The Partition Weight Enumerator of MDS Codes and its Applications.

Mostafa El-Khamy * and Robert J. McEliece**
Electrical Engineering Department
California Institute of Technology
Pasadena, CA 91125, USA

*E-mail: mostafa@systems.caltech.edu  **E-mail: rjm@systems.caltech.edu

Abstract—A closed form formula of the partition weight enumerator of maximum distance separable (MDS) codes is derived for an arbitrary number of partitions. Using this result, some properties of MDS codes are discussed. The results are extended for the average binary image of MDS codes in finite fields of characteristic two. As an application, we study the multiuser error probability of Reed Solomon codes.

I. INTRODUCTION AND SUMMARY

In this paper, we introduce a generalized weight enumerator, which we call the partition weight enumerator (PWE). Our main result is a simple closed-form expression for the PWE of an arbitrary MDS, e.g., Reed-Solomon (RS), code (Theorem 3). This generalizes the results of Kasami et al. [1] on the split weight enumerator of RS codes.

We then derive weight enumerators for the average binary image of MDS (Reed-Solomon) codes defined over finite fields of characteristic two (Section IV).

We also derive a strong symmetry property for MDS codes (Theorem 10) which allows us to obtain improved bounds on the decoder error probability for RS codes (Section VI).

Finally, we discuss possible applications of the PWE, including the analysis of the performance of RS codes in a multiuser setting (Section VII).

II. PRELIMINARIES

We begin by generalizing the notion of Hamming weight. Let \( V_n(F_q) \) denote the vectors of length \( n \) over the finite field of \( q \) elements \( F_q \). Suppose the coordinate set \( N = \{1, 2, \ldots, n\} \) is partitioned into \( p \) disjoint subsets \( N_1, \ldots, N_p \), with \( |N_i| = n_i \), for \( i = 1, \ldots, p \). Denoting this partition by \( T \), the \( T \)-weight profile of a vector \( v \in V_n(F_q) \) is defined as \( W_T(v) = (w_1, \ldots, w_p) \), where \( w_i \) is the Hamming weight of \( v \) restricted to \( N_i \). Now we generalize the notion of code weight enumerator. Given a code \( C \) of length \( n \), and an \((n_1, n_2, \ldots, n_p)\) partition \( T \) of the \( n \) coordinates of \( C \), the \( T \)-weight enumerator of \( C \) is the set of numbers

\[
A^T(w_1, \ldots, w_p) = |\{c \in C : W_T(c) = (w_1, \ldots, w_p)\}|
\]

The weight enumerator of \( C \) is

\[
E_C(w) = |\{c \in C : W(c) = w\}|	ag{1}
\]

where \( W(c) \) is the Hamming weight of \( c \). The weight generating function (WGF) of \( C \) is the polynomial \( E_C(X) = \sum_{h=0}^{n} E_C(h)X^h \). (The subscript \( C \) may be dropped when there is no ambiguity about the code.) For an \((n, k, d)\) MDS code over \( F_q \), the minimum distance is \( d = n - k + 1 \) [2] and the weight distribution is given by [3, Th. 25.7] for weights \( i \geq d \),

\[
E(i) = \binom{n}{i}^{-1} \sum_{j=0}^{i} \left(-1\right)^{i-j} (q^{j-d+1} - 1) \tag{2}
\]

The partition weight generating function (PWGF) is

\[
\mathbb{P}^T_C(X_1, \ldots, X_p) = \sum_{w_1=0}^{n_1} \ldots \sum_{w_p=0}^{n_p} A^T(w_1, \ldots, w_p)X_1^{w_1} \ldots X_p^{w_p} \tag{3}
\]

For the special case of \( p = 2 \), \( A^T(w_1, w_2) \) is termed the split weight enumerator in the literature [4]. The input-redundancy weight enumerator (IRWE), \( R(w_1, w_2) \), is the number of codewords with input weight (weight of the information vector) \( w_1 \) and redundancy weight \( w_2 \). For a systematic code, if \( T \) is an \((k, n-k)\) partition such that the first partition constitutes of the coordinates of the information symbols, then \( R(w_1, w_2) = A^T(w_1, w_2) \). The input-output weight enumerator (IOWE) \( O(w, h) \) enumerates the codewords of total Hamming weight \( h \) and input weight \( w \). Assuming that the first partition constitutes of the information symbols, then \( O(w, h) = R(w, h-w) \). For an \((k, n-k)\) partition \( T \), it is straightforward that

\[
E(h) = \sum_{w=0}^{k} A^T(w, h-w) = \sum_{w=0}^{k} O(w, h) \tag{4}
\]

The IOWE and IRWE are used in the literature to study the bit error probabilities of codes (e.g. [5]).

