Second-Order Weight Distributions

Shengtian Yang, Member, IEEE

Abstract—A fundamental property of codes, the second-order weight distribution, is proposed to solve the problems such as computing second moments of weight distributions of linear code ensembles. A series of results, parallel to those for weight distributions, are obtained. Furthermore, the application of second-order weight distributions in random coding approach is discussed. In particular, an analogue of MacWilliams identities is proved. Second- and higher-order moments of weight distributions in random coding approach are computed. As easy consequences, the second moment then gives a confidence interval of the weight distribution of an individual code with respect to any given probability. It is not the only case that one needs to compute the second moment like $E[|W(x)|^2]$. When estimating the variance of undetected error probability of an error detection scheme (see e.g. [29, p. 99] and [36]) which is expressed in terms of a random weight enumerator $W(x)$, one also needs to compute the second moment $E[|W(x)|^2]$ or $E[|A_i(C)|A_j(C)]$. Then one question arises: how can we compute these second moments? For this question, there has been some work for some specific code ensembles, e.g., the second moment of the weight distribution of a binary regular LDPC code ensemble [1], [31], [32], the covariance of the weight distribution of a linear code ensemble [36], and the second moment of the weight distribution of a random linear code generated by a uniform random generator matrix [7]. However, no systematic approach has ever been established to facilitate such kinds of computation.

To establish a systematic approach, we need a fundamental property of linear codes, which not only yields the second moment of weight distribution but also supports easy computation for various combinations of linear codes. Unfortunately, the distribution $A_i(C)^2$ or $A_i(C)A_j(C)$ are not qualified for this position. When $C$ is not random, it is clear that $E[A_i(C)^2]$ or $E[A_i(C)A_j(C)]$ provides no more information than does $E[A_i(C)]$. On the other hand, for a general random $C$, the information contained in $E[A_i(C)A_j(C)]$ is too coarse to support the computation of serially concatenated codes, even if an analogue of input-output weight distribution (see e.g. [15]) is introduced. Recall that a linear code is the kernel or image of a linear transformation. Then most kinds of combinations of linear codes can be expressed as a series of two basic operations of linear transformations, namely, the composition (serial concatenation) and the Cartesian product (parallel concatenation).

Motivated by the question above, we provide in this paper a novel property of codes, called second-order weight distributions. From the viewpoint of group actions on sets, the second-order weight is a partition induced by the group of all monomial maps acting on the set $\mathbb{F}_q^n \times \mathbb{F}_q$. This is a natural extension of weight, which is a partition induced by the same group acting on $\mathbb{F}_q^n$. A series of results,
parallel to those for weight distributions, is established for second-order weight distributions. In particular, an analogue of MacWilliams identities is proved. Equipped with this new tool, we compute the second-order weight distributions of regular LDPC code ensembles. As easy consequences, we obtain the second moments of weight distributions of regular LDPC code ensembles, which include the results of [13, 31, 32] as special cases. Furthermore, we discuss the application of second-order weight distributions in random coding approach. We compute the second-order weight distributions of the ensembles generated by a so-called 2-good random generator or parity-check matrix. A 2-good random matrix is a kind of generalization of the uniformly distributed random matrix and is very useful for solving problems that involve pairwise or triple-wise properties of sequences. We show that the 2-good property is reflected in the second-order weight distribution, which thus plays a fundamental role in some well-known problems in coding theory and combinatorics. An example of linear intersecting codes is finally provided to illustrate this fact.

The rest of this paper is organized as follows. In Section II we establish the method of second-order weight distributions. In Section III we compute the second-order weight distributions of regular LDPC code ensembles. The application of second-order weight distributions in random coding approach is discussed in Section IV. Section V concludes the paper.

In the sequel, the symbols \( \mathbb{N}, \mathbb{C}, \mathbb{S}_n \) denote the set of nonnegative integers, the field of complex numbers, and the group of all permutations on \( n \) letters, respectively. The multiplicative subgroup of nonzero elements of \( \mathbb{F}_q \) (resp. \( \mathbb{C} \)) is denoted by \( \mathbb{F}_q^* \) (resp. \( \mathbb{C}^* \)). A vector in \( \mathbb{F}_q^n \) is typically denoted in the row-vector form \( \mathbf{v} = (v_1, v_2, \ldots, v_n) \). The canonical projection \( \pi_i : \mathbb{F}_q^n \rightarrow \mathbb{F}_q \) is given by \( \mathbf{v} \mapsto v_i \). In general, for an element in a set \( A^I \), we adopt a similar notation such as \( \mathbf{v} = (v_i)_{i \in I} \) where \( v_i \in A \), and the canonical projection \( \pi_i : A^I \rightarrow A \) with \( i \in I \) is given by \( \mathbf{v} \mapsto v_i \). Given \( \mathbf{u} \in A^I \) and \( \mathbf{v} \in B^J \), if the product \( \prod_{i \in I} u_i^{v_i} \) makes sense, we write \( \mathbf{u}^{\mathbf{v}} \) as the shortening. For any set \( A \) and its subset \( B \), the indicator function \( 1_B : A \rightarrow \{0, 1\} \) is given by \( x \mapsto 1 \) for \( x \in B \) and \( x \mapsto 0 \) for \( x \notin B \). When the expression of \( B \) is long, we write \( 1_B \) in place of \( 1_B(x) \). Nonrandom codes are denoted by capital letters, while random codes are denoted by script capital letters. Matrices are denoted by boldface capital letters. By a tilde we mean that a matrix such as \( \tilde{\mathbf{A}} \) denotes \( \mathbf{A} \).

It is then reasonable to guess that the fundamental property that we are seeking may be a sum of \( 1 \{ (\mathbf{u}, \mathbf{v}) \in C \times C \} \) over some set of vector pairs. More specifically, let \( P \) be a partition of \( \mathbb{F}_q^{m} \times \mathbb{F}_q^{m} \), and then the quantity

\[
A_P(C, C) \triangleq \sum_{(\mathbf{u}, \mathbf{v}) \in P} 1 \{ (\mathbf{u}, \mathbf{v}) \in C \times C \}
\]

gives a kind of property of \( C \). Whenever \( P \) is a refinement of the partition \( Q \triangleq \{ (i, j) \mapsto \{ (\mathbf{u}, \mathbf{v}) : w(\mathbf{u}) = i, w(\mathbf{v}) = j \} \} \), \( A_P(C, C) \) can readily yield \( A_i(C)A_j(C) \).

