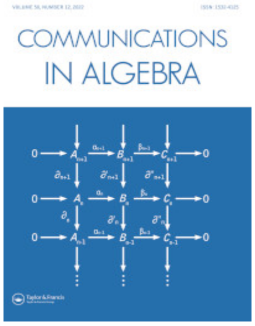

Taylor & Francis
Taylor & Francis Group

Communications in Algebra

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/lagb20

Fourth moments of the code-weights

Ibrahim Özen

COMMUNICATIONS IN ALGEBRA®
https://doi.org/10.1080/00927872.2022.2143514

Fourth moments of the code-weights

İbrahim Özen

Department of Mathematics, Marmara University, Istanbul, Turkey

ABSTRACT
In this paper we give the fourth joint moments of the weights of random linear codes. We calculate the fourth moment using mutual position of 4 lines. The solution of the 4-subspace problem is known and we obtain the information on line configurations from the set of indecomposables of the 4-subspace problem.

ARTICLE HISTORY
Received 06 August 2021
Revised 11 October 2022
Communicated by Ángel del Río Mateos

KEYWORDS
Four subspace problem; moments of the code-weights

2020 MATHEMATICS SUBJECT CLASSIFICATION
Primary: 94B05; Secondary: 94B65

1. Introduction

1.1. Basic definitions and notations

Let $\mathbb{F}_q$ be a finite field of q elements. A k dimensional subspace of $\mathbb{F}_q^n$ is called a linear $[n,k]_q$ code. Elements of such a code are called code-vectors or code-words. To every vector $u \in \mathbb{F}_q^n$ we associate the number $|u|$ of nonzero positions in u and call this quantity the weight of the vector. The minimum of these weights in the set of nonzero code-words is said to be the minimum distance of the code and it is usually denoted by d. A linear code in $\mathbb{F}_q^n$, of dimension k and minimum distance d is said to be an $[n,k,d]_q$ linear code.

Let C be a linear code and denote by A_i the number of code-words with weight i, $A_i = |\{c \in C : |c| = i\}|$. The set $\{A_i : i = 0, \dots, n\}$ is called the weight distribution or the weight spectrum of the code. The weight enumerator of C is the polynomial

$$W_C(t) = \sum_i A_i t^i = 1 + \sum_{i=d}^{n} A_i t^i.$$

Many properties about the code such as the undetected error probability [6], decoding error probability [4] etc. can be estimated using the weight distribution of the code.

Besides, we do not know if a suitable polynomial $W(t)$ really corresponds to a weight enumerator. At this point we examine the statistical properties of the weight enumerators.

1.2. Random linear codes

A random linear $[n,k]_q$ code C is the row-space of a random $k \times n$ matrix, whose entries are independently and uniformly distributed over $\mathbb{F}_q$. Some of the codes obtained this way will have smaller rank than k but the probability of this case is exponentially small as long as $k/n < 1$.

CONTACT İbrahim Özen iozen@marmara.edu.tr Marmara University, Mathematics, Istanbul, 34722 Turkey.

We will denote the code-words in a random code C by $c_0 = \mathbf{0}, c_1, c_2, \ldots, c_{q^k-1}$. If C is generated by the random matrix G, then the element c_i is given by $c_i = \alpha G$, for some $\alpha \in \mathbb{F}_q^k$.

The weights of a set of l linearly independent code-vectors c_i are statistically independent, for any $l \leq k$. Let $S = \{\alpha_1, \alpha_2, \ldots, \alpha_l\} \subset \mathbb{F}_q^k$ and $V = \{v_1, v_2, \ldots, v_l\} \subset \mathbb{F}_q^n$ be two fixed sets of linearly independent vectors. We would like to find the number of generator matrices G such that for each $i \in \{1, 2, \ldots, l\}$, $\alpha_i G = v_i$.

Consider the set of $k \times n$ matrices M_V whose first l rows are $v_1, v_2, \ldots, v_l \in V$ respectively and the remaining rows are random vectors in $\mathbb{F}_q^n$. The number of matrices in M_V is equal to $q^{n(k-l)}$. Let $G_{S,V}$ be the set of $k \times n$ matrices G with the property $\alpha_i G = v_i,\ 1 \leq i \leq l$. This set is in bijective correspondence with the set M_V. To see this, fix any nonsingular $k \times k$ matrix Q, whose first l rows are the k-tuples $\alpha_1, \alpha_2, \ldots, \alpha_l \in S$ and define

$$\begin{aligned} f_Q : M_V &\rightarrow G_{S,V} \\ G' &\mapsto Q^{-1}G' \end{aligned}$$

Clearly this map is bijective so we have

$$|G_{S,V}| = q^{n(k-l)}.$$

Finally we can conclude that the probability of having a $k \times n$ matrix G that satisfies $|\alpha_i G| = m_i$ equals to

$$\prod_{i=1}^{l} \binom{n}{m_i} \frac{(q-1)^{m_i}}{q^n}.$$

(We remind that a set of random $l \leq k$ vectors in $\mathbb{F}_q^n$ is linearly independent with high probability as long as $k/n < 1$.)

