On the binomial moments of linear codes and undetected error probability

R. Dodunekova
Chalmers University of Technology
and Göteborg University

Abstract The binomial moments of a linear code are synonymously related to its weight distribution and appear naturally in studies involving the weight distribution of the code. In particular, the binomial moments have been used for establishing bounds on the undetected error probability and, though implicitly, for the study of good and proper codes. In this work we sharpen known bounds on the binomial moments of a linear code. One consequence of this sharpening is a simple algorithm for computing the dual code distance via the binomial moments of the code. Also, we derive inequalities for the undetected error probability and simplify some previously known sufficient conditions for good and proper codes.

Keywords: linear code, binomial moments, undetected error probability, good code, proper code

1 Introduction

An $[n,k,d]_q$ linear code C is a k-dimensional subspace of the n-dimensional vector space over the finite field $GF(q)$ of q elements. The weight distribution $\{A_0,\ldots,A_n\}$ of C consists of the numbers A_i of codewords of weight i in C, $0\le i\le n$. The *binomial moments* of the weight distribution are defined to be

$$A'_\ell=\sum_{i=1}^{\ell}\binom{n-i}{n-\ell}A_i,\quad \ell=1,\ldots,n. \tag{1.1}$$

The weight distribution of C is expressed in terms of the binomial moments as (see [7])

$$A_i = \sum_{\ell=1}^{i} (-1)^{\ell-i} \binom{n-\ell}{n-i} A'_\ell, \quad i = 1, \ldots, n. \tag{1.2}$$

The binomial moments were first introduced in [29] for the case $q = 2$ but used even earlier, though implicitly, in [28] in the proof of the MacWilliams identities. The binomial moments describe the cumulative cardinality of subcodes of C with support of size at most ℓ, see e.g., [28], [23], and [7-8] and appear in a natural way in studies of the weight distribution of algebraic-geometric codes [23]. In [20] and [6] the binomial moments play a role in relating weight distributions and support weight distributions of linear codes to the classical polynomials on linear matroids. More about the use of the binomial moments may be found in [1], [10], [21], [26], and [33]. A comprehensive discussion on the subject is provided in [8].

In [24], [1], and [7] the binomial moments were used to study the undetected error probability of linear codes, and in [11-16], [2-5] and [25] as well, though there the binomial moments are not formally named and appear as $A'_i/\binom{n}{i}, \quad i = 1, \ldots, n$. We introduce notations for these numbers, following the notations in the papers mentioned above. Let

$$A^*_0 = 0, \quad A^*_\ell = \sum_{i=1}^{\ell} \frac{\ell_{(i)}}{n_{(i)}} A_i, \quad \ell = 1, \ldots, n, \tag{1.3}$$

where $j_{(i)}$ denotes the i-th factorial moment $j(j-1)\ldots(j-i+1)$. Since $\ell_{(i)}/n_{(i)} = \binom{n-i}{n-\ell}/\binom{n}{\ell}$, we obtain by (1.1)

$$A^*_\ell = \frac{1}{\binom{n}{\ell}} \sum_{i=1}^{\ell} \binom{n-i}{n-\ell} A_i = \frac{A'_\ell}{\binom{n}{\ell}}, \quad \ell = 1, 2, \ldots, n. \tag{1.4}$$

This paper deals extensively with the numbers $A^*_\ell, \quad \ell = 0, \ldots, n$. Throughout this work we will call them the star numbers of the weight distribution. Note that these numbers equal zero for $\ell \leq d-1$ and, in contrast to the binomial moments, are strictly increasing for $\ell \geq d$, since

$$\begin{aligned} A^*_\ell &= \sum_{1}^{\ell-1} \frac{\ell_{(i)}}{n_{(i)}} A_i + \frac{A_\ell}{\binom{n}{\ell}} > \sum_{1}^{\ell-1} \frac{(\ell-1)_{(i)}}{n_{(i)}} A_i + \frac{A_\ell}{\binom{n}{\ell}} \\ &= A^*_{\ell-1} + \frac{A_\ell}{\binom{n}{\ell}} > A^*_{\ell-1}, \quad \ell = d, \ldots, n. \end{aligned} \tag{1.5}$$

It will become clear below, that the monotonicity of the star numbers is essential for our study of the binomial moments and the undetected error probability of linear codes.