One obvious choice of \( P \) is the finest partition of \( \mathbb{F}_q^{m} \times \mathbb{F}_q^{m} \), i.e., \( O \triangleq \{ \{ (\mathbf{u}, \mathbf{v}) \} \} \). However, the partition \( O \) contains so much information that the complexity of induced formulas grows out of control as \( n \) increases. On the other hand, as we have shown in Section II the coarsest partition \( Q \) itself is not qualified, because it contains no enough information. Then our task is now to find an appropriate partition between \( O \) and \( Q \).

A similar story has ever happened on the weight distribution. In order to find the answer, we shall briefly review the reason why the weight distribution is so fundamental.

Let \( G \) be the random matrix uniformly distributed over the set \( \mathbb{F}_q^{m \times n} \) of all \( m \times n \) matrices over \( \mathbb{F}_q \). It is well known that the linear code ensembles \( \{ \mathbf{u}G : \mathbf{u} \in \mathbb{F}_q^m \} \) and \( \{ \mathbf{u} \in \mathbb{F}_q^n : \mathbf{G}^T \mathbf{u} = \mathbf{0} \} \) are both good for channel coding [3, 19]. Moreover, the application of \( G \) is not confined in channel coding. It also turns out to be good for Slepian-Wolf coding [12], lossless joint source-channel coding (lossless JSCC) [38], and so on.

The success of \( G \) in information theory exclusively depends on its fundamental property:

\[
P\{ F(\mathbf{u}) = \mathbf{v} \} = q^{-n}, \quad \forall \mathbf{u} \in \mathbb{F}_q^m \setminus \{ \mathbf{0} \}, \mathbf{v} \in \mathbb{F}_q^n
\]

where \( F(\mathbf{u}) \triangleq \mathbf{u}G \). In fact, any random linear transformations satisfying (1) has the same performance as \( F \) for channel coding, lossless JSCC, etc. We may call such random linear transformations good random linear transformations.

One important property of good random linear transformations is that both \( f \circ F \) and \( F \circ g \) are good for any bijective linear transformations \( f : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^m \) and \( g : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n \). In particular, a good random linear transformation is preserved under a special class of mappings called monomial maps [21, Sec. 1.7]. Let \( \mathbf{c} \in (\mathbb{F}_q^n)^m \) and \( \sigma \in \mathbb{S}_n \). We define the monomial map \( \xi_{\mathbf{c}, \sigma} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n \) by

\[
\xi_{\mathbf{c}, \sigma}(\mathbf{v}) \triangleq \left( c_1 v_{\sigma^{-1}(1)}, c_2 v_{\sigma^{-1}(2)}, \ldots, c_n v_{\sigma^{-1}(n)} \right).
\]

Furthermore, we define the uniform random monomial map \( \Xi_n \) as a random mapping uniformly distributed over the set of all monomial maps. Then given a linear transformation \( f : \mathbb{F}_q^m \rightarrow \mathbb{F}_q^m \), we define the randomization operator

\[
\mathcal{R}(f) \triangleq \Xi_n \circ f \circ \Xi_n.
\]

Note that, according to our convention, \( \Xi_m \) and \( \Xi_n \) are independent. It is clear that for any good random linear transformation \( F \),

\[
P\{ \mathcal{R}(F)(\mathbf{u}) = \mathbf{v} \} = q^{-n}, \quad \forall \mathbf{u} \in \mathbb{F}_q^m \setminus \{ \mathbf{0} \}, \mathbf{v} \in \mathbb{F}_q^n.
\]
This implies that \( \mathcal{R} \) does not deteriorate the average performance of the ensemble. Moreover, the new ensemble \( \mathcal{R}(F) \) gets larger than \( F \) and has more symmetries, which facilitate the analysis of codes. Proceeding with this notion, we may consider such a coding system, where all linear transformations are randomized by independent operators \( \mathcal{R} \). It is not a new idea. Both Turbo codes [5] and LDPC codes are constructed by this randomization technique, and the analysis of weight distributions always enjoys such code ensembles.

Let \( M_n \) be the set of all monomial maps. Then under function composition, \( M_n \) forms a group (called a monomial group) that acts on \( \mathbb{F}_q^n \). This notion then establishes the relation between \( M_n \) and weight, that is, each set of vectors with the same weight corresponds to exactly one orbit of \( M_n \) on \( \mathbb{F}_q^n \). In other words, the weight is nothing but an identification of the orbits of \( M_n \) on \( \mathbb{F}_q^n \). This explains why the average weight distribution of Turbo codes and LDPC codes is easier to compute than other codes not randomized by \( \mathcal{R} \).

Now that the orbits of \( M_n \) on \( \mathbb{F}_q^n \) induce the weight, it is natural to consider the orbits of \( M_n \) on \( \mathbb{F}_q^n \times \mathbb{F}_q^n \) by the action \((\xi, (u, v)) \mapsto (\xi(u), \xi(v))\). As we shall see later (Lemmas 2.7 and 2.9 and Theorem 2.12), these orbits give an appropriate identification of the orbits of \( M_n \) on \( \mathbb{F}_q^n \). The next lemma formally states this fact.

**Lemma 2.3:** If the monomial group \( M_n \) acts on \( \mathbb{F}_q^n \times \mathbb{F}_q^n \) by the action \((\xi, (u, v)) \mapsto (\xi(u), \xi(v))\), then the orbit of \((u, v) \in \mathbb{F}_q^n \times \mathbb{F}_q^n \) is exactly the set of all vector pairs of second-order weight \( w_2(u, v) \).

