Des. Codes Cryptogr. (2008) 48:125–140
DOI 10.1007/s10623-007-9130-1

Undetected error probability of q-ary constant weight codes

Shu-Tao Xia · Fang-Wei Fu

Received: 29 January 2007 / Revised: 5 July 2007 / Accepted: 4 September 2007 /
Published online: 29 November 2007

Abstract In this paper, we introduce a new combinatorial invariant called q-binomial moment for q-ary constant weight codes. We derive a lower bound on the q-binomial moments and introduce a new combinatorial structure called generalized (s, t)-designs which could achieve the lower bounds. Moreover, we employ the q-binomial moments to study the undetected error probability of q-ary constant weight codes. A lower bound on the undetected error probability for q-ary constant weight codes is obtained. This lower bound extends and unifies the related results of Abdel-Ghaffar for q-ary codes and Xia-Fu-Ling for binary constant weight codes. Finally, some q-ary constant weight codes which achieve the lower bounds are found.

Keywords Codes · Constant weight codes · Distance distribution · Error detection · Undetected error probability · Generalized t-design

AMS Classifications 94B05 · 94B65 · 94B70 · 05B05

1 Introduction

Let $V_q = \{0, v_1, \ldots, v_{q-1}\}$ be a finite set with q elements, where $q \geq 2$. For $\mathbf{x}, \mathbf{y}$ in V_q^n, the (Hamming) distance $d_H(\mathbf{x}, \mathbf{y})$ between $\mathbf{x}$ and $\mathbf{y}$ is defined as the number of coordinates

Dedicated to Professor Torleiv Kløve on the occasion of his 65th birthday.

S.-T. Xia (✉)
The Graduate School at Shenzhen, Tsinghua University, Shenzhen Guangdong 518055, P.R. China
e-mail: xiast@sz.tsinghua.edu.cn

S.-T. Xia
National Mobile Communications Research Laboratory, Southeast University,
Nanjing Jiangsu, P.R. China

F.-W. Fu
Chern Institute of Mathematics and KLPMC, Nankai University, Tianjin 300071, P.R. China
e-mail: fwfu@nankai.edu.cn

in which they differ. For $\mathbf{x}$ in V_q^n, its support $\mathrm{supp}(\mathbf{x})$ is defined as the set of nonzero coordinates in $\mathbf{x}$; its (Hamming) weight $w_H(\mathbf{x})$ is defined as the number of nonzero coordinates in $\mathbf{x}$, i.e., $w_H(\mathbf{x}) = |\mathrm{supp}(\mathbf{x})|$. A nonempty subset C of V_q^n with cardinality M is called a q-ary (n, M) code. The minimum distance d of C is the minimum distance between any two distinct codewords in C. The distance distribution of C is defined as

$$A'_i = \frac{1}{M} |\{(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in C,\ d_H(\mathbf{a}, \mathbf{b}) = i\}|, \quad i = 0, 1, \ldots, n. \tag{1}$$

Abdel-Ghaffar [1] defined the following combinatorial invariant F'_j of C:

$$F'_j = \sum_{i=1}^{j} A'_i \binom{n-i}{n-j}, \quad j = 1, 2, \ldots, n, \tag{2}$$

and showed that

$$A'_i = \sum_{j=1}^{i} F'_j \binom{n-j}{n-i} (-1)^{i-j}, \quad i = 1, 2, \ldots, n. \tag{3}$$

If the code C is used for error detection on a q-ary symmetric channel with symbol error probability p, $0 \le p \le (q-1)/q$, the undetected error probability is given by (see [13])

$$P_{ue}(C, p) = \sum_{i=1}^{n} A'_i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i}. \tag{4}$$

When a q-ary code is used for pure error detection, its error performance is characterized by the undetected error probability of this code. For a general introduction to the theory of error-detecting codes, we refer the reader to [13] and its references. Abdel-Ghaffar [1] found that the undetected error probability $P_{ue}(C, p)$ can be expressed by F'_j as follows:

$$P_{ue}(C, p) = \sum_{j=1}^{n} F'_j \left(\frac{p}{q-1}\right)^j \left(1 - \frac{qp}{q-1}\right)^{n-j}. \tag{5}$$

Using combinatorial arguments, Abdel-Ghaffar [1] obtained a lower bound on F'_j and then derived a lower bound on the undetected error probability $P_{ue}(C, p)$. Ashikhmin and Barg [2,3] called F'_j the binomial moments of the distance function and developed further bounds on the undetected error probability based on these. Dodunekova [6] also used the binomial moments to study the undetected error probability of linear codes.

Denote by $V_q^{n,w}$ the set of q-ary vectors of length n and weight w. A nonempty subset C of $V_q^{n,w}$ with cardinality M is called a q-ary (constant weight) (n, M, w) code. Note that a q-ary (n, M) code can be considered as a $(q+1)$-ary (n, M, n) code. Hence, the problem of studying the undetected error probability for q-ary constant weight codes extends and unifies the problems of studying ones for q-ary codes and binary constant weight codes.

Let C be a binary (n, M, w) code. Since the distance between any two codewords in C is an even number, it is more convenient to define the distance distribution of C as

$$A_i = \frac{1}{M} |\{(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in C,\ d_H(\mathbf{a}, \mathbf{b}) = 2i\}|, \quad i = 0, 1, \ldots, w. \tag{6}$$

When C is used for error detection, its undetected error probability can be written as

$$P_{ue}(C, p) = \sum_{i=1}^{w} A_i p^{2i} (1-p)^{n-2i}. \tag{7}$$

Binary constant weight codes have many applications in computer and communication systems (see [4,5,16,18]). The error detection capability of binary constant weight codes has been studied in [8–11] and [18–20]. Xia, Fu and Ling [20] introduced the following binomial moments for binary constant weight codes with distance distribution A_i:

$$F_j = \sum_{i=1}^{j} A_i \binom{w-i}{w-j}, \quad j = 1, 2, \ldots, w \tag{8}$$

and showed that

$$A_i = \sum_{j=1}^{i} F_j \binom{w-j}{w-i} (-1)^{i-j}, \quad i = 1, 2, \ldots, w, \tag{9}$$

$$P_{ue}(C, p) = (1-p)^{n-2w} \sum_{j=1}^{w} F_j p^{2j} (1-2p)^{w-j}. \tag{10}$$

By employing Q-transform quantities of the distance distribution A_i and their properties, Xia, Fu and Ling [20] obtained a lower bound on the binomial moments F_j and then derived a lower bound on the undetected error probability $P_{ue}(C, p)$ for the binary constant weight code C.

In this paper, we introduce a new combinatorial invariant for q-ary constant weight codes, which is called q-binomial moment. We derive a lower bound on the q-binomial moments and introduce a new combinatorial structure called generalized (s, t)-designs which could achieve the lower bounds. Moreover, we employ the q-binomial moments to study the undetected error probability of q-ary constant weight codes. A lower bound on the undetected error probability for q-ary constant weight codes is obtained. This lower bound extends and unifies the related results of Abdel-Ghaffar [1] for q-ary codes and Xia-Fu-Ling [20] for binary constant weight codes. Finally, some q-ary constant weight codes formed by generalized t-designs are found to achieve the lower bounds. The rest of this paper is organized as follows. In Sect. 2, we briefly review the distance distribution of q-ary constant weight codes and generalized t-designs. In Sect. 3, q-binomial moments and generalized (s, t)-designs are discussed. The applications of q-binomial moments to error detection are given in Sect. 4. Finally, we end with some concluding remarks in Sect. 5.