1.3. Moment problem

We refer to calculation of

$$\mathbb{E}\left(\prod_{j=1}^{n} W_C(x_j)\right)$$

as the nth moment problem of random codes. The moment problem gets more and more involved as we proceed from first to higher orders, so only the first three moments have been given explicitly up to now. For explicit calculations of the first three moments we refer the reader to [1]. Equivalent formulas for the first and second moments were also given and the third one was conjectured independently in [7]. In this paper we will give the fourth moment

$$\mathbb{E}\left(W_C(x)W_C(y)W_C(z)W_C(t)\right) = \sum_{i,j,l,m} \mathbb{E}(A_iA_jA_lA_m)x^iy^jz^lt^m.$$

Recall that we denote the code-vectors in a random $[n,k]_q$ code by $c_0 = \mathbf{0}, c_1, c_2, \ldots, c_{q^k-1}$. Weight enumerator of a random code is obtained by

$$W_C(t) = \sum_{i=0}^{q^k-1} \sum_{p=0}^{n} \xi_{ip} t^p,$$

where ξ_{ip} is a sequence of random variables expressed by

$$\xi_{ip} = \begin{cases} 1, & \text{if } |c_i| = p \\ 0, & \text{otherwise.} \end{cases}$$

Expectation of each ξ_{ip} is exactly the probability that $|c_i| = p$. They are given by

$$\mathbb{E}(\xi_{ip}) = \begin{cases} 1, & \text{if } i = 0, p = 0 \\ 0, & \text{if } i = 0, p \neq 0 \\ \frac{1}{q^n}\binom{n}{p}(q-1)^p, & \text{if } i > 0. \end{cases}$$

With the expectations of the ξ_{ip}, we can calculate the first moment as follows:

$$\mathbb{E}(W_C(t)) = \sum_{i=0}^{q^k-1} \sum_{p=0}^{n} \mathbb{E}(\xi_{ip})t^p = 1 + \frac{(q^k-1)}{q^n}(1+(q-1)t)^n.$$

Starting from the case $n = 2$ one has to take into consideration the linear dependencies of the random code-vectors in order to calculate the expectations $\mathrm{E}(\xi_{ip}\xi_{jr}\ldots)$. For example the expectations of the products $\xi_{ip}\xi_{jr}$ are given by

$$\mathbb{E}(\xi_{ip}\xi_{jr}) = \begin{cases} 1, & \text{if } i, j = 0 \text{ and } p = r = 0, \\ \frac{1}{q^n}\binom{n}{r}(q-1)^r, & \text{if } i = p = 0 \text{ and } j > 0, \\ \frac{1}{q^n}\binom{n}{p}(q-1)^p, & \text{if } j = r = 0 \text{ and } i > 0, \\ \frac{1}{q^n}\binom{n}{p}(q-1)^p, & \text{if } i, j > 0; p = r; c_i \text{ and } c_j \text{ are linearly dependent}, \\ \frac{1}{q^{2n}}\binom{n}{p}\binom{n}{r}(q-1)^{p+r}, & \text{if } i, j > 0; c_i \text{ and } c_j \text{ are linearly independent}. \end{cases}$$

These expectations give the second moment as

$$\begin{aligned} \mathbb{E}(W_C(x)W_C(y)) &= \sum_{i,j=0}^{q^k-1} \sum_{p,r=0}^{n} \mathbb{E}(\xi_{ip}\xi_{jr})x^p y^r \\ &= 1 + \frac{(q^k-1)}{q^n}((1+(q-1)x)^n + (1+(q-1)y)^n) \\ &\quad + \frac{(q^k-1)(q-1)}{q^n}(1+(q-1)xy)^n \\ &\quad + \frac{(q^k-1)(q^k-q)}{q^{2n}}(1+(q-1)x)^n(1+(q-1)y)^n. \end{aligned}$$

2. The 4-subspace problem and the moment problem

The third moment calculation is long because we have to keep track of linear dependencies between the random vectors. It seems inevitable to avoid listing all possible ways of how these vectors can be linearly dependent or independent for the higher cases either. Our approach to this problem is listing all possible subspaces that the random code-words can span and observe the dependencies from there. For this we have to define the 4-subspace problem.

Let $\mathbb{F}$ be an arbitrary field and let U_0 be a finite dimensional vector space over $\mathbb{F}$. If U_1, U_2, U_3, U_4 are any collection of four subspaces of U_0, then we call the ordered collection $U = (U_0; U_1, U_2, U_3, U_4)$ a quadruple of subspaces of U_0. Two quadruples U and V are said to be isomorphic if there is an $\mathbb{F}$-linear isomorphism $\phi : U_0 \to V_0$ such that $\phi(U_i) = V_i$ for each $i \in \{1, 2, 3, 4\}$. A quadruple U is called decomposable if there is a non-trivial direct sum decomposition $U_0 = U_0' \bigoplus U_0''$ such that $U_i = (U_i \cap U_0') \bigoplus (U_i \cap U_0'')$, for all $i \in \{1, 2, 3, 4\}$. The four subspace problem is the problem of classifying all indecomposable quadruples up-to isomorphism. Brenner gave a classification of indecomposables of certain types at first in [2]. Then she gave the full classification over an arbitrary field and skew fields in [3]. Independently, Gelfand and Ponomarev [5] and Nazarova [9, 10] solved the problem for algebraically

Table 1. Indecomposables of quadruples of 0 or 1 dimensional subspaces.

