Title

On the probability of undetected error for overextended Reed-Solomon codes

Journal

IEEE Transactions on Information Theory, 52(8)

ISSN

0018-9448

Authors

Han, Junsheng S
Siegel, Paul H
Lee, Patrick

Publication Date

2006-08-01

Peer reviewed

Correspondence

On the Probability of Undetected Error for Overextended Reed–Solomon Codes

Junsheng Han, Paul H. Siegel, *Fellow, IEEE*, and Patrick Lee, *Senior Member, IEEE*

***Abstract*—Upper and lower bounds on the weight distribution of overextended Reed–Solomon (OERS) codes are derived, from which tight upper and lower bounds on the probability of undetected error for OERS codes are obtained for q-ary symmetric channels.**

***Index Terms*—q-ary symmetric channel, overextended Reed–Solomon (OERS) codes, probability of undetected error, weight distribution.**

I. Introduction

In some applications, error correcting codes have been used as pure error detection codes. In particular, Reed–Solomon (RS) codes have been used for error detection in some disk drives since the 1990's because they have excellent error detection capabilities and do not exhibit the undesirable behavior characteristic of certain shortened binary cyclic redundancy check (CRC) codes [1]. A further example is the USB interface standard [2], which specifies the use of a Hamming code for error detection.

Typically, the error detecting capabilities of these codes are guaranteed only when the codeword length is limited to some maximum number of symbols. For RS codes defined over a finite field with q elements, $\mathbb{F}_q$, the maximum length is $q-1$ symbols (or q symbols for an extended code). However, for various reasons such as format efficiency, we sometimes use an *overextended code*, where the codeword length is allowed to exceed this maximum length. For example, a 16-bit, binary CRC is most often used to protect codewords consisting of $n = 2^{15}-1$ or fewer bits. However, the ultra DMA mode in the ATA standard [3] specifies the use of a 16-bit CRC for protecting data packets of length much greater than n bits.

When a block code is used solely for error detection, the decoder announces the received word to be free of error if it is found in the codebook. However, errors may have occurred in such a way that the received word is a codeword different from the one transmitted, in which case the errors will not be detected. The probability of such an event is known as the probability of undetected error, and is denoted by P_{ud}.

Consider an (n,k) linear block code over $\mathbb{F}_q$, transmitted over a q-ary symmetric channel, where each transmitted symbol is received correctly with probability $1-p$, and as any of the other $q-1$ symbols with equal probability $p/(q-1)$. Clearly, for this channel, P_{ud} can be calculated as a function of p as follows:

$$P_{ud}(p) = \sum_{i=1}^{n} A_i \left(\frac{p}{q-1}\right)^i (1-p)^{n-i} \tag{1}$$

where A_i is the number of codewords with Hamming weight i. Equation (1) relates the probability of undetected error directly to the weight distribution of the code. Alternatively, $P_{ud}(p)$ can also be obtained from the weight distribution of the dual code, as follows:

$$P_{ud}(p) = q^{-(n-k)} \sum_{i=0}^{n} A_i^{\perp} \left(1 - \frac{qp}{q-1}\right)^i - (1-p)^n \tag{2}$$

where $A_i^{\perp}$ is the number of codewords with Hamming weight i in the dual code. This can be conveniently shown from (1) using the MacWilliams identity [4], [5].

When $p = (q-1)/q$, the received symbols appear to be uniformly distributed no matter which codeword was transmitted. Therefore, undetected error occurs when the received word is any codeword except the one sent and each such codeword appears with probability q^{-n}. Since there are $q^k - 1$ such incorrect codewords, we have

$$P_{ud}\left(\frac{q-1}{q}\right) = (q^k - 1)q^{-n} < q^{-(n-k)}.$$

The same result can be obtained directly from (1). Note that this "purely random" case does not necessarily correspond to the worst-case error detection performance [6]–[9], for $0 \le p \le \frac{q-1}{q}$. Intuitively, if the weight distribution of the code is concentrated near certain weights, it is more likely that a codeword is confused with another when typically certain numbers of errors occur, rather than when typically an exceedingly large number of errors occur. For the same reasons, $P_{ud}(p)$ is not guaranteed to be a monotonic function of p for $0 \le p \le \frac{q-1}{q}$, though in [8] the authors were able to show that except for certain trivial classes of codes, $P_{ud}(p)$ is well-behaved in the vicinity of $\frac{q-1}{q}$ (i.e., $P'_{ud}(\frac{q-1}{q}) > 0$).

Following [7], [10], [11], we call a code *good* if $P_{ud}(p) < q^{-(n-k)}$ for all $0 \le p \le \frac{q-1}{q}$, and *proper* if $P_{ud}(p)$ is monotonic in p for $0 \le p \le \frac{q-1}{q}$. (Some authors have used $q^{-(n-k)} - q^{-n}$ as the goodness threshold. See [12].) Proper codes are necessarily good, but not vice versa. Properness and goodness properties of certain classes of codes are addressed in [6], [7], [9]–[11]. In particular, MDS codes (e.g., RS codes) are known to be good and proper [11]. Note also that for the ensemble of all (n,k) linear block codes over $\mathbb{F}_q$, it is known [12] that the average probability of undetected error is

$$P_{ud}^{\text{avg}}(p) = \frac{q^k - 1}{q^n - 1}(1 - (1-p)^n).$$

For systematic codes, a similar result is known [13], [8]

$$P_{ud}^{\text{sys}}(p) = q^{-(n-k)}(1 - (1-p)^k).$$

Note that in either case, the average performance of a randomly chosen code satisfies the conditions for both goodness and properness.

In this correspondence, we consider overextended RS (OERS) codes. From a practical point of view, these codes are constructed by

Manuscript received June 16, 2005; revised March 4, 2006. The material in this correspondence was presented in part at the IEEE Information Theory Workshop, Punta del Este, Uruguay, March 2006.

J. Han and P. H. Siegel are with the Center for Magnetic Recording Research, University of California, San Diego, La Jolla, CA 92093-0401 USA (e-mail: han@cts.ucsd.edu; psiegel@ucsd.edu).

P. Lee is with the Western Digital Corporation, Lake Forest, CA 92630 USA (e-mail: patrick.lee@wdc.com).

Communicated by M. P. Fossorier, Associate Editor for Coding Techniques.

Digital Object Identifier 10.1109/TIT.2006.876255

using a (shift register type) RS encoder but allowing a longer input. Let $\mathcal{C}$ be a RS code over $\mathbb{F}_q$ with length $n = q-1$ and minimum distance d. Then $\mathcal{C}$ can be described as the set of polynomials $c(x)$ such that

$$c(x) = -r(x) + x^{d-1}u(x) \tag{3}$$

where $u(x)$ is the data polynomial of degree at most $n-d$, and $r(x)$ is the remainder of $x^{d-1}u(x)$ divided by $g(x)$, the generator polynomial of $\mathcal{C}$. An OERS code $\mathcal{C}'$ can then be defined simply by allowing $u(x)$ in (3) to have degree higher than $n-d$, such that the length of the code is extended to $n' > n$. This results in a linear $(n', n'-d+1)$ code over $\mathbb{F}_q$.

The rest of the correspondence is arranged as follows. In Section II, we derive upper and lower bounds on the weight distribution of OERS codes. In Section III, we apply the results of Section II to obtain bounds on the probability of undetected error for OERS codes on q-ary symmetric channels. We show that the bounds are asymptotically tight, which is corroborated by an example. Section IV concludes the correspondence. Proofs, where not given, are either evident or can be found in Appendix.