If C is an $[n,k,d]_q$ code, the number $s(C) = n - k + 1 - d$ is called the *defect* of C. The defect of C is zero if and only if C is an MDS code. In this case, the dual code $C^\perp$ is an $[n, n-k, d^\perp]_q$ MDS code and $d + d^\perp = n + 2$. In all other cases $s(C) \geq 1$ and $d + d^\perp \leq n$.

Let C be an $[n,k,d]_q$ code of defect s and weight distribution $\{A_0, \ldots, A_n\}$, and let $d^\perp$ and $s^\perp$ be correspondingly the minimum distance and the defect of $C^\perp$. It follows from Theorem 3 of [23] that the binomial moments $A'_1, \ldots A'_n$ of C satisfy the conditions

$$A'_\ell = \binom{n}{\ell}\big(q^{\ell-n+k} - 1\big), \quad n - d^\perp + 1 \leq \ell \leq n, \tag{1.6}$$

and, when C is not an MDS code,

$$A'_\ell \geq \max\Big\{0, \binom{n}{\ell}\big(q^{\ell-n+k} - 1\big)\Big\}, \quad d \leq \ell \leq n - d^\perp, \tag{1.7}$$

$$A'_\ell \leq \binom{n}{\ell}\big(q^{\min(\ell+1-d,\, s^\perp)} - 1\big), \quad d \leq \ell \leq n - d^\perp. \tag{1.8}$$

The proof is algebraic-combinatorial and uses the fact that A'_ℓ describes the cardinality of subcodes of C with support of size at most ℓ.

In Section 2 we first derive equalities relating the star numbers of C and $C^\perp$. Using these relations we easily obtain equalities (1.6) for the binomial moments and then prove that inequalities (1.7) and (1.8) are actually strict. One consequence of this sharpening is a simple algorithm for computing the code distance of $C^\perp$ via the binomial moments of C. In Section 3 we use (1.6) and the sharpened (1.7) and (1.8) for estimating the probability of undetected error, when C is used for error detection on a symmetric channel with symbol error probability ε, defined as

$$P_{ue}(C,\varepsilon) = \sum_{i=d}^{n} A_i \Big(\frac{\varepsilon}{q-1}\Big)^i (1-\varepsilon)^{n-i}, \quad 0 \leq \varepsilon \leq \frac{q-1}{q}. \tag{1.9}$$

Our study of the undetected error probability makes use of the expression

$$P_{ue}(C,\varepsilon) = \sum_{i=d}^{n} A^*_i \binom{n}{i} \Big(\frac{\varepsilon}{q-1}\Big)^i \Big(1 - \frac{q\varepsilon}{q-1}\Big)^{n-i}$$

obtained earlier in [13].

Section 4 deals with good and proper codes, considered in general to perform well in error detection. The code C is *proper* for error detection if the undetected error probability of (1.9) is increasing in $\varepsilon \in [0, \frac{q-1}{q}]$, and C is *good*, if

$P_{ue}(C,\varepsilon) \le P_{ue}(C,\frac{q-1}{q})$ [27, 22]. Note, that a proper code is good as well. In [12-15], sufficient conditions for proper and good codes were established in terms of the star numbers of the code. These conditions were efficiently used in [2-5], [11], [16], and [25] to study the error detecting capability of particular codes and classes of codes. In Section 4 we give simplified versions of some sufficient conditions for proper and good codes obtained earlier.

In Section 5 we give a short discussion on the results presented here and related questions.

2 On the binomial moments

Let C be an $[n,k,d]_q$ code with weight distribution $\{A_0,\dots,A_n\}$ and star numbers $\{A_0^*,\dots,A_n^*\}$, and let $C^\perp$ be the dual code of weight $d^\perp$, weight distribution $\{B_0,\dots,B_n\}$ and star numbers $\{B_0^*,\dots,B_n^*\}$. Let s and $s^\perp$ denote the defect of C and $C^\perp$, respectively.

