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 $\mathcal{T}$, the $\mathcal{T}$-weight profile of a vector $\boldsymbol{v} \in V_n(F_q)$ is defined as $\mathcal{W}_{\mathcal{T}}(\boldsymbol{v}) = (w_1, \ldots, w_p)$, where w_i is the Hamming weight of $\boldsymbol{v}$ restricted to N_i. Now we generalize the notion of code weight enumerator. Given a code $\mathbb{C}$ of length n, and an $(n_1, n_2, ..., n_p)$ partition $\mathcal{T}$ of the n coordinates of $\mathbb{C}$, the $\mathcal{T}$-weight enumerator of $\mathbb{C}$ is the set of numbers

$$A^{\mathcal{T}}(w_1, \ldots, w_p) = |\{\boldsymbol{c} \in \mathbb{C} : \mathcal{W}_{\mathcal{T}}(\boldsymbol{c}) = (w_1, \ldots, w_p)\}|.$$

The weight enumerator of $\mathbb{C}$ is

$$E_{\mathbb{C}}(w) = |\{\boldsymbol{c} \in \mathbb{C} : \mathcal{W}(\boldsymbol{c}) = w\}|, \quad (2)$$

where $\mathcal{W}(\boldsymbol{c})$ is the Hamming weight of $\boldsymbol{c}$. The weight generating function (WGF) of $\mathbb{C}$ is the polynomial $\mathbb{E}_{\mathbb{C}}(\mathcal{X}) = \sum_{h=0}^{n} E_{\mathbb{C}}(h)\mathcal{X}^h$. (The subscript $\mathbb{C}$ 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 $i \geq d$,

$$E(i) = \binom{n}{i} \sum_{j=d}^{i} \binom{i}{j} (-1)^{i-j} (q^{j-d+1} - 1). \quad (3)$$

The *partition weight generating function* (PWGF) is

$$\mathbb{P}_{\mathbb{C}}^{\mathcal{T}}(\mathcal{X}_1, ..., \mathcal{X}_p) = \sum_{w_1=0}^{n_1} ... \sum_{w_p=0}^{n_p} A^{\mathcal{T}}(w_1, ..., w_p)\mathcal{X}_1^{w_1} ... \mathcal{X}_p^{w_p}. \quad (4)$$

For the special case of $p = 2$, $A^{\mathcal{T}}(w_1, w_2)$ 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 $\mathcal{T}$ is an $(k, n-k)$ partition such that the first partition constitutes of the coordinates of the information symbols, then $R(w_1, w_2) = A^{\mathcal{T}}(w_1, w_2)$. 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 $\mathcal{T}$, it is straight forward that

$$E(h) = \sum_{w=0}^{k} A^{\mathcal{T}}(w, h - w) = \sum_{w=0}^{k} O(w, h). \quad (5)$$

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 jth partition constitute of information symbols, then the jth IOWE,

$$O^j(w, h) = |\{\boldsymbol{c} \in \mathbb{C} : (\mathcal{W}(N_j) = w) \wedge (\mathcal{W}(\boldsymbol{c}) = h)\}|, \quad (6)$$

is the coefficient of $\mathcal{X}^w\mathcal{Y}^h$ in $\mathbb{O}^j(\mathcal{X}, \mathcal{Y}) = \mathbb{P}_{\mathbb{C}}^{\mathcal{T}}(\mathcal{Y}, \mathcal{Y}, ., \mathcal{X}\mathcal{Y}, ., \mathcal{Y})$ where the $\mathcal{X}_i$s in (4) are substituted by $\mathcal{X}_i \Rightarrow \mathcal{Y}$ if $i \neq j$ and $\mathcal{X}_i \Rightarrow \mathcal{X}\mathcal{Y}$ if $i = j$.