II. Weight Distribution

First, a few remarks on notation. Throughout the rest of the correspondence, unless otherwise stated, $\mathcal{C}$ is a RS code over $\mathbb{F}_q$ with length $n = q-1$, minimum distance d, and generator polynomial $g(x)$; $\mathcal{C}'$ is the OERS code constructed from $\mathcal{C}$ with length $n' > n$. In most of our discussions, $\mathcal{C}$ and $\mathcal{C}'$ will be interpreted as subsets of $\mathbb{F}_q[x]$, the ring of polynomials with coefficients in $\mathbb{F}_q$. If $c(x) \in \mathbb{F}_q[x]$, then $\deg(c(x))$, or $\deg(c)$, is the degree of $c(x)$, and $\mathrm{wt}(c(x))$, or $\mathrm{wt}(c)$, is the number of nonzero terms in $c(x)$, i.e., the Hamming weight of the corresponding vector of coefficients. For any Euclidean domain D and $a, b \in D$, $R_a[b]$ is the remainder of b divided by a. Vectors are indicated in bold. If $\boldsymbol{x}$ is a vector, then $|\boldsymbol{x}|$ is the dimension of $\boldsymbol{x}$.

From the definition of OERS codes given in the previous section, it is easy to show that $\mathcal{C}'$ is also the set of polynomials in $\mathbb{F}_q[x]$ that have degrees less than n' and are divisible by $g(x)$. This is the definition that we will use most often.

Since $g(x) \mid x^n - 1$, we know that $x^n - 1 \in \mathcal{C}'$ for all $n' > n$. Therefore, all OERS codes contain codewords of weight 2, and thus have minimum distance $\min(d, 2)$.

Let $\mathcal{A}'_i$ denote the set of weight-i codewords of $\mathcal{C}'$. We are interested in finding $A'_i = |\mathcal{A}'_i|$ for all i. For very low weights, the problem of determining the corresponding term in the weight enumerator is tractable—we can fully characterize all codewords of a given low weight and thereby count them. The results for weight-2 and weight-3 codewords are summarized in the following propositions.

Proposition 1: The number of weight-2 codewords in an OERS code is

$$A'_2 = \begin{cases} \binom{a}{2}(q-1)^2 + ab(q-1), & \text{if } d > 2 \\ \binom{n'}{2}(q-1), & \text{if } d = 2 \\ \binom{n'}{2}(q-1)^2, & \text{if } d = 1 \end{cases}$$

where a and b are integers such that $n' = an + b, 0 \le b < n$.

Proof: See Appendix A. □

Corollary 2: If $d > 2$ and $n \mid n'$, then $A'_2 = \binom{n'/n}{2}(q-1)^2$.

For example, if the OERS code has twice the length of the original RS code, then $A'_2 = (q-1)^2$ if $d > 2$.

Proposition 3: The number of weight-3 codewords in an OERS code is shown in the equation at the bottom of the page, where a and b are integers such that $n' = an + b, 0 \le b < n$.

Proof: See Appendix B. □

The study of these special cases motivates a general approach to understanding the entire weight distribution of OERS codes. The following two lemmas, though elementary, are the basis of much of the discussion that follows.

Lemma 4: If $c(x) \in \mathbb{F}_q[x]$ and $\deg(c(x)) < n'$, then $c(x) \in \mathcal{C}'$ if and only if $R_{x^n-1}[c(x)] \in \mathcal{C}$.

Proof: Note $R_{g(x)}[c(x)] = R_{g(x)}[R_{x^n-1}[c(x)]]$. □

Lemma 5: For all $c(x) \in \mathbb{F}_q[x]$

$$\mathrm{wt}(c(x)) \ge \mathrm{wt}(R_{x^n-1}[c(x)]).$$

Proof: If $c(x) = \sum_{i=0}^{m} c_i x^i$, then

$$R_{x^n-1}[c(x)] = \sum_{i=0}^{m} c_i x^{R_n[i]} = \sum_{j=0}^{n-1} r_j x^j$$

where $r_j = \sum_{i:R_n[i]=j} c_i$. For each j such that $r_j \neq 0$, there exists i, $i \equiv j \mod n$, such that $c_i \neq 0$. □

From Lemma 4, since $0 \in \mathcal{C}$, if we define $\mathcal{B}'_i := \{c(x) \in \mathbb{F}_q[x] : \mathrm{wt}(c(x)) = i, \deg(c(x)) < n', x^n - 1 \mid c(x)\}$, then $\mathcal{B}'_i \subseteq \mathcal{A}'_i$. We first show how $B'_i := |\mathcal{B}'_i|$ can be calculated. For $n' \le 2n$, the situation is particularly simple.

Proposition 6: If $n' \le 2n$, then for all i,

$$B'_i = \begin{cases} \binom{n'-n}{i/2}(q-1)^{i/2}, & \text{if } i \text{ is even} \\ 0, & \text{if } i \text{ is odd.} \end{cases} \tag{4}$$

Proof: Note that $\mathcal{B}'_i = \{c(x) \in \mathbb{F}_q[x] : \mathrm{wt}(c(x)) = i, c(x) = (x^n-1)a(x), a(x) \in \mathbb{F}_q[x], \deg(a(x)) < n' - n\}$. If $n' \le 2n$, then $\deg(a(x)) < n$, which implies that $a(x)$ and $x^n a(x)$ have no powers of x in common. Therefore, $i = \mathrm{wt}(c(x)) = 2\mathrm{wt}(a(x))$. This is only possible if i is even. And the number of such $c(x)$'s is precisely the number of $a(x)$'s such that $\deg(a(x)) < n' - n$ and $\mathrm{wt}(a(x)) = i/2$. □

In general, for every $c(x) = \sum_{j=0}^{\deg(c)} c_j x^j \in \mathbb{F}_q[x]$, denote its support set as

$$\mathcal{W}(c) := \{j : 0 \le j \le \deg(c), c_j \neq 0\}.$$

Given a positive integer n, we can write

$$\mathcal{W}(c) = \bigcup_{l=0}^{n-1} \mathcal{W}(c) \cap (l + n\mathbb{Z}) \tag{5}$$

$$A'_3 = \begin{cases} \left(\binom{a}{3}(q-1) + \binom{a}{2}b\right)(q-1)(q-2), & \text{if } d > 3 \\ \left(\binom{n'}{3} - (n'-2)\left(\binom{a}{2}(q-1) + ab\right) + q\left(\binom{a}{3}(q-1) + \binom{a}{2}b\right)\right)(q-1), & \text{if } d = 3 \\ \binom{n'}{3}(q-1)(q-2), & \text{if } d = 2 \\ \binom{n'}{3}(q-1)^3, & \text{if } d = 1 \end{cases}$$

$$= \bigcup_{l \in \mathcal{L}_n(c)} \mathcal{W}_{n,l}(c) \tag{6}$$

where $\mathcal{W}_{n,l}(c) := \mathcal{W}(c) \cap (l + n\mathbb{Z})$ are those indices in the support set of $c(x)$ that are congruent to l modulo n, and $\mathcal{L}_n(c) := \{l : 0 \leq l < n, \mathcal{W}_{n,l}(c) \neq \emptyset\}$. Clearly, $(\mathcal{W}_{n,l})_{l \in \mathcal{L}_n(c)}$ is a partition of the set $\mathcal{W}(c)$. Hence,

$$\mathrm{wt}(c) = |\mathcal{W}(c)| = \sum_{l \in \mathcal{L}_n(c)} |\mathcal{W}_{n,l}(c)|.$$

Let $\mathcal{L}_n(c)$ be ordered such that $\mathcal{L}_n(c) = \{l_1, l_2, \ldots, l_{|\mathcal{L}_n(c)|}\}$, where $l_1 < l_2 < \cdots < l_{|\mathcal{L}_n(c)|}$. Define the *$n$-ary support profile* of $c(x)$ as

$$\boldsymbol{w}_n(c) := (|\mathcal{W}_{n,l_1}(c)|, |\mathcal{W}_{n,l_2}(c)|, \ldots, |\mathcal{W}_{n,l_{|\mathcal{L}_n(c)|}}(c)|).$$

Then $\boldsymbol{w}_n(c)$ is an ordered partition of $\mathrm{wt}(c)$. We count $\mathcal{B}_i'$ by counting subsets of $\mathcal{B}_i'$ corresponding to specific n-ary support profiles. Let $\mathcal{P}_i$ be the set of all ordered partitions of i, i.e., $\mathcal{P}_i := \left\{\boldsymbol{\delta} \in \mathbb{N}^* : \sum_j \delta_j = i\right\}$, where $\mathbb{N}^* = \bigcup_{j=1}^{\infty} \mathbb{N}^j$ is the set of vectors of natural numbers. For all $\boldsymbol{\delta} \in \mathcal{P}_i$, define

$$\mathcal{B}_{i,\boldsymbol{\delta}}' := \{c(x) : c(x) \in \mathcal{B}_i', \boldsymbol{w}_n(c) = \boldsymbol{\delta}\}.$$

Then $\{\mathcal{B}_{i,\boldsymbol{\delta}}'\}_{\boldsymbol{\delta} \in \mathcal{P}_i}$ is a set partition of $\mathcal{B}_i'$. Hence, for all i,

$$B_i' = \sum_{\boldsymbol{\delta} \in \mathcal{P}_i} |\mathcal{B}_{i,\boldsymbol{\delta}}'|. \tag{7}$$

We are now ready to give the formula for B_i'.

