H(\frac{p}{\theta}) - (1-\theta)H(\frac{p}{1-\theta}).$$

If $0 \leq p \leq \frac{1}{4}$, the maximum value can be achieve at $\theta^* = \frac{1}{2}$. Hence we have $\eta_\alpha(n,p,q_e)_{n\to\infty} \geq 1 - H(2p)$. This completes the proof. ■

Theorem 14 (Upper Bound)**.** *Given* $0 < p, q_e < 1$*, we have*

$$\eta_\alpha(n,p,q_e)_{n\to\infty} \leq (1+p)[1 - H(\frac{p}{1+p})].$$

Proof: For an uniform (n, p, q_e) code correcting t asymmetric errors, we have the following observations:

1) There is at most one codeword of Hamming weight not more than t;
2) For $t + 1 \leq w \leq n$, the number of codewords of Hamming weight w is at most $\frac{\binom{n}{w-t}}{\binom{w}{t}}$.

Consequently, the total number of codewords is

$$\begin{aligned} B_\alpha(n,p,q_e) &\leq 1 + \sum_{w=t+1}^{n}\frac{\binom{n}{w-t}}{\binom{w}{t}} \\ &= 1 + \sum_{w=t+1}^{n}\frac{\binom{n+t}{w}}{\binom{n+t}{t}} \leq \frac{2^{n+t}}{\binom{n+t}{t}}. \end{aligned}$$

So when n is sufficiently large, we have

$$\begin{aligned} \eta_\alpha(n,p,q_e) &\leq \frac{1}{n}\log[\frac{2^{n+t}}{\binom{n+t}{t}}] \\ &\leq \frac{1}{n}\log\frac{2^{(1+\gamma)n}}{2^{H(\frac{\gamma}{1+\gamma})(1+\gamma)n}} \\ &= (1+\gamma) - H(\frac{\gamma}{1+\gamma})(1+\gamma) \\ &\sim (1+p)[1 - H(\frac{p}{1+p})] \end{aligned}$$

where the last step is due to the continuousness of $(1+\gamma) - H(\frac{\gamma}{1+\gamma})(1+\gamma)$ over γ. ■

We see that when $n \to \infty$, $\eta_\alpha(n,p,q_e)$ does not depends on q_e as long as $0 < q_e < 1$. That is because that when $n \to \infty$, we have $t \to pn$, which does not depend on q_e. This property is also hold by $\eta_\beta(n,p,q_e)$ when $n \to \infty$.

B. Bounds of $\lim_{n\to\infty}\eta_\beta(n,p,q_e)$

In this subsection, we study the bounds of the asymptotic efficiency of nonuniform codes. Here, we use the same idea as that for uniform codes, except we need also prove that the 'edge effect' can be ignored, i.e., the number of codewords with Hamming weight $w \ll n$ does not affect the final result.

Theorem 15 (Lower bound)**.** *Given* $0 < p, q_e < 1$*, we have*

$$\eta_\beta(n,p,q_e)_{n\to\infty} \geq \max_{0\leq\theta\leq 1-p} H(\theta) - \theta H(p) - (1-\theta)H(\frac{p\theta}{1-\theta}).$$

Proof: According to the definition of nonuniform codes, we have that

$$t(w) = \min\{s|B(s,w,p) \geq 1 - q_e\}$$

Based on Hoeffding's inequality, for any $\delta > 0$, as w becomes large enough, we have $(p-\delta)w \leq t(w) \leq (p+\delta)w$. In another word, for any $\epsilon, \delta > 0$, when n is large enough and $w \geq \epsilon n$, we have $(p-\delta)w \leq t(w) \leq (p+\delta)w$.

Let $w = \theta n$ and $t(w) = \gamma w$, then when n is large enough, if $\theta > \epsilon$, we have

$$(p-\delta) \leq \gamma \leq (p+\delta)$$

If $\theta < \epsilon$, we call it edge effect. In this case $0 \leq \gamma \leq 1$.

Now, let each codeword with Hamming weight w tolerate $t(w)$ errors, then

$$B_\beta(n,p,q_e) \geq R(n, t(w), w) \geq A(n, 2(t(w)+1), w)$$

for every w with $0 \leq w \leq n$.

