Bounds on the Probability of Undetected Error for q-Ary Codes

Xuan Wang, Huizhou Liu, Patrick Solé

entropy

MDPI

Article

Bounds on the Probability of Undetected Error for q-Ary Codes

Xuan Wang [1], Huizhou Liu [2] and Patrick Solé [3,*]

[1] School of Mathematical Sciences, Anhui University, Hefei 230601, China; wang_xuan_ah@163.com
[2] State Grid Anhui Electric Power Co., Ltd., Hefei 230601, China; 18756027866@163.com
[3] I2M, CNRS, Aix-Marseille Univetsity, Centrale Marseille, 13009 Marseilles, France
* Correspondence: patrick.sole@telecom-paris.fr

Abstract: We study the probability of an undetected error for general q-ary codes. We give upper and lower bounds on this quantity, by the Linear Programming and the Polynomial methods, as a function of the length, size, and minimum distance. Sharper bounds are obtained in the important special case of binary Hamming codes. Finally, several examples are given to illustrate the results of this paper.

Keywords: error correcting codes; probability of undetected error; linear programmming

1. Introduction

Let $A = \{a_1, \ldots, a_q\}$ be an *alphabet* with q distinct symbols, where $q \geqslant 2$ and the alphabet do not have any structure. For instance, A can be $\mathbb{F}_q$, the finite field with q elements, or $\mathbb{Z}_q$, the ring of integers modulo q. Moreover, a linear $[n, k]$ code is a subspace of the vector space $\mathbb{F}_q^n$ and k is the dimension of the subspace. For every two vectors $\boldsymbol{x}$, $\boldsymbol{y} \in A^n$, the (Hamming) distance $d_H(\boldsymbol{x}, \boldsymbol{y})$ between $\boldsymbol{x}$ and $\boldsymbol{y}$ is defined as the number of coordinates where they are different. A nonempty subset C of A^n with cardinality M is called a q-ary (n, M) code, whose elements are called *codewords*. The minimum distance d of the code C is the minimum distance between any two different codewords in C. The distance distribution of C is defined as

$$A_i = \frac{1}{M}|\{(\boldsymbol{x}, \boldsymbol{y}) : \boldsymbol{x}, \boldsymbol{y} \in C, d_H(\boldsymbol{x}, \boldsymbol{y}) = i\}|, \quad i = 0, 1, \ldots, n. \tag{1}$$

Assume that the code C is used for error detection on a discrete memoryless channel with q inputs and q outputs. Each symbol transmitted has a probability $1 - p$ of being received correctly and a probability $p_q = p/(q-1)$ of being transformed into each of the $q - 1$ other symbols. It is natural to let $0 \leqslant p \leqslant (q-1)/q$. Such a channel model is called a q-ary symmetric channel $qSC(p)$. When such a code is used on the symmetric q-ary channel $qSC(p)$, errors occur with a probability $\frac{p}{q-1}$ per symbol.

Let $\boldsymbol{x} \in C$ be the codeword transmitted and $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e} \in \mathbb{F}_q^n$ be the vector received, where $\boldsymbol{e} = \boldsymbol{y} - \boldsymbol{x}$ is the error vector from the channel noise. Obviously, $\boldsymbol{e} \in C$ if and only if $\boldsymbol{y} \in C$. Note that the decoder will accept $\boldsymbol{y}$ as error free if $\boldsymbol{y} \in C$. Clearly, this decision is wrong, and such an error is not detected. Thus, when error detection is being used, the decoder will make a mistake and accept a codeword which is not the one transmitted if and only if the error vector is a nonzero codeword [1,2]. In this way, the probability that the decoder fails to detect the existence of an error is called the probability of undetected error and denoted by $P_{ue}(C, p)$, which is defined as

$$P_{ue}(C, p) = \sum_{j=1}^{n} A_j \left(\frac{p}{q-1}\right)^j (1-p)^{n-j}. \tag{2}$$

Citation: Wang, X.; Liu, H.; Solé, P. Bounds on the Probability of Undetected Error for q-Ary Codes. *Entropy* **2023**, *25*, 1349. https://doi.org/10.3390/e25091349

Academic Editor: T. Aaron Gulliver

Received: 13 August 2023
Revised: 13 September 2023
Accepted: 15 September 2023
Published: 17 September 2023

In general, the smaller the probability of undetected error P_{ue} for some p, the better the code performs in error detection. However, this function is difficult to characterize in general.

As for the code C, comparing its P_{ue} with the average probability $\overline{P_{ue}}$ [3,4] for the ensemble of all q-ary linear $[n,k]$ codes is a natural way to decide whether C is suitable for error detection or not, where

$$\overline{P_{ue}}(p) = q^{-(n-k)}\Big(1-(1-p)^k\Big).$$

According to [4], there exists a code C such that $P_{ue}(C,p) > q^{-(n-k)}$ and there are many codes, the P_{ue} of each of whom is smaller than $q^{-(n-k)}$. In fact, it was commonly assumed that $P_{ue}(C,p) \leqslant q^{-(n-k)}$ for the linear $[n,k]$ code C in [5], where $q^{-(n-k)} = q^{-r}$ is called the q^{-r} bound. The q^{-r} bound is satisfied for certain specific codes, e.g., Hamming codes and binary perfect codes, when $0 < p < 1/2$.

For the worst channel condition, i.e., when $p = (q-1)/q$,

$$P_{ue}\left(C, \frac{q-1}{q}\right) = q^{-(n-k)}\left(1-\left(1-\frac{q-1}{q}\right)^k\right) = \overline{P_{ue}}\left(\frac{q-1}{q}\right).$$

From the above formula, a code C is called *good* if $P_{ue}(C,p) \leqslant P_{ue}((q-1)/q)$ for all $0 < p < (q-1)/q$. In particular, if $P_{ue}(C,p)$ is an increasing function of p in the interval $[0,(q-1)/q]$, then the code is good, and the code is called *proper*. There are many proper codes [1], for example, perfect codes (and their extended codes and their dual codes), primitive binary 2-error correcting BCH codes, a class of punctured of Simplex codes, MDS codes, and near MDS codes (see [5–9] for details). Moreover, for practical purposes, a *good* binary code C may be defined a bit different, i.e., $P_{ue}(C,p) \leqslant cP_{ue}(C,1/2)$ for every $0 \leqslant p \leqslant 1/2$ and a reasonably small $c \geqslant 1$. Furthermore, an infinite class $\mathcal{C}$ of binary codes is called *uniformly good* if there exists a constant c such that for every $0 \leqslant p \leqslant 1/2$ and $C \in \mathcal{C}$, the inequality $P_{ue}(C,p) \leqslant cP_{ue}(C,1/2)$ holds. Otherwise, it is called *ugly*, for example, some special Reed–Muller codes are ugly (see [10]).

Another way to assess the performance of a code for error detection is to give bounds of the probability of undetected error. In [11], Abdel-Ghaffar defined the *combinatorial invariant* F_j of the code C and proved that

$$P_{ue}(C,p) = \sum_{j=1}^{n} F_j \left(\frac{p}{q-1}\right)^j \left(1-\frac{qp}{q-1}\right)^{n-j},$$

where

$$F_j = \sum_{i=1}^{j} A_i \binom{n-i}{n-j},\ j = 1,2,\ldots,n.$$

Using combinatorial arguments, Abdel-Ghaffar [11] obtained a lower bound on the undetected error probability $P_{ue}(C,p)$. Later, Ashikhmin and Barg called F_j the binomial moments of the distance function and derived more bounds for P_{ue} (see [12,13]).