For a systematic code, let the \( j \)th partition constitute of information symbols, then the \( j \)th IOWE,

\[
O^j(w, h) = |\{c \in C : (W(N_j) = w) \land (W(c) = h)\}| \tag{5}
\]

is the coefficient of \( X^wY^h \) in \( \mathbb{P}^j_C(X, Y) = \mathbb{P}^T_C(X_1, \ldots, X_j, Y_1, \ldots, Y) \) where the \( X_i \)s in \( \mathbb{P}^T_C \) are substituted by \( X_i \Rightarrow Y \) if \( i \neq j \) and \( X_i \Rightarrow X_jY \) if \( i = j \).
III. Partition weight enumerator of MDS codes

**Theorem 1:** For a \( p \)-partition \( T \), the PWE of an \( (n, k, d) \) MDS code \( C \) over \( F_q \), \( A^T(w_1, w_2, ..., w_p) \), is given by

\[
\begin{align*}
(n_1, ..., n_p) & \quad \sum_{j_1=0}^{w_1} \binom{w_1}{j_1} (-1)^{w_1-j_1} \sum_{j_2=0}^{w_2} \binom{w_2}{j_2} (-1)^{w_2-j_2} \\
& \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \frac{(n)}{h} (\sum_{i=1}^{n} w_i) \binom{n}{h} \left(q^{n-k} - q^{n-1} \right) 
end{align*}
\]

where \( w = \sum_{i=1}^{p} w_i \) and \( E(w) = |\{c \in C : W(c) = w\}| \).

The proof of Th. 1 also follows by generalizing the proof of Lem. 2 to any number of partitions.

**Corollary 4:** The IOWE of a systematic MDS code, is \( O(w, h) = E(h) \frac{n}{h} \binom{n}{h} \left(q^{n-k} - q^{n-1} \right) \) for \( h \geq d \).

Since \( \sum_{w} O(w, h) = E(h) \) and \( \binom{n}{h} \sum_{w} \binom{n}{w} \binom{w}{h} = \binom{n}{h} \binom{n-k}{h-k} \),

we have proved this interesting identity (using (4) and (7))

\[
\sum_{w=0}^{k} \binom{k}{w} \binom{n-k}{w} h-w = \sum_{w=0}^{k} \binom{k}{w} (n-k) \Psi(w) = \Psi(0) \sum_{w=0}^{k} \binom{k}{w} \frac{(n-k)}{h-w},
\]

where \( g(h, w, i) = \binom{h-w}{i} \binom{h-i}{w}$ and

\[
\Psi(w) = \sum_{j=0}^{w} \binom{w}{j} (-1)^{w-j} \sum_{i=d-j}^{w} g(h, w, i)(q^{i+j-d+1} - 1).
\]

**Corollary 5:** For an MDS code of length \( n \), the number of codewords which are zero at a fixed subset of coordinates of cardinality \( n-h \) and are nonzero in the remaining \( h \) positions is \( E(h) \binom{n}{h} \).

**Proof:** Let \( T \) be the implied \( (h, n-h) \) partition, then the required number of codewords is \( A^T(h, 0) \) (See Lem. 2).

**Example 6:** The PGWF for the \((1, 2, 3)\) partition of the coordinates of the \((7, 3, 5)\) RS code over \( F_3 \) is

\[
\mathcal{P}(V, X, Y, Z) = 1 + 21XY^2Z + 42XY^2Z^2 + 21Y^2Z^3 + 21X^2YZ^2 + 63X^2Y^2Z^2 + 7Y^2X^3 + 14Y^2Z^3 + 14X^2Y^2Z^3 + 7Y^2Z^3 + 21Y^2Z^3 + 21X^2Y^2Z^3 + 217Y^2Z^3.
\]

It could be checked that the sum of the coefficients is \( 8^3 \).