Lemma 7: Let $\phi_q(t)$, $t \geq 1$, be the number of solutions to $\sum_{j=1}^{t} x_j = 0$, such that $x_j \in \mathbb{F}_q$, $x_j \neq 0, \forall\, j$. Then

$$\phi_q(t) = \frac{q-1}{q}\Big((q-1)^{t-1} - (-1)^{t-1}\Big). \tag{8}$$

Proof: See Appendix C. □

Proposition 8: For all i,

$$B_i' = \sum_{\boldsymbol{\delta} \in \mathcal{P}_i} \sum_{j=0}^{|\boldsymbol{\delta}|} \binom{b}{j} \binom{n-b}{|\boldsymbol{\delta}|-j} \prod_{l=1}^{|\boldsymbol{\delta}|} \binom{a+1_{\{l \leq j\}}}{\delta_l} \phi_q(\delta_l) \tag{9}$$

where

$$1_{\{l \leq j\}} = \begin{cases} 1, & \text{if } l \leq j \\ 0, & \text{otherwise,} \end{cases}$$

$\phi_q(t)$ is as given in (8), and a and b are integers such that $n' = an + b$, $0 \leq b < n$.

Proof: Note that for all $c(x) = \sum_{j=0}^{n'-1} c_j x^j \in \mathbb{F}_q[x]$,

$$R_{x^n-1}[c(x)] = \sum_{l \in \mathcal{L}_n(c)} \left(\sum_{j \in \mathcal{W}_{n,l}(c)} c_j \right) x^l.$$

Therefore, codewords in $\mathcal{B}_{i,\boldsymbol{\delta}}'$ can be enumerated with the following process.

1) Choose $\mathcal{L}_n(c) \subseteq \{0, 1, \ldots, n-1\}$ such that $|\mathcal{L}_n(c)| = |\boldsymbol{\delta}|$.
2) For each $l \in \mathcal{L}_n(c)$, choose $\mathcal{W}_{n,l}(c) \subseteq \{0, 1, \ldots, n'-1\} \cap (l + n\mathbb{Z})$ such that $|\mathcal{W}_{n,l}(c)| = \delta_l$.
3) For each $\mathcal{W}_{n,l}(c)$, choose $c_j \in \mathbb{F}_q \setminus \{0\}$ for all $j \in \mathcal{W}_{n,l}(c)$, such that $\sum_{j \in \mathcal{W}_{n,l}(c)} c_j = 0$.

In step 2, δ_l numbers are chosen from $\{0, \ldots, a\}$ if $l \leq b$, and from $\{0, \ldots, a-1\}$ otherwise. In step 1, there are $\binom{b}{j}\binom{n-b}{|\boldsymbol{\delta}|-j}$ choices such that $\mathcal{L}_n(c)$ contains exactly j numbers that are no greater than b. For each such choice, there are $\prod_{l=1}^{j}\binom{a+1}{\delta_l}\prod_{l=j+1}^{|\boldsymbol{\delta}|}\binom{a}{\delta_l}$ choices in step 2, for each of which there are $\phi_q(\delta_l)$ choices in step 3. Summing over all possible values of j, and noting (7), we immediately obtain (9). □

Corollary 9: If $n \mid n'$, then for all i,

$$B_i' = \sum_{\boldsymbol{\delta} \in \mathcal{P}_i} \binom{n}{|\boldsymbol{\delta}|} \prod_{l=1}^{|\boldsymbol{\delta}|} \binom{n'/n}{\delta_l} \phi_q(\delta_l). \tag{10}$$

Remark : Note that in (7), and consequently (9) and (10), we have summed over all partitions of i. However, not all partitions of i are valid n-ary support profiles for codewords in $\mathcal{B}_i'$. For example, if $\boldsymbol{\delta} = \boldsymbol{w}_n(c)$ for some $c(x) \in \mathcal{B}_i'$, then by definition of the n-ary support profile, it must be true that $|\boldsymbol{\delta}| \leq n$, and $\delta_l \leq \lceil n'/n \rceil$ for all l. Further, since $x^n - 1 \mid c(x)$, we have $\delta_l \neq 1$ for all l. Therefore, it suffices to consider

$$\mathcal{P}_i(n', n) := \{\boldsymbol{\delta} \in \mathcal{P}_i : |\boldsymbol{\delta}| \leq n, 2 \leq \delta_l \leq \lceil n'/n \rceil,\ \forall\, l\}. \tag{11}$$

In all our formulas for calculation of B_i', $\mathcal{P}_i$ can be replaced by $\mathcal{P}_i(n', n)$.

We now show that $A_i' = B_i'$ for all $i < d$.

Proposition 10: For all $i < d$, $A_i' = B_i'$.

Proof: We show that $\mathcal{A}_i' = \mathcal{B}_i'$. By Lemma 4, $\mathcal{B}_i' \subseteq \mathcal{A}_i'$. To show $\mathcal{A}_i' \subseteq \mathcal{B}_i'$, note that if $c(x) \in \mathcal{A}_i'$, then $R_{x^n-1}[c(x)] \in \mathcal{C}$. On the other hand, $\mathrm{wt}(R_{x^n-1}[c(x)]) \leq \mathrm{wt}(c(x)) = i < d$, which implies that $R_{x^n-1}[c(x)] = 0$. □

For $i \geq d$, the next two propositions provide upper and lower bounds on A_i', respectively.

Proposition 11: For all $i \geq d$, A_i' satisfies the following upper bound:

$$A_i' \leq \begin{cases} \binom{n'}{i}(q-1)^{i-d+1} + B_i', & \text{if } d \leq i \leq \lceil n'/n \rceil (d-2) \\ \binom{n'}{i}(q-1)^{i-d+1}, & \text{if } i > \lceil n'/n \rceil (d-2). \end{cases} \tag{12}$$

Proof: Let $c(x)$ be a polynomial of weight i, denoted by $c(x) = \sum_{j=1}^{i} c_{k_j} x^{k_j}$, $c_{k_j} \neq 0, \forall\, j$. Recall that the generator polynomial of $\mathcal{C}$ has the form $g(x) = \prod_{l=0}^{d-2}(x - \omega^{s+l})$, where ω is a primitive nth root of unity in $\mathbb{F}_q$, and s is an integer. Hence, $c(x) \in \mathcal{A}_i'$ if and only if $c(\omega^{s+l}) = 0$, for all $0 \leq l \leq d-2$. This condition can be written as

$$(\,\tilde{c}_{k_1} \quad \tilde{c}_{k_2} \quad \ldots \quad \tilde{c}_{k_i}\,) \begin{pmatrix} 1 & \omega^{k_1} & \ldots & \omega^{(d-2)k_1} \\ 1 & \omega^{k_2} & \ldots & \omega^{(d-2)k_2} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \omega^{k_i} & \ldots & \omega^{(d-2)k_i} \end{pmatrix} = \mathbf{0} \tag{13}$$

where

$$\tilde{c}_{k_j} = c_{k_j}\omega^{sk_j}, \quad \text{for all } j.$$

Note that counting $(\,c_{k_1} \quad c_{k_2} \quad \ldots \quad c_{k_i}\,)$ is equivalent to counting $(\,\tilde{c}_{k_1} \quad \tilde{c}_{k_2} \quad \ldots \quad \tilde{c}_{k_i}\,)$.