In particular, constant weight codes are attractive and many bounds are developed, for example, binary constant weight codes (see [14,15]) and q-ary constant weight codes (see [16]). In fact, the probability of an undetected error for binary constant weight codes has been studied and can be given explicitly (see [14,16]).

Note that when $A = \mathbb{F}_q$ and $p \to 0$, according to Equation (2), we have

$$P_{ue}(C,p) \sim A_d {p_q}^d (1-p)^{n-d}, \tag{3}$$

where $p_q = p/(q-1)$, d is the minimum distance of C and A_d is called the *kissing number* of the linear code C. In 2021, Solé et al. [17] studied the kissing number by Linear Programming and the Polynomial Method. They gave bounds for A_d under different conditions

and made tables for some special parameters. Motivated by the work, this paper is devoted to studying the function P_{ue} using the same techniques.

The rest of this paper is organized as follows. In Section 2, we briefly give the definition of the (dual) distance distribution of q-ary codes and give some trivial bounds of the probability of an undetected error. In Section 3.1, linear programming bounds are discussed. The applications of Krawtchouk polynomial (Polynomial Method) to error detection are given in Section 3.2. In Section 4, some bounds better than the 2^{-m} bound are given for binary Hamming codes. Finally, we end with some concluding remarks in Section 5.

2. Preliminaries

Recall some basic definitions and notations from [2,18–20]. Throughout this paper, to simplify some formulas, we let $p_q = \frac{p}{q-1}$ and $k = \log_q |C|$ for some real k. Furthermore, in this paper, it is natural to define $p < (q-1)(1-p)$, equivalently, $p_q < 1-p$.

2.1. Dual Distance Distribution

Assume that $A = \mathbb{F}_q$ is the finite field of size q and C is a subspace of $\mathbb{F}_q^n$, i.e., C is a linear code over $\mathbb{F}_q$. Then, the *dual code* $C^\perp$ of C is the orthogonal complement of the subspace C. That is to say,

$$C^\perp = \{\boldsymbol{v} \in \mathbb{F}_q^n : \boldsymbol{v} \cdot \boldsymbol{u} = 0 \text{ for all } \boldsymbol{u} \in C\},$$

where $\boldsymbol{v} \cdot \boldsymbol{u} = \sum_{i=1}^n v_i u_i$, $\boldsymbol{u} = (u_1, \ldots, u_n)$ and $\boldsymbol{v} = (v_1, \ldots, v_n)$. The distance distribution A'_i of $C^\perp$ can be determined similarly. It is well known (see Chapter 5. §2. in [2]) that

$$A'_i = \frac{1}{|C|} \sum_{i=0}^{n} A_j P_i(j), \tag{4}$$

where $P_i(j)$ denotes the Krawtchouk polynomial of degree i. For each integer $q \geqslant 2$, the *Krawtchouk polynomial* $P_k(x; n)$ is defined as

$$P_k(x; n) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j}.$$

When there is no ambiguity for n, the function $P_k(x; n)$ is often simplified to $P_k(x)$.

Note that Equation (4) holds when C is linear. When C is nonlinear, the *dual distance distribution* A'_i is defined by Equation (4). Furthermore, by the MacWilliams–Delsarte inequality,

$$A'_i \geqslant 0, \tag{5}$$

holds for all $i = 0, 1, \cdots, n$. Moreover, $A_0 = 1$ and

$$q^k = 1 + \sum_{j=1}^{n} A_j, \quad \text{when} \quad |C| = q^k. \tag{6}$$

2.2. Probability of Undetected Error

The *q-ary symmetric channel* with symbol probability p, where $0 \leqslant p \leqslant (q-1)/q$, is defined as follows: symbols from some alphabet A with q elements are transmitted over the channel, and

$$\mathcal{P}(b \text{ received} \mid a \text{ sent}) = \begin{cases} 1-p, & b = a, \\ \frac{p}{q-1}, & b \neq a, \end{cases}$$

where $\mathcal{P}(b \text{ received} \mid a \text{ sent})$ is the conditional probability that b is received, given that a is sent. For a q-ary code C, when it is used on such a channel, it is possible that the decoder fails to detect the existence of the errors. Thus, P_{ue}, the function in terms of the weight distribution of C is given in Equation (2). Clearly, this is a difficult computational problem

for large parameters n, k, d, and q (see [2]). Hence, it is better to give bounds for P_{ue}. For example, here are some trivial bounds.

Theorem 1. *For every q-ary code C with $|C| = q^k$, if $p < (q-1)(1-p)$, then*

$$(q^k - 1){p_q}^n \leqslant P_{ue}(C, p) \leqslant (q^k - 1){p_q}^d (1-p)^{n-d},$$

where $p_q = \frac{p}{q-1}$. Especially, when $q = 2$ and $0 < p < \frac{1}{2}$, we have

$$(2^k - 1)p^n \leqslant P_{ue}(C, p) \leqslant (2^k - 1)p^d (1-p)^{n-d}.$$

Proof. It is easy to check that ${p_q}^j (1-p)^{n-j} > {p_q}^{j+1}(1-p)^{n-j-1}$ if and only if $p < (q-1)(1-p)$. Hence,

$$P_{ue} = \sum_{j=d}^{n} A_j {p_q}^j (1-p)^{n-j} \leqslant {p_q}^d (1-p)^{n-d} \sum_{j=d}^{n} A_j = (q^k - 1){p_q}^d (1-p)^{n-d},$$

since ${p_q}^j (1-p)^{n-j} \leqslant {p_q}^d (1-p)^{n-d}$ when $j \geqslant d$. The lower bound can be obtained similarly. □

The above bounds are trivial. However, they are both tight, because simplex codes over the finite field $\mathbb{F}_q$ attain these bounds.

2.3. Some Special Bounds

It is clear that the general bounds given by Theorem 1 will be much larger (or smaller) than the true value of P_{ue} for a fixed code. If the distance distribution is known, one computes $P_{ue}(C, p)$ (as a function of p), and if we know some particular information about the distance distribution, then we may get some bounds. The following is a special case and more thoughts can be seen in Section 4.

Theorem 2. *Let C be a binary code with $A_n = 1$ and $A_i = A_{n-i}$ for $1 \leqslant i \leqslant n-1$, then*

$$P_{ue} = \begin{cases} p^n + \sum_{j=d}^{t} A_j \left(p^j (1-p)^{n-j} + p^{n-j}(1-p)^j\right), & n = 2t+1, \\ p^n + A_t p^t (1-p)^t + \sum_{j=d}^{t-1} A_j \left(p^j (1-p)^{n-j} + p^{n-j}(1-p)^j\right), & n = 2t. \end{cases} \tag{7}$$

Moreover, when $d \leqslant t$, we have

$$P_{ue} \leqslant \begin{cases} p^n + \left(2^{k-1} - 1\right)\left(p^d (1-p)^{n-d} + p^{t+1}(1-p)^t\right), & n = 2t+1, \\ p^n + A_t p^t (1-p)^t + \left(2^{k-1} - \frac{A_t}{2} - 1\right)\left(p^d (1-p)^{n-d} + p^{t+1}(1-p)^{t-1}\right), & n = 2t, \end{cases}$$

and

$$P_{ue} \geqslant \begin{cases} p^n + \left(2^{k-1} - 1\right)\left(p^t (1-p)^{t+1} + p^{n-d}(1-p)^d\right), & n = 2t+1, \\ p^n + A_t p^t (1-p)^t + \left(2^{k-1} - \frac{A_t}{2} - 1\right)\left(p^{t-1} (1-p)^{t+1} + p^{n-d}(1-p)^d\right), & n = 2t, \end{cases}$$

where $0 < p < \frac{1}{2}$ and $d \leqslant t$.

