

# PERFORMANCE COMPARISON OF HERMITIAN AND REED-SOLOMON CODES

Bruce E. Wahlen

Naval Command, Control and Ocean Surveillance Center (NCCOSC)  
RDT&E Division (NRaD)  
San Diego, CA 92152

Jesús Jiménez

Point Loma Nazarene College  
Department of Mathematics and Computer Science  
San Diego, CA 92106

## ABSTRACT

This paper compares the performance of low and high-rate Reed-Solomon codes with Hermitian codes, that is, algebraic-geometric codes based on Hermitian curves, over fields containing 16, 64, 256, 512, and 4096 elements. Comparisons of Reed-Solomon codes with much longer Hermitian codes over the same field demonstrate the utility of Hermitian codes with respect to the trade-off between coding gain and bandwidth expansion. Comparisons of Reed-Solomon and Hermitian codes of the same length, but over different fields, show an increasingly favorable trade-off between bandwidth expansion and complexity of finite-field arithmetic computations as code length increases.

## 1 INTRODUCTION

Error control coding is an important means of improving the performance of modern digital communications systems. In particular, Reed-Solomon (RS) codes have a number of desirable characteristics which have made them quite useful, such as a non-binary alphabet that provides significant burst-error-correcting capability when used alone or as an outer block code concatenated with an inner convolutional code. Such concatenated systems, which may also employ interleaving and soft-decision Viterbi decoding, are used in a variety of applications, including: the deep-space exploration systems of the National Aeronautics and Space Administration and the European Space Agency, where power savings is the main concern [1]; and the satellite systems of both the International Telecommunications Satellite Organization (INTELSAT) and the European Telecommunications Satellite Organization (EUTELSAT). In addition, similar concatenated systems have been considered for the transmission layer of the digital television system defined by the Moving Pictures Expert Group [1], and such systems could be effective in mitigating certain types of pulsed interference.

The performance of concatenated systems could be im-

proved by improving the performance of the outer block code. Performance of a block code, measured in terms of probability of decoding error, or coding gain, can be improved by increasing the code word length relative to the size of the chosen code word alphabet. One of the undesirable restrictions of RS codes is that code word lengths are limited to the size of the alphabet. For this reason RS codes have been generalized by Goppa [2] as algebraic-geometric (AG) codes, which allow code word lengths to be much longer than the size of the alphabet.

In this paper we compare the performance of RS codes to AG codes with much longer code words. Section 2 contains some coding theory and mathematics background material; section 3 provides a definition of AG codes; section 4 describes the methods used to compare the performance of RS and AG codes; section 5 presents the results of the comparisons; and section 6 contains our discussion and conclusions.

## 2 CODING AND MATHEMATICS BACKGROUND

All codes in this paper are defined over the symbol alphabet  $\mathbb{F}_q$ , the finite field containing  $q$  elements. Both RS and AG codes are examples of linear block codes of information word length  $k$  and code word length  $n$ . For the standard definitions of a linear block code, code rate, Hamming distance, and minimum distance  $d$ , we refer the reader to van Lint [3]; for the original definition of RS codes see Reed and Solomon [4]. Definitions necessary to describe AG codes follow.

A *homogeneous polynomial* is a polynomial such that each of its terms has the same degree; a *rational function* is the quotient of two homogeneous polynomials of the same degree. A *projective plane curve* is defined as the set of zeros of a homogeneous polynomial. The complexity of a curve is measured by a non-negative integer,  $g$ , called the *genus*, which increases with the curve's complexity. The genus of a non-singular projective plane curve of degree  $l$  is given by Plücker's formula as  $g = (l - 1)(l - 2)/2$ .