Lemma 1. *The star numbers of C and $C^\perp$ are related in the following way:*

$$A_\ell^* + 1 = q^{\ell-n+k}(B_{n-\ell}^* + 1), \quad \ell = 0,\dots,n, \tag{2.1}$$

$$B_\ell^* + 1 = q^{\ell-k}(A_{n-\ell}^* + 1), \quad \ell = 0,\dots,n. \tag{2.2}$$

Consequently, the binomial moments of C and $C^\perp$ satisfy

$$A'_\ell + \binom{n}{\ell} = q^{\ell-n+k}\left(B'_{n-\ell} + \binom{n}{n-\ell}\right), \quad \ell = 0,\dots,n. \tag{2.3}$$

Proof. The proof of (2.1) and (2.2) uses MacWilliams identity [28]

$$\sum_{i=0}^{\ell}\binom{n-i}{\ell-i}A_i = q^{-(n-k-\ell)}\sum_{i=}^{n-\ell}\binom{n-i}{\ell}B_i$$

and can be found in [15]. (2.3) follows from (1.4) and (2.1).

Lemma 2. *For any $[n,k,d]_q$ code C,*

$$A_\ell^* = q^{\ell-n+k} - 1, \quad \ell = n - d^\perp + 1,\dots,n. \tag{2.4}$$

Proof. In (2.1), $B_{n-\ell}^* = 0$ for $n-\ell = 0,\dots,d^\perp - 1$, hence (2.4). □

As (2.4) and (1.2) show, the weight distribution $\{A_0, \ldots, A_n\}$ of C is uniquely determined by $A_d, \ldots, A_{n-d^\perp}$, a result obtained earlier in [18] and [30].

For an MDS code (2.4) gives

$$A^*_\ell = q^{\ell-n+k} - 1, \quad \ell = n-k+1, \ldots, n, \quad A^*_\ell = 0, \quad 0 \le \ell \le n-k. \tag{2.5}$$

Lemma 3. *Let C be an $[n,k,d]_q$ code with $d + d^\perp \le n$. Then*

$$A^*_\ell < q^{\min\{\ell+1-d,\ s^\perp\}} - 1, \quad d \le \ell \le n - d^\perp. \tag{2.6}$$

Proof. When $d + d^\perp = n$, i.e., C is a Near-MDS code, (2.6) contains only the inequality $A^*_{n-k} < q-1$, or, equivalently, $A_{n-k} < \binom{n}{k}(q-1)$, which is true, according to [17]. Let $d + d^\perp < n$. We will use the monotonicity of the star numbers established in (1.5). Since $B^*_{\ell'} > B^*_{\ell'-1}$ for $\ell' = d^\perp, \ldots, n$, we obtain from (2.2)

$$q^{\ell'-k}(A^*_{n-\ell'} + 1) > q^{\ell'-1-k}(A^*_{n-\ell'+1} + 1),$$

or, denoting $\ell = n - \ell'$,

$$q(A^*_\ell + 1) > A^*_{\ell+1} + 1, \quad \ell = 0, \ldots, n - d^\perp. \tag{2.7}$$

For $d \le \ell + 1 \le n - d^\perp$ we apply (2.7) to its left-hand side $\ell + 1 - d$ times to get

$$q^{\ell+2-d}(A^*_{d-1} + 1) > A^*_{\ell+1} + 1, \quad \ell = d-1, \ldots, n - d^\perp - 1.$$

Since $A^*_{d-1} = 0$, the above gives

$$A^*_{\ell+1} < q^{\ell+2-d} - 1, \quad \ell = d-1, \ldots, n - d^\perp - 1,$$

or

$$A^*_\ell < q^{\ell+1-d} - 1, \quad \ell = d, \ldots, n - d^\perp. \tag{2.8}$$

Next we apply (2.8) to the star numbers of $C^\perp$ to get

$$B^*_{n-\ell} < q^{n-\ell+1-d^\perp} - 1 = q^{-\ell+n-k+s^\perp} - 1, \quad n - \ell = d^\perp, \ldots, n - d,$$

and then use this in (2.1) to obtain

$$A^*_\ell < q^{s^\perp} - 1, \quad \ell = d, \ldots, n - d^\perp. \tag{2.9}$$

The inequalities (2.6) now follow from (2.8) and (2.9). □

Lemma 4. *Let C be an $[n,k,d]_q$ code with $d^\perp + d \le n$. Then*

$$A^*_\ell > \max\{0,\ q^{\ell-n+k} - 1\}, \quad \ell = d, \ldots, n - d^\perp. \tag{2.10}$$