**Remark 2.4:** As \( q = 2 \), the second-order weight coincides with the well-known joint weight (see e.g. [16], [27]). However, they are different in general. For any \((u, v) \in \mathbb{F}_q^n \times \mathbb{F}_q^n \), the joint weight of \((u, v)\) is a 4-tuple \((w_{0,0}, w_{1,0}, w_{0,1}, w_{1,1})\) with

\[
 w_{a,b} = \sum_{i=1}^{n} \mathbf{1}\{w(u_i) = a, w(v_i) = b\} \quad \text{for } a, b = 0, 1
\]

From the viewpoint of group actions on sets, the joint weight is essentially an identification of the orbits of \( M_n \times M_n \) on \( \mathbb{F}_q^n \times \mathbb{F}_q^n \) by the action \(((\xi, (u, v)) \mapsto (\xi(u), \xi(v))\). Since the group \( M_n \) can be embedded (as a diagonal subgroup, which is proper for \( q \geq 3 \)) into \( M_n \times M_n \) by the monomorphism \( \xi \mapsto (\xi, \xi) \), the partition yielded by the second-order weight is a refinement of the partition yielded by the joint weight. Therefore, when \( q \geq 3 \), the second-order weight provides more information than the joint weight. For example, we can determine whether two vectors are linearly independent by their second-order weight, but not by their joint weight. Suppose that the second-order weight of \((u, v) \in \mathbb{F}_q^n \times \mathbb{F}_q^n \) is \( i = (i_S)_{S \in \mathcal{S}} \). Then \( u \) and \( v \) are linearly independent if and only if

\[
 \sum_{S \in \mathcal{S}, i_S > 0} \mathbf{1}\{i_S > 0\} > 1
\]

On the other hand, consider the following two pairs of vectors in \( \mathbb{F}_3^3 \):

\[
((1, 2, 0), (2, 1, 0)) \text{ and } ((1, 1, 0), (2, 1, 0)).
\]

It is clear that they have the same joint weight \((1, 0, 0, 2)\), but the first pair is linearly dependent and the second is linearly independent.

Next, we proceed to define the second-order weight distribution and the second-order weight enumerator.

**Definition 2.5:** For any \( U, V \subseteq \mathbb{F}_q^n \), the second-order weight distribution of \((U, V)\) is defined by

\[
 A_2(U, V) = \mathbb{1}\{((u, v) \in U \times V : w_2(u, v) = 1)\}
\]

where \( i \in \mathcal{P}_n \triangleq \{j \in \mathbb{N}_0^3 : \sum_{S \in \mathcal{S}} js = n\} \).
Definition 2.6: For any $U, V \subseteq \mathbb{F}_q^n$, the second-order weight enumerator of $(U, V)$ is a polynomial in $q + 2$ indeterminates defined by

$$W_{U,V}(x) \triangleq \sum_{u \in U, v \in V} x^{w_2(u,v)}$$

where $x \triangleq (x_S)_{S \in S}$. The next four lemmas give basic properties of the second-order weight distribution.

Lemma 2.7: Let $U = U_1 \times U_2$ and $V = V_1 \times V_2$, where $U_1, V_1 \subseteq \mathbb{F}_q^m$ and $U_2, V_2 \subseteq \mathbb{F}_q^n$. Then

$$W_{U,V}(x) = W_{U_1,V_1}(x)W_{U_2,V_2}(x).$$

Proof:

$$W_{U,V}(x) = \sum_{u \in U, v \in V} x^{w_2(u,v)} = \sum_{u \in U_1, v_1 \in V_1, u_2 \in U_2, v_2 \in V_2} x^{w_2(u_1,v_1)}x^{w_2(u_2,v_2)} = \sum_{u_1 \in U_1, v_1 \in V_1} x^{w_2(u_1,v_1)}\sum_{u_2 \in U_2, v_2 \in V_2} x^{w_2(u_2,v_2)} = W_{U_1,V_1}(x)W_{U_2,V_2}(x).$$

Lemma 2.8:

$$A_i(\mathbb{F}_q^n, \mathbb{F}_q^n) = \binom{n}{i}(q - 1)^{n-i}s_{i0}$$

$$W_{\mathbb{F}_q^n, \mathbb{F}_q^n}(x) = \left[ x^{s_{00}} + (q - 1) \sum_{S \in S_{i0}} x^S \right]^n$$

where

$$\binom{n}{i} \triangleq \frac{n!}{i!(n-i)!}.$$

Proof: It is clear that

$$W_{\mathbb{F}_q^n, \mathbb{F}_q^n}(x) = x^{s_{00}} + (q - 1) \sum_{S \in S_{i0}} x^S.$$

This together with Lemma 2.7 yields (4) and (5).

Lemma 2.9: Let $c \in (\mathbb{F}_q^n)^m$ and $\sigma \in S_n$. Then for any $U, V \subseteq \mathbb{F}_q^n$,

$$A_i(U, V) = A_i(\xi_{c,\sigma}(U), \xi_{c,\sigma}(V)) \quad \forall i \in \mathcal{P}_n,$$

where $\xi_{c,\sigma}$ is a monomial map defined by (2). Moreover, for any random $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_q^n$,

$$P\{u \in \Xi_n(\mathcal{U}), v \in \Xi_n(\mathcal{V})\} = \frac{E[\omega_2(u,v)](\mathcal{U}, \mathcal{V})}{\omega_2(u,v)}$$

for all $u, v \in \mathbb{F}_q^n$, where $\Xi_n$ is a uniform random monomial map.

Proof: Identity (7) clearly holds. As for (8), we note that

$$P\{u' \in \Xi_n(\mathcal{U}), v' \in \Xi_n(\mathcal{V})\} = P\{u \in \Xi_n(\mathcal{U}), v \in \Xi_n(\mathcal{V})\}$$

whenever $w_2(u', v') = w_2(u, v)$. Then we have

$$A_{\omega_2(u,v)}(\mathbb{F}_q^n, \mathbb{F}_q^n)P\{u \in \Xi_n(\mathcal{U}), v \in \Xi_n(\mathcal{V})\} = \sum_{u', v'} P\{u' \in \Xi_n(\mathcal{U}), v' \in \Xi_n(\mathcal{V})\}$$

and

$$\sum_{u', v': w_2(u', v') = w_2(u,v)} 1\{u' \in \Xi_n(\mathcal{U}), v' \in \Xi_n(\mathcal{V})\}$$

$$= E[\omega_2(u,v)](\mathcal{U}, \mathcal{V}).$$

This combined with (7) gives (8).

Remark 2.10: Lemma 2.9 can be further generalized to the case of a mapping randomized by $\mathcal{R}$ defined by (3). To this end, we need the concept of second-order input-output weight distribution, an analogue of input-output weight distribution. This generalization can facilitate the computation of the second-order weight distribution of serially concatenated codes with all component codes randomized by $\mathcal{R}$. Since Lemma 2.9 is enough for this paper, we leave this generalization to the reader.