Applying Gilbert Bound, we have

$$\begin{aligned} B_\beta(n,p,q_e) &\geq \max_w \frac{\binom{n}{w}}{\sum_{i=0}^{t(w)}\binom{w}{i}\binom{n-w}{i}} \\ &\geq \max_w \frac{\binom{n}{w}}{\max_{i\in[0,t(w)]} n\binom{w}{i}\binom{n-w}{i}} \\ &\geq \max_{w:\frac{w(n-w)}{n}\geq t(w)} \frac{\binom{n}{w}}{n\binom{w}{t(w)}\binom{n-w}{t(w)}} \end{aligned}$$

When n is large enough, we have

$$\begin{aligned}
&\eta_\beta(n,p,q_e)\\
\geq\ & \frac{1}{n}\log\max_{\theta:(1-\theta)\geq\gamma}\frac{2^{(H(\theta)-\delta)n}}{n2^{(H(\gamma)+\delta)\theta n}2^{(H(\frac{\gamma\theta}{1-\theta})+\delta)(1-\theta)n}}\\
\geq\ & \max_{\theta:(1-\theta)\geq\gamma} H(\theta)-\theta H(\gamma)-(1-\theta)H(\frac{\gamma\theta}{1-\theta})\\
& -2\delta+\frac{1}{n}\log\frac{1}{n}\\
\sim\ & \max_{\theta:(1-\theta)\geq\gamma} H(\theta)-\theta H(\gamma)-(1-\theta)H(\frac{\gamma\theta}{1-\theta})
\end{aligned}$$

Note that when $\theta<\epsilon$ for small ϵ, we have

$$H(\theta)-\theta H(\gamma)-(1-\theta)H(\frac{\gamma\theta}{1-\theta})\sim 0$$

So we can ignore this edge effect. That implies that we can write

$$p-\delta\leq\gamma\leq p+\delta$$

for any θ with $0\leq\theta\leq 1$.

Since $1-\theta\geq\gamma>0$, we know that for any fixed θ, $H(\theta)-\theta H(\gamma)-(1-\theta)H(\frac{\gamma\theta}{1-\theta})$ is a continuous function of γ. When n is large enough and δ is small enough, we have

$$\eta_\beta(n,p,q_e)\gtrsim\max_{\theta:(1-\theta)\geq p} H(\theta)-\theta H(p)-(1-\theta)H(\frac{p\theta}{1-\theta})$$

This completes the proof. ∎

Theorem 16 (Upper bound)**.** *Given* $0<p,q_e<1$*, we have*

$$\begin{aligned}
\eta_\beta(n,p,q_e)_{n\to\infty} &\leq \max_{0\leq\theta\leq 1} H((1-p)\theta)-\theta H(p)\\
&= H(\frac{1}{2^{s(p)}+1})+\frac{s(p)}{2^{s(p)}+1}
\end{aligned}$$

with $s(p)=H(p)/(1-p)$*.*

Proof: Using the same notations as above. Similar as the proof in Theorem 14, given (n,p,q_e), the maximal total number of codewords is

$$\begin{aligned}
B_\beta(n,p,q_e) &\leq 1+\sum_{w=\overline{h}(0)+1}^{n}\frac{\binom{n}{w-t(w)}}{\binom{w}{t(w)}}\\
&= \sum_{w=\overline{h}(0)}^{n}\frac{\binom{n}{w-t(w)}}{\binom{w}{t(w)}}\\
&\leq \max_{w} n\frac{\binom{n}{w-t(w)}}{\binom{w}{t(w)}}
\end{aligned}$$

When n is large enough, we have

$$\begin{aligned}
\eta_\beta(n,p,q_e) &\leq \frac{1}{n}\log\max_{0\leq\theta\leq 1} n\frac{2^{H((1-\gamma)\theta+\delta)n}}{2^{(H(\gamma)\theta-\delta)n}}\\
&= \max_{0\leq\theta\leq 1} H((1-\gamma)\theta)-\theta H(\gamma)\\
&\quad +2\delta+\frac{1}{n}\log n\\
&\sim \max_{0\leq\theta\leq 1} H((1-\gamma)\theta)-\theta H(\gamma)
\end{aligned}$$