Given a projective curve  $X$  over  $\mathbb{F}_q$ , a point  $P$  is *rational* if all its coordinates are in  $\mathbb{F}_q$ . A *divisor* on  $X$  is defined to be a formal sum  $D = \sum_{P \in X} n_P P$ , where the coefficients  $n_P$  are integers of which only finitely many are non-zero. Divisors may be added term-by-term. The *degree* of a divisor  $D$  is  $\deg(D) = \sum_{P \in X} n_P$ , and the support of  $D$  is  $\{P \in X | n_P \neq 0\}$ . A divisor  $D$  is called *effective*, denoted  $D \succeq 0$ , if all of its coefficients are non-negative, and given two divisors,  $D_1$  and  $D_2$  on  $X$ , we write  $D_1 \succeq D_2$  if  $D_1 - D_2 \succeq 0$ . For a rational function  $f$ , we define the divisor of  $f$  to be  $(f) = \sum_{P \in X} \nu_P(f) P$ , where  $\nu_P$  is a function which gives the order of the pole or zero of  $f$  at the point  $P \in X$ . If  $\nu_P(f) = n_P > 0$ ,  $f$  is said to have a *zero of order*  $n_P$  at  $P$ , and if  $\nu_P(f) = n_P < 0$ ,  $f$  is said to have a *pole of order*  $-n_P$  at  $P$ . In essence,  $(f)$  performs an accounting function by keeping track of the zeros and poles of  $f$  and their orders.

For every divisor  $D$  on  $X$  we define the vector space  $\mathcal{L}(D)$  over  $\mathbb{F}_q$  of rational functions as

$$\mathcal{L}(D) = \{f \in \mathbb{F}_q(X) | (f) \succeq -D \text{ or } f = 0\},$$

where  $\mathbb{F}_q(X)$  is the field of rational functions on  $X$ .  $\mathcal{L}(D)$  is a finite-dimensional vector space, and by the Riemann-Roch theorem it has dimension,  $\dim(\mathcal{L}(D))$ , satisfying the inequality,  $\dim(\mathcal{L}(D)) \geq \deg(D) + 1 - g$ . Furthermore, if

$$D = \sum_{i=1}^r n_i P_i - \sum_{j=1}^s m_j Q_j,$$

with  $n_i > 0$  and  $m_j > 0$ , then  $\mathcal{L}(D)$  consists of all elements  $f \in \mathbb{F}_q(X)$  such that

1.  $f$  has zeros of order greater than or equal to  $m_j$  at  $Q_j$  for  $j = 1, 2, \dots, s$ , and
2.  $f$  may have poles only at the points  $P_i$ , with the order of the pole at  $P_i$  being at most  $n_i$  for  $i = 1, 2, \dots, r$ .

### 3 AG CODES

With this background we give the definition of an AG code, which as described in [3, 6.8], is a generalization of the original RS code definition.

**Definition 1 (AG Code)** Let  $X$  be a projective curve over  $\mathbb{F}_q$  and  $P_1, P_2, \dots, P_n$  be distinct rational points on  $X$ . Form the divisor  $D = P_1 + P_2 + \dots + P_n$ , and let  $G$  be a divisor on  $X$  with support disjoint from the support of  $D$ . Then the AG code  $C_{\mathcal{L}}(D, G)$  on  $X$  is defined as

$$C_{\mathcal{L}}(D, G) = \{(f(P_1), f(P_2), \dots, f(P_n)) : f \in \mathcal{L}(G)\}.$$

We remark that BCH codes, which by definition can have code lengths greater than the size of the alphabet, are AG codes [5, II.3.9]. The following theorem, which is a direct consequence of the Riemann-Roch theorem mentioned above, provides the parameters of an AG code.

**Theorem 1** [5, II.2.3.] If  $\deg(G) < n$ , the AG code  $C_{\mathcal{L}}(D, G)$  is linear with parameters  $n = \deg(D)$ ,  $k = \dim(\mathcal{L}(G)) \geq \deg(G) + 1 - g$ , and  $d \geq d^* = n - \deg(G)$ , where  $d^*$  is called the *designed minimum distance* of the code. Furthermore, if  $\deg(G) > 2g - 2$ , then  $k = \deg(G) + 1 - g$ .