Recall that $i = \sum_{l\in\mathcal{L}_n(c)} |\mathcal{W}_{n,l}(c)| \le |\mathcal{L}_n(c)|\lceil n'/n\rceil$. If $i > \lceil n'/n\rceil(d-2)$, then $|\mathcal{L}_n(c)| \ge d-1$, which implies that $\{\omega^{k_j}\}_{j=1}^{i}$ contains at least $d-1$ distinct values. Without loss of generality, assume $\omega^{k_1},\ldots,\omega^{k_{d-1}}$ are distinct. Rewrite (13) as

$$(\tilde{c}_{k_1} \quad \ldots \quad \tilde{c}_{k_{d-1}}) \begin{pmatrix} 1 & \omega^{k_1} & \ldots & \omega^{(d-2)k_1} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \omega^{k_{d-1}} & \ldots & \omega^{(d-2)k_{d-1}} \end{pmatrix} = -(\tilde{c}_{k_d} \quad \ldots \quad \tilde{c}_{k_i}) \begin{pmatrix} 1 & \omega^{k_d} & \ldots & \omega^{(d-2)k_d} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \omega^{k_i} & \ldots & \omega^{(d-2)k_i} \end{pmatrix}. \quad (14)$$

The matrix on the left is a Vandermonde matrix and hence is invertible. For all choices of $(\tilde{c}_{k_j})_{j=d}^{i}$ that are nonzero, $(\tilde{c}_{k_j})_{j=1}^{d-1}$ is uniquely determined. By enumerating all nonzero $(\tilde{c}_{k_j})_{j=d}^{i}$, we can enumerate all valid choices of $(\tilde{c}_{k_j})_{j=1}^{i}$ that satisfy (13), possibly more (since $(\tilde{c}_{k_j})_{j=1}^{d-1}$ so determined may contain zeros). Therefore, for each given choice of $\{k_j\}_{j=1}^{i}$, there are at most $(q-1)^{i-d+1}$ codewords of weight i. The total number of weight-i codewords is hence at most $\binom{n'}{i}(q-1)^{i-d+1}$.

On the other hand, if $d \le i \le \lceil n'/n\rceil(d-2)$, we break A_i' into two parts

$$A_i' = B_i' + |\mathcal{A}_i' \setminus \mathcal{B}_i'|.$$

By Lemma 4, any codeword $c(x)$ in $\mathcal{A}_i' \setminus \mathcal{B}_i'$ must satisfy $0 \ne R_{x^n-1}[c(x)] \in \mathcal{C}$. Therefore, $\mathrm{wt}(R_{x^n-1}[c(x)]) \ge d$, which implies that $\{\omega^{k_j}\}_{j=1}^{i}$ contains at least d distinct values. The reasoning for the first case now applies and we see that $|\mathcal{A}_i' \setminus \mathcal{B}_i'|$ is upper bounded by $\binom{n'}{i}(q-1)^{i-d+1}$. □

Proposition 12: For all $i \ge d$, A_i' satisfies the following lower bound:

$$A_i' \ge \begin{cases} K_i'(q-d)(q-1)^{i-d} + B_i', & \text{if } d \le i \le \lceil n'/n\rceil(d-1) \\ \binom{n'}{i}(q-d)(q-1)^{i-d}, & \text{if } i > \lceil n'/n\rceil(d-1) \end{cases} \quad (15)$$

where

$$K_i' = \sum_{j=0}^{i} \binom{b}{j}\binom{n-b}{i-j}(a+1)^j a^{i-j} \quad (16)$$

and a and b are such that $n' = an + b$, $0 \le b < n$.

Proof: Let $c(x)$ be a polynomial of weight i, denoted by $c(x) = \sum_{j=1}^{i} c_{k_j}x^{k_j}$, $c_{k_j} \ne 0, \forall\, j$. If $i > \lceil n'/n\rceil(d-1)$, then $|\mathcal{L}_n(c)| \ge d$, which implies that $\{\omega^{k_j}\}_{j=1}^{i}$ contains at least d distinct values. Without loss of generality, assume that $\omega^{k_1},\ldots,\omega^{k_d}$ are distinct. Following the notation used in the proof of Proposition 11, we rewrite (14) as

$$(\tilde{c}_{k_1} \quad \ldots \quad \tilde{c}_{k_{d-1}}) \begin{pmatrix} 1 & \omega^{k_1} & \ldots & \omega^{(d-2)k_1} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \omega^{k_{d-1}} & \ldots & \omega^{(d-2)k_{d-1}} \end{pmatrix} = -(\tilde{c}_{k_{d+1}} \quad \ldots \quad \tilde{c}_{k_i}) \begin{pmatrix} 1 & \omega^{k_{d+1}} & \ldots & \omega^{(d-2)k_{d+1}} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \omega^{k_i} & \ldots & \omega^{(d-2)k_i} \end{pmatrix} - \tilde{c}_{k_d}(1 \quad \omega^{k_d} \quad \ldots \quad \omega^{(d-2)k_d}). \quad (17)$$

Call the matrix on the left V and the one on the right W. Note that V is invertible, so we can write

$$\begin{aligned}(\tilde{c}_{k_1} \quad \ldots \quad \tilde{c}_{k_{d-1}}) &= -(\tilde{c}_{k_{d+1}} \quad \ldots \quad \tilde{c}_{k_i})WV^{-1} \\ &\quad - \tilde{c}_{k_d}(1 \quad \omega^{k_d} \quad \ldots \quad \omega^{(d-2)k_d})V^{-1} \\ &= \boldsymbol{r} + \tilde{c}_{k_d}\boldsymbol{v},\end{aligned}$$

where

$$\boldsymbol{r} = -(\tilde{c}_{k_{d+1}} \quad \ldots \quad \tilde{c}_{k_i})WV^{-1}$$

and

$$\boldsymbol{v} = -(1 \quad \omega^{k_d} \quad \ldots \quad \omega^{(d-2)k_d})V^{-1}.$$

We now show that for all choices of $(\tilde{c}_{k_j})_{j=d+1}^{i}$ that are nonzero, no matter what $\boldsymbol{r}$ comes out to be, we always have at least $q-d$ choices of $\tilde{c}_{k_d} \ne 0$ to make $c(x)$ a weight-i codeword, i.e., at least $q-d$ choices of $\tilde{c}_{k_d}$ such that the values $\{\tilde{c}_{k_j}\}_{j=1}^{d-1}$ determined from (17) are all nonzero.

First, we claim that $\boldsymbol{v}$ does not contain zero elements. Suppose otherwise, that for some $1 \le j \le d-1$, $v_j = 0$. By definition

$$\boldsymbol{v}V = -(1 \quad \omega^{k_d} \quad \ldots \quad \omega^{(d-2)k_d}). \quad (18)$$

Since $v_j = 0$, we can ignore the jth row in V and rearrange (18) as

$$(v_1 \quad \ldots \quad v_{j-1} \quad v_{j+1} \quad \ldots \quad v_{d-1} \quad 1) \times \begin{pmatrix} 1 & \omega^{k_1} & \ldots & \omega^{(d-2)k_1} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \omega^{k_{j-1}} & \ldots & \omega^{(d-2)k_{j-1}} \\ 1 & \omega^{k_{j+1}} & \ldots & \omega^{(d-2)k_{j+1}} \\ \vdots & \vdots & \ldots & \vdots \\ 1 & \omega^{k_d} & \ldots & \omega^{(d-2)k_d} \end{pmatrix} = \mathbf{0}.$$

Note that since $\{\omega^{k_j}\}_{j=1}^{d}$ are all distinct, the matrix on the left is invertible, which implies that $(v_1 \quad \ldots \quad v_{j-1} \quad v_{j+1} \quad \ldots \quad v_{d-1} \quad 1) = \mathbf{0}$, a contradiction.