Lemma 2.11: For $U, V \subseteq \mathbb{F}_q^n$, the product $W_{U,V}(x)$ can be obtained from the second-order weight enumerator $W_{U,V}(x)$ by the substitution

$$x_S \mapsto x^{w(\pi_1(\rho(S)))}x^{w(\pi_2(\rho(S)))} \quad \forall S \in S$$

(9)

where $\pi_i$ ($i = 1, 2$) is the canonical projection $\mathbb{F}_q^2 \rightarrow \mathbb{F}_q$ given by $(v_1, v_2) \rightarrow v_i$. As a consequence, we have

$$A_j(U)A_k(V) = \sum_{l=0}^{\min\{j,k\}} \sum_{i=0}^{\min\{j,k\}} A_i(U, V).$$

(10)

The proof is left to the reader. Note that $A_j(U)A_k(V) = \text{cof}(W_U(x)V_V(y), x^iy^k)$.

One of the most famous results in coding theory is the MacWilliams identity [28]. Now, we shall derive an analogue of MacWilliams identities for the second-order weight distribution.

Theorem 2.12: For any $V \subseteq \mathbb{F}_q^n$, we define the orthogonal set $V^\perp$ by

$$V^\perp \triangleq \left\{ v' \in \mathbb{F}_q^n : v \cdot v' = \sum_{i=1}^{n} v_i v'_i = 0 \text{ for all } v \in V \right\}.$$ (11)

Then for any subspaces $U, V \subseteq \mathbb{F}_q^n$,

$$W_{U,V^\perp}(x) = \frac{1}{|V||V^\perp|}W_{U,V}(xK)$$

(12)

where $K$ is a $(q + 2) \times (q + 2)$ matrix $(K_{S,T})_{S,T \in S}$ defined by

$$K_{S,T} \triangleq \begin{cases} |S|, & T \subseteq S^\perp \quad (13a) \\ -1, & T \nsubseteq S^\perp \end{cases}$$

(13b)

Proof: Since $U$ and $V$ are subspaces of $\mathbb{F}_q^n$, it follows
from Lemma A.1 that
\[
W_{U \perp, V \perp}(x) = \sum_{u' \in U, v' \in V} \chi(u \cdot u' + v \cdot v') x^{w_2(u, v')}.
\]
Applying Lemma A.2 then gives
\[
W_{U \perp, V \perp}(x) = \frac{1}{|U||V|} \sum_{u \in U, v \in V} \sum_{u' \in U, v' \in V} \chi(u \cdot u' + v \cdot v') x^{w_2(u', v')}.
\]

Applying Lemma A.2 then gives
\[
W_{U \perp, V \perp}(x) = \frac{1}{|U||V|} \sum_{u \in U, v \in V} (xK)^{w_2(u, v)}
\]
as desired.

Remark 2.13: The set \( F_q^2 \), as a direct product of \( F_q \), is a Frobenius ring because \( F_q \) is a Frobenius ring and the class of Frobenius rings is closed under finite direct products of rings. Consequently, Theorem 2.12 can be regarded as a consequence of the generalized MacWilliams identities for linear codes over finite Frobenius rings [20, 37].

III. SECOND-ORDER WEIGHT DISTRIBUTIONS OF REGULAR LDPC CODE ENSEMBLES

Equipped with the tool established in Section II, we proceed to compute the second-order weight distributions of regular LDPC code ensembles.

At first, we compute the second-order weight distributions of two simple codes, the single symbol repetition code and the single symbol check code.

Definition 3.1: A single symbol repetition map \( f_{\text{rep}}^c : F_q \rightarrow F_q^c \) with the parameter \( c \) is given by \( v \mapsto (v, v, \ldots, v) \). The image of \( f_{\text{rep}}^c \) is called a single symbol repetition code, which we denote by \( C_{\text{rep}}^c \).

Lemma 3.2: For the single symbol repetition code \( C_{\text{rep}}^c \),
\[
W_{C_{\text{rep}}^c, C_{\text{rep}}^c}(x) = x^c_{S_{00}} + (q - 1) \sum_{S \in S_{00}} x^c_S.
\]
The proof is left to the reader.

Definition 3.3: A single symbol check map \( f_{\text{chk}}^d : F_q^c \rightarrow F_q \) with the parameter \( d \) is given by \( v \mapsto \sum_{i=1}^{\frac{d}{2}} v_i \). The kernel of \( f_{\text{chk}}^d \) is called a single symbol check code, which we denote by \( C_{\text{chk}}^d \).

Lemma 3.4: For the single symbol check code \( C_{\text{chk}}^d \),
\[
W_{C_{\text{chk}}^d, C_{\text{chk}}^d}(x) = \frac{1}{q^{d/2}} \left[ \left( \sum_{S \in S} x^c_S K_{S, S_{00}} \right)^d \right] + (q - 1) \left( \sum_{T \in S_{00}} \left( \sum_{S \in S} x^c_S K_{S, T} \right)^d \right)
\]
where \( K_{S, T} \) is defined by (13).

Proof: Use Theorems 2.12 and Lemma 3.2 with \( C_{\text{chk}}^d = (C_{\text{rep}}^c)_\perp \).

Example 3.5: When \( q = 3 \), Lemma 3.4 gives
\[
W_{C_{\text{chk}}^d, C_{\text{chk}}^d}(x) = \frac{1}{9} \left[ \left( x_0^{2d} + 2x_1^{d} \right) + \left( x_0 + x_1 \right)^d \right]
\]

The regular LDPC code ensemble \( I \), which we denote by \( C_{c,d,n} \), is defined as the intersection of \( c \) independent copies of the kernel of \( F_{d,n}^c \).

According to this definition, \( C_{c,d,n} \) is the solution space of the random equations
\[
H^{(i)}(v) = 0, \quad i = 1, 2, \ldots, c
\]
where \( H^{(i)} \) is the \( i \)th independent copy of \( F_{d,n}^c \). In other words, the parity-check matrix of \( C_{c,d,n} \) consists of \( c \) submatrices, each being an independent copy of the transformation matrix of \( F_{d,n}^c \) (with input vectors in column-vector form).

Since the transformation matrix of \( F_{d,n}^c \) contains exactly one nonzero entry in each column and \( d \) nonzero entries in each row, the resulting parity-check matrix is a \((nc/d)\)-by-\( n \) random sparse matrix with \( c \) nonzero entries in each column and \( d \) nonzero entries in each row, which motivates the term “regular low-density parity-check code ensemble”.

Theorem 3.7: For the regular LDPC code ensemble \( C_{c,d,n} \),
\[
E[A_t(c_{c,d,n})]_{c,d,n} = \frac{\text{coeff}(W_{C_{\text{chk}}^d, C_{\text{chk}}^d}(x)^n/d, x^i)}{c} \left[ \left( \frac{q}{c} \right) (q - 1)^{n-1} \right]_{i=1}
\]
where \( i \in \mathcal{P} \).

