REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
		Reprint

4. TITLE AND SUBTITLE

TITLE ON REPRINT

5. FUNDING NUMBERS

DAAD19-99-1-0289

6. AUTHOR(S)

AUTHOR(S) ON REPRINT

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(ES)

Clemson University

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

ARO 39007.7-CI

11. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12 b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

ABSTRACT ON REPRINT

20010413 145

14. SUBJECT TERMS

15. NUMBER IF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Draft paper submitted to the *2001 IEEE Military Communications Conference*.

FREQUENCY-HOP SPREAD-SPECTRUM PACKET RADIO WITH HERMITIAN CODES

Thomas G. Macdonald
Michael B. Pursley

Department of Electrical and Computer Engineering
Fluor Daniel Engineering Innovation Building
Clemson University, Clemson, SC 29634

ABSTRACT

Hermitian codes are an attractive alternative to Reed-Solomon codes for use in frequency-hop (FH) spread-spectrum packet radio networks. For a given alphabet size a Hermitian code has a much longer block length than a Reed-Solomon code. This and other considerations suggest that Hermitian codes may be superior for certain applications. Analytical results are developed for the evaluation of the packet error probability for FH transmissions using Hermitian coding. We find there are several situations for which Hermitian codes provide much lower packet error probabilities than can be obtained with Reed-Solomon codes. In general, as the code rate decreases or the symbol alphabet size increases the relative performance of the Hermitian codes improves with respect to the Reed-Solomon codes. Performance evaluations are presented for an additive white Gaussian noise channel and for certain partial-band interference channels, and the packet error probability is evaluated for both errors-only and errors-and-erasures decoding.

INTRODUCTION

Reed-Solomon codes have been adopted for a wide range of applications [1] including the SINCGARS slow-frequency-hop packet radio [2]. Hermitian codes, which are not as well known as Reed-Solomon codes, offer some of the same benefits, but they also have the potential for extending the effective range of the frequency-hop (FH) transmissions beyond that attainable with Reed-Solomon codes. This potential is due to the fact that for the same alphabet size M the block length of a Hermitian code is longer by a factor of $\sqrt{M}$ than the block length of a Reed-Solomon code, and this provides a performance advantage in combating Gaussian noise.

As an example we consider Hermitian and Reed-Solomon codes that have an alphabet of size $M = 16$, the Hermitian code words are of length 64 and the singly extended Reed-Solomon code words are of length 16. Thus the number of code symbols in one Hermitian code word is equal to the total number of code symbols in four Reed-Solomon code words. Similarly if $M = 64$ the length of one Hermitian code word is equal to the combined length of eight Reed-Solomon code words. In general if the code rate and the number of information bits per packet are the same for the two codes, there are $\sqrt{M}$ more code words per packet for Reed-Solomon coding than for Hermitian coding. This allows the Hermitian code to correct combinations of errors that are not correctable by the Reed-Solomon code.

The results presented in this paper permit the evaluation of the packet error probability for FH transmission with Reed-Solomon coding or Hermitian coding. Analytical results are given for both the additive white Gaussian noise channel and the partial-band catastrophic-interference channel. This latter channel is a good model for strong partial-band jamming or FH multiple-access interference. For values of M of interest in this paper, the defining feature of the partial-band catastrophic-interference channel is that the probability of error is approximately one for an M-ary symbol that transmitted in a frequency slot containing interference. Numerical results on the packet error probability are given for both channel models and for both errors-only and errors-and-erasures decoding.

Performance comparisons based on the bit error probability, rather than the packet error probability, are given in [3] for Hermitian and Reed-Solomon codes. These results are limited to the additive white Gaussian noise channel. Even for this channel model the bit errors at the decoder output are statistically dependent, so the packet error probability cannot be determined from the bit error probability. Because we also consider the partial-band interference channel, the performance comparisons provided in this paper are more appropriate for the typical operating environment of a FH packet radio network.