Now, since $v_j \ne 0$ for all $1 \le j \le d-1$, for any given j, there is at most one nonzero value that $\tilde{c}_{k_d}$ can take such that $r_j + \tilde{c}_{k_d}v_j = 0$. Therefore, there are at least $(q-1)-(d-1) = q-d$ nonzero values that $\tilde{c}_{k_d}$ can take such that $\tilde{c}_{k_j} = r_j + \tilde{c}_{k_d}v_j \ne 0$ for all j. Thus, for any given $\{k_j\}_{j=1}^{i}$, there are at least $(q-1)^{i-d}(q-d)$ codewords of weight i. So the total number of weight-i codewords is at least $\binom{n'}{i}(q-1)^{i-d}(q-d)$.

If $d \le i \le \lceil n'/n\rceil(d-1)$, we break A_i' into two parts

$$A_i' = B_i' + |\mathcal{A}_i' \setminus \mathcal{B}_i'|.$$

Consider the subset of codewords in $\mathcal{A}_i'$ whose n-ary support profile is the all-ones vector, i.e., $\boldsymbol{w}_n(c) = (1,\ldots,1)$. All these codewords must be contained in $\mathcal{A}_i' \setminus \mathcal{B}_i'$, as codewords in $\mathcal{B}_i'$ have n-ary support profiles whose elements are no less than 2. There are

$$K_i' = \sum_{j=0}^{i} \binom{b}{j}\binom{n-b}{i-j}(a+1)^j a^{i-j}$$

choices of $\{k_j\}_{j=1}^{i}$ (i.e., $\mathcal{W}(c)$) corresponding to the all-ones support profile and they all satisfy $|\mathcal{L}_n(c)| = i \ge d$. Therefore, the reasoning

of the first case applies and we see that the number of codewords in $\mathcal{A}_i' \setminus \mathcal{B}_i'$ is at least $K_i'(q-d)(q-1)^{i-d}$. □

III. Probability of Undetected Error

First, note that any term in (1) is a lower bound on $P_{ud}(p)$. In particular, for a code with length n and minimum distance d, we have

$$P_{ud}(p) \geq A_d \left(\frac{p}{q-1}\right)^d (1-p)^{n-d}.$$

This bound is interesting because for any given code, it is the dominant term in the sum as $p \to 0$. From Proposition 1, we immediately obtain the following result.

Proposition 13: If $d > 2$, then

$$P_{ud}(p) \geq P_{ud}^{(2)}(p)$$

where

$$P_{ud}^{(2)}(p) = \left(\binom{a}{2} + \frac{ab}{q-1}\right) p^2 (1-p)^{n'-2} \tag{19}$$

and a and b are integers such that $n' = a(q-1)+b$, $0 \leq b < q-1$.

Note that

$$\max_{0\leq p\leq 1} P_{ud}^{(2)}(p) = \left(\binom{a}{2} + \frac{ab}{q-1}\right) \left(\frac{2}{n'}\right)^2 \left(1 - \frac{2}{n'}\right)^{n'-2}$$

which we denote by $P_{\max}^{(2)}$. In many cases, we have $P_{\max}^{(2)} > q^{-(d-1)}$, which implies that the corresponding OERS codes are not good. For example, if n'/n is fixed, then as $q \to \infty$, $P_{\max}^{(2)} \sim Cq^{-2}$,[1] where C is a constant that depends only on n'/n. Therefore, for all $d > 3$ and $q > 1/C$, the corresponding OERS codes are not good. The intuition here is that the number of weight-2 codewords in an OERS code does *not* depend on the number of parity-check symbols ($d-1$ in this case). While P_{ud}^{avg} is expected to decrease exponentially with d, $P_{\max}^{(2)}$ is not affected. For practical values of q, $P_{\max}^{(2)}$ can be orders of magnitude larger than $q^{-(d-1)}$, even when d is just moderately larger than 3.

Next, better bounds can be obtained by simply plugging the results of Proposition 10, Proposition 12, and Proposition 11 into (1).

Proposition 14: For OERS codes

$$\underline{P}_{ud}(p) \leq P_{ud}(p) \leq \overline{P}_{ud}(p)$$

where

$$\begin{aligned}\underline{P}_{ud}(p) = &\sum_{i=1}^{\lceil \frac{n'}{n} \rceil (d-1)} B_i' \left(\frac{p}{q-1}\right)^i (1-p)^{n'-i} \\ &+ \frac{q-d}{(q-1)^d}\left(1 - \sum_{i=0}^{\lceil \frac{n'}{n} \rceil (d-1)} \binom{n'}{i} p^i (1-p)^{n'-i}\right) \\ &+ \frac{q-d}{(q-1)^d} \sum_{i=d}^{\lceil \frac{n'}{n} \rceil (d-1)} K_i' p^i (1-p)^{n'-i}\end{aligned} \tag{20}$$

and

$$\begin{aligned}\overline{P}_{ud}(p) = &\sum_{i=1}^{\lceil \frac{n'}{n} \rceil (d-2)} B_i' \left(\frac{p}{q-1}\right)^i (1-p)^{n'-i} \\ &+ \frac{1}{(q-1)^{d-1}}\left(1 - \sum_{i=0}^{d-1} \binom{n'}{i} p^i (1-p)^{n'-i}\right),\end{aligned} \tag{21}$$

where B_i' is given by (9), and K_i' by (16).

[1]We adopt the standard asymptotic notations that can be found in, for example, [14]

The worst case probability of undetected error, $P_{ud}^{\max} := \max_{0\leq p\leq 1} P_{ud}(p)$, is then bounded between the maximum values of the upper and lower bounds.

Corollary 15: For OERS codes

$$\underline{P}_{ud}^{\max} \leq P_{ud}^{\max} \leq \overline{P}_{ud}^{\max}$$

where

$$\underline{P}_{ud}^{\max} := \max_{0\leq p\leq 1} \underline{P}_{ud}(p) \quad \text{and} \quad \overline{P}_{ud}^{\max} := \max_{0\leq p\leq 1} \overline{P}_{ud}(p).$$

We now discuss the tightness of the bounds that we have derived. First, we show that the bounds given by Proposition 14 are asymptotically tight for all p as $q \to \infty$.

Lemma 16: Let n'/n be fixed. For any fixed i, as $q \to \infty$,

$$K_i' \sim \binom{n'}{i} \tag{22}$$

where K_i' is as defined in (16).

Proof: See Appendix D. □

Proposition 17: Let n'/n and d be fixed. Then for all $0 < p \leq 1$, as $q \to \infty$,

$$\underline{P}_{ud}(p) \sim P_{ud}(p) \sim \overline{P}_{ud}(p). \tag{23}$$

Proof: It suffices to show that $\overline{P}_{ud}(p) - \underline{P}_{ud}(p) = o(\overline{P}_{ud}(p))$. First, note that $\overline{P}_{ud}(p)$ can be rewritten as

$$\overline{P}_{ud}(p) = \sum_{i=1}^{\lceil \frac{n'}{n} \rceil (d-2)} B_i' \left(\frac{p}{q-1}\right)^i (1-p)^{n'-i} + P_1(p) + P_2(p)$$

where

$$P_1(p) = \frac{1}{(q-1)^{d-1}}\left(1 - \sum_{i=0}^{\lceil \frac{n'}{n} \rceil (d-1)} \binom{n'}{i} p^i (1-p)^{n'-i}\right)$$

and

$$P_2(p) = \frac{1}{(q-1)^{d-1}} \sum_{i=d}^{\lceil \frac{n'}{n} \rceil (d-1)} \binom{n'}{i} p^i (1-p)^{n'-i}.$$

Next, from the expressions above and (20), it is easy to show that

$$\overline{P}_{ud}(p) - \underline{P}_{ud}(p) \leq \Delta_1(p) + \Delta_2(p)$$

where

$$\Delta_1(p) = \frac{d-1}{(q-1)^d}\left(1 - \sum_{i=0}^{\lceil \frac{n'}{n} \rceil (d-1)} \binom{n'}{i} p^i (1-p)^{n'-i}\right)$$

and

$$\Delta_2(p) = \frac{1}{(q-1)^{d-1}} \sum_{i=d}^{\lceil \frac{n'}{n} \rceil (d-1)} \left(\binom{n'}{i} - \frac{q-d}{q-1} K_i'\right) p^i (1-p)^{n'-i}.$$

Finally, note that $\Delta_1(p) = o(P_1(p))$. And by Lemma 16, $\Delta_2(p) = o(P_2(p))$. Therefore, $\overline{P}_{ud}(p) - \underline{P}_{ud}(p) = o(\overline{P}_{ud}(p))$.