Proof. By the definition of P_{ue}, Equation (7) holds if $A_i = A_{n-i}$ and $A_n = 1$. Due to $0 < p < \frac{1}{2}$, It is easy to check that $p^{n-j}(1-p)^j \leqslant p^j (1-p)^{n-j}$, where $0 \leqslant j \leqslant \lfloor n/2 \rfloor$. In addition, if $n = 2t+1$, then $\sum_{j=d}^{t} A_j = (2^k - 2)/2 = 2^{k-1} - 1$. Similarly for the case $n = 2t$. Hence, we get the bounds. □

Remark 1. *If the binary code C satisfies $A_i = A_{n-i}$ and $A_n = 0$, we can get the following bounds:*

$$P_{ue} \leqslant \begin{cases} 2^{k-1}\left(p^d(1-p)^{n-d}+p^{t+1}(1-p)^t\right), & n=2t+1, \\ A_t p^t(1-p)^t+\left(2^{k-1}-\frac{A_t+A_0}{2}\right)\left(p^d(1-p)^{n-d}+p^{t+1}(1-p)^{t-1}\right), & n=2t, \end{cases}$$

and

$$P_{ue} \geqslant \begin{cases} 2^{k-1}\left(p^t(1-p)^{t+1}+p^{n-d}(1-p)^d\right), & n=2t+1, \\ A_t p^t(1-p)^t+\left(2^{k-1}-\frac{A_t+A_0}{2}\right)\left(p^{t-1}(1-p)^{t+1}+p^{n-d}(1-p)^d\right), & n=2t. \end{cases}$$

Here, $\mathbf{0}$, the all zero vector, may not be a codeword.

Example 1. *For a binary linear code, if the all-one vector $\mathbf{1}$ is a codeword, then $A_i = A_{n-i}$. So, Theorem 2 can be applied to many codes, for example, Hamming codes. It is known that the binary Hamming code $\mathcal{H}_m$ is a linear $[n = 2^m - 1, k = 2^n - 1 - m, 3]$ code. The distance distribution of the $[15,\ 11,\ 3]$ Hamming code $\mathcal{H}_4$ is listed in Table 1. According to Theorem 2, the values of the bounds and true probability can be seen in Figure 1.*

Table 1. Distance Distribution of the Hamming Code $\mathcal{H}_4$.

i	0	3	4	5	6	7	8	9	10	11	12	15
A_i	1	35	105	168	280	435	435	280	168	105	35	1

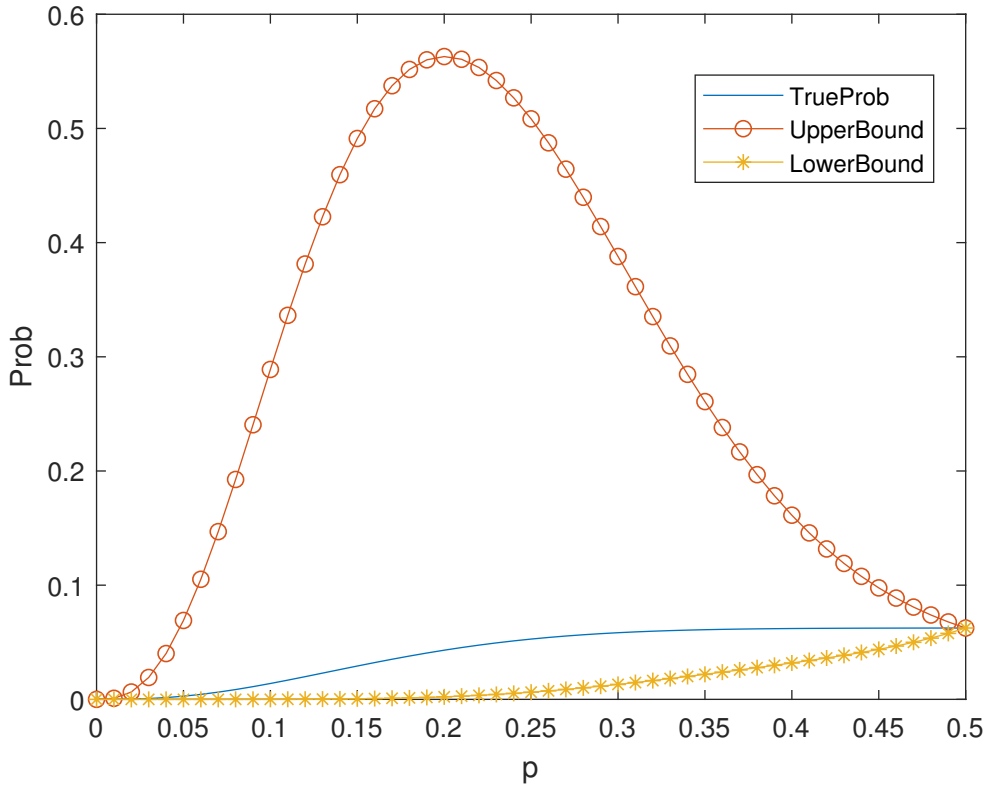

Figure 1. Bounds in Theorem 2 of P_{ue} for the Hamming Code $\mathcal{H}_4$.

3. Universal Bounds for q-Ary Codes

In this section, we will discuss the bounds for P_{ue} using different methods. These bounds are for general codes, thus they do not look so good. Meanwhile, compared with some known bounds, they do not perform better. However, it is the first as far as we know

to give bounds for P_{ue} using the following two methods, though they have been shown in [21,22] due to different thoughts.

3.1. Linear Programming Bounds

Consider the linear programming problem $M(n,k,d,p)$ that maximizes the objective function

$$\sum_{j=1}^{n} A_j {p_q}^j (1-p)^{n-j}$$

under the constraints:

(1) $A_j \geqslant 0$,
(2) $\sum_{j=1}^{n} A_j = q^k - 1$,
(3) $\sum_{j=1}^{n} A_j P_i(j) \geqslant -P_i(0)$,
(4) $A_1 = A_2 = \cdots = A_{d-1} = 0$.

Likewise, let $m(n,k,d,p)$ be the minimization of the same objective function under the same constraints.

Theorem 3. *If C is a q-ary code of parameters (n, q^k, d), then $m(n,k,d,p) \leqslant P_{ue} \leqslant M(n,k,d,p)$.*

Proof. The objective function expression comes from (2). Constraint (1) is immediate by the definition of the distance distribution. Constraints (2) and (3) come from Equation (6) and Equation (5), respectively. Constraint (4) is a consequence of the definition of minimum distance. □

Remark 2. *Let $f(x)$ and $g(x)$ be two functions of x, then $f \lesssim g$ if $f < g$ or $f \sim g$, when $x \to 0$, where $0 < x < 1$. For example, let $f(x) = x^2 + x$ and $g(x) = x^3 + x$, then $f(x) > g(x)$ when $0 < x < 1$. But $f(x) \sim g(x)$, then $f(x) \lesssim g(x)$ when $0 < x < 1$ and $x \to 0$.*

Motivated by Equation (3) and [17], we have the following result.

Theorem 4. *Let C be a q-ary $[n,k,d]_q$ linear code, then when $p \to 0$,*

$$(q^k - 1 - \lfloor L \rfloor) {p_q}^d (1-p)^{n-d} \leqslant P_{ue}(C,p) \lesssim (q^k - 1 - \lceil S \rceil) {p_q}^d (1-p)^{n-d}, \tag{8}$$

where L (resp. S) denotes the maximum (resp. minimum) of $\sum_{j=d+1}^{n} A_j$ subject to the $2n-d$ constraints

$$-P_i(0) - (q^k - 1) P_i(d) \leqslant \sum_{j=d+1}^{n} A_j (P_i(j) - P_i(d)),$$

for $i = 1, 2, \ldots, n$ and $j = d+1, d+2, \ldots, n$.