The inequality involving  $d$  in this theorem provides justification for searching for long AG codes because of their improved error-correcting capability. The theorem also supports the previous assertion that the search for long AG codes means a search for algebraic curves containing many rational points.

The number of rational points on a curve is clearly finite, and in fact, for a given field size,  $q$ , and genus,  $g$ , the number of rational points,  $N_q(g)$ , does not exceed the Serre upper bound [5, V.3.1] given by

$$N_q(g) \leq q + g \lfloor 2\sqrt{q} \rfloor + 1,$$

where for a positive number  $a$ ,  $\lfloor a \rfloor$  denotes the integer part of  $a$ . Curves whose number of rational points attains the Serre upper bound are called *maximal curves*. It is clear that this happens only if the field size is a square. It has been shown that over a finite field containing  $q^2$  elements, where  $q$  is a power of a prime, the *Hermitian plane curves*, given by the equation

$$y^q + y = x^{q+1},$$

are maximal curves with genus  $g = (q^2 - q)/2$  and these curves contain  $q^3 + 1$  rational points as given by the Serre bound [5, VI.4.4].

### 4 METHODS

For the performance comparisons with RS codes we considered *Hermitian codes*, that is, AG codes based on Hermitian curves, because these curves are maximal and a great amount of encoding and decoding research for AG codes has concentrated on codes based on these curves (see references in [6]). We further restricted our attention to the case where the divisor  $G$  in Definition 1 has only a single point in its support because this is the simplest case and the case which allows for the longest code length, and also since this is the case most often considered by encoding/decoding researchers (see references in [6]).

Specifically, we let  $X$  be a Hermitian curve over  $\mathbb{F}_{q^2}$  containing rational points  $P_1, P_2, \dots, P_n, Q$ , where  $n = q^3$  and  $Q$  is the point at infinity, and defined the divisors  $D = P_1 + P_2 + \dots + P_n$  and  $G = mQ$ , where  $\deg(G) = m < n$  as required in Theorem 1.  $\mathcal{L}(G)$  is then the vector space of rational functions on  $X$  which may have a pole only at  $Q$  with order at most  $m$ . Clearly,  $D$  and  $G$  have disjoint support, and so by Theorem 1 this defines a code  $C_{\mathcal{L}}(D, G)$  with parameters  $n = q^3$ ,  $k \geq m + 1 - g$ , and  $d \geq q^3 - m$ . Yang and Kumar [7] provide formulas for computing the

values of  $k$  and  $d$  for all values of the parameter  $m$ .

To address the trade-off between coding gain and bandwidth expansion, we compared the performance of high and low-rate RS codes with much longer Hermitian codes of various rates over the same field. For these comparisons we selected three fields,  $\mathbb{F}_{16}$ ,  $\mathbb{F}_{64}$ , and  $\mathbb{F}_{256}$ , and we chose RS codes with rates as close as possible to 0.92 for the high-rate and 0.70 for the low-rate, two reasonably bandwidth-efficient rates; however, over  $\mathbb{F}_{16}$ , the RS code with highest rate which corrected at least one error was 0.88, and the RS code with rate closest to 0.70 was 0.69. To address the trade-off between bandwidth expansion and complexity of finite-field arithmetic computations, we compared the performance of RS and Hermitian codes of the same length, but over necessarily different fields. For these comparisons we selected three code lengths, 64, 512, and 4096, and RS codes with rates 0.92 and 0.70.

Performance comparisons were made in terms of code rate or its inverse, bandwidth expansion, and coding gain, where coding gain of Hermitian codes relative to RS codes is determined from graphs of *bit error probability* ( $P_b$ ) versus *signal-to-noise ratio* ( $E_b/N_0$ ). These comparisons assume a communications system containing RS or Hermitian coding, BPSK modulation, additive white Gaussian noise (AWGN) channel, and hard-decision demodulation. In his master's thesis, Rao [8] made similar comparisons for Digital Video Broadcast cable television transmission systems, which include RS coding, interleaving, and 64-QAM modulation rather than BPSK modulation, and which require very low bit error probabilities.

