Bit-level erasure decoding beyond design distance of Reed-Solomon codes over $GF(2^m)$

Todd K. Moon and Scott Budge
{tmoon,scott}@ece.usu.edu
Electrical and Computer Engineering Department
Utah State University

Abstract

This paper explores the question of how to extend the capability of a Reed-Solomon code beyond the design distance in the case that symbols are affected on the bit level as would occur, for example, if data is obtained via packet interleaving on *bits* of the information sequence, so that packet losses result in bit-level erasures. It is shown that it is possible to decode beyond the erasure design distance for many codes. On the basis of simulation, the correction capability and plots showing the probability of uncorrectable erasures are provided.

Extended summary

Background: In many network-based multimedia applications, latency is a critical performance factor. In the interest of controlling latency, many applications avoid potential retransmission inherent in the guaranteed delivery of TCP protocol by employing UDP protocols as a base layer and protecting the data with a combination of forward error correction, employing packet retransmission only when necessary. In such cases, data may be interleaved so that the loss of a data packet results in only a small loss of a codeword, which may be reconstructed using an error correction code. Since a lost packet is known to be lost, this results in erasures in the data, as opposed to errors, essentially doubling the correction capability of the code.

This paper explores the question of how to extend the capability of a Reed-Solomon code beyond the design distance in the case that symbols are affected on the bit level as would occur, for example, if packet interleaving was performed on *bits* of the information sequence, so that packet losses result in bit-level erasures. It is shown that it is possible to decode beyond the design distance for many codes. On the basis of simulation, the correction capability and plots showing the probability of uncorrectable erasures are provided. For example, for a (255,250) RS code, the method is able to correct 19 bit erasures more than would be expected using conventional bounded distance decoding.

There has recently been considerable work done on decoding beyond the design distance. Sudan [1] then Guruswami-Sudan [2] published work on decoding beyond the $d/2$ bound. The algorithm was put in a computationally efficient form by Kötter [3] and Roth-Ruckenstein [4]. These works rely on some algebraic geometry. The method of this paper, on the other hand, is based on conventional syndrome decoding. While not providing necessarily the same capability as the Guruswami-Sudan method (for example, it deals only with erasures and not errors), the method of this paper is quite straightforward to implement and does not require a background in algebraic geometry.

In the case that the number of erasures exceeds the design distance there are an insufficient number of conventional syndrome equations, so that additional syndrome equations must be created to solve for more erasures. These are obtained by exploiting the fact that $(x+y)^2 = x^2 + y^2$ for $x, y \in GF(2)$. If

$$X_0 \mathbf{b} = \mathbf{s}_0$$

is a matrix equation representing the error-value problem (for erasure correction), then it is shown that additional

equations can be obtained of the form

$$\begin{bmatrix} X_0 \\ X_0^{\cdot 2} \\ X_0^{\cdot 4} \\ \vdots \end{bmatrix} \mathbf{b} = \begin{bmatrix} \mathbf{s}_0 \\ \mathbf{s}_0^{\cdot 2} \\ \mathbf{s}_0^{\cdot 4} \\ \vdots \end{bmatrix}$$

where $X^{\cdot n}$ represents element-by-element exponentiation of the elements of X. The augmented equation can be solved using conventional Gaussian elimination.

As the paper shows, it is also possible to reduce the computational complexity. This is accomplished by recognizing that the matrix has elements of Vandermonde structure in it, when some correction terms are withdrawn. Using a Vandermonde solver and the matrix inversion lemma, the decoding complexity can be reduced to $O(n^2)$.

Table 1 shows the erasure correction capability of some high-rate RS codes, where ν_d is the number of erasures the method is able to provide, and $\nu_d - (n-k)$ indicates the improved capability over conventional decoding algorithms. Figure 1 shows some simulation results, indicating that even when the number of erasures exceeds the capability of this code, it is probable that effective decoding can nevertheless be obtained.