2 Preliminary

2.1 Distance distribution of q-ary constant weight codes

For $\mathbf{x}, \mathbf{y} \in V_q^{n,w}$, we denote (see [17])

$$f(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq 0,\ y_i \neq 0\}|, \quad e(\mathbf{x}, \mathbf{y}) = |\{i : x_i = y_i \neq 0\}|. \tag{11}$$

Then

$$d_H(\mathbf{x}, \mathbf{y}) = w_H(\mathbf{x}) + w_H(\mathbf{y}) - f(\mathbf{x}, \mathbf{y}) - e(\mathbf{x}, \mathbf{y}). \tag{12}$$

Let C be a q-ary (n, M, w) code. For a pair of integers (i, j), where $0 \leq j \leq i \leq w$, and $\mathbf{c} \in C$, define

$$A_{ij}(\mathbf{c}) = |\{\mathbf{c}' \in C \ :\ e(\mathbf{c}, \mathbf{c}') = w - i,\ \ f(\mathbf{c}, \mathbf{c}') = w - j\}|$$

and $A_{ij} = \frac{1}{M}\sum_{\mathbf{c}\in C} A_{ij}(\mathbf{c})$. Then, we have

$$A_{ij} = \frac{1}{M}|\{(\mathbf{x},\mathbf{y}) \in C \times C \ : \ e(\mathbf{x},\mathbf{y}) = w - i, \ \ f(\mathbf{x},\mathbf{y}) = w - j\}| \tag{13}$$

and

$$A_{00} = 1, \quad \sum_{i=0}^{w}\sum_{j=0}^{i} A_{ij} = M. \tag{14}$$

It follows from (12) that the relation between the distance distribution $\{A'_l\}$ and $\{A_{ij}\}$ is given by

$$A'_l = \sum_{0\le j\le i\le w,\ i+j=l} A_{ij}. \tag{15}$$

2.2 Generalized t-designs, H-designs, and generalized Steiner systems

Let X be a finite set of n elements called points, and let $\mathcal{B}$ be a finite family of w-subsets of X called blocks. Then the pair $(X, \mathcal{B})$ is called a t-(n, w, λ)-design, or briefly a *t-design*, if any t-subset of X is contained in exactly λ blocks. A *Steiner system* is a t-$(n, w, 1)$-design, and is usually denoted by $S(t, w, n)$. It is known [14, p. 63] that a binary constant weight code of length n, weight w, and minimum distance at least $2(w - t + 1)$ can be obtained from an $S(t, w, n)$. Below we give the definition of a generalized t-design over V_q introduced by Etzion [7].

Definition 1 Let X be a set of points whose cardinality is nk where $k = q - 1$, and let $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$ be a partition of X into n sets of cardinality k. The members of $\mathcal{G}$ are called groups. A *transverse* of $\mathcal{G}$ is a subset of X that meets each group in at most one point. Let $\mathcal{B}$ be a finite family of w-element transverses of $\mathcal{G}$ called blocks. Then the triple $(X, \mathcal{G}, \mathcal{B})$ is called a generalized t-(n, w, λ, k)-design, or briefly a *generalized t-design*, if any t-element transverse of $\mathcal{G}$ is contained in exactly λ blocks.

Clearly, a generalized t-(n, w, λ, k)-design has $\lambda(q-1)^t\binom{n}{t}/\binom{w}{t}$ blocks. When $\lambda = 1$ the generalized t-design is the $H(n, k, w, t)$-design introduced by Hanani [12] (the notation of H-design is due to Mills [15]). Etzion [7] presented a method to construct a q-ary constant weight code from a generalized t-design.

Proposition 1 [7] *A q-ary constant weight code $C \subseteq V_q^{n,w}$ can be obtained from a generalized t-design $(X, \mathcal{G}, \mathcal{B})$ as follows:*
Let $G_i = \{\alpha_{1i}, \alpha_{2i}, \ldots, \alpha_{ki}\}$, $i = 1, 2, \ldots, n$. The code C has a codeword for each block. Let $\{\alpha_{j_1 i_1}, \alpha_{j_2 i_2}, \ldots, \alpha_{j_w i_w}\}$ or $\{[i_1, j_1], [i_2, j_2], \ldots, [i_w, j_w]\}$ be a block in $\mathcal{B}$. By the definition of w-transverse, $i_1, i_2, \ldots, i_w$ are pairwise different. Recall that $V_q = \{0, v_1, \ldots, v_{q-1}\}$. The corresponding codeword is given by $\mathbf{c} = (c_1, c_2, \ldots, c_n)$, where $c_{i_1} = v_{j_1}, c_{i_2} = v_{j_2}, \ldots, c_{i_w} = v_{j_w}$ and all other components are zero.

It is known that an H-design can give a q-ary constant weight code with minimum distance between $w-t+1$ and $2(w-t)+1$ [7]. An H-design $H(n, k, w, t)$ which forms a q-ary constant weight code with minimum distance at least $2(w-t)+1$ is called a generalized Steiner system $GS(t, w, n, k)$ by Etzion [7]. Clearly, a generalized t-design is still a generalized t'-design for any $t' \le t$.

3 Q-binomial moments and generalized (s, t)-designs

Let (u, v) be a pair of integers, where $0 \le v \le u \le w$. Let $J^{(w-v)} = \emptyset$ if $v = w$ and $J^{(w-v)} = \{j_1, j_2, \ldots, j_{w-v}\}$ be an ordered set of positions if $v < w$, where $1 \le j_1 < j_2 < \cdots < j_{w-v} \le n$. Let $I^{(w-u)} = \emptyset$ if $u = w$ and $I^{(w-u)} = \{i_1, i_2, \ldots, i_{w-u}\}$ be an ordered subset of $J^{(w-v)}$ if $u < w$, i.e., $I^{(w-u)} \subseteq J^{(w-v)}$ and $i_1 < i_2 < \cdots < i_{w-u}$. Let $E^{(w-u)} = \emptyset$ if $u = w$ and $E^{(w-u)} = \{e_1, e_2, \ldots, e_{w-u}\} \subseteq V_q \setminus \{0\}$ if $u < w$. Let C be a q-ary (n, M, w) code. Define a subset $C(\cdot, \cdot, \cdot)$ of C as follows:

$$C(\emptyset; \emptyset; \emptyset) = C \quad \text{if } u = v = w, \tag{16}$$

and

$$C(J^{(w-v)}; \emptyset; \emptyset) = \{(c_1, \ldots, c_n) \in C : c_{j_1} \neq 0, \ldots, c_{j_{w-v}} \neq 0\} \text{ if } v < u = w, \tag{17}$$

and otherwise, i.e., if $v \le u < w$,

$$\begin{aligned} C(J^{(w-v)}; I^{(w-u)}; E^{(w-u)}) &= C(j_1, \ldots, j_{w-v}; i_1, \ldots, i_{w-u}; e_1, \ldots, e_{w-u}) \\ &= \{(c_1, \ldots, c_n) \in C : c_{j_1} \neq 0, \ldots, c_{j_{w-v}} \neq 0;\ c_{i_1} = e_1, \ldots, c_{i_{w-u}} = e_{w-u}\}. \end{aligned} \tag{18}$$