III. Partition weight enumerator of MDS codes

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

$$\binom{n_1}{w_1}....\binom{n_p}{w_p}\sum_{j_1=0}^{w_1}\binom{w_1}{j_1}(-1)^{w_1-j_1}\sum_{j_2=0}^{w_2}\binom{w_2}{j_2}(-1)^{w_2-j_2} .... \sum_{j_p=d-\sum_{z=1}^{p-1}j_z}^{w_p}\binom{w_p}{j_p}(-1)^{w_p-j_p}(q^{k-n+\sum_{z=1}^{p}j_z}-1).$$

Sketch of Proof: Let R_i be a subset of N_i for $i=1,2,..p$. Define $S(\boldsymbol{c})$ to be the support set of the codeword $\boldsymbol{c}$ and $f(R_1,..,R_p)\triangleq|\boldsymbol{c}:\{S(\boldsymbol{c})\cap N_i\}=R_i,\ \ \forall\ i|$. Let $S_i\subseteq N_i$, then from the MDS property of $\mathbb{C}$, we have

$$g(S_1,...,S_p)\triangleq\sum_{R_1\subseteq S_1}...\sum_{R_p\subseteq S_p}f(R_1,...,R_p) = \begin{cases}1, & \sum_{i=1}^{p}|S_i|<d;\\ q^{1-d+\sum_{i=1}^{p}|S_i|}, & n\geq\sum_{i=1}^{p}|S_i|\geq d.\end{cases} \quad (7)$$

Successively applying Möbius Inversion [3, Th. 25.1], and observing that the PWE is equal to

$$A^{\mathcal{T}}(w_1,...,w_p)=\prod_{i=1}^{p}\left(\sum_{R_i\subseteq N_i,|R_i|=w_i}\right)f(R_1,...,R_p),$$

the result follows. ∎

Lemma 2: Let $\mathcal{T}$ be an (n_1,n_2) partition, then $A^{\mathcal{T}}(w_1,w_2)=E(w_1+w_2)\frac{\binom{n_1}{w_1}\binom{n_2}{w_2}}{\binom{n}{w_1+w_2}}$.

Sketch of Proof: From Th. 1, the split weight enumerator is

$$A^{\mathcal{T}}(w_1,w_2)=\binom{n_1}{w_1}\binom{n_2}{w_2}\sum_{j=0}^{w_1}\binom{w_1}{j}(-1)^{w_1-j}\sum_{i=d-j}^{w_2}\binom{w_2}{i}(-1)^{w_2-i}(q^{i+j-d+1}-1). \quad (9)$$

By changing the order of the summations, doing a change of variables and comparing with (3), we are done. ∎

The PWE of MDS codes does not depend on the orientation of the coordinates with respect to the partitions but only on the partitions' sizes and weights (see (7)). Thus the ratio of $A^{\mathcal{T}}(w_1,w_2,...,w_p)$ to $E\left(\sum_{i=1}^{p}w_i\right)$ is the probability that the nonzero symbols are distributed among the partitions with a $\mathcal{T}$-profile $(w_1,w_2,...,w_p)$, i.e.,

Theorem 3: For an (n,k,d) MDS code $\mathbb{C}$ the p-partition weight enumerator is given by

$$A^{\mathcal{T}}(w_1,w_2,...,w_p)=E(w)\frac{\binom{n_1}{w_1}\binom{n_2}{w_2}....\binom{n_p}{w_p}}{\binom{n}{w}},$$

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

The proof of Th. 3 also follows by generalizing the proof of Lem. 2 to any number of partitions.

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

Since $\sum_w O(w,h)=E(h)$ and $\binom{n}{h}=\sum_{w=0}^{k}\binom{k}{w}\binom{n-k}{h-w}$, we have proved this interesting identity (using (3) and (9))

$$\sum_{w=0}^{k}\binom{k}{w}\binom{n-k}{h-w}\Psi(w)=\Psi(0)\sum_{w=0}^{k}\binom{k}{w}\binom{n-k}{h-w}, \quad (10)$$

where $g(h,w,i)\triangleq\binom{h-w}{i}(-1)^{h-w-i}$ and

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

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 $\frac{E(h)}{\binom{n}{h}}$.