The calculations of bit error probability in this paper are based on the standard formulas for the probability of a BPSK-modulated channel symbol error over an AWGN channel and the probability of a block code symbol error. These calculations were performed on a Pentium-based PC using MATLAB and the MATLAB-based Digital Communications Toolbox (DigComT), a product of Native Intelligence.

## 5 RESULTS

The first three sections describe the comparisons between RS and Hermitian codes of different lengths over the same field, addressing the trade-off between coding gain and bandwidth expansion. The fourth section describes the comparison between RS and Hermitian codes of the same length but over different fields, addressing the trade-off between bandwidth expansion and complexity of finite-field arithmetic computations.

### 5.1 Comparisons over $\mathbb{F}_{16}$

The high-rate comparison (Fig.1) revealed positive coding gain relative to the RS code only for Hermitian codes with rates less than that of the RS code. By contrast, the low-

rate comparison (Fig.1) demonstrated positive coding gain of the rate 0.69, 0.75, 0.80, and 0.84 Hermitian codes relative to the rate 0.69 RS code at bit error probabilities below  $10^{-3}$ . In particular, at  $P_b = 10^{-5}$ , coding gain for these Hermitian codes ranged from approximately 0.2 dB for the 0.84 rate code to 1.5 dB for the 0.69 rate code; at  $P_b = 10^{-8}$ , coding gain ranged from approximately 0.4 dB for the rate 0.84 code to 2.2 dB for the 0.69 rate code (Table 1).

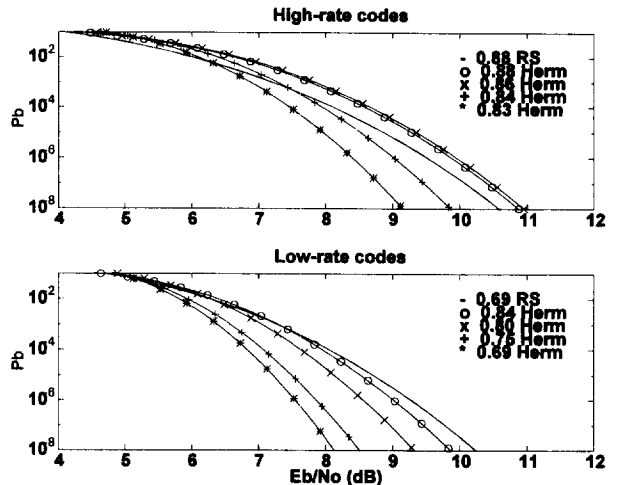


Figure 1: Bit error probability vs SNR for RS and Hermitian codes over  $\mathbb{F}_{16}$ .

### 5.2 Comparisons over $\mathbb{F}_{64}$

The high-rate comparison (Fig.2) showed positive coding gain of the rate 0.92, 0.93, and 0.94 rate Hermitian codes relative to the rate 0.92 RS code at bit error probabilities below  $10^{-3}$ ,  $10^{-6}$ , and  $10^{-8}$ , respectively. Specifically, at  $P_b = 10^{-5}$ , coding gain for these Hermitian codes ranged from approximately  $-0.3$  dB for the 0.94 rate code to 0.5 dB for the 0.92 rate code; at  $P_b = 10^{-8}$ , coding gain ranged from approximately 0.0 dB for the rate 0.94 code to 1.2 dB for the 0.92 rate code (Table 1).

The low-rate comparison (Fig.2) demonstrated positive coding gain of the rate 0.70, 0.75, 0.80, and 0.85 Hermitian codes relative to the rate 0.70 RS code at bit error probabilities below  $10^{-3}$ . At  $P_b = 10^{-5}$ , coding gain for these Hermitian codes ranged from approximately 0.4 dB for the 0.85 rate code to 1.0 dB for the 0.70 rate code; at  $P_b = 10^{-8}$ , coding gain ranged from approximately 0.8 dB for the rate 0.85 code to 1.5 dB for the 0.70 rate code (Table 1).