Since the result of Proposition 17 holds for all $p \in (0, 1]$, it follows that $\underline{P}_{ud}^{\max}$ and $\overline{P}_{ud}^{\max}$ are also tight bounds for $P_{ud}^{\max}$.

Corollary 18: Let n'/n and d be fixed. Then for all $0 < p \leq 1$, as $q \to \infty$,

$$\underline{P}_{ud}^{\max} \sim P_{ud}^{\max} \sim \overline{P}_{ud}^{\max}.$$

We now show that in many cases, $P_{ud}^{\max}$ consists predominantly of the contribution from weight-2 codewords.

Lemma 19: Let n'/n be fixed. For any fixed i, as $q \to \infty$,

$$B_i' = O(q^i). \tag{24}$$

Proof:: See Appendix E. □

Proposition 20: Let n'/n and d, $d > 3$, be fixed. As $q \to \infty$,

$$P_{\max}^{(2)} \sim P_{ud}^{\max}.$$

Proof: Since $P_{\max}^{(2)} \leq P_{ud}^{\max} \leq \overline{P}_{ud}^{\max}$, it suffices to show that $P_{\max}^{(2)} \sim \overline{P}_{ud}^{\max}$. Note that

$$\begin{aligned}
&\overline{P}_{ud}^{\max} - P_{\max}^{(2)} \\
&\quad = \max_p \overline{P}_{ud}(p) - \max_p P_{ud}^{(2)}(p) \\
&\quad \leq \max_p \left\{ \overline{P}_{ud}(p) - P_{ud}^{(2)}(p) \right\} \\
&\quad = \max_p \left\{ \sum_{i=3}^{\left\lceil \frac{n'}{n} \right\rceil (d-2)} B_i' \left(\frac{p}{q-1} \right)^i (1-p)^{n'-i} \right. \\
&\qquad \left. + \frac{1}{(q-1)^{d-1}} \left(1 - \sum_{i=0}^{d-1} \binom{n'}{i} p^i (1-p)^{n'-i} \right) \right\} \\
&\quad \leq \sum_{i=3}^{\left\lceil \frac{n'}{n} \right\rceil (d-2)} \max_p \left\{ B_i' \left(\frac{p}{q-1} \right)^i (1-p)^{n'-i} \right\} + \frac{1}{(q-1)^{d-1}} \\
&\quad = \sum_{i=3}^{\left\lceil \frac{n'}{n} \right\rceil (d-2)} \frac{B_i'}{(q-1)^i} \left(\frac{i}{q-1} \right)^i \left(1 - \frac{i}{q-1} \right)^{n'-i} + \frac{1}{(q-1)^{d-1}} \\
&\quad = \sum_{i=3}^{\left\lceil \frac{n'}{n} \right\rceil (d-2)} O(q^{-i}) + O(q^{-(d-1)}) \\
&\quad = O(q^{-3}).
\end{aligned}$$

Recall that in the discussion following Proposition 13, we have shown that for this case $P_{\max}^{(2)} = \Theta(q^{-2})$. Therefore, $\overline{P}_{ud}^{\max} - P_{\max}^{(2)} = o\left(P_{\max}^{(2)}\right)$, implying $P_{\max}^{(2)} \sim P_{ud}^{\max}$. □

We should note that since RS codes are usually used with relatively short block lengths, the asymptotic analysis might not seem very useful. However, it is clear from the proofs that as long as $n' \gg \lceil \frac{n'}{n} \rceil (d-1)$, i.e., $n \gg d-1$, the actual behavior of the code should be well approximated by the asymptotic analysis. In applications such as data storage, where high rate codes are commonly used, this condition is usually satisfied.

The asymptotic results can also be used to simplify the bounds. For example, from Lemma 16 and Lemma 19, we see that in the lower bound of (15), B_i' is negligibly small and can be safely ignored. This would reduce the number of B_i''s that need be calculated in the lower bound of (20).

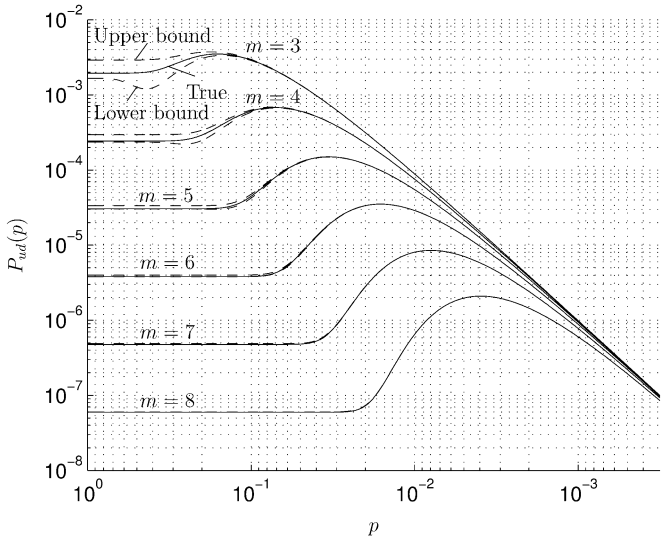

Fig. 1. Upper and lower bounds on $P_{ud}(p)$ for $(2^{m+1}-2, 2^{m+1}-5)$ OERS codes over $\mathbb{F}_{2^m}$.

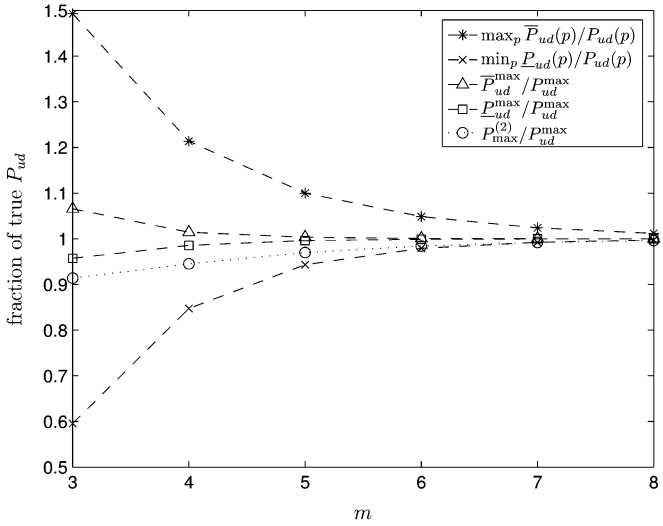

Fig. 2. Convergence of P_{ud} bounds for $(2^{m+1}-2, 2^{m+1}-5)$ OERS codes over $\mathbb{F}_{2^m}$.

We end our discussion with an example. Let $\mathcal{C}'$ be an OERS code obtained by doubling the code length of $\mathcal{C}$, a RS code over $\mathbb{F}_{2^m}$ with minimum distance $d = 4$. Fig. 1 plots $\underline{P}_{ud}(p)$ and $\overline{P}_{ud}(p)$ together with the true $P_{ud}(p)$ for various values of m. Fig. 2 shows more explicitly how the upper and lower bounds converge to the true probability as m increases. The true $P_{ud}(p)$ values are obtained through (2), where the weight distribution of the dual code of $\mathcal{C}'$ is found through enumeration of codewords. It should be noted that this brute-force procedure is only possible when d is small (so that the dual code is of low dimension). Even for $d = 4$, as in our case, for $m > 6$, the enumeration becomes a rather long process.