SYSTEM DESCRIPTION

In this paper a singly-extended RS code is designated by $(n_R, k_R, d_R)_M$, where M is the size of the symbol alphabet and d_R is the minimum distance of the code. For a singly-extended RS code $n_R = M$, and since RS codes are maximum distance separable $d_R = n_R - k_R + 1$. In a similar manner, a Hermitian code is denoted by $(n_H, k_H, d_H)_M$. As explained in [4], Hermitian codes do not exist for all values of M. We consider the class of Hermitian codes for which $M = 4^z$, where z is a positive integer. The block length for a Hermitian code with alphabet size M is $n_H = M\sqrt{M} = 8^z$. The range of values for k_H for Hermitian codes is given in [5]. Finally, in [5] the authors show that a lower bound on the minimum distance for a Hermitian code is $d_H \geq d = n_H - k_H - \frac{1}{2}(M - \sqrt{M}) + 1$. For the performance evaluations presented in this paper it is assumed that the minimum distance is exactly d.

The applications considered in this paper are for binary modulation, so the M-ary code symbols are transmitted as

This research was supported by the U.S. Army Research Office under grant number DAAD19-99-1-0289 and the Office of Naval Research under grant number N00014-00-1-0565.

{1,1}	{2,1}	...	{L,1}
{1,2}	{2,2}		{L,2}
{1,3}	{2,3}		{L,3}
.	.		.
.	.		.
.	.	...	.
{1,n_{RS}}	{2,n_{RS}}		{L,n_{RS}}

Reed-Solomon

{1,1}	{1,2}	...	{1,L}
{1,L+1}	{1,L+2}		{1,2L}
{1,2L+1}	{1,2L+2}		{1,3L}
.	.		.
.	.		.
.	.		.
{1,n_H-(L-1)}	{1,n_H-(L-2)}	...	{1,n_H}

Hermitian

Figure 1. Packet formats

$m = \log_2 M$ binary symbols. Equal-energy orthogonal signals are employed with standard noncoherent demodulation and bounded-distance decoding.

Performance comparisons are based on the packet error probability, and so for a fair comparison the packet size is the same for each system. The packet format for each type of coding is illustrated in Figure 1. For Hermitian coding there is one code word per packet, and for RS coding there are $L = \sqrt{M}$ code words per packet. For the packet formats illustrated in Figure 1, all of the symbols in a row are transmitted in the same dwell interval, and each row corresponds to a different dwell interval. The transmission of a packet requires M consecutive dwell intervals regardless of which code is used.

PERFORMANCE EVALUATIONS

In this section the performance of FH systems with Hermitian codes is compared to the performance of systems with RS codes for two types of channels. The packet error probabilities for the systems with RS codes are derived from the analytical expressions given in [6]. Analytical expressions are developed for the packet error probability for FH packet radios with Hermitian coding for both an additive white Gaussian noise channel and a channel with catastrophic partial-band interference.

A. ADDITIVE WHITE GAUSSIAN NOISE CHANNEL

The first performance comparison we present is for Hermitian codes and RS codes for an additive white Gaussian noise (AWGN) channel and errors-only decoding. An errors-only decoding algorithm for Hermitian codes is given in [7]. Since bounded distance decoding is employed, a received word is decoded correctly if twice the number of errors in the received word is less than the minimum distance of the code. Otherwise a decoding error or decoding failure occurs. Cyclic redundancy check (CRC) codes or other error-detecting codes are employed to detect decoding errors, although such errors are rare for RS codes and errors-only decoding unless $n - k$ is very small [8]. If a received word at the decoder input produces a code word at the decoder output in which no errors are detected, we say the received word *decodes*. If a received word at the decoder input either does not produce a code word at the decoder output (decoding failure) or produces a code word in which errors are detected (decoding error), we say that received word does *not decode*. A packet error occurs if at least one received word in the packet does not decode.