Proof. It is clear that $P_{ue}(C,p) \geqslant A^d {p_q}^d (1-p)^{n-d}$, then by [17], we get the left side of Equation (8). As for the right side, if $A_d < q^k - 1 - \lceil S \rceil$ and p is small enough, then by Equation (3), $P_{ue}(C,p) < (q^k - 1 - \lceil S \rceil) {p_q}^d (1-p)^{n-d}$. Otherwise, $A_d = q^k - 1 - \lceil S \rceil$ and then, $P_{ue}(C,p) \sim (q^k - 1 - \lceil S \rceil) {p_q}^d (1-p)^{n-d}$. □

Table 2 is a part of Table I in [17], which is helpful to give bounds for P_{ue}.

Table 2. Bounds of A_d for Some Binary Codes.

Parameters	**[9, 4, 4]**	**[10, 4, 4]**	**[11, 4, 5]**	**[12, 4, 6]**	**[13, 4, 6]**	**[14, 4, 7]**	**[15, 4, 8]**
Upper Bound	14	15	7	14	14	8	15
Lower Bound	6	12	5	11	4	8	15

Example 2. *Let C_1 be a binary $[15,\ 4,\ 8]$ code, then*

$$P_{ue}(C_1, p) \sim 15p^8(1-p)^7.$$

As for the binary $[12,\ 4,\ 6]$ code C_2, we have

$$11p^6(1-p)^6 < P_{ue}(C_2, p) < 14p^6(1-p)^6.$$

Obviously, for any $[n,\ k,\ d]$ code, one can give bounds for its P_{ue}.

Remark 3. *From the above discussion, it is clear that our bounds depend solely on the three parameters $[n,\ k,\ d]$ of the code, and $[n,\ k,\ d]$ is the minimal requirement to use a code in practice.*

3.2. Polynomial Method

In this section, we will give some general bounds for P_{ue} for any binary $(n, 2^k, d)$ code. Recall the definition of the Krawtchouk polynomials and some properties. The following identity is a Polynomial Method of expressing the duality of LP.

Lemma 1. *Let $\beta(x) \in \mathbb{Q}[x]$ be the polynomial whose Krawtchouk expansion is*

$$\beta(x) = \sum_{j=0}^{n} \beta_j P_j(x).$$

Then we have the following identity

$$\sum_{i=0}^{n} \beta(i) A_i = q^k \sum_{j=0}^{n} \beta_j A'_j. \tag{9}$$

Proof. Immediate by Equation (4), upon swapping the order of summation. □

From now on, we denote the coefficient of Krawtchouk expansion of the polynomial $f(x)$ of degree n by f_j, $j = 0, 1, \cdots, n$, i.e., $f(x) = \sum_{j=0}^{n} f_j P_j(x)$.

The first main result of this section is inspired by Theorem 1 in [23], and given as follows.

Theorem 5. *Let $\beta(x)$ and $\gamma(x)$ be polynomials over $\mathbb{Q}$ such that $\beta_j \leqslant 0$, $\gamma_j \geqslant 0$ for $j \geqslant 1$ and $\gamma(i) \leqslant {p_q}^i(1-p)^{n-i} \leqslant \beta(i)$ for all i with $A_i \neq 0$. Then we have the upper bound*

$$P_{ue} \leqslant q^k \beta_0 - \beta(0), \tag{10}$$

and the lower bound

$$P_{ue} \geqslant q^k \gamma_0 - \gamma(0). \tag{11}$$

Proof. By Lemma 1, we have

$$\sum_{j=0}^{n} A_j \beta(j) \leqslant \beta_0 q^k.$$

Returning to the definition of P_{ue} and using the property of $\beta(j) \geqslant {p_q}^j(1-p)^{n-j}$, we get

$$P_{ue} = \sum_{j=1}^{n} A_j {p_q}^j (1-p)^{n-j} \leqslant \sum_{j=1}^{n} A_j \beta(j) \leqslant q^k \beta_0 - \beta(0).$$

The proof of the lower bound is analogous and ommitted. □

Remark 4. *The above result is a special case of Proposition 5 in [22]. More general setting of the linear programming bounds from Section 3 (Theorem 5) were already considered in [21,22].*

The following are some properties of the Krawtchouk expansion, and we omit the proof, since they are not difficult.

Lemma 2 ([24] Corollary 3.13)**.** *Let $f(x) = \sum_{j=0}^{n} f_j P_j(x)$ and $g(x) = \sum_{j=0}^{n} g_j P_j(x)$ be polynomials over $\mathbb{Q}$, where $f_j \geqslant 0, g_j \geqslant 0$, $0 \leqslant j \leqslant n$. Then the coefficients of the Krawtchouk expansion of $\lambda f(x) + \mu g(x)$ are nonnegative, where λ, μ are nonnegative rational numbers.*

3.2.1. Upper Bounds

For convenience, let $\delta_{i,j}$ be the Kronecker symbol, i.e.,

$$\delta_{i,j} = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Lemma 3. *For general q, the coefficients of the Krawtchouk expansion of the following polynomial*

$$g_i(x) = \frac{(-1)^{i-1}}{(i-1)!(n-i)!} \frac{\prod_{j=1}^{n}(j-x)}{i-x},$$

are all nonnegative if and only if i is odd, where $1 \leqslant i \leqslant n$ is an integer and $0! = 1$. Moreover, $g_i(j) = \delta_{i,j}$.

Proof. Let

$$h(x) = \frac{q^{n-d+1}}{s-x} \prod_{j=d}^{n} \left(1 - \frac{x}{j}\right) = \sum_{j=0}^{n} h_j P_j(x),$$

where $d \leqslant s \leqslant n$. Then, by Proposition 5.8.2 in [20],

$$\begin{aligned} h_i &= \frac{1}{q^n} \sum_{j=0}^{n} h(j) P_j(i) = \frac{1}{q^{d-1}} \sum_{j=0}^{d-1} \binom{n-j}{n-d+1} \frac{P_j(i)}{s-j} \Big/ \binom{n}{d-1} \\ &\geqslant \frac{1}{q^{d-1} s} \sum_{j=0}^{d-1} \binom{n-j}{n-d+1} P_j(i) \Big/ \binom{n}{d-1} \\ &= \frac{1}{s} \binom{n-i}{d-1} \Big/ \binom{n}{d-1} \geqslant 0. \end{aligned}$$

Note that if $d = 1$, we have

$$h(x) = \frac{q^n}{n!} (-1)^{i-1} (i-1)!(n-i)! g_s(x).$$

According to Lemma 2, the coefficients of the Krawtchouk expansion of $(-1)^{i-1} g_i(x)$ are all nonnegative.

Obviously, for any $j \neq i$, $g_i(j) = 0$, because j is a root of $g_i(x)$. Moreover,

$$\begin{aligned} g_i(i) &= \frac{(-1)^{i-1}}{(i-1)!(n-i)!} \prod_{\ell=1}^{i-1} (\ell - i) \prod_{\ell=i+1}^{n} (\ell - i) \\ &= \frac{(-1)^{i-1}}{(i-1)!(n-i)!} \Big((-1)^{i-1} (i-1)!(n-i)! \Big) = 1, \end{aligned}$$

which means $g_i(j) = \delta_{i,j}$. □

Theorem 6. *Let C be a binary code with the distance distribution A_j, where $A_j = 0$ for all possible odd j, then*

$$P_{ue} \leqslant \sum_{\text{even } i} p^i (1-p)^{n-i} \binom{n}{i} \left(\frac{1}{2^{n-k}} + 1 \right), \tag{12}$$

where even i means that i runs through the even intergers between d and n.