Type 1.	$d = (2; 1, 1, 1, 1)$	$\begin{bmatrix} 1 & 0 & a & c \\ 0 & 1 & b & d \end{bmatrix}$	$a \neq 0, b \neq 0, d \neq 0, c \neq 0, c \neq ad/b.$
Type 2.	$d = (2; 1, 1, 1, 1)$	$\begin{bmatrix} 1 & a & 0 & 0 \\ 0 & b & 1 & c \end{bmatrix}$	$a \neq 0, b \neq 0, c \neq 0.$
Type 3.	$d = (1; 1, 1, 0, 0)$	$\begin{bmatrix} 1 & a & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	$a \neq 0.$
Type 4.	$d = (1; 1, 0, 0, 0)$	$\begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix}$	
Type 5.	$d = (1; 0, 1, 1, 1)$	$\begin{bmatrix} 0 & 1 & a & b \end{bmatrix}$	$a \neq 0, b \neq 0.$
Type 6.	$d = (2; 1, 1, 1, 0)$	$\begin{bmatrix} 1 & 0 & a & 0 \\ 0 & 1 & b & 0 \end{bmatrix}$	$a \neq 0, b \neq 0.$
Type 7.	$d = (3; 1, 1, 1, 1)$	$\begin{bmatrix} 1 & 0 & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \end{bmatrix}$	$a \neq 0, b \neq 0, c \neq 0.$
Type 8.	$d = (1; 1, 1, 1, 1)$	$\begin{bmatrix} 1 & a & b & c \end{bmatrix}$	$a \neq 0, b \neq 0, c \neq 0.$

closed fields and arbitrary fields respectively. Medina and Zavadskij gave an elementary proof in [8] and we use their notation in this paper.

The dimension vector of a quadruple U is the tuple $\underline{\dim}(U) = (d_0; d_1, d_2, d_3, d_4)$, $d_i = \dim(U_i)$ for each i. We will be concerned with dimension vectors where the dimensions of the component spaces can be at most 1. This is because we want to understand the subspaces spanned by the codewords.

Let U be a quadruple and let us fix a basis of the space U_0. Then consider the coordinate vectors of an arbitrarily chosen basis in each U_i, $1 \leq i \leq 4$, with respect to the fixed basis of U_0. The quadruple U is represented by a matrix

$$M_U = [M_1|M_2|M_3|M_4],$$

where the columns in each vertical stripe is the coordinate vectors of the basis in each U_i, $1 \leq i \leq 4$. The number of rows in M_U is $\dim(U_0)$ and the number of columns in each M_i is d_i. If U and V are two quadruples then they are isomorphic if and only if their matrix representations M_U and M_V can be transformed to each other by the following two set of operations:

1. elementary row operations on the whole M_U,
2. elementary column operations in each stripe M_i.

Medina and Zavadskij give the list of indecomposable quadruples in the matrix form [8]. There are a total of 9 types of indecomposables, up-to isomorphism and up-to permutations of the subspaces. When we consider quadruples of subspaces of dimension at most 1, we have 8 types. We give the dimension vectors and the matrix forms of the indecomposables, up-to permutations of the subspaces and up-to isomorphism, without proof, in Table 1.

3. Calculation of the fourth moment

When we pass to calculation of the fourth moment

$$\mathbb{E}(W_C(x)W_C(y)W_C(z)W_C(t)) = \sum_{i,j,l,m=0}^{q^k-1} \sum_{p,r,s,u=0}^{n} \mathbb{E}(\xi_{ip}\xi_{jr}\xi_{ls}\xi_{mu})x^p y^r z^s t^u, \quad (1)$$

we will have to consider each quadruple's contribution. So we denote the quadruples of code-words by (c_i, c_j, c_l, c_m). The quadruple (c_i, c_j, c_l, c_m) may be in various shape of decompositions with respect to the subspaces each code-word spans. After identifying the decomposition, we will find the contribution of each case to the fourth moment.

Case 1. $i = j = l = m = 0, p = r = s = u = 0.$

In this case clearly the contribution is

$$E_1(x, y, z, t) = 1. \tag{2}$$

Case 2. Three of the indices i, j, l, m and three of the corresponding weights p, r, s, u are zero.