For a codeword $\mathbf{c} = (c_1, \ldots, c_n) \in C$, we say that $\mathbf{c}$ *covers* $(I^{(w-u)}; E^{(w-u)})$ if $c_{i_1} = e_1, c_{i_2} = e_2, \ldots, c_{i_{w-u}} = e_{w-u}$. By Definition 1 and Proposition 1, it is easy to see that C is formed by a generalized t-$(n, w, \lambda, q-1)$-design if and only if there are exactly λ codewords in C such that each of which covers $(I^{(t)}; E^{(t)})$ for any $(I^{(t)}; E^{(t)})$. Define

$$\xi_{uv} = \frac{(q-1)^{w-u} \begin{pmatrix} n \\ w-v \end{pmatrix}}{\begin{pmatrix} w \\ w-v \end{pmatrix}} = \frac{(q-1)^{w-u} \begin{pmatrix} n \\ w \end{pmatrix}}{\begin{pmatrix} n-w+v \\ v \end{pmatrix}}. \tag{19}$$

Clearly, $J^{(w-v)} \subseteq \{1, 2, \ldots, n\}$ has $\begin{pmatrix} n \\ w-v \end{pmatrix}$ choices, $I^{(w-u)} \subseteq J^{(w-v)}$ has $\begin{pmatrix} w-v \\ w-u \end{pmatrix}$ choices for fixed $J^{(w-v)}$, and $E^{(w-u)}$ has $(q-1)^{w-u}$ choices. Since $\begin{pmatrix} w \\ w-v \end{pmatrix} \begin{pmatrix} w-v \\ w-u \end{pmatrix} = \begin{pmatrix} w \\ u \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$, there is a total of

$$\begin{pmatrix} n \\ w-v \end{pmatrix} \begin{pmatrix} w-v \\ w-u \end{pmatrix} (q-1)^{w-u} = \begin{pmatrix} w \\ u \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} \xi_{uv} \tag{20}$$

different ways of choosing $J^{(w-v)}$, $I^{(w-u)} \subseteq J^{(w-v)}$, and $E^{(w-u)}$.

Lemma 1 *For a pair of integers* (u, v), *where* $0 \le v \le u \le w$,

$$\sum_{J^{(w-v)}} \sum_{I^{(w-u)} \subseteq J^{(w-v)}} \sum_{E^{(w-u)}} |C(J^{(w-v)}; I^{(w-u)}; E^{(w-u)})| = \begin{pmatrix} w \\ u \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} M. \tag{21}$$

Proof When $u = v = w$, the left-hand side of (21) becomes $|C|$ and the conclusion follows. When $v < u = w$, the left-hand side of (21) becomes $\sum_{J^{(w-v)}} |C(J^{(w-v)}; \emptyset; \emptyset)|$ and the conclusion follows by the fact that each codeword is counted $\begin{pmatrix} w \\ w-v \end{pmatrix}$ times. When

$v \le u < w$, noting that $\binom{w}{w-v}\binom{w-v}{w-u} = \binom{w}{u}\binom{u}{v}$, the conclusion follows by the fact that each codeword is counted $\binom{w}{w-v}\binom{w-v}{w-u}$ times. □

Definition 2 For $u = 1, 2, \ldots, w$ and $v = 0, 1, \ldots, u$, the quantities

$$F_{uv} = \frac{1}{M} \sum_{J^{(w-v)}} \sum_{I^{(w-u)} \subseteq J^{(w-v)}} \sum_{E^{(w-u)}} |C(J^{(w-v)}; I^{(w-u)}; E^{(w-u)})| \cdot (|C(J^{(w-v)}; I^{(w-u)}; E^{(w-u)})| - 1) \tag{22}$$

are called q-binomial moments of a q-ary (n, M, w) code C.

By convention, let $0^0 = 1$, $\binom{0}{0} = 1$; $\binom{n}{j} = 0$ for $j < 0$ or $n < j$; $\sum_{k=i}^{j} a_k = 0$ if $i > j$; $A_{ij} = F_{ij} = 0$ if $i < j$, and $F_{00} = 0$. In Definition 2 we call F_{uv} the q-binomial moments of C since we have the following lemma.

Lemma 2

$$F_{uv} = \sum_{i=1}^{u} \sum_{j=0}^{v} A_{ij} \binom{w-i}{w-u} \binom{u-j}{u-v}, \quad 1 \le u \le w, \ 0 \le v \le u. \tag{23}$$

In particular,

$$F_{ww} = M - 1. \tag{24}$$

Proof For a given codeword $\mathbf{c} = (c_1, \ldots, c_n) \in C$, form an $(M-1) \times \binom{w}{w-v}\binom{w-v}{w-u}$ matrix as follows. The rows are labelled by codewords different from $\mathbf{c}$ and the columns are labelled by $J^{(w-v)} \subseteq \mathrm{supp}(\mathbf{c})$ and $I^{(w-u)} \subseteq J^{(w-v)}$. The entry in the row labelled by $\mathbf{c}'$ and the column labelled by $(J^{(w-v)}; I^{(w-u)})$ is equal to one if

$$\mathbf{c}' \in C(J^{(w-v)}; I^{(w-u)}; c_{i_1}, \ldots, c_{i_{w-u}})$$

and zero otherwise. There are exactly

$$|C(J^{(w-v)}; I^{(w-u)}; c_{i_1}, \ldots, c_{i_{w-u}})| - 1$$

codewords in $C(J^{(w-v)}; I^{(w-u)}; c_{i_1}, \ldots, c_{i_{w-u}})$ different from $\mathbf{c}$. Hence, the column labelled by $(J^{(w-v)}; I^{(w-u)})$ has exactly that many ones.

On the other hand, for a codeword $\mathbf{c}' \in C \setminus \{\mathbf{c}\}$ such that $e(\mathbf{c}', \mathbf{c}) = w - i$ and $f(\mathbf{c}', \mathbf{c}) = w - j$, it is easy to see that the row labelled by $\mathbf{c}'$ has exactly $\binom{w-i}{w-u}\binom{u-j}{u-v}$ ones.

Summing the total number of ones in the matrix in two different ways depending on whether rows or columns are considered first, we get

$$\sum_{i=1}^{u} \sum_{j=0}^{v} A_{ij}(\mathbf{c}) \binom{w-i}{w-u} \binom{u-j}{u-v} = \sum_{J^{(w-v)} \subseteq \mathrm{supp}(\mathbf{c})} \sum_{I^{(w-u)} \subseteq J^{(w-v)}} (|C(J^{(w-v)}; I^{(w-u)}; c_{i_1}, \ldots, c_{i_{w-u}})| - 1).$$