Proof. According to Lemma 3, the coefficients of the Krawtchouk expansion of the following polynomial:

$$g_i(x) = \frac{(-1)^{i-1}}{(i-1)!(n-i)!} \frac{\prod_{j=1}^{n}(j-x)}{i-x}$$

are nonnegative if and only if i is odd. Then, let

$$f(x) = \sum_{\text{even } i} p^i (1-p)^{n-i} g_i(x) = \sum_{j=0}^{n} f_j P_j(x).$$

Hence, $f_j \leqslant 0$, $f(i) = p^i(1-p)^{n-i}$ for even i and $f(i) = 0$ for odd i. By the proof of Theorem 5,

$$P_{ue} \leqslant 2^k f_0 - f(0),$$

where

$$f(0) = \sum_{\text{even } i} (-1) p^i (1-p)^{n-i} \binom{n}{i},$$

and

$$f_0 = \frac{1}{2^n} \sum_{\text{even } i} p^i (1-p)^{n-i} \binom{n}{i}.$$

Thus, the upper bound follows from Theorem 5. □

Remark 5. *If C is linear, then A_i is the number of codewords of weight i, which implies that $A_i \leqslant \binom{n}{i}$. Hence,*

$$P_{ue} \leqslant \sum_{i \in I} p^i (1-p)^{n-i} \binom{n}{i},$$

where $I = \{i | A_i \neq 0\}$. Moreover, if $A_i = 0$ for all odd i, then

$$P_{ue} \leqslant \sum_{\text{even } i} p^i (1-p)^{n-i} \binom{n}{i}. \tag{13}$$

Example 3. *Consider the Nordstrom–Robinson code, it is a binary nonlinear code with the distance distribution in Table 3. Moreover, the weight distribution is the same as the distance distribution. By Equation (2),*

$$P_{ue} = 112p^6(1-p)^{10} + 30p^8(1-p)^8 + 112p^{10}(1-p)^6 + p^{16}.$$

According to Theorem 6, the values of the upper bound and true probability can be seen in Figure 2.

Table 3. Distance Distribution of the Nordstrom–Robinson Code.

i	0	6	8	10	16
A_i	1	112	30	112	1

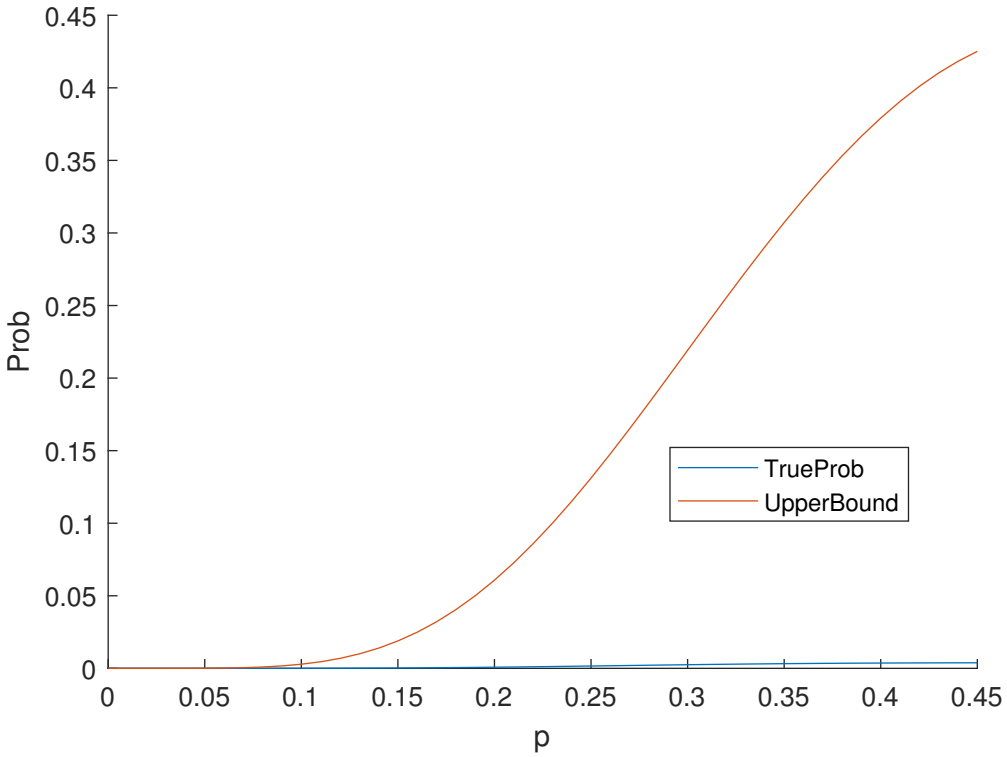

Figure 2. The Probability of Undetected Error of the Nordstrom–Robinson Code.

Example 4. *Let $\mathcal{E}$ be the set of binary vectors of length n and even weight, then it is actually the Reed–Muller code $RM(n-1,n)$ in Problem 5 in [2] and is generated by all the binary vectors of weight 2. Hence,*

$$P_{ue}(\mathcal{E},p)=\sum_{i=1}^{\lfloor n/2\rfloor}\binom{n}{2i}p^{2i}(1-p)^{n-2i}.$$

Remark 6. *The bound is suitable for many codes, and thus it seems not good. In fact, there exists some code C, whose P_{ue} is very large.*

Motivated by [17], we have the following upper bounds for linear codes over $\mathbb{F}_2$.

Proposition 1. *When C is a q-ary linear $[n,\ k,\ d]$ code and p is small enough, we have the following statements:*

(1) If $n+1+qd-nq>0$, then

$$P_{ue}\lesssim\frac{q^k+nq-n-1}{n-nq+1+qd}{p_q}^d(1-p)^{n-d};$$

(2) If $n+qd-nq-1<0$, then

$$P_{ue}\lesssim\frac{q^{k-2}n(qn-n-qd+1)+n(d-1)}{n-d}{p_q}^d(1-p)^{n-d};$$

(3) If $q=2$, $n-2d>0$, $(n-2d+2)^2>n$, and $A_i\neq 0$ only if $d\leqslant i\leqslant n-2d$, then

$$P_{ue}\lesssim\frac{2^{k-2}((n-2d+2)^2-n)+(d-1)(n-d+1)}{n+1-2d}p^d(1-p)^{n-d}.$$

Proof. These three bounds can be deduced easily by Equation (3) and Corollaries 4–6 in [17]. □

Remark 7. *The results in Corollary 4–6 in [17] are actually the upper bounds of A_d under different conditions. Considering Equation (3), it is necessary to make p small enough. According to the proof of Theorem 4, if A_d does not meet such bounds, then "<" holds.*

3.2.2. Lower Bounds

Similar to Proposition 1, by Corollaries 1–3 in [17], we have

Proposition 2. *If C is a q-ary linear code, then we have the following statements:*

(1) If $d = \lceil (n-1)(q-1)/q \rceil$, then

$$P_{ue} \geqslant \frac{q^k - nq + n - 1}{(n-d)q - n + 1} {p_q}^d (1-p)^{n-d};$$

(2) If $qd > nq - n - 2q + 1$, then

$$P_{ue} \geqslant \frac{q^{k-2} n(n - qn + qd + 2q - 1) - nd - n}{n-d} {p_q}^d (1-p)^{n-d};$$

(3) If $q = 2$ and all weights of C are in $[d, n-d]$, with $n - 2d > 0$ and $(n-2d-1)^2 < n+1$, then

$$P_{ue} \geqslant \left(\frac{2^{k-2}(n^2 - 4nd - 3n) + (2^k + 1)d(d+1)}{2d - n} - d - 1 \right) p^d (1-p)^{n-d}.$$

When using quadratic polynomials, we have the following bound.