### 5.3 Comparisons over $\mathbb{F}_{256}$

The high-rate comparison (Fig.3) showed positive coding gain of the rate 0.92, 0.93, 0.94, and 0.95 Hermitian codes relative to the rate 0.92 RS code at bit error probabilities

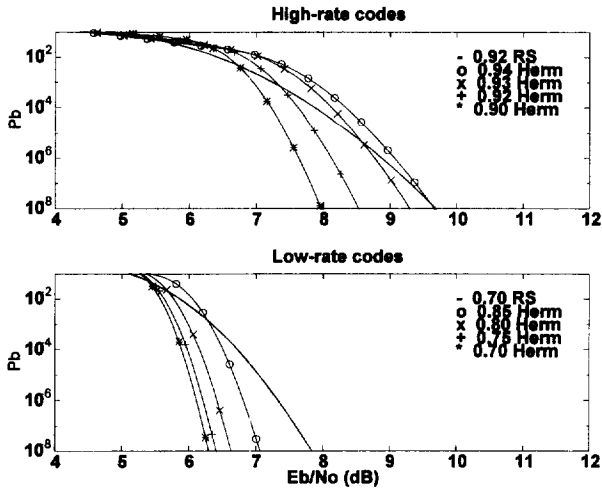


Figure 2: Bit error probability vs SNR for RS and Hermitian codes over  $\mathbb{F}_{64}$ .

below  $10^{-3}$ ,  $10^{-4}$ ,  $10^{-5}$ , and  $10^{-7}$ , respectively. At  $P_b = 10^{-5}$ , coding gain for these Hermitian codes ranged from approximately  $-0.2$  dB for the 0.95 rate code to  $0.4$  dB for the 0.92 rate code; while at  $P_b = 10^{-8}$ , coding gain ranged from approximately  $0.2$  dB for the rate 0.95 code to  $0.9$  dB for the 0.92 rate code (Table 1).

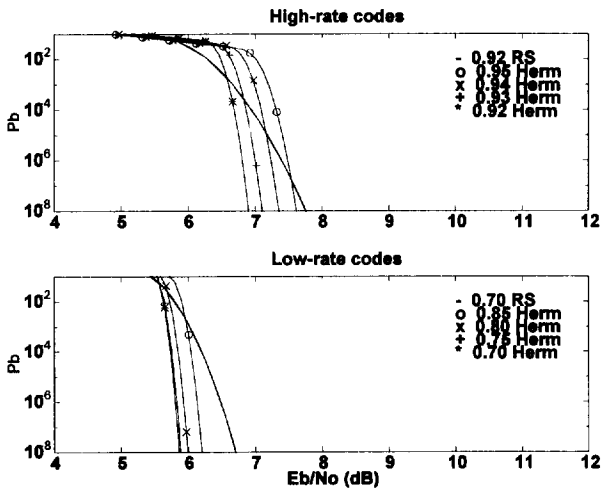


Figure 3: Bit error probability vs SNR for RS and Hermitian codes over  $\mathbb{F}_{256}$ .

The low-rate comparison (Fig.3) demonstrated positive coding gain of the rate 0.70, 0.75, 0.80, and 0.85 Hermitian codes relative to the rate 0.70 RS code at bit error probabilities below  $10^{-3}$ . At  $P_b = 10^{-5}$ , coding gain for these Hermitian codes ranged from approximately  $0.3$  dB for the 0.85 rate code to  $0.6$  dB for the 0.70 rate code; at  $P_b = 10^{-8}$ , coding gain ranged from approximately  $0.5$  dB for the rate

0.85 code to  $0.8$  dB for the 0.70 rate code (Table 1).