Averaging over all codewords $\mathbf{c}$ in C, the left-hand side is equal to

$$\sum_{i=1}^{u}\sum_{j=0}^{v} A_{ij}\binom{w-i}{w-u}\binom{u-j}{u-v},$$

and the right-hand-side is equal to

$$\begin{aligned}&\frac{1}{M}\sum_{\mathbf{c}\in C}\sum_{J^{(w-v)}\subseteq \mathrm{supp}(\mathbf{c})}\sum_{I^{(w-u)}\subseteq J^{(w-v)}}(|C(J^{(w-v)};I^{(w-u)};c_{i_1},\ldots,c_{i_{w-u}})|-1)\\&=\frac{1}{M}\sum_{J^{(w-v)}}\sum_{I^{(w-u)}\subseteq J^{(w-v)}}\sum_{E^{(w-u)}}\\&\qquad\sum_{\mathbf{c}\in C(J^{(w-v)};I^{(w-u)};E^{(w-u)})}(|C(J^{(w-v)};I^{(w-u)};c_{i_1},\ldots,c_{i_{w-u}})|-1),\end{aligned}$$

which equals F_{uv} by (22). In particular, when $u=v=w$, by (23) and (14),

$$F_{ww}=\sum_{i=1}^{w}\sum_{j=0}^{i}A_{ij}=\sum_{i=0}^{w}\sum_{j=0}^{i}A_{ij}-A_{00}=M-1.$$

□

Remark 1 For any $1\le u\le w$ and $0\le v\le u$, it follows from Lemma 2 that $F_{uv}=0$ if and only if $A_{ij}=0$ for any $1\le i\le u$ and $0\le j\le v$. This is equivalent to the fact that $F_{u'v'}=0$ for any $1\le u'\le u$ and $0\le v'\le v$. Moreover, $d>u+v$ implies $F_{uv}=0$, where d is the minimum distance of C.

Remark 2 **(i)** For the case of $w=n$, C can be considered as a $(q-1)$-ary code. By (11) and (13), $A_{ij}=0$ if $j>0$. Hence, by Lemma 2 and (2), when $w=n$,

$$F_{uv}=\binom{u}{v}F'_u, \tag{25}$$

where F'_u are the binomial moments of the $(q-1)$-ary code C defined in (2).

(ii) For the case of $q=2$, C is a binary constant weight code. By (11) and (13), $A_{ij}=0$ if $j<i$. Hence, by Lemma 2 and (8), when $q=2$,

$$F_{uv}=\binom{w-v}{w-u}F_v, \tag{26}$$

where F_v are the binomial moments of the binary constant weight code C defined in (8).

Lemma 3 *For any* $1\le i\le w$ *and* $0\le j\le i$,

$$A_{ij}=\sum_{u=1}^{i}\sum_{v=0}^{j}F_{uv}\binom{w-u}{w-i}\binom{u-v}{u-j}(-1)^{i+j-u-v}. \tag{27}$$

Proof For any $1 \le i' \le w$ and $0 \le j' \le i'$,

$$\begin{aligned}
&\sum_{u=i'}^{i}\sum_{v=j'}^{j}\binom{w-i'}{w-i}\binom{i-i'}{u-i'}\binom{u-j'}{u-j}\binom{j-j'}{v-j'}(-1)^{i+j-u-v}\\
&\quad=\sum_{u=i'}^{i}\binom{w-i'}{w-i}\binom{i-i'}{u-i'}(-1)^{i-u}\cdot\binom{u-j'}{u-j}\sum_{v=j'}^{j}\binom{j-j'}{v-j'}(-1)^{j-v}\\
&\quad=\sum_{u=i'}^{i}\binom{w-i'}{w-i}\binom{i-i'}{u-i'}(-1)^{i-u}\cdot\delta_{jj'}=\delta_{ii'}\delta_{jj'},
\end{aligned}$$

where $\delta_{xy}=1$ if $x=y$ and $\delta_{xy}=0$ otherwise. Hence, by Lemma 2,

$$\begin{aligned}
&\sum_{u=1}^{i}\sum_{v=0}^{j}F_{uv}\binom{w-u}{w-i}\binom{u-v}{u-j}(-1)^{i+j-u-v}\\
&\quad=\sum_{u=1}^{i}\sum_{v=0}^{j}\sum_{i'=1}^{u}\sum_{j'=0}^{v}A_{i'j'}\binom{w-i'}{w-u}\binom{u-j'}{u-v}\binom{w-u}{w-i}\binom{u-v}{u-j}(-1)^{i+j-u-v}\\
&\quad=\sum_{i'=1}^{i}\sum_{j'=0}^{j}A_{i'j'}\sum_{u=i'}^{i}\sum_{v=j'}^{i'}\binom{w-i'}{w-i}\binom{i-i'}{u-i'}\binom{u-j'}{u-j}\binom{j-j'}{v-j'}(-1)^{i+j-u-v}\\
&\quad=\sum_{i'=1}^{i}\sum_{j'=0}^{j}A_{i'j'}\delta_{ii'}\delta_{jj'}\;=\;A_{ij}.
\end{aligned}$$

□

We need the following lemma [1] to establish our results.

Lemma 4 [1] *Given t nonnegative integers $T_1,\ldots,T_t$ that sum to T, then*

$$\sum_{l=1}^{t}T_l(T_l-1)\ge(\lceil T/t\rceil-1)(2T-t\lceil T/t\rceil),\tag{28}$$

where equality holds if and only if $\lfloor T/t\rfloor\le T_l\le\lceil T/t\rceil$ for all $l=1,2,\ldots,t$.

Now we give a lower bound on the q-binomial moments of q-ary constant weight codes.

Theorem 1 *Let C be a q-ary (n,M,w) code. Let (u,v) be a pair of integers, where $1\le u\le w$ and $0\le v\le u$. Let F_{uv} be the q-binomial moments of C defined in (22) and (23). Then*

$$F_{uv}\ge\alpha_{uv}\triangleq\frac{\binom{w}{u}\binom{u}{v}}{M}\left(\left\lceil\frac{M}{\xi_{uv}}\right\rceil-1\right)\left(2M-\xi_{uv}\left\lceil\frac{M}{\xi_{uv}}\right\rceil\right),\tag{29}$$

where ξ_{uv} is defined in (19). In a slightly weaker version,

$$F_{uv}\ge\beta_{uv}\triangleq\max\left\{\binom{w}{u}\binom{u}{v}\left(\frac{M}{\xi_{uv}}-1\right),0\right\}.\tag{30}$$

Moreover,

(i) *when* $M \le \xi_{uv}$, $F_{uv} = \beta_{uv}$ *if and only if* $F_{uv} = 0$;

(ii) *when* $M > \xi_{uv}$, $F_{uv} = \beta_{uv}$ *if and only if* M/ξ_{uv} *is an integer and* $|C(J^{(w-v)}; I^{(w-u)}; E^{(w-u)})| = M/\xi_{uv}$ *for any* $J^{(w-v)}$, $I^{(w-u)} \subseteq J^{(w-v)}$, *and* $E^{(w-u)}$.

Proof Set $T = \binom{w}{u}\binom{u}{v} M$. By (20), there are totally $t = \binom{w}{u}\binom{u}{v}\xi_{uv}$ different ways of choosing $J^{(w-v)}$, $I^{(w-u)} \subseteq J^{(w-v)}$, and $E^{(w-u)}$. We index the corresponding $C(J^{(w-v)}; I^{(w-u)}; E^{(w-u)})$ by $l = 1, 2, \ldots, t$ and set $T_l = |C(J^{(w-v)}; I^{(w-u)}; E^{(w-u)})|$. Then $T/t = M/\xi_{uv}$ and $\sum_{l=1}^{t} T_l = T$ by Lemma 1. Hence, (29) follows from (22) and Lemma 4.

The case of $M \le \xi_{uv}$: It is easy to see that $\alpha_{uv} = \beta_{uv} = 0$. Hence, (30) holds and (i) is obvious.