Proof: For any \( u, v \in F_q^n \) with \( w_2(u, v) = i \),
\[
P\{u, v \in \ker F_{d,n}^c \} \left( A_t \right) = \frac{\text{coeff}(W_{C_{\text{chk}}^d, C_{\text{chk}}^d}(x)^n/d, x^i)}{A_t(F_{d,n}^c, F_q^n)} \left( \frac{q}{c} \right) (q - 1)^{n-1} \left( \frac{q}{c} \right)
\]

A ring \( R \) is said to be a Frobenius ring if there exists a group homomorphism \( f : (R, +) \rightarrow C^* \) (character of \((R, +)) \), whose kernel contains no nonzero or right ideal of \( R \). Such a homomorphism is called a generating character of \( R \). The reader is referred to [23, Sec. 16] for background information on Frobenius rings.
where (a) follows from Definition 3.6, (b) from Lemma 2.9, (c) follows from Lemmas 2.7 and 2.8. This together with the identity

\[ E[A_i(c_{c,d,n}, c_{c,d,n})] = \sum_{u,v:w_2(u,v)=i} P\{u, v \in c_{c,d,n}\} \]

\[ = \sum_{u,v:w_2(u,v)=i} (P\{u, v \in \ker F_{c,d,n}^{ld1}\})^c \]

establishes the theorem.

The second ensemble of regular LDPC codes is the regular bipartite graph ensemble suggested by [4], [26], [34].

**Definition 3.8:** Let c, d, and n be positive integers such that d divides cn. Let \( F_{c,d,n}^{ld2} : F_q^n \rightarrow F_q^{cn/d} \) be a random linear transformation defined by

\[ F_{c,d,n}^{ld2}(v) \triangleq f_{c,d,cn/d}^\text{chk} (\Xi cn (f_{c,d,cn/d}^\text{rep} (v))). \]

The regular LDPC code ensemble II, which we denote by \( C_{c,d,n}^{ld2} \), is defined as the kernel of \( F_{c,d,n}^{ld2} \).

**Theorem 3.9:** For the regular LDPC code ensemble \( C_{c,d,n}^{ld2} \),

\[ E[A_i(C_{c,d,n}^{ld2}, c_{c,d,n})] = \left( \binom{n}{c} \right)^c \frac{\text{coef}((W_{cn/d}^c \mathcal{C}(\mathbf{x}))^{cn/d}, \mathbf{x}^i)}{\binom{cn}{c+1} (q-1)^c} \]

where (a) follows from Definition 3.8, (b) from Lemma 2.9, (c) follows from Lemmas 2.7 and 2.8. This together with the identity

\[ E[A_i(C_{c,d,n}^{ld2}, c_{c,d,n})] = \sum_{u,v:w_2(u,v)=i} P\{u, v \in c_{c,d,n}\} \]

establishes the theorem.

**Remark 3.10:** When \( q = 2 \), Lemma 3.4 and Theorems 3.7 and 3.9 give

\[ E[A_i(C_{c,d,n}^{ld1}, c_{c,d,n})] = \left( \binom{n}{c} \right)^c \frac{\text{coef}((g_d(\mathbf{x}))^{n/d}, \mathbf{x}^i)}{\binom{nc}{ci} (q-1)^c} \]

and

\[ E[A_i(c_{c,d,n}^{ld1}, c_{c,d,n})] = \left( \binom{n}{c} \right)^c \frac{\text{coef}((g_d(\mathbf{x}))^{n/d}, \mathbf{x}^i)}{\binom{nc}{ci} (q-1)^c} \]

4If regarding \( f_{c,d,cn/d}^\text{rep} \) as n variable nodes (each with c sockets) and \( f_{c,d,cn/d}^\text{chk} \) as \( cn/d \) check nodes (each with d sockets), we immediately obtain the well-known bipartite graph model, where the connections between variable nodes and check nodes are given by the uniform random monomial map \( \Xi cn \).

where

\[ g_d(\mathbf{x}) \triangleq \frac{1}{4} \left[ \left( x_{(0,0)} + x_{(0,1)} + x_{(1,0)} + x_{(1,1)} \right)^d \\
+ \left( x_{(0,0)} - x_{(0,1)} + x_{(1,0)} - x_{(1,1)} \right)^d \\
+ \left( x_{(0,0)} + x_{(0,1)} - x_{(1,0)} - x_{(1,1)} \right)^d \\
+ \left( x_{(0,0)} - x_{(0,1)} - x_{(1,0)} + x_{(1,1)} \right)^d \right] . \]

Furthermore, Lemma 2.11 shows that

\[ E[A_j(C_{c,d,n}^{ld1}) A_k(C_{c,d,n}^{ld1})] = \sum_{l=0}^{\min\{j,k\}} \left[ \left( \binom{n}{j-l-k-l-n-j-k+l} \frac{1}{(c-1)} \right) \times \left( \text{coef}((g_d(\mathbf{x}))^{n/d}, x_{(0,0)}^j x_{(0,1)}^l x_{(1,0)}^c x_{(1,1)}^l) \right) \right] \]

and

\[ E[A_j(C_{c,d,n}^{ld2}) A_k(c_{c,d,n}^{ld2})] = \sum_{l=0}^{\min\{j,k\}} \left[ \left( \binom{n}{j-l-k-l-n-j-k+l} \right) \times \left( \text{coef}((g_d(\mathbf{x}))^{n/d}, x_{(0,0)}^j x_{(0,1)}^l x_{(1,0)}^c x_{(1,1)}^l) \right) \right] . \]

The second formula with \( j = k \) coincides with the second-moment formula of binary regular LDPC codes given by [11], [31], [32].

**IV. APPLICATIONS IN RANDOM CODING APPROACH**

As discussed in Section [11] the uniformly distributed random \( m \times n \) matrix \( \mathbf{G} \) plays an important role in information theory because of the property that \( \mathbf{uG} \) is uniformly distributed over \( F_q^m \) for every nonzero \( \mathbf{u} \in F_q^n \). But it is not the end of the story.