Table 1: Performance of some high-rate codes

(n,k)	b_{opt}	ν_d	$\nu_d-(n-k)$
(7,3)	6	5	1
(7,4)	3	4	1
(7,5)	6	3	1
(7,6)	2	2	1
(15,10)	1	7	2
(15,11)	14	5	1
(15,12)	12	3	0
(15,13)	5	3	1
(15,14)	2	2	1
(31,25)	6	14	8
(31,26)	23	12	7
(31,27)	15	7	3
(31,28)	26	4	1
(31,29)	30	3	1
(31,30)	3	2	1
(63,57)	21	13	7
(63,58)	13	14	9
(63,59)	13	9	5
(63,60)	12	5	2
(63,61)	62	3	1
(63,62)	51	2	1
(127,121)	104	20	14
(127,122)	113	19	14
(127,123)	109	12	8
(127,124)	31	7	4
(127,125)	103	3	1
(127,126)	73	1	0
(255,250)	137	24	19
(255,251)	181	17	13
(255,252)	208	9	6
(255,253)	56	3	1
(255,254)	239	1	0

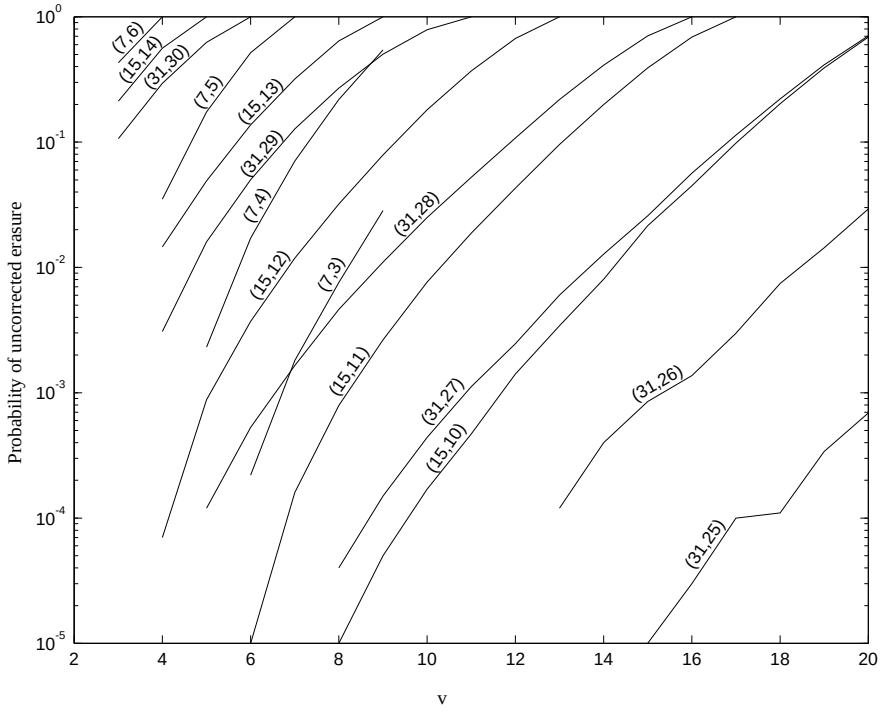

Figure 1: Probability of uncorrected erasure

References

[1] M. Sudan, "Decoding of reed-solomon codes beyond the error-correction bound," *J. Complexity*, vol. 13, pp. 180–193, 1997.

[2] V. Guruswami and M. Sudan, "Improved decoding of reed-solomon codes and algebraic geometry codes," *IEEE Trans. Information Theory*, vol. 45, pp. 1757–1767, Sept. 1999.

[3] R. Kötter, "Fast generalized minimum-distance decoding of algebraic-geometry and reed-solomon codes," *IEEE Trans. Information Theory*, vol. 42, pp. 721–736, May 1996.

[4] R. Roth and G. Ruckenstein, "Efficient decoding of reed-solomon codes beyond half the minimum distance," *IEEE Trans. Information Theory*, vol. 46, pp. 246–257, Jan. 2000.