The case of $M > \xi_{uv}$: Let $M = a\xi_{uv} + b$, where $a \ge 1$ and $0 \le b < \xi_{uv}$. Clearly, $\alpha_{uv} = \beta_{uv}$ if $b = 0$. On the other hand, if $0 < b < \xi_{uv}$, then $\left\lceil \frac{M}{\xi_{uv}} \right\rceil = a + 1$. Since $0 < (\xi_{uv} - b)b \le \xi_{uv}^2/4$, we have

$$0 < \alpha_{uv} - \beta_{uv} = \binom{w}{u}\binom{u}{v} \frac{(\xi_{uv} - b)b}{(a\xi_{uv} + b)\xi_{uv}} \le \binom{w}{u}\binom{u}{v} \frac{\xi_{uv}}{4M} < \binom{w}{u}\binom{u}{v}/4.$$

Hence, $\alpha_{uv} \ge \beta_{uv}$, which implies (30), and $\alpha_{uv} = \beta_{uv} \iff M/\xi_{uv}$ is an integer. Furthermore, $F_{uv} = \beta_{uv}$ is equivalent to $\alpha_{uv} = \beta_{uv}$ and $F_{uv} = \alpha_{uv}$. Therefore, by Lemma 4, $F_{uv} = \beta_{uv}$ if and only if M/ξ_{uv} is an integer and $T_l = M/\xi_{uv}$ for all $l = 1, 2, \ldots, t$. □

Remark 3 Let C be a q-ary (n, M) code. Then C can be considered as a $(q+1)$-ary (n, M, n) code. Using Theorem 1 for a $(q+1)$-ary (n, M, n) code, and noting that $\xi_{uv} = q^{n-u}$ by (19), and $F_{uv} = \binom{u}{v} F'_u$ by Remark 2, we have

$$F'_u \ge \eta_u \triangleq \frac{\binom{w}{u}}{M}\left(\left\lceil \frac{M}{q^{n-u}} \right\rceil - 1\right)\left(2M - q^{n-u}\left\lceil \frac{M}{q^{n-u}} \right\rceil\right), \tag{31}$$

$$F'_u \ge \theta_u \triangleq \max\left\{\binom{w}{u}\left(\frac{M}{q^{n-u}} - 1\right), 0\right\}. \tag{32}$$

These are just the Abdel-Ghaffar bounds (see [1,Lemma 4] and [2,Theorem 9]) on the binomial moments of q-ary codes.

Remark 4 Let C be a binary (n, M, w) code. By Theorem 1, and noting that when $q = 2$, $\xi_{uv} = \binom{n}{w} \Big/ \binom{n-w+v}{v}$ by (19), and $F_{uv} = \binom{w-v}{w-u} F_v$ by Remark 2, we have

$$F_v \ge \rho_v \triangleq \frac{\binom{w}{v}}{M}\left(\left\lceil \frac{M\binom{n-w+v}{v}}{\binom{n}{w}} \right\rceil - 1\right)\left(2M - \frac{\binom{n}{w}}{\binom{n-w+v}{v}}\left\lceil \frac{M\binom{n-w+v}{v}}{\binom{n}{w}} \right\rceil\right), \tag{33}$$

$$F_v \ge \tau_v \triangleq \max\left\{\binom{w}{v}\left(\frac{M\binom{n-w+v}{v}}{\binom{n}{w}} - 1\right), 0\right\}. \tag{34}$$

Bound (34) is just the Xia-Fu-Ling bound (see [20,Proof of Theorem 1]) on the binomial moments of binary constant weight codes. By the proof of Theorem 1, if $M\binom{n-w+v}{v}\Big/\binom{n}{w} \leq 1$ or $M\binom{n-w+v}{v}\Big/\binom{n}{w}$ is an integer, $\rho_v = \tau_v$; otherwise, $0 < \rho_v - \tau_v < \binom{w}{v}/4$. Hence, (33) slightly improves on (34) if $M\binom{n-w+v}{v}\Big/\binom{n}{w} > 1$ and $M\binom{n-w+v}{v}\Big/\binom{n}{w}$ is not an integer.

In order to further characterize the condition for which the bound (30) in Theorem 1 is tight, we introduce a new combinatorial structure called generalized (s, t)-design over V_q. With the same notations as in Sect. 2.2, let X be a set of nk points, where $k = q - 1$, and $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$ a partition of X, where G_i are groups and $|G_i| = k$, and $\mathcal{B}$ a finite family of blocks which are w-element transverses of $\mathcal{G}$. For a transverse S, the *support* of S, say $\mathrm{supp}(S)$, is defined as the set of index $i \in \{1, 2, \ldots, n\}$ such that S meets G_i in exactly one point. For two fixed integers s, t where $1 \leq s \leq t \leq w$, let S be an s-element transverse, and $L^{(t)}$ be a t-subset of $\{1, 2, \ldots, n\}$ such that $\mathrm{supp}(S) \subseteq L^{(t)} \subseteq \{1, 2, \ldots, n\}$. The *restriction* of $\mathcal{B}$ to $L^{(t)}$, say $\mathcal{B}(L^{(t)})$, is defined as the set of blocks such that each block meets G_i in exactly one point for any $i \in L^{(t)}$.

Definition 3 The triple $(X, \mathcal{G}, \mathcal{B})$ is called a generalized (s, t)-(n, w, λ, k)-design, or briefly a *generalized* (s, t)*-design*, if any s-element transverse of $\mathcal{G}$, say S, is contained in exactly λ blocks in $\mathcal{B}(L^{(t)})$ for any t-subset $L^{(t)}$ of $\{1, 2, \ldots, n\}$ such that $L^{(t)} \supseteq \mathrm{supp}(S)$.

Clearly, a generalized (s, t)-design has $M = \lambda(q-1)^s\binom{n}{t}\Big/\binom{w}{t}$ blocks. Like Proposition 1, we can also form a q-ary (n, M, w) code from the generalized (s, t)-design.

Proposition 2 *For any two pairs of integers* (s, t) *and* (s', t') *such that* $1 \leq s' \leq s$ *and* $s' \leq t' \leq t$, *a generalized* (s, t)-(n, w, λ, k)*-design is also a generalized* (s', t')-(n, w, λ', k)*-design with* $\lambda' = \lambda(q-1)^{s-s'}\binom{n-t'}{t-t'}\Big/\binom{w-t'}{t-t'}$.

Proof Suppose $(X, \mathcal{G}, \mathcal{B})$ is a generalized (s, t)-(n, w, λ, k)-design. The proof is broken into two parts.

First, we show that for any s' where $1 \leq s' \leq s$, $(X, \mathcal{G}, \mathcal{B})$ is a generalized (s', t)-design. Given any s'-element transverse S and any t-subset $L^{(t)}$ of $\{1, 2, \ldots, n\}$ such that $L^{(t)} \supseteq \mathrm{supp}(S)$. Since $(X, \mathcal{G}, \mathcal{B})$ is a generalized (s, t)-design, it is easy to see that there are $\lambda(q-1)^{s-s'}$ blocks in $\mathcal{B}(L^{(t)})$ which contain S. This implies that $(X, \mathcal{G}, \mathcal{B})$ is a generalized (s', t)-(n, w, λ_1, k)-design with $\lambda_1 = \lambda(q-1)^{s-s'}$.