Theorem B.1 shows that \( \mathbf{UG} \) is uniformly distributed over \( F_q^m \times n \) for every invertible matrix \( \mathbf{U} \in F_q^{m \times m} \). In particular, if \( m \geq 2 \), the product \( \mathbf{UG} \) is uniformly distributed over \( F_q^2 \) for every matrix \( \mathbf{U} \in F_q^{2 \times m} \) of rank 2. In other words, for any two linearly independent vectors \( \mathbf{u}, \mathbf{v} \in F_q^m \), the random vectors \( \mathbf{uA}, \mathbf{vA} \) are uniformly distributed and independent (see Corollary B.2). In this section, we shall show that this property is reflected in the second-order weight distribution, which thus plays an important role in some well-known problems in coding theory and combinatorics.

At first, for positive integers \( m, n, k \) with \( k \leq \min\{m, n\} \), a random \( m \times n \) matrix \( \mathbf{A} \) is said to be \( k \)-good if \( \mathbf{UA} \) is uniformly distributed over \( F_q^{k \times n} \) for every matrix \( \mathbf{U} \in F_q^{k \times m} \) of rank \( k \).

In this paper, we are only concerned with the cases \( k = 1, 2 \). It is clear that the uniformly distributed random \( m \times n \) matrix \( \mathbf{G} \) with \( m, n \geq 2 \) is \( 2 \)-good and \( 2 \)-goodness implies 1-goodness. However, a 1-good random matrix is not necessarily 2-good and there are also other 2-good random matrices than \( \mathbf{G} \). The next example illustrates these two facts.

In the sequel, when speaking of a \( k \)-good random \( m \times n \) matrix, we shall tacitly assume that \( k \leq \min\{m, n\} \).
Example 4.1: Consider the matrix space $\mathbb{F}_2^{3\times 3}$, which is identified with $\mathbb{F}_2^3$ by viewing the columns of $\mathbf{A} \in \mathbb{F}_2^{3\times 3}$ as coordinate vectors relative to $1, \alpha, \alpha^2$, where $\alpha^3 + \alpha + 1 = 0$. The random matrix uniformly distributed over the set

$$A_1 \triangleq \{x(1, \alpha, \alpha^2) : x \in \mathbb{F}_8\}$$

is 1-good but not 2-good. The random matrix uniformly distributed over the set

$$A_2 \triangleq \{x(1, \alpha, \alpha^2) + y(1, \alpha^2, \alpha^4) : x, y \in \mathbb{F}_8\}$$

is 2-good and it is clear that $A_2$ is a proper subset of $\mathbb{F}_2^{3\times 3}$. In fact, both $A_1$ and $A_2$ are maximum-rank-distance (MRD) codes $[13, 18, 35]$. The reader is referred to $[39]$ for a detailed investigation of the relation between $k$-good random matrices and MRD codes.

Next, let us compute the second-order weight distribution of linear code ensembles generated by a 2-good random generator or parity-check matrix.

Theorem 4.2: Let $\mathbf{A}$ be a 2-good random $m \times n$ matrices with $m < n$. Let $C_{m,n}^{\text{lic}}$ and $C_{m,n}^{\text{lic2}}$ be two random linear code ensembles generated by the generator matrix $\mathbf{A}$ and the parity-check matrix $\mathbf{A}^\perp$, respectively. Then we have

$$E \left[ \frac{W_{C_{m,n}^{\text{lic}},C_{m,n}^{\text{lic}}} (x)}{|C_{m,n}^{\text{lic}}|^2} \right] = \frac{1}{q^{2m}} x_{S_{00}}^n + \frac{q^m - 1}{q^{2m}} \sum_{S \in S_{00}} \left( \frac{1}{q} x_{S_{00}} + \frac{q - 1}{q^2} \sum_{S \in S_{00}} x_S \right)^n + \frac{1}{q^{2m}} \left( x_{S_{00}} + (q - 1) \sum_{S \in S_{00}} x_S \right)^n.$$

and

$$E[W_{C_{m,n}^{\text{lic2}},C_{m,n}^{\text{lic2}}} (x)] = \frac{(q^m - 1)(q^m - q)}{q^{2m}} x_{S_{00}}^n + \frac{q^m - 1}{q^{2m}} \sum_{S \in S_{00}} \left( x_{S_{00}} + (q - 1) x_S \right)^n + \frac{1}{q^{2m}} \left( x_{S_{00}} + (q - 1) \sum_{S \in S_{00}} x_S \right)^n.$$

Proof: Since $C_{m,n}^{\text{lic}} = \{u\mathbf{A} : u \in \mathbb{F}_q^m\}$, we have

$$E \left[ \frac{W_{C_{m,n}^{\text{lic}},C_{m,n}^{\text{lic}}} (x)}{|C_{m,n}^{\text{lic}}|^2} \right] = E \left[ \frac{\sum_{\nu, \nu' \in C_{m,n}^{\text{lic}}} x_{w_2(\nu, \nu')}}{|C_{m,n}^{\text{lic}}|^2} \right] = \frac{1}{q^{2m}} E \left[ \sum_{u, u' \in \mathbb{F}_q^m} x_{w_2(u\mathbf{A}, u'\mathbf{A})} \right] = \frac{1}{q^{2m}} E \left[ x_{w_2(0, 0)} + \sum_{u \neq 0, u' \neq 0} x_{w_2(u\mathbf{A}, u'\mathbf{A})} \right] + \frac{1}{q^m} \left( x_{S_{00}} + (q - 1) \sum_{S \in S_{00}} x_S \right)^n.$$

Remark 4.3: Note that the size of $C_{m,n}^{\text{lic}}$ is random and it may be less than $q^m$. For this reason, we give in Theorem 4.2
the expectation of the ratio $W_{C_{m,n}}(x)/|C_{m,n}|^2$ instead of $W_{C_{m,n}}(x)$. Theorems 4.2 and Lemma 2.11 show that

$$E \left[ \frac{W_{C_{m,n}}(x)W_{C_{m,n}}(y)}{|C_{m,n}|^2} \right] = \frac{1}{q^{2m}} q^{-1} + \frac{q^m - 1}{q^{2m}} \left( \frac{1}{q} + \frac{q}{x} \right)^n$$

$$+ \frac{q^m - 1}{q^{2m}} \left( \frac{1}{q} + \frac{q}{y} \right)^n$$

$$+ \frac{(q^m - 1)(q - 1)}{q^{2m}} \left( \frac{1}{q} + \frac{q}{xy} \right)^n$$

$$+ \frac{(q^m - 1)(q^m - q)}{q^{2m}} \left( \frac{1}{q} + \frac{q}{x} \right)^n \left( \frac{1}{q} + \frac{q}{y} \right)^n \cdot$$