Proof. Write (2.7) in the form

$$A_\ell^* + 1 > q^{-1}(A_{\ell+1}^* + 1), \quad \ell = 0, \ldots, n - d^\perp$$

and apply the above inequality to its right-hand side $n - d^\perp - \ell$ times to obtain

$$A_\ell^* + 1 > q^{\ell-(n-d^\perp+1)}(A_{n-d^\perp+1}^* + 1), \quad \ell = 0, \ldots, n - d^\perp.$$

By (2.4), $A_{n-d^\perp+1}^* = q^{(n-d^\perp+1)-n+k} - 1$ and the above thus gives

$$A_\ell^* > q^{\ell-n+k} - 1, \quad \ell = 0, \ldots, n - d^\perp.$$

Since $A_\ell^* > 0$ for $= \ell \geq d$, (2.9) follows. □

Theorem 1. *Let C be an $[n, k, d]_q$ code of defect s, dual defect $s^\perp$, and dual code distance $d^\perp$. The binomial moments $\{A'_1, \ldots, A'_n\}$ of C satisfy*

$$A'_\ell = \binom{n}{\ell}(q^{\ell-n+k} - 1), \quad \ell = n - d^\perp + 1, \ldots, n, \tag{2.11}$$

and, if $d + d^\perp \leq n$,

$$\begin{aligned} &\max\left\{0, \binom{n}{\ell}\left(q^{\ell-n+k} - 1\right)\right\} < A'_\ell \\ &< \binom{n}{\ell}\left(q^{\min\{\ell-n+k+s,\, s^\perp\}} - 1\right), \quad \ell = d, \ldots, n - d^\perp. \end{aligned} \tag{2.12}$$

Proof. The results follow by applying (1.4) in (2.4), (2.6) and (2.10). □

As we mentioned before, (2.11) was first proved in [23] and then in [7] and [1] by different methods. (2.12) is a sharpening of the results (1.7) and (1.8) obtained in [23]. As our proof shows, equalities are impossible in (2.12).

Equalities (2.11) and the left-hand side of (2.12) suggest the following way of computing the dual code distance via the binomial moments.

Theorem 2. *Let C be an $[n, k, d]_q$ non-MDS code of weight distribution $\{A_0, \ldots, A_n\}$ and let*

$$\ell_0 = \min_{\ell \leq n}\{\ell : A'_\ell = \binom{n}{\ell}(q^{\ell-n+k} - 1). \tag{2.13}$$

The dual distance of C is then

$$d^\perp = n + 1 - \ell_0. \tag{2.14}$$

Finally we give some relations between the binomial moments, the star numbers, and the code weight distribution.

Theorem 3. *Let C be an $[n,k,d]_q$ code of weight distribution $\{A_0,\ldots,A_n\}$, star moments $\{A_0^*,\ldots,A_n^*\}$, and binomial moments $\{A_1',\ldots,A_n'\}$. Then*

$$A_\ell' > \frac{n-\ell+1}{\ell}A_{\ell-1}', \quad \ell = d,\ldots,n-d^\perp, \tag{2.15}$$

and

$$A_\ell' - \frac{n-\ell+1}{\ell}A_{\ell-1}' = \binom{n}{\ell}(A_\ell^* - A_{\ell-1}^*) > A_\ell, \quad \ell = d+1,\ldots,n. \tag{2.16}$$

Proof. (2.15) and (2.16) follow from (1.5) and (1.4). □

We note that (2.15) is a sharpening of Lemma 3 of [8].

3 Bounds for $P_{ue}(C,\varepsilon)$

In terms of the star numbers the probability of undetected error for an $[n,k,d]_q$ code C in (1.9) may be written as (see [13])

$$P_{ue}(C,\varepsilon) = \sum_{i=d}^{n} A_i^* q^{-i} R_i\Big(\frac{q\varepsilon}{q-1}\Big), \quad 0 \le \varepsilon \le \frac{q-1}{q}, \tag{3.1}$$

where

$$R_i(z) = \binom{n}{i} z^i (1-z)^{n-i}, \quad 0 \le z \le 1, \quad i = 1,\ldots,n. \tag{3.2}$$

For an MDS code, (2.5) and (3.1)give

$$P_{ue}(C,\varepsilon) = \sum_{i=n-k+1}^{n} (q^{-n+k} - q^{-i}) R_i\Big(\frac{q\varepsilon}{q-1}\Big). \tag{3.3}$$