Then, we show that for any t' where $s' \leq t' \leq t$, $(X, \mathcal{G}, \mathcal{B})$ is a generalized (s', t')-design. Given any s'-element transverse S and any t'-subset $L^{(t')}$ of $\{1, 2, \ldots, n\}$ such that $L^{(t')} \supseteq \mathrm{supp}(S)$, there are $\binom{n-t'}{t-t'}$ choices of $L^{(t)}$ such that $L^{(t)} \supseteq L^{(t')}$. Since $(X, \mathcal{G}, \mathcal{B})$ is a generalized (s', t)-design, it is easy to see that there are $\lambda_1\binom{n-t'}{t-t'}\Big/\binom{w-t'}{t-t}$ blocks in $\mathcal{B}(L^{(t')})$ which contain S since there are $\binom{w-t'}{t-t'}$ repetitions for each desirable

block. This implies that $(X, \mathcal{G}, \mathcal{B})$ is a generalized (s', t)-(n, w, λ', k)-design with $\lambda' = \lambda_1 \binom{n-t'}{t-t'} \Big/ \binom{w-t'}{t-t'}$.

Combining these assertions, the proposition follows. □

By Proposition 2, the next result is obvious.

Proposition 3 *A necessary condition for the existence of a generalized (s, t)-design is that for each pair (s', t') where $1 \le s' \le s$ and $s' \le t' \le t$, $\lambda(q-1)^{s-s'} \binom{n-t'}{t-t'} \Big/ \binom{w-t'}{t-t'}$ is an integer.*

It is easy to see that a generalized t-design is equivalent to a generalized (t, t)-design. Hence, Proposition 2 implies the following results.

Proposition 4 *For $1 \le s \le t \le w$, a generalized (s, t)-design is a generalized s-design and a generalized t-design is a generalized (s, t)-design.*

Combining Theorem 1 and the definition of generalized (s, t)-designs, we have:

Corollary 1 *For any $1 \le u \le w$ and $0 \le v \le u$, $F_{uv} = \beta_{uv}$ if and only if*

(i) *when $M \le \xi_{uv}$, $A_{ij} = 0$ for any $1 \le i \le u, 0 \le j \le v$;*

(ii) *when $M > \xi_{uv}$, C is formed by a generalized $(w-u, w-v)$-design.*

Proof (i) follows from Theorem 1 (i) and Remark 1.

Below, we assume that $M > \xi_{uv}$. By the construction procedure of a q-ary (n, M, w) code C from a generalized $(w-u, w-v)$-design, we know that

(a1) a $(w-u)$-transverse S corresponds to a pair of sets $(I^{(w-u)}; E^{(w-u)})$ such that supp $(S) = I^{(w-u)}$;
(a2) $L^{(w-v)} = J^{(w-v)}$ and $L^{(w-v)} \supseteq \text{supp}(S) \Leftrightarrow I^{(w-u)} \subseteq J^{(w-v)}$;
(a3) the codewords in $C(J^{(w-v)}; I^{(w-u)}; E^{(w-u)})$ correspond to the blocks in $\mathcal{B}(L^{(w-v)})$ which contain S.

Suppose that $F_{uv} = \beta_{uv}$. By Theorem 1 (ii), M/ξ_{uv} is an integer. For a fixed $(w-u)$-transverse S and any $(w-v)$-subset $L^{(w-v)}$ of $\{1, 2, \ldots, n\}$ such that $L^{(w-v)} \supseteq \text{supp}(S)$, by (a1) and (a2), S and $L^{(w-v)}$ correspond to a triple $(J^{(w-v)}, I^{(w-u)}, E^{(w-u)})$, where $I^{(w-u)} \subseteq J^{(w-v)}$. By (a3) and Theorem 1 (ii), the number of blocks in $\mathcal{B}(L^{(w-v)})$ which contain S is equal to $|C(J^{(w-v)}; I^{(w-u)}; E^{(w-u)})| = M/\xi_{uv}$. In other words, C is formed by a generalized $(w-u, w-v)$-design with $\lambda = M/\xi_{uv}$.

On the other hand, suppose C is formed by a generalized $(w-u, w-v)$-design. It is easy to check that a generalized $(w-u, w-v)$-design with M blocks must satisfy $\lambda = M/\xi_{uv}$, which implies that M/ξ_{uv} should be an integer. Moreover, for any $J^{(w-v)}$, $I^{(w-u)} \subseteq J^{(w-v)}$, and $E^{(w-u)}$, by (a1), (a2), and the definition of generalized $(w-u, w-v)$-designs, the $(w-u)$-transverse S which corresponds to $(I^{(w-u)}; E^{(w-u)})$ is contained in exactly $\lambda = M/\xi_{uv}$ blocks in $\mathcal{B}(L^{(w-v)})$ since $L^{(w-v)} = J^{(w-v)} \supseteq I^{(w-u)} = \text{supp}(S)$. Furthermore, by (a3), we have $|C(J^{(w-v)}; I^{(w-u)}; E^{(w-u)})| = \lambda = M/\xi_{uv}$. Hence, by Theorem 1 (ii), $F_{uv} = \beta_{uv}$. □

By Corollary 1 and Proposition 4, the next corollary follows.

Corollary 2 *Suppose* $M > \xi_{uv}$.

(i) *If* C *is formed by a generalized* $(w-v)$*-design, then* $F_{uv} = \beta_{uv}$.

(ii) *If* $F_{uv} = \beta_{uv}$, *then* C *is formed by a generalized* $(w-u)$*-design.*

4 Lower bounds on $P_{ue}(C, p)$

Applications of q-binomial moments F_{uv} to error detection are discussed in this section. We obtain an alternative expression in terms of F_{uv} for the undetected error probability $P_{ue}(C, p)$ of a q-ary constant weight code C. Then, we derive two lower bounds on $P_{ue}(C, p)$ by employing the two lower bounds on F_{uv} in the last section. These lower bounds on $P_{ue}(C, p)$ extend and unify the related results of Abdel-Ghaffar for q-ary codes and Xia-Fu-Ling for binary constant weight codes. Finally, some q-ary constant weight codes formed by generalized t-designs are found to achieve one of the lower bounds.

Clearly, by (4) and (15), we can write $P_{ue}(C, p)$ in terms of A_{ij} as follows:

$$P_{ue}(C, p) = \sum_{i=1}^{w} \sum_{j=0}^{i} A_{ij} \left(\frac{p}{q-1}\right)^{i+j} (1-p)^{n-i-j}. \tag{35}$$

Note that

$$P_{ue}(C, 0) = 0, \quad P_{ue}\left(C, \frac{q-1}{q}\right) = \frac{M-1}{q^n}. \tag{36}$$

The next lemma shows that $P_{ue}(C, p)$ can be alternatively expressed in terms of F_{uv}.