IV. AVERAGE BINARY PARTITION WEIGHT ENUMERATOR OF MDS CODES

The binary image \( C^b \) of an \((n, k)\) code \( C \) over \( F_{2^m} \) is obtained by representing each symbol by an \( m \)-dimensional binary vector in terms of a basis of the field \( [2] \). The weight enumerator of \( C^b \) will vary according to the basis used. For performance analysis, one could average the performance over all possible binary representations of \( C \). Assuming that the distribution of the bits in the non-zero symbol follows a binomial distribution, the average binary WGF, \( \bar{E}^b_h(\bar{X}) = E^b_h(\bar{X})^m \), could be shown to be \[ E^b_h(\bar{X}) = \sum_{h=0}^{n} \frac{E(h)}{(2^m-1)^h} ((1+\lambda)^m - 1)^h. \]

In [6], it was shown that the average binary weight enumerator approaches that of a normalized binomial distribution for all weights greater than the average binary minimum distance, \( d^b \), of the code

\[
\bar{E}(h) \approx q^{n-k} \left( \frac{m}{h} \right) \text{ for } h \geq d^b.
\]

Consequently, lower bounds on the average binary minimum distance were derived [6].

The average binary PGWF gives the average number of codewords with a specific profile of Hamming weights in the binary images of the specified partitions.

**Theorem 7:** Let \( F^b_h(\bar{X}_1, ..., \bar{X}_p) \) be the PGWF of an \((n, k)\) code \( C \) over \( F_{2^m} \), and \( T \) be the partition of the coordinates of \( C^b \) induced by \( T \) when the symbols are represented by bits. Given that \( F(Z) = \frac{1}{2^m-1} ((1+Z)^m - 1) \), the averaged PGWF of \( C^b \) is \( \bar{F}^b_h(\bar{Z}_1, ..., \bar{Z}_p) = \frac{1}{2^m} \left( F(Z_1), ..., F(Z_p) \right) \).
Sketch of Proof: Assuming a binomial distribution of the
bits in a nonzero symbol, the binary WGF of a partition
of symbol weight \( w_j \) is \( \left( \frac{1}{m} \sum_{i=1}^{m} (\binom{m}{i}) \right)^{w_j} \). If the T-
profile of a codeword is \( (w_1, w_2, \ldots, w_p) \), then its WGF is
\( \prod_{j=1}^{p} (F(Z))^n \). By multiplying with the number of such
codewords, \( A^T (w_1, w_2, \ldots, w_p) \), the result follows.

The average binary IOWE \( \bar{O}(w, h_b) \) enumerates the codewords
with an input weight \( w \) and an output weights \( h_b \) in the
average binary image.

Corollary 8: Let \( T \) be an \((n, s - n)\) partition of the
coordinates of \( C \) and \( Oc(w, h) \) be the corresponding IOWE,
then the averaged IOWE of \( C^b \) for the partition \( T_b \) is given by
\[
\bar{O}_{C^b}(w_b, h_b) = \frac{n}{|C|} \sum_{w=0}^{1} \sum_{h=0}^{n} Oc(w, h) \left( \frac{n - w}{(2^m - 1)^h} \right) \left( \frac{w}{j} \right) \left( \frac{h - w}{j} \right) \left( \frac{w}{h - w} \right) \left( \frac{h - w}{j} \right).
\]

The average binary image \( \bar{O}(w, h_b) \) is equal to
\( \prod_{j=1}^{p} (F(Z))^n \). If the T-
profile of a codeword is \( (w_1, w_2, \ldots, w_p) \), then its WGF is
\( \prod_{j=1}^{p} (F(Z))^n \). By multiplying with the number of such
codewords, \( A^T (w_1, w_2, \ldots, w_p) \), the result follows.

Sketch of Proof: Let \( T \) be an \((1, n - 1)\) partition, the required
number of codewords is \( A^T (1, h - 1) \). (See Lem. 4)

Since the PWE does not depend on the orientation of the
coordinates, we have the following theorem.

Theorem 10: For an \((n, k, d)\) MDS code \( C \), the ratio of the
total weight of any \( s \) coordinates of \( C^b \) to the total weight of
\( C^b \) is \( \frac{n}{n} \). If the \( s \) coordinates are ‘input’ coordinates, then
\( \sum_{w=0}^{n} O(w, h) = h^w E(h) \) for all Hamming weights \( h \).