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

Example 6: The PWGF for the $(1,1,2,3)$ partition of the coordinates of the $(7,3,5)$ RS code over F_8 is $\mathbb{P}(\mathcal{V},\mathcal{X},\mathcal{Y},\mathcal{Z}) = 1+21\mathcal{V}\mathcal{X}\mathcal{Y}^2\mathcal{Z}+42\mathcal{V}\mathcal{X}\mathcal{Y}\mathcal{Z}^2+21\mathcal{V}\mathcal{Y}^2\mathcal{Z}^2+21\mathcal{X}\mathcal{Y}^2\mathcal{Z}^2+63\mathcal{V}\mathcal{X}\mathcal{Y}^2\mathcal{Z}^2+7\mathcal{V}\mathcal{X}\mathcal{Z}^3+14\mathcal{V}\mathcal{Y}\mathcal{Z}^3+14\mathcal{X}\mathcal{Y}\mathcal{Z}^3+42\mathcal{V}\mathcal{X}\mathcal{Y}\mathcal{Z}^3+7\mathcal{Y}^2\mathcal{Z}^3+21\mathcal{V}\mathcal{Y}^2\mathcal{Z}^3+21\mathcal{X}\mathcal{Y}^2\mathcal{Z}^3+217\mathcal{V}\mathcal{X}\mathcal{Y}^2\mathcal{Z}^3$.

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 $\mathbb{C}^b$ of an (n,k) code $\mathbb{C}$ 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 $\mathbb{C}^b$ will vary according to the basis used. For performance analysis, one could average the performance over all possible binary representations of $\mathbb{C}$. Assuming that the distribution of the bits in the non-zero symbol follows a binomial distribution, the *average binary* WGF, $\tilde{\mathbb{E}}_{\mathbb{C}^b}(\mathcal{X})=\sum_{h=0}^{nm}\tilde{E}(h)\mathcal{X}^h$, could be shown to be [6], [7],

$$\tilde{\mathbb{E}}_{\mathbb{C}^b}(\mathcal{X})=\sum_{h=0}^{n}\frac{E(h)}{(2^m-1)^h}\left((1+\mathcal{X})^m-1\right)^h. \quad (12)$$

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, $\tilde{d}^b$, of the code

$$\tilde{E}(h)\approx q^{-(n-k)}\binom{mn}{h}\ ;h\geq\tilde{d}^b. \quad (13)$$

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

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

Theorem 7: Let $\mathbb{P}_{\mathbb{C}}^{\mathcal{T}}(\mathcal{X}_1,...,\mathcal{X}_p)$ be the PWGF of an (n,k) code $\mathbb{C}$ over F_{2^m}, and $\mathcal{T}_b$ be the partition of the coordinates of $\mathbb{C}^b$ induced by $\mathcal{T}$ when the symbols are represented by bits. Given that $F(\mathcal{Z})=\frac{1}{2^m-1}((1+\mathcal{Z})^m-1)$, the averaged PWGF of $\mathbb{C}^b$ is $\tilde{\mathbb{P}}_{\mathbb{C}^b}^{\mathcal{T}_b}(\mathcal{Z}_1,...,\mathcal{Z}_p)=\mathbb{P}_{\mathbb{C}}^{\mathcal{T}}(F(\mathcal{Z}_1),...,F(\mathcal{Z}_p))$.

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 $\left(\frac{1}{2^m-1}\sum_{i=1}^{m}\binom{m}{i}\mathcal{Z}_j^i\right)^{w_j}$. If the $\mathcal{T}$-profile of a codeword is $(w_1, w_2, ..., w_j)$, then its WGF is $\prod_{j=1}^{p}(F(\mathcal{Z}))^{w_j}$. By multiplying with the number of such codewords, $A^{\mathcal{T}}(w_1, w_2, ..., w_p)$, the result follows. ■

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

Corollary 8: Let $\mathcal{T}$ be an $(s, n-s)$ partition of the coordinates of $\mathbb{C}$ and $O_{\mathbb{C}}(w, h)$ be the corresponding IOWE, then the averaged IOWE of $\mathbb{C}^b$ for the partition $\mathcal{T}_b$ is given by

$$\tilde{O}_{\mathbb{C}^b}(w_b, h_b) = \sum_{w=0}^{s}\sum_{h=w}^{n}\frac{O_{\mathbb{C}}(w,h)}{(2^m-1)^h}\left(\sum_{j=0}^{h-w}(-1)^{h-w-j}\right.$$
$$\left.\binom{h-w}{j}\binom{jm}{h_b-w_b}\right)\left(\sum_{j=0}^{w}(-1)^{w-j}\binom{w}{j}\binom{jm}{w_b}\right). \quad (14)$$

The proof follows by some algebra [8].