Consider $i = j = l = 0$ and $p = r = s = 0$. In this case the quadruple is of Type 4 with dimension vector $d = (1; 0, 0, 0, 1)$. Contribution of such a configuration to the fourth moment is

$$(q^k - 1) \sum_{u=0}^{n} \frac{1}{q^n} \binom{n}{u} (q-1)^u t^u = \frac{(q^k - 1)}{q^n} (1 + (q-1)t)^n.$$

If we consider all the cases where triplets of i, j, l, m are zero, we get the contribution

$$\begin{aligned} E_2(x, y, z, t) = & \frac{(q^k - 1)}{q^n} ((1 + (q-1)x)^n + (1 + (q-1)y)^n \\ & + (1 + (q-1)z)^n + (1 + (q-1)t)^n). \end{aligned} \tag{3}$$

Case 3. Two of the indices in $\{i, j, l, m\}$ and two of the corresponding weights in $\{p, r, s, u\}$ are zero.

Let $i = j = 0$ and $p = r = 0$. Then the corresponding configuration will be one of Type 4 $\bigoplus$ Type 4 with dimension vector $d = (1; 0, 0, 1, 0) \oplus (1; 0, 0, 0, 1)$ or it will be given by a Type 3 indecomposable with dimension vector $d = (1; 0, 0, 1, 1)$.

Case 3a. Contribution of a Type 4 $\bigoplus$ Type 4 quadruple with dimension vector $d = (1; 0, 0, 1, 0) \oplus (1; 0, 0, 0, 1)$ is given by

$$\begin{aligned} & (q^k - 1)(q^k - q) \sum_{s,u=0}^{n} \frac{1}{q^{2n}} \binom{n}{s} \binom{n}{u} (q-1)^{s+u} z^s t^u \\ & = \frac{(q^k - 1)(q^k - q)}{q^{2n}} ((1 + (q-1)z)^n (1 + (q-1)t)^n). \end{aligned}$$

If we consider all permutations of the zero vectors in $\{c_i, c_j, c_l, c_m\}$ we get 6 similar cases and the total contribution of this case is

$$\begin{aligned} E_3(x, y, z, t) = & \frac{(q^k - 1)(q^k - q)}{q^{2n}} ((1 + (q-1)x)^n (1 + (q-1)y)^n \\ & + (1 + (q-1)x)^n (1 + (q-1)z)^n + (1 + (q-1)x)^n (1 + (q-1)t)^n \\ & + (1 + (q-1)y)^n (1 + (q-1)z)^n + (1 + (q-1)y)^n (1 + (q-1)t)^n \\ & + (1 + (q-1)z)^n (1 + (q-1)t)^n). \end{aligned} \tag{4}$$

Case 3b. If we have a Type 3 indecomposable with dimension vector $d = (1; 0, 0, 1, 1)$, contribution from this configuration will be

$$(q^k - 1)(q - 1) \sum_{s=0}^{n} \frac{1}{q^n} \binom{n}{s} (q-1)^s (zt)^s = \frac{(q^k - 1)(q-1)}{q^n} (1 + (q-1)zt)^n.$$

Again considering all permutations of the zero component subspaces in Type 3 indecomposables, the totality of their contribution is

$$\begin{aligned} E_4(x, y, z, t) = & \frac{(q^k - 1)(q-1)}{q^n} \Big((1 + (q-1)xy)^n + (1 + (q-1)xz)^n \\ & + (1 + (q-1)xt)^n + (1 + (q-1)yz)^n + (1 + (q-1)yt)^n \\ & + (1 + (q-1)zt)^n \Big). \end{aligned} \tag{5}$$

Case 4. Only one of the code-words is **0**. In this case we may have a configuration of Type 3 $\bigoplus$ Type 4 or Type 4 $\bigoplus$ Type 4 $\bigoplus$ Type 4 or Type 5 or Type 6.

Case 4a. Let $i = 0$ and $p = 0$. Then the contribution of a configuration Type 3 $\bigoplus$ Type 4 with dimension vector $d = (1; 0, 1, 1, 0) \oplus (1; 0, 0, 0, 1)$ to the fourth moment is

$$\begin{aligned}
(q^k - 1)(q^k - q)(q - 1) & \sum_{r,u=0}^{n} \frac{1}{q^{2n}} \binom{n}{r}\binom{n}{u}(q-1)^{r+u}(yz)^r t^u \\
&= \frac{(q^k - 1)(q^k - q)(q - 1)}{q^{2n}} \Big((1 + (q-1)yz)^n (1 + (q-1)t)^n \Big).
\end{aligned}$$

Again if we take into consideration first the nonzero positions in Type 3 indecomposable and then the zero component in the quadruple (c_i, c_j, c_l, c_m), we get a total contribution from this case as follows

$$\begin{aligned}
E_5(x,y,z,t) = & \frac{(q^k - 1)(q^k - q)(q - 1)}{q^{2n}} \\
& \Big((1 + (q-1)x)^n \big((1 + (q-1)yz)^n + (1 + (q-1)yt)^n + (1 + (q-1)zt)^n \big) \\
& + (1 + (q-1)y)^n \big((1 + (q-1)xz)^n + (1 + (q-1)xt)^n + (1 + (q-1)zt)^n \big) \\
& + (1 + (q-1)z)^n \big((1 + (q-1)xy)^n + (1 + (q-1)xt)^n + (1 + (q-1)yt)^n \big) \\
& + (1 + (q-1)t)^n \big((1 + (q-1)xy)^n + (1 + (q-1)xz)^n + (1 + (q-1)yz)^n \big) \Big).
\end{aligned} \tag{6}$$