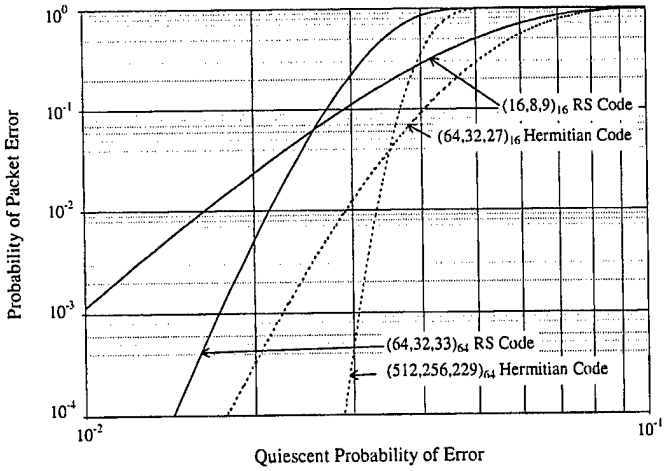

Figure 2. AWGN channel

The performance curves presented in this paper show the probability of a packet error as a function of the quiescent error probability q, which is defined as the probability a binary symbol is in error The probability p of a channel symbol error is $p = 1-(1-q)^m$, where $m = \log_2 M$. The probability of a packet error for the system employing the Hermitian codes is

$$P_e = 1 - \sum_{t=0}^{t_H} \binom{n_H}{t} p^t (1-p)^{n_H - t},$$

where $t_H = \lfloor \frac{d_H - 1}{2} \rfloor$ and $\lfloor x \rfloor$ denotes the integer part of the real number x. The parameter t_H is the maximum number of errors a received word can contain and still decode.

Performance comparisons for Hermitian codes and RS codes are shown in Figure 2. The results in Figure 2 are for rate 1/2 codes for $M = 16$ and $M = 64$. For each symbol alphabet size the Hermitian codes outperform the RS codes. For $M = 16$ and a rate 1/2 code, $d_H = 27$, $d_R = 9$, and there are 4 RS code words per packet. The maximum number of errors that can be corrected per packet is greater for the RS code (16) than for the Hermitian code (13), but as illustrated in Figure 2 the Hermitian code results in better performance. The reason for this apparent contradiction is that unlike for the RS code the decoding of a packet for the Hermitian code does not depend on the distribution of the errors within the packet.

The communication range for systems with Hermitian

codes is greater than the range of systems using RS codes. Let the desired packet error probability be 10^{-3} and consider two systems that have a fixed transmitter power level and the same receiver noise figure. One system employs Hermitian coding and the other system uses RS coding. Assume that the received power is inversely proportional to the square of the distance between the transmitter and receiver. For the systems of Figure 2 the communication range for the Hermitian codes is approximately 10% greater than the range of RS codes.

B. PARTIAL-BAND INTERFERENCE CHANNEL

In this section the performance of FH packet radios is determined for channels with partial-band interference. The partial-band interference is catastrophic [6], which means that the probability that a binary symbol is in error is 1/2 given that the symbol is transmitted in a frequency slot that has interference. The probability that a binary symbol is error given that it is transmitted in a frequency slot with no partial-band interference is q, the quiescent probability of error. Let ρ denote the fraction of the frequency slots that contain interference. A dwell interval that contains partial-band interference is said to be *hit*. Thermal noise is present in all of the dwell intervals. For a symbol transmitted in a frequency slot with catastrophic partial-band interference the probability of error is $1 - M^{-1}$. For the expressions derived in this section we assume that an M-ary symbol transmitted in a dwell interval with partial-band interference is received in error.

Since there is only one Hermitian code word per packet, the probability of a packet error is the same as the probability that a received word does not decode. For a catastrophic partial-band interference channel the packet error probability for a system that uses Hermitian coding and errors-only decoding is

$$P_e = 1 - \sum_{j=0}^{\lfloor t_H/L \rfloor} \binom{M}{j} \rho^j (1-\rho)^{M-j} P(j),$$

where $P(j)$ is the conditional probability that a received word decodes given that there is partial-band interference in j dwell intervals. There are L symbol errors for every dwell interval that is hit, and thus as long as at most $\lfloor t_H/L \rfloor$ dwell intervals are hit the error-correcting capability of the code is not exceeded.. Since there are Lj symbol errors from partial-band interference, the received word decodes as long as there are not more than $t_H - Lj$ errors in the $n_H - Lj$ remaining symbols. Therefore we can express $P(j)$ as

$$P(j) = \sum_{t=0}^{t_H - Lj} \binom{n_H - Lj}{t} p^t (1-p)^{n_H - Lj - t}.$$

Packet error probabilities are given in Figure 3 for an additive white Gaussian noise channel and a catastrophic partial-band interference channel with four different values of ρ. As ρ increases, the performance of the Hermitian codes degrades relative to that of the RS code.