High-Rate					
		$P_b = 10^{-5}$		$P_b = 10^{-8}$	
Field		Minimum	Maximum	Minimum	Maximum
$\mathbb{F}_{16}$		-0.4(0.88)	-0.4(0.88)	-0.3(0.88)	-0.3(0.88)
$\mathbb{F}_{64}$		-0.3(0.94)	0.5(0.92)	0.0(0.94)	1.2(0.92)
$\mathbb{F}_{256}$		-0.2(0.95)	0.4(0.92)	0.2(0.95)	0.9(0.92)
Low-Rate					
		$P_b = 10^{-5}$		$P_b = 10^{-8}$	
Field		Minimum	Maximum	Minimum	Maximum
$\mathbb{F}_{16}$		0.2(0.84)	1.5(0.69)	0.4(0.84)	2.2(0.69)
$\mathbb{F}_{64}$		0.4(0.85)	1.0(0.70)	0.8(0.85)	1.5(0.70)
$\mathbb{F}_{256}$		0.3(0.85)	0.6(0.70)	0.5(0.85)	0.8(0.70)

Table 1: Coding gain in dB's of Hermitian codes relative to high and low-rate RS codes over fields with 16, 64, and 256 elements at bit error probabilities of  $10^{-5}$  and  $10^{-8}$  with Hermitian codes rates in parentheses. (Results for Hermitian codes with rates less than RS codes not included.)

#### 5.4 Comparisons of Codes of Equal Lengths

Results for the comparisons of Hermitian codes of length 64 over  $\mathbb{F}_{16}$  with RS codes of length 64 over  $\mathbb{F}_{64}$  may be obtained by comparing Figures 1 and 2. From these plots, it is evident that in the high-rate case comparable or improved performance was attained by Hermitian codes with rates less than or equal to 0.84, which represents a +10% bandwidth expansion and a reduction in field size by a factor of 4 relative to the rate 0.92 RS code (Table 2). In the low-rate case comparable or improved performance was attained by Hermitian codes with rates less than or equal to 0.64, which represents a +9% bandwidth expansion and a reduction in field size by a factor of 4 relative to the rate 0.70 RS code (Table 2).

Plots for codes of length 512 and 4096 (not included here) revealed a more favorable trade-off between bandwidth expansion and complexity of finite-field arithmetic computations as code length increases. For codes of length 512 comparable or improved performance was attained by Hermitian codes over  $\mathbb{F}_{64}$  with rates less than or equal to 0.87, which represents a +6% bandwidth expansion and a reduction in field size by a factor of 8 relative to the high-rate 0.92 RS code over  $\mathbb{F}_{512}$  (Table 2); in the low-rate case comparable or improved performance was attained by Hermitian codes with rates less than or equal to 0.70, which represents a 0% bandwidth expansion and a reduction in field size by a factor of 8 relative to the rate 0.70 RS code over  $\mathbb{F}_{512}$  (Table 2). For codes of length 4096 comparable or improved performance was attained by Hermitian codes over  $\mathbb{F}_{256}$  with rates less than or equal to 0.91, which represents a +1% bandwidth expansion and a reduction in field

size by a factor of 16 relative to the high-rate 0.92 RS code over  $\mathbb{F}_{4096}$  (Table 2).

High-Rate					
Field			Rate		
Length	H	RS	H	RS	BWE
64	$\mathbb{F}_{16}$	$\mathbb{F}_{64}$	0.84	0.92	+10%
512	$\mathbb{F}_{64}$	$\mathbb{F}_{512}$	0.87	0.92	+6%
4096	$\mathbb{F}_{256}$	$\mathbb{F}_{4096}$	0.91	0.92	+1%
Low-Rate					
Field			Rate		
Length	H	RS	H	RS	BWE
64	$\mathbb{F}_{16}$	$\mathbb{F}_{64}$	0.64	0.70	+9%
512	$\mathbb{F}_{64}$	$\mathbb{F}_{512}$	0.70	0.70	0%

Table 2: Bandwidth expansion (BWE) relative to high and low-rate RS codes for Hermitian (H) codes of the same length and comparable performance.