For other codes, $d + d^\perp \le n$ and by (2.4) and (3.1,

$$\begin{aligned} P_{ue}(C,\varepsilon) = &\sum_{i=d}^{n-d^\perp} A_i^* q^{-i} R_i\Big(\frac{q\varepsilon}{q-1}\Big) \\ &+ \sum_{i=n-d^\perp+1}^{n} (q^{-n+k} - q^{-i}) R_i\Big(\frac{q\varepsilon}{q-1}\Big). \end{aligned} \tag{3.4}$$

Theorem 4. *Let C be an $[n,k,d]_q$ code with $d+d^\perp \le n$. Then*

$$P_{ue}(C,\varepsilon) \ge \sum_{i=d}^{n-k} A_i^* q^{-i} R_i\Big(\frac{q\varepsilon}{q-1}\Big) + \sum_{i=n-k+1}^{n} (q^{-n+k}-q^{-i}) R_i\Big(\frac{q\varepsilon}{q-1}\Big), \qquad (3.5)$$

with equality only when $d^\perp = k$.

Proof. When $d^\perp = k$, i.e., when $C^\perp$ is an Almost MDS code [9], (3.4) implies (3.5) with equality. Otherwise $n-k+1 < n-d^\perp+1$, and (2.10) implies (3.5) with strict inequality . □

Note that the second sum in the right-hand side of (3.5) is the same as in (3.3) and would represent the probability of undetected error of an $[n,k]_q$ MDS code, if such a code would exist. That the right-hand side of (3.3) is a strict lower bound of the undetected error probability of non-MDS codes was shown earlier in [1] and in [7] by different methods. However, (3.5) provides information about the error in this lower bound.

Next theorem presents a lower bound for the undetected error probability of non-MDS codes in terms of the code parameters and the number A_d of codewords of minimum weight.

Theorem 5. *Let C be an $[n,k,d]_q$ code with $d+d^\perp \le n$. Then*

$$\begin{aligned} P_{ue}(C,\varepsilon) \ge{}& \frac{A_d}{n_{(d)}} \sum_{i=d}^{n-d^\perp} i_{(d)} q^{-i} R_i\Big(\frac{q\varepsilon}{q-1}\Big) \\ &+ \sum_{i=n-d^\perp+1}^{n} (q^{n+k}-q^{-i}) R_i\Big(\frac{q\varepsilon}{q-1}\Big). \end{aligned} \qquad (3.6)$$

Equality is attained only if C is a Near-MDS code or if

$$A_{d+1} = \ldots = A_{n-d^\perp} = 0. \qquad (3.7)$$

In particular, MMD codes attain the bound in (3.6).

Proof. C is a Near-MDS code [17] if and only if $d+d^\perp = n$. Since $d = n-k$ in this case, $A_d^* = A_d/\binom{n}{d}$ and rest of the binomial numbers is determined by (2.4), i.e., (3.6) reduces to (3.4).

Let $d+d^\perp < n$. From (1.4) we have

$$A_i^* = \frac{i_{(d)}}{n_{(d)}} A_d + \sum_{j=d+1}^{i} \frac{i_{(j)}}{n_{(j)}} A_j \ge \frac{i_{(d)}}{n_{(d)}} A_d, \quad d+1 \le i \le n-d^\perp, \qquad (3.8)$$

where equality is possible only when (3.7) holds true. This together with (3.4) prove (3.6). In particular, MMD codes [19, 32] satisfy (3.7) (see [11]). □

Theorem 6. *Let C be an $[n,k,d]_q$ code with $d+d^\perp \le n$. Then*

$$\begin{aligned} P_{ue}(C,\varepsilon) \le A^*_{n-d^\perp} \sum_{i=d}^{n-d^\perp} q^{-i} R_i\Big(\frac{q\varepsilon}{q-1}\Big) \\ + \sum_{i=n-d^\perp+1}^{n} (q^{-n+k}-q^{-i}) R_i\Big(\frac{q\varepsilon}{q-1}\Big). \end{aligned} \tag{3.9}$$

Equality is attained only if C is a Near-MDS code.