Lemma 5 *Let* C *be a* q*-ary* (n, M, w) *code. Let* F_{uv} *be the* q*-binomial moments of* C *defined in* (22) *and* (23). *Then*

$$P_{ue}(C, p) = \sum_{u=1}^{w} \sum_{v=0}^{u} F_{uv} \left(1 - \frac{qp}{q-1}\right)^{w-v} \left(\frac{p}{q-1}\right)^{u+v} (1-p)^{n-w-u}. \tag{37}$$

Proof It is easy to see that for $1 \le u \le w$ and $0 \le v \le u$,

$$\begin{aligned}
&\sum_{i=u}^{w} \sum_{j=v}^{u} \binom{w-u}{w-i} \binom{u-v}{u-j} (-1)^{i+j-u-v} \left(\frac{p}{q-1}\right)^{i+j} (1-p)^{n-i-j} \\
&= \sum_{i=u}^{w} \binom{w-u}{w-i} (-1)^{i-u} \sum_{j=0}^{u-v} \binom{u-v}{u-v-j} (-1)^{j} \left(\frac{p}{q-1}\right)^{i+v+j} (1-p)^{n-i-v-j} \\
&= \sum_{i=u}^{w} \binom{w-u}{w-i} (-1)^{i-u} \left(\frac{p}{q-1}\right)^{i+v} (1-p)^{n-i-u} \left(1 - \frac{qp}{q-1}\right)^{u-v} \\
&= \left(1 - \frac{qp}{q-1}\right)^{w-v} \left(\frac{p}{q-1}\right)^{u+v} (1-p)^{n-w-u}.
\end{aligned} \tag{38}$$

Hence, by (35), (38) and Lemma 3,

$$P_{ue}(C,p) = \sum_{i=1}^{w}\sum_{j=0}^{i} A_{ij}\left(\frac{p}{q-1}\right)^{i+j}(1-p)^{n-i-j}$$
$$= \sum_{u=1}^{w}\sum_{v=0}^{u} F_{uv}\sum_{i=u}^{w}\sum_{j=v}^{u}\binom{w-u}{w-i}\binom{u-v}{u-j}(-1)^{i+j-u-v}\left(\frac{p}{q-1}\right)^{i+j}(1-p)^{n-i-j}$$
$$= \sum_{u=1}^{w}\sum_{v=0}^{u} F_{uv}\left(1-\frac{qp}{q-1}\right)^{w-v}\left(\frac{p}{q-1}\right)^{u+v}(1-p)^{n-w-u}.$$

□

Remark 5 **(i)** Let C be a q-ary (n, M) code. Then C can be considered as a $(q+1)$-ary (n, M, n) code. Note that C is used for error detection on a q-ary symmetric channel with symbol error probability p (not a $(q+1)$-ary symmetric channel) since the codewords of C have no zero components. It is easy to see from Lemma 5 and Remark 2(i) that (5) follows directly from (37).

(ii) Let C be a binary (n, M, w) code. It is easy to see from Lemma 5 and Remark 2(ii) that (10) follows directly from (37).

Theorem 2 *Let C be a q-ary (n, M, w) code. Then*

$$P_{ue}(C,p) \geq \sum_{u=1}^{w}\sum_{v=0}^{u}\alpha_{uv}\left(1-\frac{qp}{q-1}\right)^{w-v}\left(\frac{p}{q-1}\right)^{u+v}(1-p)^{n-w-u} \tag{39}$$
$$\geq \sum_{u=1}^{w}\sum_{v=0}^{u}\beta_{uv}\left(1-\frac{qp}{q-1}\right)^{w-v}\left(\frac{p}{q-1}\right)^{u+v}(1-p)^{n-w-u}, \tag{40}$$

where α_{uv} and β_{uv} are defined in Theorem 1. Moreover, (i) *equalities in* (39) *and* (40) *hold for $p = 0, (q-1)/q$ respectively;* (ii) *equality in* (39) *holds for a fixed $0 < p < (q-1)/q$ if and only if $F_{uv} = \alpha_{uv}$ for any $1 \leq u \leq w$ and $0 \leq v \leq u$;* (iii) *equality in* (40) *holds for a fixed $0 < p < (q-1)/q$ if and only if $F_{uv} = \beta_{uv}$ for any $1 \leq u \leq w$ and $0 \leq v \leq u$.*

Proof (39) and (40) follow from Theorem 1 and Lemma 5. By (36) and (24), it is easy to see that equalities in (39) and (40) hold for $p = 0, (q-1)/q$. For a fixed $0 < p < (q-1)/q$, it is obvious that (ii) and (iii) follow from Theorem 1 and Lemma 5. □

Remark 6 Let C be a q-ary (n, M) code used for error detection on a q-ary symmetric channel with symbol error probability p. From (5), (31) and (32), Abdel-Ghaffar [1,Theorem 2] obtained the following lower bounds on the undetected error probability $P_{ue}(C, p)$:

$$P_{ue}(C,p) \geq \sum_{u=1}^{n}\eta_u\left(1-\frac{qp}{q-1}\right)^{n-u}\left(\frac{p}{q-1}\right)^{u} \tag{41}$$
$$\geq \sum_{u=1}^{n}\theta_u\left(1-\frac{qp}{q-1}\right)^{n-u}\left(\frac{p}{q-1}\right)^{u}, \tag{42}$$

where η_u and θ_u are defined in (31) and (32), respectively. It is easy to see from Remark 5(i), Remark 3, and Theorem 2 that the lower bounds (41) and (42) follow directly from (39) and (40), respectively.

Remark 7 Let C be a binary (n, M, w) code. By Remark 4 and Theorem 2, the lower bounds (39) and (40) reduce to the following bounds:

$$P_{ue}(C, p) \geq \sum_{v=1}^{w} \rho_v (1-2p)^{w-v} p^{2v} (1-p)^{n-2w} \tag{43}$$

$$\geq \sum_{v=1}^{w} \tau_v (1-2p)^{w-v} p^{2v} (1-p)^{n-2w} \tag{44}$$

where ρ_v and τ_v are defined in (33) and (34), respectively. The lower bound (44) is just the Xia-Fu-Ling bound [20,Theorem 1] which was obtained directly from (10) and (34). By Remark 4, (43) slightly improves on (44). Note that we can also obtain (43) directly from (10) and (33).

It is known [1,2] that the maximum-distance-separable codes achieve the lower bound (42). It was shown [20] that the lower bound (44) is tight if and only if the binary constant weight codes are generated from certain t-designs. Now, we discuss the q-ary constant weight codes which achieve the lower bound (40) in Theorem 2 for the case of $w \neq n$ and $q > 2$.

Proposition 5 *Let $q \geq 3$ be a power of prime and C be the q-ary constant weight code formed by all the weight-3 codewords of a q-ary Hamming code with length $q+1$. Then C achieves the lower bound (40) in Theorem 2.*

Proof Let $\mathcal{H}(m, q)$ denote a $[(q^m-1)/(q-1), (q^m-1)/(q-1)-m, 3]$ Hamming code over GF(q). Let $m = 2$ and C be the set of weight-3 codewords of $\mathcal{H}(2, q)$. It is known [7] that C is formed by $GS(2, 3, q+1, q-1)$ and $M = (q+1)q(q-1)^2/6$. Since $q \geq 3$, it is easy to check that $M \leq \xi_{uv}$ if and only if $(u, v) = (1, 0), (1, 1), (2, 0)$, or $M > \xi_{uv}$ if and only if $(u, v) = (3, 0), (2, 1), (3, 1), (3, 2), (3, 3)$. Since C is formed by $GS(2, 3, q+1, q-1)$, the minimum distance of C satisfies $d = 3$, which implies that $A_{10} = A_{11} = A_{20} = 0$. Moreover, by Corollary 2 and the fact that C is formed by a generalized 2-design, we have $w - v \leq 2$ and $F_{uv} = \beta_{uv}$ for $(u, v) = (2, 1), (3, 1), (3, 2), (3, 3)$. Hence, by Theorem 2 and Corollary 1 (i), it is enough to show $F_{30} = \beta_{30}$, or $A_{30} = q-2$. For a fixed codeword $\mathbf{c} \in C$, it is easy to see that $A_{30} = A_{30}(\mathbf{c}) = |\{\mu\mathbf{c} : \mu \in \text{GF}(q)\backslash\{0, 1\}\}| = q-2$, which completes the proof. □