Note that when $\theta<\epsilon$ for small ϵ, we have

$$H((1-\gamma)\theta)-\theta H(\gamma)\sim 0$$

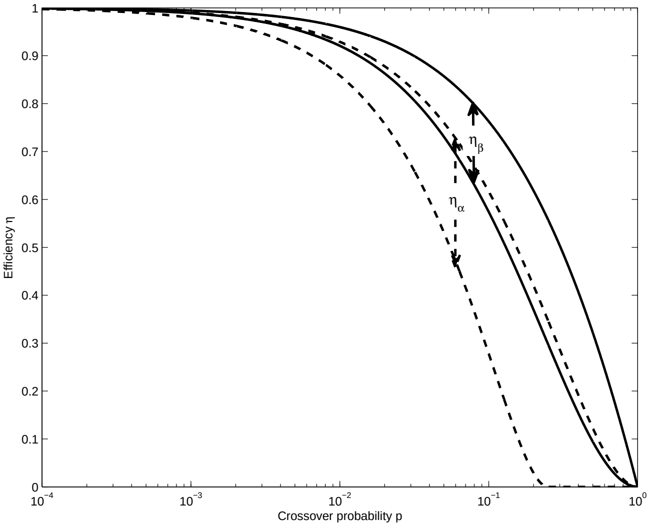


Fig. 4. Bounds to $\eta_\alpha(n,p,q_e)_{n\to\infty}$ and $\eta_\beta(n,p,q_e)_{n\to\infty}$. The dashed curves represent the lower and upper bounds to $\eta_\alpha(n,p,q_e)_{n\to\infty}$, and the solid curves represent the lower and upper bounds to $\eta_\beta(n,p,q_e)_{n\to\infty}$.

So we can ignore the edge effect. That implies that we can write

$$p-\delta\leq\gamma\leq p+\delta$$

for any θ with $0\leq\theta\leq 1$.

Since for any fixed θ with $0\leq\theta\leq 1$, $H((1-\gamma)\theta)-\theta H(\gamma)$ is a continuous function of γ. When n is large enough and δ is small enough, we have

$$\eta_\beta(n,p,q_e)\lesssim\max_{0\leq\theta\leq 1} H((1-p)\theta)-\theta H(p)$$

which equals to

$$H(\frac{1}{2^{s(p)}+1})+\frac{s(p)}{2^{s(p)}+1}$$

with $s(p)=H(p)/(1-p)$. This completes the proof. ∎

C. Comparison of Asymptotic Efficiencies

Table I summarizes the upper bounds and lower bounds of $\eta_\alpha(n,p,q_e)_{n\to\infty}$ and $\eta_\beta(n,p,q_e)_{n\to\infty}$ obtained in this section. We plot them in Fig. 4. The gap between the bounds for the two codes indicate the potential improvement in efficiency by using the nonuniform codes (compared to using uniform codes) when the codeword length is large. We see that the upper bound in Theorem 16 is also the capacity of the Z-channel, derived in [24]. It means that nonuniform codes may be able to achieve the Z-channel capacity as n becomes large, while uniform codes cannot.

VII. Conclusion

In storage systems with asymmetric errors, it is very desirable to design a code such that the reliability of the worst codeword is guaranteed and the size of the code is maximized. This motivates us to propose the concept of nonuniform codes,

	Lower Bound	Upper Bound
$\eta_\alpha(n,p,q_e)_{n\to\infty}$	$[1-H(2p)]I_{0\leq p\leq \frac{1}{4}}$	$(1+p)[1-H(\frac{p}{1+p})]$
$\eta_\beta(n,p,q_e)_{n\to\infty}$	$\max_{0\leq\theta\leq 1-p} H(\theta)-\theta H(p)-(1-\theta)H(\frac{p\theta}{1-\theta})$	$\max_{0\leq\theta\leq 1} H((1-p)\theta)-\theta H(p)$

TABLE I

whose codewords can tolerate different numbers of asymmetric errors depending on their Hamming weights, so that all codewords can achieve (almost the same) high reliability. In this paper, we give an almost explicit upper bound for the sizes of nonuniform codes and study the asymptotic efficiency of nonuniform codes and uniform codes, which shows the potential performance gain by nonuniform codes. We also present two general constructions of nonuniform codes, including layered codes and flipping codes. Since more needs to be known on the efficient mapping between information bits and codewords for layered codes, and the efficiency of flipping codes still needs improvement when p is not small, how to design simple and efficient nonuniform codes is still an open problem.