If $s^\perp$ is the defect of $C^\perp$ we have the following upper bound for $P_{ue}(C,\varepsilon)$:

$$\begin{aligned} P_{ue}(C,\varepsilon) < (q^{s^\perp}-1) \sum_{i=d}^{n-d^\perp} q^{-i} R_i\Big(\frac{q\varepsilon}{q-1}\Big) \\ + \sum_{i=n-d^\perp+1}^{n} (q^{-n+k}-q^{-i}) R_i\Big(\frac{q\varepsilon}{q-1}\Big). \end{aligned} \tag{3.10}$$

Proof. For a Near-MDS code, (3.9) is just the equality (3.4). Otherwise $d+d^\perp < n$ and for $i = d, \ldots, n-d^\perp-1$ we have by (1.5) that $A^*_i < A^*_{n-d^\perp}$. Using this in (3.4), we get (3.9). Since by (2.6) $A^*_{n-d^\perp} < q^{s^\perp}-1$, (3.10) follows from (3.9). □

Theorem 7. *Let C be an $[n,k,d]_q$ code with $d+d^\perp \le n$ and dual defect $s^\perp$. Then*

$$\begin{aligned} P_{ue}(C,\varepsilon) < \sum_{i=d}^{n-d^\perp} (q^{\min(1-d,\, s^\perp-i)} - q^{-i}) R_i\Big(\frac{q\varepsilon}{q-1}\Big) \\ + \sum_{i=n-d^\perp+1}^{n} (q^{-n+k}-q^{-i}) R_i\Big(\frac{q\varepsilon}{q-1}\Big). \end{aligned} \tag{3.11}$$

Proof. The statement follows immediately by applying (2.6) in (3.4). □

4 Proper and good codes

The representation (3.1) of undetected error probability made it possible to derive in [13] and [15] sufficient conditions in terms of the star numbers for good and

proper error detection codes. Theorem 2 of [13] states that if the star numbers of C satisfy

$$A_i^* \geq qA_{i-1}^*, \quad i = d+1, \ldots, n, \tag{4.1}$$

then C is proper. However, by (2.4)

$$A_i^* = q^{i-n+k} - 1 > q(q^{i-1-n+k} - 1) = qA_{i-1}^*, \quad i = n - d^\perp + 2, \ldots, n.$$

The above shows that an MDS code is proper, and that for an non-MDS code the number of inequalities to check in (4.1) is actually only $n - d - d^\perp + 1$ rather than $n - d$. Thus for non-MDS codes Theorem 2 of [13] can be stated as follows.

Theorem 8. *Let C be an $[n, k, d]_q$ code with $d + d^\perp \leq n$ and star numbers $\{A_1^*, \ldots, A_n^*\}$. If*

$$A_\ell^* \geq qA_{\ell-1}^*, \quad \ell = d+1, \ldots, n - d^\perp + 1, \tag{4.2}$$

then C is proper.

Theorem 2 of [15] restates the sufficient conditions (4.1) in terms of the dual star numbers by making use of (2.1) and (2.2). (In situations when the number of non-zero weights in the dual code or the co-dimension is small, the dual sufficient conditions are technically more effective.) By Theorem 8, for non-MDS codes the number of inequalities in the dual sufficient conditions may be reduced from $n - d$ to $n - d - d^\perp + 1$ and we can thus state the following.

Theorem 9. *Let C be an $[n, k, d]_q$ code with $d + d^\perp \leq n$ and dual star numbers $\{B_1^*, \ldots, B_n^*\}$. If*

$$B_{n-\ell}^* \leq B_{n-\ell+1}^* - q^{n-k-\ell}(q-1), \quad \ell = d+1, \ldots, n - d^\perp + 1, \tag{4.3}$$

then C is proper.

Theorem 1 of [13] says that the inequalities

$$A_\ell^* q^{-\ell} \leq q^{-n}(q^k - 1), \quad \ell = d, \ldots, n-1, \tag{4.4}$$

are sufficient for a code to be good, and Theorem 1 of [15] states the above conditions in terms of the dual star numbers. It is easily seen from (2.4) that for $\ell \geq n - d^\perp + 1$ the corresponding inequalities in (4.4) are true. In this way, for non-MDS codes the two theorems can be formulated with a reduced number of conditions.

Theorem 10. *Let C be an $[n,k,d]_q$ code with $d+d^\perp \le n$ and star numbers $\{A_1^*,\ldots,A_n^*\}$. If*

$$A_\ell^* q^{-\ell} \le q^{-n}(q^k-1), \quad i=d,\ldots,n-d^\perp, \tag{4.5}$$

then C is good.