From the figures, we see that our upper and lower bounds are very tight, except for very small values of m. As the field size increases, the bounds converge to the true probability of undetected error very quickly. This is especially true for the bounds on $P_{ud}^{\max}$. Even $P_{\max}^{(2)}$ converges rather fast. The numerical values of bounds on $P_{ud}^{\max}$ are shown in Table I. Also, from Fig. 1, we note that when p is small, both bounds are tight regardless of the field size. This is expected because,

TABLE I
BOUNDS ON $P_{ud}^{\max}$ FOR $(2^{m+1}-2, 2^{m+1}-5)$OERS CODES OVER $\mathbb{F}_{2^m}$

	$P_{ud}^{\max}$	$\underline{P}_{ud}^{\max}$	$\overline{P}_{ud}^{\max}$	$P_{\max}^{(2)}$
$m=3$	3.5120e-03	3.3622e-03	3.7427e-03	3.2095e-03
$m=4$	6.8138e-04	6.7156e-04	6.9102e-04	6.4394e-04
$m=5$	1.5004e-04	1.4946e-04	1.5054e-04	1.4550e-04
$m=6$	3.5204e-05	3.5170e-05	3.5232e-05	3.4647e-05
$m=7$	8.5262e-06	8.5241e-06	8.5279e-06	8.4573e-06
$m=8$	2.0980e-06	2.0979e-06	2.0981e-06	2.0895e-06

as $p \to 0$, both bounds consist predominantly of $P_{ud}^{(2)}(p)$, which is asymptotically p^2.

IV. CONCLUSION

OERS codes are of practical interest as they have been used in data storage systems. In this work, we have examined their performance in terms of probability of undetected error when the codes are used solely for error detection over a q-ary symmetric channel. We have obtained upper and lower bounds on $P_{ud}(p)$, which have been shown to be asymptotically tight. The bounds are also relatively easy to evaluate for high rate codes, which are commonly used in storage systems.

Our bounds on the probability of undetected error have been derived by bounding the weight distribution of the code. The techniques involved in obtaining the weight distribution bounds can potentially be applied to the study of other RS- or BCH-derived codes.

APPENDIX
ADDITIONAL PROOFS

A. Proof of Proposition 1

If $d>2$, we show that every $c(x) \in \mathcal{A}_2'$ is of the form $\alpha(x^i - x^j)$, where $i \equiv j \mod n$. Clearly, if $c(x)=\alpha(x^i-x^j)$ and $i \equiv j \mod n$, then $g(x) \mid x^n-1 \mid c(x)$; hence $c(x) \in \mathcal{A}_2'$. On the other hand, if $c(x)=\alpha x^i+\beta x^j \in \mathcal{A}_2'$, then $g(x) \mid c(x)$. For $d>2$, $(x-\omega^s)(x-\omega^{s+1}) \mid g(x)$ for some primitive nth root of unity $\omega \in \mathbb{F}_q$ and some integer s. Hence, $c(\omega^s)=c(\omega^{s+1})=0$, from which it is easy to show that $\omega^i=\omega^j$ (hence $i \equiv j \mod n$) and $\alpha+\beta=0$. Now, note that $\mathcal{A}_2'$ can be written as the following union of disjoint subsets

$$\mathcal{A}_2' = \bigcup_{j=1}^{a} \Big\{ \alpha(x^{jn+i}-x^i) : \alpha \in \mathbb{F}_q \setminus \{0\}, \; i = 0,1,\ldots,\max\{n'-jn-1, b-1\} \Big\}.$$

The result follows from simple counting.

If $d=2$, then $g(x)=x-\omega^s$. A weight-2 polynomial $c(x)=\alpha x^i+\beta x^j \in \mathbb{F}_q[x]$ is a codeword if and only if $c(\omega^s)=0$, that is, if and only if $\beta=-\alpha\omega^{s(i-j)}$. So the number of weight-2 codewords is simply the number of $\{i,j\}$ pairs times the number of nonzero choices of α.

If $d=1$, any polynomial in $\mathbb{F}_q[x]$ that has degree less than n' is a codeword. Hence, $A_2'=\binom{n'}{2}(q-1)^2$. □

B. Proof of Proposition 3

For $d>3$, the proof is similar in spirit to the first part of the proof of Proposition 1, and the result is a specialization of Proposition 8 and Proposition 10. Details of the proof are thus omitted. Essentially, we show that every $c(x) \in \mathcal{A}_3'$ has the form $\alpha x^i+\beta x^j+\gamma x^l$, such that $\alpha+\beta+\gamma=0$ and $i \equiv j \equiv l \mod n$.

If $d=3$, then $g(x)=(x-\omega^s)(x-\omega^{s+1})$ for some primitive nth root of unity $\omega \in \mathbb{F}_q$ and some integer s. A weight-3 polynomial $c(x)=\alpha x^i+\beta x^j+\gamma x^l \in \mathbb{F}_q[x]$ is a codeword if and only if $c(\omega^s)=c(\omega^{s+1})=0$, i.e.,

$$(\alpha \quad \beta \quad \gamma)\begin{pmatrix} \omega^{si} & \omega^{(s+1)i} \\ \omega^{sj} & \omega^{(s+1)j} \\ \omega^{sl} & \omega^{(s+1)l} \end{pmatrix} = \mathbf{0}. \tag{25}$$

If $i \equiv j \equiv l \mod n$, the equation above is satisfied if and only if $\alpha+\beta+\gamma=0$. This corresponds to $\left(\binom{a}{3}(q-1)+\binom{a}{2}b\right)(q-1)(q-2)$ weight-3 codewords as has been calculated for $d>3$. Otherwise, without loss of generality, suppose $i \not\equiv j \mod n$ so that $\omega^i \neq \omega^j$. From the fact that $\alpha,\beta,\gamma \neq 0$, it is easy to show that it must also be true that $j \not\equiv l \mod n$ and $l \not\equiv i \mod n$. This implies that if $\{i,j,l\}$ is chosen, we can fix any nonzero value for γ and (α,β) will be uniquely determined. From the inclusion-exclusion principle, we see that the number of $\{i,j,l\}$'s such that no two of the numbers are congruent modulo n is $\binom{n'}{3} - \binom{n'-2}{1}\left[\binom{a}{2}(q-1)+ab\right]+2\left[\binom{a}{3}(q-1)+\binom{a}{2}b\right]$. The result now follows after some algebra.

If $d=2$, then $g(x)=x-\omega^s$. We have $c(x)=\alpha x^i+\beta x^j+\gamma x^l \in \mathbb{F}_q[x]$ is a codeword if and only if $c(\omega^s)=0$, which is true if and only if $\gamma=-\alpha\omega^{s(i-l)}-\beta\omega^{s(j-l)}$. There are $\binom{n'}{3}$ choices of $\{i,j,l\}$, for each of which there are $(q-1)$ choices of $\alpha \neq 0$ and subsequently $(q-2)$ choices of $\beta \neq 0$ and $\beta \neq -\alpha\omega^{s(i-j)}$. Therefore, $A_3'=\binom{n'}{3}(q-1)(q-2)$.