As a side result, we have proven this identity (c.f. (5))
\[
\sum_{w=1}^{n} \left( \frac{s}{w} \right) \left( \frac{n - s}{h} \right) \left( \frac{h - w}{w} \right) \Psi(w) = \Psi(0) \sum_{w=1}^{n} \left( \frac{s - 1}{w} \right) \left( \frac{n - s}{h} \right) \left( \frac{h - w}{w} \right).
\]

Definition 11: An \((n, k)\) code \( C \) (not necessarily MDS)
is said to have property \( A \), if it satisfies Th. 10 for all \( s \) and \( h \).

Observe that Th. 10 is not true for all linear codes. For example,
the \((5, 3)\) binary code defined by the generator matrix
\[
G = \begin{pmatrix}
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1
0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1
0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1
\end{pmatrix}
\]
is composed of the 8 codewords, \{00000, 10011, 01001, 00111, 11010, 00101, 10110, 01100, and 11111\}, and doesn’t have property \( A \). (Let the input partition be composed of the first
3 coordinates.)

It is to be noted that all cyclic codes have property \( A \). This is
partially justified by the fact that any cyclic shift of a codeword
of weight \( h \) is also a codeword of weight \( h \) with \( h/n \) of the
coordinates holding non-zero elements. However, this neither
implies Th. 10 nor is it implied by Th. 10 (An extended RS
code is an MDS code but not a cyclic code while an \((7, 4)\)
binary Hamming code is cyclic but not MDS.) Also, if a code
satisfies property \( A \), it is not necessary that the code is cyclic or
MDS. For example, the first order Reed Muller codes \((3, 3)\)
as well as their duals, the extended Hamming codes \((4, 4)\), have
property \( A \) but are neither cyclic nor MDS.

Theorem 12: The first order Reed Muller codes have property \( A \).

Proof: By construction from Hadamard matrices \([8]\).

In fact, we prove here that if a linear code has property \( A \) then its dual has property \( A \). This result also strengthens Th. 10. We will start by the MacWilliams identity relating the
PWE of a code with that of the dual code.

Theorem 13: Let \( C \) be an \((n, k)\) linear code over \( F_q \) and
\( C^\perp \) be its dual code. If \( T \) is an \((n1, n2)\) partition of their
coordinates, \( A(\alpha, \beta) \) and \( A^\perp(\alpha, \beta) \) are the PWEs of \( C \) and \( C^\perp \)
respectively, then \( A(\alpha, \beta) \) and \( A^\perp(\alpha, \beta) \) are related by
\[
A^\perp(\alpha, \beta) = \frac{1}{|C|} \sum_{w=0}^{n} \sum_{v=0}^{n} A(w, v)K_{\alpha}(w, n1)K_{\beta}(v, n2),
\]
such that the Krawtchouk polynomial is \( K_{\beta}(v, \gamma) = \sum_{j=0}^{\beta} (-1)^j (q - 1)^{\beta - j} \) for \( \beta = 0, 1, \ldots, \gamma \).

Definition 12: \( A^\perp(\alpha, \beta) \) and \( A^\perp(\alpha, \beta) \) to be the PWEs of \( C \) and \( C^\perp \)
respectively for an \((n, k)\) linear code over \( F_q \) has property \( A \).

Sketch of Proof: From Th. 13 the PWE of \( C^\perp \) is
\[
A^\perp(1, \beta) = \frac{1}{|C|} \sum_{w=0}^{n} \sum_{v=0}^{n} A(w, v)K_{\alpha}(w, 1)K_{\beta}(v, n - 1),
\]
\( (12) \)
Since \( C \) has property \( A \), then \( A_i(1, v) \) and \( A_i(0, v) \) don’t
depend on the choice of the coordinate \( i \). Counting the total
weight of the codewords in \( C^\perp \) by two different ways, we get
\( \sum_{v=1}^{n} A_i(1, \beta) = (\beta + 1)E_{\perp}(\beta + 1) \) (c.f. Lem. 9).

The converse follows from that if \( C^\perp \) has property \( A \) then
\( (C^\perp)^\perp = C \) has property \( A \).

Corollary 15: The extended Hamming codes have property \( A \).

A similar property holds for the binary image of MDS codes
defined over \( F_{2^m} \).