Case 4b. A decomposition of the form Type 4 $\bigoplus$ Type 4 $\bigoplus$ Type 4 with dimension vector $d = (1; 0, 1, 0, 0) \oplus (1; 0, 0, 1, 0) \oplus (1; 0, 0, 0, 1)$ gives a contribution

$$\begin{aligned}
(q^k - 1)(q^k - q)(q^k - q^2) & \sum_{r,s,u=0}^{n} \frac{1}{q^{3n}} \binom{n}{r}\binom{n}{s}\binom{n}{u}(q-1)^{r+s+u} y^r z^s t^u \\
&= \frac{(q^k - 1)(q^k - q)(q^k - q^2)}{q^{3n}} \Big((1 + (q-1)y)^n (1 + (q-1)z)^n (1 + (q-1)t)^n \Big).
\end{aligned} \tag{7}$$

With all 4 permutations of the zero component we get a total contribution from this case as follows

$$\begin{aligned}
E_6(x,y,z,t) = & \frac{(q^k - 1)(q^k - q)(q^k - q^2)}{q^{3n}} \\
& \Big((1 + (q-1)x)^n (1 + (q-1)y)^n (1 + (q-1)z)^n \\
& + (1 + (q-1)x)^n (1 + (q-1)y)^n (1 + (q-1)t)^n \\
& + (1 + (q-1)x)^n (1 + (q-1)z)^n (1 + (q-1)t)^n \\
& + (1 + (q-1)y)^n (1 + (q-1)z)^n (1 + (q-1)t)^n \Big).
\end{aligned} \tag{8}$$

Case 4c. Suppose we have a configuration of code-words of Type 5, with dimension vector $d = (1; 0, 1, 1, 1)$. In this case the contribution from such a configuration is

$$(q^k - 1)(q - 1)^2 \sum_{r=0}^{n} \frac{1}{q^n}(q-1)^r (yzt)^r = \frac{(q^k - 1)(q - 1)^2}{q^n}(1 + (q-1)yzt)^n. \tag{9}$$

Table 2. Number of zero and non-zero positions in code-words in Case 4d with dimension vector (2; 0, 1, 1, 1).

n_1	The number of positions where c_j and c_l are nonzero and c_m is zero.
n_2	The number of positions where c_l and c_m are nonzero and c_j is zero.
n_3	The number of positions where c_j and c_m are nonzero and c_l is zero.
n_4	The number of positions where c_j, c_l, c_m are all nonzero.

Taking into account all four cases where the **0** vector is permuted in four positions we get

$$E_7(x,y,z,t) = \frac{(q^k-1)(q-1)^2}{q^n}\Big((1+(q-1)xyz)^n + (1+(q-1)xyt)^n + (1+(q-1)xzt)^n + (1+(q-1)yzt)^n\Big). \tag{10}$$

Case 4d. If we have a configuration of code-vectors of Type 6 with dimension vector $d=(2;0,1,1,1)$ its contribution to the expectation will be

$$\frac{(q^k-1)(q^k-q)(q-1)^2}{q^{2n}} \sum_{n_1,n_2,n_3,n_4} \left\{ \binom{n}{n_1,n_2,n_3,n_4} (q-1)^{n_1+n_2+n_3}((q-1)(q-2))^{n_4}(yz)^{n_1}(zt)^{n_2}(yt)^{n_3}(yzt)^{n_4} \right\}$$
$$= \frac{(q^k-1)(q^k-q)(q-1)^2}{q^{2n}}\Big(1+(q-1)(yz+yt+zt)+(q-1)(q-2)yzt\Big)^n,$$

where

$$\binom{n}{n_1,n_2,\ldots,n_r} = \frac{n!}{n_1!\ldots n_r!(n-n_1-\ldots-n_r)!}$$

will always denote the multinomial coefficient.

Here we used the notation given in the Table 2.

The factor $((q-1)(q-2))^{n_4}$ appears because of the following. We have $c_m = ac_j + bc_l$. When we put arbitrarily a non-zero value for a fixed position in c_j, there are $(q-2)$ possible choices for c_l's position to make the corresponding coordinate in c_m non-zero.

Permuting the position of the **0** vector we get a total contribution from Type 6 configurations as follows

$$E_8(x,y,z,t) = \frac{(q^k-1)(q^k-q)(q-1)^2}{q^{2n}} \Big(\big(1+(q-1)(yz+yt+zt)+(q-1)(q-2)yzt\big)^n + \big(1+(q-1)(xz+xt+zt)+(q-1)(q-2)xzt\big)^n + \big(1+(q-1)(xy+xt+yt)+(q-1)(q-2)xyt\big)^n + \big(1+(q-1)(xy+xz+yz)+(q-1)(q-2)xyz\big)^n\Big). \tag{11}$$

Case 5. None of the indices i,j,l,m is zero. In this case we want to determine the contributions from the indecomposables where all the components have dimension 1.