V. A relationship between Coordinate weight and the codeword weight.

Define $\mathbb{C}_h \triangleq \{\boldsymbol{c} \in \mathbb{C} : \mathcal{W}(\boldsymbol{c}) = h\}$. We prove an important property of MDS codes in the following lemma.

Lemma 9: For an (n, k, d) MDS code $\mathbb{C}$, the total Hamming weight of any coordinate, summed over all codewords in $\mathbb{C}_h$, is equal to $\frac{hE(h)}{n}$, where $\mathbb{C}_h$ is the set of codewords of $\mathbb{C}$ with Hamming weight h.

Sketch of Proof: Let $\mathcal{T}$ be an $(1, n-1)$ partition, the required number of codewords is $A^{\mathcal{T}}(1, h-1)$. (See Lem. 2.) ■

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 $\mathbb{C}$, the ratio of the total weight of any s coordinates of $\mathbb{C}_h$ to the total weight of $\mathbb{C}_h$ is $\frac{s}{n}$. If the s coordinates are 'input' coordinates, then $\sum_{w=1}^{s} w\tilde{O}(w, h) = \frac{s}{n}hE(h)$ for all Hamming weights h.

As a side result, we have proven this identity (c.f. (10))

$$\sum_{w=1}^{s}\binom{s-1}{w-1}\binom{n-s}{h-w}\Psi(w) = \Psi(0)\sum_{w=1}^{s}\binom{s-1}{w-1}\binom{n-s}{h-w}.$$

Definition 11: An (n, k) code $\mathbb{C}$ (not necessary MDS) is said to have property $\mathcal{A}$, 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

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

is composed of the 8 codewords, {00000, 10011, 01001, 11010, 00101, 10110, 01100, and 11111}, and doesn't have property $\mathcal{A}$. (Let the input partition be composed of the first 3 coordinates.)

It is to be noted that all cyclic codes have property $\mathcal{A}$. 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 $\mathcal{A}$, it is not necessary that the code is cyclic or MDS. For example, the first order Reed Muller codes [3] as well as their duals, the extended Hamming codes [4], have property $\mathcal{A}$ but are neither cyclic nor MDS;

Theorem 12: The first order Reed Muller codes have property $\mathcal{A}$.

Proof: By construction from Hadamard matrices [8]. ■

In fact, we prove here that if a linear code has property $\mathcal{A}$ then its dual has property $\mathcal{A}$. 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 $\mathbb{C}$ be an (n, k) linear code over F_q and $\mathbb{C}^{\perp}$ be its dual code. If $\mathcal{T}$ is an $(n1, n2)$ partition of their coordinates, $A(\alpha, \beta)$ and $A^{\perp}(\alpha, \beta)$ are the PWEs of $\mathbb{C}$ and $\mathbb{C}^{\perp}$ respectively, then $A(\alpha, \beta)$ and $A^{\perp}(\alpha, \beta)$ are related by

$$A^{\perp}(\alpha, \beta) = \frac{1}{|\mathbb{C}|}\sum_{v=0}^{n_2}\sum_{w=0}^{n_1}A(w, v)\mathcal{K}_{\alpha}(w, n_1)\mathcal{K}_{\beta}(v, n_2),$$

such that the Krawtchouk polynomial is $\mathcal{K}_{\beta}(v, \gamma) = \sum_{j=0}^{\beta}\binom{\gamma-v}{\beta-j}\binom{v}{j}(-1)^j(q-1)^{\beta-j}$ for $\beta = 0, 1, ..., \gamma$.

Proof: By a straight forward manipulation of the Macwilliams identity for the split weight enumerator [4, Ch. 5, Eq. 52], [9]. ■.

Define $A_j(\alpha, \beta)$ and $A_j^{\perp}(\alpha, \beta)$ to be the PWEs of $\mathbb{C}$ and $\mathbb{C}^{\perp}$ respectively for an $(1, n-1)$ partition of their coordinates such that the first partition is composed of the jth symbol.

Theorem 14: An (n, k) linear code over F_q has property $\mathcal{A}$ iff its dual has property $\mathcal{A}$.