Proposition 3. *Let f_0, f_1 and f_2 be nonnegative rational numbers such that*

$$f_0 - f_1 n + f_2 \binom{n}{2} \leqslant p^d (1-p)^{n-d} \quad \text{and} \quad f_1 + n f_2 \leqslant 2 d f_2,$$

then, for a binary $(n, 2^k, d)$ code, we have

$$P_{ue} \geqslant 2^k f_0 - p^d (1-p)^{n-d} - 2 f_1 n,$$

where $0 \leqslant p \leqslant \frac{1}{2}$.

Proof. It is known that, when $q = 2$, $P_0(x) = 1$, $P_1(x) = n - 2x$ and $P_2(x) = 2x^2 - 2nx + \binom{n}{2}$. Let $f(x) = f_0 P_0(x) + f_1 P_1(x) + f_2 P_2(x)$ and then it is a quadratic function whose axis of symmetry is $\frac{f_1 + n f_2}{2 f_2}$. Considering that $p^{i+1}(1-p)^{n-i-1} \geqslant p^i (1-p)^{n-i}$, it is sufficient to show that

$$f(n) \leqslant p^d (1-p)^{n-d} \text{ and } \frac{f_1 + n f_2}{2 f_2} \leqslant d,$$

i.e., $f(i) \leqslant f(n) \leqslant p^d (1-p)^{n-d} \leqslant p^i (1-p)^{n-i}$ for $i \geqslant d$. Equivalently,

$$f_0 - f_1 n + f_2 \binom{n}{2} \leqslant p^d (1-p)^{n-d}, \quad f_1 + n f_2 \leqslant 2 d f_2.$$

The result follows from Theorem 5. □

4. Good Bounds for Hamming Codes

Recall that the *weight enumerator* of the code C is the homogeneous polynomial

$$W_C(x, y) = \sum_{\boldsymbol{c} \in C} x^{n - wt(\boldsymbol{u})} y^{wt(\boldsymbol{u})},$$

where $wt(\boldsymbol{u})$ means the Hamming weight the codeword $\boldsymbol{u}$. The binary Hamming code $\mathcal{H}_m$ is a $[n = 2^m - 1, k = n - m, d = 3]$ code, with the weight enumerator

$$\frac{(x+y)^n + n(x+y)^{(n-1)/2}(x-y)^{(n+1)/2}}{n+1},$$

whose distance distribution A_i satisfies

$$\sum_{i=1}^{n} iA_i y^{i-1} + \sum_{i=0}^{n} A_i y^i + \sum_{i=0}^{n-1} (n-i)A_i y^{i+1} = (1+y)^n,$$

and the recurrence $A_0 = 1$, $A_1 = 0$,

$$(i+1)A_{i+1} + A_i + (n-i+1)A_{i-1} = \binom{n}{i}.$$

Moreover,

$$\begin{aligned}(1+y)^n &= \frac{\sum_{i=1}^{n} iA_i y^i}{y} + \sum_{i=0}^{n} A_i y^i + ny \sum_{i=0}^{n-1} A_i y^i - y \sum_{i=0}^{n-1} iA_i y^i \\ &= \sum_{i=1}^{n-1} A_i y^i \left(\frac{i}{y} - iy\right) + (ny+1) \sum_{i=1}^{n-1} A_i y^i + y^n + ny^{n-1} + ny + 1.\end{aligned}$$

Let $\alpha \in \mathbb{F}_{2^m}$ be a primitive element and let $g(x) \in \mathbb{F}_2[x]$ be the minimal polynomial of α with respect to $\mathbb{F}_2$. According to Exercise 7.20 in [20], $g(x)$ can be regarded as the generator polynomial of a Hamming code. Since $\deg(g(x)) = m > 1$, then

$$g(x) \left| \frac{x^n - 1}{x - 1} \right. = 1 + x + x^2 + \cdots + x^{n-1},$$

which implies that the all-one vector is a codeword of the Hamming code and $A_n = 1$.

Note that

$$P_{ue} = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i} = (1-p)^n \sum_{i=1}^{n} A_i \left(\frac{p}{1-p}\right)^i.$$

Hence,

$$\sum_{i=1}^{n-1} A_i \left(\frac{p}{1-p}\right)^i = \frac{P_{ue} - p^n}{(1-p)^n}.$$

Let $y = \varepsilon = \frac{p}{1-p}$, where $p \in (0, 1/2)$, then

$$\begin{aligned}&(n\varepsilon + 1)(P_{ue} - p^n) + (1-p)^n \sum_{i=1}^{n-1} A_i \varepsilon^i \left(\frac{i}{\varepsilon} - i\varepsilon\right) \\ &= 1 - p^n - np(1-p)^{n-1} - np^{n-1}(1-p) - (1-p)^n.\end{aligned}$$

According to Chapter 6, Exercise(E2), page 157 in [2], there are $n - 4$ nonzero weights of $\mathcal{H}_m$. Considering that $A_n = 1$, we have $A_i = 0$ if and only if $i = 1, 2, n-1, n-2$. Since $0 < p < 1/2$, then $0 < \varepsilon < 1$ and we have

$$\frac{3}{\varepsilon} - 3\varepsilon \leqslant \frac{i}{\varepsilon} - i\varepsilon \leqslant \frac{n-3}{\varepsilon} - (n-3)\varepsilon.$$

Obviously,

$$\begin{aligned}(1-p)^n \sum_{i=1}^{n-1} A_i \varepsilon^i \left(\frac{i}{\varepsilon} - i\varepsilon\right) &\leqslant (1-p)^n \sum_{i=1}^{n-1} A_i \varepsilon^i \left(\frac{n-3}{\varepsilon} - (n-3)\varepsilon\right) \\ &= \left(\frac{n-3}{\varepsilon} - (n-3)\varepsilon\right) \sum_{i=1}^{n-1} A_i p^i (1-p)^{n-i} \\ &= \left(\frac{n-3}{\varepsilon} - (n-3)\varepsilon\right)(P_{ue} - p^n).\end{aligned}$$

Similarly,

$$(1-p)^n \sum_{i=1}^{n-1} A_i \varepsilon^i \left(\frac{i}{\varepsilon} - i\varepsilon\right) \geqslant \left(\frac{3}{\varepsilon} - 3\varepsilon\right)(P_{ue} - p^n).$$

Thus,

$$\begin{aligned}P_{ue} &\leqslant \frac{1 - p^n - np(1-p)^{n-1} - np^{n-1}(1-p) - (1-p)^n}{\frac{3}{\varepsilon} - 3\varepsilon + n\varepsilon + 1} + p^n \\ &= \frac{p(1-p) - p^{n+1}(1-p) - np^2(1-p)^n - np^n(1-p)^2 - p(1-p)^{n+1}}{(n-1)p^2 - 5p + 3} + p^n\end{aligned} \tag{14}$$

and

$$\begin{aligned}P_{ue} &\geqslant \frac{1 - p^n - np(1-p)^{n-1} - np^{n-1}(1-p) - (1-p)^n}{\frac{n-3}{\varepsilon} - (n-3)\varepsilon + n\varepsilon + 1} + p^n \\ &= \frac{p(1-p) - p^{n+1}(1-p) - np^2(1-p)^n - np^n(1-p)^2 - p(1-p)^{n+1}}{(n-1)p^2 - (2n-7)p + n - 3} + p^n.\end{aligned} \tag{15}$$