Case 5a. We have quadruples with decomposition Type 4 $\bigoplus$ Type 4 $\bigoplus$ Type 4 $\bigoplus$ Type 4. Such a configuration has dimension vector $d = (1;1,0,0,0) \oplus (1;0,1,0,0) \oplus (1;0,0,1,0) \oplus (1;0,0,0,1)$. Contribution from these configurations of code-vectors is

$$E_9(x,y,z,t) = \frac{(q^k-1)(q^k-q)(q^k-q^2)(q^k-q^3)}{q^{4n}} \Big((1+(q-1)x)^n(1+(q-1)y)^n(1+(q-1)z)^n(1+(q-1)t)^n\Big). \tag{12}$$

Case 5b. We may have a quadruple of code-vectors spanning a space as in Type 3 $\bigoplus$ Type 4 $\bigoplus$ Type 4. Such a decomposition will have dimension vector $d = (1;1,1,0,0) \oplus (1;0,0,1,0) \oplus (1;0,0,0,1)$.

In this case the contribution from such a quadruple is

$$\frac{(q^k-1)(q^k-q)(q^k-q^2)(q-1)}{q^{3n}}\Big((1+(q-1)xy)^n(1+(q-1)z)^n(1+(q-1)t)^n\Big).$$

With similar decompositions where permutations of the component lines are considered we get a total contribution

$$\begin{aligned}E_{10}(x,y,z,t) = {} & \frac{(q^k-1)(q^k-q)(q^k-q^2)(q-1)}{q^{3n}}\\ & \Big((1+(q-1)xy)^n(1+(q-1)z)^n(1+(q-1)t)^n\\ & +(1+(q-1)xz)^n(1+(q-1)y)^n(1+(q-1)t)^n\\ & +(1+(q-1)xt)^n(1+(q-1)y)^n(1+(q-1)z)^n\\ & +(1+(q-1)yz)^n(1+(q-1)x)^n(1+(q-1)t)^n\\ & +(1+(q-1)yt)^n(1+(q-1)x)^n(1+(q-1)z)^n\\ & +(1+(q-1)zt)^n(1+(q-1)x)^n(1+(q-1)y)^n\Big). \end{aligned} \tag{13}$$

Case 5c. The quadruple of code-vectors may span a space with a decomposition as in Type 3 $\bigoplus$ Type 3. One of the possible dimension vectors of such a decomposition is $d = (1;1,1,0,0) \oplus (1;0,0,1,1)$. Such a configuration contributes to the expectation as follows

$$\frac{(q^k-1)(q^k-q)(q-1)^2}{q^{2n}}\Big((1+(q-1)xy)^n(1+(q-1)zt)^n\Big).$$

The permutations of the components give a total contribution

$$\begin{aligned}E_{11}(x,y,z,t) = {} & \frac{(q^k-1)(q^k-q)(q-1)^2}{q^{2n}}\\ & \Big((1+(q-1)xy)^n(1+(q-1)zt)^n\\ & +(1+(q-1)xz)^n(1+(q-1)yt)^n\\ & +(1+(q-1)xt)^n(1+(q-1)yz)^n\Big). \end{aligned} \tag{14}$$

Case 5d. A quadruple of code-vectors may span a space with decomposition Type 4 $\bigoplus$ Type 5 with dimension vector $d = (1;1,0,0,0) \oplus (1;0,1,1,1)$. Contribution of such a configuration is

$$\frac{(q^k-1)(q^k-q)(q-1)^2}{q^{2n}}\Big((1+(q-1)x)^n(1+(q-1)yzt)^n\Big).$$

With all possible permutations of the components we get a total contribution

$$\begin{aligned}E_{12}(x,y,z,t) = {} & \frac{(q^k-1)(q^k-q)(q-1)^2}{q^{2n}}\\ & \Big((1+(q-1)x)^n(1+(q-1)yzt)^n\\ & +(1+(q-1)y)^n(1+(q-1)xzt)^n\\ & +(1+(q-1)z)^n(1+(q-1)xyt)^n\\ & +(1+(q-1)t)^n(1+(q-1)xyz)^n\Big). \end{aligned} \tag{15}$$

Table 3. Number of zero and non-zero positions in code-words in Case 5f with dimension vector (3; 1, 1, 1, 1).

n_1	The number of positions where c_i and c_m are nonzero and c_j and c_l are zero.
n_2	The number of positions where c_j and c_m are nonzero and c_i and c_l are zero.
n_3	The number of positions where c_l and c_m are nonzero and c_i and c_j are zero.
n_4	The number of positions where c_i and c_j are nonzero and c_l and c_m are zero.
n_5	The number of positions where c_i and c_l are nonzero and c_j and c_m are zero.
n_6	The number of positions where c_j and c_l are nonzero and c_i and c_m are zero.
n_7	The number of positions where c_i, c_j, c_m are all nonzero and c_l is zero.
n_8	The number of positions where c_i, c_l, c_m are all nonzero and c_j is zero.
n_9	The number of positions where c_j, c_l, c_m are all nonzero and c_i is zero.
n_{10}	The number of positions where c_i, c_j, c_l are all nonzero and c_m is zero.
n_{11}	The number of positions where c_i, c_j, c_l, c_m are all nonzero.