Sketch of Proof: From Th. 13, the PWE of $\mathbb{C}^{\perp}$ is

$$A_i^{\perp}(1, \beta) = \frac{1}{|\mathbb{C}|}\sum_{v=0}^{n-1}\sum_{w=0}^{1}A_i(w, v)\mathcal{K}_1(w, 1)\mathcal{K}_{\beta}(v, n-1). \quad (18)$$

Since $\mathbb{C}$ has property $\mathcal{A}$, 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 $\mathbb{C}_{\beta+1}^{\perp}$ by two different ways, we get $\sum_{i=1}^{n}A_i^{\perp}(1, \beta) = (\beta+1)E_{\mathbb{C}^{\perp}}(\beta+1)$ (c.f Lem. 9). The converse follows from that if $\mathbb{C}^{\perp}$ has property $\mathcal{A}$ then $(\mathbb{C}^{\perp})^{\perp} = \mathbb{C}$ has property $\mathcal{A}$. ■

Corollary 15: The extended Hamming codes have property $\mathcal{A}$.

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

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

Sketch of Proof: Let $s = 1$. Since $\mathbb{C}$ has property $\mathcal{A}$, then $O(1, h) = \frac{h}{n}E(h)$. One can show that $\sum_{w_b=1}^{m} w_b\tilde{O}(w_b, h_b) = \frac{h_b}{n}\tilde{E}(h_b)$ (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 γ and is given by [11] [12, Eq. 10-9:20]

$$\Phi_C(\gamma) = \sum_{h=d}^{n} E(h) \sum_{t=0}^{\tau} P_t^h(\gamma), \tag{19}$$

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 $O_h = \sum_{w=1}^{k} \frac{w}{k} O(w,h)$, (e.g., [12, Eq. 10-14]). From Th. 10, the common approximation $O_h \approx \frac{h}{n} E(h)$ is exact and

$$\Phi_S(\gamma) = \Phi_C(\gamma)\,\big|_{E(h) \Rightarrow O_h} = \sum_{h=d}^{n} \frac{h}{n} E(h) \sum_{t=0}^{\tau} P_t^h(\gamma).$$

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 hard-decision 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 $\Phi_C(\gamma) = \sum_{h=d}^{nm} \tilde{E}(h) F(\gamma, h)$. It follows that the bit error probability (BEP) is (e.g., [5], [15])

$$\Phi_B(\gamma) = \Phi_C(\gamma)\,\Big|_{\tilde{E}(h) \Rightarrow \tilde{O}_h} = \sum_{h=d}^{nm} \tilde{O}_h F(\gamma, h). \tag{21}$$

From Th. 16, $\tilde{O}_h = \sum_{w=1}^{mk} \frac{w}{mk} \tilde{O}(w,h) = \frac{h}{mn} \tilde{E}(h)$.

VII. Multiuser Error Probability

We consider the case when a systematic RS codeword is shared among more than user or application, where the ith partition of size n_i is assigned to the ith user and the last partition constitutes of the redundancy symbols. It follows that the jth user's SEP and BEP are, respectively,

$$\Phi_S^j(\gamma) = \Phi_C(\gamma)\,\Big|_{E(h) \Rightarrow O_h^j}, \tag{22}$$

$$\Phi_B^j(\gamma) = \Phi_C(\gamma)\,\Big|_{\tilde{E}(h) \Rightarrow \tilde{O}_h^j}, \tag{23}$$

where $O_h^j = \sum_{w=1}^{n_j} \frac{w}{n_j} O^j(w,h)$, $\tilde{O}_h^j = \sum_{w=1}^{n_j m} \frac{w}{mn_j} \tilde{O}^j(w,h)$ and $O^j(w,h)$ is given by (6).

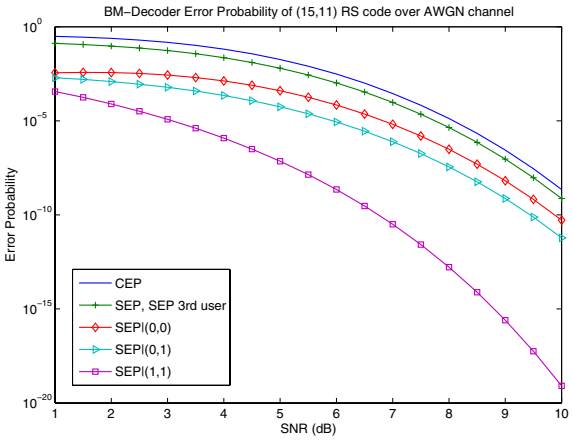

Fig. 1. Multiuser error probability of the BM decoder.