Theorem 16: Let \( C \) be an MDS code over \( F_{2^m} \) with property \( A \). If \( O(w, h) \) is the IOWE of \( C^b \), where the partition
of the coordinates of \( C^b \) is induced by an \((s, n - s)\) partition of
the coordinates of \( C \), then \( \sum_{w=1}^{m} wO(w, h_b) = h_b E(h_b) \).

Sketch of Proof: Let \( s = 1 \). Since \( C \) has property \( A \), then
\( O(1, h) = h_b E(h_b) \). One can show that \( \sum_{w=1}^{m} wO(w, h_b) = h_b E(h_b) \) (See Cor. 8) by some algebraic manipulations.
VI. SYMBOL AND BIT ERROR PROBABILITIES OF RS CODES

In this section, we discuss the application of the PWE in determining the symbol or bit error probability when systematic RS codes are used for transmission. (Maximum likelihood (ML) decoding of binary linear codes achieves the least bit error probability when the code is systematic [10].)

The codeword error probability (CEP) is the probability that the received word lies in the decoding sphere of a codeword other than the transmitted word. The CEP for an \((n, k, d)\) RS code is determined by the weight enumerator of the code and the signal to noise ratio \(\gamma\) and is given by [11] [12, Eq. 10-9:20]

\[
\Phi_{C}(\gamma) = \sum_{h=0}^{\frac{n}{k}} E(h) \sum_{t=0}^{\tau} P_{t}^{h}(\gamma),
\]

(13)

where \(P_{t}^{h}(\gamma)\) is the probability that a received word is exactly Hamming distance \(t\) from a codeword of weight \(h\) and \(\tau = \lfloor (d-1)/2 \rfloor\) is the Hamming decoding radius.

It is well known that the symbol error probability (SEP) \(\Phi_{S}(\gamma)\) is derived from \(\Phi_{C}(\gamma)\) by substituting \(E(h)\) with \(O_{h} = \sum_{w=1}^{\gamma} \frac{1}{\gamma} O(w, h)\), (e.g., [12, Eq. 10-14]). From Th. 10 the common approximation \(O_{h} \approx \frac{n}{\gamma} E(h)\) is exact and

\[
\Phi_{S}(\gamma) = \Phi_{C}(\gamma) \mid_{E(h) \Rightarrow O_{h}} = \sum_{h=0}^{\frac{n}{k}} \frac{h}{n} E(h) \sum_{t=0}^{\tau} P_{t}^{h}(\gamma).
\]

In case the binary image of an RS code is transmitted, tight bounds on the CEP of the optimum ML decoder are obtained by using the average binary weight enumerator in conjunction with well-known bounds [6]. In case of harddecision ML decoding of binary linear codes over an additive white Gaussian noise (AWGN) channel, the Poltyrev bound for binary symmetric channels [13] is a tight upper bound. Tight bounds on the CEP of soft-decision ML decoding of binary linear block codes over AWGN channels are known (e.g., [13], [14]). The bounds on the CEP are often of the form \(\Phi_{C}(\gamma) = \sum_{h=0}^{n} E(h) F(\gamma, h)\). It follows that the bit error probability (BEP) is (e.g., [5], [15])

\[
\Phi_{B}(\gamma) = \Phi_{C}(\gamma) \mid_{E(h) \Rightarrow O_{h}} = \sum_{h=0}^{\frac{n}{k}} \frac{n}{m} O_{h} F(\gamma, h).
\]

(14)

From Th. 10 \(\hat{O}_{h} = \sum_{w=1}^{\frac{n}{m}} \frac{w}{m} \hat{O}(w, h) = \frac{n}{m} E(h)\).

VII. MULTIUSER ERROR PROBABILITY

We consider the case when a systematic RS codeword is shared among more than user or application, where the \(i\)th partition of size \(n_{i}\) is assigned to the \(i\)th user and the last partition constitutes of the redundancy symbols. It follows that the \(j\)th user’s SEP and BEP are, respectively,

\[
\Phi_{S}^{j}(\gamma) = \Phi_{C}(\gamma) \mid_{E(h) \Rightarrow O_{h}^{j}},
\]

(15)

\[
\Phi_{B}^{j}(\gamma) = \Phi_{C}(\gamma) \mid_{E(h) \Rightarrow O_{h}^{j}},
\]