Summarize the above discussions, we get

Theorem 7. *Let $\mathcal{H}_m$ be the binary $[n = 2^m - 1, k = n - m, 3]$ Hamming code, then when $0 < p < 1/2$ and $m \geqslant 3$, we have the upper bound Equation (14) and the lower bound Equation (15) for P_{ue}, respectively.*

Proof. Note that the upper bound should be larger or equal than the lower bound, then

$$(-(2n-7)p + n - 3) - (-5p + 3) = (n-6)(1-2p) \geqslant 0.$$

It is sufficient to solve the inequality $n = 2^m - 1 > 6$, due to $1 - 2p > 0$. Hence, $m \geqslant 3$. □

Remark 8. *The difference of the upper bound and the lower bound is small.*

Let $U(n,p) = H_1/H$ and $L(n,p) = H_2/H$ be the bound given by Equation (14) and Equation (15), respectively, where $H_1 = (n-1)p^2 - 5p + 3$, $H_2 = (n-1)p^2 - (2n-7)p + n - 3$ and

$$H = p(1-p) - p^{n+1}(1-p) - np^2(1-p)^n - np^n(1-p)^2 - p(1-p)^{n+1}.$$

In fact, H is a polynomial of p whose degree $n+2$ and the leading coefficient is

$$h_{n+2} = 1 + (-1)^{n+2}n - n + (-1)^{n+2} = (1 + (-1)^n) + n((-1)^n - 1) \neq 0,$$

while the product H_1H_2 is just a polynomial whose degree is 4*. Then,*

$$U(n,p) - L(n,p) = \frac{(H_2 - H_1)H}{H_1H_2} = \frac{(n-6)(1-2p)H}{H_1H_2} \longrightarrow \frac{(n-6)(1-2p)h_{n+2}p^{n+2}}{(n-1)^2p^4} \longrightarrow 0 \quad (n \to +\infty).$$

That is to say, the lower bound and the upper bound are very close. On the other hand,

$$H_1 \geqslant \frac{12n-37}{4(n-1)} \quad \text{and} \quad H_2 \geqslant \frac{n+1}{4}.$$

Then,

$$\begin{aligned} U(n,p) - L(n,p) &= \frac{(H_2 - H_1)H}{H_1H_2} = \frac{(n-6)(1-2p)H}{H_1H_2} \\ &< \frac{(n-6)(1-2p)p(1-p)}{H_1H_2} < \frac{(n-6)(1-2p)p(1-p)}{\frac{12n-37}{4(n-1)}\frac{n+1}{4}} \\ &= \frac{16(n-1)(n-6)}{(n+1)(12n-37)}p(1-p)(1-2p) \\ &\leqslant \frac{\sqrt{3}}{18}\frac{16(n-1)(n-6)}{(n+1)(12n-37)} \longrightarrow \frac{2\sqrt{3}}{27} \approx 0.1283 \quad (n \to +\infty). \end{aligned}$$

Here, let $F(p) = p(1-p)(1-2p)$, then its derivative is $F'(p) = 6p^2 - 6p + 1$. Note that the roots of $F'(p)$ are $\frac{3\pm\sqrt{3}}{6}$. Since $0 < p < 1/2$, then we choose the root $p_0 = \frac{3-\sqrt{3}}{6}$. Hence,

$$F(p) \leqslant F(p_0) = \frac{\sqrt{3}}{18} \approx 0.0962.$$

Thus the difference of the upper bound and the lower bound is about 0.1283 *at most, and tends to* 0 *when $n \to +\infty$.*

Example 5. *Using the bounds in Theorem 7, the results in Figure 1 can be improved. See Figure 3.*

When $m = 5$, the bounds Equations (15) and (14) are also valid. See Figure 4.

Note that the difference of the bounds Equations (15) and (14) is about 0.05*, which is much smaller than the given* 0.1283*.*

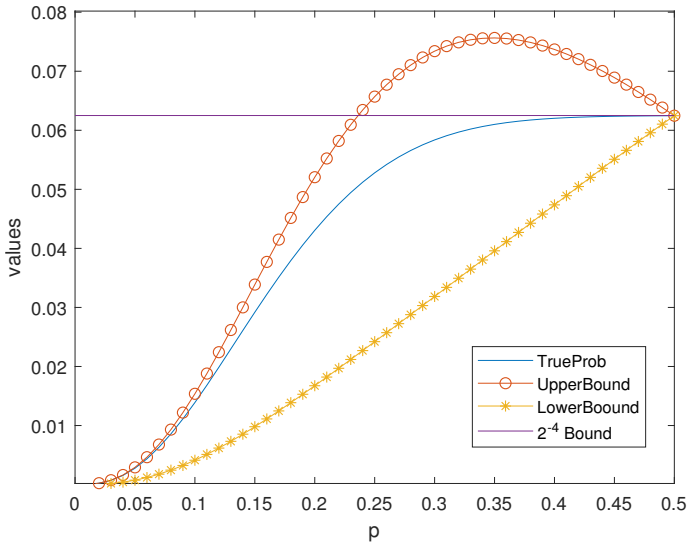

Figure 3. Bounds in Theorem 7 of P_{ue} for the Hamming Code $\mathcal{H}_4$.

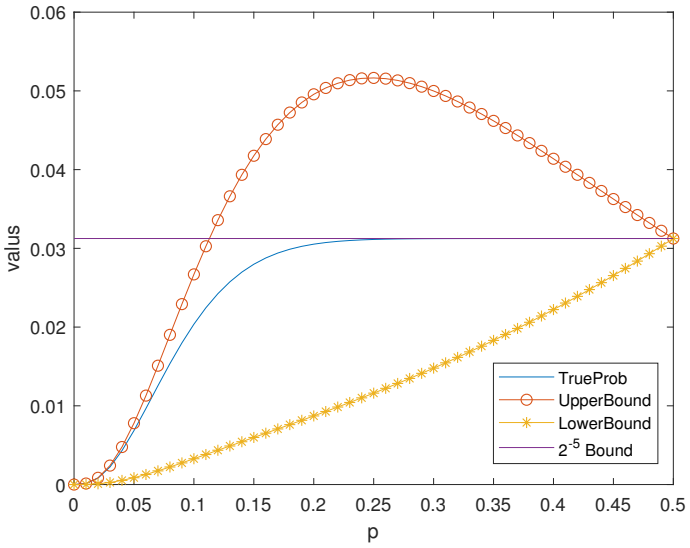

Figure 4. Bounds in Theorem 7 of P_{ue} for the Hamming Code $\mathcal{H}_5$.

It is known that the Hamming codes satisfy the 2^{-m} bound when $0 < p < 1/2$ i.e., $P_{ue} \leqslant 2^{-m}$. See [5] for more details. In fact, the obtained new bound is better than the ordinary 2^{-m} bound, when p is not large.

Theorem 8. *Let $\mathcal{H}_m$ be the binary $[n = 2^m - 1, k = n - m, 3]$ Hamming code, then when $0 < p < 1/2$ and $m \geq 3$, we have*

$$P_{ue} \leqslant \frac{p - p^2}{(n-1)p^2 - 5p + 3} + p^n. \tag{16}$$

Moreover, if $p < p_0$, this upper bound is better than the 2^{-m} bound, where p_0 is the smaller root of the equation $(2^{m+1} - 2)x^2 - (2^m + 5)x + 3 = 0$.