If $d=1$, any polynomial in $\mathbb{F}_q[x]$ that has degree less than n' is a codeword. Hence, $A_3'=\binom{n'}{3}(q-1)^3$. □

C. Proof of Lemma 7

Clearly, $\phi_q(1)=0$. For $t \geq 2$, note that to satisfy the equation we must have $x_t=-\sum_{j=1}^{t-1}x_j$. So x_t is determined if $(x_j)_{j=1}^{t-1}$ are chosen. Among the $(q-1)^{t-1}$ choices of $(x_j)_{j=1}^{t-1}$ that are nonzero, a choice is a valid solution if and only if $\sum_{j=1}^{t-1}x_j \neq 0$. By definition the number of such choices is $\phi_q(t)$. On the other hand, also by definition, the number of choices corresponding to $\sum_{j=1}^{t-1}x_j=0$ is $\phi_q(t-1)$. Therefore,

$$\phi_q(t)+\phi_q(t-1)=(q-1)^{t-1}, \quad \forall\, t \geq 2. \tag{26}$$

Consider the sequence of equations

$$\begin{aligned} \phi_q(2) &= q-1, \\ \phi_q(3)+\phi_q(2) &= (q-1)^2, \\ &\vdots \\ \phi_q(t)+\phi_q(t-1) &= (q-1)^{t-1}. \end{aligned}$$

Multiplying the equation corresponding to $(q-1)^{t-1-j}$ by $(-1)^j$ and summing up, we obtain

$$\begin{aligned} \phi_q(t) &= \sum_{j=0}^{t-2}(-1)^j(q-1)^{t-1-j} \\ &= (q-1)^{t-1}\sum_{j=0}^{t-2}\left(\frac{-1}{q-1}\right)^j \\ &= \frac{q-1}{q}\left((q-1)^{t-1}-(-1)^{t-1}\right), \quad \forall\, t \geq 2. \end{aligned}$$

It is readily verified that the expression above also holds for $t=1$. □

D. Proof of Lemma 16

Let $n' = an + b$, where a, b are integers such that $0 \le b < n$. Note that for all fixed α and i, as $n \to \infty$

$$\binom{n}{i}\alpha^i \sim \binom{\alpha n}{i}. \tag{27}$$

If $b = 0$, we have

$$K_i' = \binom{n}{i}a^i \sim \binom{an}{i} = \binom{n'}{i}.$$

If $b \neq 0$, then $b, n-b \to \infty$ as $n \to \infty$. Hence, we have

$$\begin{aligned} K_i' &= \sum_{j=0}^{i}\binom{b}{j}\binom{n-b}{i-j}(a+1)^j a^{i-j} \\ &\sim \sum_{j=0}^{i}\binom{(a+1)b}{j}\binom{a(n-b)}{i-j} \\ &= \sum_{j=0}^{i}\binom{(a+1)b}{j}\binom{n'-(a+1)b}{i-j} \\ &= \binom{n'}{i}. \end{aligned}$$

□

E. Proof of Lemma 19

We have

$$\begin{aligned} B_i' &\le \sum_{\boldsymbol{\delta}\in\mathcal{P}_i(n',n)}\binom{n}{|\boldsymbol{\delta}|}\prod_{l=1}^{|\boldsymbol{\delta}|}\binom{\lceil\frac{n'}{n}\rceil}{\delta_l}\phi_q(\delta_l) \\ &\sim \sum_{\boldsymbol{\delta}\in\mathcal{P}_i(n',n)}\frac{q^{|\boldsymbol{\delta}|}}{|\boldsymbol{\delta}|!}\prod_{l=1}^{|\boldsymbol{\delta}|}\binom{\lceil\frac{n'}{n}\rceil}{\delta_l}\prod_{l=1}^{|\boldsymbol{\delta}|}q^{\delta_l-1} \\ &= \sum_{\boldsymbol{\delta}\in\mathcal{P}_i(n',n)}\frac{q^{|\boldsymbol{\delta}|}}{|\boldsymbol{\delta}|!}\left(\prod_{l=1}^{|\boldsymbol{\delta}|}\binom{\lceil\frac{n'}{n}\rceil}{\delta_l}\right)q^{i-|\boldsymbol{\delta}|} \\ &= q^i\sum_{\boldsymbol{\delta}\in\mathcal{P}_i(n',n)}\frac{1}{|\boldsymbol{\delta}|!}\prod_{l=1}^{|\boldsymbol{\delta}|}\binom{\lceil\frac{n'}{n}\rceil}{\delta_l} \\ &\le q^i\sum_{\boldsymbol{\delta}\in\mathcal{P}_i}\frac{1}{|\boldsymbol{\delta}|!}\prod_{l=1}^{|\boldsymbol{\delta}|}\binom{\lceil\frac{n'}{n}\rceil}{\delta_l} \\ &= O(q^i) \end{aligned}$$

□

ACKNOWLEDGMENT

The authors wish to express their appreciation to the anonymous reviewers whose comments and suggestions greatly improved this correspondence.

REFERENCES

[1] J. K. Wolf and R. D. Blakeney, II, "An exact evaluation of the probability of undetected error for certain shortened binary CRC codes," in *Proc. MILCOM 88*, Oct. 1988, pp. 287–292.

[2] Universal Serial Bus Specification 2000, Revision 2.

[3] ATA 6 Specification Document Number T13/1410D, Revision 3B.

[4] F. J. M. Williams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, vol. 42, pp. 79–94, Jan. 1963.

[5] S.-C. Chang and J. K. Wolf, "A simple derivation of the MacWilliams identity for linear codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 476–477, Jul. 1980.

[6] S. K. Leung-Yan-Cheong and M. E. Hellman, "Concerning a bound on undetected error probability," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 235–237, Mar. 1976.

[7] S. K. Leung-Yan-Cheong, E. R. Barnes, and D. U. Friedman, "On some properties of the undetected error probability of linear codes," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 110–112, Jan. 1979.

[8] J. K. Wolf, A. M. Michelson, and A. H. Levesque, "On the probability of undetected error for linear block codes," *IEEE Trans. Commun.*, vol. COM-30, pp. 317–324, Feb. 1982.

[9] T. Fujiwara, T. Kasami, A. Kitai, and S. Lin, "On the undetected error probability for shortened hamming codes," *IEEE Trans. Commun.*, vol. COM-33, pp. 570–574, Jun. 1985.

[10] T. Kasami, T. Kløve, and S. Lin, "Linear block codes for error detection," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 131–136, Jan. 1983.

[11] T. Kasami and S. Lin, "On the probability of undetected error for the maximum distance separable codes," *IEEE Trans. Commun.*, vol. COM-32, pp. 998–1006, Sep. 1984.

[12] T. Kløve and V. I. Korzhik, *Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems*. Boston, MA: Kluwer, 1995.

[13] J. Massey, "Coding techniques for digital networks," in *Proc. International Conference on Information Theory Systems*, Berlin, Germany, Sep. 1978, pp. 307–315.

[14] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, 2nd ed. Reading, MA: Addison-Wesley, 1994.

On Construction of the $(24, 12, 8)$ Golay Codes

Xiao-Hong Peng, *Member, IEEE*, and
Paddy G. Farrell, *Life Fellow, IEEE*

***Abstract*—Two product array codes are used to construct the $(24, 12, 8)$ binary Golay code through the direct sum operation. This construction provides a systematic way to find proper $(8, 4, 4)$ linear block component codes for generating the Golay code, and it generates and extends previously existing methods that use a similar construction framework. The code constructed is simple to decode.**

***Index Terms*—Array codes, block codes, code construction, direct sum, Golay codes.**

I. INTRODUCTION

The $(24, 12, 8)$ binary block code, denoted by C_{24}, was originally constructed by extending the $(23, 12, 7)$ Golay code [1], a unique 3-error correcting perfect code. Because of the optimality and attractive structure of C_{24} which is *self dual* and *doubly even* [2], it has received considerable attention, leading to a large number

Manuscript received January 19, 2005; revised December 15, 2005.

X.-H. Peng is with the Electronic Engineering Subject Group, School of Engineering & Applied Science, Aston University, Birmingham B4 7ET, U.K. (e-mail: x-h.peng@aston.ac.uk).

P. G. Farrell is Visiting Professor in the Department of Communication Systems, Lancaster University, Lancaster LA1 4WA, U.K. He is at 7 The Drive, Deal, Kent, CT14 9AE, U.K. (e-mail: Paddy.Farrell@virgin.net).

Communicated by R. J. McEliece, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2006.876247