Case 5e. The subspace spanned by the quadruple of code-vectors is of the form Type 4 $\bigoplus$ Type 6 with dimension vector $d = (1; 1, 0, 0, 0) \oplus (2; 0, 1, 1, 1)$. In this case we get a contribution of the form

$$\frac{(q^k-1)(q^k-q)(q^k-q^2)(q-1)^2}{q^{3n}} \Big((1+(q-1)x)^n\big(1+(q-1)(yz+yt+zt)+(q-1)(q-2)yzt\big)^n\Big).$$

We also have other cases where the zero component in the Type 6 indecomposable is permuted. With all the permutations we get the following contribution from this case

$$\begin{aligned} E_{13}(x,y,z,t) = {} & \frac{(q^k-1)(q^k-q)(q^k-q^2)(q-1)^2}{q^{3n}} \\ & \Big((1+(q-1)x)^n\big(1+(q-1)(yz+yt+zt)+(q-1)(q-2)yzt\big)^n \\ & +(1+(q-1)y)^n\big(1+(q-1)(xz+xt+zt)+(q-1)(q-2)xzt\big)^n \\ & +(1+(q-1)z)^n\big(1+(q-1)(xy+xt+yt)+(q-1)(q-2)xyt\big)^n \\ & +(1+(q-1)t)^n\big(1+(q-1)(xy+xz+yz)+(q-1)(q-2)xyz\big)^n\Big). \end{aligned} \quad (16)$$

Case 5f. The span of the quadruple is a Type 7 indecomposable with dimension vector $d = (3; 1, 1, 1, 1)$. In this case the contribution is

$$\begin{aligned} E_{14}(x,y,z,t) = {} & \frac{(q^k-1)(q^k-q)(q^k-q^2)(q-1)^3}{q^{3n}} \\ & \Big[\Big((q-1)(q^2-3q+3)xyzt+(q-1)(q-2)(xyz+xyt+yzt+ztx) \\ & \quad +(q-1)(xy+xz+xt+yz+yt+zt)+1\Big)^n\Big]. \end{aligned} \quad (17)$$

We partition the set of n positions on the vectors as in Table 3.

Remember that $c_m = ac_i + bc_j + cc_l$. The contribution of this indecomposable to the expectation is the following sum

Table 4. Number of zero and non-zero positions in code-words in Case 5i.

n_1	The number of positions where c_i, c_l, c_m are all nonzero and c_j is zero.
n_2	The number of positions where c_i and c_j are nonzero and c_l and c_m are zero.
n_3	The number of positions where c_i, c_j, c_l, c_m are all nonzero.
n_4	The number of positions where c_j, c_l, c_m are all nonzero and c_i is zero.

$$\frac{(q^k-1)(q^k-q)(q^k-q^2)(q-1)^3}{q^{3n}} \sum_{n_1,\ldots,n_{11}} \left\{ \binom{n}{n_1, n_2, \ldots, n_{11}} ((q-1)(q^2-3q+3)xyzt)^{n_{11}} \right.$$
$$+((q-1)(q-2)xyz)^{n_{10}} + ((q-1)(q-2)xyt)^{n_7} + ((q-1)(q-2)xzt)^{n_8}$$
$$+((q-1)(q-2)yzt)^{n_9} + ((q-1)xy)^{n_4} + ((q-1)xz)^{n_5} + ((q-1)yz)^{n_6}$$
$$\left. +((q-1)xt)^{n_1} + ((q-1)yt)^{n_2} + ((q-1)zt)^{n_3} \right\}. \tag{18}$$

The coefficient $((q-1)(q^2-3q+3))^{n_{11}}$ above is the number of ways we can form the positions of the code-vectors where c_i, c_j, c_l, and c_m are all nonzero.

Case 5g. We have a Type 1 configuration with dimension vector $d = (2; 1, 1, 1, 1)$. In this case the contribution of this configuration is

$$E_{15}(x,y,z,t) = \frac{(q^k-1)(q^k-q)(q-1)^3(q-2)}{q^{2n}}$$
$$\Big(\big(1 + (q-1)(xyz + xyt + yzt + xzt) + (q-1)(q-3)xyzt\big)^n\Big). \tag{19}$$

Case 5h. We may have a Type 8 indecomposable which gives the span of the code-vectors. In this case the dimension vector is $d = (1; 1, 1, 1, 1)$. The contribution from these quadruples is

$$E_{16}(x,y,z,t) = \frac{(q^k-1)(q-1)^3}{q^n}\Big(1 + (q-1)xyzt\Big)^n. \tag{20}$$

Case 5i. The code-vectors span a space given by an indecomposable of Type 2 with dimension vector $d = (2; 1, 1, 1, 1)$ and with matrix representation

$$\begin{bmatrix} 1 & a & 0 & 0 \\ 0 & b & 1 & c \end{bmatrix}, \; a \neq 0, b \neq 0, c \neq 0. \tag{21}$$