Proposition 6 *Let C be the q-ary $(n, M, 3)$ code formed by $GS(2, 3, n, q-1)$. If $n \geq (q-1)^2+2$, then C achieves the lower bound (40) in Theorem 2 if and only if $A_{30} = 0$, i.e., there are no pairs of codewords in C which have the same supports.*

Proof Clearly, $M = (q-1)^2 n(n-1)/6$ and $\xi_{30} = n(n-1)(n-2)/6$, which implies that $M \leq \xi_{30}$ if and only if $n \geq (q-1)^2+2$. Hence, for $n \geq (q-1)^2+2$ and $1 \leq u \leq 3, 0 \leq v \leq u$, it is easy to check that $M \leq \xi_{uv}$ if and only if $(u, v) = (1, 0), (1, 1), (2, 0), (3, 0)$, or $M > \xi_{uv}$ if and only if $(u, v) = (2, 1), (3, 1), (3, 2), (3, 3)$. Since C is formed by $GS(2, 3, n, q-1)$, the minimum distance of C satisfies $d = 3$, which implies that $A_{10} = A_{11} = A_{20} = 0$. Moreover, by Corollary 2 and the fact that C is formed by a generalized 2-design, we have $w - v \leq 2$ and $F_{uv} = \beta_{uv}$ for $(u, v) = (2, 1), (3, 1), (3, 2), (3, 3)$. Therefore, by Theorem 2 and Corollary 1 (i), $A_{30} = 0$ if and only if C achieves the lower bound (40). □

By Proposition 6, it is easy to check that the ternary constant weight codes formed by $GS(2, 3, 7, 2)$ and $GS(2, 3, 9, 2)$ in [7,Appendix] achieve the lower bound (40) in Theorem 2.

Using the same arguments in the proof of Proposition 6, we have the following propositions.

Proposition 7 *Let C be the q-ary $(n, M, 4)$ code formed by $GS(2, 4, n, q-1)$. If $n \geq 2(q-1)^2+2$, then C achieves the lower bound (40) of Theorem 2 if and only if $A_{41} = 0$.*

Proposition 8 *Let C be the q-ary $(n, M, 4)$ code formed by $GS(3, 4, n, q-1)$. If $n \geq (q-1)^3+3$, then C achieves the lower bound (40) of Theorem 2 if and only if $A_{30} = A_{40} = 0$, i.e., there are no pairs of codewords in C which have the same supports.*

5 Conclusions

In this paper, we introduced the q-binomial moments for q-ary constant weight codes. A lower bound on the q-binomial moments for q-ary constant weight codes was derived. The generalized (s, t)-designs were introduced to characterize the sufficient and necessary conditions for these bounds to be tight. As applications to error detection, we derived a new formula for the undetected error probability of q-ary constant weight codes. A lower bound on the undetected error probability of q-ary constant weight codes was obtained. This bound unified and extended the Abdel-Ghaffar bound for q-ary codes and the Xia-Fu-Ling bound for binary constant weight codes. Moreover, we obtained a lower bound on the undetected error probability of binary constant weight codes which slightly improves on the Xia-Fu-Ling bound. Finally, we showed that these bounds could be achieved by some q-ary constant weight codes.

Acknowledgments The authors would like to thank the three anonymous reviewers for their valuable suggestions and comments that helped to greatly improve the paper. This research is supported in part by the National Natural Science Foundation of China under Grant No. 60402031, the NSFC-GDSF Joint Fund under Grant No. U0675001, and the open research fund of National Mobile Communications Research Laboratory, Southeast University.

References

1. Abdel-Ghaffar K.A.S.: A lower bound on the undetected error probability and strictly optimal codes. IEEE Trans. Inform. Theory **43**, 1489–1502 (1997).
2. Ashikhmin A., Barg A.: Binomial moments of the distance distribution: bounds and applications. IEEE Trans. Inform. Theory **45**, 438–452 (1999).
3. Barg A., Ashikhmin A.: Binomial moments of the distance distribution and the probability of undetected error. Des. Codes and Cryptogr. **16**, 103–116 (1999).
4. Blaum M., Bruck J.: Coding for tolerance and detection of skew in parallel asynchronous communications. IEEE Trans. Inform. Theory **46**, 2329–2335 (2000).
5. Chung F.R.K., Salehi J.A., Wei V.K.: Optical orthogonal codes: Design, analysis, and applications. IEEE Trans. Inform. Theory **35**, 595–604 (1989).
6. Dodunekova R.: Extended binomial moments of a linear code and undetected error probability. Probl. Inform. Transmission **39**, 255–265 (2003).
7. Etzion T.: Optimal constant weight codes over $\mathbf{Z}_k$ and generalized designs. Discrete Math. **169**, 55–82 (1997).
8. Fu F.-W., Xia S.-T.: Binary constant weight codes for error detection. IEEE Trans. Inform. Theory **44**, 1294–1299 (1998).
9. Fu F.-W., Kløve T., Wei V.K.: On the undetected error probability for binary codes. IEEE Trans. Inform. Theory **49**, 382–390 (2003).
10. Fu F.-W., Kløve T., Xia S.-T.: On the undetected error probability of m-out-of-n codes on the binary symmetric channel. In: Buchmann J., Høholdt T., Stichtenoth H., Tapia-Recillas H. (eds.) Coding Theory, Cryptography, and Related Areas, pp. 102–110, Springer (2000).

11. Fu F.-W., Kløve T., Xia S.-T.: The undetected error probability threshold of m-out-of-n codes. IEEE Trans. Inform. Theory **46**, 1597–1599 (2000).
12. Hanani H.: On some tactical configurations. Canad. J. Math. **15**, 702–722 (1963).
13. Kløve T., Korzhik V.: Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems. Kluwer Acad. Press, Boston (1995).
14. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1981).
15. Mills W.H.: On the covering of triples by quadruple. In: Proceedings of the Fifth Southeastern Conference on Combinatorics, Graph Theory and Algorithms, pp. 573–581 (1974).
16. Tallini L.G., Bose B.: Design of balanced and constant weight codes for VLSI systems. IEEE Trans. Comput. **47**, 556–572 (1998).
17. Tarnanen H., Aaltonen M., Goethals J-.M.: On the nonbinary Johnson scheme. Eur. J. Combin. **6**, 279–285 (1985).
18. Wang X.M., Yang Y.X.: On the undetected error probability of nonlinear binary constant weight codes. IEEE Trans. Commun. **42**, 2390–2393 (1994).
19. Xia S.-T., Fu F.-W., Jiang Y., Ling S.: The probability of undetected error for binary constant weight codes. IEEE Trans. Inform. Theory **51**, 3364–3373 (2005).
20. 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 **52**, 4235–4243 (2006).