Proof. Assume that

$$\frac{p - p^2}{(n-1)p^2 - 5p + 3} < \frac{1}{2^m},$$

then it is sufficient to solve the inequality

$$(2^{m+1} - 2)p^2 - (2^m + 5)p + 3 > 0.$$

Obviously, the inequality holds when $p < p_0$, where

$$p_0 = \frac{(2^m + 5) - \sqrt{(2^m + 5)^2 - 12(2^{m+1} - 2)}}{2(2^{m+1} - 2)}$$

is the smaller root of the equation $(2^{m+1} - 2)x^2 - (2^m + 5)x + 3 = 0$. □

Example 6. *It is clear that when p is small enough, the new upper bound Equation (14) is smaller than the 2^{-m} bound in Figures 3 and 4.*

Remark 9. *Of course, the weight distribution of the binary Hamming codes can be computed and expressed by the sum of combinatorial numbers, which are usually very large when m is large. So, the method in this section is to estimate P_{ue} quickly. Compared with the 2^{-m} bound, our bounds are better when p is small enough.*

5. Conclusions

In this paper, we studied the probability of an undetected error P_{ue} and gave many bounds for P_{ue}. The main contributions of this paper are the following:

(1) The bounds obtained from the linear programming problem are given in Theorem 4. The bounds obtained from the Polynomial Method are given. According to the main Theorem 5, we get Theorem 6 (applied to the codes with even distances) and Proposition 3.
(2) Combining the results of [17], we give the bounds in Propositions 1 and 2.
(3) We find sharper bounds for binary Hamming codes (see Theorems 7 and 8).

To the best of our knowledge, that is the very first time that the LP method has been applied to bound P_{ue}. Even though computing P_{ue} exactly requires knowledge of the code weight spectrum, our bounds depend solely on the three parameters $[n, k, d]$, of the code. The weight frequencies are only used as variables in the LP program. Knowing the three parameters $[n, k, d]$ is the minimal requirement to use a code in applications.

To sum up, our bounds are most useful when the exact weight distribution is too hard to compute. Our bounds perform well when p is small enough and the kissing number A_d is known, and there are many such codes.

We mention the following open problems. The readers interested in Hamming codes are suggested to derive bounds for general q-ary Hamming codes with $q > 2$. Moreover, it is worth mentioning that the linear programming problem works better numerically than the Polynomial Method. The interest of the latter lies in producing bounds with closed formulas. It is a challenging open problem to derive better bounds with polynomials of degree higher than 2.

Author Contributions: Conceptualization, P.S.; methodology, P.S.; software, H.L.; validation, X.W. and P.S.; formal analysis, X.W. and P.S.; investigation, X.W. and P.S.; resources, H.L.; data curation, H.L.; writing—original draft preparation, X.W.; writing—review and editing, X.W. and P.S.; visualization, H.L.; supervision, P.S.; project administration, P.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Data are available in a publicly accessible repository

Acknowledgments: The authors are grateful to Minjia Shi, Li Chen, and his colleagues for their helpful suggestions for improving the presentation of the material in this paper and pointing out the references [6,21,22,24].

Conflicts of Interest: The authors have no conflict of interest to declare that are relevant to the content of this article.

References

1. Dodunekova, R.; Dodunekov, S.M.; Nikolova, E. A survey on proper codes. *Discret. Appl. Math.* **2008**, *156*, 1499–1509. [CrossRef]
2. MacWilliams, F.J.; Sloane, N.J.A. *The Theory of Error Correcting Codes*; Elsevier: Amsterdam, The Netherlands, 1981.
3. Massey, J. Coding techniques for digital data networks. In Proceedings of the International Conference on Information Theory and Systems, NTG-Fachberichte, Berlin, Germany, 18–20 September 1978; Volume 65.
4. Wolf, J.K.; Michelson, A.M.; Levesque, A.H. On the probability of undetected error for linear block codes. *IEEE Trans. Commun.* **1982**, *30*, 317–324. [CrossRef]
5. Leung-Yan-Cheong, S.K.; Hellman, M.E. Concerning a bound on undetected error probability. *IEEE Trans. Inform. Theory* **1976**, *22*, 235–237. [CrossRef]
6. Baldi, M.; Bianchi, M.; Chiaraluce, F.; Kløve, T. A class of punctured Simplex codes which are proper for error detection. *IEEE Trans. Inform. Theory* **2012**, *58*, 3861–3880. [CrossRef]
7. Kasami, T.; Lin, S. On the probability of undetected error for the maximum distance separable codes. *IEEE Trans. Commun.* **1984**, *32*, 998–1006. [CrossRef]
8. Leung-Yan-Cheong, S.K.; Barnes, E.R.; Friedman, D.U. On some properties of the undetected error probability of linear codes. *IEEE Trans. Inform. Theory* **1979**, *25*, 110–112. [CrossRef]

9. Ong, C.; Leung, C. On the undetected error probability of triple-error-correcting BCH codes. *IEEE Trans. Inform. Theory* **1991**, *37*, 673–678. [CrossRef]
10. Kløve, T. Reed-Muller codes for error detection: The good the bad and the ugly. *IEEE Trans. Inform. Theory* **1996**, *42*, 1615–1622. [CrossRef]
11. Abdel-Ghaffar, K.A.S. A lower bound on the undetected error probability and strictly optimal codes. *IEEE Trans. Inform. Theory* **1997**, *43*, 1489–1502. [CrossRef]
12. Ashikhmin, A.; Barg, A. Binomial moments of the distance distribution: Bounds and applications. *IEEE Trans. Inform. Theory* **1999**, *45*, 438–452. [CrossRef]
13. Barg, A.; Ashikhmin, A. Binomial moments of the distance distribution and the probability of undetected error. *Des. Codes Cryptogr.* **1999**, *16*, 103–116. [CrossRef]
14. Xia, S.T.; Fu, F.W.; Jiang, Y.; Ling, S. The probability of undetected error for binary constant weight codes. *IEEE Trans. Inform. Theory* **2005**, *51*, 3364–3373. [CrossRef]
15. Xia, S.T.; Fu, F.W.; Ling, S. A lower bound on the probability of undetected error for binary constant weight codes. *IEEE Trans. Inform. Theory* **2006**, *52*, 4235–4243. [CrossRef]
16. Xia, S.T.; Fu, F.W. Undetected error probability of q-ary constant weight codes. *Des. Codes Cryptogr.* **2008**, *48*, 125–140. [CrossRef]
17. Solé, P.; Liu, Y.; Cheng, W.; Guilley, S.; Rioul, O. Linear programming bounds on the kissing number of q-ary Codes. In Proceedings of the 2021 IEEE Information Theory Workshop (ITW), Kanazawa, Japan, 17–21 October 2021; pp. 1–5.
18. Kløve, T. *Codes for Error Detection*; Kluwer: Singapore, 2007.
19. Van Lint, J.H. *Introduction to Coding Theory*, 3rd ed.; Springer: Berlin/Heidelberg, Germany; New York, NY, USA, 1999.
20. Xing, C.; Ling, S. *Coding Theory: A First Course*; Cambridge University Press: Cambridge, UK, 2003.
21. Boyvalenkov, P.; Dragnev, P.; Hardin, D.; Saff, E.; Stoyanova, M. Energy bounds for codes in polynomial metric spaces. *Anal. Math. Phys.* **2019**, *9*, 781–808. [CrossRef]
22. Cohn, H.; Zhao, Y. Energy-minimizing error-correcting codes. *IEEE Trans. Inform. Theory* **2014**, *60*, 7442–7450. [CrossRef]
23. Ashikmin, A.; Barg, A.; Litsyn, S. Estimates on the distance distribution of codes and designs. *IEEE Trans. Inform. Theory* **2001**, *47*, 1050–1061. [CrossRef]
24. Levenshtein, V. Universal bounds for codes and designs. In *Chapter 6 of Handbook of Coding Theory*; Pless, V.S., Huffman, W.C., Eds.; Elsevier: Amsterdam, The Netherlands, 1998; pp. 499–648.