The dependence of the packet error probability on both the size of the symbol alphabet M and the code rate r is

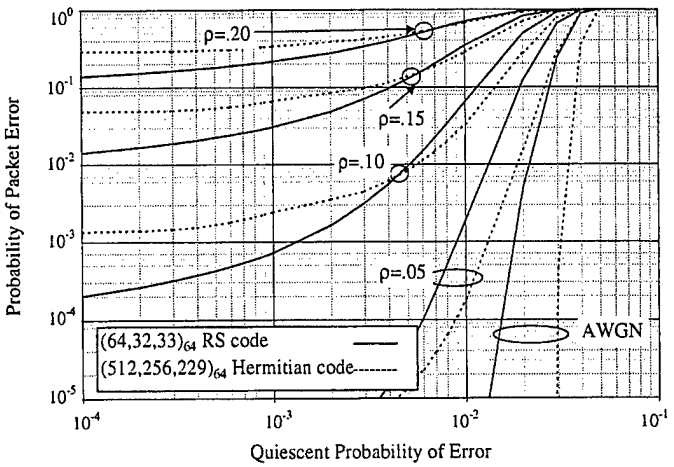

Figure 3. Packet error probabilities for M=64, rate 1/2 codes, and a catastrophic partial-band interference channel

illustrated in Figure 4. To help quantify this dependence we introduce the metric ψ, which is defined as the ratio of the maximum number of errors per packet that can be corrected by the Hermitian code to the maximum number that can be corrected by the Reed-Solomon code of the same rate and alphabet size. This metric is suitable for errors-only, bounded-distance decoding. For a given symbol alphabet size M and a given code rate r, a Reed-Solomon code can correct up to $t_m = M(1-r)/2$ errors per received word. Since there are $\sqrt{M}$ Reed-Solomon code words per packet, up to $\sqrt{M}t_m = M\sqrt{M}(1-r)/2$ errors can be corrected in a given packet. Even if there are fewer than $\sqrt{M}t_m$ errors in a packet, the packet does not necessarily decode, since there may be one or more received words with more than t_m errors. For a packet to successfully decode with $\sqrt{M}t_m$ errors there must be exactly t_m errors in each received word. On the other hand, since there is only one Hermitian code word per packet, the error-correcting capability of the Hermitian code is independent of the distribution of errors within the packet. Manipulating the expression given in [4] and [5] to couch the result in terms of M and r, we see that the Hermitian code can correct up to $M\sqrt{M}(1-r)/2 - (M-\sqrt{M})/4$ errors per packet, and thus

$$\psi = 1 - \frac{\sqrt{M}-1}{2M(1-r)}.$$

Values of ψ for several symbol alphabet sizes and code rates of interest are given in Table 1. From Figure 4 we see that as ψ increases the relative performance of the Hermitian code increases. Therefore, as the code rate is reduced or the symbol alphabet size is increased, there is an improvement in the relative performance of Hermitian codes.

Let ρ_H be the value of ρ for which Hermitian coding and RS coding achieve a packet error probability of 10^{-4} for the same value of the quiescent probability of error. Hermitian coding outperforms RS coding for $0 \le \rho \le \rho_H$. The parameter ρ_H is directly proportional to ψ, and thus ρ_H increases