This is equivalent to the formula \[7\, Eq. (2)], in which a linear code is allowed to contain duplicated codewords, so that $E[(A_0(C_{m,n}))^2] > 1$

Now let us show that the 2-good property is reflected in the second-order weight distribution given by Theorem 4.2

**Proposition 4.4**: Let $D$ be a random linear code having the same average second-order weight distribution as $C_{m,n}$. Then we have

$$P\{u \in \Xi_n(D)\} = q^{-m}$$

for any nonzero $u \in \mathbb{F}_q^n$ and

$$P\{u \in \Xi_n(D), v \in \Xi_n(D)\} = q^{-2m}$$

for any linearly independent $u, v \in \mathbb{F}_q^n$

**Proof**: From Lemma 2.9 and Theorem 4.2 it follows that for any nonzero $u \in \mathbb{F}_q^n$

$$P\{u \in \Xi_n(D)\} = E[A_{w_2}(u,0)(C_{m,n}^2)]\}

= \frac{E[A_{w_2}(u,0)(\mathbb{F}_q^n \times \mathbb{F}_q^n)]}{A_{w_2}(u,0)(\mathbb{F}_q^n \times \mathbb{F}_q^n)} = q^{-m}.$$ 

Similarly, for any linearly independent $u, v \in \mathbb{F}_q^n$, it follows from Lemma 2.9 and Theorem 4.2 that

$$P\{u \in \Xi_n(D), v \in \Xi_n(D)\} = \frac{E[A_{w_2}(u,v)(C_{m,n}^2)]}{A_{w_2}(u,v)(\mathbb{F}_q^n \times \mathbb{F}_q^n)} = q^{-2m}.$$ 

Clearly, the second identity in Proposition 4.4 reflects the 2-good property. The 2-good property is very useful for solving problems that involve pairwise or triple-wise properties of sequences (see \[39\]). Now based on Proposition 4.4 we shall provide an example of linear intersecting codes to show the fundamental position and potential application of second-order weight distribution in some problems in coding theory and combinatorics.

A pair of vectors in $\mathbb{F}_q^n$ is said to be intersecting if there is at least one position $i$ such that their $i$th components are both nonzero. A linear code is said to be intersecting if its any two linearly independent codewords intersect. Recall that linear intersecting codes have a close relation to many problems in combinatorics, such as separating systems \[30\], qualitative independence \[9\], frameproof codes \[10\], and so on.

Let $D$ be a random linear code having the same average second-order weight distribution as $C_{m,n}$ with $0 < m < n$. From Proposition 4.4 it follows that for any linearly independent $u, v \in \mathbb{F}_q^n$, $P\{u, v \in \Xi_n(D)\} = q^{2(m-n)}$. Then the probability that $\Xi_n(D)$ contains a given pair of non-intersecting and linearly independent vectors is $q^{2(m-n)}$, and hence the probability that $\Xi_n(D)$ contains at least one pair of non-intersecting and linearly independent vectors is bounded above by

$$(2q - 1)^n q^{2(m-n)} = q^{-2n(1-m/n-\log_2(2q-1)/2)}.$$ 

Consequently, the probability that $\Xi_n(D)$ is not intersecting converges to 0 as $n \to \infty$ whenever the ratio

$$R \triangleq \frac{m}{n} < 1 - \frac{1}{2} \log_q(2q - 1).$$

The right-hand side of the inequality is the asymptotic (random coding) lower bound of maximum rate of linear intersecting codes. In order to finally relate this bound with the random coding rate of $\Xi_n(D)$, we still need to study the coding rate of sample codes in $\Xi_n(D)$. From Proposition 4.4 it follows that

$$E[|\Xi_n(D)|] = \sum_{u \in \mathbb{F}_q^n} P\{u \in \Xi_n(D)\} = q^m + 1 - q^{m-n}$$

and

$$E[|\Xi_n(D)|] - E[|\Xi_n(D)|]^2 = E[|\Xi_n(D)|^2] - E[|\Xi_n(D)|]^2 = \sum_{u,v \in \mathbb{F}_q^n} (P\{u \in \Xi_n(D), v \in \Xi_n(D)\}$$

$$- P\{u \in \Xi_n(D)\} P\{v \in \Xi_n(D)\}) = \sum_{u,v \in \mathbb{F}_q^n \setminus \{0\}} (q^{m-n} - q^{2(m-n)})$$

$$= q^{m-n}(q - 1)(q - 1) - q^{m-n} < q^{m+1}.$$ 

Applying Chebyshev’s inequality then gives

$$P\left\{|\Xi_n(D)| - q^m \geq 2nq^{m+1}/2\right\} \leq P\left\{|\Xi_n(D)| - E[|\Xi_n(D)|] | q^{m+1}/2\right\} \leq \frac{1}{n^2}.$$ 

Using $R = m/n$ and the simple inequality

$$|\ln(1 + x)| \leq 2|x| \quad \text{for} \quad |x| < \frac{1}{2}$$

we finally obtain

$$P\left\{n \log_q |\Xi_n(D)| - R < \frac{4q^{(1-n/2)}R}{\ln q}\right\} \geq 1 - \frac{1}{n^2}$$

for sufficiently large $n$. Roughly speaking, the coding rate of $\Xi_n(D)$ is $R$ with high probability, provided the length $n$ is large enough.
V. Conclusion

We established the method of second-order weight distributions. An analogue of MacWilliams identities for second-order weight distributions was proved. We computed the second-order weight distributions of several important code ensembles and discussed the application of second-order weight distribution in random coding approach. The obtained second-order weight distributions are very complex, so understanding their significance will be our future work.

ACKNOWLEDGMENT

The author would like to thank Dr. T. Honold for his help in providing background information about joint weight. The author would also like to thank the Associate Editor, G. Cohen, and the anonymous reviewers for their helpful comments.