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.

Proof Idea: For any two users i and j, $O_h^j = O_h^i = \frac{h}{n} E(h)$, regardless of n_i and n_j. For the average binary case, we also have $\tilde{O}_h^j = \tilde{O}_h^i = \frac{h}{mn} \tilde{E}(h)$. ■

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 jth user's symbols are received in error for any transmitted codeword is given by [1]

$$\underline{\Phi_C}(\gamma) = \sum_{h=d}^{n} \sum_{w_j=0}^{\lfloor p n_j \rfloor} O^j(w_j, h) \sum_{t=0}^{\tau} P_t^h. \tag{24}$$

(Recall that $E(h) = \sum_{w_j=0}^{n_j} O^j(w_j, h)$.) Let $O(0, n_j; h) \triangleq |\{\boldsymbol{c} \in \mathbb{C} : (\mathcal{W}(\boldsymbol{c}) = h) \wedge (\mathcal{W}(P_i) = 0) \wedge (\mathcal{W}(P_j) = n_j)\}|$. The conditional CEP given that a codeword error results in all ith user's symbols received correctly while all jth user's symbols received erroneously is given by

$$\underline{\Phi_C}(\gamma) = \sum_{h=d}^{n} O(0, n_j, h) \sum_{t=0}^{\tau} P_t^h. \tag{25}$$

In general for a p-partition of the coordinates, let Ω and Υ be the set of users (partitions) whose symbols are all received correctly and erroneously, respectively, in case of a codeword error. Let Δ 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 Υ and a zero weight for the coordinates in Ω. By considering only such combinations in the sum of (4), the conditional PWGF $\underline{\mathbb{P}}(\mathcal{X}_1, \mathcal{X}_2, ..., \mathcal{X}_p)$ is derived. The

[1] Conditional functions will have have the same notation as the unconditional ones except for an underbar.

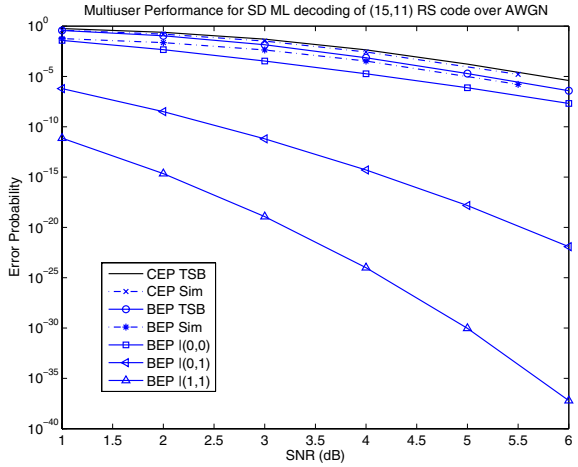

Fig. 2. Multiuser error probability of the SD-ML decoder

conditional SEP of the jth user is

$$\underline{\Phi_S^j}(\gamma) = \Phi_C(\gamma)\Big|_{E(h)\Rightarrow \underline{O_h^j}}, \tag{26}$$

where $\underline{O_h^j} = \sum_{w=1}^{n_j} \frac{w}{n_j}\underline{O^j}(w,h)$ and $\underline{O^j}(w,h)$ is the conditional IOWE of the jth partition and is derived from $\underline{\mathbb{P}}(\mathcal{X}_1, \mathcal{X}_2, ..., \mathcal{X}_p)$ (see (6)).

Similarly, for bit-level decoding of the code's binary image, $\underline{\tilde{O}_h^j}$ will be derived from $\underline{\tilde{\mathbb{P}}}(\mathcal{X}_1, \mathcal{X}_2, ..., \mathcal{X}_p)$. This conditional binary PWGF only takes into account such codewords that have a zero weight for the partitions in Ω and a full binary Hamming weight for the partitions in Υ.The conditional BEP of the jth user follows by the substitution $\tilde{E}(h) \Rightarrow \underline{\tilde{O}_h^j}$ in (23).

Example 18: Consider an 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 BEP of the third user given the three cases; BEP 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 BEP 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 seperable 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. 30833090.

[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," TMO 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.