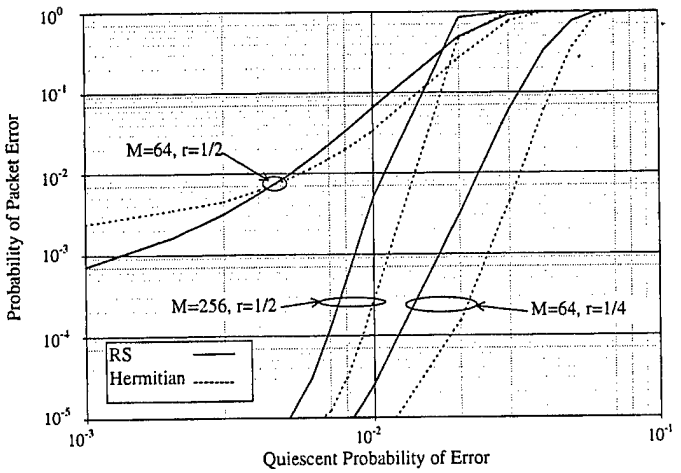

Figure 4. Packet error probabilities for a catastrophic partial-band interference channel with ρ=1/8

	M=16	M=64	M=256
r=3/4	0.63	0.78	0.88
r=1/2	0.81	0.89	0.94
r=1/4	0.87	0.93	0.96

Table 1. Values of ψ

as the code rate is reduced or the symbol alphabet size is increased. In addition, ρ_H is larger for errors-and-erasures decoding or partial-band interference that is not catastrophic. Although the results are not given in this paper, we have found that as the strength of the partial-band interference is reduced the value of ρ_H increases. This finding is consistent with the fact that Hermitian codes provide better performance than RS codes for an additive white Gaussian noise channel.

Up to this point only errors-only decoding has been considered. It is well known that for FH systems employing RS codes the performance can be greatly improved by using errors-and-erasures decoding [9]. At the present time an errors-and-erasures decoding algorithm for Hermitian codes has not been published, but our results indicate that errors-and-erasures decoding provides a performance improvement for Hermitian codes. If a received symbol is erased the decoder does not use the symbol to estimate the transmitted data. Symbol erasures are based on side information that provides a measure of reliability of each of the received symbols. Methods of developing side information include parity bits [10], staggered interleaving [11], Bayesian decision theory [12], and ratio threshold tests [13], but in this paper we focus on side information developed from test symbols [14].

A number N_{TS} of binary test symbols are transmitted in each dwell interval. If more than a certain number γ of these test symbols are in error, the dwell interval is deemed unreliable and all symbols in that dwell interval are erased. If the side information correctly indicates that partial-band interference is present in a frequency slot used for transmission, the interference is said to be *detected.* If interference that is in a dwell interval used for transmission is not detected, a *miss* is said to occur. A *false alarm* occurs if the side information indicates partial-band interference is present in a frequency slot that has no such interference. The false alarm probability and detection probability are denoted α and β, respectively. For binary test symbols and catastrophic partial-band interference,

$$\alpha = \sum_{\ell=\gamma}^{N_{TS}} \binom{N_{TS}}{\ell} q^i (1-q)^{N_{TS}-i},$$

and

$$\beta = 2^{-N_{TS}} \sum_{\ell=\gamma}^{N_{TS}} \binom{N_{TS}}{\ell}.$$

The analytical expression for P_e, the packet error probability for Hermitian coding and errors-and-erasures decoding, is too complicated to present as a single equation. The following development is similar to the expressions given in [6] for RS encoding and errors-and-erasures decoding. First note that $P_e = 1 - P_c$, where P_c is the probability that the Hermitian word (i.e., the packet) decodes. The probability that the received word decodes is

$$P_c = \sum_{j=0}^{\lambda} \binom{M}{j} \rho^j (1-\rho)^{M-j} P_3(j), \qquad (1)$$

where $\lambda = \lfloor (d_H - 1)/L \rfloor$ and $P_3(j)$ is the conditional probability that the received word decodes given that partial-band interference is present in j of the M frequency slots. If the symbols in more than λ dwell intervals are erased it is not possible to decode the packet. The probability the received word is decoded given that partial-band interference is present in j of the frequency slots is

$$P_3(j) = \sum_{i=i'}^{j} \binom{j}{i} \beta^i (1-\beta)^{j-i} P_2(i;j),$$

where $i' = \max(0, 2j - \lambda)$ and $P_2(i;j)$ is the probability that the received word decodes given that there are j hits and that i of them are detected. The integer i' is chosen so that the error-correcting capability of the code is not exceeded. The probability $P_2(i;j)$ is given by