Theorem 11. *Let C be an $[n,k,d]_q$ code with $d+d^\perp \le n$ and dual star numbers $\{B_1^*,\ldots,B_n^*\}$. If*

$$q^{-n+\ell} B_{n-\ell}^* \le q^{-k} - q^{-n-k+\ell}, \quad \ell=d,\ldots,n-d^\perp, \tag{4.6}$$

then C is good.

5 Discussions

Though the binomial moments appear in many problems of combinatorial coding theory (see, e.g., [1], [6-8], [10-16], [20-21], [23-26], [28], [33]), their potential for application does not seem to be sufficiently elucidated, and the present work may be considered as an attempt to do so.

Formulas (1.2) and (2.5) show that the weight distribution $\{A_0,\ldots,A_n\}$ of any $[n,k,d]_q$ linear code with dual distance $d^\perp$ is entirely determined by $A_d,\ldots,A_{n-d^\perp}$. Indeed, a formula expressing $A_{n-d^\perp+1},\ldots,$ and A_n in terms of $A_d,\ldots,A_{n-d^\perp}$ has been independently discovered, as claimed in [32], in [30], and [18], see also [31]. This relationship might provide a possibility for simplifying linear programming methods for search of new codes.

The result (2.12) is a sharpening of (1.7) and (1.8), earlier known from [23] and partially from [1] and [7-8]. Our proof here seems to be the shortest, by making use of the relations (2.1) and (2.2) between the star numbers and the dual star numbers. These relations are actually equivalent to (2.3), relating the binomial moments to the dual binomial moments. This latter relation seems to be new, like the strong inequalities between the binomial moments (2.15), and (2.16), establishing upper bounds on the number of codewords of fixed weight by the binomial moments. The algorithm for computing the dual code distance via the binomial moments (2.13)-(2.14) also appears to be new.

Inequalities (3.6) and (3.9) establishing bounds on the undetected error probability might be of some interest. The first one gives a lower bound involving the number of codewords of minimum weight in the code. The second one presents an upper bound involving the star moment $A_{n-d^\perp}^*$, which is in fact determined by the number of codewords of minimum weight in the dual code, according to (2.2)

and (1.4). Note that the inequalities (3.10) and (3.11) suggest that codes with small defect or small dual defect might be more appropriate for error detection.

The representation (3.3) of the probability of undetected error in terms of the star numbers turned out to be very efficient for studying good and proper linear codes. Sufficient conditions for good and proper codes, based on this representation, were derived in [12-15] and used in [2-5], [11], [16], and [25] for investigation of the error detecting performance of some classes of codes. In particular, results in [2] and [25] show that some standardized CRC codes are not even good, while some non-standardized CRC codes turn out to be proper.

References

[1] K. A. S. Abdel-Ghaffar, "A lower bound on the undetected error probability and strictly optimal codes", *IEEE Trans. Inform Theory*, vol. 43, pp. 1489-1502, Sept. 1997.

[2] A. Baicheva, S. M. Dodunekov, and P. Kazakov, "On the cyclic redundancy-check codes with 8-bit redundancy", *Computer communications* 21 (1998) 1030-1033.

[3] T. Baicheva, S. M. Dodunekov, and P. Kazakov, "On the cyclic redundancy-check codes of 16-bit redundancy, in: Proc. VI Intern". Workshop on ACCT (Pskov, Russia, 1998) 17-21.

[4] T. Baicheva, S. M. Dodunekov, and P. Kazakov, "On the error detection performance of some standardized CRC codes", in: Proc. Telecom 98 (Drujba, Bulgaria, 1998).

[5] T. Baicheva, S. N. Dodunekov, and P. Kazakov, "Undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy", *IEEE Proc. Commun.,* 147 (2000), 253-256.

[6] A. Barg, "The matroid of supports of a linear code", *Applicable Algebra in Eng., Commun. and Comput.*, vol. 8, pp. 165-172, 1997.

[7] A. Barg and A. Ashikhmin, "Binomial moments of the distance distribution and the probability of undetected error", *Des, Codes Cryptogr.*, no. 2, pp. 103-116, 1999.

[8] A. Barg and A. Ashikhmin, "Binomial Moments of the Distance Distribution: Bounds and Applications", *IEEE Trans. Inform. Theory*, vol. 45, no 2, pp. 483-452, March 1999.

[9] M. A. de Boer, "Almost MDS codes", *Des, Codes Cryptogr.*, no. 9, pp. 143-154, 1996.