APPENDIX A

TWO LEMMAS FOR THE PROOF OF THEOREM 2.12

Lemma A.1: Let $V$ be a subspace of $\mathbb{F}_q^n$. Then

$$1_{V^\perp}(v') = \frac{1}{|V|} \sum_{v \in V} \chi(v \cdot v')$$

where

$$\chi(v) = e^{2\pi i \text{Tr}(v)/p} \quad \forall v \in \mathbb{F}_q$$

$$\text{Tr}(v) = v + v^p + \ldots + v^{p-1} \mod p \quad \forall v \in \mathbb{F}_q.$$  

Proof: First note that Tr($v$) is an $\mathbb{F}_p$-module epimorphism of $\mathbb{F}_q$ onto $\mathbb{F}_p$, and hence $\chi(v)$ is a homomorphism from the additive group of $\mathbb{F}_q$ to $\mathbb{C}^*$. For a fixed $v' \in \mathbb{F}_q$, the mapping $\tau : V \rightarrow \mathbb{F}_q$ given by $v \mapsto v \cdot v'$ is an $\mathbb{F}_q$-module homomorphism of $V$ into $\mathbb{F}_q$, and hence the image set $\tau(V)$ is also a vector space over $\mathbb{F}_q$, which must be either $\{0\}$ or $\mathbb{F}_q$.

If $v' \in V^\perp$, then $\chi(v \cdot v') = \chi(0) = 1$ for all $v \in V$, and hence identity (14) holds. If however $v' \not\in V^\perp$, then

$$\frac{1}{|V|} \sum_{v \in V} \chi(v \cdot v') = \frac{1}{q} \sum_{v \in \mathbb{F}_q} \chi(v) = 0.$$  

The proof is complete.

Lemma A.2: For any $u, v \in \mathbb{F}_q^n$,

$$\sum_{u',v' \in \mathbb{F}_q^n} \chi(u \cdot u' + v \cdot v')x^{w_2(u',v')} = (xK)^{w_2(u,v)}$$

where $K$ is defined by (13).

Proof: First, we have

$$\sum_{u',v' \in \mathbb{F}_q^n} \chi(u \cdot u' + v \cdot v')x^{w_2(u',v')} = \sum_{u',v' \in \mathbb{F}_q^n} \prod_{i=1}^n \chi(u_iu'_i + v_iv'_i)x^{w_2(u'_i,v'_i)}$$

$$= \prod_{i=1}^n \sum_{u_i,v_i \in \mathbb{F}_q} \chi((u_i,v_i) \cdot (u'_i,v'_i))x^{w_2(u'_i,v'_i)}$$

$$= \prod_{i=1}^n \sum_{S \in \mathbb{F}_q} x_S \sum_{(u'_i,v'_i) \in S} \chi((u_i,v_i) \cdot (u'_i,v'_i)).$$

From Lemma A.1 it follows that

$$\sum_{(u',v') \in S} \chi((u_i,v_i) \cdot (u',v')) = \begin{cases} |S|, & (u_i,v_i) \in S^\perp \\ -1, & (u_i,v_i) \not\in S^\perp. \end{cases}$$

Therefore we have

$$\sum_{u',v' \in \mathbb{F}_q^n} \chi(u \cdot u' + v \cdot v')x^{w_2(u',v')} = \prod_{T \in S} \left( \sum_{S \in \mathbb{F}_q} x_S K_{S,T}^{w_2(u,v)} \right)$$

as desired. □

APPENDIX B

PROPERTIES OF UNIFORMLY DISTRIBUTED RANDOM MATRICES

Theorem B.1: Let $\hat{G}$ be a random $m \times n$ matrix uniformly distributed over the set $\mathbb{F}_q^{m \times n}$ of all $m \times n$ matrices over $\mathbb{F}_q$. Then for any invertible matrix $U \in \mathbb{F}_q^{m \times m}$, the product $UG$ is uniformly distributed over $\mathbb{F}_q^{m \times n}$.

Proof: For any matrix $U \in \mathbb{F}_q^{m \times m}$, we denote by $U^*$ the mapping $\mathbb{F}_q^{m \times n} \rightarrow \mathbb{F}_q^{m \times n}$ given by $X \mapsto UX$. It is clear that $U^*$ is a surjective linear transformation for any invertible matrix $U \in \mathbb{F}_q^{m \times m}$, so that $UG$ is uniformly distributed over $\mathbb{F}_q^{m \times n}$. □

A corollary follows immediately.

Corollary B.2 (cf. [7] and the references therein): Let $\hat{G}$ be a random $m \times n$ matrix uniformly distributed over the set $\mathbb{F}_q^{m \times n}$ of all $m \times n$ matrices over $\mathbb{F}_q$. Then for any $x, x' \in \mathbb{F}_q^m$ and $y, y' \in \mathbb{F}_q^n$,

$$P\{x\hat{G} = y, x'\hat{G} = y'\} = \begin{cases} 1\{|y = 0, y' = 0\}, & x = x' = 0 \\ q^{-n}\{1\{|y = 0\}, & x = 0, x' \neq 0 \\ q^{-n}\{1\{|y' = 0\}, & x \neq 0, x' = 0 \\ q^{-n}\{1\{|y' = ay\}, & x \neq 0, x' = ax \text{ with } a \in \mathbb{F}_q^* \} \end{cases}$$

$x, x'$ are linearly independent.

REFERENCES

[1] O. Barak and D. Burshtein, “Lower bounds on the spectrum and error rate of LDPC code ensembles,” in Proc. IEEE Int. Symp. Information Theory, Adelaide, Australia, Sep. 2005, pp. 42–46.

[2] A. Barg and G. D. Forney, Jr., “Lower bounds on the error rate of LDPC code ensembles,” IEEE Trans. Inf. Theory, vol. 53, no. 11, pp. 4225–4236, Nov. 2007.

[3] A. Barg and G. D. Forney, Jr., “Codes: Minimum distances and error exponents,” IEEE Trans. Inf. Theory, vol. 48, no. 9, pp. 2568–2573, Sep. 2002.

[4] A. Bennatan and D. Burshtein, “On the application of LDPC codes to arbitrary discrete-memoryless channels,” IEEE Trans. Inf. Theory, vol. 50, no. 3, pp. 417–437, Mar. 2004.

[5] C. Berrou, A. Glavieux, and P. Thitimajshima, “Near Shannon limit error-correcting coding and decoding: Turbo codes,” in Proc. Int. Conf. Commun., Geneva, Switzerland, May 1993, pp. 1064–1070.

[6] V. Blinovsky, Asymptotic Combinatorial Coding Theory. Boston: Kluwer, 1997.

[7] V. Blinovsky, U. Erez, and S. Litsyn, “Weight distribution moments of random linear/coset codes,” Designs, Codes and Cryptography, vol. 57, no. 2, pp. 127–138, Nov. 2010.