(16)

where \(O_{h}^{j} = \sum_{w=1}^{n_{j}} \frac{w}{n_{j}} O^{j}(w, h), O_{h}^{j} = \sum_{w=1}^{n_{j}} \frac{w}{mn} \hat{O}^{j}(w, h)\) and \(O^{j}(w, h)\) is given by 4.

\[\text{Fig. 1. Multiuser error probability of the BM decoder.}\]

\[\text{Theorem 17: For a systematic linear MDS code, the unconditional SEP (BEP) of all the users is the same regardless of the size of the partition assigned to each of them.}\]

\[\text{Proof Idea: For any two users } i \text{ and } j, O_{h}^{i} = O_{h}^{j} = \frac{n}{m} E(h), \text{ regardless of } n_{i} \text{ and } n_{j}. \text{ For the average binary case, we also have } O_{h}^{j} = O_{h}^{i} = \frac{n}{m} E(h).\]

Using the results in this paper, one could answer interesting questions about the conditional multiuser error probability. Since the code is linear, we will assume that the all-zero codeword is transmitted. For example, the conditional CEP given that no more than a fraction \(p\) of the \(j\)th user’s symbols are received in error for any transmitted codeword is given by 1

\[
\Phi_{C}^{j}(\gamma) = \sum_{h=0}^{\frac{n}{k}} \sum_{w_{j}=0}^{P_{t}} O^{j}(w_{j}, h) \sum_{t=0}^{\tau} P_{t}^{h}.
\]

(17)

(Recall that \(E(h) = \sum_{w_{j}=0}^{P_{t}} O^{j}(w_{j}, h)\)). Let \(O(0, n_{j}; h) \triangleq |\{c \in \mathbb{C} : |W(c) = h \theta W(P_{j}) = 0 \land (W(P_{j}) = n_{j})\}|\).

The conditional CEP given that a codeword error results in all \(i\)th user’s symbols received correctly while all \(j\)th user’s symbols received erroneously is given by

\[
\Phi_{C}^{j}(\gamma) = \sum_{h=0}^{\frac{n}{k}} O(0, n_{j}, h) \sum_{t=0}^{\tau} P_{t}^{h}.
\]

(18)

In general for a \(p\)-partition of the coordinates, let \(\Omega\) and \(\Upsilon\) be the set of users (partitions) whose symbols are all received correctly and erroneously, respectively, in case of a codeword error. Let \(\Delta\) be the set of users with no condition on their error probability. The conditional error probability is calculated by considering only the codewords which have a full weight for the coordinates in \(\Upsilon\) and a zero weight for the coordinates in \(\Omega\). By considering only such combinations in the sum of 4, the conditional PWGF \(E(\lambda_{1}, \lambda_{2}, ..., \lambda_{p})\) is derived.

1Conditional functions will have have the same notation as the unconditional ones except for an underbar.
The conditional SEP of the $j$th user is

\[ \Phi_j^i(\gamma) = \Phi(C(\gamma)) \bigg|_{E(h) \Rightarrow \hat{O}^i_j}, \]

(19)

where $\hat{O}^i_j = \sum_{w=1}^{n_j} \frac{1}{w} \Omega^j_i(w, h)$ and $\Omega^j_i(w, h)$ is the conditional TOWE of the $j$th partition and is derived from $P(X_1, X_2, ..., X_p)$ (see (5)).

Similarly, for bit-level decoding of the code’s binary image, $\hat{O}^i_j$ will be derived from $P(X_1, X_2, ..., X_p)$. This conditional binary PWGF only takes into account such codewords that have a zero weight for the partitions in $\Omega$ and a full binary Hamming weight for the partitions in $\mathcal{T}$. The conditional SEP of the $j$th user follows by the substitution $E(h) \Rightarrow \hat{O}^i_j$ in (16).