$$P_2(i;j) = \sum_{s=0}^{s^*} \binom{M-j}{s} \alpha^s (1-\alpha)^{M-j-s} P_1(s;i,j),$$

where $s^* = \lambda - 2j + i$ and $P_1(s;i,j)$ is the probability that the code word is correct given j hits, i detected hits, and s false alarms. Once again the limits of the summation are chosen to insure that the error-correcting capability of the code is not exceeded. Finally, the probability $P_1(s;i,j)$ is given by

$$P_1(s;i,j) = \sum_{t=0}^{t^*} \binom{n_H - L(j+s)}{t} p^s (1-p)^{n_H - L(j+s) - t},$$

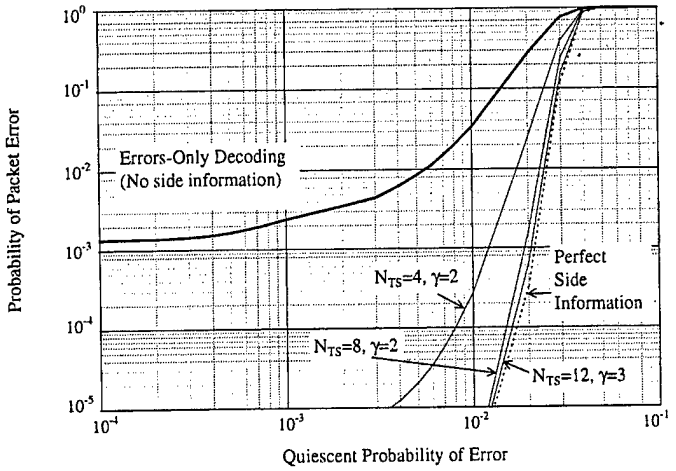

Figure 5. Packet error probabilities for a $(512, 256, 229)_{64}$ Hermitian code for a catastrophic partial-band interference channel with ρ=1/10

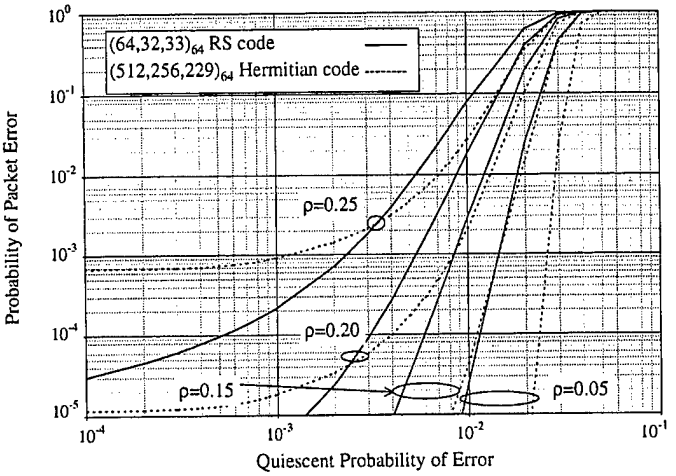

Figure 6. Packet error probabilities for errors-and-erasures decoding

where $t^* = \lfloor (d_H - 1 + L(i-s))/2 \rfloor - Lj$ is the maximum number of errors the Hermitian code can correct if there are j hits, i detected hits, and s false alarms.

The relative performance of errors-only decoding and errors-and-erasures decoding for Hermitian codes with $M = 64$ is illustrated in Figure 5. For each value of N_{TS} the value of the threshold γ is chosen to provide the smallest packet error probability. The use of side information dramatically improves the system performance even for $N_{TS} = 4$, and the performance for $N_{TS} = 12$ and $\gamma = 3$ is almost identical to the performance of a system that has perfect side information (i.e., $\alpha = 0$ and $\beta = 1$).