References

[1] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck. “Codes for asymmetric limited-magnitude errors with application to multilevel flash memories,” *IEEE Trans. Inform. Theory*, vol. 56, no. 4, pp. 1582-1595, 2010.

[2] T. Kløve, “Error correcting codes for the asymmetric channel,” Technical Report, Dept. of Informatics, University of Bergen, 1981. (Updated in 1995.)

[3] K. A. S. Abdel-Ghaffar and H. C. Ferreira, “Systematic encoding of the VarshamovCTenengolts codes and the Constantin-Rao codes,” *IEEE Trans. Inform. Theory*, vol. 44, pp. 340-345, Jan. 1998.

[4] B. Bose and S. Al-Bassam, “On systematic single asymmetric errorcorrecting codes,” *IEEE Trans. Inform. Theory*, vol. 46, pp. 669-672, Mar. 2000.

[5] 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.

[6] 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.

[7] T. Etzion, “Lower bounds for asymmetric and unidirectional codes,” *IEEE Trans. Inform. Theory*, vol. 37, pp. 1696-1704, Nov. 1991.

[8] 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.

[9] 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.

[10] F. Fu, S. Ling, and C. Xing, “New lower bounds and constructions for binary codes correcting asymmetric errors’”, *IEEE Trans. Inform. Theory*, vol. 49, pp. 3294-3299, Dec. 2003.

[11] C. Wang, S. R. Kulkarni, and H. V. Poor, “Density evolution for asymmetric memoryless channels,” *IEEE Trans. Inform. Theory*, vol. 51, pp. 4216-4236, Dec. 2005.

[12] R. R. Varshamov, “Some features of linear codes that correct asymmetric errors” (in Russian), *Doklady Akad. Nauk. SSSR*, vol. 157, no. 3, pp. 546-548, 1964. (Trans: *Soviet Physics-Doklady 9*, pp. 538-540, 1965.)

[13] P. Delsarte and P. Piret, “Bounds and constructions for binary asymmetric error correcting codes,” *IEEE Trans. Inform. Theory*, vol. 27, no. 1, pp. 125-128, Jan. 1981.

[14] J. H. Weber, C. de Vroedt, and D. E. Beokee, “New upper bounds on the size of codes correcting asymmetric errors,” *IEEE Trans. Inform. Theory*, vol. 33, no. 3, pp. 434-437, 1987.

[15] J. H. Weber, C. de Vroedt, and D. E. Beokee, “Bounds and constructions for binary codes of length less than 24 and asymmetric distance less than 6,” *IEEE Trans. Inform. Theory*, vol. 34, no. 5, pp. 1321-1331, 1988.

[16] T. Kløve, “Upper bounds on codes correcting asymmetric errors,” *IEEE Trans. Inform. Theory*, vol. 27, no. 1, pp. 128-131, 1981.

[17] R. R. Varshamov, “A class of codes for asymmetric channels and a problem from the additive theory of numbers,” *IEEE Trans. Inform. Theory*, vol. 19, no. 1, pp. 92-95, 1973.

[18] 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.

[19] P. Delsarte and P. Piret, “Bounds and constructions for binary asymmetric error-correcting codes,” *IEEE Trans. Inform. Theory*, vol. 27, pp. 125-128, 1981.

[20] J. H. Weber, C. de Vroedt, and D. E. Boekee, “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.

[21] 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. 19, pp. 137, Jan. 1973.

[22] I. Krasikov and S. Litsyn, “On spectra of BCH codes,” *IEEE Trans. Inform. Theory*, vol. 41, pp. 786-788, May 1995.

[23] R. L. Graham, and N. J. A. Sloane, “Lower bounds for constant weight codes,” *IEEE Trans. Inform. Theory*, vol. 26, no. 1, pp. 37-43, 1980.

[24] S. Verdú, “Channel Capacity,” Ch. 73.5 in the *Electrical Enginnering Handbook*, IEEE and CRC Press, pp. 1671-1678, 1997.