**Example 18**: Consider a systematic $(15, 11)$ RS code and a partition $\mathcal{T} = (3, 3, 5, 4)$ of its coordinates where the last partition has the redundancy symbols and each of the first three partitions is assigned to a different user. Let the RS code (in fact its binary image) be transmitted over an AWGN channel and decoded by the Berlekamp-Massey (BM) decoder. In Fig. 1 the unconditional CEP and SEP (which by Th. 17 is equal to the SEP of the 3rd user) are plotted. The conditional SEP of the 3rd user is plotted for three cases; a codeword error results in user 1 and 2 having a SEP of i) zero (labeled (0, 0)), ii) zero and one respectively (0, 1), iii) one (1, 1). In Fig. 2 we consider the case when the decoder is the soft-decision ML decoder. Using the averaged binary PWE derived in this paper and the Poltyrev tangential sphere bound [13], we calculate the averaged conditional SEP of the third user given the three cases; SEP of the first and second users are (0, 0), (0, 1) and (1, 1) respectively in case of a codeword error. The bounds on the unconditional CEP and SEP are also plotted and are shown to be tight by comparing with the simulations (for a specific basis representation), ‘CEP Sim’ and ‘BEP Sim’ respectively.

It is observed, in Fig. 1 and Fig. 2 that the conditional SEP or BEP of a specific user decreases as the number of users receiving erroneous symbols, in case of a codeword error, increases.

**VIII. Conclusion**

In this paper, a closed form formula for the partition weight enumerator of maximum distance separable (MDS) codes is derived. The average PWE is derived for the binary image of MDS codes defined over a field of characteristic two. We show that for MDS codes, all the coordinates have the same weight in the subcode composed of codewords with equal weight. We prove that a code has this property iff its dual code has this property. Consequently, it is shown that the first order Reed Muller codes and the extended Hamming codes have this property. A common approximation used to evaluate the symbol and bit error probabilities is shown to be exact for MDS codes. These results are employed to study the error probability when a Reed Solomon code is shared among different users and the decoder is either a bounded minimum distance decoder or a maximum likelihood decoder.

**Acknowledgment**

This research was supported by NSF grant no. CCR-0118670 and grants from Sony, Qualcomm, and the Lee Center for Advanced Networking.

**References**

[1] T. Kasami, T. Takata, K. Yamachita, T. Fujiwara, and S. Lin, “On bit error probability of a concatenated coding scheme,” *IEEE Trans. Commun.*, vol. 45, no. 5, pp. 536–543, May 1997.

[2] R. J. McEliece, *The Theory of Information and Coding*, 2nd ed. Cambridge: Cambridge U. Press, 2002.

[3] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed. Cambridge: Cambridge U. Press, 2001.

[4] F. J. MacWilliams and N. J. Sloane, *The Theory of Error Correcting Codes*. Amsterdam: North Holland, 1977.

[5] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, “Serial concatenation of interleaved codes: Performance analysis, design and iterative decoding,” *IEEE Trans. Inform. Theory*, vol. 44, no. 3, pp. 909–926, May 1998.

[6] M. El-Khamy and R. J. McEliece, “Bounds on the average binary minimum distance and the maximum likelihood performance of Reed Solomon codes,” in *42nd Allerton Conf. on Communication, Control and Computing*, 2004.

[7] C. Retter, “The average binary weight enumerator for a class of generalized Reed-Solomon codes,” *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 346–349, March 1991.

[8] M. El-Khamy and R. J. McEliece, “The partition weight enumerator of maximum distance separable codes and its applications,” extended manuscript in preparation.

[9] T.-Y. Hwang, “A relation between the row weight and column weight distributions of a matrix,” *IEEE Trans. Inform. Theory*.

[10] M. Fossorier, S. Lin, and D. Rhee, “Bit-error probability for maximum-likelihood decoding of linear block codes and related soft-decision decoding methods,” *IEEE Trans. Inform. Theory*, vol. 44, no. 7, p. 3083–3090.

[11] R. J. McEliece and L. Swanson, “On the decoder error probability of Reed-Solomon codes,” *IEEE Trans. Inform. Theory*, vol. 32, no. 5, pp. 701–703, Sep. 1986.

[12] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*. Prentice Hall, 1995.

[13] G. Poltyrev, “Bounds on the decoding error probability of binary linear codes via their spectra,” *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1284–1292, July 1994.

[14] D. Divsalar, “A simple tight bound on error probability of block codes with application to turbo codes,” *TM0 Progress Report, NASA JPL*, Tech. Rep. 42–139, 1999.
[15] I. Sason and S. Shamai, “Improved upper bounds on the ml decoding error probability of parallel and serial concatenated turbo codes via their ensemble distance spectrum.” IEEE Trans. Inform. Theory, vol. 46, no. 1, pp. 24–47, Jan 2000.