The performance of FH systems employing errors-and-erasures decoding is shown in Figure 6 for different values of ρ. The results in Figure 6 are for $N_{TS} = 12$ and $\gamma = 3$. These values of N_{TS} and γ provide the best performance over a wide range of quiescent error probabilities. Since the error probability for each system depends on the parameters (α and β) the relative performance of the two systems remains fairly constant as N_{TS} and γ are varied. By comparing Figure 3 and Figure 6 we see that, as expected, there is an improvement in the performance of both systems by using errors-and-erasures decoding rather than errors-only decoding. The performance of Hermitian codes also improves relative to RS codes if errors-and-erasures (EE) decoding is used instead of errors-only (EO) decoding. From Figure 6 we see that for errors-and-erasures decoding, $M = 64$, and $r = 1/2$ the value of ρ_H is greater than 0.2. Some values of ρ_H are given in Table 2. The results in Table 2 demonstrate that both ψ and ρ_H increase as M is increased, and that ρ_H is larger for errors-and-erasures decoding than it is for errors-only decoding.

M	r	ψ	EO	EE
64	1/2	0.89	$\rho_H > 0.05$	$\rho_H = 0.20$
256	1/2	0.94	$\rho_H > 0.10$	$\rho_H > 0.30$

Table 2. Values of ρ_H

REFERENCES

[1] S. B. Wicker and V. K. Bhargava (eds.), "Reed-Solomon codes in frequency-hop communications," IEEE Press, New York, 1994.

[2] A. Shohara *et al.*, "Design Plan: SINCGARS packet switch overlay," SRI International Report, SRI Project No. 1244, under Contract DAAB07-85-C-K581, May 1, 1986.

[3] B. E. Whalen and J. Jimenez, "Performance comparison of Hermitian and Reed-Solomon codes," *Proceedings of the 1997 IEEE Military Communications Conference*, vol. 1, pp. 15-19, November 1997.

[4] H. Stichtenoth, "A note on Hermitian codes over GF(q^2)," *IEEE Transactions on Information Theory*, vol. 34, no. 5, pp. 1345-1348, September 1988.

[5] J. H. van Lint and T. A. Springer, "Generalized Reed-Solomon codes from algebraic geometry," *IEEE Transactions on Information Theory*, vol. IT-33, no. 3, pp. 305-309, May 1987.

[6] M. B. Pursley, "Reed-Solomon codes in frequency-hop communications," Chapter 8 in *Reed-Solomon Codes and Their Applications*, S. B. Wicker and V. K. Bhargava (eds.), pp. 150-174, IEEE Press, New York, 1994.

[7] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen and T. Hoholdt, "Fast decoding of algebraic-geometric codes up to the designed minimum distance," *IEEE Transactions on Information Theory*, vol. 41, no. 5, pp. 16772-1677, September 1995.

[8] R. J. McEliece and L. Swanson, "On the decoder error probability for Reed-Solomon codes," *IEEE Transactions on Information Theory*, vol. IT-32, pp. 701-703, September 1986.

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

[10] A. W. Lam and D. V. Sarwate, "A comparison of two methods for generation of side information in frequency-hop spread-spectrum multiaccess communications," *Proceedings of the Conference of Information Sciences and Systems*, pp. 426-431, March 1987.

[11] J. P. Coon, T. G. Macdonald, and M. B. Pursley, "A new method for obtaining side information in frequency-hop spread-spectrum

systems," *Proceedings of the 2000 IEEE Military Communications Conference*, vol. 1, pp. 5.2.1-5, October 2000.

[12] C. A. Baum and M. B. Pursley, "Bayesian methods for erasure insertion in frequency-hop communications systems with partial-band interference," *IEEE Transactions on Communications*, vol. 40, pp. 1231-1238, July 1992.

[13] A. J. Viterbi, "A robust ratio-threshold technique to mitigate tone and partial band jamming in coded MFSK systems," *Proceedings of the 1982 IEEE Military Communications Conference*, vol. 1, pp. 22.4.1-5, October 1992.

[14] M. B. Pursley, "Packet error probabilities in frequency-hop radio networks – Coping with statistical dependence and noisy side information," *Proceedings of the 1986 IEEE Global Telecommunications Conference*, vol. 1, pp. 165-170, December 1986.