To find the contribution of quadruples of this isomorphism type, we evaluate the following sum

$$\frac{(q^k-1)(q^k-q)(q-1)^3}{q^{2n}} \sum_{n_1,n_2,n_3,n_4} \binom{n}{n_1, n_2, n_3, n_4}$$
$$(q-1)^{(n_1+n_2+n_3+n_4)}(q-2)^{n_3} x^{(n_1+n_2+n_3)} y^{(n_2+n_3+n_4)} (zt)^{(n_1+n_3+n_4)}$$
$$= \frac{(q^k-1)(q^k-q)(q-1)^3}{q^{2n}}$$
$$\big[((q-1)xy + (q-1)zt(x+y) + (q-1)(q-2)xyzt + 1)^n\big]. \tag{22}$$

In the summation above, we take into consideration the fact that $c_j = ac_i + bc_l$. We use Table 4 to give the partition of the code-positions depending on whether they are 0 or not.

It is clear that the only possible case apart from those in the table is that c_i, c_j, c_l, c_m are all zero. The number of such positions is $n - (n_1 + n_2 + n_3 + n_4)$.

The following set of permutations (acting on the columns) of the matrix in Equation (21) give exactly the same isomorphism class of the quadruple,

$$\{i, (12), (34), (12)(34)\}.$$

The set of permutations which give all non-isomorphic quadruples is $\{i, (23), (24), (13), (14), (14)(23)\}$. After action of these permutations, we get the totality of the contribution as

$$\begin{aligned} E_{17}(x,y,z,t) = {} & \frac{(q^k-1)(q^k-q)(q-1)^3}{q^{2n}} \\ & \Big(\big((q-1)xy + (q-1)zt(x+y) + (q-1)(q-2)xyzt + 1\big)^n \\ & + \big((q-1)xz + (q-1)yt(x+z) + (q-1)(q-2)xyzt + 1\big)^n \\ & + \big((q-1)xt + (q-1)yz(x+t) + (q-1)(q-2)xyzt + 1\big)^n \\ & + \big((q-1)yz + (q-1)xt(y+z) + (q-1)(q-2)xyzt + 1\big)^n \\ & + \big((q-1)yt + (q-1)xz(y+t) + (q-1)(q-2)xyzt + 1\big)^n \\ & + \big((q-1)zt + (q-1)xy(z+t) + (q-1)(q-2)xyzt + 1\big)^n \Big). \end{aligned} \tag{23}$$

We have considered all the cases how configurations of code-vectors can contribute to $\mathbb{E}\big(W_C(x)W_C(y)W_C(z)W_C(t)\big)$. The fourth moment of the weight enumerator of an $[n,k]_q$ random code is

$$\begin{aligned} \mathbb{E}\left(W_C(x)W_C(y)W_C(z)W_C(t)\right) &= \sum_{i,j,l,m} \mathbb{E}(A_iA_jA_lA_m)x^iy^jz^lt^m \\ &= \sum_{i=1}^{17} E_i(x,y,z,t), \end{aligned} \tag{24}$$

where each of the E_i's are given above.

Acknowledgments

The author is grateful to the anonymous referee who has helped improve the manuscript by advising on the random linear code ensemble definition.

References

[1] Blinovsky, V., Erez, U., Litsyn, S. (2010). Weight distribution moments of random linear/coset codes. *Des. Codes Cryptogr.* 57:127–138. DOI: 10.1007/s10623-009-9356-1.
[2] Brenner, S. (1967). Endomorphism algebras of vector spaces with distinguished sets of subspaces. *J. Algebra* 6:100–114.
[3] Brenner, S. (1974). On four subspaces of a vector space. *J. Algebra* 29:587–599.
[4] Gallager R. G. (1963). *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press.
[5] Gel'fand, I. M., Ponomarev, V. A. (1970). Problems of linear algebra and classification of quadruples of subspaces in a finite dimensional vector space. *Colloq. Math. Soc. János Bolyai* 5:163–237.
[6] Kløve, T. (2007). *Codes for Error Detection*. Singapore: World Scientific.
[7] Klyachko, A. A., Özen, İ. (2009). Correlations between the ranks of submatrices and weights of random codes. *Finite Fields Appl.* 15:497–516. DOI: 10.1016/j.ffa.2009.03.002.
[8] Medina, G., Zavadskij, A. (2004). The four subspace problem: An elementary solution. *Linear Algebra Appl.* 392:11–23. DOI: 10.1016/j.laa.2004.05.010.
[9] Nazarova, L. A. (1967). Representations of a tetrad. *Izv. AN SSSR Ser. Mat.* 31(6):1361–1378 (1967) (in Russian); English transl. in: Math. USSR Izvestija 1(6):1305–1321.
[10] Nazarova, L. A. (1973). Representations of quivers of infinite type. *Izv. AN SSSR Ser. Mat.* 37:752–791 (1973) (In Russian); English transl. in: Math USSR Izvestija 7:749–792.