## 6 DISCUSSION AND CONCLUSIONS

The comparisons in §5.1 – §5.3 of RS codes with much longer Hermitian codes over the same field demonstrate the utility of the Hermitian codes, with respect to the trade-off between coding gain and bandwidth expansion. For each of the low-rate comparisons and for the high-rate comparisons over the two larger fields, positive coding gain was attained at bit error probabilities below  $10^{-3}$  by Hermitian codes with rates equal to or greater than the RS code. In the low-rate comparisons, gains of up to 1.5 and 2.2 dB at  $P_b = 10^{-5}$  and  $10^{-8}$ , respectively, were recorded over  $\mathbb{F}_{16}$ ; in the high-rate comparisons, gains of up to 0.5 and 1.2 dB at  $P_b = 10^{-5}$  and  $10^{-8}$ , respectively, were recorded over  $\mathbb{F}_{64}$ . These comparisons, however, ignore issues involving the complexity of encoding/decoding algorithms and of finite-field arithmetic computations.

Høholdt and Pellikaan [6] characterize algorithm development according to three successive stages, which they call the existence, effective, and efficient stages. They state that decoding algorithms for RS codes have reached the third stage of development, but that decoding algorithms for AG codes have just passed the second and are now entering the third stage. Therefore, since Hermitian codes are much longer and since at present their decoding algorithms are not efficient compared to decoding algorithms for RS codes, considerable progress in algorithm development will have to be made before Hermitian codes can be considered competitive with RS codes over the same field, except perhaps in the case of low-rate satellite communications where the inefficiencies of AG codes could be tolerated for the gain of 2+ dB.

The comparisons in §5.4 of RS and Hermitian codes of

the same length (Table 2) demonstrate that the same performance of RS codes is achievable by Hermitian codes over much smaller fields, with presumably much simpler finite-field arithmetic computations, at the cost of some bandwidth expansion. Further, the results showed an increasingly favorable trade-off between bandwidth expansion and complexity of finite-field arithmetic computations as code length increases.

Finally, future research will consider the effects of concatenated codes and will investigate AG codes based on non-Hermitian curves which provide coding gain but allow for simpler encoding/decoding algorithms.

## 7 ACKNOWLEDGMENTS

We gratefully acknowledge the support of the first author by the Independent Research Program of the Naval Command, Control and Ocean Surveillance Center, RDT&E Division, and of the second author by the Mathematics and Computer Science Alumni Association of Point Loma Nazarene College.

## REFERENCES

- [1] Hagenauer, J., E. Offer, and L. Papke (1994), Matching Viterbi decoders and Reed-Solomon decoders in a concatenated system, *In* Wicker, S. B. and V. K. Bhargava, eds., *Reed-Solomon Codes and Their Applications* (IEEE Press, New York).
- [2] Goppa, V. D. (1981), Codes on algebraic curves, *Soviet Mathematics. Doklady*, Volume 24, pp. 170–172.
- [3] van Lint, J. H. (1992), *Introduction to Coding Theory*, 2nd ed. (Springer-Verlag, New York).
- [4] Reed, I. S. and G. Solomon (1960), Polynomial codes over certain finite fields, *SIAM Journal of Applied Mathematics*, Volume 8, pp. 300–304.
- [5] Stichtenoth, H. (1991), *Algebraic Function Fields and Codes* (Springer-Verlag, New York).
- [6] Høholdt, T. and R. Pellikaan (1995), On the decoding of algebraic-geometric codes, *IEEE Transactions on Information Theory*, Volume 41, pp. 1589–1614.
- [7] Yang, K. and P. V. Kumar (1992), On the true minimum distance of Hermitian codes, *In* Stichtenoth, H. and M. A. Tsfasman, eds., *Coding Theory and Algebraic Geometry-Proceedings Luminy, 1991*, Lecture Notes in Mathematics No. 1518 (Springer-Verlag, New York).
- [8] Rao, S. P. N. (1996), Performance evaluation of multidimensional cyclic codes and algebraic-geometric codes, M.S. Thesis, Cornell Univ. (Ithaca, NY).