[10] P. Delsarte, "Bilinear forms over a finite field, with applications to coding theory", *J. Comb. Theory Ser. A*, vol. 25, pp. 226-241, 1978.

[11] R. Dodunekova, "The duals of the MMD codes are proper for error detection", *preprint* 2002:20, Chalmers University of Technology and Göteborg University, 2002.

[12] R. Dodunekova and S. M. Dodunekov, "On the probability of undetected error for Near-MDS codes", *preprint* 1995-25, Chalmers University of Technology and Göteborg University, 1995.

[13] R. Dodunekova and S. M. Dodunekov, "Sufficient conditions for good and proper error detecting codes", *IEEE Trans. Inform. Theory* 43 (1997) 2023-2026.

[14] R. Dodunekova, S. M. Dodunekov, and T. Kløve, " Almost-MDS codes and near MDS codes for error detection", *IEEE Trans. Inform. Theory* 43 (1997) 285-290.

[15] R. Dodunekova and S. M. Dodunekov, "Sufficient Conditions for Good and Proper Linear Error Detecting Codes via Their Duals", Mathematica Balkanica (New Series) 11 (1997) 375-381.

[16] R. Dodunekova and S. M. Dodunekov, "The MMD codes are proper for error detection", *preprint* 2002:7, Chalmers University of Technology and Göteborg University, 2002.

[17] S. M. Dodunekov and I. N. Landgev, "On Near-MDS codes", *Journal of Geometry*, vol. 54, pp. 30-43, 1995.

[18] A. Faldum and W. Willems, "Codes of small defects", *Des, Codes Cryptogr.*, vol. 19, pp. 341-350, 1997.

[19] A. Faldum and W. Willems, "A characterization of MMD codes", *IEEE Trans. Inform. Theory* 44 (1998) 1555-1558.

[20] C. Greene, "Weight enumeration and the geometry of linear codes", *Stud. Appl. Math.,* 55 (1976) 119-128.

[21] T. Helleseth, T. Kløve, and V. I. Levenshtein, "On the information function of an error-correcting code", *IEEE Trans. Inform. Theory*, vol. 43, pp. 549-557, Mar. 1997.

[22] T. Kasami and S. Lin, "On the probability of undetected error for the Maximum Distance Separable codes", *IEEE Trans. Inform. Theory* IT-25 (1979) 110-112.

[23] G. L. Katsman and M. A. Tsfasman, "Spectra of algebraic geometric codes", *Probl. Pered. Inform.*, vol. 23, no. 4, pp. 19-34, 1988.

[24] G. L. Katsman, M. A. Tsfasman, and S. G. Vlăduţ, "Spectra of linear codes and error probability of decoding", in *Coding Theory and Algebraic Geometry (Lecture Notes in Mathematics*, vol. 1518), H. Stichtenoth and M. A. Tsfasman, Eds. Berlin: Springer, 1992, pp. 82-98.

[25] P. Kazakov, "Application of Polynomials to CRC and Spherical Codes", PhD Thesis, Technishe Universitet Delft, 2000.

[26] T. Kløve and V. Korzhik, "Error detecting codes, General Theory and Their Application in Feedback Communication systems" (Kluwer, Boston, MA 1995).

[27] S K. Leung, E. R. Barnes, and D. U. Friedman, "Some properties of undetected error probability of linear codes", *IEEE Thans. Inform. Theory* IT-25 (1979) 110-112.

[28] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code", *Bell syst. Tech. J.*, vol. 42, pp. 79-94, 1963.

[29] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes" (North-Holland, New York, 1997).

[30] J. Olsson, "On near-near-MDS codes", in *Prc. 5th Int. Workshop on Algebraic and Combinatorial Coding Theory* (Sozopol, Bulgaria, June 1-7, 1996), pp. 231-236

[31] J. Olsson, "Linear codes with performance close to the Singleton bound", thesis no 683, LIU-TEK-LIC-1998:18, Linköping Univ., Linköping, Sweden

[32] J. Olsson and W. Willems, "A Characterization of Certain Griesmer Codes: MMD Codes in a More General Sense", *IEEE Trans. Inform. Theory* 45 (1999) 2138-2142.

[33] J. Simonis, "The effective length of subcodes", *Applicable Algebra in Eng., Commun. and Comput.*, vol. 5, pp. 371-377, 1994.